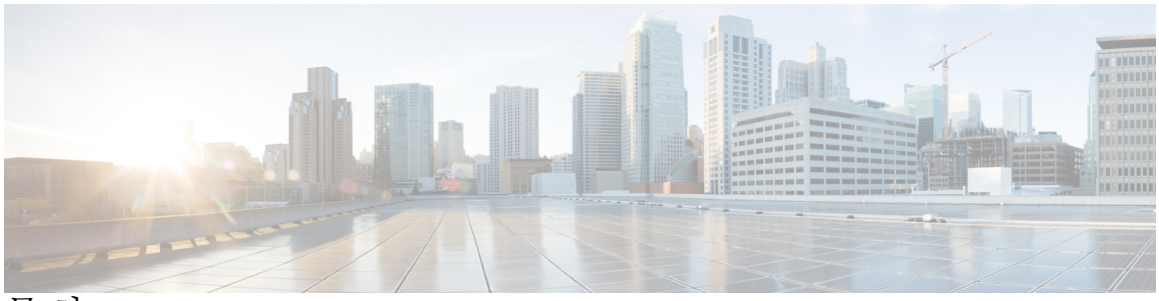
CLI 설명서 1: Cisco ASA Series 일반 운영 CLI 구성 가이드, 9.10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

가이드 정보

다음 주제에서는 이 가이드를 사용하는 방법을 설명합니다.

문서 목적

이 가이드는 CLI(Command Line Interface)를 사용하여 Cisco ASA Series의 일반적인 운영을 구성하는 것을 지원하기 위해 마련되었습니다. 여기서는 모든 기능을 다루기보다는 가장 대표적인 구성 시나리오에 대해서만 설명합니다.

웹 기반 GUI 애플리케이션인 ASDM(Adaptive Security Device Manager)을 사용하여 ASA를 구성하고 모니터링할 수도 있습니다. ASDM에는 몇 가지 일반적인 구성 시나리오를 안내하는 구성 마법사와 특수한 시나리오에 대한 온라인 도움말이 포함되어 있습니다.

이 가이드에서 "ASA"라는 용어는 별도로 지정하지 않는 한, 일반적으로 지원되는 모델에 적용됩니다.

관련 문서

자세한 내용은 http://www.cisco.com/go/asadocs에서 Navigating the Cisco ASA Series Documentation(Cisco ASA Series 설명서 찾기)을 참조하십시오.

문서 표기 규칙

이 문서는 다음 텍스트 표기, 표시 및 경고 규칙을 따릅니다.

가이드 정보

텍스트 표기 규칙

표기 규칙	표시
boldface	명령, 키워드, 버튼 레이블, 필드 이름 및 사용자 입력 텍스트는 **boldface**에 나타납니다. 메뉴 기반 명령의 경우, 명령에 대한 전체 경로가 표시됩니다.
기울임꼴	제공하는 값에 대한 변수는 기울임꼴 서체로 표시됩니다. 기울임꼴 유형은 문서 제목 및 일반적인 강조 시에도 사용됩니다.
monospace	시스템에 표시되는 터미널 세션 및 정보는 monospace 유형으로 표시됩니다.
{x | y | z}	필수 대체 키워드는 중괄호로 묶어 세로 선으로 구분합니다.
[ ]	대괄호로 묶인 요소는 선택적 요소입니다.
[x | y | z]	선택적 대체 키워드는 대괄호로 묶어 세로 선으로 구분합니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에도 표시됩니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 숫자 기호(#)는 코멘트 행을 나타냅니다.

독자 알림

이 문서에서는 독자에게 알리기 위해 다음 사항을 사용합니다.

참고 독자가 주목해야 하는 내용을 의미합니다. 참고에는 유용한 제안이나 해당 설명서에서 다루지 않는 자료에 대한 참조 정보가 포함됩니다.

팁 다음 정보가 문제를 해결하는 데 도움이 된다는 것을 의미합니다.

주의 독자가 유의해야 하는 내용임을 의미합니다. 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 한다는 내용이 포함됩니다.

간편한 방법 설명한 작업이 시간을 절약함을 의미합니다. 단락에서 설명한 작업을 수행함으로써 시간을 절약할 수 있습니다.

경고! 독자에게 경고하는 내용을 의미합니다. 이러한 상황에서는 신체 상해로 이어질 수 있는 작업을 수행해야 할 수 있습니다.

통신, 서비스 및 추가 정보

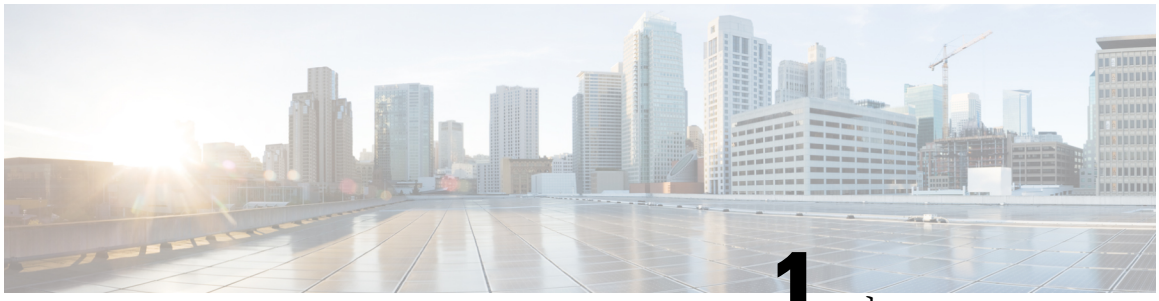
- Cisco에서 시기에 맞는 관련된 정보를 받으려면 Cisco Profile Manager에 로그인합니다.
- 중요한 기술로 원하는 비즈니스 결과를 얻으려면 Cisco Services를 참조하십시오.
- 서비스 요청을 제출하려면 Cisco 지원을 참조하십시오.
- 안전하고 검증된 엔터프라이즈급 앱, 제품, 솔루션 및 서비스를 검색하고 찾아보려면 Cisco Marketplace를 참조하십시오.
- 일반 네트워킹, 교육 및 인증서 제목을 얻으려면 Cisco Press를 참조하십시오.
- 특정 제품 또는 제품군에 대한 보증 정보를 찾으려면 Cisco Warranty Finder에 액세스합니다.

Cisco Bug Search Tool

Cisco BST(Bug Search Tool)는 Cisco 제품 및 소프트웨어에 있는 결함 및 취약점의 종합적인 목록을 유지관리하는 Cisco 버그 추적 시스템에 대한 게이트웨이 역할을 하는 웹 기반 툴입니다. BST에서는 제품 및 소프트웨어에 대한 자세한 결함 정보를 제공합니다.

I 부

ASA 시작하기



1 장

Cisco ASA 소개

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 장치 기능을 하나의 디바이스에서 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다.

하드웨어 및 소프트웨어 호환성

지원되는 하드웨어 및 소프트웨어의 전체 목록을 보려면 Cisco ASA 호환성을 참조하십시오.

VPN 호환성

지원되는 VPN 플랫폼, Cisco ASA Series를 참조하십시오.

새로운 기능

이 섹션에는 각 릴리스의 새로운 기능이 나와 있습니다.

참고 syslog 메시지 가이드에는 새 syslog 메시지, 변경된 syslog 메시지, 사용이 중단된 syslog 메시지가 나와 있습니다.

ASA 9.10(1)의 새로운 기능

릴리스 날짜: **2018**년 **10**월 **25**일

기능	설명
플랫폼 기능	
Azure에 대한 ASAv VHD 맞춤형 이미지	이제 Cisco에서 사용 가능한 압축된 VHD 이미지를 사용하여 Azure에서 고유한 맞춤형 ASAv 이미지를 생성할 수 있습니다. VHD 이미지를 사용하여 구축하려면 Azure 스토리지 어카운트에 VHD 이미지를 업로드합니다. 그런 다음, 업로드된 디스크 이미지 및 Azure Resource Manager 템플릿을 사용하여 매니지드 이미지를 생성할 수 있습니다. Azure 템플릿은 리소스 설명 및 파라미터 정의를 포함하는 JSON 파일입니다.
DPDK에 대한 ASAv 지원	DPDK(Dataplane Development Kit)는 폴링 모드 드라이버를 사용하여 ASAv의 데이터 플레인에 통합됩니다.
FirePOWER 모듈 버전 6.3에 대한 ISA 3000 지원	이전에는 FirePOWER 5.4 버전이 지원되었습니다.
방화벽 기능	
Cisco Umbrella 지원	Cisco Umbrella로 DNS 요청을 리디렉션하기 위해 디바이스를 구성할 수 있어 Cisco Umbrella에 정의되어 있는 사용자의 엔터프라이즈 보안 정책을 사용자 연결에 적용할 수 있습니다. FQDN을 기반으로 연결을 허용하거나 차단할 수 있습니다. 또는 의심스러운 FQDN의 경우 URL 필터링을 수행할 수 있는 Cisco Umbrella 지능형 프록시로 사용자를 리디렉션할 수 있습니다. Umbrella 구성은 DNS 검사 정책의 일부입니다. 신규/수정된 명령: **umbrella**, **umbrella-global**, **token**, **public-key**, **timeout edns**, **dnscrypt**, **show service-policy inspect dns detail**
MSISDN 및 선택 모드 필터링, 재생 방지 및 사용자 스푸핑 보호를 위한 GTP 검사 개선 사항	이제 MSISDN(Mobile Station International Subscriber Directory Number) 또는 선택 모드를 기반으로 PDP 상황 생성 메시지를 삭제하기 위해 GTP 검사를 구성할 수 있습니다. 또한 재생 방지 및 사용자 스푸핑 보호를 구현할 수 있습니다. 신규/수정된 명령: **anti-replay**, **gtp-u-header-check**, **match msisdn**, **match selection-mode**
TCP 상태 우회에 대한 기본 유휴 시간 제한	TCP 상태 우회 연결에 대한 기본 유휴 시간 제한은 이제 1시간이 아닌 2분입니다.

기능	설명
컷스루 프록시 로그인 페이지에서 로그아웃 버튼 제거에 대한 지원	사용자 ID 정보(AAA 인증 리스너)를 얻기 위해 컷스루 프록시를 구성하는 경우, 이제 페이지에서 로그아웃 버튼을 제거할 수 있습니다. 사용자가 NAT 디바이스 뒤에서 연결되어 있으며 IP 주소로 구별할 수 없는 경우 이러한 지원이 유용합니다. 한 명의 사용자가 로그아웃하면 해당 IP 주소의 모든 사용자가 로그아웃됩니다. 신규/수정된 명령: **aaa authentication listener no-logout-button** *9.8(3)*의 경우도 마찬가지입니다.
Trustsec SXP 연결 구성 가능 삭제 보류 타이머	기본 SXP 연결 보류 타이머는 120초입니다. 이제 120~64000초 사이로 이 타이머를 구성할 수 있습니다. 신규/수정된 명령: **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections** *9.8(3)*의 경우도 마찬가지입니다.
투명 모드에서 NATed 플로우 오프로드에 대한 지원	플로우 오프로드(**flow-offload enable** 및 **set connection advanced-options flow-offload** 명령)를 사용 중인 경우 오프로드된 플로우는 이제 투명 모드에서 NAT를 필요로 하는 플로우를 포함할 수 있습니다.
Firepower 4100/9300 ASA 논리적 디바이스에 대한 투명 모드 구축 지원	이제 Firepower 4100/9300에 ASA를 구축할 때 투명 또는 라우티드 모드를 지정할 수 있습니다. 신규/수정된 FXOS 명령: **enter bootstrap-key FIREWALL_MODE**, **set value routed**, **set value transparent**
VPN 기능	
레거시 SAML 인증에 대한 지원	CSCvg65072에 대한 수정 사항이 포함된 ASA를 구축하는 경우, 기본 SAML 동작은 AnyConnect 4.4 또는 4.5에서 지원되지 않는 임베드된 브라우저를 사용하는 것입니다. 따라서 AnyConnect 4.4 또는 4.5를 계속 사용하려면 레거시 외부 브라우저 SAML 인증 방법을 활성화해야 합니다. 보안 제한상의 이유로, 이 옵션은 AnyConnect 4.6 이상 버전으로 마이그레이션하기 위한 임시 계획에 포함된 경우에만 사용하십시오. 이 옵션은 가까운 시일 내에 사용이 중단될 예정입니다. 신규/수정된 명령: **saml external-browser** *9.8(3)*의 경우도 마찬가지입니다.
AnyConnect VPN 원격 액세스 연결에 대한 DTLS 1.2 지원	RFC- 6347에 설명된 대로 현재 지원되는 DTLS 1.0(1.1 버전 번호는 DTLS에 사용되지 않음) 외에 이제 DTLS 1.2가 AnyConnect 원격 액세스에 지원됩니다. 이 버전은 5506-X, 5508-X 및 5516-X를 제외한 모든 ASA 모델에 적용되며 ASA가 클라이언트가 아니라 서버로서 작동할 때 적용됩니다. DTLS 1.2는 추가 암호뿐만 아니라 모든 현재 TLS/DTLS 암호와 더 큰 쿠키 크기를 지원합니다. 신규/수정된 명령: **show run ssl**, **show vpn-sessiondb detail anyconnectssl cipher**, **ssl server-version**
고가용성 및 확장성 기능	

기능	설명
Firepower 4100/9300에 대한 클러스터 제어 링크의 맞춤화 가능한 IP 주소	기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 이제 FXOS에서 클러스터를 구축하는 경우 네트워크를 설정할 수 있습니다. 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 따라서 이제 FXOS에서 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외하고 클러스터 제어 링크의 맞춤형 /16 서브넷을 설정할 수 있습니다. 신규/수정된 FXOS 명령: **set cluster-control-link network**
Firepower 9300 섀시당 클러스터 유닛의 병렬 조인	Firepower 9300에서는 이 기능을 통해 섀시에서 보안 모듈이 클러스터에 동시에 조인하게 되므로 트래픽이 모듈 간에 고르게 분산됩니다. 모듈이 다른 모듈보다 훨씬 먼저 조인하는 경우, 다른 모듈이 로드를 아직 공유할 수 없기 때문에 이 모듈은 원하는 트래픽보다 더 많은 트래픽을 받을 수 있습니다. 신규/수정된 명령: **unit parallel-join**
이제 클러스터 인터페이스 디바운스 시간이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다.	인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA에서는 **health-check monitor-interface debounce-time** 명령 또는 ASDM **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** 화면에 지정되어 있는 밀리초 동안 대기합니다. 이제 이 기능이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다. 예를 들어 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다. 명령은 수정하지 않았습니다.
Microsoft Azure Government Cloud에서 ASAv용 액티브/백업 고가용성	액티브 ASAv 장애 때문에 Microsoft Azure 퍼블릭 클라우드에서 백업 ASAv로 시스템의 자동 장애 조치를 트리거하게 만드는 스테이트리스 액티브/백업 솔루션을 이제 Azure Government Cloud에서 사용할 수 있습니다. 신규 또는 수정된 명령: **failover cloud** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Failover(**장애 조치**)** > **Status(**상태**)** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Failover(**장애 조치**)** > **History(**기록**)**
인터페이스 기능	
Firepower 2100/4100/9300에 대한 수퍼바이저 연결을 표시하기 위한 **show interface ip brief** 및 **show ipv6 interface** 출력 개선 사항	Firepower 2100/4100/9300의 경우 명령의 출력이 인터페이스의 수퍼바이저 연결 상태를 표시하도록 개선되었습니다. 신규/수정된 명령: **show interface ip brief**, **show ipv6 interface**

기능	설명
Firepower 2100에서 **set lacp-mode** 명령이 **set port-channel-mode**로 변경됨	Firepower 4100/9300의 명령 사용법과 일치하도록 **set lacp-mode** 명령이 **set port-channel-mode**로 변경되었습니다. 신규/수정된 FXOS 명령: **set port-channel-mode**
관리 및 트러블슈팅 기능	
Firepower 2100에서 NTP 인증에 대한 지원	이제 FXOS에서 SHA1 NTP 서버 인증을 구성할 수 있습니다. 신규/수정된 FXOS 명령: **enable ntp-authentication, set ntp-sha1-key-id, set ntp-sha1-key-string** 신규/수정된 Firepower Chassis Manager 화면: **Platform Settings(**플랫폼 설정**)** > **NTP** 신규/수정된 옵션: **NTP Server Authentication: Enable(NTP** 서버 인증**:** 활성화**)** 확인란, **Authentication Key(**인증 키**)** 필드, **Authentication Value(**인증 값**)** 필드
ACL을 사용하지 않고 일치하는 IPv6 트래픽에 대한 패킷 캡처 지원	**capture** 명령에 **match** 키워드를 사용하는 경우, **any** 키워드는 IPv4 트래픽하고만 일치합니다. 이제는 IPv4 또는 IPv6 트래픽을 캡처하기 위해 **any4**와 **any6** 키워드를 지정할 수 있습니다. **any** 키워드는 IPv4 트래픽하고만 계속 일치합니다. 신규/수정된 명령: **capture match**
Firepower 2100의 FXOS에 대한 SSH용 공개 키 인증 지원	비밀번호 인증과 함께 또는 비밀번호 인증 대신 공개 키 인증을 사용할 수 있도록 SSH 키를 설정할 수 있습니다. 신규/수정된 FXOS 명령: **set sshkey**
GRE 및 IPinIP 캡슐화에 대한 지원	내부 인터페이스에서 패킷 캡처를 수행할 때 ICMP, UDP, TCP 및 기타 대상에서 GRE 및 IPinIP 캡슐화를 표시하도록 명령의 출력이 개선되었습니다. 신규/수정된 명령: **show capture**
애플리케이션 캐시 할당을 제한하는 메모리 임계값의 활성화 지원	특정 메모리 임계값에 도달 시 애플리케이션 캐시 할당을 제한하여 디바이스의 관리 효율성 및 안정성을 유지하기 위한 메모리 예약이 가능하도록 할 수 있습니다. 신규/수정된 명령: **memory threshold enable, show run memory threshold,clear conf memory threshold**
RFC 5424 로깅 타임스탬프에 대한 지원	RFC 5424 형식에 따라 로깅 타임 스탬프를 활성화할 수 있습니다. 신규/수정된 명령: **logging timestamp**
TCB-IPS의 메모리 사용량을 표시하도록 지원	TCB-IPS에 대한 애플리케이션 수준 메모리 캐시를 표시합니다. 신규/수정된 명령: **show memory app-cache**

방화벽 기능 개요

방화벽은 외부 네트워크의 사용자가 내부 네트워크에 무단 액세스하는 것을 차단합니다. 또한 방화벽을 통해 내부 네트워크끼리도 보호할 수 있습니다. 이를테면 인사부 네트워크를 사용자 네트워크와 분리할 수 있습니다. 웹 또는 FTP 서버 같이 외부 사용자에게 제공해야 하는 네트워크 리소스가 있을 경우, 이러한 리소스를 방화벽 뒤에 있는 DMZ(*Demilitarized Zone*)라는 별도의 네트워크에 배치할 수 있습니다. 방화벽에서는 DMZ에 제한된 액세스를 허용하지만 DMZ에는 공용 서버만 포함되므로, 이곳에 공격이 발생할 경우 해당 서버에만 영향을 미치며 다른 내부 네트워크에서는 영향을 미치지 않습니다. 또한 특정 주소만 내보내도록 허용하거나, 인증이나 권한을 요청하거나, 외부 URL 필터링 서버와 조율하는 방식을 통해 내부 사용자가 외부 네트워크에 액세스(예: 인터넷 액세스)하는 것도 제어할 수 있습니다.

방화벽에 연결된 네트워크를 이야기할 때, 외부 네트워크는 방화벽 앞에 있는 네트워크, 내부 네트워크는 방화벽 뒤에서 보호되고 있는 네트워크, *DMZ*는 방화벽 뒤에 있으나 외부 사용자에게 제한된 액세스를 허용하는 네트워크를 말합니다. 그러나 ASA에서는 여러 가지 보안 정책으로 많은 인터페이스(예: 많은 내부 인터페이스, 여러 DMZ, 필요한 경우 더 많은 외부 인터페이스)를 구성할 수 있도록 지원하므로 이러한 용어는 일반적인 의미로만 사용됩니다.

보안 정책 개요

보안 정책은 어떤 트래픽이 방화벽을 통과하여 다른 네트워크에 액세스하도록 허용할지 여부를 결정합니다. 기본적으로 ASA에서는 내부 네트워크(상위 보안 수준)에서 외부 네트워크(하위 보안 수준)로 트래픽이 자유롭게 이동하도록 허용합니다. 트래픽에 몇 가지 조치를 취하여 보안 정책을 맞춤화할 수 있습니다.

액세스 목록 규칙으로 트래픽 허용 또는 거부

액세스 규칙을 적용하여 내부에서 외부로 나가는 트래픽을 제한하거나, 외부에서 내부로 들어오는 트래픽을 허용할 수 있습니다. 브리지 그룹 인터페이스의 경우 이더 타입 액세스 규칙을 적용하여 비 IP 트래픽을 허용할 수도 있습니다.

NAT 적용

NAT의 몇 가지 이점은 다음과 같습니다.

- 내부 네트워크에서 사설 주소를 사용할 수 있습니다. 사설 주소는 인터넷에서 라우팅할 수 없습니다.
- NAT는 다른 네트워크의 로컬 주소를 숨기므로 공격자가 호스트의 실제 주소를 알 수 없습니다.
- NAT는 IP 주소 중복을 지원하여 IP 라우팅 문제를 해결할 수 있습니다.

IP 프래그먼트 방지

ASA에서는 IP 프래그먼트 방지 기능을 제공합니다. 이 기능에서는 모든 ICMP 오류 메시지를 완전히 재조합하고 ASA를 통해 라우팅된 나머지 IP 프래그먼트를 가상으로 재조합하는 작업을 수행합니다.

보안 검사에 실패한 프래그먼트는 폐기되고 로깅됩니다. 가상 재조합 기능은 비활성화할 수 없습니다.

HTTP, HTTPS 또는 FTP 필터링 적용

액세스 목록을 사용하여 특정 웹 사이트 또는 FTP 서버에 대한 아웃바운드 액세스를 방지할 수는 있으나, 인터넷의 규모와 동적 특징을 감안했을 때 이러한 방식으로 웹 사용을 구성하고 관리하는 것은 실용적이지 않습니다.

ASA에서 Cloud Web Security를 구성하거나, URL 및 기타 필터링 서비스(예: ASA CX 또는 ASA FirePOWER)를 제공하는 ASA 모듈을 설치할 수 있습니다. ASA를 Cisco WSA(Web Security Appliance) 같은 외부 제품과 함께 사용할 수도 있습니다.

애플리케이션 감시 적용

사용자 데이터 패킷에 IP 주소 정보가 포함된 서비스 또는 동적으로 할당된 포트에서 보조 채널을 여는 서비스에는 검사 엔진이 필요합니다. 이러한 프로토콜의 경우 ASA에서 심층 패킷 검사를 수행해야 합니다.

지원되는 하드웨어 또는 소프트웨어 모듈에 트래픽 전송

일부 ASA 모델에서는 고급 서비스를 제공하기 위해 소프트웨어 모듈을 구성하거나 섀시에 하드웨어 모듈을 삽입할 수 있습니다. 이러한 모듈에서는 추가적인 트래픽 감시를 제공하며 구성된 정책을 바탕으로 트래픽을 차단할 수 있습니다. 이러한 모듈에 트래픽을 전송하여 이와 같은 고급 서비스를 이용할 수 있습니다.

QoS 정책 적용

음성과 비디오 등 일부 네트워크 트래픽은 긴 레이턴시를 허용하지 않습니다. QoS는 이러한 유형의 트래픽에 우선순위를 부여할 수 있는 기능입니다. QoS에서는 네트워크의 기능을 참조하여 선택된 네트워크 트래픽에 더 개선된 서비스를 제공할 수 있도록 합니다.

연결 제한 및 TCP 표준화 적용

TCP 및 UDP 연결과 초기 연결을 제한할 수 있습니다. 연결 및 초기 연결 수를 제한하면 DoS 공격을 방지할 수 있습니다. ASA에서는 초기 제한을 사용하여 TCP 가로채기를 시작하며, 이렇게 하면 TCP SYN 패킷을 인터페이스에 플러딩하여 시행된 DoS 공격으로부터 내부 시스템을 보호할 수 있습니다. 원시 연결은 소스와 대상 간에 필요한 핸드셰이크를 완료하지 않은 연결 요청입니다.

TCP 표준화는 정상으로 보이지 않는 패킷을 폐기하기 위해 고안된 고급 TCP 연결 설정으로 이루어진 기능입니다.

위협 감지 활성화

위협 감지 검사 및 기본 위협 감지를 구성할 수 있으며, 통계를 활용하여 위협을 분석하는 방법도 구성할 수 있습니다.

기본 위협 감지 기능에서는 공격(예: DoS 공격)과 관련될 가능성이 있는 활동을 감지하고, 시스템 로그 메시지를 자동으로 전송합니다.

일반적인 스캐닝 공격은 서브넷의 모든 IP 주소에 대한 액세스 가능성을 테스트하는 호스트로 구성됩니다(서브넷의 여러 호스트를 통해 스캔하거나 호스트 또는 서브넷의 여러 포트를 스위핑함). 스캐닝 위협 감지 기능은 호스트에서 스캔을 수행하는 시점을 결정합니다. 트래픽 시그니처를 기반으로 하는 IPS 스캔 감지와는 달리 ASA 스캔 위협 감지 기능은 스캔 활동에 대해 분석할 수 있는 호스트 통계가 포함된 폭넓은 데이터베이스를 유지 관리합니다.

호스트 데이터베이스는 반환 활동이 없는 연결, 닫힌 서비스 포트 액세스, 취약한 TCP 동작(예: 무작위가 아닌 IPID), 기타 여러 동작 등 의심스러운 활동을 추적합니다.

공격자에 관한 시스템 로그 메시지를 보내도록 ASA를 구성하거나 호스트를 자동으로 차단할 수 있습니다.

방화벽 모드 개요

ASA는 서로 다른 2개의 방화벽 모드에서 실행됩니다.

- 라우팅됨
- 투명

라우팅 모드에서 ASA는 네트워크의 라우터 홉으로 간주됩니다.

투명 모드에서 ASA는 "BITW(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하며, 라우터 홉으로 간주되지 않습니다. ASA는 "브리지 그룹"의 내부 및 외부 인터페이스에서 동일한 네트워크에 연결됩니다.

투명 방화벽을 사용하여 네트워크 컨피그레이션을 간소화할 수 있습니다. 공격자에게 방화벽이 보이지 않게 하려는 경우 투명 모드가 유용합니다. 라우팅 모드에서 차단할 트래픽에도 투명 방화벽을 사용할 수 있습니다. 예를 들어 투명 방화벽에서는 EtherType 액세스 목록을 사용한 멀티캐스트 스트림을 지원합니다.

라우팅 모드는 통합 라우팅 및 브리징을 지원하므로 라우팅 모드에서 브리지 그룹을 구성하고 브리지 그룹과 일반 인터페이스 간의 경로를 구성할 수도 있습니다. 라우팅 모드에서 투명 모드 기능을 복제할 수 있습니다. 다중 상황 모드 또는 클러스터링이 필요하지 않은 경우, 라우팅 모드를 대신 사용하는 방법을 고려할 수 있습니다.

상태 저장 감시 개요

ASA를 통과하는 모든 트래픽은 Adaptive Security Algorithm으로 감시를 받아 허용되거나 거부됩니다. 간단한 패킷 필터로 올바른 소스 주소, 목적지 주소, 포트를 확인할 수 있으나 패킷 시퀀스 또는 플래그가 올바른지는 확인할 수 없습니다. 또한 필터의 경우 해당 필터를 기준으로 모든 패킷을 확인하므로, 프로세스가 느릴 수 있습니다.

참고 TCP 상태 우회 기능을 사용하면 패킷 플로우를 사용자 정의할 수 있습니다.

그러나 ASA와 같은 스테이트풀 방화벽에서는 패킷의 상태를 고려합니다.

- 새 연결인가?

  새 연결일 경우 ASA에서 액세스 목록을 기준으로 패킷을 확인하고 기타 작업을 수행하여 패킷을 허용 또는 거부할지 결정해야 합니다. 이러한 확인을 위해 세션의 첫 번째 패킷은 "세션 관리 경로"를 통과하며, 트래픽의 유형에 따라 "컨트롤 플레인 경로"를 통과할 수도 있습니다.

  세션 관리 경로는 다음 작업을 담당합니다.

  - 액세스 목록 확인 수행
  - 경로 조회 수행
  - NAT 변환 할당(xlates)
  - "빠른 경로"에 세션 설정

  ASA에서는 TCP 트래픽의 빠른 경로에서 순방향 및 역방향 플로우를 생성합니다. 또한 ASA에서는 UDP, ICMP 등 연결 없는 프로토콜에 대한 연결 상태 정보를 생성하여(ICMP 검사를 활성화하는 경우) 해당 프로토콜에서도 빠른 경로를 사용할 수 있게 합니다.

  참고 ASA의 경우 SCTP와 같은 다른 IP 프로토콜에 대해서는 역방향 경로 플로우를 생성하지 않습니다. 결과적으로 이러한 연결을 참조하는 ICMP 오류 패킷은 폐기됩니다.

  레이어 7 감시(패킷 페이로드를 감시하거나 변경해야 함)가 필요한 일부 패킷은 컨트롤 플레인 경로로 전달됩니다. 레이어 7 감시 엔진의 경우 둘 이상의 채널(데이터 채널에서는 알려진 포트 번호를 사용하고, 제어 채널에서는 세션마다 다른 포트 번호를 사용함)이 포함된 프로토콜이 필요합니다. 이러한 프로토콜에는 FTP, H.323, SNMP가 포함됩니다.

- 설정되어 있는 연결인가?

  이미 연결이 설정되어 있는 경우 ASA에서는 패킷을 다시 확인할 필요가 없습니다. 일치하는 대부분의 패킷은 양방향에서 모두 “빠른” 경로를 통과할 수 있습니다. 빠른 경로에서 다음 작업을 담당합니다.

  - IP 체크섬 확인
  - 세션 조회
  - TCP 시퀀스 번호 확인
  - 기존 세션을 바탕으로 NAT 변환
  - 레이어 3 및 레이어 4 헤더 조정

  레이어 7 검사가 필요한 프로토콜의 데이터 패킷도 빠른 경로를 통과할 수 있습니다.

  설정된 세션 패킷 중 일부는 계속 세션 관리 경로 또는 컨트롤 플레인 경로를 통해 전달되어야 합니다. 세션 관리 경로를 통과하는 패킷에는 감시 또는 콘텐츠 필터링이 필요한 HTTP 패킷이 포함되어 있습니다. 컨트롤 플레인 경로를 통과하는 패킷에는 레이어 7 검사가 필요한 프로토콜의 제어 패킷이 포함되어 있습니다.

VPN 기능 개요

VPN은 사설 연결처럼 보이는 TCP/IP 네트워크(예: 인터넷) 전반의 보안 연결입니다. 이 보안 연결을 터널이라고 부릅니다. ASA에서는 터널링 프로토콜을 사용하여 보안 파라미터를 협상하고, 터널을 생성 및 관리하고, 패킷을 캡슐화하고, 터널을 통해 패킷을 주고받고, 캡슐화를 해제합니다. ASA에서는 양방향 터널 엔드포인트로서의 기능을 수행합니다. 플레인 패킷을 수신하고, 이를 캡슐화한 다음, 해당 패킷의 캡슐화가 해제되고 최종 대상으로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 대상으로 전송할 수도 있습니다. ASA에서는 다양한 표준 프로토콜을 호출하여 이러한 기능을 구현합니다.

ASA에서는 다음과 같은 기능을 수행합니다.

- 터널 설정
- 터널 매개변수 협상
- 사용자 인증
- 사용자 주소 지정
- 데이터 암호화 및 해독
- 보안 키 관리
- 터널을 통한 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로 데이터 전송 인바운드 및 아웃바운드 관리

ASA에서는 다양한 표준 프로토콜을 호출하여 이러한 기능을 구현합니다.

보안 상황 개요

단일 ASA를 보안 컨텍스트라고 하는 다중 가상 장치로 분할할 수 있습니다. 각 컨텍스트는 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스입니다. 다중 컨텍스트는 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 다중 컨텍스트 모드에서는 라우팅 테이블, 방화벽 기능, IPS, 관리 기능을 비롯한 다양한 기능이 지원되지만 몇 가지 기능은 지원되지 않습니다. 자세한 내용은 기능 장을 참조하십시오.

다중 상황 모드에서는 ASA에 보안 정책, 인터페이스 및 독립형 디바이스에서 구성할 수 있는 거의 모든 옵션을 식별하는 각 상황에 대한 구성이 포함됩니다. 시스템 관리자는 시스템 컨피그레이션(단일 모드 컨피그레이션과 마찬가지로 시작 컨피그레이션)에서 컨텍스트를 구성하여 컨텍스트를 추가하고 관리할 수 있습니다. 시스템 구성은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 컨피그레이션은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 컨텍스트 다운로드) 관리 컨텍스트로 지정된 컨텍스트 중 하나를 사용합니다.

관리자 컨텍스트는 다른 모든 컨텍스트와 같지만 예외 사항이 있습니다. 관리자 컨텍스트에 로그인한 사용자는 시스템 관리자 권한을 갖게 되며, 시스템 및 기타 모든 컨텍스트에 액세스할 수 있습니다.

ASA 클러스터링 개요

ASA 클러스터링을 사용하면 여러 개의 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

마스터 유닛에서만 모든 컨피그레이션(부트스트랩 컨피그레이션 제외)을 수행해야 합니다. 그러면 멤버 유닛에 컨피그레이션이 복제됩니다.

특별 서비스 및 레거시 서비스

일부 서비스의 설명서는 주요 컨피그레이션 가이드 및 온라인 도움말 이외의 위치에 있습니다.

특별 서비스 설명서

특별 서비스에서는 ASA와 기타 Cisco 제품 간의 상호 운용을 지원합니다. 전화 서비스용 보안 프록시를 제공하거나(Unified Communications), 봇넷 트래픽 필터링을 Cisco 업데이트 서버의 동적 데이터베이스와 결합하여 제공하거나, Cisco Web Security Appliance용 WCCP 서비스를 제공하는 경우를 예로 들 수 있습니다. 이러한 특별 서비스 중 일부는 별도의 설명서에서 다룹니다.

- Cisco ASA 봇넷 트래픽 필터 가이드Cisco ASA 봇네트(botnet) 트래픽 필터 가이드
- Cisco ASA NetFlow 구현 가이드
- Cisco ASA Unified Communications 가이드
- Cisco ASA WCCP 트래픽 리디렉션 가이드
- SNMP 버전 3 도구 구현 가이드SNMP 버전 3 툴 구현 가이드

레거시 서비스 설명서

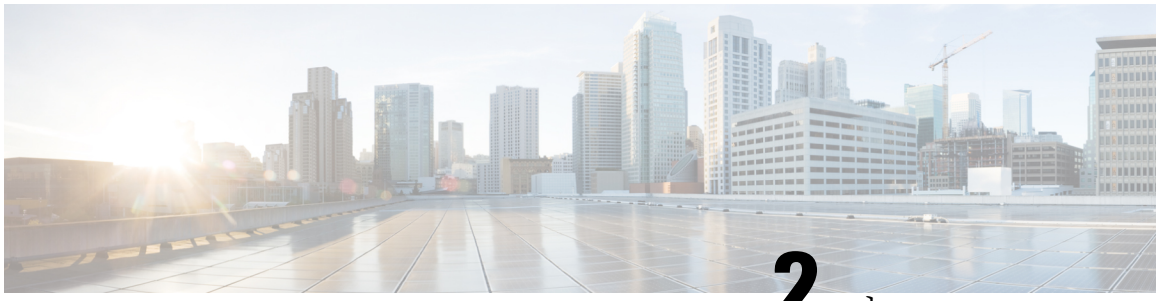
레거시 서비스는 ASA에서 계속 지원되지만, 해당 서비스를 대체하는 더 우수한 서비스가 제공될 수 있습니다. 레거시 서비스는 별도의 가이드에서 다룹니다.

Cisco ASA 레거시 기능 가이드

이 가이드는 다음과 같은 장으로 구성되어 있습니다.

- RIP 구성
- 네트워크 액세스용 AAA 규칙
- IP 스푸핑 방지(**ip verify reverse-path**), 프래그먼트 크기 구성(**fragment**), 원치 않는 연결 차단(**shun**), TCP 옵션 구성(ASDM용) 및 기본 IPS 지원을 위한 IP 감사 구성(**ip audit**) 등의 보호 툴 사용

- 필터링 서비스 구성



2 장

시작하기

이 장에서는 Cisco ASA를 시작하는 방법을 설명합니다.

명령줄 인터페이스용 콘솔 액세스

초기 컨피그레이션의 경우에는 콘솔 포트에서 CLI에 직접 액세스합니다. 나중에 텔넷이나 SSH를 사용하여 #unique_32에 따라 원격 액세스를 구성할 수 있습니다. 시스템이 이미 다중 상황 모드에 있는 경우 콘솔 포트에 액세스하면 시스템 실행 영역으로 이동합니다.

참고 ASAv 콘솔 액세스에 대한 내용은 ASAv 빠른 시작 설명서를 참조하십시오.

어플라이언스 콘솔 액세스

어플라이언스 콘솔에 액세스하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 제공된 콘솔 케이블을 사용하여 컴퓨터를 콘솔 포트에 연결하고, 전송 속도 9600, 8개 데이터 비트, 패리티 없음, 1개 정지 비트, 흐름 제어 없음으로 설정된 터미널 에뮬레이터를 사용하여 콘솔에 연결합니다.

콘솔 케이블에 대한 자세한 내용은 ASA 하드웨어 가이드를 참조하십시오.

단계 **2** **Enter** 키를 누르면 다음 프롬프트가 표시됩니다.

```
ciscoasa>
```

이 프롬프트는 현재 사용자 EXEC 모드에 있음을 의미합니다. 사용자 EXEC 모드에서는 기본 명령만 사용 가능합니다.

단계 **3** 특권 EXEC 모드에 액세스합니다.

enable

비밀번호를 묻는 프롬프트가 표시됩니다. 기본적으로 비밀번호는 비어 있으며 계속하려면 **Enter** 키를 누릅니다. enable 비밀번호를 변경하려면 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정, 681 페이지를 참조하십시오.

예제:

```
ciscoasa> enable
Password:
ciscoasa#
```

모든 비 컨피그레이션 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 컨피그레이션 모드를 입력할 수도 있습니다.

특권 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

단계 **4** 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

예제:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

전역 구성 모드에서 ASA 구성을 시작할 수 있습니다. 전역 컨피그레이션 모드를 종료하려면 **exit**, **quit** 또는 **end** 명령을 입력합니다.

Firepower 2100 콘솔 액세스

Firepower 2100 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. FXOS CLI에서 ASA 콘솔에 연결한 다음 반대로 다시 연결할 수 있습니다. SSH를 통해 FXOS에 연결하는 경우 ASA CLI에 연결할 수도 있습니다. SSH로부터의 연결은 콘솔 연결이 아니므로 FXOS SSH 연결로부터의 여러 ASA 연결을 사용할 수 있습니다. 마찬가지로, SSH를 통해 ASA에 연결하는 경우 FXOS CLI에 연결할 수 있습니다.

시작하기 전에

한 번에 하나의 콘솔 연결만 유지할 수 있습니다. FXOS 콘솔에서 ASA 콘솔에 연결하는 경우 이 연결은 텔넷 또는 SSH 연결과 달리 영구 콘솔 연결입니다.

프로시저

단계 **1** 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 2100은 DB-9~RJ-45 시리얼 케이블과 함께 제공되므로 연결을 설정하려면 서드파티 시리얼-USB 케이블이 필요합니다. 운영 체제에 필요한 모든 USB 시리얼 드라이버를 설치해야 합니다. 다음 시리얼 설정을 사용하십시오.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

FXOS CLI에 연결합니다. 사용자 크리덴셜을 입력합니다. 기본적으로 **admin** 사용자 및 기본 비밀번호인 **Admin123**으로 로그인할 수 있습니다.

단계 **2** ASA에 연결합니다.

connect asa

예제:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

단계 **3** 특권 EXEC 모드에 액세스합니다.

enable

비밀번호를 묻는 메시지가 표시됩니다. 기본적으로 비밀번호는 비어 있으며 계속하려면 **Enter** 키를 누릅니다. enable 비밀번호를 변경하려면 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정, 681 페이지를 참조하십시오.

예제:

```
ciscoasa> enable
Password:
ciscoasa#
```

모든 비 컨피그레이션 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 컨피그레이션 모드를 입력할 수도 있습니다.

특권 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

단계 **4** 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

예제:

```
ciscoasa# configure terminal
```

```
ciscoasa(config)#
```

전역 구성 모드에서 ASA 구성을 시작할 수 있습니다. 전역 컨피그레이션 모드를 종료하려면 **exit**, **quit** 또는 **end** 명령을 입력합니다.

단계 **5** FXOS 콘솔로 돌아가려면 **Ctrl+a**, **d**를 입력합니다.

단계 **6** ASA에서 SSH 액세스를 구성한 후 SSH를 통해 ASA에 연결하는 경우 FXOS CLI에 연결합니다.

connect fxos

FXOS에 대한 인증을 수행하라는 프롬프트가 표시됩니다. 기본 사용자 이름(**admin**)과 비밀번호(**Admin123**)를 사용합니다. ASA CLI로 돌아가려면 **exit**을 입력하거나 **Ctrl-Shift-6**, **x**를 입력합니다.

예제:

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

ASA 콘솔 액세스 - Firepower 4100/9300 섀시

초기 구성의 경우에는 Firepower 4100/9300 섀시 수퍼바이저에 연결(콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음, ASA 보안 모듈에 연결하여 명령줄 인터페이스에 액세스합니다.

프로시저

단계 **1** Firepower 4100/9300 섀시 수퍼바이저 CLI(콘솔 또는 SSH)에 연결한 다음, 세션을 ASA에 연결합니다.

connect module 슬롯 {**console** | **telnet**}

텔넷 연결 사용 시에는 동시에 여러 세션을 모듈에 연결할 수 있으며 연결 속도가 더 빠르다는 이점이 있습니다.

모듈에 처음 액세스할 때, FXOS 모듈 CLI에 액세스합니다. 그런 다음 ASA 애플리케이션에 연결해야 합니다.

connect asa

예제:

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

단계 **2** 가장 권한 수준이 높은 특권 EXEC 모드에 액세스합니다.

enable

비밀번호를 묻는 메시지가 표시됩니다. 기본적으로 비밀번호는 비어 있으며 계속하려면 **Enter** 키를 누릅니다. enable 비밀번호를 변경하려면 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정, 681 페이지를 참조하십시오.

예제:

```
asa> enable
Password:
asa#
```

모든 비 컨피그레이션 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 컨피그레이션 모드를 입력할 수도 있습니다.

특권 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

단계 **3** 전역 구성 모드를 시작합니다.

configure terminal

예제:

```
asa# configure terminal
asa(config)#
```

전역 구성 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

단계 **4** FXOS 모듈 CLI에 대한 애플리케이션 콘솔은 **Ctrl-a, d**를 입력하여 종료합니다.

문제 해결을 위해 FXOS 모듈 CLI를 사용할 수 있습니다.

단계 **5** FXOS CLI의 Supervisor(관리자) 수준으로 돌아갑니다.

콘솔을 종료합니다**.**

a) ~를 입력합니다.

텔넷 애플리케이션을 종료합니다.

b) 텔넷 애플리케이션을 종료하려면 다음을 입력합니다.

telnet>**quit**

텔넷 세션을 종료합니다**.**

a) **Ctrl-], .**를 입력합니다.

ASA 서비스 모듈 콘솔 액세스

초기 구성의 경우에는 스위치에 연결(콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음, ASASM에 연결하여 명령줄 인터페이스에 액세스합니다. 이 섹션에서는 ASASM CLI에 액세스하는 방법을 설명합니다.

연결 방법 소개

스위치 CLI에서 다음과 같은 두 가지 방법을 사용하여 ASASM에 연결할 수 있습니다.

- 가상 콘솔 연결 — **service-module session** 명령을 사용하여 ASASM에 대한 가상 콘솔 연결을 생성(실제 콘솔 연결의 이점과 제한 사항 모두 포함)합니다.

  혜택은 다음과 같습니다.

  - 다시 로드하더라도 연결이 유지되며 시간 초과되지 않습니다.
  - ASASM이 다시 로드되는 동안 연결을 유지하고 시작 메시지를 볼 수 있습니다.
  - ASASM에서 이미지를 로드할 수 없는 경우 ROMMON에 액세스할 수 있습니다.
  - 초기 비밀번호 컨피그레이션이 필요하지 않습니다.

  제한 사항은 다음과 같습니다.

  - 연결이 느립니다(9600보드).
  - 한 번에 하나의 콘솔 연결만 활성 상태로 유지할 수 있습니다.
  - **Ctrl-Shift-6**, **x**가 터미널 서버 프롬프트로 돌아가는 이스케이프 시퀀스인 경우 이 명령을 터미널 서버와 함께 사용할 수 없습니다. **Ctrl-Shift-6**, **x**는 ASASM 콘솔에서 벗어나 스위치 프롬프트로 돌아가는 시퀀스이기도 합니다. 따라서 이러한 상황에서 ASASM 콘솔을 종료하려는 경우 터미널 서버 프롬프트에 대한 모든 방법을 종료해야 합니다. 스위치에 터미널 서버를 다시 연결하는 경우 ASASM 콘솔 세션은 계속 활성화되어 있지만 스위치 프롬프트는 종료할 수 없게 됩니다. 콘솔에서 스위치 프롬프트로 돌아가려면 직접 직렬 연결을 사용해야 합니다. 이 경우 Cisco IOS 소프트웨어에서 터미널 서버 또는 스위치 이스케이프 문자를 변경하거나, 텔넷 **session** 명령을 대신 사용합니다.

  참고 ASASM에서 올바르게 로그아웃하지 않을 경우 콘솔 연결 상태가 계속 유지되어 의도한 시간보다 연결이 오래 지속될 수 있습니다. 다른 사람이 로그인하려면 기존 연결을 끊어야 합니다.

- 텔넷 연결 — **session** 명령을 사용하여 ASASM에 대한 텔넷 연결을 생성합니다.

  참고 새 ASASM에는 이 방법을 사용하여 연결할 수 없습니다. 이 방법을 사용하려면 ASASM에서 텔넷 로그인 비밀번호를 구성해야 합니다(기본 비밀번호 없음). **passwd** 명령을 사용하여 비밀번호를 설정하면 이 방법을 사용할 수 있습니다.

  혜택은 다음과 같습니다.

  - ASASM에 대해 여러 세션을 동시에 보유할 수 있습니다.
  - 텔넷 세션은 빠른 연결입니다.

  제한 사항은 다음과 같습니다.

  - ASASM이 다시 로드되면 텔넷 세션이 종료되고 시간이 초과될 수 있습니다.
  - 완전히 로드될 때까지는 ASASM에 액세스할 수 없습니다. ROMMON에 액세스할 수 없습니다.
  - 먼저 텔넷 로그인 비밀번호를 설정해야 합니다. 기본 비밀번호는 없습니다.

ASA 서비스 모듈에 로그인

초기 구성의 경우에는 스위치에 연결(스위치 콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음, ASASM에 연결하여 명령줄 인터페이스에 액세스합니다.

시스템이 이미 다중 상황 모드에 있는 경우 스위치에서 ASASM에 액세스하면 시스템 실행 영역으로 이동합니다.

나중에 텔넷이나 SSH를 사용하여 ASASM에 대한 직접 원격 액세스를 구성할 수 있습니다.

프로시저

단계 **1** 스위치에서 다음 중 하나를 수행합니다.

- 초기 액세스에 사용 가능한 방법 — 스위치 CLI에서 다음 명령을 입력하여 ASASM에 대한 콘솔 액세스 권한을 얻습니다.

  service-module session [**switch** {**1** | **2**}] **slot** *number*

  예:

  ```
  Router# service-module session slot 3
  ciscoasa>
  ```

  VSS에 있는 스위치의 경우 **switch** 인수를 입력합니다.

  모듈 슬롯 번호를 보려면 스위치 프롬프트에서 **show module** 명령을 입력합니다.

사용자 EXEC 모드에 액세스할 수 있습니다.

- 로그인 비밀번호 구성 후 사용 가능 — 스위치 CLI에서 텔넷에 다음 명령을 입력하여 백플레인을 통해 ASASM에 연결합니다.

  session [**switch** {**1** | | **2**}] **slot** *number* **processor 1**

  로그인 비밀번호를 묻는 메시지가 표시됩니다.

  ```
  ciscoasa passwd:
  ```

  예:

  ```
  Router# session slot 3 processor 1
  ciscoasa passwd: cisco
  ciscoasa>
  ```

  VSS에 있는 스위치의 경우 **switch** 인수를 입력합니다.

  다른 서비스 모듈에서 지원되는 **session** *slot* **processor 0** 명령은 ASASM에서 지원되지 않습니다. ASASM에는 프로세서 0이 없습니다.

  모듈 슬롯 번호를 보려면 스위치 프롬프트에서 **show module** 명령을 입력합니다.

  ASASM에 대한 로그인 비밀번호를 입력합니다. **passwd** 명령을 사용하여 비밀번호를 설정합니다. 비밀번호는 기본값이 없습니다.

  사용자 EXEC 모드에 액세스할 수 있습니다.

단계 **2** 가장 권한 수준이 높은 특권 EXEC 모드에 액세스합니다.

enable

비밀번호를 묻는 메시지가 표시됩니다. 기본적으로 비밀번호는 비어 있으며 계속하려면 **Enter** 키를 누릅니다. enable 비밀번호를 변경하려면 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정, 681 페이지를 참조하십시오.

예제**:**

```
ciscoasa> enable
Password:
ciscoasa#
```

모든 비 컨피그레이션 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 컨피그레이션 모드를 입력할 수도 있습니다.

특권 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

단계 **3** 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

전역 컨피그레이션 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

관련 항목

관리 액세스에 대한 지침

호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정, 681 페이지

콘솔 세션에서 로그아웃

ASASM에서 로그아웃하지 않으면 콘솔 연결이 지속되므로 시간 제한이 없습니다. ASASM 콘솔 세션을 종료하고 스위치 CLI에 액세스하려면 다음 단계를 수행합니다.

다른 사용자가 의도치 않게 열어둔 활성화된 연결을 끊으려면 활성화된 콘솔 연결 끊기, 21 페이지를 참조하십시오.

프로시저

스위치 CLI로 돌아가려면 다음을 입력합니다.

Ctrl-Shift-6, **x**

스위치 프롬프트로 다시 돌아갑니다.

```
asasm# [Ctrl-Shift-6, x]
Router#
```

참고 미국 및 영국 키보드에서 Shift-6을 누르면 캐럿 기호(^)가 생성됩니다. 다른 키보드를 사용 중이고 탈자 기호(^)를 독립 문자로 생성할 수 없는 경우, 이스케이프 문자를 다른 문자로 변경하는 것이 일시적으로 또는 영구적으로 불가능합니다. **terminal escape-character** *ascii_number* 명령(이 세션에서 변경하려는 경우) 또는 **default escape-character** *ascii_number* 명령(영구적으로 변경하려는 경우)을 사용하십시오. 예를 들어, 현재 세션의 시퀀스를 **Ctrl-w**, **x**로 변경하려면 **terminal escape-character 23**을 입력합니다.

활성화된 콘솔 연결 끊기

ASASM에서 올바르게 로그아웃하지 않을 경우 콘솔 연결 상태가 계속 유지되어 의도한 시간보다 연결이 오래 지속될 수 있습니다. 다른 사람이 로그인하려면 기존 연결을 끊어야 합니다.

프로시저

단계 **1** 스위치 CLI에서 **show users** 명령을 사용하여 연결된 사용자를 표시합니다. 콘솔 사용자는 "con"으로 표시됩니다. 호스트 주소는 127.0.0.*slot*0으로 표시되며 여기서 *slot*은 모듈의 슬롯 번호입니다.

show users

예를 들어, 다음 명령의 출력 값에는 슬롯 2의 모듈 0에 있는 사용자 "con"이 표시됩니다.

```
Router# show users
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20           00:00:02
```

단계 **2** 콘솔 연결이 포함된 행을 지우려면 다음 명령을 입력합니다.

clear *line number*

예를 들면 다음과 같습니다.

```
Router# clear line 0
```

텔넷 세션에서 로그아웃

텔넷 세션을 종료하고 스위치 CLI에 액세스하여 다음 단계를 수행합니다.

프로시저

스위치 CLI로 돌아가려면 ASASM 특권 또는 사용자 EXEC 모드에서 **exit**를 입력합니다. 컨피그레이션 모드인 경우 텔넷 세션을 종료할 때까지 **exit**를 반복 입력합니다.

스위치 프롬프트로 다시 돌아갑니다.

```
asasm# exit
Router#
```

참고 또는 이스케이프 시퀀스 **Ctrl-Shift-6**, **x**를 사용하여 텔넷 세션을 종료할 수 있습니다. 이러한 이스케이프 시퀀스를 사용하면 스위치 프롬프트에서 **Enter** 키를 눌러 텔넷 세션을 다시 시작할 수 있습니다. 스위치에서 텔넷 세션의 연결을 끊으려면 스위치 CLI에서 **disconnect**를 입력합니다. 세션의 연결을 끊지 않을 경우 ASASM 구성에 따라 결국 시간이 초과될 수 있습니다.

소프트웨어 모듈 콘솔 액세스

ASA 5506-X에 ASA FirePOWER 모듈과 같은 소프트웨어 모듈이 설치된 경우 모듈 콘솔과의 세션을 시작할 수 있습니다.

참고 **session** 명령을 사용하여 ASA 백플레인을 통해 하드웨어 모듈 CLI에 액세스할 수 없습니다.

프로시저

ASA CLI에서 모듈에 대한 세션은 다음과 같습니다.

session {sfr | cxsc | ips} console

예제:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ASA 5506W-X Wireless Access Point 콘솔 액세스

무선 액세스 포인트 콘솔에 액세스하려면 다음 단계를 수행합니다.

프로시저

단계 **1** ASA CLI에서 액세스 포인트에 대한 세션은 다음과 같습니다.

session wlan console

예제:

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

단계 **2** 액세스 포인트 CLI에 대한 자세한 내용은 자동 Aironet 액세스 포인트를 위한 Cisco IOS 구성 가이드를 참조하십시오.

ASDM 액세스 구성

이 섹션에서는 기본 컨피그레이션을 사용하여 ASDM에 액세스하는 방법과 기본 컨피그레이션이 없는 경우 액세스를 컨피그레이션하는 방법에 대해 알아봅니다.

ASDM 액세스에 공장 기본 컨피그레이션 사용(어플라이언스, ASAv)

공장 기본 컨피그레이션을 사용할 경우 ASDM 연결은 기본 네트워크 설정으로 사전 구성됩니다.

프로시저

다음 인터페이스 및 네트워크 설정을 사용하여 ASDM에 연결합니다.

- 관리 인터페이스는 사용하는 모델에 따라 달라집니다.
  - ASA 5506-X, ASA 5508-X, ASA 5516-X—ASDM에 연결하는 인터페이스는 GigabitEthernet 1/2입니다.
  - ASA 5512-X 이상 — ASDM에 연결하는 인터페이스는 Management 0/0입니다.
  - ASAv — ASDM에 연결하는 인터페이스는 Management 0/0입니다.
  - ISA 3000 — ASDM에 연결하는 인터페이스는 Management 1/1입니다.
  - Firepower 4100/9300 섀시의 ASA — ASDM에 연결하는 인터페이스는 FXOS 섀시 수퍼바이저에 정의되어 있으며 사용자가 선택한 관리 유형 인터페이스입니다.
- 기본 관리 주소는 다음과 같습니다.
  - ASA 어플라이언스 — 192.168.1.1.
  - ASAv — 구축 과정에서 관리 인터페이스 IP 주소를 설정합니다.
  - Firepower 4100/9300 섀시의 ASA — 구축 과정에서 관리 인터페이스 IP 주소를 설정합니다.
- 클라이언트에서는 ASDM 액세스를 허용합니다.
  - ASA 어플라이언스 — 클라이언트는 192.168.1.0/24 네트워크에 있어야 합니다. 기본 컨피그레이션의 경우 DHCP를 지원하므로 관리 스테이션에서는 이 범위 내에 IP 주소를 할당할 수 있습니다.
  - ASAv — 구축 과정에서 관리 클라이언트 IP 주소를 설정합니다. ASAv는 연결된 클라이언트에 대해 DHCP 서버로 작동하지 않습니다.
  - Firepower 4100/9300 섀시의 ASA — 모든 호스트는 관리 인터페이스에서 ASDM에 액세스할 수 있습니다. ASAv는 연결된 클라이언트의 DHCP 서버로 작동하지 않습니다.

참고 다중 컨텍스트 모드로 변경할 경우, 위의 네트워크 설정을 사용하여 관리자 컨텍스트에서 ASDM에 액세스할 수 있습니다.

관련 항목

공장 기본 컨피그레이션, 31 페이지
다중 상황 모드 활성화 또는 비활성화, 232 페이지

ASDM 시작, 30 페이지

ASDM 액세스 맞춤화

이 절차는 ASA Services Module을 제외한 모든 모델에 적용됩니다.

다음 조건 중 하나 이상이 해당되는 경우 이 절차를 사용하십시오.

- 공장 기본 컨피그레이션이 없는 경우
- 관리 IP 주소를 변경하려는 경우
- 투명 방화벽 모드를 변경하려는 경우
- 다중 컨텍스트 모드로 변경하려는 경우

단일 라우팅 모드의 경우 ASDM에 쉽고 빠르게 액세스하려면 고유한 관리 IP 주소를 설정하는 옵션에 공장 기본 컨피그레이션을 적용하는 것이 좋습니다. 이 섹션의 절차는 투명 또는 다중 컨텍스트 모드 설정 같은 특수한 상황 또는 유지해야 할 다른 컨피그레이션이 있는 경우에만 사용하십시오.

참고 ASAv의 경우 구축 시 투명 모드를 구성할 수 있습니다. 따라서 이 절차는 주로 구축 이후에, 예를 들어 구성을 지워야 하는 경우에 유용합니다.

프로시저

단계 **1** 콘솔 포트에서 CLI에 액세스합니다.

단계 **2** (선택 사항) 투명 방화벽 모드를 활성화합니다.

이 명령을 실행하면 컨피그레이션이 지워집니다.

firewall transparent

단계 **3** 관리 인터페이스를 구성합니다.

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

예제:

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level은 1 ~ 100의 숫자로 설정하며 100이 가장 안전한 수준입니다.

단계 **4** (직접 연결된 관리 호스트의 경우) 관리 네트워크에 DHCP 풀을 설정합니다.

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

예제:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

범위에 인터페이스 주소가 포함되어 있지 않은지 확인합니다.

단계 **5** (원격 관리 호스트의 경우) 관리 호스트에 대한 경로를 구성합니다.

route *management_ifc management_host_ip mask gateway_ip* **1**

예제:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

단계 **6** ASDM에 대한 HTTP 서버를 활성화합니다.

http server enable

단계 **7** 관리 호스트에서 ASDM에 액세스하도록 허용합니다.

http *ip_address mask interface_name*

예제:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

단계 **8** 구성을 저장합니다.

write memory

단계 **9** (선택 사항) 모드를 다중 모드로 설정합니다.

mode multiple

프롬프트가 표시되면 기존 컨피그레이션을 관리자 컨텍스트로 변환할 것을 확인합니다. 그러면 ASA를 다시 로드하라는 메시지가 표시됩니다.

예

다음 컨피그레이션에서는 방화벽 모드를 투명 모드로 변환하고, Management 0/0 인터페이스를 컨피그레이션하고, 관리 호스트에 대한 ASDM을 활성화합니다.

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

관련 항목

공장 기본 컨피그레이션 복원, 32 페이지
방화벽 모드, 198 페이지
어플라이언스 콘솔 액세스, 13 페이지
ASDM 시작, 30 페이지

ASA 서비스 모듈을 위한 ASDM 액세스 구성

ASASM에는 물리적 인터페이스가 없으므로 ASDM 액세스에 대해 사전 구성되어 있지 않습니다. ASASM에서 CLI를 사용하여 ASDM 액세스를 구성해야 합니다. ASDM 액세스를 위해 ASASM을 구성하려면 다음을 수행하십시오.

시작하기 전에

ASASM 빠른 시작 가이드에 따라 ASASM에 VLAN 인터페이스를 할당하십시오.

프로시저

단계 **1** ASASM에 연결하고 전역 구성 모드에 액세스합니다.

단계 **2** (선택 사항) 투명 방화벽 모드를 활성화합니다.

firewall transparent

이 명령을 실행하면 컨피그레이션이 지워집니다.

단계 **3** 현재 사용 중인 모드에 따라, 다음 중 하나를 수행하여 관리 인터페이스를 구성합니다.

- 라우팅 모드 — 라우팅 모드에서는 인터페이스를 다음과 같이 구성합니다.

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

예:

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level은 1~100 사이의 숫자로 설정하며 100이 가장 안전한 수준입니다.

- 투명 모드 — 브리지 가상 인터페이스를 구성하고 브리지 그룹에 관리 VLAN을 할당합니다.

```
interface bvi number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

예:

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level은 1~100 사이의 숫자로 설정하며 100이 가장 안전한 수준입니다.

단계 **4** (직접 연결된 관리 호스트의 경우) 관리 인터페이스 네트워크의 관리 호스트에 대한 DHCP 풀을 활성화합니다.

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

예제:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

범위에 관리 주소가 포함되어 있지 않은지 확인합니다.

단계 **5** (원격 관리 호스트의 경우) 관리 호스트에 대한 경로를 구성합니다.

route *management_ifc management_host_ip mask gateway_ip* **1**

예제:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

단계 **6** ASDM에 대한 HTTP 서버를 활성화합니다.

http server enable

단계 **7** 관리 호스트에서 ASDM에 액세스하도록 허용합니다.

http *ip_address mask interface_name*

예제**:**

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

단계 **8** 구성을 저장합니다.

write memory

단계 **9** (선택 사항) 모드를 다중 모드로 설정합니다.

mode multiple

프롬프트가 표시되면 기존 컨피그레이션을 관리자 컨텍스트로 변환할 것을 확인합니다. 그러면 ASASM을 다시 로드하라는 프롬프트가 표시됩니다.

예

다음 라우팅 모드 컨피그레이션에서는 VLAN 1 인터페이스를 컨피그레이션하고 관리 호스트에 대한 ASDM를 활성화합니다.

```
interface vlan 1
nameif inside
ip address 192.168.1.1 255.255.255.0
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

다음 컨피그레이션에서는 방화벽 모드를 투명 모드로 변환하고, VLAN 1 인터페이스를 구성하고 이를 BVI 1에 할당하며, 관리 호스트에 대한 ASDM을 활성화합니다.

```
firewall transparent
interface bvi 1

ip address 192.168.1.1 255.255.255.0
interface vlan 1
bridge-group 1
nameif inside
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

관련 항목

ASA 서비스 모듈 콘솔 액세스, 18 페이지
방화벽 모드, 198 페이지

ASDM 시작

다음 두 가지 방법을 사용하여 ASDM을 시작할 수 있습니다.

- ASDM-IDM Launcher — Launcher는 모든 ASA IP 주소에 연결하는 데 사용할 수 있는 웹 브라우저를 사용하여 ASA에서 다운로드하는 애플리케이션입니다. 다른 ASA에 연결하려면 Launcher를 다시 다운로드하지 않아도 됩니다.
- Java Web Start — 관리하는 각 ASA를 웹 브라우저와 연결한 다음, Java Web Start 애플리케이션을 저장하거나 실행해야 합니다. 원하는 경우 컴퓨터에 바로가기를 저장할 수는 있으나 ASA IP 주소마다 별도의 바로가기를 지정해야 합니다.

참고 Web Start를 사용하는 경우 Java 캐시를 지우십시오. 그렇지 않으면 Hostscan와 같은 일부 사전 로그인 정책의 변경 사항이 손실될 수 있습니다. Launcher를 사용하는 경우 이 문제는 발생하지 않습니다.

ASDM 내에서는 서로 다른 ASA IP 주소를 선택하여 관리할 수 있습니다. Launcher와 Java Web Start 기능의 주요 차이점은 처음에 ASA에 연결하고 ASDM을 실행하는 방법에 있습니다.

이 섹션에서는 맨 처음 ASDM에 연결한 다음 Launcher 또는 Java Web Start를 사용하여 ASDM을 시작하는 방법에 대해 설명합니다.

ASDM에서는 파일을 캐시, 로그 및 환경 설정 등의 로컬 \Users\<user_id>\.asdm 디렉터리 및 AnyConnect 프로필 등의 Temp 디렉터리에 저장합니다.

프로시저

단계 **1** ASDM 클라이언트로 지정한 컴퓨터에서 다음 URL을 입력합니다.

https://*asa_ip_address*/**admin**

다음 버튼이 있는 ASDM 시작 페이지가 나타납니다.

- **Install ASDM Launcher and Run ASDM(ASDM Launcher** 설치 및 **ASDM** 실행**)**
- **Run ASDM(ASDM** 실행**)**
- **Run Startup Wizard(**시작 마법사 실행**)**

단계 **2** Launcher를 다운로드하려면

a) **Install ASDM Launcher and Run ASDM(ASDM Launcher** 설치 및 **ASDM** 실행**)**을 클릭합니다.

b) 사용자 이름 및 비밀번호 필드를 비어 있는 상태로 두고(새로 설치하는 경우) **OK(**확인**)**를 클릭합니다. 어떤 HTTPS 인증도 구성되지 않았으므로 사용자 이름 없이, **enable** 비밀번호(기본적으로 비어 있음)를 사용하여 ASDM에 액세스할 수 있습니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다. 인증을 사용하지 않고 로그인 화면에서 사용자 이름을 비워 두는 대신 사용자 이름과 비밀번호를 입력하는 경우 ASDM에서는 로컬 데이터베이스에 일치하는 항목이 있는지 확인합니다.

c) 설치 프로그램을 컴퓨터에 저장한 다음 시작합니다. 설치가 완료되면 ASDM-IDM Launcher가 자동으로 열립니다.

d) 관리 IP 주소, 동일한 사용자 이름과 비밀번호(새로 설치하는 경우 비어 있음)를 입력한 다음, **OK(**확인**)**를 클릭합니다.

단계 **3** Java Web Start를 사용하려면

a) **Run ASDM(ASDM** 실행**)** 또는 **Run Startup Wizard(**시작 마법사 실행**)**를 클릭합니다.

b) 프롬프트에 따라 바로가기를 컴퓨터에 저장합니다. 저장하지 않고 열 수도 있습니다.

c) 바로가기에서 Java Web Start를 시작합니다.

d) 표시되는 대화 상자의 안내에 따라 인증서를 승인합니다. Cisco ASDM-IDM Launcher가 나타납니다.

e) 사용자 이름 및 비밀번호 필드를 비어 있는 상태로 두고(새로 설치하는 경우) **OK(**확인**)**를 클릭합니다. 어떤 HTTPS 인증도 구성되지 않았으므로 사용자 이름 없이, **enable** 비밀번호(기본적으로 비어 있음)를 사용하여 ASDM에 액세스할 수 있습니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다. 인증을 사용하지 않고 로그인 화면에서 (사용자 이름을 비워 두지 않고) 사용자 이름과 비밀번호를 입력한 경우 ASDM은 로컬 데이터베이스에 일치하는 항목이 있는지 확인합니다.

공장 기본 컨피그레이션

공장 기본 구성은 Cisco에서 새 ASA에 적용하는 구성입니다.

- ASA 어플라이언스 — 공장 기본 구성을 통해 관리용 인터페이스가 구성되므로 ASDM을 사용하여 ASA 어플라이언스에 연결하고 구성을 완료할 수 있습니다.
- Firepower 4100/9300 섀시의 ASA — ASA의 독립형 또는 클러스터를 구축할 경우 공장 기본 구성을 통해 관리용 인터페이스가 구성되므로 ASDM 사용하여 ASA 어플라이언스에 연결하고 구성을 완료할 수 있습니다.
- ASAv — 하이퍼바이저에 따라 구축 과정에서 구축 구성(초기 가상 구축 설정)을 통해 관리용 인터페이스가 구성되므로 ASDM을 사용하여 ASAv에 연결하고 구성을 완료할 수 있습니다. 또한 장애 조치 IP 주소를 구성할 수 있습니다. 필요한 경우 "공장 초기화" 컨피그레이션을 적용할 수 있습니다.
- ASASM — 기본 구성이 없습니다. 컨피그레이션을 시작하려면 ASA 서비스 모듈 콘솔 액세스, 18 페이지를 참조하십시오.

Firepower 4100/9300 섀시의 어플라이언스 및 ASA의 경우 공장 기본 구성은 라우팅 방화벽 모드 및 단일 상황 모드에만 사용할 수 있습니다. ASAv의 경우 구축 시 투명 모드 또는 라우팅 모드를 선택할 수 있습니다.

참고 이미지 파일 및 (숨겨진) 기본 컨피그레이션 외에, 플래시 메모리에서는 log/, crypto_archive/ 및 coredumpinfo/coredump.cfg 폴더와 파일이 표준입니다. 이러한 파일의 날짜는 플래시 메모리에 있는 이미지 파일의 날짜와 일치하지 않을 수 있습니다. 이러한 파일은 잠재적인 문제 해결에 도움이 될 수 있으며 오류가 발생한 것으로 간주하지 않습니다.

공장 기본 컨피그레이션 복원

이 섹션에서는 공장 기본 컨피그레이션을 복원하는 방법에 대해 설명합니다. ASAv의 경우 이 절차에서는 구축 구성을 지우고 ASA 어플라이언스에 적용되는 것과 동일한 공장 기본 구성을 적용합니다.

참고 ASASM에서 공장 기본 구성을 복원하면 단순히 구성이 지워집니다. 공장 기본 구성이 존재하지 않기 때문입니다. Firepower 9300 ASA 보안 모듈에서 공장 기본 구성을 복원하면 단순히 구성이 지워집니다. 기본 구성을 복원하려면 수퍼바이저에서 ASA를 다시 구축해야 합니다.

시작하기 전에

이 기능은 라우팅 방화벽 모드 에서만 사용할 수 있으며, 투명 모드에서는 인터페이스에 대한 IP 주소를 지원하지 않습니다. 또한 이 기능은 단일 상황 모드에서만 사용할 수 있습니다. 구성이 지워진 ASA에는 이 기능을 사용하여 자동으로 구성할 수 있는 정의된 상황이 없습니다.

프로시저

단계 **1** 공장 기본 컨피그레이션을 복원합니다.

configure factory-default [*ip_address* [*mask*]]

예제**:**

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

*ip_address*를 지정한 경우, 현재 사용 중인 모델에 따라 기본 IP 주소 192.168.1.1 대신 내부 또는 관리 인터페이스 IP 주소를 설정합니다. http 명령어에서는 사용자가 지정하는 서브넷을 사용합니다. 이와 마찬가지로 **dhcpd address** 명령어 범위는 사용자가 지정하는 서브넷 내의 주소로 구성됩니다.

이 명령을 사용하면 **boot** system 명령(있는 경우)과 함께 나머지 구성도 지워집니다. **boot** system 명령을 사용하면 외부 플래시 메모리 카드의 이미지 등 특정 이미지에서 부팅할 수 있습니다. 공장 구성

을 복원한 후 다음에 ASA를 다시 로드하는 경우 내부 플래시 메모리의 첫 번째 이미지에서 부팅이 이루어집니다. 내부 플래시 메모리에 이미지가 없는 경우 ASA에서는 부팅을 수행하지 않습니다.

단계 **2** 플래시 메모리에 기본 컨피그레이션을 저장합니다.

write memory

이 명령을 사용하면 현재 실행 중인 구성이 시작 구성의 기본 위치에 저장되며, 이는 이전에 **boot** config 명령을 구성하여 다른 위치를 설정한 경우에도 마찬가지입니다. 해당 구성이 지워지면 이 경로도 지워집니다.

ASAv 구축 컨피그레이션 복원

이 섹션에서는 ASAv 구축(Day 0) 구성을 복원하는 방법에 대해 설명합니다.

프로시저

단계 **1** 장애 조치를 수행하려면 스탠바이 유닛의 전원을 끕니다.

스탠바이 유닛이 활성화되지 않도록 하려면 전원을 꺼야 합니다. 전원을 계속 켜두면 액티브 유닛 컨피그레이션을 지울 때 스탠바이 유닛이 활성화됩니다. 장애 조치 링크를 통해 이전 액티브 유닛이 다시 로드되고 연결될 경우, 새 액티브 유닛에서 기존 컨피그레이션이 동기화되어 사용자가 원하는 구축 컨피그레이션이 지워집니다.

단계 **2** 다시 로드한 후 구축 컨피그레이션을 복원합니다. 장애 조치를 수행하려면 액티브 유닛에 다음 명령을 입력합니다.

write erase

참고 ASAv에서는 현재 실행 중인 이미지를 부팅하므로 원래 부트 이미지로 되돌아가지 않습니다. 원래 부트 이미지를 사용하려면 **boot image** 명령을 참조하십시오.

컨피그레이션을 저장하지 마십시오.

단계 **3** ASAv를 다시 로드하고 구축 구성을 로드합니다.

reload

단계 **4** 장애 조치를 수행하려면 스탠바이 유닛의 전원을 켭니다.

액티브 유닛이 다시 로드되면 스탠바이 유닛의 전원을 켭니다. 구축 컨피그레이션은 스탠바이 유닛에 동기화됩니다.

ASA 5506-X Series 기본 구성

ASA 5506-X Series에 대한 공장 기본 구성을 사용하면 다음이 구성됩니다.

- 통합 라우팅 및 브리징 기능 — 브리지 그룹 1에 속하는 GigabitEthernet 1/2~1/8, BVI(Bridge Virtual Interface) 1
- 내부 --> 외부 트래픽 플로우 — GigabitEthernet 1/1(외부), BVI 1(내부)
- DHCP로부터의 외부 IP 주소, 내부 IP 주소—192.168.1.1
- (ASA 5506W-X) wifi <--> 내부, wifi --> 외부 트래픽 흐름—GigabitEthernet 1/9(wifi)
- (ASA 5506W-X) wifi IP 주소—192.168.10.1
- 내부의 클라이언트에 대한 DHCP 및 wifi. 액세스 포인트 자체와 모든 클라이언트는 ASA를 DHCP 서버로 사용합니다.
- ASDM 액세스—내부 및 wifi 호스트가 허용됩니다.
- NAT — 내부, wfi, 관리에서 외부로 가는 모든 트래픽을 위한 인터페이스 PAT.

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface GigabitEthernet1/2
  nameif inside_1
  security-level 100
  bridge-group 1
  no shutdown
interface GigabitEthernet1/3
  nameif inside_2
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/4
  nameif inside_3
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/5
  nameif inside_4
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/6
  nameif inside_5
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/7
  nameif inside_6
  security-level 100
```

```
  no shutdown
  bridge-group 1
interface GigabitEthernet1/8
  nameif inside_7
  security-level 100
  no shutdown
  bridge-group 1
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
object network obj_any1
 subnet 0.0.0.0 0.0.0.0
 nat (inside_1,outside) dynamic interface
object network obj_any2
 subnet 0.0.0.0 0.0.0.0
 nat (inside_2,outside) dynamic interface
object network obj_any3
 subnet 0.0.0.0 0.0.0.0
 nat (inside_3,outside) dynamic interface
object network obj_any4
 subnet 0.0.0.0 0.0.0.0
 nat (inside_4,outside) dynamic interface
object network obj_any5
 subnet 0.0.0.0 0.0.0.0
 nat (inside_5,outside) dynamic interface
object network obj_any6
 subnet 0.0.0.0 0.0.0.0
 nat (inside_6,outside) dynamic interface
object network obj_any7
 subnet 0.0.0.0 0.0.0.0
 nat (inside_7,outside) dynamic interface
!
same-security-traffic permit inter-interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5506W-X의 경우 다음 명령도 포함됩니다.

```
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
object network obj_any_wifi
 subnet 0.0.0.0 0.0.0.0
 nat (wifi,outside) dynamic interface
```

```
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5508-X 및 5516-X 기본 구성

ASA 5508-X 및 5516-X에 대한 공장 기본 구성을 사용하면 다음이 구성됩니다.

- 내부 --> 외부 트래픽 흐름—GigabitEthernet 1/1(외부), GigabitEthernet 1/2(내부)
- DHCP로부터의 외부 IP 주소, 내부 IP 주소—192.168.1.1
- 내부의 클라이언트에 대한 DHCP.
- Management 1/1 인터페이스가 작동 중이지만 그 밖에는 구성되지 않은 상태입니다. 그러면 ASA FirePOWER 모듈은 이 인터페이스를 사용하여 네트워크 내부의 ASA에 액세스하고 내부 인터페이스를 인터넷에 대한 게이트웨이로 사용할 수 있습니다.
- ASDM 액세스—내부 호스트가 허용됩니다.
- NAT — 내부 관리에서 외부로 가는 모든 트래픽을 위한 인터페이스 PAT

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface GigabitEthernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5512-X, 5515-X, 5525-X 이상 기본 컨피그레이션

ASA 5512-X, 5515-X, 5525-X 이상에 대한 공장 기본 컨피그레이션은 다음 항목을 구성합니다.

- 관리 인터페이스—Management 0/0(관리)
- IP 주소 — 관리 주소는 192.168.1.1/24입니다.
- DHCP 서버 — 관리 호스트에 사용되며 관리 인터페이스에 연결된 컴퓨터에서는 192.168.1.2 ~ 192.168.1.254의 주소를 받게 됩니다.
- ASDM 액세스 — 관리 호스트를 허용합니다.

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Firepower 2100 기본 구성의 ASA

ASA 컨피그레이션

Firepower 2100의 ASA에 대한 공장 기본 구성을 사용하면 다음이 구성됩니다.

- 내부 --> 외부 트래픽 플로우 — Ethernet 1/1(외부), Ethernet 1/2(내부)
- DHCP로부터의 외부 IP 주소, 내부 IP 주소—192.168.1.1
- 내부 인터페이스의 DHCP 서버 — 192.168.1.20-192.168.1.254
- 외부 DHCP의 기본 경로
- 관리 — Management 1/1(관리), IP 주소: 192.168.45.1
- ASDM 액세스 — 관리 호스트를 허용합니다.
- NAT— 내부에서 외부로 가는 모든 트래픽을 위한 인터페이스 PAT
- FXOS 관리 트래픽 시작 — FXOS 새시는 ASA 외부 인터페이스에서 관리 트래픽을 시작할 수 있습니다.
- DNS 서버 — OpenDNS 서버는 사전에 구성되어 있습니다.

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside

ip-client outside

dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

FXOS 구성

Firepower 2100의 FXOS에 대한 공장 기본 구성을 사용하면 다음이 구성됩니다.

- Management 1/1 — IP 주소: 192.168.45.45
- 기본 게이트웨이 — ASA 데이터 인터페이스
- Firepower Chassis Manager 및 SSH 액세스 — 관리 네트워크에서 지원됨
- 기본 사용자 이름 — **admin**, 기본 비밀번호: **Admin123**
- DHCP 서버 — 클라이언트 IP 주소 범위: 192.168.45.10-192.168.45.12
- NTP 서버 — Cisco NTP 서버: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- DNS 서버 — OpenDNS: 208.67.222.222, 208.67.220.220
- Ethernet 1/1 및 Ethernet 1/2 — 활성화됨

Firepower 4100/9300 섀시 기본 구성의 ASA

Firepower 4100/9300 섀시에서 ASA를 구축할 경우 ASDM을 사용하여 관리 인터페이스에 연결할 수 있도록 지원하는 여러 파라미터를 사전에 설정할 수 있습니다. 일반적인 컨피그레이션에는 다음과 같은 설정이 포함됩니다.

- 관리 인터페이스:
  - Firepower 4100/9300 섀시 수퍼바이저에 정의되어 있으며 사용자가 선택한 관리 유형 인터페이스
  - 이름이 지정된 "관리"
  - 선택한 IP 주소
  - 보안 수준 0
  - Management-only
- 관리 인터페이스를 통과하는 기본 경로
- ASDM 액세스 — 모든 호스트가 허용됩니다.

독립형 유닛의 구성은 다음 명령으로 구성됩니다. 클러스터링된 유닛의 추가 구성에 대해서는 ASA 클러스터 생성, 491 페이지의 내용을 참조하십시오.

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 기본 구성

ISA 3000에 대한 공장 기본 구성을 사용하면 다음이 구성됩니다.

- 투명 방화벽 모드 — 투명 방화벽은 "BITW(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)"와 같은 역할을 수행하는 Layer 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.
- 브리지 가상 인터페이스 1개 — 모든 멤버 인터페이스는 동일한 네트워크에 있습니다(**IP** 주소는 사전에 구성되지 않음**,** 네트워크와 일치하도록 설정해야 함)(GigabitEthernet 1/1(outside1), GigabitEthernet 1/2(inside1), GigabitEthernet 1/3(outside2), GigabitEthernet 1/4(inside2)).
- 모든 내부 및 외부 인터페이스는 서로 통신할 수 있습니다.

- Management 1/1 인터페이스 — ASDM 액세스를 위한 192.168.1.1/24
- 관리를 위한 클라이언트용 DHCP입니다.
- ASDM 액세스 — 관리 호스트를 허용합니다.
- 하드웨어 우회가 GigabitEthernet 1/1 및 1/2, GigabitEthernet 1/3 및 1/4 인터페이스 쌍에 대해 활성화되어 있습니다.

참고 ISA 3000이 전력 손실로 하드웨어 우회 모드로 전환되는 경우, 인터페이스 쌍을 통해서만 통신할 수 있습니다. inside1과 inside2, outside1과 outside2는 더 이상 통신할 수 없습니다. 이러한 인터페이스 간에 모든 기존 연결이 손실됩니다. 전원이 다시 들어오면 ASA가 플로우를 인계받을 때 잠시 연결이 중단됩니다.

- ASA FirePOWER 모듈 — 모든 트래픽은 인라인 탭 모니터링 전용 모드로 전송됩니다. 이 모드에서는 모니터링 목적으로만 트래픽의 복제 스트림을 ASA Firepower 모듈로 전송합니다.
- Precision Time Protocol — PTP 트래픽은 FirePOWER 모듈에 전송되지 않습니다.

컨피그레이션은 다음 명령으로 구성됩니다.

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
```

```
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management


access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
  sfr fail-open monitor-only
service-policy global_policy global
```

ASAv 구축 컨피그레이션

ASAv를 구축할 경우 ASDM을 사용하여 Management 0/0 인터페이스에 연결할 수 있도록 지원하는 여러 파라미터를 사전에 설정할 수 있습니다. 일반적인 컨피그레이션에는 다음과 같은 설정이 포함됩니다.

- 라우팅 또는 투명 방화벽 모드
- Management 0/0 인터페이스:
  - 이름이 지정된 "관리"
  - IP 주소 또는 DHCP
  - 보안 수준 0
- 관리 호스트 IP 주소를 위한 고정 경로(관리 서브넷에 있지 않을 경우)
- HTTP 서버 활성화 또는 비활성화
- 관리 호스트 IP 주소에 대한 HTTP 액세스
- (선택 사항) GigabitEthernet 0/8 및 Management 0/0 스탠바이 IP 주소에 대한 장애 조치 링크 IP 주소
- DNS 서버
- 스마트 라이센싱 ID 토큰
- 스마트 라이센싱 처리량 레벨 및 표준 기능 계층
- (선택 사항) 스마트 콜 홈 HTTP 프록시 URL 및 포트
- (선택 사항) SSH 관리 설정

- 클라이언트 IP 주소
- 로컬 사용자 이름 및 비밀번호
- LOCAL 데이터베이스를 사용하는 SSH에 인증 필요

- (선택 사항) REST API 활성화 또는 비활성화

참고 ASAv를 Cisco Licensing Authority에 등록하려면 ASAv에 인터넷 액세스가 필요합니다. 구축 후 인터넷 액세스 및 성공적인 라이센스 등록을 위해 추가 컨피그레이션이 필요할 수 있습니다.

독립형 유닛의 경우 다음 샘플 컨피그레이션을 참조하십시오.

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

장애 조치 쌍에 있는 기본 유닛의 경우 다음 샘플 컨피그레이션을 참조하십시오.

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
```

```
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

컨피그레이션 작업

이 섹션에서는 컨피그레이션을 수행하는 방법에 대해 설명합니다. ASA에서는 시작 구성이라는 텍스트 파일에서 구성을 로드합니다. 이 파일은 기본적으로 내부 플래시 메모리의 숨겨진 파일로 상주합니다. 그러나 시작 컨피그레이션의 다른 경로를 지정할 수 있습니다.

명령을 입력할 경우 메모리에서 실행 중인 컨피그레이션에만 변경 사항이 적용됩니다. 재부팅 후 변경 사항을 유지하려면 실행 중인 컨피그레이션을 시작 컨피그레이션에 수동으로 저장해야 합니다.

이 섹션의 정보는 별도로 명시한 경우를 제외하고 단일 및 다중 보안 컨텍스트에 모두 적용됩니다.

구성 변경사항 저장

이 섹션에서는 컨피그레이션을 저장하는 방법에 대해 설명합니다.

단일 컨텍스트 모드에서 컨피그레이션 변경 사항 저장

실행 중인 컨피그레이션을 시작 컨피그레이션에 저장하려면 다음 절차를 수행합니다.

프로시저

실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.

write memory

참고 **copy running-config startup-config** 명령은 **write memory** 명령과 같습니다.

다중 컨텍스트 모드에서 컨피그레이션 변경 사항 저장

각 컨텍스트(및 시스템) 컨피그레이션을 개별적으로 저장하거나, 모든 컨텍스트 컨피그레이션을 동시에 저장할 수 있습니다.

각 컨텍스트 및 시스템을 개별적으로 저장

시스템 또는 컨텍스트 컨피그레이션을 저장하려면 다음 절차를 사용합니다.

프로시저

컨텍스트 또는 시스템에서 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.

write memory

다중 컨텍스트 모드의 경우 컨텍스트 시작 컨피그레이션이 외부 서버에 상주할 수 있습니다. 이 경우 ASA에서는 상황 URL에서 확인된 서버에 구성을 다시 저장합니다. 이때 HTTP 또는 HTTPS URL을 사용하면 구성을 서버에 저장할 수 없으므로 이러한 URL은 제외됩니다.

참고 **copy running-config startup-config** 명령은 **write memory** 명령과 같습니다.

모든 컨텍스트 컨피그레이션을 동시에 저장

모든 컨텍스트 컨피그레이션 및 시스템 컨피그레이션을 동시에 저장하려면 다음 절차를 사용합니다.

프로시저

시스템 실행 영역에서 모든 컨텍스트 및 시스템 컨피그레이션에 대한 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.

write memory all [**/noconfirm**]

/noconfirm 키워드를 입력하지 않을 경우 다음 프롬프트가 표시됩니다.

```
Are you sure [Y/N]:
```

Y를 입력하고 나면 ASA에서 시스템 구성 및 각 상황을 저장합니다. 컨텍스트 시작 컨피그레이션은 외부 서버에 상주할 수 있습니다. 이 경우 ASA에서는 상황 URL에서 확인된 서버에 구성을 다시 저장합니다. 이때 HTTP 또는 HTTPS URL을 사용하면 구성을 서버에 저장할 수 없으므로 이러한 URL은 제외됩니다.

ASA에서 각 상황을 저장하고 나면 다음 메시지가 표시됩니다.

```
‘Saving context ‘b’ ... ( 1/3 contexts saved ) ’
```

오류로 인해 컨텍스트가 저장되지 않는 경우가 있습니다. 오류에 대한 내용은 다음 정보를 참조하십시오.

- 적은 메모리로 인해 컨텍스트가 저장되지 않은 경우 다음과 같은 메시지가 표시됩니다.

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- 원격 대상에 연결할 수 없어 저장되지 않는 상황의 경우 다음 메시지가 표시됩니다.

```
The context 'context a' could not be saved due to non-reachability of destination
```

- 컨텍스트가 잠겨 있어 컨텍스트가 저장되지 않은 경우 다음과 같은 메시지가 표시됩니다.

```
Unable to save the configuration for the following contexts as these contexts are locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

  컨텍스트는 다른 사용자가 컨피그레이션을 이미 저장하고 있거나 컨텍스트를 삭제하는 중인 경우에만 잠깁니다.

- 시작 컨피그레이션이 읽기 전용(예: HTTP 서버)이라 컨텍스트가 저장되지 않은 경우, 모든 다른 메시지의 하단에 다음과 같은 메시지 보고가 출력됩니다.

```
Unable to save the configuration for the following contexts as these contexts have
read-only config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- 플래시 메모리의 불량 섹터로 인해 컨텍스트가 저장되지 않은 경우 다음과 같은 메시지가 표시됩니다.

```
The context 'context a' could not be saved due to Unknown errors
```

실행 중인 컨피그레이션에 시작 컨피그레이션 복사

다음 명령 중 하나를 사용하여 새로운 시작 컨피그레이션을 실행 중인 컨피그레이션에 복사합니다.

- **copy startup-config running-config**

  시작 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다. 병합은 새 컨피그레이션의 새로운 명령을 실행 중인 컨피그레이션에 추가합니다. 컨피그레이션이 동일할 경우 어떤 변경도 없습니다. 명령이 충돌하거나 명령이 상황 실행에 영향을 줄 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다.

- **reload**

  ASA를 다시 로드하면 시작 구성이 로드되고 실행 중인 구성이 지워집니다.

- **clear configure all** and then **copy startup-config running-config**

  시작 컨피그레이션이 로드되며 다시 로드할 필요 없이 실행 중인 컨피그레이션이 지워집니다.

컨피그레이션 보기

다음 명령을 사용하면 실행 중인 컨피그레이션 및 시작 컨피그레이션을 볼 수 있습니다.

- **show running-config**

  실행 중인 컨피그레이션을 봅니다.

- **show running-config** *command*

  특정 명령의 실행 중인 컨피그레이션을 봅니다.

- **show startup-config**

  시작 컨피그레이션을 봅니다.

컨피그레이션 설정 지우기 및 제거

설정을 지우려면 다음 명령 중 하나를 입력합니다.

- **clear configure** *configurationcommand* [*level2configurationcommand*]

  지정된 명령에 대한 모든 컨피그레이션을 지웁니다. 특정 버전의 명령에 대한 컨피그레이션만 지우려면 *level2configurationcommand*에 대한 값을 입력하면 됩니다.

  예를 들어, 모든 **aaa** 명령에 대한 컨피그레이션을 지우려면 다음 명령을 입력합니다.

  ```
  ciscoasa(config)# clear configure aaa
  ```

  aaa authentication 명령에 대한 컨피그레이션만 지우려면 다음 명령을 입력합니다.

  ```
  ciscoasa(config)# clear configure aaa authentication
  ```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  명령의 특정 매개변수 또는 옵션을 비활성화합니다. 이 경우 *qualifier*로 확인된 특정 구성을 제거하려면 **no** 명령을 사용합니다.

  예를 들어, 특정 **access-list** 명령을 제거하려면 이를 고유하게 확인하는 데 필요한 충분한 양의 명령을 입력합니다. 전체 명령을 입력할 수도 있습니다.

  ```
  ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1
  ```

- **write erase**

  시작 구성을 지웁니다.

  참고 ASAv에서 이 명령을 사용하면 다시 로드한 후 구축 구성이 복원됩니다. 컨피그레이션을 완전히 지우려면 **clear configure all** 명령을 사용합니다.

- **clear configure all**

실행 중인 컨피그레이션을 지웁니다.

참고 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 **clear configure all**을 입력하면 모든 컨텍스트가 제거되고 실행이 중지됩니다. 컨텍스트 컨피그레이션 파일은 지워지지 않으며 원래 위치에 유지됩니다.

이 명령을 사용하면 **boot** system 명령과 함께 나머지 구성도 지워집니다. **boot** system 명령을 사용하면 외부 플래시 메모리 카드의 이미지를 비롯한 특정 이미지에서 부팅할 수 있습니다. 다음에 ASA를 다시 로드하는 경우 내부 플래시 메모리의 첫 번째 이미지에서 부팅이 이루어집니다. 내부 플래시 메모리에 이미지가 없는 경우 ASA에서는 부팅을 수행하지 않습니다.

오프라인에서 텍스트 컨피그레이션 파일 생성

이 가이드에서는 CLI를 사용하여 ASA를 구성하는 방법에 대해 설명합니다. 명령을 저장하면 변경 사항이 텍스트 파일에 작성됩니다. 그러나 CLI를 사용하는 대신 컴퓨터에서 직접 텍스트 파일을 편집하여 컨피그레이션 모드 명령줄 프롬프트에 컨피그레이션을 전체 또는 한 줄씩 붙여넣을 수도 있습니다. 또는 ASA 내부 플래시 메모리에 텍스트 파일을 다운로드할 수 있습니다. 소프트웨어 및 컨피그레이션, 1157 페이지에서 ASA에 구성 파일을 다운로드하는 방법을 참조하십시오.

대부분의 경우, 이 설명서에 설명된 명령은 CLI 프롬프트 앞에 나옵니다. 다음 예의 프롬프트는 “ciscoasa(config)#”입니다.

```
ciscoasa(config)# context a
```

텍스트 컨피그레이션 파일에서는 명령을 입력하라는 메시지가 표시되지 않으므로 다음과 같이 프롬프트가 생략됩니다.

```
context a
```

파일 형식 지정에 대한 자세한 내용은 명령줄 인터페이스 사용, 1367 페이지을 참조하십시오.

연결에 컨피그레이션 변경 사항 적용

컨피그레이션에 대한 보안 정책을 변경하면 모든 새 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결 설정 시 구성된 정책을 계속해서 사용합니다. 기존 연결에 대한 **show** 명령 출력에는 기존 명령이 반영되며, 기존 연결에 대한 데이터를 포함하지 않는 경우도 있습니다.

예를 들어, 인터페이스에서 QoS **service-policy**를 제거하고 수정된 버전을 다시 추가할 경우, **show service-policy** 명령에서는 새 서비스 정책과 일치하는 새 연결과 연관된 QoS 카운터만 표시합니다. 명령 출력에는 기존 정책에 대한 기존 연결이 더 이상 표시되지 않습니다.

모든 연결에 새 정책이 사용되도록 하려면 현재 연결을 끊은 다음 모든 연결에서 새 정책을 사용하여 다시 연결하도록 해야 합니다.

연결을 끊으려면 다음 명령 중 하나를 입력합니다.

- **clear local-host** [*ip_address*] [**all**]

  이 명령을 사용하면 연결 제한 및 초기 제한 같은 클라이언트당 런타임 상태가 다시 초기화됩니다. 결과적으로 이 명령을 사용하면 이러한 제한을 사용하는 모든 연결이 제거됩니다. 호스트당 모든 현재 연결을 보려면 **show local-host all** 명령을 참조하십시오.

  인수가 없는 경우에도 이 명령을 사용하면 영향을 받는 모든 스루더박스(through-the-box) 연결이 지워집니다. 투더박스(to-the-box) 연결(현재 관리 세션 포함)도 지우려면 **all** 키워드를 사용합니다. 특정 IP 주소에서 연결을 지우려면 *ip_address* 인수를 사용합니다.

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip* [-*src_ip*] [**netmask** *mask*]] [**port** *src_port* [-*src_port*]] [**address** *dest_ip* [-*dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[-*dest_port*]]

  이 명령을 사용하면 모든 상태의 연결이 종료됩니다. 모든 현재 연결을 보려면 **show conn** 명령을 참조하십시오.

  인수가 없는 경우에도 이 명령을 사용하면 모든 스루더박스(through-the-box) 연결이 지워집니다. 투더박스(to-the-box) 연결(현재 관리 세션 포함)도 지우려면 **all** 키워드를 사용합니다. 소스 IP 주소, 목적지 IP 주소, 포트 및/또는 프로토콜을 기준으로 특정 연결을 지우기 위해 원하는 옵션을 지정할 수 있습니다.

ASA 다시 로드

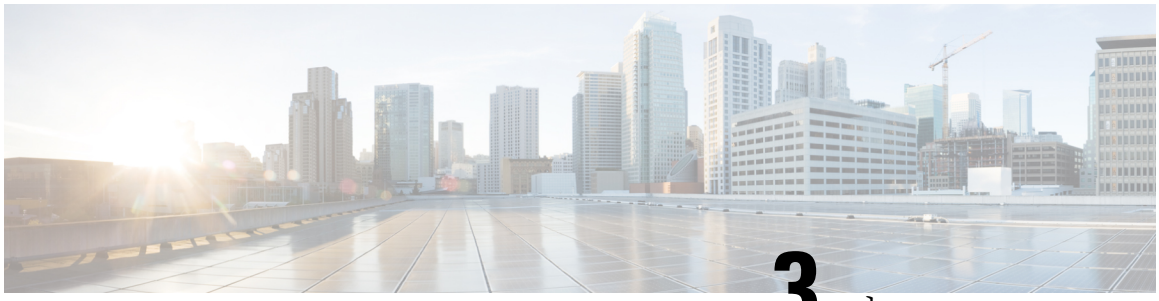
ASA를 다시 로드하려면 다음 절차를 완료하십시오.

프로시저

ASA를 다시 로드합니다.

reload

참고 다중 컨텍스트 모드의 경우 시스템 실행 공간에서만 다시 로드할 수 있습니다.



3 장

라이선스: 제품 인증 키 라이선싱

라이선스는 해당 Cisco ASA에서 활성화되는 옵션을 지정합니다. 이 문서는 모든 물리적 ASA의 PAK(제품 인증 키) 라이센스에 대해 설명합니다. ASAv에 대해서는 라이선스: Smart Software Licensing(Firepower에서의 ASAv, ASA), 115 페이지의 내용을 참조하십시오.

PAK 라이센스 정보

라이선스에 따라 해당 Cisco ASA에서 활성화되는 옵션이 지정됩니다. 라이센스는 160비트(32비트 또는 20바이트 단어 5개) 값으로 된 액티베이션 키로 나타냅니다. 이 값은 일련 번호(11자 문자열) 및 활성화된 기능으로 인코딩됩니다.

사전 설치된 라이센스

기본적으로 ASA는 라이선스가 이미 설치된 상태로 배송됩니다. 이러한 라이센스는 원하는 라이센스를 더 추가할 수 있는 Base 라이센스일 수 있습니다. 또는 주문 내역 및 공급업체에서 설치한 내역에 따라 모든 라이센스가 이미 설치되어 있을 수 있습니다.

관련 항목

PAK 라이센스 모니터링, 94 페이지

영구 라이선스

단일한 영구 액티베이션 키를 설치할 수 있습니다. 영구 액티베이션 키에는 단일한 키로 모든 라이센스 기능이 포함됩니다. 기간별 라이선스를 설치할 경우, ASA에서는 영구 라이선스와 기간별 라이선스를 실행 중인 라이선스로 통합합니다.

관련 항목

영구 라이센스와 기간별 라이센스가 통합되는 원리, 51 페이지

시간 기반 라이센스

영구 라이센스 외에도, 기간별 라이센스를 구매하거나 기간 제한이 있는 평가판 라이센스를 제공받을 수 있습니다. 예를 들어, 단기간에 급증한 동시 SSL VPN 사용자 수를 처리하기 위해 기간별 AnyConnect Premium 라이선스를 구매하거나, 유효 기간이 1년인 Botnet Traffic Filter 기간별 라이선스를 주문할 수 있습니다.

참고 ASA 5506-X 및 ASA 5506W-X에서는 기간별 라이선스를 지원하지 않습니다.

기간별 라이센스 활성화 지침

- 같은 기능을 지원하는 여러 개의 라이센스를 포함하여, 여러 개의 기간별 라이센스를 설치할 수 있습니다. 그러나 기능당 기간별 라이센스는 한 번에 하나만 활성화할 수 있습니다. 비활성 라이센스는 설치된 채로 유지되며 사용할 준비가 되어 있습니다. 예를 들어, 1000-세션 AnyConnect Premium 라이선스 및 2500-세션 AnyConnect Premium 라이선스를 설치할 경우, 이러한 라이선스 중 하나만 활성화할 수 있습니다.
- 키에 여러 기능이 포함된 평가판 라이센스를 활성화할 경우 포함된 기능 중 하나를 지원하기 위해 다른 기간별 라이센스를 활성화할 수 없습니다. 예를 들어, 평가판 라이선스에 Botnet Traffic Filter 및 1000-세션 AnyConnect Premium 라이선스가 포함된 경우 독립형 기간별 2500-세션 AnyConnect Premium 라이선스도 활성화할 수는 없습니다.

기간별 라이센스 타이머 작동 방식

- 기간별 라이선스의 타이머는 ASA에서 해당 라이선스를 활성화할 때 카운트다운이 시작됩니다.
- 라이센스의 기간이 만료되기 전에 기간별 라이센스 사용을 중단할 경우 타이머가 중지됩니다. 타이머는 기간별 라이센스를 다시 활성화할 경우에만 다시 시작됩니다.
- 기간별 라이선스가 활성화되어 있는데 ASA를 종료하면 타이머의 카운트다운이 중지됩니다. ASA가 실행 중일 때는 기간별 라이선스만 계산됩니다. 시스템 클럭 설정은 라이선스에 영향을 주지 않으며, 라이선스 기간에 대한 ASA 작동 계수에만 영향을 줍니다.

영구 라이센스와 기간별 라이센스가 통합되는 원리

기간별 라이센스를 활성화하면 영구 라이센스와 기간별 라이센스의 기능이 통합되어 실행 중인 라이센스가 형성됩니다. 영구 라이센스와 기간별 라이센스가 통합되는 방식은 라이센스의 유형에 따라 달라집니다. 다음 표에는 각 기능 라이센스의 통합 규칙이 나와 있습니다.

참고 영구 라이센스를 사용할 경우에도 기간별 라이센스가 활성화되어 있으면 카운트다운이 계속 진행됩니다.

표 *1:* 기간별 라이센스 통합 규칙

기간별 기능	통합된 라이센스 규칙
AnyConnect Premium 세션	기간별 또는 영구 라이센스 중 더 높은 값이 사용됩니다. 예를 들어, 영구 라이센스가 1000개 세션이고 기간별 라이센스가 2500개 세션일 경우 2500개 세션이 활성화됩니다. 일반적으로 영구 라이센스보다 기능이 적은 기간별 라이센스는 설치하지 않습니다. 이러한 라이센스를 설치할 경우 영구 라이센스가 사용됩니다.
Unified Communications 프록시 세션	기간별 라이센스 세션이 플랫폼 한도 내에서 영구 라이센스에 추가됩니다. 예를 들어, 영구 라이센스가 2500개 세션이고 기간별 라이센스가 1000개 세션일 경우 기간별 라이센스가 활성화되어 있는 한 3500개 세션이 활성화됩니다.
보안 상황	기간별 라이센스 세션이 플랫폼 한도 내에서 영구 컨텍스트에 추가됩니다. 예를 들어, 영구 라이센스가 10개 컨텍스트이고 기간별 라이센스가 20개 컨텍스트일 경우 기간별 라이센스가 활성화되어 있는 한 30개 컨텍스트가 활성화됩니다.
봇네트 트래픽 필터	사용 가능한 Botnet Traffic Filter 라이센스가 없으며 기간별 라이센스가 사용됩니다.
기타	기간별 또는 영구 라이센스 중 더 높은 값이 사용됩니다. 상태가 활성화 또는 비활성화된 라이센스의 경우, 상태가 활성화된 라이센스가 사용됩니다. 숫자 계층이 있는 라이센스의 경우, 더 높은 값이 사용됩니다. 일반적으로 영구 라이센스보다 기능이 적은 기간별 라이센스는 설치하지 않습니다. 이러한 라이센스를 설치할 경우 영구 라이센스가 사용됩니다.

관련 항목

PAK 라이센스 모니터링, 94 페이지

기간별 라이센스 스태킹

대부분의 경우 기간별 라이센스를 갱신해야 할 수 있으며, 기존 라이센스에서 새 라이센스로 원활하게 전환할 수 있습니다. 기간별 라이센스에만 제공되는 기능의 경우, 새 라이센스를 적용하려면 그전에 라이센스가 만료되지 않도록 하는 것이 특히 중요합니다. ASA에서는 기간별 라이선스를 스태킹할 수 있도록 지원하므로 새 라이선스를 조기에 설치하여 라이선스가 만료되거나 라이선스의 기간이 짧아지지 않을까 걱정하지 않아도 됩니다.

기존에 설치된 라이센스와 동일한 기간별 라이센스를 설치한 경우, 라이센스가 통합되며 기간은 통합된 기간과 같습니다.

예를 들면 다음과 같습니다.

1. 52주 Botnet Traffic Filter 라이센스를 설치하고 해당 라이센스를 25주간 사용합니다(27주가 남음).
2. 이후 또 다른 52주 Botnet Traffic Filter 라이센스를 구매합니다. 두 번째 라이센스를 설치할 때 라이센스가 통합되어 기간이 79주가 됩니다(52주 + 27주).

유사한 사례:

1. 8주 1000-세션 AnyConnect Premium 라이선스를 설치하고 2주간 사용합니다(6주 남음).
2. 그런 다음 또 다른 8주 1000-세션 라이센스를 설치하면 라이센스가 통합되어 14주(8주 + 6주) 1000-세션 라이센스가 됩니다.

라이선스가 동일하지 않은 경우(예를 들어 1000-세션 AnyConnect Premium 라이선스 및 2500-세션 라이선스) 라이선스는 통합되지 않습니다. 기능당 기간별 라이센스를 하나만 활성화할 수 있으므로 여러 라이센스 중 하나만 활성화할 수 있습니다.

동일하지 않은 라이선스는 통합되지 않지만 현재 라이선스가 만료될 경우, 같은 기능 라이선스가 설치되어 있으면 ASA에서는 이를 자동으로 활성화합니다.

관련 항목

키 활성화 또는 비활성화, 67 페이지
기간별 라이센스 만료, 52 페이지

기간별 라이센스 만료

현재 기능 라이선스가 만료될 경우, 같은 기능 라이선스가 설치되어 있으면 ASA에서는 이를 자동으로 활성화합니다. 기능에 사용할 수 있는 기간별 라이센스가 없으면 영구 라이센스가 사용됩니다.

기능을 지원하는 추가 기간별 라이선스가 여러 개 있는 경우 ASA에서는 첫 번째 라이선스를 사용합니다. 이 라이선스는 사용자 구성이 가능하지 않으며 내부 작업에 따라 달라집니다. ASA에서 활성화한 라이선스가 아닌 다른 기간별 라이선스를 사용하려면 원하는 라이선스를 수동으로 활성화해야 합니다.

기간별 2500-세션 AnyConnect Premium 라이선스(활성), 기간별 1000-세션 AnyConnect Premium 라이선스(비활성), 영구 500-세션 AnyConnect Premium 라이선스가 있는 경우를 예로 들어보겠습니다. 2500-세션 라이선스가 만료되면 ASA에서는 1000-세션 라이선스를 활성화합니다. 1000-세션 라이선스가 만료되면 ASA에서는 500-세션 영구 라이선스를 사용합니다.

관련 항목

키 활성화 또는 비활성화, 67 페이지

라이센스 참고 사항

다음 섹션에는 라이선스에 대한 자세한 정보가 나와 있습니다.

AnyConnect Plus 및 APEX 라이선스

AnyConnect Plus 또는 Apex 라이선스는 여러 ASA에 적용할 수 있는 다용도 라이선스입니다. 이 모두는 라이선스에서 지정한 대로 사용자 풀을 공유합니다. https://www.cisco.com/go/license를 참조하고 각 ASA에 PAK를 개별적으로 할당하십시오. ASA에 결과 액티베이션 키를 적용하면 VPN 기능이 허용되는 최댓값으로 전환되지만 라이선스를 공유하는 모든 ASA에서 고유한 사용자의 실제 수는 라이선스 한도를 초과하지 않아야 합니다. 자세한 내용은 다음 링크를 참조하십시오.

- Cisco AnyConnect 주문 설명서
- AnyConnect 라이선싱 FAQ(자주 묻는 질문)

참고 AnyConnect Apex 라이선스는 다중 상황 모드에 필요합니다. 또한 다중 상황 모드에서 이 라이선스는 장애 조치 쌍의 각 유닛에 적용되어야 하며, 이 경우 라이선스는 집계되지 않습니다.

기타 VPN 라이선스

기타 VPN 세션에는 다음과 같은 VPN 유형이 포함됩니다.

- IKEv1을 사용하는 IPsec 원격 액세스 VPN
- IKEv1을 사용하는 IPsec 사이트 대 사이트 VPN
- IKEv2를 사용하는 IPsec 사이트 대 사이트 VPN

이 라이센스는 Base 라이센스에 포함됩니다.

결합된 총 VPN 세션, 모든 유형

- 최대 VPN AnyConnect 및 기타 VPN 세션보다 많은 상태에서 최대 VPN 세션이 추가되더라도 전체 세션은 VPN 세션 한도를 초과하면 안 됩니다. 최대 VPN 세션 수를 초과할 경우, ASA가 오버로드될 수 있으므로 네트워크의 크기를 적절하게 조정해야 합니다.

- 클라이언트리스 SSL VPN 세션을 시작한 후 포털에서 AnyConnect 클라이언트 세션을 시작한 경우, 총 1개의 세션이 사용됩니다. 그러나 처음에 AnyConnect 클라이언트를 시작한 후(예: 독립형 클라이언트에서) 클라이언트리스 SSL VPN 포털에 로그인할 경우 2개의 세션이 사용됩니다.

VPN 로드 밸런싱

VPN 로드 밸런싱에는 Strong Encryption(3DES/AES) 라이센스가 필요합니다.

레거시 VPN 라이선스

라이선싱에 관한 모든 관련 정보는 AnyConnect용 보충 최종 사용자 라이선스 계약을 참조하십시오.

참고 다중 상황 모드에서 AnyConnect Apex 라이선스가 필요합니다. 기본 라이선스 또는 레거시 라이선스는 사용할 수 없습니다.

암호화 라이선스

DES 라이센스는 비활성화할 수 없습니다. 3DES 라이센스를 설치한 경우 DES를 계속 사용할 수 있습니다. Strong Encryption만 사용하고 DES를 사용하지 않으려면 모든 관련 명령에서 Strong Encryption만 사용하도록 구성해야 합니다.

캐리어 라이센스

캐리어 라이선스를 사용하면 다음과 같은 검사 기능이 활성화됩니다.

- 배율
- GTP/GPRS
- SCTP

총 TLS 프록시 세션

암호화된 음성 검사에 대한 각 TLS 프록시 세션의 수는 TLS 라이선스 한도를 기준으로 계산됩니다.

TLS 프록시 세션을 사용하는 기타 애플리케이션의 경우 TLS 한도에 가산되지 않습니다. Mobility Advantage Proxy(라이선스가 필요하지 않음)를 예로 들 수 있습니다.

일부 애플리케이션에서는 연결에 다중 세션을 사용할 수 있습니다. 예를 들어, 전화를 기본으로 구성하고 Cisco Unified Communications Manager를 백업할 경우, 2개의 TLS 프록시 연결이 있습니다.

tls-proxy maximum-sessions 명령을 사용하거나 ASDM에서 **Configuration(구성) > Firewall(방화벽) > Unified Communications > TLS Proxy(TLS 프록시)** 창을 사용하여 TLS 프록시 한도를 개별적으로 설정할 수 있습니다. 모델의 한도를 보려면 **tls-proxy maximum-sessions ?** 명령을 입력합니다. 기본 TLS 프록시 한도보다 높은 TLS 프록시 라이선스를 적용할 경우, ASA에서는 TLS 프록시 한도를 라이선스에 맞게 자동으로 설정합니다. TLS 프록시 한도는 라이선스 한도보다 우선합니다. TLS 프록시 한도를 해당 라이선스보다 작게 설정하면 라이선스에서 모든 세션을 사용할 수 없습니다.

참고 라이센스 부품 번호가 "K8"로 끝날 경우(예: 사용자 수 250명 이하의 라이센스), TLS 프록시 세션은 1000으로 제한됩니다. 라이센스 부품 번호가 "K9"로 끝날 경우(예: 사용자 수가 250명 이상인 라이센스), TLS 프록시 세션 한도는 컨피그레이션 및 모델 한도에 따라 달라집니다. K8 및 K9의 경우 해당 라이센스의 내보내기 제한 여부를 참조하며, K8은 제한되지 않고 K9는 제한됩니다.

예를 들어, **clear configure all** 명령을 사용하여 구성을 지우면 TLS 프록시 한도가 모델의 기본값으로 설정됩니다. 이 기본값이 라이선스 한도보다 낮을 경우, **tls-proxy maximum-sessions** 명령을 사용하여 한도를 다시 높이라는 오류 메시지가 표시됩니다(ASDM에서 **TLS Proxy(TLS** 프록시**)** 창 사용). 장애 조치를 사용 중이고 **write standby** 명령을 입력하거나 ASDM에서 **File(**파일**) > Save Running Configuration to Standby Unit(**실행 중인 구성을 대기 유닛에 저장**)**을 사용하여 기본 유닛에서 컨피그레이션 동기화를 시행할 경우, 보조 유닛에서 **clear configure all** 명령이 자동으로 생성되므로 보조 유닛에 경고 메시지가 표시될 수 있습니다. 컨피그레이션 동기화는 기본 유닛에서 TLS 프록시 한도 설정을 복원하므로 이러한 경고 메시지는 무시해도 좋습니다.

연결에 SRTP 암호화 세션을 사용할 수도 있습니다.

- K8 라이센스의 경우 SRTP 세션이 250개로 제한됩니다.
- K9 라이선스의 경우 제한이 없습니다.

참고 미디어 암호화/해독이 필요한 호출만 SRTP 한도에 가산됩니다. 호출에 통과가 설정되어 있으면 두 범례가 모두 SRTP인 경우에도 해당 호출은 한도에 가산되지 않습니다.

VLAN, 최대 개수

어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예를 들면 다음과 같습니다.

```
interface gigabitethernet 0/0.100
vlan 100
```

Botnet Traffic Filter 라이센스

동적 데이터베이스를 다운로드하려면 Strong Encryption(3DES/AES) 라이센스가 필요합니다.

IPS 모듈 라이선스

IPS 모듈 라이선스를 사용하면 ASA에서 IPS 소프트웨어 모듈을 실행할 수 있습니다. 또한 IPS 측에 IPS 서명 서브스크립션이 있어야 합니다.

다음 지침을 참조하십시오.

- 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다.
- 장애 조치의 경우 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이 서브스크립션은 ASA 라이선스가 아니므로 장애 조치에서 공유되지 않습니다.
- 장애 조치를 수행하려면 IPS 서명 서브스크립션에 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이선스와 마찬가지로, IPS 모듈 라이선스는 장애 조치 클러스터 라이선스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 장애 조치 시 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.

공유 AnyConnect 프리미엄 라이센스(AnyConnect 3 및 이전 버전)

참고 ASA에서 공유 라이센스 기능은 AnyConnect 4 이상 라이센싱에서 지원되지 않습니다. AnyConnect 라이센스는 공유되므로 공유 서버 또는 참가자 라이센스가 더 이상 필요하지 않습니다.

공유 라이선스를 사용하면 AnyConnect Premium 세션을 대량으로 구매할 수 있으며, ASA 중 하나를 공유 라이선싱 서버로 구성하고 나머지는 공유 라이선싱 참가자로 구성하여 필요에 따라 ASA의 그룹 간에 세션을 공유할 수 있습니다.

장애 조치 또는 ASA 클러스터 라이센스

몇 가지 예외 사항을 제외하고, 장애 조치 및 클러스터 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 이전 버전의 경우 해당 버전의 라이센스 설명서를 참조하십시오.

장애 조치 라이센스 요구 사항 및 예외 사항

장애 조치 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다. 이 규칙에도 몇 가지 예외가 있습니다. 장애 조치에 대한 올바른 라이센싱 요건은 다음 표를 참조하십시오.

모델	라이센스 요건
ASA 5506-X 및 ASA 5506W-X	• 활성/대기 — Security Plus 라이센스. • 활성/활성 — 지원되지 않음. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.

모델	라이센스 요건
ASA 5512-X - ASA 5555-X	• ASA 5512 X — Security Plus 라이센스. • 기타 모델 — 기본 라이센스. 참고 • 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다. • 다중 상황 모드에서 각 유닛에는 동일한 AnyConnect Apex 라이선스가 있어야 합니다. • 각 유닛에는 동일한 IPS 모듈 라이선스가 있어야 합니다. 또한 두 유닛의 IPS에는 IPS 서명 서브스크립션이 필요합니다. 다음 지침을 참조하십시오. • 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다. • 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이선스가 아니므로 장애 조치에서 공유되지 않습니다. • IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이선스와 마찬가지로, IPS 모듈 라이선스는 장애 조치 클러스터 라이선스 내에서 기술적으로 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
ASAv	ASAv의 장애 조치 라이선스, 124 페이지을 참조하십시오.
Firepower 2100의 ASA	Firepower 2100의 장애 조치 라이선스, 125 페이지을 참조하십시오.
ASA - Firepower 4100/9300 섀시	ASA의 장애 조치 라이선스 - Firepower 4100/9300 섀시, 126 페이지을 참조하십시오.

모델	라이센스 요건
기타 모든 모델	Base 라이선스 또는 Standard 라이선스. 참고 • 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다. • 다중 상황 모드에서 각 유닛에는 동일한 AnyConnect Apex 라이선스가 있어야 합니다.

참고 유효한 영구 키가 필요합니다. 드문 경우지만 PAK 인증 키를 제거할 수 있습니다. 키가 모두 0으로 구성되어 있으면 장애 조치를 활성화하기 전에 유효한 인증 키를 다시 설치해야 합니다.

ASA 클러스터 라이센스 요구 사항 및 예외 사항

클러스터 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 일반적으로 마스터 유닛에만 라이센스를 구매하며, 슬레이브 유닛에서는 마스터 라이센스를 상속합니다. 여러 유닛에 라이센스가 있는 경우, 해당 라이센스는 단일하게 실행되는 ASA 클러스터 라이센스로 통합됩니다.

이 규칙에는 예외가 있습니다. 클러스터링에 대한 올바른 라이센스 요건은 다음 표를 참조하십시오.

모델	라이센스 요건
ASA 5585-X	클러스터 라이센스, 최대 16개까지 지원. 참고 각 유닛에 동일한 암호화 라이센스가 있어야 합니다. 각 유닛에 동일한 10개의 GE I/O/Security Plus 라이센스(SSP-10 및 -20이 포함된 ASA 5585-X)가 있어야 합니다.
ASA 5516-X	Base 라이선스, 유닛 2개 지원. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
ASA 5512-X	Security Plus 라이센스, 유닛 2개 지원. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Base 라이센스, 유닛 2개 지원. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.

모델	라이센스 요건
ASA Firepower 4100/9300 섀시	ASA의 ASA 클러스터 라이선스 - Firepower 4100/9300 섀시, 127 페이지을 참조하십시오.
다른 모든 모델	지원 안 함

장애 조치 또는 ASA 클러스터 통합 방식

장애 조치 쌍 또는 ASA 클러스터의 경우, 각 유닛의 라이센스는 단일하게 실행되는 클러스터 라이센스로 통합됩니다. 각 유닛에 별도의 라이센스를 구매할 경우, 통합된 라이센스에서는 다음 규칙을 사용합니다.

- 숫자 계층(예: 세션 수)이 있는 라이센스의 경우, 각 유닛의 라이센스 값은 플랫폼 한도 내에서 통합됩니다. 사용 중인 모든 라이센스가 기간별 라이센스인 경우, 라이센스의 기간이 동시에 카운트다운됩니다.

  장애 조치 예:

  - 2개의 ASA에 각각 10개의 TLS 프록시 세션이 설치되어 있습니다. 이러한 라이선스는 총 20개의 TLS 프록시 세션으로 통합됩니다.
  - 1000개의 TLS 프록시 세션이 있는 ASA 5545-X를 사용 중이며 다른 제품에는 2000개의 세션이 있습니다. 플랫폼 한도가 2000개이므로 통합된 라이선스에서는 2000개의 TLS 프록시 세션을 허용합니다.
  - 2개의 ASA 5545-X ASA 중 하나에는 20개의 상황이 있고 나머지에는 10개의 상황이 있습니다. 통합된 라이선스에서는 30개의 상황을 허용합니다. 액티브/액티브 장애 조치의 경우 컨텍스트는 두 유닛 간에 분리됩니다. 예를 들어, 한 유닛에서 18개의 컨텍스트를 사용하고 다른 유닛에서 12개의 컨텍스트를 사용하는 방식으로 총 30개를 사용할 수 있습니다.

  ASA 클러스터링 예:

  - 기본값인 2개의 상황이 있는 ASA 5516-X ASA를 2개 보유하고 있습니다. 플랫폼 한도가 5개이므로 통합된 라이선스에서는 최대 4개의 상황을 허용합니다. 따라서 기본 유닛에서 최대 4개의 상황을 구성할 수 있습니다. 각 보조 유닛에서도 구성 복제를 통해 4개의 상황을 포함할 수 있습니다.
  - 4개의 ASA 5516-X ASA가 있으며, 3개의 각 유닛에는 5개의 상황이 있고 1개 유닛에는 기본값인 2개의 상황이 있습니다. 플랫폼 한도가 5개이므로 라이선스가 통합되면 총 5개의 상황을 지원합니다. 따라서 기본 유닛에서 최대 5개의 상황을 구성할 수 있습니다. 각 보조 유닛에서도 구성 복제를 통해 5개의 상황을 포함할 수 있습니다.

- 상태가 활성화 또는 비활성화된 라이센스의 경우, 상태가 활성화된 라이센스가 사용됩니다.
- 활성화 또는 비활성화된 기간별 라이센스(숫자 계층이 없는)의 경우, 모든 라이센스의 기간이 통합됩니다. 기본/마스터 유닛에서 라이센스 기간의 카운트다운을 먼저 시작하며, 해당 기간이 만료되면 보조/슬레이브 유닛에서 라이센스 기간의 카운트다운을 시작하는 순으로 진행됩니다.

이 규칙은 액티브/액티브 장애 조치 및 ASA 클러스터링에도 적용되며 모든 유닛이 활성화 상태로 작동되는 경우에도 마찬가지입니다.

예를 들어, 두 유닛에 48주의 기간이 남은 Botnet Traffic Filter 라이센스가 있을 경우 통합된 기간은 96주입니다.

관련 항목

PAK 라이센스 모니터링, 94 페이지

장애 조치 또는 ASA 클러스터 유닛 간의 통신 해제

유닛의 통신이 30일 이상 끊어지면 각 유닛에서는 설치된 라이센스를 로컬로 전환합니다. 30일의 유예 기간 동안, 실행 중인 통합 라이센스는 모든 유닛에서 계속 사용됩니다.

30일의 유예 기간 도중 통신이 복원되면 기간별 라이센스의 경우 기본/마스터 라이센스에서 경과된 시간이 공제됩니다. 기본/마스터 라이센스가 만료된 경우, 보조/슬레이브 라이센스에서만 카운트다운을 시작합니다.

30일 동안 통신이 복원되지 않으면 기간별 라이센스의 경우 모든 유닛 라이센스(설치된 경우)에서 시간이 공제됩니다. 이러한 라이센스는 별도의 라이센스로 처리되며 통합된 라이센스의 이점을 누릴 수 없습니다. 경과된 시간에는 30일의 유예 기간이 포함됩니다.

예를 들면 다음과 같습니다.

1. 두 유닛에 52주 Botnet Traffic Filter 라이센스가 설치되어 있습니다. 실행 중인 통합된 라이센스에서는 총 104주의 기간을 허용합니다.
2. 유닛은 10주간 장애 조치 유닛/ASA 클러스터 역할을 수행하면, 94주는 통합된 라이센스에 남습니다(42주는 기본/마스터에, 52주는 보조/슬레이브에).
3. 유닛의 통신이 끊길 경우(예: 기본/마스터 유닛에 오류가 발생할 경우), 보조/슬레이브 유닛에서 통합된 라이센스를 계속 사용하며 94주부터 카운트다운을 계속 진행합니다.
4. 기간별 라이센스 동작은 통신이 언제 복원되었는지에 따라 달라집니다.
   - 30일 이내 — 경과된 시간이 기본/마스터 유닛 라이센스에서 공제됩니다. 이 경우, 4주 후에 통신이 복원되었습니다. 따라서 기본/마스터 라이센스에서 4주가 공제되어 90주로 통합되었습니다(38주는 기본에, 52주는 보조에).
   - 30일 후 — 경과된 시간이 두 유닛에서 모두 공제됩니다. 이 경우, 6주 후에 통신이 복원되었습니다. 따라서 두 기본/마스터 및 보조/슬레이브 라이센스에서 6주가 공제되어, 84주로 통합되었습니다(36주는 기본/마스터에, 46주는 보조/슬레이브에).

장애 조치 쌍 업그레이드

장애 조치 쌍의 경우 두 유닛에 동일한 라이센스가 필요하지 않으므로, 다운타임 없이 각 유닛에 새 라이센스를 적용할 수 있습니다. 다시 로드해야 하는 영구 라이센스를 적용할 경우 다시 로드하는 동안 다른 유닛으로 장애 조치가 시작될 수 있습니다. 두 유닛을 모두 다시 로드해야 하는 경우 이를 별도로 다시 로드하여 다운타임을 방지할 수 있습니다.

관련 항목

키 활성화 또는 비활성화, 67 페이지

No Payload Encryption 모델

일부 No Payload Encryption 모델을 구입할 수 있습니다. 일부 국가의 경우, Cisco ASA Series에서 페이로드 암호화를 활성화할 수 없습니다. ASA 소프트웨어에서는 No Payload Encryption 모델을 감지하고 다음 기능을 비활성화할 수 있습니다.

- 통합 통신
- VPN

여전히 Strong Encryption(3DES/AES) 라이센스를 관리 연결에 사용하도록 설치할 수 있습니다. 예를 들어 ASDM HTTPS/SSL, SSHv2, 텔넷 및 SNMPv3를 사용할 수 있습니다. 또한 봇넷(Botnet) Traffic Filter(SSL 사용)용 동적 데이터베이스를 다운로드할 수도 있습니다.

라이센스를 볼 경우, VPN 및 통합 통신 라이센스가 나열되지 않습니다.

관련 항목

PAK 라이센스 모니터링, 94 페이지

라이센스 FAQ

AnyConnect Premium 및 **Botnet Traffic Filter** 같은 여러 개의 기간별 라이센스를 활성화할 수 있습니까**?**

예. 기능당 기능별 라이센스는 한 번에 하나씩 활성화할 수 있습니다.

기간별 라이센스를 "스태킹"하여 시간 제한이 만료되었을 때 다음 라이센스를 자동으로 사용하도록 할 수 있습니까**?**

예. 동일한 라이센스의 경우, 여러 기간별 라이센스를 설치할 때 시간 제한이 통합됩니다. 동일하지 않은 라이선스의 경우(예: 1000-세션 AnyConnect Premium 라이선스 및 2500-세션 라이선스), ASA에서는 기능에 사용할 수 있는 다음 기간별 라이선스를 자동으로 활성화합니다.

활성 상태인 기간별 라이센스는 그대로 유지하면서 새 영구 라이센스를 설치할 수 있습니까**?**

예. 영구 라이센스를 활성화해도 기간별 라이센스에는 영향을 미치지 않습니다.

장애 조치를 위해 공유 라이센스 서버를 기본 유닛으로 사용하고**,** 공유 라이센스 백업 서버를 보조 유닛으로 사용할 수 있습니까**?**

아니요. 보조 유닛에는 기본 유닛에서 실행 중인 것과 동일한 라이센스가 있습니다. 공유 라이센스 서버에는 서버 라이센스가 필요합니다. 백업 서버에는 참가자 라이센스가 필요합니다. 백업 서버는 두 백업 서버의 개별적인 장애 조치 쌍이 될 수 있습니다.

장애 조치 쌍의 보조 유닛에 동일한 라이센스를 구매해야 합니까**?**

아니요. 버전 8.3(1)부터는 두 유닛에 같은 라이센스가 없어도 됩니다. 일반적으로 기본 유닛에만 라이센스를 구매하며, 보조 유닛이 액티브 유닛이 되면 보조 유닛에서 기본 라이센스를 상속합

니다. 보조 유닛에 별도의 라이센스가 있는 경우(예: 이전 8.3 소프트웨어에 같은 라이센스를 구매한 경우), 라이센스는 모델의 한도 내에서 하나의 실행 중인 장애 조치 클러스터 라이센스로 통합됩니다.

공유 **AnyConnect Premium** 라이센스 외에 기간별 또는 영구 **AnyConnect Premium** 라이센스를 사용할 수 있습니까**?**

예. 공유 라이센스는 로컬로 설치된 라이센스(기간별 또는 영구)가 모두 사용된 세션 이후에만 사용됩니다.

참고 공유 라이선싱 서버에서는 영구 AnyConnect Premium 라이선스가 사용되지 않습니다. 그러나 기간별 라이선스는 공유 라이선싱 서버 라이선스와 동시에 사용할 수 있습니다. 이 경우, 기간별 라이센스 세션은 로컬 AnyConnect Premium 세션에만 사용할 수 있습니다. 해당 세션은 참가자가 사용할 공유 라이센스 풀에 추가할 수 없습니다.

PAK 라이센스에 대한 지침

상황 모드 지침

다중 컨텍스트 모드의 경우 시스템 실행 영역에서 액티베이션 키를 적용합니다.

장애 조치 지침

장애 조치 또는 ASA 클러스터 라이센스, 56 페이지를 참조하십시오.

모델 지침

- 스마트 라이센싱은 ASAv에서만 지원됩니다.
- 공유 라이센스는 ASAv, ASA 5506-X, ASA 5508-X 및 ASA 5516-X에서 지원되지 않습니다.
- ASA 5506-X 및 ASA 5506W-X는 기간별 라이선스를 지원하지 않습니다.

업그레이드 및 다운그레이드 지침

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 액티베이션 키는 계속 호환 가능합니다. 그러나 다운그레이드 기능을 유지하려는 경우 문제가 생길 수 있습니다.

- 버전 8.1 이하로 다운그레이드 — 업그레이드 후 *8.2* 이전에 도입된 추가 기능 라이센스를 활성화할 경우, 다운그레이드를 수행하면 액티베이션 키가 이전 버전과 계속 호환됩니다. 그러나 *8.2* 이상 버전에 도입된 기능 라이센스를 활성화할 경우에는 액티베이션 키가 이전 버전과 호환되지 않습니다. 호환되지 않는 라이센스 키가 있을 경우 다음 지침을 참조하십시오.
  - 이전에 이전 버전에서 액티베이션 키를 입력한 경우 ASA에서는 해당 키를 사용합니다(8.2 이상 버전에서 활성화한 새 라이선스가 없는 경우).

- 새 시스템이 있으나 이전 액티베이션 키가 없는 경우, 이전 버전과 호환되는 새 액티베이션 키를 요청해야 합니다.

- 버전 8.2 이하로 다운그레이드 — 버전 8.3에는 더욱 강력한 기간별 키 용도 및 장애 조치 라이센스 변경 사항이 도입되었습니다.
  - 둘 이상의 시간 기준 액티베이션 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다. 최근 기간별 라이센스가 8.3에 도입된 기능에 사용되는 라이센스인 경우, 이전 버전에서 사용할 수 없더라도 해당 라이센스는 활성화 라이센스 상태로 유지됩니다. 영구 키 또는 유효한 기간별 키를 다시 입력합니다.
  - 장애 조치 쌍에 일치하지 않는 라이센스가 있을 경우 다운그레이드를 수행하면 장애 조치가 비활성화됩니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.
  - 기간별 라이센스를 설치하였으나 8.3 버전에 도입된 기능에 사용되는 라이센스인 경우, 다운그레이드를 수행하면 해당 기간별 라이센스가 활성화 상태로 유지됩니다. 기간별 라이센스를 비활성화하려면 영구 키를 다시 입력해야 합니다.

추가 지침

- 액티베이션 키는 컨피그레이션 파일에 저장되지 않으며, 플래시 메모리에 숨겨진 파일로 저장됩니다.
- 액티베이션 키는 디바이스의 일련 번호와 연결되어 있습니다. 기능 라이센스는 디바이스 간에 이동할 수 없습니다(하드웨어 오류가 발생한 경우는 예외). 하드웨어 오류로 인해 디바이스를 교체해야 하고 Cisco TAC에서 지원되는 문제인 경우, Cisco Licensing Team에 문의하여 기존 라이센스를 새 일련 번호에 보낼 수 있습니다. Cisco Licensing Team에서는 제품 승인 키 참조 번호와 기존 일련 번호를 요청합니다.
- 라이선싱에 사용된 일련 번호는 **show version** 출력에서 확인된 일련 번호입니다. 이 시리얼 번호는 하드웨어 외부에 인쇄된 섀시 시리얼 번호와는 다릅니다. 섀시 시리얼 번호는 기술 지원에 사용되지만 라이선싱에 대해서는 사용되지 않습니다.
- 구매한 후에는 환불 또는 라이센스 업그레이드를 위해 라이센스를 반환할 수 없습니다.
- 하나의 유닛에 동일한 기능을 지원하는 2개의 개별 라이센스를 함께 추가할 수 없습니다. 예를 들어, 25-세션 SSL VPN 라이센스를 구매하고 나중에 50-세션 라이센스를 구매한 경우, 세션 75개를 사용할 수 없으며 최대 50개의 세션을 사용할 수 있습니다. (업그레이드 가격으로 더 많은 라이센스(예: 25개에서 75개 세션)를 구매하게 될 수 있습니다. 이러한 유형의 업그레이드는 2개의 개별 라이센스를 함께 추가하는 경우와 구분해야 합니다.)
- 모든 라이센스 유형을 활성화할 수 있으나, 일부 기능은 서로 호환되지 않을 수 있습니다. AnyConnect Essentials 라이센스의 경우 AnyConnect Premium 라이센스, Shared AnyConnect Premium 라이센스, Advanced Endpoint Assessment 라이센스와 호환되지 않습니다. 기본적으로 AnyConnect Essentials 라이센스를 설치할 경우(해당 모델에 사용 가능한 경우), 위의 라이센스 대신 이 라이

센스가 사용됩니다. **webvpn**을 사용한 다음, **no anyconnect-essentials** 명령 을 사용하여 구성에서 AnyConnect Essentials 라이선스를 비활성화하면 다른 라이선스의 사용을 복원할 수 있습니다.

PAK 라이센스 구성

이 섹션에서는 활성화 키를 얻는 방법 및 이를 활성화하는 방법에 대해 설명합니다. 이 키를 비활성화할 수도 있습니다.

라이선스 PAK 주문 및 활성화 키 획득

ASA에서 라이선스를 설치하려면 제품 인증 키가 필요하며 액티베이션 키는 Cisco.com에 등록하여 얻을 수 있습니다. 그런 다음 ASA에서 액티베이션 키를 입력할 수 있습니다. 각 기능 라이선스별로 별도의 제품 인증 키를 구매해야 합니다. 단일 액티베이션 키를 제공하도록 PAK가 통합됩니다. 디바이스의 상자에서 모든 라이선스 PAK를 받을 수도 있습니다. ASA에는 사용할 자격이 있는 경우 강력한 암호화(3DES/AES) 라이선스와 함께 Base 또는 Security Plus 라이선스가 사전에 설치됩니다. 강력한 암호화 라이선스(무료)를 수동으로 요청해야 하는 경우, http://www.cisco.com/go/license를 참조하십시오.

시작하기 전에

디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager에서 라이선스를 관리할 수 있습니다.

https://software.cisco.com/#module/SmartLicensing

아직 어카운트가 없는 경우 새 어카운트를 설정합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

프로시저

단계 **1** 추가 라이선스를 구매하려면 http://www.cisco.com/go/ccw를 참조하십시오. 다음 AnyConnect 주문 가이드 및 FAQ를 참조하십시오.

- Cisco AnyConnect 주문 설명서
- AnyConnect 라이선싱 FAQ(자주 묻는 질문)

라이선스를 주문하면 제품 인증 키(PAK)와 이메일을 받게 됩니다. AnyConnect 라이선스의 경우, 사용자 세션의 동일한 풀을 사용하는 여러 ASA에 적용할 수 있는 다용도의 PAK를 받습니다. 경우에 따라 PAK 이메일을 받는 데 며칠이 걸릴 수 있습니다.

ASA FirePOWER 모듈은 ASA에서 제공되는 별도의 라이선싱 메커니즘을 사용합니다. 자세한 내용은 모듈용 빠른 시작 가이드를 참조하십시오.

단계 **2** 다음 명령을 입력하여 ASA의 시리얼 번호를 가져옵니다.

show version | grep Serial

라이선싱에 사용된 일련 번호는 하드웨어 외부에 인쇄된 섀시 일련 번호와는 다릅니다. 섀시 시리얼 번호는 기술 지원에 사용되지만 라이선싱에 대해서는 사용되지 않습니다.

단계 **3** 액티베이션 키를 얻으려면 다음 라이선싱 웹 페이지로 이동합니다.

http://www.cisco.com/go/license

단계 **4** 메시지가 표시되면 다음 정보를 입력합니다.

- 제품 승인 키(키가 여러 개 있는 경우, 그중 첫 번째 키를 입력합니다. 각 키를 별도의 프로세스로 입력해야 합니다.)
- ASA의 일련 번호
- 이메일 주소

액티베이션 키는 자동으로 생성되며 사용자가 제공한 이메일 주소로 전송됩니다. 이 키에는 영구 라이센스에 대해 현재까지 등록한 모든 기능이 포함됩니다. 기간별 라이센스의 경우, 각 라이센스에는 별도의 액티베이션 키가 있습니다.

단계 **5** 추가 제품 인증 키가 있는 경우 각 제품 인증 키의 프로세스를 반복합니다. 제품 승인 키를 모두 입력하면, 등록한 모든 영구 기능이 포함된 최종 액티베이션 키가 제공됩니다.

단계 **6** 키 활성화 또는 비활성화, 67 페이지에 따라 액티베이션 키를 설치합니다.

강력한 암호화 라이선스 획득

ASDM(및 기타 다른 기능)을 사용하려면 강력한 암호화(3DES/AES) 라이선스를 설치해야 합니다. ASA에 강력한 암호화 라이선스가 사전에 설치되어 있지 않으면 무료로 요청할 수 있습니다. 국가별로 강력한 암호화 라이선스 자격을 얻어야 합니다.

프로시저

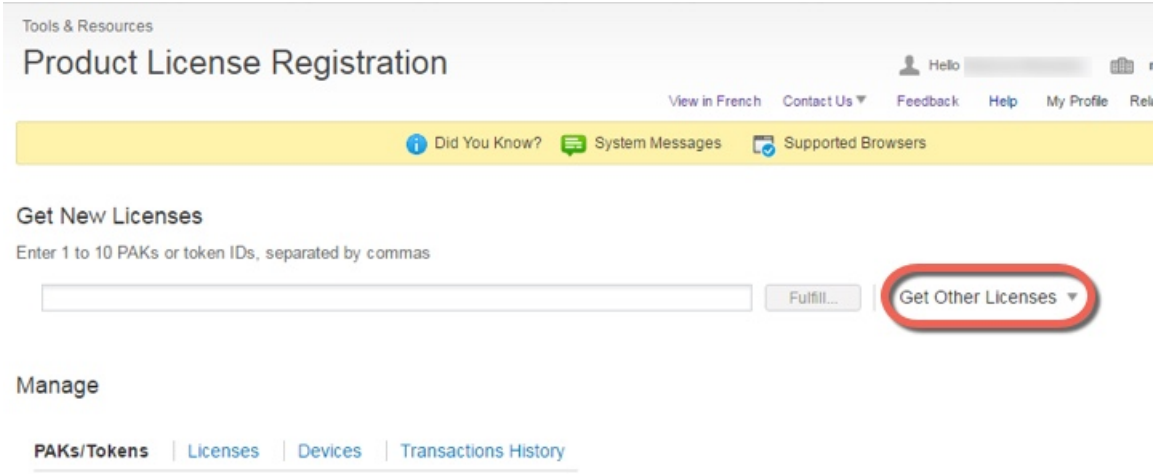
단계 **1** 다음 명령을 입력하여 ASA의 시리얼 번호를 가져옵니다.

show version | grep Serial

이 시리얼 번호는 하드웨어 외부에 인쇄된 섀시 시리얼 번호와는 다릅니다. 섀시 시리얼 번호는 기술 지원에 사용되지만 라이선싱에 대해서는 사용되지 않습니다.

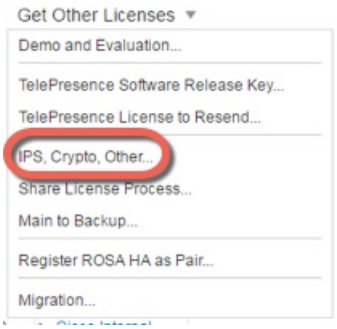
단계 **2** https://www.cisco.com/go/license를 참조하고 **Get Other Licenses**(기타 라이선스 가져오기)를 클릭합니다.

그림 *1:* 다른 라이선스 가져오기



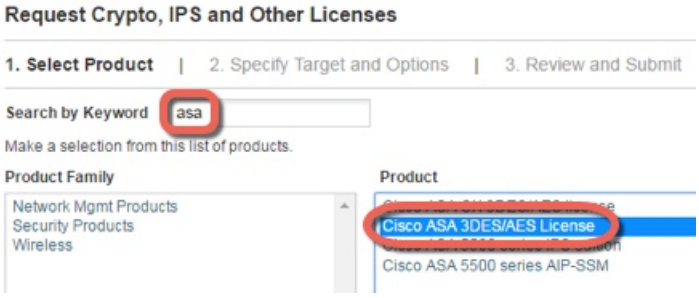
단계 **3** **IPS, Crypto, Other(IPS,** 암호화**,** 기타**)**를 선택합니다.

그림 *2: IPS,* 암호화*,* 기타



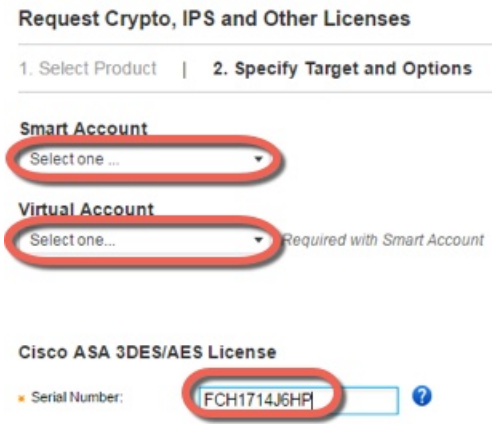
단계 **4** **Search by Keyword(**키워드별 검색**)** 필드에서 **asa**를 입력하고 **Cisco ASA 3DES/AES License(Cisco ASA 3DES/AES** 라이선스**)**를 선택합니다.

그림 *3: Cisco ASA 3DES/AES* 라이선스



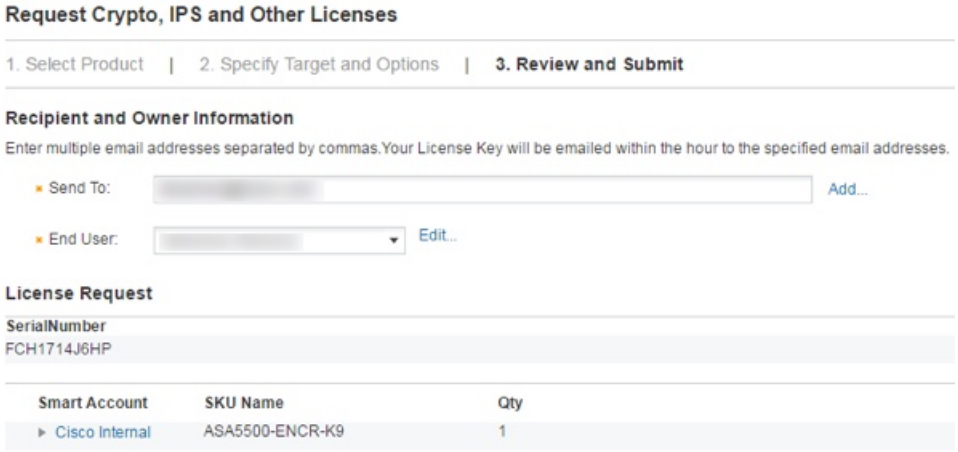
단계 **5** **Smart Account(**스마트 어카운트**), Virtual Account(**가상 어카운트**)**를 선택하고 ASA **Serial Number(**시리얼 번호**)**를 입력한 후에 **Next(**다음**)**를 클릭합니다.

그림 *4:* 스마트 어카운트, 가상 어카운트, 및 시리얼 번호



단계 **6** 이메일 전송 주소 및 최종 사용자 이름이 자동으로 채워집니다. 필요 시 추가 이메일 주소를 입력합니다. **I Agree(**동의합니다**.)** 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

그림 *5:* 제출



단계 **7** 그러면 액티베이션 키가 포함된 이메일이 수신됩니다. 하지만 **Manage(**관리**)** > **Licenses(**라이선스**)** 영역에서 키를 즉시 다운로드할 수도 있습니다.

단계 **8** 키 활성화 또는 비활성화, 67 페이지에 따라 액티베이션 키를 적용합니다.

키 활성화 또는 비활성화

이 섹션에서는 새 액티베이션 키를 입력하고, 기간별 키를 활성화 및 비활성화하는 방법을 설명합니다.

시작하기 전에

- 다중 컨텍스트 모드인 경우, 시스템 실행 영역에 액티베이션 키를 입력합니다.

- 일부 영구 라이선스의 경우 활성화한 후 ASA를 다시 로드해야 합니다. 다음 표에는 다시 로드해야 하는 라이센스가 나열되어 있습니다.

표 *2:* 영구 라이센스 다시 로드 요건

모델	다시 로드해야 하는 라이센스 작업
모든 모델	암호화 라이센스 다운그레이드

프로시저

단계 **1** ASA에 액티베이션 키를 적용합니다.

activation-key *key* [**activate** | **deactivate**]

예제**:**

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

이 키는 각 요소 간에 하나의 공백이 있는 5개 요소로 된 16진수 문자열입니다. 맨 앞의 0x 지정자는 선택 사항이며, 모든 값은 16진수로 가정합니다.

하나의 영구 키를 설치하고, 여러 개의 기간별 키를 설치할 수 있습니다. 새 영구 키를 입력하면 이전에 설치한 키를 덮어씁니다.

activate 및 **deactivate** 키워드는 기간별 키에만 사용할 수 있습니다. 값을 입력하지 않으면 **activate**가 기본값이 됩니다. 지정된 기능에 활성화한 최종 기간별 키가 활성화 상태의 키입니다. 활성화된 기간별 키를 비활성화려면 **deactivate** 키워드를 입력합니다. 키를 처음 입력하고 **deactivate**를 지정하면 ASA에 설치된 키가 비활성 상태가 됩니다.

단계 **2** (필요할 수 있음) ASA를 다시 로드합니다.

reload

일부 영구 라이선스의 경우 새 액티베이션 키를 입력한 후 ASA를 다시 로드해야 합니다. 다시 로드해야 할 경우 다음과 같은 메시지가 표시됩니다.

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

관련 항목

시간 기반 라이센스, 50 페이지

공유 라이센스 구성(AnyConnect 3 및 이전 버전)

참고 ASA에서 공유 라이센스 기능은 AnyConnect 4 이상 라이센싱에서 지원되지 않습니다. AnyConnect 라이센스는 공유되므로 공유 서버 또는 참가자 라이센스가 더 이상 필요하지 않습니다.

이 섹션에서는 공유 라이센스 서버 및 참가자를 구성하는 방법을 설명합니다.

공유 라이센스 정보

공유 라이선스를 사용하면 AnyConnect Premium 세션을 대량으로 구매할 수 있으며, ASA 중 하나를 공유 라이선스 서버로 구성하고 나머지는 공유 라이선스 참가자로 구성하여 필요에 따라 ASA의 그룹 간에 세션을 공유할 수 있습니다.

공유 라이센스 서버 및 참가자 정보

다음 단계에서는 공유 라이센스가 어떤 방식으로 운영되는지 설명합니다.

1. 어떤 ASA가 공유 라이선싱 서버가 되어야 하는지 결정하고, 디바이스 일련 번호를 사용하여 공유 라이선싱 서버의 라이선스를 구매합니다.
2. 어떤 ASA가 공유 라이선싱 참가자(공유 백업 서버 포함)가 되어야 하는지 결정하고, 각 디바이스 일련 번호를 사용하여 각 디바이스의 공유 라이선싱 참가자 라이선스를 얻습니다.
3. (선택 사항) 두 번째 ASA를 공유 라이선싱 백업 서버로 지정합니다. 하나의 백업 서버만 지정할 수 있습니다.

참고 공유 라이센스 백업 서버에는 참가자 라이센스만 필요합니다.

4. 공유 라이센스 서버에서 공유 암호를 구성합니다. 공유 암호를 보유한 모든 참가자는 공유 라이센스를 사용할 수 있습니다.
5. ASA를 참가자로 구성하면 ASA에서는 로컬 라이선스 및 모델 정보를 비롯한 자체 정보를 전송하여 공유 라이선싱 서버에 등록합니다.

참고 참가자는 IP 네트워크를 통해 서버와 통신을 수행할 수 있어야 하며, 같은 서브넷에 있을 필요는 없습니다.

6. 공유 라이센스 서버에서는 참가자가 서버에 폴링하는 빈도와 관련된 정보에 응답합니다.
7. 참가자가 로컬 라이센스의 세션을 모두 사용할 경우, 추가 세션을 50-세션 늘려달라는 요청이 공유 서버에 전송됩니다.

8. 공유 라이센스 서버에서는 공유 라이센스에 응답합니다. 참가자가 사용한 총 세션 수는 플랫폼 모델의 최대 세션 수를 초과할 수 없습니다.

참고 공유 라이센스 서버는 공유 라이센스 풀에도 참가할 수 있습니다. 참가를 위해 참가자 라이센스 및 서버 라이센스를 구매하지 않아도 됩니다.

   1. 공유 라이센스 풀에 참가자가 사용할 세션이 충분히 남아 있지 않은 경우, 서버에서는 최대한 사용 가능한 세션 수에 응답합니다.
   2. 참가자는 서버에서 요청을 충분히 충족할 때까지 추가 세션을 요청하는 새로 고침 메시지를 계속 전송하게 됩니다.

9. 참가자에 대한 로드가 줄어들면 공유 세션을 릴리스하라는 메시지가 서버에 전송됩니다.

참고 ASA에서는 서버와 참가자 간에 SSL을 사용하여 모든 통신을 암호화합니다.

참가자와 서버 간의 통신 문제

참가자와 서버 간의 통신 문제에 대한 내용은 다음 지침을 참조하십시오.

- 참가자가 새로 고침 간격이 3번 지난 후 새로 고침 메시지를 전송하지 못하면 서버에서는 공유 라이센스 풀에 세션을 다시 릴리스합니다.
- 참가자가 새로 고침을 전송할 라이센스 서버에 도달하지 못할 경우, 참가자는 서버에서 받은 공유 라이센스를 최대 24시간 동안 계속 사용할 수 있습니다.
- 24시간 후에도 참가자가 라이센스 서버와 계속 통신을 수행하지 못하면, 세션이 여전히 필요한 경우에도 참가자는 공유 라이센스를 릴리스합니다. 참가자는 설정된 기존 연결을 남겨두지만 라이센스 제한을 넘는 새 연결은 수락할 수 없습니다.
- 참가자가 24시간이 만료되기 전에 서버에 다시 연결하였으나 서버에서 참가자 세션이 만료된 경우, 참가자는 해당 세션에 대해 새 요청을 전송해야 합니다. 서버에서는 참가자에게 다시 할당할 수 있는 최대한 많은 수의 세션에 응답합니다.

공유 라이센싱 백업 서버 정보

백업 역할을 수행할 수 있도록 하려면 공유 라이센스 백업 서버를 기본 공유 라이센스 서버로 올바르게 등록해야 합니다. 등록이 완료되면 기본 공유 라이센스 서버 설정 및 공유 라이센스 정보(예: 등록된 참가자 목록 및 현재 라이센스 사용량 포함)가 백업과 동기화됩니다. 기본 서버 및 백업 서버에서는 10초 간격으로 데이터를 동기화합니다. 최초 동기화를 완료하면 백업 서버에서는 다시 로드된 경우에도 백업 업무를 성공적으로 수행할 수 있습니다.

기본 서버가 중단되면 백업 서버에서 서버 작업을 이어받습니다. 백업 서버의 참가자에 대한 발급 세션이 중단되고, 기존 세션이 만료된 후 백업 서버에서는 최대 30일간 연속으로 작업을 수행할 수 있

습니다. 30일 내에 기본 서버를 복구해야 합니다. 15일에 중요도가 높은 syslog 메시지가 전송되며 30일에 다시 한 번 전송됩니다.

기본 서버가 다시 가동되면 기본 서버에서는 백업 서버와 동기화를 수행한 후 서버 작업을 이어받습니다.

백업 서버가 활성화되어 있지 않을 때에는 기본 공유 라이센스 서버의 일반 참가자 역할을 수행합니다.

참고 기본 공유 라이센스 서버를 처음 시작할 경우, 백업 서버는 개별적으로 5일 동안만 작동될 수 있습니다. 작동 한도는 30일에 도달할 때까지 일별로 증가합니다. 또한 기본 서버가 해당 기간에 중단될 경우, 백업 서버의 작동 한도는 일별로 감소합니다. 기본 서버가 다시 작동되면 백업 서버의 한도는 다시 일별로 증가합니다. 예를 들어, 기본 서버가 20일간 중단되었고 백업 서버가 해당 기간 동안 활성화되어 있었다면, 백업 서버의 남은 기간 한도는 10일밖에 되지 않습니다. 백업 서버에서는 20일 이상 백업을 비활성 상태로 유지한 후 최대 30일을 "재충전"할 수 있습니다. 이러한 재충전 기능은 공유 라이센스의 남용을 줄이기 위해 구현되었습니다.

장애 조치 및 공유 라이센스

이 섹션에서는 공유 라이센스가 장애 조치와 어떻게 상호 작용하는지 설명합니다.

장애 조치 및 공유 라이센스 서버

이 섹션에서는 기본 서버와 백업 서버가 장애 조치와 어떤 방식으로 상호 작용하는지 설명합니다. 공유 라이선싱 서버에서는 ASA와 마찬가지로 일반적인 업무(예: VPN 게이트웨이 및 방화벽과 같은 기능 수행)도 수행하므로, 안정성을 높이기 위해서는 기본 및 백업 공유 라이선싱 서버에 대한 장애 조치를 구성해야 할 수 있습니다.

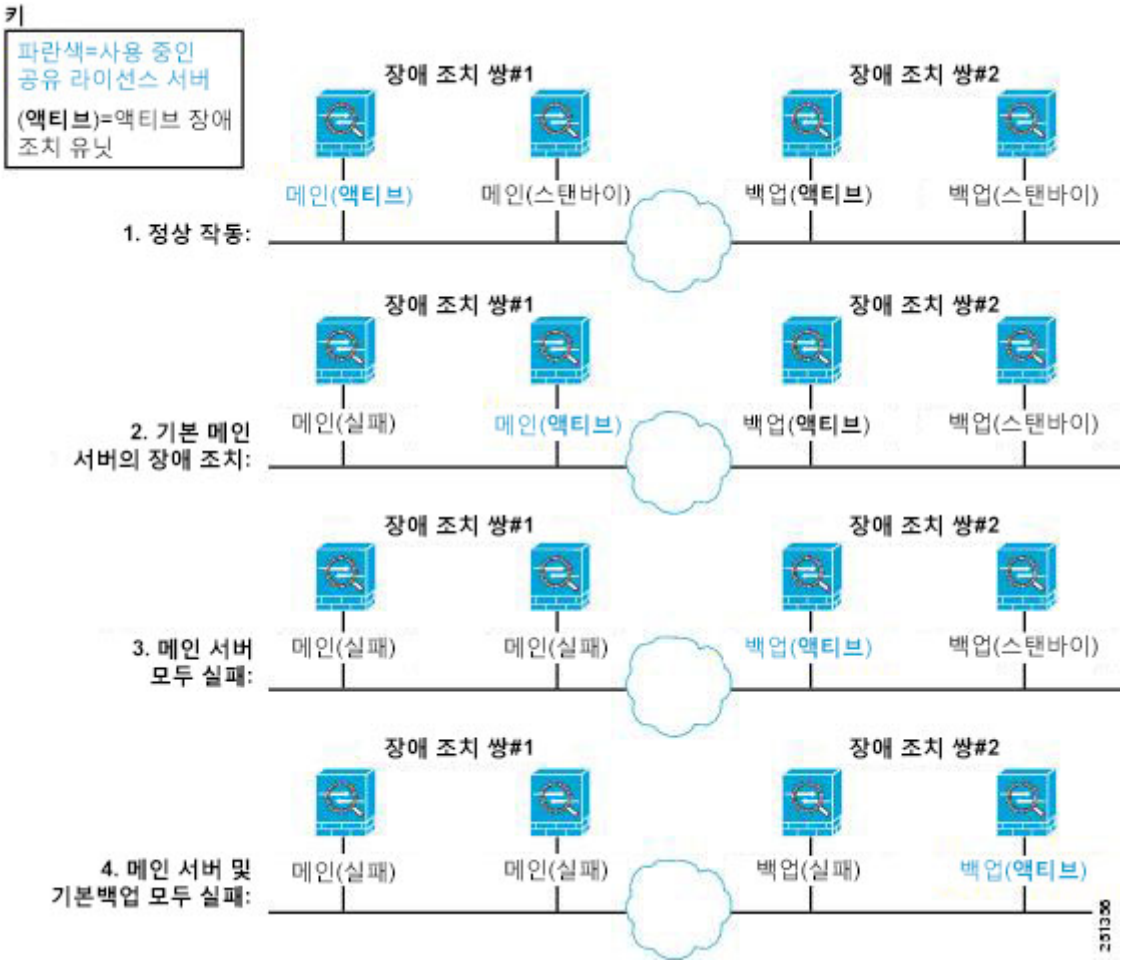
참고 백업 서버 메커니즘은 장애 조치와 분리되어 있지만 호환 가능합니다.

공유 라이센스는 단일 컨텍스트 모드에서만 지원되므로 액티브/액티브 장애 조치는 지원되지 않습니다.

액티브/스탠바이 장애 조치의 경우, 기본 유닛이 기본 공유 라이센스 서버 역할을 하며 장애 조치 후에는 스탠바이 유닛이 기본 공유 라이센스 서버 역할을 합니다. 스탠바이 유닛은 백업 공유 라이센스 서버 역할을 하지 않습니다. 그 대신, 원하는 경우 백업 서버 역할을 하는 두 번째 유닛 쌍을 사용할 수 있습니다.

2개의 장애 조치 쌍이 있는 네트워크를 예로 들어 보겠습니다. 1번 쌍에는 기본 라이센스 서버가 포함됩니다. 2번 쌍에는 백업 서버가 포함됩니다. 1번 쌍의 기본 유닛이 중단되면, 스탠바이 유닛이 즉시 새로운 기본 라이센스 서버가 됩니다. 2번 쌍의 백업 서버는 사용되지 않습니다. 1번 쌍의 두 유닛이 모두 중단될 경우에만 2번 쌍의 백업 서버가 공유 라이센스 서버로 사용됩니다. 1번 쌍이 중단된 상태인데 2번 쌍의 기본 유닛이 중단될 경우 2번 쌍의 스탠바이 유닛이 공유 라이선싱 서버로 사용됩니다(다음 그림 참조).

그림 *6:* 장애 조치 및 공유 라이센스 서버



스탠바이 백업 서버에서는 기본 백업 서버와 동일한 작동 한도를 공유합니다. 스탠바이 유닛이 액티브 상태가 되면, 기본 유닛이 중단된 곳에서 카운트다운을 계속 진행합니다.

관련 항목

공유 라이센싱 백업 서버 정보, 70 페이지

장애 조치 및 공유 라이센스 참가자

참가자 쌍의 경우, 별도의 참가자 ID를 사용하여 두 유닛을 모두 공유 라이센스 서버에 등록합니다. 액티브 유닛은 스탠바이 유닛으로 참가자 ID를 동기화합니다. 스탠바이 유닛에서는 이 ID를 사용하여 액티브 역할로 전환될 경우 전송 요청을 생성합니다. 이러한 전송 요청은 이전의 액티브 유닛에서 새 액티브 유닛으로 공유 세션을 이동하는 데 사용됩니다.

최대 참가자 수

ASA에서는 공유 라이선스의 참가자 수를 제한하지 않습니다. 그러나 공유 네트워크가 너무 클 경우 라이선싱 서버의 성능에 영향을 미칠 수 있습니다. 이러한 경우 참가자 새로 고침의 지연 간격을 늘리거나, 2개의 공유 네트워크를 생성할 수 있습니다.

공유 라이센싱 서버 구성

이 섹션에서는 ASA를 공유 라이선싱 서버로 구성하는 방법을 설명합니다.

시작하기 전에

서버에는 공유 라이센스 서버 키가 있어야 합니다.

프로시저

단계 **1** 공유 암호를 설정합니다.

license-server secret *secret*

예제**:**

```
ciscoasa(config)# license-server secret farscape
```

*secret*은 4~128자의 ASCII 문자열입니다. 이 공유 비밀을 보유한 모든 참가자는 라이센스 서버를 사용할 수 있습니다.

단계 **2** (선택사항) 새로 고침 간격을 설정합니다.

license-server refresh-interval *seconds*

예제**:**

```
ciscoasa(config)# license-server refresh-interval 100
```

새로 고침 간격을 10~300초 사이로 설정합니다. 이 값은 참가자에게 제공되어 참가자가 서버와 통신을 수행해야 하는 빈도를 설정할 수 있도록 합니다. 기본값은 30초입니다.

단계 **3** (선택사항) 서버가 참가자의 SSL 연결을 수신 대기하는 포트를 설정합니다.

license-server port *port*

예제**:**

```
ciscoasa(config)# license-server port 40000
```

*port*는 1~65535 사이입니다. 기본값은 TCP 포트 50554입니다.

단계 **4** (선택사항) 백업 서버 IP 주소와 일련 번호를 식별합니다.

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

예제**:**

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

백업 서버가 장애 조치 쌍에 포함될 경우, 스탠바이 유닛 일련 번호도 식별합니다. 1개의 백업 서버 및 선택적 스탠바이 유닛만 식별할 수 있습니다.

단계 **5** 이 유닛을 공유 라이센싱 서버로 활성화합니다.

license-server enable *interface_name*

예제**:**

```
ciscoasa(config)# license-server enable inside
```

참가자가 서버에 접속하는 인터페이스를 지정합니다. 이 명령을 원하는 인터페이스 수에 반복할 수 있습니다.

예

다음 예에서는 공유 암호를 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 dmz 인터페이스에서 이러한 유닛을 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

공유 라이센싱 백업 서버 구성(선택사항)

이 섹션에서는 기본 서버가 중단되었을 경우 공유 라이센스 참가자를 활성화하여 백업 서버 역할을 수행하도록 합니다.

시작하기 전에

백업 서버에는 공유 라이센스 참가자 키가 있어야 합니다.

프로시저

단계 **1** 공유 라이센싱 서버 IP 주소 및 공유 암호를 식별합니다.

license-server address *address* **secret** *secret* [**port** *port*]

예제**:**

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

서버 컨피그레이션에서 기본 포트를 변경한 경우 백업 서버와 일치하도록 포트를 조정해야 합니다.

단계 **2** 이 유닛을 공유 라이센싱 백업 서버로 활성화합니다.

license-server backup enable *interface_name*

예제**:**

```
ciscoasa(config)# license-server backup enable inside
```

참가자가 서버에 접속하는 인터페이스를 지정합니다. 이 명령을 원하는 인터페이스 수에 반복할 수 있습니다.

예

다음 예에서는 라이센스 서버 및 공유 비밀을 식별하고, 내부 인터페이스 및 dmz 인터페이스에서 이 유닛을 백업 공유 라이센스 서버로 활성화합니다.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

공유 라이선싱 참가자 구성

이 섹션에서는 공유 라이선싱 서버와 통신하는 공유 라이선싱 참가자를 구성하는 방법과

시작하기 전에

참가자는 공유 라이센스 참가자 키가 있어야 합니다.

프로시저

단계 **1** 공유 라이센싱 서버 IP 주소 및 공유 암호를 식별합니다.

license-server address *address* **secret** *secret* [**port** *port*]

예제**:**

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

서버 컨피그레이션에서 기본 포트를 변경한 경우 참가자와 일치하도록 포트를 조정해야 합니다.

단계 **2** (선택사항) 백업 서버를 구성한 경우, 백업 서버 주소를 입력합니다.

license-server backup address *address*

예제**:**

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

예

다음 예에서는 라이센스 서버 IP 주소와 공유 비밀 및 백업 라이센스 서버 IP 주소를 설정합니다.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

모델당 지원되는 기능 라이센스

이 섹션에서는 각 모델에 제공되는 라이센스 및 라이센스에 대한 중요한 참고 사항을 설명합니다.

모델당 라이센스

이 섹션에는 각 모델에 제공되는 기능 라이센스가 나와 있습니다.

기울임 꼴로 된 항목은 Base(또는 Security Plus 등) 라이센스 버전을 대체할 수 있는 별도로 선택 가능한 라이센스입니다. 선택적 라이선스를 혼합하고 매칭할 수 있습니다.

참고 일부 기능은 서로 호환되지 않습니다. 호환성 정보에 대한 내용은 개별 기능이 설명된 장을 참조하십시오.

No Payload Encryption 모델을 사용할 경우 아래의 기능 중 일부가 지원되지 않을 수 있습니다. 지원되지 않는 기능에 대한 목록은 No Payload Encryption 모델, 61 페이지를 참조하십시오.

라이센스에 대한 자세한 내용은 라이센스 참고 사항, 53 페이지를 참조하십시오.

ASA 5506-X 및 ASA 5506W-X 라이선스 기능

다음 표에는 ASA 5506-X 및 ASA 5506W-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스	**Security Plus** 라이센스
방화벽 라이센스		
봇넷 트래픽 필터	지원 안 함	지원 안 함

라이센스	기본 라이센스		**Security Plus** 라이센스	
방화벽 연결, 동시	20,000		50,000	
캐리어	지원 안 함		지원 안 함	
총 TLS 프록시 세션	160		160	
VPN 라이선스				
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *50*개	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *50*개
기타 VPN 피어	10		50	
총 VPN 피어, 모든 유형 통합	50		50	
VPN 로드 밸런싱	지원 안 함		지원 안 함	
일반 라이센스				
암호화	Base(DES)	선택적 라이센스*:* 강력*(3DES/AES)*	Base(DES)	선택적 라이센스*:* 강력*(3DES/AES)*
장애 조치	지원 안 함		활성/대기	
보안 상황	지원 안 함		지원 안 함	
클러스터링	지원 안 함		지원 안 함	
VLAN, 최대 개수	5		30	

ASA 5506H-X 라이선스 기능

다음 표에는 ASA 5506H-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스	
방화벽 라이센스		
봇네트 트래픽 필터	지원 안 함	
방화벽 연결, 동시	50,000	
캐리어	지원 안 함	
총 UC 프록시 세션	160	
VPN 라이선스		
AnyConnect Plus 또는 Apex 라이선스(별도 구매), 최대 프리미엄 피어 수	50	
총 VPN 피어, 모든 유형 통합	50	
기타 VPN 피어	50	
VPN 로드 밸런싱	활성화됨	
일반 라이센스		
암호화	Base(DES)	선택적 라이센스*:* 강력*(3DES/AES)*
장애 조치	액티브/스탠바이 또는 액티브/액티브	
보안 상황	지원 안 함	
클러스터링	지원 안 함	
VLAN, 최대 개수	30	

ASA 5508-X 라이센스 기능

다음 표에는 ASA 5508-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스			
방화벽 라이센스				
봇네트 트래픽 필터	지원 안 함			
방화벽 연결, 동시	100,000			
캐리어	지원 안 함			
총 TLS 프록시 세션	320			
VPN 라이선스				
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *100*개		
총 VPN 피어, 모든 유형 통합	100			
기타 VPN 피어	100			
VPN 로드 밸런싱	활성화됨			
일반 라이센스				
암호화	Base(DES)	선택적 라이센스*:* 강력*(3DES/AES)*		
장애 조치	액티브/스탠바이 또는 액티브/액티브			
보안 상황	2	옵션 라이센스	*5*	
클러스터링	지원 안 함			
VLAN, 최대 개수	50			

ASA 5512-X 라이센스 기능

다음 표에는 ASA 5512-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스					Security Plus 라이센스				
방화벽 라이센스										
봇네트 트래픽 필터	비활성화됨	선택적 기간별 라이센스: 사용 가능				비활성화됨	선택적 기간별 라이센스: 사용 가능			
방화벽 연결, 동시	100,000					250,000				
캐리어	지원 안 함					지원 안 함				
총 TLS 프록시 세션	2	옵션 라이센스				2	옵션 라이센스			
		24	*50*	*100*	*250*	*500*	*24*	*50*	*100*	*250*	*500*
VPN 라이선스										
AnyConnect 피어	비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *250*개				비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *250*개			
기타 VPN 피어	250					250				
총 VPN 피어, 모든 유형 통합	250					250				
VPN 로드 밸런싱	지원 안 함					활성화됨				
일반 라이센스										
암호화	Base(DES)	선택적 라이센스: 강력*(3DES/AES)*				Base(DES)	선택적 라이센스: 강력*(3DES/AES)*			
장애 조치	지원 안 함					액티브/스탠바이 또는 액티브/액티브				
보안 상황	지원 안 함					2	옵션 라이센스			*5*
클러스터링	지원 안 함					2				

라이센스	기본 라이센스		**Security Plus** 라이센스	
IPS 모듈	비활성화됨	선택적 라이센스: 사용 가능	비활성화됨	선택적 라이센스: 사용 가능
VLAN, 최대 개수	50		100	

ASA 5515-X 라이센스 기능

다음 표에는 ASA 5515-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스						
방화벽 라이센스							
봇넷 트래픽 필터	비활성화됨	선택적 기간별 라이센스: 사용 가능					
방화벽 연결, 동시	250,000						
캐리어	지원 안 함						
총 TLS 프록시 세션	2	옵션 라이센스	*24*	*50*	*100*	*250*	*500*
VPN 라이선스							
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *250*개					
기타 VPN 피어	250						
총 VPN 피어, 모든 유형 통합	250						

라이센스	기본 라이센스		
VPN 로드 밸런싱	활성화됨		
일반 라이센스			
암호화	Base(DES)	선택적 라이센스*: Strong(3DES/AES)*	
장애 조치	액티브/스탠바이 또는 액티브/액티브		
보안 상황	2	옵션 라이센스	*5*
클러스터링	2		
IPS 모듈	비활성화됨	선택적 라이센스: 사용 가능	
VLAN, 최대 개수	100		

ASA 5516-X 라이센스 기능

다음 표에는 ASA 5516-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스
방화벽 라이센스	
봇네트 트래픽 필터	지원 안 함
방화벽 연결, 동시	250,000
캐리어	지원 안 함
총 TLS 프록시 세션	1000
VPN 라이선스	

라이센스	기본 라이센스	
AnyConnect 피어	비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *300*개
기타 VPN 피어	300	
총 VPN 피어, 모든 유형 통합	300	
VPN 로드 밸런싱	활성화됨	
일반 라이센스		
암호화	Base(DES)	선택적 라이센스*:* 강력*(3DES/AES)*
장애 조치	액티브/스탠바이 또는 액티브/액티브	
보안 상황	2	옵션 라이센스 *5*
클러스터링	2	
VLAN, 최대 개수	150	

ASA 5525-X 라이센스 기능

다음 표에는 ASA 5525-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스								
방화벽 라이센스									
봇넷 트래픽 필터	비활성화됨	선택적 기간별 라이센스*:* 사용 가능							
방화벽 연결, 동시	500,000								
캐리어	비활성화됨	선택적 라이센스*:* 사용 가능							
총 TLS 프록시 세션	2	옵션 라이센스	*24*	*50*	*100*	*250*	*500*	*750*	*1000*

라이센스	기본 라이센스				
VPN 라이선스					
AnyConnect 피어	비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *750*개			
기타 VPN 피어	750				
총 VPN 피어, 모든 유형 통합	750				
VPN 로드 밸런싱	활성화됨				
일반 라이센스					
암호화	Base(DES)	선택적 라이센스*: Strong(3DES/AES)*			
장애 조치	액티브/스탠바이 또는 액티브/액티브				
보안 상황	2	옵션 라이센스	*5*	*10*	*20*
클러스터링	2				
IPS 모듈	비활성화됨	선택적 라이센스*:* 사용 가능			
VLAN, 최대 개수	200				

ASA 5545-X 라이센스 기능

다음 표에는 ASA 5545-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스
방화벽 라이센스	

라이센스	기본 라이센스									
봇네트 트래픽 필터	비활성화됨	선택적 기간별 라이센스: 사용 가능								
방화벽 연결, 동시	750,000									
캐리어	비활성화됨	선택적 라이센스: 사용 가능								
총 TLS 프록시 세션	2	옵션 라이센스	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN 라이선스										
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *2500*개								
기타 VPN 피어	2500									
총 VPN 피어, 모든 유형 통합	2500									
VPN 로드 밸런싱	활성화됨									
일반 라이센스										
암호화	Base(DES)	선택적 라이센스*: Strong(3DES/AES)*								
장애 조치	액티브/스탠바이 또는 액티브/액티브									
보안 상황	2	옵션 라이센스	*5*	*10*	*20*	*50*				
클러스터링	2									

라이센스	기본 라이센스	
IPS 모듈	비활성화됨	선택적 라이센스: 사용 가능
VLAN, 최대 개수	300	

ASA 5555-X 라이센스 기능

다음 표에는 ASA 5555-X에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스								
방화벽 라이센스									
봇넷 트래픽 필터	비활성화됨	선택적 기간별 라이센스: 사용 가능							
방화벽 연결, 동시	1,000,000								
캐리어	비활성화됨	선택적 라이센스: 사용 가능							
총 TLS 프록시 세션	2	옵션 라이센스							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 라이선스									
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *5000*개							
기타 VPN 피어	5000								
총 VPN 피어, 모든 유형 통합	5000								

라이센스	기본 라이센스						
VPN 로드 밸런싱	활성화됨						
일반 라이센스							
암호화	Base(DES)	선택적 라이센스*: Strong(3DES/AES)*					
장애 조치	액티브/스탠바이 또는 액티브/액티브						
보안 상황	2	옵션 라이센스	*5*	*10*	*20*	*50*	*100*
클러스터링	2						
IPS 모듈	비활성화됨	선택적 라이센스*:* 사용 가능					
VLAN, 최대 개수	500						

SSP-10 라이센스 기능이 포함된 ASA 5585-X

다음 표에는 SSP-10이 포함된 ASA 5585-X에 대한 라이선스 기능이 나와 있습니다.

동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-20이 포함된 SSP-10은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다.

라이센스	**Base** 및 **Security Plus** 라이센스	
방화벽 라이센스		
봇네트 트래픽 필터	비활성화됨	선택적 기간별 라이센스*:* 사용 가능
방화벽 연결, 동시	1,000,000	

라이센스	**Base** 및 **Security Plus** 라이센스								
캐리어	비활성화됨	선택적 라이센스: 사용 가능							
총 TLS 프록시 세션	2	옵션 라이센스							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 라이선스									
AnyConnect 피어	비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *5000*개							
기타 VPN 피어	5000								
총 VPN 피어, 모든 유형 통합	5000								
VPN 로드 밸런싱	활성화됨								
일반 라이센스									
10 GE I/O	**Base** 라이센스: 비활성화됨, 1GE에서 파이버 ifcs 실행					**Security Plus** 라이센스: 활성화됨, 10GE에서 ifcs 실행			
암호화	Base(DES)	선택적 라이센스: *Strong(3DES/AES)*							
장애 조치	액티브/스탠바이 또는 액티브/액티브								
보안 상황	2	옵션 라이센스	*5*	*10*	*20*	*50*	*100*		
클러스터링	비활성화됨	선택적 라이센스: *16*개 유닛에 제공							
VLAN, 최대 개수	1024								

SSP-20 라이센스 기능이 포함된 ASA 5585-X

다음 표에는 SSP-20이 포함된 ASA 5585-X에 대한 라이선스 기능이 나와 있습니다.

동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-40이 포함된 SSP-20은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다.

참고 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

라이센스	**Base** 및 **Security Plus** 라이센스										
방화벽 라이센스											
봇네트 트래픽 필터	비활성화됨	선택적 기간별 라이센스: 사용 가능									
방화벽 연결, 동시	2,000,000										
캐리어	비활성화됨	선택적 라이센스: 사용 가능									
총 TLS 프록시 세션	2	옵션 라이센스									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*
VPN 라이선스											
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *10,000*개									
기타 VPN 피어	10,000										
총 VPN 피어, 모든 유형 통합	10,000										

라이센스	**Base** 및 **Security Plus** 라이센스							
VPN 로드 밸런싱	활성화됨							
일반 라이센스								
10 GE I/O	**Base** 라이센스: 비활성화됨, 1GE에서 파이버 ifcs 실행				**Security Plus** 라이센스: 활성화됨, 10GE에서 ifcs 실행			
암호화	Base(DES)	선택적 라이센스*: Strong(3DES/AES)*						
장애 조치	액티브/스탠바이 또는 액티브/액티브							
보안 상황	2	옵션 라이센스	*5*	*10*	*20*	*50*	*100*	*250*
클러스터링	비활성화됨	선택적 라이센스*: 16*개 유닛에 제공						
VLAN, 최대 개수	1024							

SSP-40 및 -60 라이센스 기능이 포함된 ASA 5585-X

다음 표에는 SSP-40 및 -60이 포함된 ASA 5585-X에 대한 라이선스 기능이 나와 있습니다.

동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-40이 포함된 SSP-60은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다.

참고 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

라이센스	기본 라이센스	
방화벽 라이센스		
봇넷 트래픽 필터	비활성화됨	선택적 기간별 라이센스*:* 사용 가능

라이센스	기본 라이센스										
방화벽 연결, 동시	**SSP-40**이 포함된 **5585-X**: 4,000,000					**SSP-60**이 포함된 **5585-X**: 10,000,000					
캐리어	비활성화됨	선택적 라이센스*:* 사용 가능									
총 TLS 프록시 세션	2	옵션 라이센스									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*
VPN 라이선스											
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *10,000*개									
기타 VPN 피어	10,000										
총 VPN 피어, 모든 유형 통합	10,000										
VPN 로드 밸런싱	활성화됨										
일반 라이센스											
10 GE I/O	활성화됨, 10GE에서 파이버 ifcs 실행										
암호화	Base(DES)	선택적 라이센스*: Strong(3DES/AES)*									
장애 조치	액티브/스탠바이 또는 액티브/액티브										
보안 상황	2	옵션 라이센스	*5*	*10*	*20*	*50*	*100*	*250*			
클러스터링	비활성화됨	선택적 라이센스*: 16*개 유닛에 제공									
VLAN, 최대 개수	1024										

ASASM 라이선스 기능

다음 표에는 ASA Services Module에 대한 라이선스 기능이 나와 있습니다.

참고 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

라이센스	기본 라이센스										
방화벽 라이센스											
봇네트 트래픽 필터	비활성화됨	선택적 기간별 라이센스: 사용 가능									
방화벽 연결, 동시	10,000,000										
캐리어	비활성화됨	선택적 라이센스: 사용 가능									
총 TLS 프록시 세션	2	옵션 라이센스									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*
VPN 라이선스											
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스: 최대 *10,000*개									
기타 VPN 피어	10,000										
총 VPN 피어, 모든 유형 통합	10,000										
VPN 로드 밸런싱	활성화됨										
일반 라이센스											
암호화	Base(DES)	선택적 라이센스: *Strong(3DES/AES)*									

라이센스	기본 라이센스						
장애 조치	액티브/스탠바이 또는 액티브/액티브						
보안 상황	2	옵션 라이센스					
		5	*10*	*20*	*50*	*100*	*250*
클러스터링	지원 안 함						
VLAN, 최대 개수	1000						

ISA 3000 라이선스 기능

다음 표에는 ISA 3000에 대한 라이선스 기능이 나와 있습니다.

라이센스	기본 라이센스		**Security Plus** 라이센스	
방화벽 라이센스				
봇네트 트래픽 필터	지원 안 함		지원 안 함	
방화벽 연결, 동시	20,000		50,000	
캐리어	지원 안 함		지원 안 함	
총 TLS 프록시 세션	160		160	
VPN 라이선스				
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *25*개	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *25*개
기타 VPN 피어	10		50	

라이센스	기본 라이센스		Security Plus 라이센스	
총 VPN 피어, 모든 유형 통합	25		50	
VPN 로드 밸런싱	지원 안 함		지원 안 함	
일반 라이센스				
암호화	Base(DES)	선택적 라이센스: 강력*(3DES/AES)*	Base(DES)	선택적 라이센스: 강력*(3DES/AES)*
장애 조치	지원 안 함		활성/대기	
보안 상황	지원 안 함		지원 안 함	
클러스터링	지원 안 함		지원 안 함	
VLAN, 최대 개수	5		25	

PAK 라이센스 모니터링

이 섹션에서는 라이센스 정보를 확인하는 방법을 설명합니다.

현재 라이센스 보기

이 섹션에서는 최신 라이센스를 확인하는 방법 및 시간 기반 활성화 키의 경우 라이센스 기간이 얼마나 남았는지 확인하는 방법을 설명합니다.

시작하기 전에

No Payload Encryption 모델을 보유한 상태에서 라이센스를 보려면 VPN 및 Unified Communications 라이센스가 나열되지 않습니다. 자세한 내용은 No Payload Encryption 모델, 61 페이지를 참조하십시오.

프로시저

영구 라이센스, 활성 시간 기반 라이센스 및 실행 중인 라이센스(영구 라이센스와 활성 시간 기반 라이센스의 조합)를 표시합니다.

show activation-key [detail]

detail 키워드를 사용하면 비활성화된 기간별 라이센스가 표시됩니다.

장애 조치 또는 클러스터 유닛에 대해 이 명령을 사용하면 모든 유닛의 통합된 키인 "클러스터" 라이센스가 표시됩니다.

예

예 **1: show activation-key** 명령에 대한 독립형 유닛 출력

다음은 독립형 디바이스에 대한 **show activation-key** 명령의 샘플 출력으로, 실행 중인 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)와 각 활성 시간 기반 라이센스를 보여 줍니다.

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
```

```
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

예 2: show activation-key detail에 대한 독립형 유닛 출력

다음은 독립형 디바이스에 대한 **show activation-key detail** 명령의 샘플 출력으로, 실행 중인 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)와 영구 라이센스 및 설치된 각 시간 기반 라이센스(활성 및 비활성)를 보여 줍니다.

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
```

```
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

예 3: show activation-key detail에 대한 장애 조치 쌍의 기본 유닛 출력

다음은 기본 장애 조치 디바이스에 대한 **show activation-key detail** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 기본 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이선스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 기본 디바이스 영구 라이센스
- 기본 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성)

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
```

```
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
Security Contexts             : 12             perpetual
GTP/GPRS                      : Enabled        perpetual
AnyConnect Premium Peers      : 4           perpetual
AnyConnect Essentials            : Disabled       perpetual
Other VPN Peers                  : 750            perpetual
Total VPN Peers                  : 750            perpetual
Shared License                   : Disabled       perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone   : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
UC Phone Proxy Sessions       : 4              perpetual
Total UC Proxy Sessions       : 4              perpetual
Botnet Traffic Filter         : Enabled        33 days
Intercompany Media Engine     : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces   : Unlimited      perpetual
Maximum VLANs                 : 150            perpetual
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Disabled       perpetual
Security Contexts             : 2              perpetual
GTP/GPRS                      : Disabled       perpetual
AnyConnect Premium Peers         : 2              perpetual
AnyConnect Essentials            : Disabled       perpetual
Other VPN Peers                  : 750            perpetual
Total VPN Peers                  : 750            perpetual
Shared License                   : Disabled        perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone   : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
UC Phone Proxy Sessions       : 2              perpetual
Total UC Proxy Sessions       : 2              perpetual
Botnet Traffic Filter         : Disabled       perpetual
Intercompany Media Engine     : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter          : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts              : 2          7 days
AnyConnect Premium Peers                 : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions        : 100        14 days
```

예 4: show activation-key detail에 대한 장애 조치 쌍의 보조 유닛 출력

다음은 보조 장애 조치 디바이스에 대한 **show activation-key detail** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 보조 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이선스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 보조 디바이스 영구 라이센스
- 보조 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성) 이 디바이스에는 시간 기반 라이센스가 없으므로 이 샘플 출력에는 none이 표시됩니다.

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
```

```
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

예 5: show activation-key에 대한 장애 조치 쌍의 ASA Services Module에 대한 기본 유닛 출력

다음은 기본 장애 조치 디바이스에 대한 **show activation-key** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 기본 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이선스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 기본 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성)

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces               : 1024           perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
DES                              : Enabled        perpetual
3DES-AES                         : Enabled        perpetual
Security Contexts                : 25             perpetual
GTP/GPRS                         : Enabled        perpetual
Botnet Traffic Filter            : Enabled        330 days
```

```
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

예 6: show activation-key에 대한 장애 조치 쌍의 ASA Services Module에 대한 보조 유닛 출력

다음은 보조 장애 조치 디바이스에 대한 **show activation-key** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 보조 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이선스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 보조 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성) 이 디바이스에는 시간 기반 라이센스가 없으므로 이 샘플 출력에는 none이 표시됩니다.

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
```

```
Security Contexts                : 50 perpetual
GTP/GPRS                         : Enabled perpetual
Botnet Traffic Filter            : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

예 7: show activation-key에 대한 클러스터의 출력

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
```

```
This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

공유 라이센스 모니터링

공유 라이센스를 모니터링하려면 를 선택하고 다음 명령 중 하나를 입력합니다.

- **show shared license** [**detail** | **client** [*hostname*] | **backup**]

  공유 라이센스 통계를 표시합니다. 라이센스 서버에만 사용 가능한 선택적 키워드: **detail** 키워드를 사용하면 참가자당 통계가 표시됩니다. 표시 내용을 한 명의 참가자로 제한하려면 **client** 키워드를 사용합니다. **backup** 키워드를 사용하면 백업 서버에 대한 정보가 표시됩니다.

  공유 라이선스 통계를 지우려면 **clear shared license** 명령을 입력합니다.

  다음은 라이센스 참가자에 대한 **show shared license** 명령의 샘플 출력입니다.

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

  다음은 라이센스 서버에 대한 **show shared license detail** 명령의 샘플 출력입니다.

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
```

```
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

- **show activation-key**

  ASA에 설치된 라이선스를 표시합니다. **show version** 명령을 사용하면 라이센스 정보도 표시됩니다.

- **show vpn-sessiondb**

  VPN 세션에 대한 라이센스 정보를 표시합니다.

PAK 라이센스 내역

기능 이름	플랫폼 릴리스	설명
연결 및 VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base 라이센스 연결이 32000에서 5000으로 증가하고, VLAN이 0에서 10으로 증가 • ASA5510 Security Plus 라이센스 연결이 64000에서 130000으로 증가하고, VLAN이 10에서 25으로 증가 • ASA5520 연결이 130000에서 280000으로 증가하고, VLAN이 25에서 100으로 증가 • ASA5540 연결이 280000에서 400000으로 증가하고, VLAN이 100에서 200으로 증가

기능 이름	플랫폼 릴리스	설명
SSL VPN 라이센스	7.1(1)	SSL VPN 라이센스가 도입되었습니다.
SSL VPN 라이센스 증가	7.2(1)	ASA 5550 이상 버전에 5000-사용자 SSL VPN 라이센스가 도입되었습니다.
ASA 5510의 Base 라이센스 인터페이스 증가	7.2(2)	ASA 5510의 Base 라이센스의 경우, 인터페이스의 최대 수가 3개에서 관리 인터페이스까지 추가하여 무제한 인터페이스로 증가했습니다.
VLAN 증가	7.2(2)	ASA 5505 Security Plus 라이센스의 VLAN 최대 개수를 5개(3개는 전 기능, 1개는 장애 조치, 1개는 백업 인터페이스에 한정)에서 20개 전 기능 인터페이스로 늘렸습니다. 또한 트렁크 포트 수도 1개에서 8개로 늘렸습니다. 현재 전체 기능을 지원하는 인터페이스가 20개이므로 백업 인터페이스 명령을 사용하여 백업 ISP 인터페이스를 비활성화할 필요가 없으며, 여기에 전체 기능을 지원하는 인터페이스를 사용할 수 있습니다. 백업 인터페이스 명령은 Easy 컨피그레이션에서 여전히 유용합니다. ASA 5510의 VLAN 한도도 늘어났습니다. Base 라이센스는 10개에서 50개로, Security Plus 라이센스는 25개에서 100개로 늘어났습니다. ASA 5520은 100개에서 150개로, ASA 5550은 200개에서 250개로 늘어났습니다.

기능 이름	플랫폼 릴리스	설명
ASA 5510 Security Plus 라이센스의 기가비트 이더넷 지원	7.2(3)	이제 ASA 5510에서는 Security Plus 라이센스와 함께 Ethernet 0/0 및 0/1 포트에 기가비트 이더넷(1000 Mbps)을 지원합니다. Base 라이센스에서는 이를 고속 이더넷(100 Mbps) 포트로 계속 사용할 수 있습니다. Ethernet 0/2, 0/3, 0/4는 두 라이센스에서 모두 고속 이더넷 포트로 유지됩니다. 참고 인터페이스 이름은 Ethernet 0/0 및 Ethernet 0/1로 유지됩니다. **speed** 명령을 사용하여 인터페이스의 속도를 변경하고, **show interface** 명령을 사용하여 각 인터페이스에 현재 구성된 속도를 확인합니다.
고급 끝점 진단 라이센스	8.0(2)	Advanced Endpoint Assessment 라이센스가 도입되었습니다. Cisco AnyConnect 또는 클라이언트리스 SSL VPN 연결의 완벽한 상태를 지원하기 위해, 방대한 범위로 수집된 안티바이러스 및 안티스파이웨어 애플리케이션, 방화벽, 운영 체제, 관련 업데이트 정보를 원격 컴퓨터에서 검사합니다. 모든 레지스트리 항목, 파일 이름 및 사용자가 지정하는 프로세스 이름까지 검사합니다. 스캔 결과는 ASA로 전송됩니다. ASA에서는 사용자 로그인 크리덴셜과 컴퓨터 스캔 결과를 모두 사용하여 DAP(Dynamic Access Policy)를 할당합니다. Advanced Endpoint Assessment 라이센스를 사용하면 버전 요구 사항을 충족하지 않는 비호환 컴퓨터를 업데이트하도록 구성하여 Host Scan 기능을 개선할 수 있습니다. Cisco에서는 Cisco Secure Desktop과 별개인 Host Scan에서 지원하는 애플리케이션 및 버전 목록의 업데이트를 적시에 패키지로 제공합니다.

기능 이름	플랫폼 릴리스	설명
ASA 5510을 위한 VPN 로드 밸런싱	8.0(2)	이제 ASA 5510 Security Plus에서 VPN 로드 밸런싱이 지원됩니다.
AnyConnect for Mobile 라이센스	8.0(3)	AnyConnect for Mobile 라이센스가 도입되었습니다. 이 라이선스는 Windows 모바일 디바이스에서 AnyConnect 클라이언트를 사용하여 ASA에 연결할 수 있도록 지원합니다.
기간별 라이센스	8.0(4), 8.1(2)	기간별 라이센스에 대한 지원이 도입되었습니다.
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
Unified Communications Proxy Sessions 라이센스	8.0(4)	The UC Proxy Sessions 라이센스가 도입되었습니다. 전화 프록시, 프레즌스 페더레이션 프록시, 암호화된 음성 감시 애플리케이션에서는 TLS 프록시 세션을 사용하여 연결을 수행합니다. 각 TLS 프록시 세션의 수는 UC 라이센스 한도를 기준으로 계산됩니다. 이러한 애플리케이션은 UC 프록시를 통해 라이센스가 제공되며, 서로 조합할 수 있습니다. 이 기능은 버전 8.1에는 제공되지 않습니다.
Botnet Traffic Filter 라이센스	8.2(1)	Botnet Traffic Filter 라이센스가 도입되었습니다. Botnet Traffic Filter에서는 알려진 악성 도메인 이름 및 IP 주소에 대한 연결을 추적하여 악성코드 네트워크 활동을 차단합니다.

기능 이름	플랫폼 릴리스	설명
AnyConnect Essentials 라이센스	8.2(1)	AnyConnect Essentials 라이센스가 도입되었습니다. 이 라이선스는 AnyConnect VPN 클라이언트가 ASA에 액세스할 수 있도록 지원합니다. 이 라이센스에서는 브라우저 기반 SSL VPN 액세스 또는 Cisco Secure Desktop을 지원하지 않습니다. 이러한 기능의 경우 AnyConnect Essentials 대신 AnyConnect Premium 라이센스를 활성화합니다. 참고 AnyConnect Essentials 라이센스를 이용할 경우 VPN 사용자는 웹 브라우저를 사용하여 로그인하고 AnyConnect 클라이언트를 다운로드 및 시작(WebLaunch)할 수 있습니다. AnyConnect 클라이언트 소프트웨어를 이 라이센스로 활성화하거나 AnyConnect Premium 라이센스로 활성화하는 모든 경우 동일한 클라이언트 기능이 제공됩니다. AnyConnect Essentials 라이선스는 해당 ASA에서 AnyConnect Premium 라이선스(모든 유형) 또는 Advanced Endpoint Assessment 라이선스와 동시에 활성화될 수 없습니다. 그러나 같은 네트워크의 다른 ASA에서는 AnyConnect Essentials 라이선스와 AnyConnect Premium 라이선스를 실행할 수 있습니다. 기본적으로 ASA에서는 AnyConnect Essentials 라이선스를 사용하지만, **webvpn**를 사용한 다음 **no anyconnect-essentials** 명령을 사용하여 다른 라이선스를 사용하도록 이 라이선스를 비활성화할 수 있습니다.
SSL VPN 라이센스는 AnyConnect Premium SSL VPN Edition 라이센스로 변경되었습니다.	8.2(1)	SSL VPN 라이센스 이름은 AnyConnect Premium SSL VPN Edition 라이센스로 변경되었습니다.

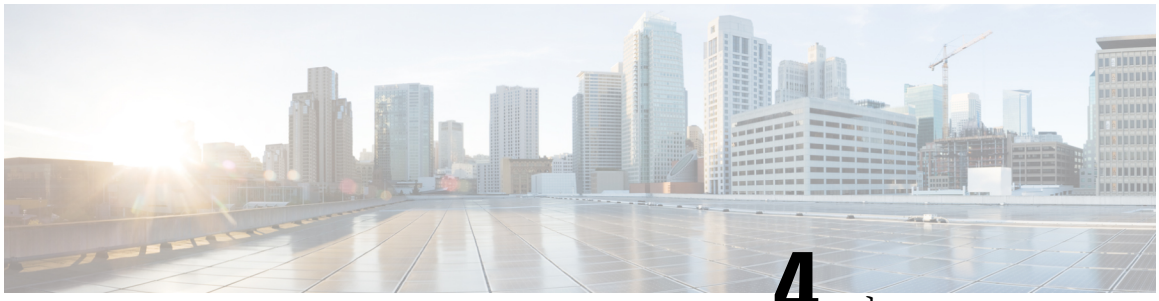
기능 이름	플랫폼 릴리스	설명
SSL VPN의 공유 라이센스	8.2(1)	SSL VPN용 공유 라이센스가 도입되었습니다. 여러 ASA에서 필요에 따라 SSL VPN 세션 풀을 공유할 수 있습니다.
Mobility Proxy 애플리케이션에 Unified Communications Proxy 라이센스가 더 이상 필요하지 않습니다.	8.2(2)	Mobility Proxy에 UC Proxy 라이센스가 더 이상 필요하지 않습니다.
SSP-20이 포함된 ASA 5585-X용 10 GE I/O 라이센스	8.2(3)	파이버 포트에 10기가비트 이더넷 속도를 지원하기 위해 SSP-20이 포함된 ASA 5585-X용 10 GE I/O 라이센스를 도입했습니다. SSP-60에서는 기본적으로 10기가비트 이더넷 속도를 지원합니다. 참고 ASA 5585-X는 8.3(x)에서 지원되지 않습니다.
SSP-10이 포함된 ASA 5585-X용 10 GE I/O 라이센스	8.2(4)	파이버 포트에 10기가비트 이더넷 속도를 지원하기 위해 SSP-10이 포함된 ASA 5585-X용 10 GE I/O 라이센스를 도입했습니다. SSP-40에서는 기본적으로 10기가비트 이더넷 속도를 지원합니다. 참고 ASA 5585-X는 8.3(x)에서 지원되지 않습니다.
동일하지 않은 장애 조치 라이센스	8.3(1)	각 유닛의 장애 조치 라이센스가 더 이상 동일하지 않아도 됩니다. 두 유닛에 사용되는 라이센스는 기본 및 보조 유닛에서 통합된 라이센스입니다. 다음 명령을 수정했습니다. **show activation-key** 및 **show version**

기능 이름	플랫폼 릴리스	설명
스태킹 가능한 기간별 라이센스	8.3(1)	기간별 라이센스는 스태킹이 가능합니다. 대부분의 경우 기간별 라이센스를 갱신해야 할 수 있으며, 기존 라이센스에서 새 라이센스로 원활하게 전환할 수 있습니다. 기간별 라이센스에만 제공되는 기능의 경우, 새 라이센스를 적용하려면 그전에 라이센스가 만료되지 않도록 하는 것이 특히 중요합니다. ASA에서는 기간별 라이선스를 스태킹할 수 있도록 지원하므로, 새 라이선스를 조기에 설치하여 라이선스가 만료되거나 라이선스의 기간이 짧아지지 않을까 걱정하지 않아도 됩니다.
Intercompany Media Engine 라이센스	8.3(1)	IME 라이센스가 도입되었습니다.
한 번에 여러 기간별 라이센스를 활성화	8.3(1)	이제 여러 기간별 라이센스를 설치할 수 있으며, 기능당 라이센스는 한 번에 하나만 활성화할 수 있습니다. 다음 명령을 수정했습니다. **show activation-key** 및 **show version**
기간별 라이센스를 별도로 활성화 및 비활성화	8.3(1)	명령을 사용하여 기간별 라이센스를 활성화하거나 비활성화할 수 있습니다. 다음 명령을 수정했습니다. **activation-key** [**activate** | **deactivate**]
AnyConnect Premium SSL VPN Edition 라이센스가 AnyConnect Premium SSL VPN 라이센스로 변경	8.3(1)	AnyConnect Premium SSL VPN Edition 라이센스 이름이 AnyConnect Premium SSL VPN 라이센스로 변경되었습니다.
수출용 No Payload Encryption 이미지	8.3(2)	ASA 5505~5550 버전에서 No Payload Encryption 소프트웨어를 설치할 경우 Unified Communications, Strong Encryption VPN, Strong Encryption 관리 프로토콜을 비활성화할 수 있습니다. 참고 이러한 특수 이미지는 8.3(x)에서만 지원됩니다. 8.4(1) 이상 버전에서 No Payload Encryption을 지원하려면 특수 하드웨어 버전의 ASA를 구매해야 합니다.

기능 이름	플랫폼 릴리스	설명
ASA 5550, 5580, 5585-X 컨텍스트 증가	8.4(1)	SSP-10이 포함된 ASA 5550~ASA 5585-X의 경우, 최대 컨텍스트 수가 50에서 100으로 증가했습니다. SSP-20 이상이 포함된 ASA 5580 및 5585-X의 경우 최대 개수가 50개에서 250개으로 늘어났습니다.
ASA 5580 및 5585-X의 VLAN 증가	8.4(1)	ASA 5580 및 5585-X의 최대 VLAN 수가 250에서 1024로 증가했습니다.
ASA 5580 및 5585-X의 연결 수 증가	8.4(1)	다음과 같이 방화벽 연결 한도를 증가하였습니다. • ASA 5580-20 — 1,000,000에서 2,000,000으로 증가 • ASA 5580-40 — 2,000,000에서 4,000,000으로 증가 • ASA 5585-X(SSP-10 포함): 750,000에서 1,000,000으로 증가 • ASA 5585-X(SSP-20 포함): 1,000,000에서 2,000,000으로 증가 • ASA 5585-X(SSP-40 포함): 2,000,000에서 4,000,000으로 증가 • ASA 5585-X(SSP-60 포함): 2,000,000에서 10,000,000으로 증가
AnyConnect Premium SSL VPN 라이센스가 AnyConnect Premium 라이센스로 변경	8.4(1)	AnyConnect Premium SSL VPN 라이센스 이름이 the AnyConnect Premium 라이센스로 변경되었습니다. 라이센스 정보 표시가 “SSL VPN Peers”에서 “AnyConnect Premium Peers”로 변경되었습니다.
ASA 5580의 AnyConnect VPN 세션 수 증가	8.4(1)	AnyConnect VPN 세션 제한이 5,000에서 10,000으로 증가했습니다.
ASA 5580의 기타 VPN 세션 수 증가	8.4(1)	기타 VPN 세션 제한이 5,000에서 10,000으로 증가했습니다.

기능 이름	플랫폼 릴리스	설명
IKEv2를 사용하는 IPsec 원격 액세스 VPN	8.4(1)	IKEv2를 사용하는 IPsec 원격 액세스 VPN이 AnyConnect Essentials 및 AnyConnect Premium 라이센스에 추가되었습니다. 참고 ASA에서 IKEv2를 지원하는 데는 다음과 같은 제한사항이 있습니다. 현재 중복 보안 연결은 지원되지 않습니다. IKEv2 사이트 대 사이트 세션이 다른 VPN 라이센스에 추가되었습니다(이전의 IPsec VPN). 기타 VPN 라이센스는 Base 라이센스에 포함됩니다.
수출용 No Payload Encryption 하드웨어	8.4(1)	No Payload Encryption이 제공되는 모델(예: ASA 5585-X)의 경우, ASA를 특정 국가에 수출할 수 있도록 ASA 소프트웨어에서 Unified Communications 및 VPN 기능을 비활성화합니다.
SSP-20 및 SSP-40용 이중 SSP	8.4(2)	SSP-40 및 SSP-60의 경우, 동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-40이 포함된 SSP-60은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다. 섀시에 2개의 SSP를 사용할 경우, VPN이 지원되지 않으나, VPN은 비활성화되지 않습니다.
ASA 5512-X~ASA 5555-X용 IPS Module 라이센스	8.6(1)	ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X에서 IPS SSP 소프트웨어 모듈을 사용하려면 IPS 모듈 라이센스가 있어야 합니다.
ASA 5580 및 ASA 5585-X용 클러스터링 라이센스	9.0(1)	ASA 5580 및 ASA 5585-X용 클러스터링 라이센스가 추가되었습니다.
ASASM의 VPN에 대한 지원	9.0(1)	이제 ASASM에서 모든 VPN 기능을 지원합니다.
ASASM에서의 Unified Communications 지원	9.0(1)	이제 ASASM에서 모든 Unified Communications 기능을 지원합니다.

기능 이름	플랫폼 릴리스	설명
SSP-10 및 SSP-20(SSP-40 및 SSP-60 포함)에 ASA 5585-X 이중 SSP 지원, 이중 SSP에 VPN 지원	9.0(1)	이제 ASA 5585-X에서는 모든 SSP 모델을 사용하여 이중 SSP를 지원합니다(동일한 섀시에서 같은 수준의 SSP를 2개 사용할 수 있음). 이제 이중 SSP를 사용할 경우 VPN이 지원됩니다.
ASA 5500-X support for clustering	9.1(4)	이제 ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X에서는 2-유닛 클러스터를 지원합니다. 유닛 2개의 클러스터링은 Base 라이센스에서 기본적으로 활성화되어 있으며, ASA 5512-X의 경우 Security Plus 라이센스가 필요합니다.
ASA 5585-X에 클러스터 멤버 16개 지원	9.2(1)	이제 ASA 5585-X에서는 16-유닛 클러스터를 지원합니다.
ASAv4 및 ASAv30 Standard 및 Premium 모델 라이선스가 도입됨	9.2(1)	ASAv에 간단한 라이선싱 체계(ASAv4 및 ASAv30의 Standard 또는 Premium 수준 영구 라이선스)가 도입되었습니다. 추가 라이센스는 제공되지 않습니다.



4 장

라이선스: Smart Software Licensing(Firepower에서의 ASAv, ASA)

Cisco 스마트 소프트웨어 라이센싱에서는 중앙 집중식으로 라이센스 풀을 구매하여 관리할 수 있습니다. 스마트 라이센스는 PAK(product authorization key) 라이센스와 달리 특정 일련 번호에 묶여 있지 않습니다. 각 유닛의 라이선스 키를 관리할 필요 없이 손쉽게 ASA를 구축하거나 사용 중단할 수 있습니다. 또한 스마트 소프트웨어 라이선싱에서는 라이선스 사용량 및 필요량을 한눈에 볼 수 있습니다.

참고 Smart Software Licensing은 ASAv 및 ASA Firepower 섀시에서만 지원됩니다. 기타 모델에서는 PAK 라이선스를 사용합니다. PAK 라이센스 정보, 49 페이지를 참조하십시오.

Smart Software Licensing 정보

이 섹션에서는 Smart Software Licensing이 적용되는 방법에 관해 설명합니다.

ASA용 Smart Software Licensing - Firepower 4100/9300 섀시

Firepower 4100/9300 섀시의 ASA의 경우, Smart Software Licensing 구성은 Firepower 4100/9300 섀시 수퍼바이저와 ASA로 나뉩니다.

- Firepower 4100/9300 섀시— 섀시에서 모든 Smart Software Licensing 인프라를 구성합니다(License Authority와 통신하는 데 필요한 파라미터 포함). Firepower 4100/9300 섀시 자체는 작동하기 위한 라이선스가 필요하지 않습니다.

  참고 섀시 간 클러스터링에서는 클러스터의 각 섀시에서 동일한 Smart Licensing 방법을 활성화해야 합니다.

- ASA 애플리케이션 — ASA에서 모든 라이선스 엔타이틀먼트를 구성합니다.

Smart Software Manager 및 어카운트

디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager에서 라이선스를 관리할 수 있습니다.

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

참고 아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

기본적으로 마스터 계정의 기본 가상 계정에 라이선스가 지정됩니다. 계정 관리자는 선택적으로 추가 가상 계정을 만들 수 있습니다. 이를테면 지역, 부서, 자회사를 위한 계정을 만들 수 있습니다. 여러 가상 계정이 있으면 많은 수의 라이선스 및 디바이스를 더 편리하게 관리할 수 있습니다.

오프라인 관리

디바이스에서 인터넷에 액세스할 수 없으며 License Authority에 등록할 수 없는 경우 오프라인 라이선싱을 구성할 수 있습니다.

ASAv

보안상의 이유로 디바이스에서 인터넷에 액세스할 수 없는 경우 선택적으로 각 ASA에 대한 영구 라이선스를 요청할 수 있습니다. 영구 라이선스 사용 시에는 License Authority에 주기적으로 액세스할 필요가 없습니다. PAK 라이선스와 마찬가지로 라이선스를 구매한 후 ASA용 라이선스 키를 설치하면 됩니다. 그러나 PAK 라이선스와는 달리 Smart Software Manager를 사용하여 라이선스를 받고 관리합니다. 일반 Smart Licensing 모드와 영구 라이선스 예약 모드 간을 쉽게 전환할 수 있습니다.

ASAv 영구 라이선스 예약

모델에 맞는 올바른 최대 처리량을 갖춘 Standard 계층 등 모든 기능을 활성화하는 모델별 라이선스를 얻을 수 있습니다.

- ASAv5
- ASAv10
- ASAv30
- ASAv50

ASAv를 구축할 동안 사용할 모델 수준을 선택해야 합니다. 모델 수준에 따라 요청하는 모델 수준이 결정됩니다. 나중에 유닛의 모델 수준을 변경하려면 현재 라이선스를 반환하고 올바른 모델 수준에서 새 라이선스를 요청해야 합니다. 이미 구축된 ASAv의 모델을 변경하려는 경우, 하이퍼바이저에서 새로운 모델 요구 사항과 일치하도록 vCPU 및 DRAM 설정을 변경할 수 있습니다. 이러한 값에 대한 내용은 ASAv 빠른 시작 가이드를 참조하십시오.

라이선스 사용을 중단하는 경우 ASAv에서 반환 코드를 생성한 다음, 해당 코드를 Smart Software Manager에 입력하여 라이선스를 반환해야 합니다. 사용하지 않은 라이선스 비용을 지불하지 않으려면 반환 프로세스를 올바르게 따르십시오.

영구 라이선스 예약은 Azure 하이퍼바이저에 지원되지 않습니다.

Firepower 2100 영구 라이선스 예약

최대 보안 상황 수를 지닌 Standard 계층 등 모든 기능을 활성화하는 라이선스를 얻을 수 있습니다. ASA에서 엔타이틀먼트 사용을 허용하도록 ASA 구성에서 엔타이틀먼트도 요청해야 합니다.

라이선스 사용을 중단하는 경우 ASA에서 반환 코드를 생성한 다음, 해당 코드를 Smart Software Manager에 입력하여 라이선스를 반환해야 합니다. 사용하지 않은 라이선스 비용을 지불하지 않으려면 반환 프로세스를 올바르게 따르십시오.

Firepower 4100/9300 섀시 영구 라이선스 예약

Carrier 라이선스 및 최대 보안 컨텍스트를 갖춘 표준 Tier 등 모든 기능을 활성화하는 라이선스를 얻을 수 있습니다. 이 라이선스는 Firepower 4100/9300 섀시에서 관리되지만 ASA에서 엔타이틀먼트 사용을 허용하도록 ASA 구성의 엔타이틀먼트도 요청해야 합니다.

라이선스 사용을 중단하는 경우 Firepower 4100/9300 섀시에서 반환 코드를 생성한 다음, 해당 코드를 Smart Software Manager에 입력하여 라이선스를 반환해야 합니다. 사용하지 않은 라이선스 비용을 지불하지 않으려면 반환 프로세스를 올바르게 따르십시오.

Satellite 서버

보안상의 이유로 디바이스가 인터넷에 액세스할 수 없는 경우 선택적으로 로컬 Smart Software Manager Satellite 서버를 VM(가상 머신)으로 설치할 수 있습니다. Smart Software Manager 기능의 하위 집합을 제공하는 이 Satellite을 통해 모든 로컬 디바이스에 필수 라이선싱 서비스를 제공할 수 있습니다. Satellite는 라이선스 사용량 동기화를 위해 메인 License Authority에 주기적으로 연결하기만 하면 됩니다. 일정에 따라 동기화하거나 수동으로 동기화할 수 있습니다.

Satellite 서버에서 다음과 같은 기능을 수행할 수 있습니다.

- 라이선스 활성화 또는 등록

- 회사의 라이선스 보기
- 회사 엔터티 간 라이선스 양도

자세한 내용은 Smart Software Manager Satellite를 참조하십시오.

가상 어카운트별로 관리되는 라이선스 및 디바이스

라이선스 및 디바이스는 가상 어카운트별로 관리됩니다. 가상 계정의 디바이스에서만 해당 계정에 지정된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 디바이스를 이전할 수도 있습니다.

Firepower 4100/9300 섀시의 ASA의 경우 — 섀시만 디바이스로 등록합니다. 섀시의 ASA 애플리케이션에서는 고유한 라이선스를 요청합니다. 예를 들어, 보안 모듈이 3개 있는 Firepower 9300 섀시의 경우 섀시는 디바이스 1개로 간주되지만 모듈은 개별 라이선스 3개를 사용합니다.

평가판 라이선스

ASAv

ASAv에서는 평가 모드를 지원하지 않습니다. ASAv는 Licensing Authority에 등록되기 전에 속도가 매우 제한된 상태로 작동됩니다.

Firepower 2100

Firepower 2100은 Licensing Authority에 등록되기 전에 90일(총 사용량) 동안 평가 모드로 작동됩니다. 기본 엔타이틀먼트만 활성화됩니다. 이 기간이 종료되면 Firepower 2100은 컴플라이언스 미준수 상태가 됩니다.

참고 강력한 암호화(3DES/AES)를 위한 평가 라이선스를 받을 수 없습니다. 강력한 암호화(3DES/AES) 라이선스를 활성화하는 내보내기-컴플라이언스 토큰을 받으려면 License Authority에 등록해야 합니다.

Firepower 4100/9300 섀시

Firepower 4100/9300 섀시는 두 가지 유형의 평가판 라이선스를 지원합니다.

- 섀시 레벨 평가 모드 — Firepower 4100/9300 섀시가 Licensing Authority에 등록되기 전에 평가 모드로 90일(총 사용량) 동안 작동됩니다. 이 모드에서 ASA는 특정 엔타이틀먼트를 요청할 수 없으며 기본 엔타이틀먼트만 활성화됩니다. 이 기간이 종료되면 Firepower 4100/9300 섀시는 컴플라이언스 미준수 상태가 됩니다.
- 엔타이틀먼트 기반 평가 모드 - Firepower 4100/9300 섀시가 Licensing Authority에 등록되고 나면 ASA에 할당할 수 있는 시간 기반 평가판 라이선스를 받을 수 있습니다. ASA에서는 평소대로 엔타이틀먼트를 요청합니다. 시간 기반 라이선스가 만료되면 시간 기반 라이선스를 갱신하거나 영구 라이선스를 받아야 합니다.

참고 강력한 암호화(3DES/AES)를 위한 평가 라이선스를 받을 수 없습니다. 강력한 암호화(3DES/AES) 라이선스를 활성화하는 내보내기-컴플라이언스 토큰을 받으려면 License Authority에 등록하고 영구 라이선스를 획득해야 합니다.

Smart Software Manager 통신

이 섹션에서는 디바이스가 Smart Software Manager와 통신하는 방법을 설명합니다.

디바이스 등록 및 토큰

각 가상 어카운트에서 등록 토큰을 만들 수 있습니다. 이 토큰은 기본적으로 30일간 유효합니다. 각 디바이스를 구축할 때 또는 기존 디바이스를 등록할 때 이 토큰 ID와 엔타이틀먼트 레벨을 입력합니다. 기존 토큰이 만료되면 새 토큰을 생성할 수 있습니다.

참고 Firepower 4100/9300 섀시 — 디바이스 등록은 ASA 논리적 디바이스가 아니라 섀시에서 구성됩니다.

구축 이후 시작할 때 또는 기존 디바이스에서 이 매개변수를 수동으로 구성한 후에 디바이스가 Cisco License Authority에 등록됩니다. 디바이스를 토큰과 함께 등록하면 License Authority는 디바이스와 License Authority 간의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다.

License Authority와의 정기적인 통신

디바이스는 30일마다 License Authority와 통신합니다. Smart Software Manager에서 변경할 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다.

선택 사항으로 HTTP 프록시를 구성할 수 있습니다.

최소 90일마다 ASAv가 직접 또는 HTTP 프록시를 통해 인터넷에 연결되어야 합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 디바이스는 최대 90일간 콜 홈 없이 규정 준수 상태를 유지할 수 있습니다. 유예 기간이 지난 후에는 Licensing Authority에 연락해야 하며, 연락하지 않으면 ASAv가 컴플라이언스 미준수 상태가 됩니다.

최소 90일마다 Firepower 4100/9300 섀시가 직접 또는 HTTP 프록시를 통해 인터넷에 연결되어야 합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 디바이스는 최대 90일간 콜 홈 없이 작동할 수 있습니다. 유예 기간이 지난 후 Licensing Authority에 연락해야 합니다. 아니면 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다.

규정 위반 상태

디바이스는 다음과 같은 상황에서 규정 위반이 될 수 있습니다.

- 과다 사용 — 디바이스에서 사용 불가한 라이선스를 사용할 경우.
- 라이선스 만료—한시적인 라이선스가 만료된 경우.
- 통신 부재 — 디바이스에서 권한 재부여를 위해 Licensing Authority에 연결하지 못한 경우.

어카운트가 컴플라이언스 미준수 상태인지 또는 컴플라이언스 미준수 상태에 근접한지를 확인하려면 디바이스에서 현재 사용 중인 엔타이틀먼트와 Smart Account의 엔타이틀먼트를 비교해야 합니다.

컴플라이언스 미준수 상태인 디바이스는 모델에 따라 제한될 수 있습니다.

- ASAv — ASAv는 영향을 받지 않습니다.
- Firepower 2100의 ASA — 특별 라이선스가 필요한 기능의 구성을 변경할 수 없지만 작업은 달리 영향을 받지 않습니다. 예를 들어 표준 라이선스 한도를 초과하는 기존 컨텍스트를 계속 실행할 수 있으며 해당 구성을 수정할 수는 있지만 새 컨텍스트를 추가할 수는 없습니다.
- Firepower 4100/9300 섀시의 ASA — 특별 라이선스가 필요한 기능의 컨피그레이션을 변경할 수 없지만 작업은 달리 영향을 받지 않습니다. 예를 들어 표준 라이선스 한도를 초과하는 기존 컨텍스트를 계속 실행할 수 있으며 해당 구성을 수정할 수는 있지만 새 컨텍스트를 추가할 수는 없습니다.

Smart Call Home 인프라

기본적으로, Smart Call Home 프로파일은 Licensing Authority의 URL을 지정하는 컨피그레이션에 있습니다. 이 프로필을 제거할 수 없습니다. License 프로필의 유일한 구성 옵션은 License Authority의 대상 주소 URL입니다. Cisco TAC에서 지시하지 않는 한 License Authority URL을 변경해서는 안 됩니다.

참고 Firepower 4100/9300 섀시의 경우, 라이선싱을 위한 Smart Call Home은 ASA가 아닌 Firepower 4100/9300 섀시 관리자(Supervisor)에서 구성됩니다.

Smart Software Licensing의 Smart Call Home을 비활성화할 수 없습니다. 예를 들어, **no service call-home** 명령을 사용하여 Smart Call Home을 비활성화하는 경우에도 Smart Software Licensing은 비활성화되지 않습니다.

다른 Smart Call Home 기능은 명시적으로 구성하지 않는 한 켜지지 않습니다.

스마트 라이선스 인증서 관리

ASA에서는 Smart Call Home 서버 인증서를 발급한 CA의 인증서가 포함된 트러스트 포인트를 자동으로 생성합니다. 서버 인증서의 발급 계층이 변경되는 경우 서비스 중단을 방지하려면 **auto-update** 명령을 구성하여 주기적으로 신뢰풀 번들의 자동 업데이트를 활성화합니다.

Smart License Server에서 받은 서버 인증서는 Extended Key Usage(확장 키 사용) 필드에서 "ServAuth"를 포함해야 합니다. 이 확인은 비 SSC(자가서명 인증서)에서만 수행됩니다. SSC(자가서명 인증서)는 이 필드에서 값을 제공하지 않습니다.

라이센스 참고 사항

다음 표에서는 라이센스에 대한 자세한 정보가 나와 있습니다.

AnyConnect Plus 및 APEX 라이선스

AnyConnect Plus 또는 Apex 라이선스는 여러 ASA에 적용할 수 있는 다용도 라이선스입니다. 이 모두는 라이선스에서 지정한 대로 사용자 풀을 공유합니다. Smart Licensing을 사용하는 디바이스에서는 AnyConnect 라이선스를 실제 플랫폼에 물리적으로 적용할 필요가 없습니다. 하지만 SW Center에 액세스하고 기술 지원을 받으려면 여전히 동일한 라이선스를 구매해야 하며 계약 번호를 Cisco.com ID에 연결해야 합니다. 자세한 내용은 다음 링크를 참조하십시오.

- Cisco AnyConnect 주문 설명서
- AnyConnect 라이선싱 FAQ(자주 묻는 질문)

기타 VPN 라이선스

기타 VPN 세션에는 다음과 같은 VPN 유형이 포함됩니다.

- IKEv1을 사용하는 IPsec 원격 액세스 VPN
- IKEv1을 사용하는 IPsec 사이트 대 사이트 VPN
- IKEv2를 사용하는 IPsec 사이트 대 사이트 VPN

이 라이센스는 Base 라이센스에 포함됩니다.

결합된 총 VPN 세션, 모든 유형

- 최대 VPN AnyConnect 및 기타 VPN 세션보다 많은 상태에서 최대 VPN 세션이 추가되더라도 전체 세션은 VPN 세션 한도를 초과하면 안 됩니다. 최대 VPN 세션 수를 초과할 경우, ASA가 오버로드될 수 있으므로 네트워크의 크기를 적절하게 조정해야 합니다.
- 클라이언트리스 SSL VPN 세션을 시작한 후 포털에서 AnyConnect 클라이언트 세션을 시작한 경우, 총 1개의 세션이 사용됩니다. 그러나 처음에 AnyConnect 클라이언트를 시작한 후(예: 독립형 클라이언트에서) 클라이언트리스 SSL VPN 포털에 로그인할 경우 2개의 세션이 사용됩니다.

암호화 라이선스

강력한 암호화**: ASAv**

강력한 암호화(3DES/AES)는 License Authority 또는 Satellite 서버에 연결하기 전에 관리 연결에 사용할 수 있습니다. 따라서 ASDM을 실행하고 License Authority에 연결할 수 있습니다. through-the-box 트래픽의 경우 License Authority에 연결하고 강력한 암호화 라이선스를 획득할 때까지 처리량이 매우 제한됩니다.

Smart Software Licensing 어카운트에서 ASAv에 대한 등록 토큰을 요청할 때 **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내

기 제어 기능 허용**)** 확인란을 선택하여 강력한 암호화(3DES/AES) 라이선스를 적용하십시오(사용하기 위해서는 어카운트가 유효해야 함). ASAv가 나중에 컴플라이언스 미준수 상태가 되는 경우 내보내기 컴플라이언스 토큰을 적용한 경우에 한해 ASAv가 라이선스를 유지하고 속도가 제한되는 상태로 되돌아가지 않습니다. ASAv를 다시 등록하고 내보내기 컴플라이언스가 비활성화되는 경우 또는 ASAv를 공장 기본 설정으로 복원하는 경우 라이선스가 제거됩니다.

강력한 암호화 없이 ASAv를 처음 등록하고 나중에 강력한 암호화를 추가하는 경우, 새 라이선스를 적용하려면 ASAv를 다시 로드해야 합니다.

Satellite 서버 2.3.0 이전 버전의 경우, ASA 구성(내보내기 컴플라이언스 토큰이 지원되지 않음) 시 강력한 암호화 라이선스를 직접 요청해야 합니다. 이 경우 ASAv가 컴플라이언스 미준수 상태가 되면 처리량이 매우 제한됩니다.

강력한 암호화**: Firepower 2100**

강력한 암호화(3DES/AES)는 ASDM을 실행할 수 있도록 License Authority 또는 Satellite 서버에 연결하기 전에 관리 연결에 사용할 수 있습니다. ASDM 액세스는 기본 암호화를 사용하는 관리 전용 인터페이스에서만 사용할 수 있습니다. through-the-box 트래픽은 강력한 암호화 라이선스에 연결하여 라이선스를 획득한 후에만 허용됩니다.

Smart Software Licensing 어카운트에서 ASA에 대한 등록 토큰을 요청할 때 **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** 확인란을 선택하여 강력한 암호화(3DES/AES) 라이선스를 적용하십시오(사용하기 위해서는 어카운트가 유효해야 함). ASA가 나중에 컴플라이언스 미준수 상태가 되면 내보내기 컴플라이언스 토큰을 적용한 경우에 한해, ASA에서 through-the-box 트래픽을 계속 허용합니다. ASA를 다시 등록하고 내보내기 컴플라이언스가 비활성화되어 있는 경우에도 라이선스는 활성화된 상태로 유지됩니다. ASA를 공장 기본 설정으로 복원하는 경우 라이선스는 제거됩니다.

강력한 암호화 없이 ASA를 처음 등록하고 나중에 강력한 암호화를 추가하는 경우, 새 라이선스를 적용하려면 ASA를 다시 로드해야 합니다.

Satellite 서버 2.3.0 이전 버전의 경우, ASA 구성(내보내기 컴플라이언스 토큰이 지원되지 않음) 시 강력한 암호화 라이선스를 직접 요청해야 합니다. 이 경우 ASA가 컴플라이언스 미준수 상태가 되면 통과 트래픽이 허용되지 않습니다.

강력한 암호화**: Firepower 4100/9300** 섀시

Smart Software Licensing 어카운트에서 Firepower 섀시에 대한 등록 토큰을 요청할 때 **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** 확인란을 선택하여 강력한 암호화(3DES/AES) 라이선스를 적용하십시오(사용하기 위해서는 어카운트가 유효해야 함).

ASA가 논리적 디바이스로 구축되는 경우 섀시에서 강력한 암호화 라이선스를 상속받으므로 ASDM을 실행하고 통과 트래픽에 다른 기능을 즉시 사용할 수 있습니다. ASA가 나중에 컴플라이언스 미준수 상태가 되면 내보내기 컴플라이언스 토큰을 적용한 경우에 한해, ASA는 through-the-box 트래픽을 계속 허용합니다. 섀시를 다시 등록하고 내보내기 컴플라이언스가 비활성화되어 있는 경우 또는 섀시를 공장 기본 설정으로 복원하는 경우 라이선스가 제거됩니다.

강력한 암호화 없이 섀시를 처음 등록하고 나중에 강력한 암호화를 추가하는 경우, 새 라이선스를 적용하려면 ASA 애플리케이션을 다시 로드해야 합니다.

내보내기 컴플라이언스 토큰을 지원하지 않는 Satellite 서버 2.3.0 이전 버전의 경우, ASDM에 3DES가 필요하므로 CLI를 사용하여 ASA 구성에서 강력한 암호화 라이선스를 직접 요청해야 합니다. ASA가 컴플라이언스 미준수 상태가 되면 이 라이선스를 필요로 하는 통과 트래픽 및 관리 트래픽 모두 허용되지 않습니다.

DES: 모든 모델

DES 라이센스는 비활성화할 수 없습니다. 3DES 라이센스를 설치한 경우 DES를 계속 사용할 수 있습니다. Strong Encryption만 사용하고 DES를 사용하지 않으려면 모든 관련 명령에서 Strong Encryption만 사용하도록 구성해야 합니다.

통신 사업자 라이선스

통신 사업자 라이선스를 사용하면 다음과 같은 검사 기능을 활성화됩니다.

- 배율
- GTP/GPRS
- SCTP

총 **TLS** 프록시 세션

암호화된 음성 검사에 대한 각 TLS 프록시 세션의 수는 TLS 라이선스 한도를 기준으로 계산됩니다.

TLS 프록시 세션을 사용하는 기타 애플리케이션의 경우 TLS 한도에 가산되지 않습니다. Mobility Advantage Proxy(라이선스가 필요하지 않음)를 예로 들 수 있습니다.

일부 애플리케이션에서는 연결에 다중 세션을 사용할 수 있습니다. 예를 들어, 전화를 기본으로 구성하고 Cisco Unified Communications Manager를 백업할 경우, 2개의 TLS 프록시 연결이 있습니다.

tls-proxy maximum-sessions 명령을 사용하거나 ASDM에서 **Configuration(**구성**) > Firewall(**방화벽**) > Unified Communications > TLS Proxy(TLS** 프록시**)** 창을 사용하여 TLS 프록시 한도를 개별적으로 설정할 수 있습니다. 모델의 한도를 보려면 **tls-proxy maximum-sessions ?** 명령을 입력합니다. 기본 TLS 프록시 한도보다 높은 TLS 프록시 라이선스를 적용할 경우, ASA에서는 TLS 프록시 한도를 라이선스에 맞게 자동으로 설정합니다. TLS 프록시 한도는 라이선스 한도보다 우선합니다. TLS 프록시 한도를 해당 라이선스보다 작게 설정하면 라이선스에서 모든 세션을 사용할 수 없습니다.

참고 라이센스 부품 번호가 "K8"로 끝날 경우(예: 사용자 수 250명 이하의 라이센스), TLS 프록시 세션은 1000으로 제한됩니다. 라이센스 부품 번호가 "K9"로 끝날 경우(예: 사용자 수가 250명 이상인 라이센스), TLS 프록시 세션 한도는 컨피그레이션 및 모델 한도에 따라 달라집니다. K8 및 K9의 경우 해당 라이센스의 내보내기 제한 여부를 참조하며, K8은 제한되지 않고 K9는 제한됩니다.

예를 들어, **clear configure all** 명령을 사용하여 구성을 지우면 TLS 프록시 한도가 모델의 기본값으로 설정됩니다. 이 기본값이 라이선스 한도보다 낮을 경우, **tls-proxy maximum-sessions** 명령을 사용하여 한도를 다시 높이라는 오류 메시지가 표시됩니다(ASDM에서 **TLS Proxy(TLS** 프록시**)** 창 사용). 장애 조치를 사용 중이고 **write standby** 명령을 입력하거나 ASDM에서 **File(**파일**) > Save Running Configuration to Standby Unit(**실행 중인 구성을 대기 유닛에 저장**)**을 사용하여 기본 유닛에서 컨피그레이션 동기화를 시행할 경우, 보조 유닛에서 **clear configure all** 명령이 자동으로 생성되므로 보조 유닛에 경고 메시지가 표시될 수 있습니다. 컨피그레이션 동기화는 기본 유닛에서 TLS 프록시 한도 설정을 복원하므로 이러한 경고 메시지는 무시해도 좋습니다.

연결에 SRTP 암호화 세션을 사용할 수도 있습니다.

- K8 라이센스의 경우 SRTP 세션이 250개로 제한됩니다.
- K9 라이선스의 경우 제한이 없습니다.

참고 미디어 암호화/해독이 필요한 호출만 SRTP 한도에 가산됩니다. 호출에 통과가 설정되어 있으면 두 범례가 모두 SRTP인 경우에도 해당 호출은 한도에 가산되지 않습니다.

VLAN, 최대 개수

어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예를 들면 다음과 같습니다.

```
interface gigabitethernet 0/0.100
vlan 100
```

Botnet Traffic Filter 라이센스

동적 데이터베이스를 다운로드하려면 Strong Encryption(3DES/AES) 라이센스가 필요합니다.

장애 조치 또는 ASA 클러스터 라이센스

ASAv의 장애 조치 라이선스

스탠바이 유닛에는 기본 유닛과 동일한 모델 라이선스가 필요합니다.

Firepower 2100의 장애 조치 라이선스

각 Firepower 2100은 License Authority 또는 Satellite 서버에 등록해야 합니다. 보조 유닛에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 섀시용으로 별도의 라이선스를 구매해야 합니다.

각 ASA에는 동일한 암호화 라이선스가 있어야 합니다. 사용자가 등록 토큰을 적용하면 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화됩니다. Cisco Smart Software Manager Satellite 2.3.0 이전 버전 구축에 대해서는 아래 내용을 참조하십시오.

액티브/스탠바이 장애 조치의 경우 액티브 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 액티브/액티브 장애 조치의 경우 장애 조치 그룹 1이 액티브 상태인 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 스탠바이 유닛에 구성이 복제되지만 스탠바이 유닛은 구성을 사용하지 않으며 캐시된 상태로 유지됩니다. 액티브 유닛만 서버에서 라이선스를 요청합니다. 라이선스는 장애 조치 쌍에서 공유된 단일 장애 조치 라이선스로 집계되고 이 집계된 라이선스는 나중에 액티브 유닛이 되면 사용할 스탠바이 유닛에서도 캐시됩니다. 각 라이선스 유형은 다음과 같이 관리됩니다.

- Standard — 액티브 유닛만 서버에서 이 라이선스를 요청하는 경우에도 스탠바이 유닛에서는 기본적으로 Standard 라이선스가 활성화되어 있어 이를 사용하기 위해 서버에 등록할 필요가 없습니다.
- Context — 액티브 유닛에서만 이 라이선스를 요청합니다. 하지만, Standard 라이선스는 기본적으로 2개의 상황을 포함하며 두 유닛에 있습니다. 각 유닛의 Standard 라이선스 값과 액티브 유닛의 Context 라이선스 값은 플랫폼 한도에 도달할 때까지 통합됩니다. 예를 들면 다음과 같습니다.
  - Standard 라이선스는 2개의 상황을 포함하며, 2개의 Firepower 2130 유닛의 경우 이러한 라이선스에서는 최대 4개의 상황을 추가합니다. 액티브/스탠바이 쌍의 액티브 유닛에서 30개의 Context 라이선스를 구성합니다. 따라서 집계된 장애 조치 라이선스에서는 34개의 상황을 포함합니다. 그러나, 유닛 1개에 대한 플랫폼 한도가 30개이므로 통합된 라이선스에서는 최대 30개의 상황만 허용합니다. 이 경우 액티브 Context 라이선스만 25개의 상황으로 구성할 수 있습니다.
  - Standard 라이선스는 2개의 상황을 포함하고 2개의 Firepower 2130 유닛의 경우 이러한 라이선스는 최대 4개의 상황을 추가합니다. 액티브/액티브 쌍의 기본 유닛에서 10개의 Context 라이선스를 구성합니다. 따라서 집계된 장애 조치 라이선스에서는 14개의 상황을 포함합니다. 예를 들어, 한 유닛에서 9개의 상황을 사용하고 다른 유닛에서 5개의 상황을 사용하는 방식으로 총 14개를 사용할 수 있습니다. 유닛 1개에 대한 플랫폼 한도가 30개이므로 통합된 라이선스에서는 최대 30개의 상황을 허용합니다. 14개의 상황은 한도를 초과하지 않습니다.
- 강력한 암호화(3DES/AES)(Cisco Smart Software Manager Satellite 2.3.0 이전 버전 구축에만 해당) — 액티브 유닛에서만 이 라이선스를 요청하며, 라이선스 집계 덕분에 두 유닛에서 모두 이 라이선스를 사용할 수 있습니다. Smart Software Manager Satellite 구축의 경우 ASDM 및 기타 강력한 암호화 기능을 사용하려면 ASA CLI를 사용하여 액티브 유닛에서 강력한 암호화(3DES) 라이선스를 활성화해야 합니다. 강력한 암호화(3DES/AES) 라이선스는 어떤 유형의 평가 라이선스하고도 함께 사용할 수 없습니다.

장애 조치 후 새 액티브 유닛에서는 집계된 라이선스를 계속 사용합니다. 이러한 유닛에서는 캐시된 라이선스 구성을 사용하여 서버에서 엔타이틀먼트를 다시 요청합니다. 이전 액티브 유닛에서는 스탠바이 유닛으로 쌍을 다시 조인하는 경우, 라이선스 엔타이틀먼트를 릴리스합니다. 스탠바이 유닛

에서 엔타이틀먼트를 릴리스하기 전에, 어카운트에 사용 가능한 라이선스가 없는 경우 새 액티브 유닛의 라이선스는 컴플라이언스 미준수 상태일 수 있습니다. 장애 조치 쌍은 30일 동안 집계된 라이선스를 사용할 수 있지만 유예 기간이 지난 후에도 계속 컴플라이언스 미준수 상태인 경우에는 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다(예: 상황 추가). 이를 제외하면 작동에 영향을 미치지 않습니다. 새 액티브 유닛에서는 라이선스가 준수 상태가 될 때까지 35초마다 엔타이틀먼트 권한 부여 갱신 요청을 보냅니다. 장애 조치 쌍을 해제하면 액티브 유닛에서 엔타이틀먼트를 릴리스하고, 두 유닛은 캐시된 상태에서 라이선싱 구성을 유지합니다. 라이선싱을 다시 활성화하려면 각 유닛에서 구성을 지운 다음 다시 구성해야 합니다.

ASA의 장애 조치 라이선스 - Firepower 4100/9300 섀시

각 Firepower 4100/9300 섀시을 License Authority 또는 Satellite 서버에 등록해야 합니다. 보조 유닛에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 새시용으로 별도의 라이선스를 구매해야 합니다.

각 ASA에는 동일한 암호화 라이선스가 있어야 합니다. 일반 Smart Software Manager 사용자의 경우 Firepower 4100/9300 섀시에서 등록 토큰을 적용할 때 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화됩니다. Cisco Smart Software Manager Satellite 구축에 대해서는 아래 내용을 참조하십시오.

액티브/스탠바이 장애 조치에 대한 ASA 라이선스 구성에서는 액티브 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 액티브/액티브 장애 조치의 경우 장애 조치 그룹 1이 액티브 상태인 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 스탠바이 유닛에 구성이 복제되지만 스탠바이 유닛은 구성을 사용하지 않으며 캐시된 상태로 유지됩니다. 액티브 유닛만 서버에서 라이선스를 요청합니다. 라이선스는 장애 조치 쌍에서 공유된 단일 장애 조치 라이선스로 집계되고 이 집계된 라이선스는 스탠바이 유닛 중 하나가 나중에 액티브 유닛이 되면 사용할 스탠바이 유닛에서도 캐시됩니다. 각 라이선스 유형은 다음과 같이 관리됩니다.

- 표준 — 액티브 유닛만 서버에서 이 라이선스를 요청하는 경우에도 스탠바이 유닛에서는 기본적으로 Standard 라이선스가 활성화되어 있어 이를 사용하기 위해 서버에 등록할 필요가 없습니다.
- 상황 — 액티브 유닛만 이 라이선스를 요청합니다. 하지만, Standard 라이선스는 기본적으로 10개의 상황을 포함하며 두 유닛에 있습니다. 각 유닛의 Standard 라이선스 값과 액티브 유닛의 상황 라이선스 값은 플랫폼 제한이 될 때까지 결합됩니다. 예를 들면 다음과 같습니다.
  - Standard 라이선스는 10개의 상황을 포함하고 2개의 유닛의 경우 이러한 라이선스는 최대 20개의 상황을 추가합니다. 액티브/스탠바이 쌍의 액티브 유닛에서 250개의 Context 라이선스를 구성합니다. 따라서 집계된 장애 조치 라이선스는 270개의 상황을 포함합니다. 그러나, 1개의 유닛당 플랫폼 한도가 250개이므로 통합 라이선스에서는 최대 250개의 상황만 허용합니다. 이 경우 액티브 Context 라이선스만 230개의 상황으로 구성해야 합니다.
  - Standard 라이선스는 10개의 상황을 포함하고 2개의 유닛의 경우 이러한 라이선스는 최대 20개의 상황을 추가합니다. 액티브/액티브 쌍의 기본 유닛에서 10개의 상황 라이선스를 구성합니다. 따라서 집계된 장애 조치 라이선스에서는 30개의 상황을 포함합니다. 예를 들어, 한 유닛에서 17개의 상황을 사용하고 다른 유닛에서 13개의 상황을 사용하는 방식으로 총 30개를 사용할 수 있습니다. 유닛 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 30개의 상황은 한도를 초과하지 않습니다.

- 통신 사업자 — 액티브 유닛에서만 이 라이선스를 요청할 수 있으며 라이선스 집계 덕분에 두 유닛 모두 이 라이선스를 사용할 수 있습니다.
- 강력한 암호화(3DES)(Cisco Smart Software Manager Satellite 2.3.0 이전 버전 구축에만 해당) — 액티브 유닛에서만 이 라이선스를 요청하며 라이선스 집계 덕분에 두 유닛에서 해당 라이선스를 사용할 수 있습니다. Smart Software Manager Satellite 구축의 경우 ASDM 및 기타 강력한 암호화 기능을 사용하려면 클러스터를 구축한 후에 ASA CLI를 사용하여 액티브 유닛에서 강력한 암호화(3DES) 라이선스를 활성화해야 합니다. 강력한 암호화(3DES) 라이선스는 어떤 유형의 평가 라이선스하고도 함께 사용할 수 없습니다.

장애 조치 후 새 액티브 유닛은 집계된 라이선스를 계속 사용합니다. 이러한 유닛은 캐시된 라이선스 구성을 사용하여 서버에서 엔타이틀먼트를 다시 요청합니다. 이전 액티브 유닛이 스탠바이 유닛으로 쌍을 다시 조인하는 경우, 라이선스 엔타이틀먼트를 릴리스합니다. 스탠바이 유닛이 엔타이틀먼트를 릴리스하기 전에 어카운트에서 사용 가능한 라이선스가 없는 경우 새 액티브 유닛의 라이선스는 컴플라이언스 미준수 상태일 수 있습니다. 장애 조치 쌍은 30일 동안 집계된 라이선스를 사용할 수 있지만 유예 기간이 지난 후에도 계속 컴플라이언스 미준수 상태인 경우에는 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다. 새 액티브 유닛은 라이선스 준수 상태가 될 때까지 35초마다 엔타이틀먼트 권한 부여 갱신 요청을 보냅니다. 장애 조치 쌍을 해제하면 액티브 유닛에서 엔타이틀먼트를 릴리스하고, 두 유닛은 캐시된 상태에서 라이선싱 구성을 유지합니다. 라이선싱을 다시 활성화하려면 각 유닛에서 구성을 지운 다음 다시 구성해야 합니다.

ASA의 ASA 클러스터 라이선스 - Firepower 4100/9300 섀시

각 Firepower 4100/9300 섀시를 License Authority 또는 Satellite 서버에 등록해야 합니다. 슬레이브 유닛에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 섀시용으로 별도의 라이선스를 구매해야 합니다.

각 ASA에는 동일한 암호화 라이선스가 있어야 합니다. 일반 Smart Software Manager 사용자의 경우 Firepower 4100/9300 섀시에서 등록 토큰을 적용할 때 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화됩니다. 이전 Cisco Smart Software Manager Satellite 구축에 대해서는 아래 내용을 참조하십시오.

ASA 라이선스 구성에서는 마스터 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 구성은 슬레이브 유닛에 복제됩니다. 하지만 일부 라이선스의 경우 구성을 사용하지 않고 캐시된 상태로 남으며, 마스터 유닛만 라이선스를 요청합니다. 라이선스는 클러스터 유닛에서 공유된 단일 클러스터 라이선스로 집계되고, 이 집계된 라이선스는 슬레이브 유닛 중 하나가 나중에 마스터 유닛이 되면 사용할 슬레이브 유닛에서도 캐시됩니다. 각 라이선스 유형은 다음과 같이 관리됩니다.

- Standard — 마스터 유닛만 서버에서 Standard 라이선스를 요청합니다. 슬레이브 유닛에서는 기본적으로 Standard 라이선스가 활성화되어 있으므로 이를 사용하기 위해 서버에 등록할 필요가 없습니다.
- Context — 마스터 유닛만 서버에서 Context 라이선스를 요청합니다. Standard 라이선스는 기본적으로 10개의 상황을 포함하며 모든 클러스터 멤버에 있습니다. 각 유닛의 Standard 라이선스 값과 마스터 유닛의 Context 라이선스 값은 집계된 클러스터 라이선스에서 플랫폼 한도에 도달할 때까지 통합됩니다. 예를 들면 다음과 같습니다.

- 클러스터에 6개의 Firepower 9300 모듈을 갖고 있습니다. Standard 라이선스는 10개의 상황을 포함하고 이러한 라이선스는 6개 유닛에 최대 60개의 상황을 추가합니다. 마스터 유닛에서 20개의 추가 Context 라이선스를 구성합니다. 따라서 집계된 클러스터 라이선스에서는 80개의 상황을 포함합니다. 모듈 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 80개의 상황은 제한을 초과하지 않습니다. 따라서 마스터 유닛에서 최대 80개의 상황을 구성할 수 있습니다. 각 슬레이브 유닛에서도 구성 복제를 통해 80개의 상황을 포함할 수 있습니다.
- 클러스터에 3개의 Firepower 4110 유닛을 갖고 있습니다. Standard 라이선스는 10개의 상황을 포함하고 이러한 라이선스는 3개 유닛에 최대 30개의 상황을 추가합니다. 마스터 유닛에서 250개의 추가 Context 라이선스를 구성합니다. 따라서 집계된 클러스터 라이선스에서는 280개의 상황을 포함합니다. 유닛 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 280개의 상황은 제한을 초과합니다. 따라서 마스터 유닛에서는 최대 250개의 상황만 구성할 수 있습니다. 각 슬레이브 유닛에서도 구성 복제를 통해 250개의 상황을 포함할 수 있습니다. 이 경우 마스터 Context 라이선스만 220개의 상황으로 구성해야 합니다.

- 통신 사업자 — 분산 S2S VPN에 필요합니다. 이 라이선스는 유닛당 엔타이틀먼트이며 각 유닛은 서버에서 고유한 라이선스를 요청합니다. 이 라이선스 구성은 슬레이브 유닛에 복제됩니다.
- 강력한 암호화(3DES)(2.3.0 이전 Cisco Smart Software Manager Satellite 구축에만 해당) — 이 라이선스는 유닛당 엔타이틀먼트이며 각 유닛은 서버에서 고유한 라이선스를 요청합니다. Smart Software Manager Satellite 구축의 경우 ASDM 및 기타 강력한 암호화 기능을 사용하려면 클러스터를 구축한 후에 ASA CLI를 사용하여 마스터 유닛에서 강력한 암호화(3DES) 라이선스를 활성화해야 합니다. 이 라이선스 구성은 슬레이브 유닛에 복제됩니다. 강력한 암호화(3DES) 라이선스는 어떤 유형의 평가 라이선스하고도 함께 사용할 수 없습니다.

새 마스터 유닛이 선택되면 새 마스터 유닛은 집계된 라이선스를 계속해서 사용합니다. 또한 마스터 라이선스를 다시 요청하기 위해 캐시된 라이선스 구성을 사용합니다. 이전 마스터 유닛이 클러스터를 슬레이브 유닛으로 다시 조인하는 경우, 마스터 유닛 라이선스 엔타이틀먼트를 릴리스합니다. 슬레이브 유닛이 라이선스를 릴리스하기 전에 어카운트에서 사용 가능한 라이선스가 없는 경우 마스터 유닛의 라이선스는 비준수 상태일 수 있습니다. 유지된 라이선스는 30일 동안 유효하지만 유예 기간이 지난 후에도 계속해서 비준수 상태인 경우 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다. 새 액티브 유닛은 라이선스 준수 상태가 될 때까지 12시간마다 엔타이틀먼트 권한 부여 갱신 요청을 보냅니다. 라이선스 요청이 완전히 처리될 때까지 구성을 변경하지 않아야 합니다. 유닛이 클러스터를 떠나는 경우, 캐시된 마스터 구성은 제거되는 반면, 유닛당 엔타이틀먼트는 유지됩니다. 특히, 비클러스터 유닛에서 Context 라이선스를 다시 요청해야 합니다.

Smart Software Licensing 사전 요구 사항

- Cisco Smart Software Manager에서 마스터 계정을 만듭니다.

  https://software.cisco.com/#module/SmartLicensing

아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

- Cisco Commerce Workspace에서 라이선스를 1개 이상 구매합니다. 홈 페이지의 **Find Products and Solutions(**제품 및 솔루션 찾기**)** 검색 필드에서 라이선스 PID를 검색합니다. 일부 라이선스는 무료이지만 Smart Software Licensing 어카운트에 추가해야 합니다.
- ASAv 및 Firepower 2100: 디바이스에서 인터넷 액세스 또는 HTTP 프록시 액세스 또는 Satellite 서버 액세스를 지원합니다. 또는 영구 라이선스 예약을 사용할 수 있습니다.
- ASAv 및 Firepower 2100: 디바이스에서 Licensing Authority의 이름을 확인할 수 있도록 DNS 서버를 구성합니다.
- ASAv 및 Firepower 2100: 디바이스의 클럭을 설정합니다. Firepower 2100의 FXOS에서 클럭을 설정합니다.
- ASAv: 영구 라이선스 예약은 Azure 하이퍼바이저에서 지원되지 않습니다.
- Firepower 4100/9300 섀시: ASA 라이선싱 엔타이틀먼트를 구성하기 전에 Firepower 4100/9300 섀시에서 Smart Software Licensing 인프라를 구성합니다.

스마트 소프트웨어 라이센싱을 위한 지침

- 스마트 소프트웨어 라이센싱만 지원됩니다. ASAv의 이전 소프트웨어에서 기존 PAK 라이선스 ASAv를 업그레이드하는 경우 이전에 설치한 액티베이션 키는 무시되지만 디바이스에 유지됩니다. ASAv를 다운그레이드할 경우 액티베이션 키가 복구됩니다.
- 영구 라이선스 예약을 위해 디바이스를 해제하기 전에 라이선스를 반환해야 합니다. 공식적으로 라이선스를 반환하지 않는 경우 라이선스는 사용된 상태로 유지되고 새 디바이스용으로 재사용할 수 없습니다.

Smart Software Licensing의 기본값

ASAv

- ASAv 기본 구성에는 Smart Call Home 프로필인 “라이선스”(Licensing Authority의 URL을 지정)가 포함되어 있습니다.

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

- ASAv를 구축할 때 기능 계층 및 처리량 레벨을 설정합니다. 현재는 표준 레벨만 사용 가능합니다. 영구 라이선스 예약의 경우 이러한 파라미터를 설정할 필요가 없습니다. 영구 라이선스 예약을 활성화하는 경우 이러한 명령이 구성에서 제거됩니다.

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
```

- 또한 구축 과정에서 선택적으로 HTTP 프록시를 구성할 수 있습니다.

```
call-home
  http-proxy ip_address port port
```

Firepower 2100

Firepower 2100 기본 구성에는 Smart Call Home 프로필인 "라이선스"(Licensing Authority의 URL을 지정)가 포함되어 있습니다.

```
call-home
  profile License
   destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

ASA Firepower 4100/9300 섀시

기본 구성이 없습니다. Standard 라이선스 계층 및 기타 선택 사항인 라이선스를 수동으로 활성화해야 합니다.

ASAv: Smart Software Licensing 구성

이 섹션에서는 ASAv에 대한 Smart Software Licensing을 구성하는 방법에 관해 설명합니다. 다음 방법 중 하나를 선택합니다.

프로시저

단계 **1** ASAv: 일반 Smart Software Licensing 구성, 130 페이지.

단계 **2** ASAv: 영구 라이선스 예약 구성, 135 페이지.

ASAv: 일반 Smart Software Licensing 구성

ASAv를 구축하는 경우 디바이스를 사전에 구성하고 등록 토큰을 포함하여 License Authority에 등록하고 Smart Software Licensing을 활성화할 수 있습니다. HTTP 프록시 서버, 라이선스 엔타이틀먼트를 변경해야 하거나 ASAv를 등록해야 하는 경우(예를 들어, Day 0 구성에 ID 토큰을 포함하지 않은 경우) 이 작업을 수행하십시오.

참고 ASAv를 구축한 경우 HTTP 프록시 및 라이선스 엔타이틀먼트를 사전에 구성했을 수 있습니다. ASAv를 구축한 경우 Day 0 구성에 등록 토큰을 포함했을 수도 있습니다. 그렇게 한 경우, 이 절차를 사용하여 다시 등록할 필요가 없습니다.

프로시저

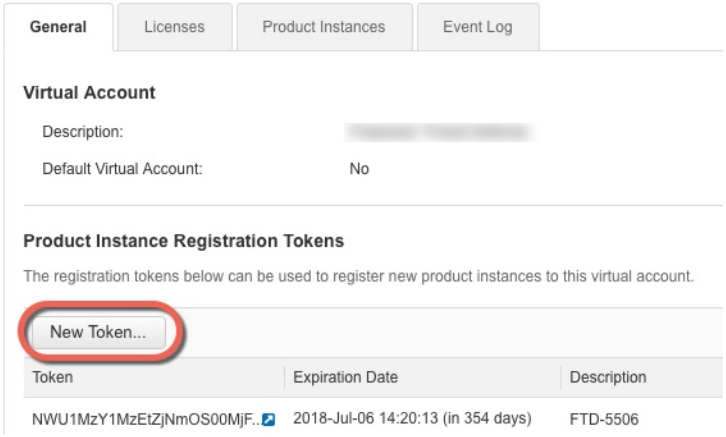
단계 **1** Smart Software Manager(Cisco Smart Software Manager)에서 이 디바이스를 추가하려는 가상 계정에 대한 등록 토큰을 요청 및 복사합니다.

a) **Inventory(**인벤토리**)**를 클릭합니다.

그림 ***7:*** 인벤토리

b) **General(**일반**)** 탭에서 **New Token(**새 토큰**)**을 클릭합니다.

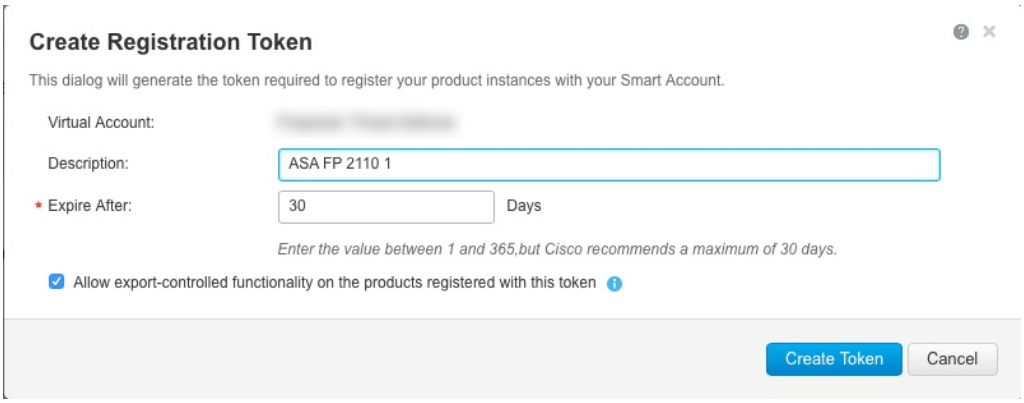
그림 ***8:*** 새 토큰



c) **Create Registration Token(**등록 토큰 생성**)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(**토큰 생성**)**을 클릭합니다.

- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.
- **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** — export-compliance 플래그를 활성화합니다.

그림 *9:* 등록 토큰 생성



토큰이 인벤토리에 추가됩니다.

d) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(**토큰**)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 ASA를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

그림 *10:* 토큰 보기

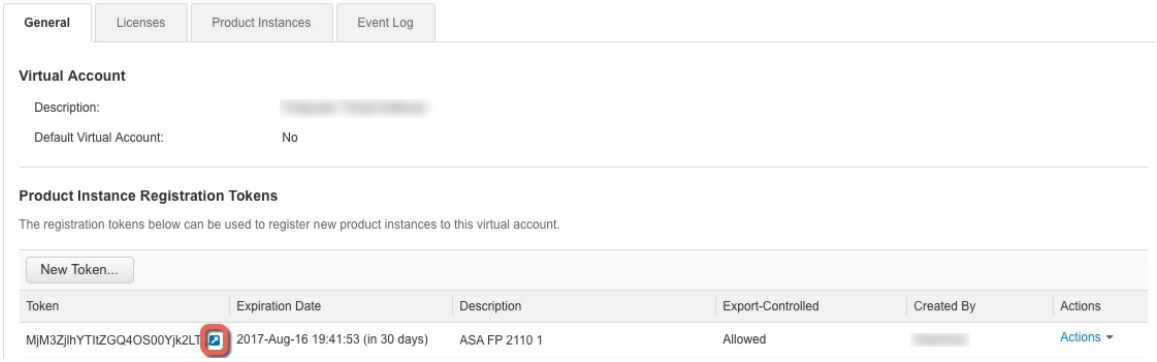
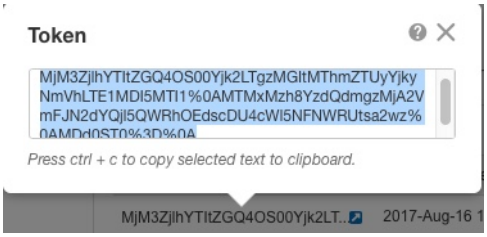


그림 *11:* 토큰 복사



단계 **2** (선택 사항) ASAv에서 HTTP 프록시 URL을 지정합니다.

call-home

http-proxy *ip_address* **port** *port*

네트워크에서 인터넷 액세스를 위해 HTTP 프록시를 사용하는 경우, Smart Software Licensing에 대해 프록시 주소를 구성해야 합니다. 일반적으로 이 프록시는 Smart Call Home에도 사용됩니다.

예제:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

단계 **3** 라이선스 엔타이틀먼트를 구성합니다.

a) 라이센스 스마트 컨피그레이션 모드를 시작합니다.

license smart

예제:

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 기능 계층을 설정합니다.

feature tier standard

표준 계층만 사용 가능합니다..

c) 처리량 레벨을 설정합니다.

throughput level {**100M** | **1G** | **2G** | **10G**}

예제:

```
ciscoasa(config-smart-lic)# throughput level 2G
```

a) 변경 사항을 적용하기 위해 라이센스 스마트 모드를 종료합니다.

exit

라이센스 스마트 구성 모드를 명시적으로 종료하거나(**exit** 또는 **end**) 다른 모드를 시작하는 명령을 입력하여 종료할 때까지 변경사항이 적용되지 않습니다.

예제:

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

단계 **4** License Authority에 ASAv를 등록합니다.

ASAv를 등록할 때 License Authority에서는 ASAv와 License Authority 간의 통신을 위해 ID 인증서를 발급합니다. 또한 ASAv를 적절한 가상 어카운트에 할당합니다. 일반적으로 이 절차는 1회 수행됩니다. 그러나 예를 들어 통신 문제 때문에 ID 인증서가 만료되면 나중에 ASAv를 다시 등록해야 할 수 있습니다.

a) ASAv에 등록 토큰을 입력합니다.

license smart register idtoken *id_token* [**force**]

예제:

이미 등록되었지만 License Authority와 동기화되지 않았을 수 있는 ASAv를 등록하려면 **force** 키워드를 사용합니다. 예를 들어 Smart Software Manager에서 실수로 ASAv를 제거한 경우 **force**를 사용합니다.

ASAv에서는 License Authority에 등록을 시도하고 구성된 라이선스 엔타이틀먼트에 대한 권한 부여를 요청합니다.

예제:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASAv: Satellite Smart Software Licensing 구성

이 절차는 Satellite Smart Software Licensing 서버를 사용하는 ASAv에 적용됩니다.

시작하기 전에

Cisco.com에서 Smart Software Manager Satellite OVA 파일을 다운로드하고 VMwareESXi 서버에 이 파일을 설치 및 구성합니다. 자세한 내용은 Smart Software Manager Satellite를 참조하십시오.

프로시저

단계 **1** Satellite 서버에서 등록 토큰을 요청합니다.

단계 **2** (선택 사항) ASA에서 HTTP 프록시 URL을 지정합니다.

call-home

http-proxy *ip_address* **port** *port*

네트워크에서 인터넷 액세스를 위해 HTTP 프록시를 사용하는 경우, Smart Software Licensing에 대해 프록시 주소를 구성해야 합니다. 일반적으로 이 프록시는 Smart Call Home에도 사용됩니다.

예제:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

단계 **3** Satellite 서버로 이동하려면 라이선스 서버 URL을 변경합니다.

call-home

profile License

destination address http https://*satellite_ip_address***/Transportgateway/services/DeviceRequestHandler**

예제:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

단계 **4** 1단계에서 요청한 토큰을 사용하여 ASA를 등록합니다.

license smart register idtoken *id-token*

예제:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA에서는 Satellite 서버에 등록하고 구성된 라이선스 엔타이틀먼트에 대한 권한 부여를 요청합니다. 어카운트에서 허용하는 경우 Satellite 서버에서는 강력한 암호화(3DES/AES) 라이선스도 적용합니다. 라이선스 상태 및 사용량을 확인하려면 **show license summary** 명령을 사용합니다.

예제:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

ASAv: 영구 라이선스 예약 구성

ASAv에 영구 라이선스를 할당할 수 있습니다. 이 섹션에서는 ASAv를 사용 중단하거나 모델 계층을 변경하고 새 라이선스가 필요한 경우 라이선스를 반환하는 방법도 설명합니다.

프로시저

단계 1 ASAv 영구 라이선스 설치, 136 페이지

단계 2 (선택 사항) (선택 사항) ASAv 영구 라이선스 반환, 138 페이지

ASAv 영구 라이선스 설치

인터넷에 액세스할 수 없는 ASAv의 경우, Smart Software Manager에서 영구 라이선스를 요청할 수 있습니다.

참고 영구 라이선스 예약을 위해 ASAv를 해제하기 전에 라이선스를 반환해야 합니다. 공식적으로 라이선스를 반환하지 않는 경우 라이선스는 사용된 상태로 유지되고 새 ASAv용으로 재사용할 수 없습니다. (선택 사항) ASAv 영구 라이선스 반환, 138 페이지을 참조하십시오.

참고 영구 라이선스를 설치한 후에 구성을 지우는 경우(예를 들어 **write erase** 사용), 1단계에 표시된 인수 없이 **license smart reservation** 명령을 사용하여 영구 라이선스 예약을 다시 활성화하기만 하면 됩니다. 즉, 이 절차의 나머지 부분은 수행할 필요가 없습니다.

시작하기 전에

- Smart Software Manager에서 사용할 수 있도록 영구 라이선스를 구매하십시오. 모든 계정에 대해 영구 라이선스 예약이 승인되는 것은 아닙니다. 구성을 시도하기 전에 Cisco에서 이 기능에 대한 승인을 받았는지 확인하십시오.
- ASAv가 시작된 후에 영구 라이선스를 요청해야 합니다. 영구 라이선스는 Day 0 구성의 일환으로 설치할 수 없습니다.

프로시저

단계 1 ASAv CLI에서 영구 라이선스 예약을 활성화합니다.

license smart reservation

예제:

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

다음과 같은 명령이 제거되었습니다.

```
license smart
```

```
feature tier standard
throughput level {100M | 1G | 2G | 10G}
```

일반 스마트 라이선싱을 사용하려면 이 명령의 **no** 형식을 사용하고 위의 명령을 다시 입력합니다. 다른 Smart Call Home 구성은 그대로 유지되지만 사용되지 않으므로 이러한 명령을 다시 입력할 필요가 없습니다.

단계 **2** Smart Software Manager에서 입력할 라이선스 코드를 요청합니다.

license smart reservation request universal

예제**:**

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

ASAv 구축 시 사용할 모델 수준(ASAv5/ASAv10/ASAv30/ASAv50)을 선택해야 합니다. 모델 레벨에 따라 요청하는 모델 레벨이 결정됩니다. 나중에 유닛의 모델 레벨을 변경하려면 현재 라이선스를 반환하고 올바른 모델 레벨에서 새 라이선스를 요청해야 합니다. 하이퍼바이저에서 이미 구축된 ASAv의 모델을 변경하려는 경우, 새로운 모델 요구 사항과 일치하도록 vCPU 및 DRAM 설정을 변경할 수 있습니다. 이 값에 대한 내용은 ASAv 빠른 시작 가이드를 참조하십시오. 현재 모델을 보려면 **show vm** 명령을 사용합니다.

이 명령을 다시 입력하는 경우, 다시 로드된 이후라도 동일한 코드가 표시됩니다. 이 코드를 Smart Software Manager에 아직 입력하지 않았으며 요청을 취소하려는 경우 다음을 입력합니다.

license smart reservation cancel

영구 라이선스 예약을 비활성화하면 모든 보류 중인 요청이 취소됩니다. 코드를 Smart Software Manager에 이미 입력한 경우, 라이선스를 ASAv에 적용하려면 이 절차를 완료해야 합니다. 이 절차를 완료한 이후 원하는 경우 라이선스를 반환할 수 있습니다. (선택 사항) ASAv 영구 라이선스 반환, 138 페이지을 참조하십시오.

단계 **3** Smart Software Manager Inventory(인벤토리) 화면으로 이동하여 **Licenses(**라이선스**)** 탭을 클릭합니다.

https://software.cisco.com/#SmartLicensing-Inventory

Licenses(라이선스**)** 탭에는 계정과 연결된 모든 기존 라이선스(일반 및 영구)가 표시됩니다.

단계 **4** **License Reservation(**라이선스 예약**)**을 클릭하고 ASAv 코드를 상자에 입력합니다. **Reserve License(**라이선스 예약**)**를 클릭합니다.

Smart Software Manager에서 인증 코드를 생성합니다. 코드를 다운로드하거나 클립보드로 복사할 수 있습니다. 이 시점에서는 Smart Software Manager에 따라 라이선스가 사용됩니다.

License Reservation(라이선스 예약**)** 버튼이 표시되지 않으면 어카운트가 영구 라이선스 예약에 대해 인증되지 않은 것입니다. 이 경우 영구 라이선스 예약을 비활성화하고 일반 smart license 명령을 다시 입력해야 합니다.

단계 **5** ASAv에서 인증 코드를 입력합니다.

license smart reservation install *code*

예제:

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

이제 ASAv에 완전히 라이선스가 부여되었습니다.

(선택 사항) ASAv 영구 라이선스 반환

영구 라이선스가 더 이상 필요하지 않은 경우(예를 들어, ASAv를 사용 중단하거나 모델 수준을 변경하여 새 라이선스가 필요한 경우) 이 절차를 사용하여 라이선스를 Smart Software Manager에 공식적으로 반환해야 합니다. 모든 단계를 수행하지 않으면 라이선스가 사용된 상태로 유지되므로 다른 곳에서 사용할 수 있도록 쉽게 해제될 수 없습니다.

프로시저

단계 1 ASAv에서 반환 코드를 생성합니다.

license smart reservation return

예제:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ASAv의 라이선스가 즉시 해제되고 Evaluation(평가) 상태로 전환됩니다. 이 코드를 다시 확인해야 할 경우 이 명령을 다시 입력합니다. 새 영구 라이선스(**license smart reservation request universal**)를 요청하거나 ASAv 모델 수준을 변경하는 경우(vCPU/RAM의 전원을 끄고 변경하여) 이 코드를 다시 표시할 수 없습니다. 반환을 완료하려면 코드를 캡처하십시오.

단계 2 Smart Software Manager에서 이 ASAv 인스턴스를 찾을 수 있도록 ASAv UDI(Universal Device Identifier)를 확인합니다.

show license udi

예제:

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

단계 3 Smart Software Manager Inventory(인벤토리) 화면으로 이동하여 **Product Instances(**제품 인스턴스**)** 탭을 클릭합니다.

https://software.cisco.com/#SmartLicensing-Inventory

Product Instances(제품 인스턴스**)** 탭에는 UDI별로 모든 라이선스가 부여된 제품이 표시됩니다.

단계 4 라이선스를 해제하려는 ASAv를 찾고 **Actions(작업) > Remove(제거)**를 선택한 후 ASAv 반환 코드를 상자에 입력합니다. **Remove Product Instance(제품 인스턴스 제거)**를 클릭합니다.

영구 라이선스가 사용 가능한 풀로 반환됩니다.

(선택 사항) ASAv 등록 취소(일반 및 Satellite)

ASAv를 등록 취소하면 어카운트에서 ASAv가 제거됩니다. ASAv의 모든 라이선스 엔타이틀먼트 및 인증서가 제거됩니다. 새 ASAv의 라이선스를 확보하기 위해 등록을 취소하는 경우가 있습니다. 또는 Smart Software Manager에서 ASAv를 제거할 수 있습니다.

프로시저

ASAv를 등록 취소합니다.

license smart deregister

그러면 ASAv가 다시 로드됩니다.

(선택 사항) ASAv ID 인증서 또는 라이선스 엔타이틀먼트 갱신(일반 및 Satellite)

기본적으로 ID 인증서는 6개월마다 자동으로 갱신되며, 라이선스 엔타이틀먼트는 30일마다 갱신됩니다. 예를 들어 인터넷 액세스 기간이 제한된 경우 또는 Smart Software Manager에서 라이선스를 변경한 경우, 이러한 항목 중 하나에 대한 등록을 수동으로 갱신할 수 있습니다.

프로시저

단계 1 ID 인증서를 갱신합니다.

license smart renew id

단계 2 라이센스 엔타이틀먼트를 갱신합니다.

license smart renew auth

Firepower 2100: Smart Software 라이선싱 구성

이 섹션에서는 Firepower 2100에 대한 Smart Software Licensing을 구성하는 방법에 관해 설명합니다. 다음 방법 중 하나를 선택합니다.

프로시저

단계 1 Firepower 2100: 일반 Smart Software 라이선싱 구성, 140 페이지.

(선택 사항) Firepower 2100 등록 취소(일반 및 Satellite), 149 페이지 또는 (선택 사항) Firepower 2100 ID 인증서 또는 라이선스 엔타이틀먼트 갱신(일반 및 Satellite), 149 페이지 작업을 수행할 수도 있습니다.

단계 2 Firepower 2100: Satellite Smart Software 라이선싱 구성, 144 페이지.

(선택 사항) Firepower 2100 등록 취소(일반 및 Satellite), 149 페이지 또는 (선택 사항) Firepower 2100 ID 인증서 또는 라이선스 엔타이틀먼트 갱신(일반 및 Satellite), 149 페이지 작업을 수행할 수도 있습니다.

단계 3 Firepower 2100: 영구 라이선스 예약 구성, 146 페이지.

Firepower 2100: 일반 Smart Software 라이선싱 구성

이 절차는 License Authority를 사용하는 ASA에 적용됩니다.

프로시저

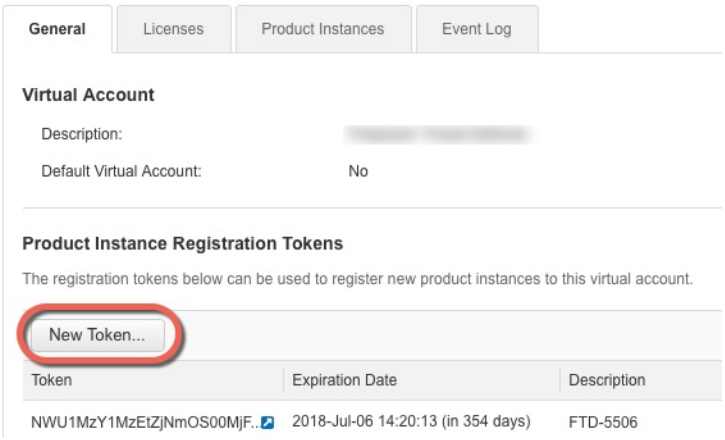
단계 1 Smart Software Manager(Cisco Smart Software Manager)에서 이 디바이스를 추가하려는 가상 계정에 대한 등록 토큰을 요청 및 복사합니다.

a) **Inventory**(인벤토리)를 클릭합니다.

그림 *12:* 인벤토리

b) **General**(일반) 탭에서 **New Token**(새 토큰)을 클릭합니다.

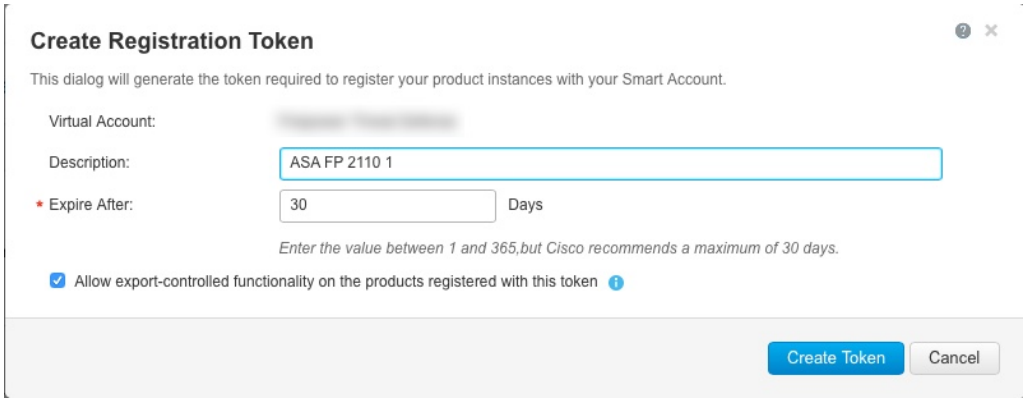
그림 *13:* 새 토큰



c) **Create Registration Token(**등록 토큰 생성**)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(**토큰 생성**)**을 클릭합니다.

- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.
- **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** — export-compliance 플래그를 활성화합니다.

그림 *14:* 등록 토큰 생성



토큰이 인벤토리에 추가됩니다.

d) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(**토큰**)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 ASA를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

그림 *15:* 토큰 보기

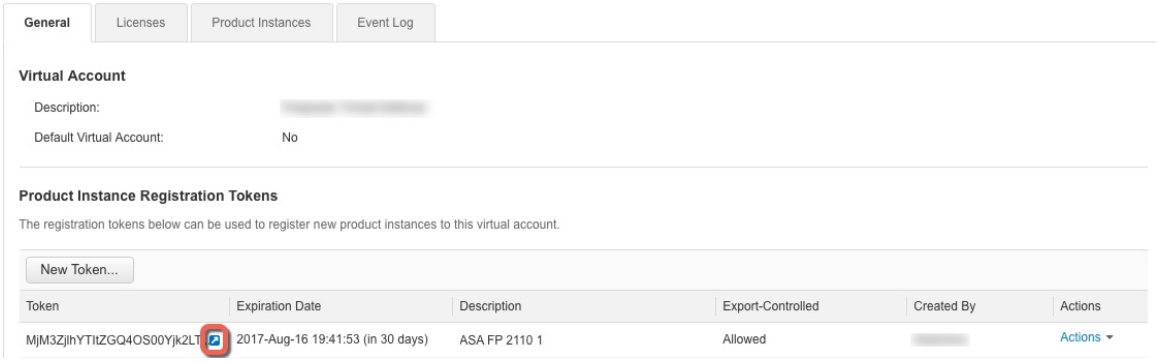
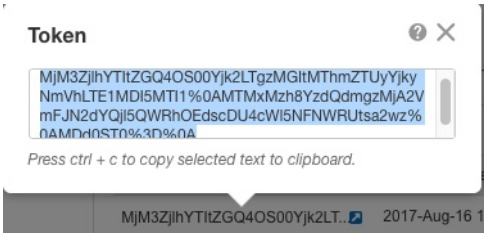


그림 *16:* 토큰 복사



단계 **2** (선택 사항) ASA에서 HTTP 프록시 URL을 지정합니다.

call-home

http-proxy *ip_address* **port** *port*

네트워크에서 인터넷 액세스를 위해 HTTP 프록시를 사용하는 경우, Smart Software Licensing에 대해 프록시 주소를 구성해야 합니다. 일반적으로 이 프록시는 Smart Call Home에도 사용됩니다.

예제:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

단계 **3** ASA에서 라이선스 엔타이틀먼트를 요청합니다.

a) 라이센스 스마트 컨피그레이션 모드를 시작합니다.

license smart

예제:

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 기능 계층을 설정합니다.

feature tier standard

표준 계층만 사용 가능합니다.. 다른 기능 라이센스를 추가하려면 기본적으로 계층 라이센스가 있어야 합니다.

c) 보안 상황 라이선스를 요청합니다.

feature context *number*

상황의 최대 수는 모델에 따라 다릅니다. 기본적으로 ASA에서는 2개의 상황을 지원하므로 2개의 기본 상황에서 빼고 싶은 상황 수를 요청해야 합니다.

예제:

```
ciscoasa(config-smart-lic)# feature context 18
```

단계 **4** 1단계에서 복사한 토큰을 사용하여 ASA를 등록합니다.

license smart register idtoken *id-token*

예제:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA는 License Authority에 등록하고 구성된 라이선스 엔타이틀먼트에 대한 권한 부여를 요청합니다. 계정에서 허용하는 경우 License Authority는 강력한 암호화(3DES/AES) 라이선스도 적용합니다. 라이선스 상태 및 사용량을 확인하려면 **show license summary** 명령을 사용합니다.

예제:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

Firepower 2100: Satellite Smart Software 라이선싱 구성

이 절차는 Satellite Smart Software Licensing 서버를 사용하는 ASA에 적용됩니다.

시작하기 전에

Cisco.com에서 Smart Software Manager Satellite OVA 파일을 다운로드하고 VMwareESXi 서버에 이 파일을 설치 및 구성합니다. 자세한 내용은 Smart Software Manager Satellite를 참조하십시오.

프로시저

단계 **1** Satellite 서버에서 등록 토큰을 요청합니다.

단계 **2** (선택 사항) ASA에서 HTTP 프록시 URL을 지정합니다.

call-home

http-proxy *ip_address* **port** *port*

네트워크에서 인터넷 액세스를 위해 HTTP 프록시를 사용하는 경우, Smart Software Licensing에 대해 프록시 주소를 구성해야 합니다. 일반적으로 이 프록시는 Smart Call Home에도 사용됩니다.

예제:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

단계 **3** Satellite 서버로 이동하려면 라이선스 서버 URL을 변경합니다.

call-home

profile License

destination address http https://*satellite_ip_address***/Transportgateway/services/DeviceRequestHandler**

예제:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

단계 **4** ASA에서 라이선스 엔타이틀먼트를 요청합니다.

a) 라이센스 스마트 컨피그레이션 모드를 시작합니다.

license smart

예제:

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 기능 계층을 설정합니다.

feature tier standard

표준 계층만 사용 가능합니다.. 다른 기능 라이센스를 추가하려면 기본적으로 계층 라이센스가 있어야 합니다.

c) 보안 상황 라이선스를 요청합니다.

feature context *number*

상황의 최대 수는 모델에 따라 다릅니다. 기본적으로 ASA는 2개의 상황을 지원하므로 2개의 기본 상황에서 빼고 싶은 상황 수를 요청해야 합니다.

예제:

```
ciscoasa(config-smart-lic)# feature context 18
```

단계 **5** 1단계에서 요청한 토큰을 사용하여 ASA를 등록합니다.

license smart register idtoken *id-token*

예제:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA는 Satellite 서버에 등록하고 구성된 라이선스 엔타이틀먼트에 대한 권한 부여를 요청합니다. 어카운트에서 허용하는 경우 Satellite 서버는 강력한 암호화(3DES/AES) 라이선스도 적용합니다. 라이선스 상태 및 사용량을 확인하려면 **show license summary** 명령을 사용합니다.

예제:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

Firepower 2100: 영구 라이선스 예약 구성

Firepower 2100에 영구 라이선스를 할당할 수 있습니다. 이 섹션에서는 ASA를 사용 중단하는 경우 라이선스를 반환하는 방법도 설명합니다.

프로시저

단계 1 Firepower 2100 영구 라이선스 설치, 146 페이지.

단계 2 (선택 사항) (선택 사항) Firepower 2100 영구 라이선스 반환, 148 페이지.

Firepower 2100 영구 라이선스 설치

인터넷에 액세스할 수 없는 ASA의 경우, Smart Software Manager에서 영구 라이선스를 요청할 수 있습니다. 영구 라이선스에서는 최대 보안 상황 수를 지닌 Standard 계층 등 모든 기능을 활성화합니다.

참고 영구 라이선스 예약을 위해 ASA를 해제하기 전에 라이선스를 반환해야 합니다. 공식적으로 라이선스를 반환하지 않는 경우 라이선스는 사용된 상태로 유지되고 새 ASA용으로 재사용할 수 없습니다. (선택 사항) Firepower 2100 영구 라이선스 반환, 148 페이지을 참조하십시오.

시작하기 전에

Smart Software Manager에서 사용할 수 있도록 영구 라이선스를 구매하십시오. 모든 계정에 대해 영구 라이선스 예약이 승인되는 것은 아닙니다. 구성을 시도하기 전에 Cisco에서 이 기능에 대한 승인을 받았는지 확인하십시오.

프로시저

단계 1 ASA CLI에서 영구 라이선스 예약을 활성화합니다.

license smart reservation

예제:

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

단계 2 Smart Software Manager에서 입력할 라이선스 코드를 요청합니다.

license smart reservation request universal

예제:

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

이 명령을 다시 입력하는 경우, 다시 로드된 이후라도 동일한 코드가 표시됩니다. 이 코드를 Smart Software Manager에 아직 입력하지 않았으며 요청을 취소하려는 경우 다음을 입력합니다.

license smart reservation cancel

영구 라이선스 예약을 비활성화하면 모든 보류 중인 요청이 취소됩니다. 코드를 Smart Software Manager에 이미 입력한 경우, 라이선스를 ASA에 적용하려면 이 절차를 완료해야 합니다. 이 절차를 완료한 이후 원하는 경우 라이선스를 반환할 수 있습니다. (선택 사항) Firepower 2100 영구 라이선스 반환, 148 페이지을 참조하십시오.

단계 **3** Smart Software Manager 인벤토리 화면으로 이동하여 **Licenses(**라이선스**)** 탭을 클릭합니다.

https://software.cisco.com/#SmartLicensing-Inventory

Licenses(라이선스**)** 탭에는 계정과 연결된 모든 기존 라이선스(일반 및 영구)가 표시됩니다.

단계 **4** **License Reservation(**라이선스 예약**)**을 클릭하고 ASA 코드를 상자에 입력합니다. **Reserve License(**라이선스 예약**)**를 클릭합니다.

Smart Software Manager에서 인증 코드를 생성합니다. 코드를 다운로드하거나 클립보드로 복사할 수 있습니다. 이 시점에서는 Smart Software Manager에 따라 라이선스가 사용됩니다.

License Reservation(라이선스 예약**)** 버튼이 표시되지 않으면 어카운트가 영구 라이선스 예약에 대해 인증되지 않은 것입니다. 이 경우 영구 라이선스 예약을 비활성화하고 일반 smart license 명령을 다시 입력해야 합니다.

단계 **5** ASA에서 인증 코드를 입력합니다.

license smart reservation install *code*

예제**:**

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

단계 **6** ASA에서 라이선스 엔타이틀먼트를 요청합니다.

ASA에서 엔타이틀먼트 사용을 허용하도록 ASA 구성에서 엔타이틀먼트를 요청해야 합니다.

a) 라이센스 스마트 컨피그레이션 모드를 시작합니다.

license smart

예제**:**

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 기능 계층을 설정합니다.

feature tier standard

표준 계층만 사용 가능합니다.. 다른 기능 라이센스를 추가하려면 기본적으로 계층 라이센스가 있어야 합니다.

c) 보안 상황 라이선스를 요청합니다.

feature context *number*

상황의 최대 수는 모델에 따라 달라집니다. 영구 라이선스가 상황의 최대 수를 포함하기 때문에 최댓값을 요청하고 2개의 기본 상황을 빼야 합니다.

예제:

```
ciscoasa(config-smart-lic)# feature context 18
```

(선택 사항) Firepower 2100 영구 라이선스 반환

영구 라이선스가 더 이상 필요하지 않은 경우(예를 들어, ASA를 사용 중단하는 경우) 이 절차를 사용하여 라이선스를 Smart Software Manager에 공식적으로 반환해야 합니다. 모든 단계를 수행하지 않으면 라이선스가 사용된 상태로 유지되므로 다른 곳에서 사용하기 위해 쉽게 해제될 수 없습니다.

프로시저

단계 **1** ASA에서 반환 코드를 생성합니다.

license smart reservation return

예제:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ASA의 라이선스가 즉시 해제되고 Evaluation(평가) 상태로 전환됩니다. 이 코드를 다시 확인해야 할 경우 이 명령을 다시 입력합니다. 새 영구 라이선스를 요청하는 경우(**license smart reservation request universal**), 이 코드를 다시 표시할 수 없습니다. 반환을 완료하려면 코드를 캡처하십시오.

단계 **2** Smart Software Manager에서 이 ASA 인스턴스를 찾을 수 있도록 ASA UDI(Universal Device Identifier)를 확인합니다.

show license udi

예제:

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

단계 **3** Smart Software Manager 인벤토리 화면으로 이동하여 **Product Instances(**제품 인스턴스**)** 탭을 클릭합니다.

https://software.cisco.com/#SmartLicensing-Inventory

Product Instances(제품 인스턴스**)** 탭은 UDI별로 모든 라이선스가 부여된 제품을 표시합니다.

단계 **4** 라이선스를 해제하려는 ASA를 찾고 **Actions(**작업**)** > **Remove(**제거**)**를 선택한 후 ASA 반환 코드를 상자에 입력합니다. **Remove Product Instance(**제품 인스턴스 제거**)**를 클릭합니다.

영구 라이선스가 사용 가능한 풀로 반환됩니다.

(선택 사항) Firepower 2100 등록 취소(일반 및 Satellite)

ASA를 등록 취소하면 어카운트에서 ASA가 제거됩니다. ASA의 모든 라이선스 엔타이틀먼트 및 인증서가 제거됩니다. 새 ASA의 라이선스를 확보하기 위해 등록을 취소하는 경우가 있습니다. 또는 Smart Software Manager에서 ASA를 제거할 수 있습니다.

프로시저

ASA를 등록 취소합니다.

license smart deregister

그러면 ASA가 다시 로드됩니다.

(선택 사항) Firepower 2100 ID 인증서 또는 라이선스 엔타이틀먼트 갱신(일반 및 Satellite)

기본적으로 ID 인증서는 6개월마다 자동으로 갱신되며, 라이선스 엔타이틀먼트는 30일마다 갱신됩니다. 예를 들어 인터넷 액세스 기간이 제한된 경우 또는 Smart Software Manager에서 라이선싱을 변경한 경우, 이러한 항목 중 하나에 대한 등록을 수동으로 갱신할 수 있습니다.

프로시저

단계 **1** ID 인증서를 갱신합니다.

license smart renew id

단계 **2** 라이센스 엔타이틀먼트를 갱신합니다.

license smart renew auth

Firepower 4100/9300 섀시: Smart Software Licensing 구성

이 절차는 License Authority를 사용하는 섀시, Satellite 서버 사용자 또는 영구 라이선스 예약에 적용됩니다. 사용자의 방법을 사전 요구 사항으로 구성하려면 FXOS 구성 가이드를 참조하십시오.

영구 라이선스 예약을 위해 라이선스에서는 최대 보안 상황 수를 지닌 Standard 계층 및 통신 사업자 라이선스 등 모든 기능을 활성화합니다. 그러나 ASA에서 이러한 기능을 "파악"하고 사용하도록 하려면 ASA에서 이러한 기능을 활성화해야 합니다.

참고 Smart Software Manager Satellite 2.3.0 이전 버전 사용자의 경우, 강력한 암호화(3DES/AES) 라이선스는 기본적으로 활성화되어 있지 않으므로 ASA CLI를 사용하여 강력한 암호화 라이선스를 요청할 때까지 ASDM을 사용하여 ASA를 구성할 수 없습니다. 기타 강력한 암호화 기능(VPN 포함)도 그렇게 할 때까지는 사용할 수 없습니다.

시작하기 전에

ASA 클러스터의 경우, 구성을 위해서는 기본 유닛에 액세스해야 합니다. 어느 유닛이 기본 유닛인지 보려면 Firepower Chassis Manager를 확인합니다. 이 절차에 나와 있는 대로 ASA CLI에서도 확인할 수 있습니다.

프로시저

단계 **1** Firepower 4100/9300 섀시 CLI(콘솔 또는 SSH)에 연결한 다음, 세션을 ASA에 연결합니다.

connect module 슬롯 **console connect asa**

예제**:**

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

다음에 ASA 콘솔에 연결할 때는 ASA로 바로 이동하므로 **connect asa**를 다시 입력할 필요가 없습니다.

ASA 클러스터의 경우, 라이선스 구성 및 기타 구성을 위해 마스터 유닛에만 액세스하면 됩니다. 일반적으로 마스터 유닛은 슬롯 1에 있으므로 해당 모듈에 먼저 연결해야 합니다.

단계 **2** ASA CLI에서 전역 구성 모드를 시작합니다. 기본적으로 enable 비밀번호는 비어을 처음 입력하면 비밀번호를 변경하라는 프롬프트가 표시됩니다.

enable configure terminal

예제**:**

```
asa> enable
Password:
asa# configure terminal
asa(config)#
```

단계 **3** 필요한 경우 ASA 클러스터에 대해 이 유닛이 기본 유닛인지 확인합니다.

show cluster info

예제:

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

다른 유닛이 기본 유닛인 경우, 연결을 종료하고 올바른 유닛에 연결합니다. 연결 종료에 대한 내용은 아래를 참조해 주십시오.

단계 **4** 라이센스 스마트 컨피그레이션 모드를 시작합니다.

license smart

예제:

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

단계 **5** 기능 계층을 설정합니다.

feature tier standard

표준 계층만 사용 가능합니다.. 다른 기능 라이센스를 추가하려면 기본적으로 계층 라이센스가 있어야 합니다.

단계 **6** 다음 기능 중 하나 이상을 요청합니다.

- 통신 사업자(GTP/GPRS, Diameter 및 SCTP 검사)

  feature carrier

- 보안 상황

  feature context <*1-248*>

  영구 라이선스 예약을 위해 최대 상황 수(248)를 지정할 수 있습니다.

- **Satellite** 서버 **2.3.0** 이전 버전 사용자만 해당**:** 강력한 암호화(3DES/AES)

  feature strong-encryption

예제**:**

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

단계 **7** ASA 콘솔을 종료하려면 프롬프트에서 ~을 입력하여 텔넷 애플리케이션을 종료합니다. **quit**을 입력하여 종료하고 수퍼바이저 CLI로 돌아갑니다.

모델당 라이센스

이 섹션에는 ASAv 및 Firepower 4100/9300 섀시 ASA 보안 모듈에 사용 가능한 라이선스 엔타이틀먼트가 나와 있습니다.

ASAv

다음 표에는 ASAv Series에 대한 라이선스 기능이 나와 있습니다.

라이센스	**Standard** 라이센스
방화벽 라이센스	
봇네트 트래픽 필터	활성화됨
방화벽 연결, 동시	ASAv5: 50,000개 ASAv10: 100,000개 ASAv30: 500,000개 ASAv50: 2,000,000개
캐리어	활성화됨

라이센스	**Standard** 라이센스	
총 TLS 프록시 세션	ASAv5: 500개 ASAv10: 500개 ASAv30: 1,000개 ASAv50: 10,000개	
VPN 라이선스		
AnyConnect 피어	비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스, 최댓값*:* *ASAv5: 50*개 *ASAv10: 250*개 *ASAv30: 750*개 *ASAv50: 10,000*개
기타 VPN 피어	ASAv5: 50개 ASAv10: 250개 ASAv30: 1,000개 ASAv50: 10,000개	
총 VPN 피어, 모든 유형 통합	ASAv5: 50 ASAv10: 250개 ASAv30: 1,000개 ASAv50: 10,000개	
일반 라이센스		
처리량 레벨	ASAv5: 100Mbps ASAv10: 1Gbps ASAv30: 2Gbps ASAv50: 10Gbps	
암호화	기본(DES) 또는 강력(3DES/AES), 어카운트의 내보내기 컴플라이언스 설정에 따라 다름	
장애 조치	활성/대기	
보안 상황	지원 안 함	
클러스터링	지원 안 함	

라이센스	**Standard** 라이센스
VLAN, 최대 개수	ASAv5: 25개 ASAv10: 50개 ASAv30: 200개 ASAv50: 1,024개
RAM, vCPU	ASAv5: 1GB, vCPU 1개 (선택 사항) ASAv5: 1.5GB, vCPU 1개(9.8(2) 이상). ASAv5에서 메모리가 소모되는 경우 더 많은 메모리를 할당할 수도 있습니다. ASAv10: 2GB, vCPU 1개 ASAv30: 8GB, vCPU 4개 ASAv50: 16GB, vCPU 8개

Firepower 2100 Series

다음 표에는 Firepower 2100 Series에 대한 라이선스 기능이 나와 있습니다.

라이센스	**Standard** 라이센스
방화벽 라이센스	
봇네트 트래픽 필터	지원 안 함.
방화벽 연결, 동시	Firepower 2110: 1,000,000개 Firepower 2120: 1,500,000개 Firepower 2130: 2,000,000개 Firepower 2140: 3,000,000개
캐리어	지원 안 함 SCTP 검사 맵이 지원되지 않는 경우에도 ACL을 사용하는 SCTP 스테이트풀 검사는 지원됩니다.
총 TLS 프록시 세션	Firepower 2110: 4,000개 Firepower 2120: 8,000개 Firepower 2130: 8,000개 Firepower 2140: 10,000개
VPN 라이선스	

라이센스	**Standard** 라이센스	
AnyConnect 피어	비활성화됨	*(선택 사항) AnyConnect Plus* 또는 *Apex* 라이선스, 최대값*:* *Firepower 2110: 1,500*개 *Firepower 2120: 3,500*개 *Firepower 2130: 7,500*개 *Firepower 2140: 10,000*개
기타 VPN 피어	Firepower 2110: 1,500개 Firepower 2120: 3,500개 Firepower 2130: 7,500개 Firepower 2140: 10,000개	
총 VPN 피어, 모든 유형 통합	Firepower 2110: 1,500개 Firepower 2120: 3,500개 Firepower 2130: 7,500개 Firepower 2140: 10,000개	
일반 라이센스		
암호화	기본(DES) 또는 강력(3DES/AES), 어카운트 내보내기 컴플라이언스 설정에 따라 다름	
보안 상황	2	*(선택 사항)* 라이선스, 최댓값*(5* 또는 *10*씩 증가*):* *Firepower 2110: 25*개 *Firepower 2120: 25*개 *Firepower 2130: 30*개 *Firepower 2140: 40*개
클러스터링	지원 안 함	
VLAN, 최대 개수	1024	

Firepower 4100 Series ASA 애플리케이션

다음 표에는 Firepower 4100 Series ASA 애플리케이션에 대한 라이선스 기능이 나와 있습니다.

라이센스	**Standard** 라이센스	
방화벽 라이센스		
봇네트 트래픽 필터	지원 안 함.	
방화벽 연결, 동시	Firepower 4110: 10,000,000개 Firepower 4120: 15,000,000개 Firepower 4140: 25,000,000개 Firepower 4150: 35,000,000개	
캐리어	비활성화됨	*(*선택 사항*)* 라이선스*:* 통신 사업자
총 TLS 프록시 세션	10,000	
VPN 라이선스		
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *10,000*개
기타 VPN 피어	10,000	
총 VPN 피어, 모든 유형 통합	10,000	
일반 라이센스		
암호화	기본(DES) 또는 강력(3DES/AES), 어카운트 내보내기 컴플라이언스 설정에 따라 다름	
보안 상황	10	*(*선택 사항*)* 라이선스*:* 최댓값 - *250*개*, 10*씩 증가
클러스터링	활성화됨	
VLAN, 최대 개수	1024	

Firepower 9300 ASA 애플리케이션

다음 표에는 Firepower 9300 ASA 애플리케이션에 대한 라이선스 기능이 나와 있습니다.

라이센스	**Standard** 라이센스
방화벽 라이센스	
봇네트 트래픽 필터	지원 안 함.

라이센스	**Standard** 라이센스	
방화벽 연결, 동시	Firepower 9300 SM-44: 60,000,000개, 3개의 모듈을 포함하는 섀시의 경우 최대 70,000,000개 Firepower 9300 SM-36: 60,000,000개, 3개의 모듈을 포함하는 섀시의 경우 최대 70,000,000개 Firepower 9300 SM-24: 55,000,000개, 3개의 모듈을 포함하는 섀시의 경우 최대 70,000,000개	
캐리어	비활성화됨	*(*선택 사항*)* 라이선스*:* 통신 사업자
총 TLS 프록시 세션	15,000	
VPN 라이선스		
AnyConnect 피어	비활성화됨	*(*선택 사항*) AnyConnect Plus* 또는 *Apex* 라이선스*:* 최대 *20,000*개
기타 VPN 피어	20,000	
총 VPN 피어, 모든 유형 통합	20,000	
일반 라이센스		
암호화	기본(DES) 또는 강력(3DES/AES), 어카운트의 내보내기 컴플라이언스 설정에 따라 다름	
보안 상황	10	선택적 라이선스*:* 최대값 *- 250*개*, 10*씩 증가
클러스터링	활성화됨	
VLAN, 최대 개수	1024	

Smart Software Licensing 모니터링

라이센스 기능, 상태, 인증서를 모니터링하고 디버그 메시지를 활성화할 수 있습니다.

현재 라이센스 보기

라이선스를 보려면 다음 명령을 참조하십시오.

- **show license features**

  다음 예에는 기본 라이선스만 있는 ASAv가 나와 있습니다(현재 라이선스 엔타이틀먼트 없음).

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

스마트 라이센스 상태 보기

라이선스 상태를 보려면 다음 명령을 참고하십시오.

- **show license all**

  Smart Software Licensing의 상태, Smart Agent 버전, UDI 정보, Smart Agent 상태, 전역 컴플라이언스 상태, 엔타이틀먼트 상태, 라이선싱 인증서 정보 및 예약된 Smart Agent 작업이 표시됩니다.

  다음 예에는 ASAv 라이선스가 나와 있습니다.

```
ciscoasa# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
```

```
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
====================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=============
Smart Agent for Licensing: 1.6_reservation/36
```

- 라이선스 상태 보기

  스마트 라이선스 상태가 표시됩니다.

  다음 예에는 일반 Smart Software Licensing을 사용하는 ASAv의 상태가 나와 있습니다.

```
ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

  다음 예에는 영구 라이선스 예약을 사용하는 ASAv의 상태가 나와 있습니다.

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC
```

```
Licensing HA configuration error:
    No Reservation Ha config error
```

- **show license summary**

  스마트 라이선스 상태 및 사용량의 요약이 표시됩니다.

  다음 예에는 일반 Smart Software Licensing을 사용하는 ASAv에 대한 요약이 나와 있습니다.

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (ASAv-STD-1G)                     1 AUTHORIZED
```

  다음 예에는 영구 라이선스 예약을 사용하는 ASAv에 대한 요약이 나와 있습니다.

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  스마트 라이선스 사용량이 표시됩니다.

  다음 예에는 ASAv의 사용량이 나와 있습니다.

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
```

```
Version: 1.0
Status: AUTHORIZED
```

UDI 보기

UDI(Universal Product Identifier)를 보려면 다음 명령을 참조하십시오.

show license udi

다음 예에는 ASAv의 UDI가 나와 있습니다.

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

스마트 소프트웨어 라이센싱 디버깅

클러스터링 디버깅에 대해서는 다음 명령을 참조하십시오.

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  스마트 에이전트에서 디버깅을 켭니다.

- **debug license** *level*

  Smart Software Licensing Manager의 여러 디버깅 레벨을 켭니다.

Smart Software Licensing 기록

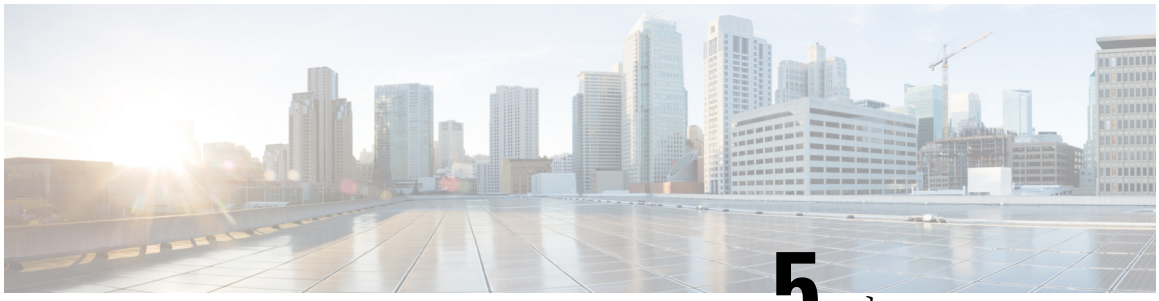
기능 이름	플랫폼 릴리스	설명
ASA 장애 조치 쌍에 대한 라이선싱 변경 사항. Firepower 4100/9300 섀시	9.7(1)	액티브 유닛만 라이선스 엔타이틀먼트를 요청합니다. 이전에는 두 유닛 모두 라이선스 엔타이틀먼트를 요청했습니다. FXOS 2.1.1에서 지원됩니다.
ASAv 짧은 문자열에 대한 영구 라이선스 예약 개선 사항	9.6(2)	Smart Agent(1.6.4 버전까지)의 업데이트 덕분에 이제 요청 및 인증 코드에서 짧은 문자열을 사용합니다. 명령은 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	설명
ASAv에 대한 Satellite 서버 지원	9.6(2)	보안상의 이유로 디바이스가 인터넷에 액세스할 수 없는 경우 선택적으로 로컬 Smart Software Manager Satellite 서버를 VM(가상 머신)으로 설치할 수 있습니다. 명령은 수정하지 않았습니다.
ASAv의 영구 라이선스 예약 Firepower 4100/9300 섀시	9.6(2)	Cisco Smart Software Manager와의 통신이 허용되지 않은 매우 안전한 환경의 경우, Firepower 9300 및 Firepower 4100에서 ASAv에 대한 영구 라이선스를 요청할 수 있습니다. 모든 사용 가능한 라이선스 엔타이틀먼트는 표준 계층, 강력한 암호화(자격이 있는 경우), 보안 상황 및 통신 사업자 라이선스를 포함하는 영구 라이선스에 포함되어 있습니다. FXOS 2.0.1이 필요합니다. 모든 구성은 Firepower 4100/9300 섀시에서 수행됩니다. ASA에서 구성할 필요가 없습니다.
ASAv의 영구 라이선스 예약	9.5(2.200) 9.6(2)	Cisco Smart Software Manager와의 통신이 허용되지 않은 매우 안전한 환경의 경우, ASAv에 대한 영구 라이선스를 요청할 수 있습니다. 9.6(2)에서는 Amazon Web Services의 이 ASAv 기능에 대한 지원을 추가했습니다. 이 기능은 Microsoft Azure에서 지원되지 않습니다. 다음 명령을 도입했습니다. **license smart reservation, license smartreservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return**

기능 이름	플랫폼 릴리스	설명
Smart Agent의 버전 1.6으로의 업그레이드	9.5(2.200) 9.6(2)	Smart Agent가 버전 1.1에서 버전 1.6으로 업그레이드되었습니다. 이 업그레이드는 영구 라이선스 예약을 지원하고 라이선스 어카운트에 설정된 권한에 따라 강력한 암호화(3DES/AES) 라이선스 엔타이틀먼트 설정도 지원합니다. 참고 버전 9.5(2.200)에서 다운그레이드하는 경우, ASAv는 라이선싱 등록 상태를 유지하지 않습니다. **license smart register idtoken** *id_token* **force** 명령을 사용하여 다시 등록하고 Smart Software Manager에서 ID 토큰을 얻어야 합니다. 도입된 명령: **show license status, show license summary, show license udi, show license usage** 다음 명령을 수정했습니다. **show license all, show tech-support license** 다음 명령의 사용을 중단했습니다. **show license cert, show license entitlement, show license pool, show license registration**
Firepower 9300에서 ASA에 대해 자동으로 적용되는 강력한 암호화(3DES) 라이선스	9.5(2.1)	일반 Cisco Smart Software Manager 사용자의 경우 Firepower 9300에서 등록 토큰을 적용할 때 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화됩니다. 참고 Smart Software Manager Satellite 구축을 사용하는 경우, ASDM 및 기타 강력한 암호화 기능을 사용하려면 ASA를 구축한 후에 ASA CLI를 사용하여 강력한 암호화(3DES) 라이선스를 활성화해야 합니다. 이 기능에는 FXOS 1.1.3이 필요합니다. 비 satellite 구성의 다음 명령을 제거했습니다. **feature strong-encryption**

기능 이름	플랫폼 릴리스	설명
서버 인증서의 발급 계층 변경 시 Smart Call Home/스마트 라이선싱 인증서의 검증	9.5(2)	스마트 라이선싱은 Smart Call Home 인프라를 사용합니다. ASA가 백그라운드에서 Smart Call Home 익명 보고를 제일 먼저 구성할 경우, ASA는 Smart Call Home 서버 인증서를 발급한 CA의 인증서를 포함하는 트러스트 포인트를 자동으로 생성합니다. ASA는 이제 서버 인증서의 발급 계층이 변경되는 경우 인증서 검증을 지원합니다. 트러스트 풀 번들의 자동 업데이트를 주기적인 간격으로 활성화할 수 있습니다. 다음 명령을 도입했습니다. **auto-import**
새 통신 사업자 라이선스	9.5(2)	새 통신 사업자 라이선스는 기존의 GTP/GPRS 라이선스를 대체하고 SCTP 및 Diameter 검사에 대한 지원도 포함합니다. Firepower 9300의 ASA에서 **feature mobile-sp** 명령은 **feature carrier** 명령으로 자동으로 마이그레이션됩니다. 다음 명령을 도입하거나 수정했습니다. **feature carrier, show activation-key, show license, show tech-support, show version**
Firepower 9300의 ASA를 위한 Cisco Smart Software Licensing	9.4(1.150)	Firepower 9300의 ASA를 위한 Smart Software Licensing을 도입했습니다. 다음 명령을 도입했습니다. **feature strong-encryption, feature mobile-sp, feature context**

기능 이름	플랫폼 릴리스	설명
ASAv의 Cisco Smart Software Licensing	9.3(2)	스마트 소프트웨어 라이센싱에서는 라이센스 풀을 구매하여 관리할 수 있습니다. 스마트 라이센스는 PAK 라이센스와 달리 특정 일련 번호에 묶여 있지 않습니다. 각 유닛의 라이선스 키를 관리할 필요 없이 손쉽게 ASAv를 구축하거나 사용 중단할 수 있습니다. 또한 스마트 소프트웨어 라이선싱에서는 라이선스 사용량 및 필요량을 한눈에 볼 수 있습니다. 다음 명령을 도입했습니다. **clear configure license, debug license agent, feature tier, http-proxy, license smart, license smart deregister, license smart register, license smart renew, show license, show running-config license, throughput level**



5 장

논리적 디바이스 - Firepower 4100/9300

Firepower 4100/9300은 하나 이상의 논리적 디바이스를 설치할 수 있는 유연한 보안 플랫폼입니다. 이 장에서는 기본 인터페이스 구성 및 Firepower Chassis Manager를 사용하여 독립형 디바이스 또는 고가용성 논리적 디바이스를 추가하는 방법을 설명합니다. 클러스터형 논리적 디바이스를 추가하려면 ASA 클러스터 - Firepower 4100/9300 섀시, 469 페이지의 내용을 참조하십시오. FXOS CLI를 사용하려면 FXOS CLI 구성 가이드를 참조하십시오. 고급 FXOS 절차 및 트러블슈팅에 대한 자세한 내용은 FXOS 구성 가이드를 참조하십시오.

Firepower 인터페이스 정보

Firepower 4100/9300 섀시에서는 물리적 인터페이스 및 EtherChannel(포트-채널) 인터페이스를 지원합니다. EtherChannel 인터페이스는 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다.

섀시 관리 인터페이스

섀시 관리 인터페이스는 SSH 또는 Firepower Chassis Manager를 통한 FXOS 섀시 관리에 사용됩니다. 이 인터페이스는 애플리케이션 관리용 논리적 디바이스에 할당하는 관리 유형 인터페이스와는 별개입니다.

이 인터페이스의 파라미터는 CLI에서 구성해야 합니다. FXOS CLI에서 이 인터페이스에 대한 정보를 확인하려면 로컬 관리에 연결한 다음 관리 포트를 표시합니다.

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

실제 케이블이나 SFP 모듈 연결을 해제하거나 **mgmt-port shut** 명령을 수행하더라도 섀시 관리 인터페이스는 계속 작동합니다.

인터페이스 유형

각 인터페이스는 다음 유형 중 하나일 수 있습니다.

- 데이터 — 데이터 인터페이스는 논리적 디바이스 간에 공유할 수 없습니다.
- Data-sharing(데이터 공유) - 컨테이너 인스턴스에서만 지원되는 이러한 데이터 인터페이스는 하나 이상의 논리적 디바이스/컨테이너 인스턴스(FTD 전용)에서 공유할 수 있습니다. 각 컨테이너 인스턴스는 이 인터페이스를 공유하는 다른 모든 인스턴스와 백플레인을 통해 통신할 수 있습니다. 공유 인터페이스는 구축할 수 있는 컨테이너 인스턴스 수에 영향을 줄 수 있습니다 섹션을 참조하십시오. 브리지 그룹 멤버 인터페이스(투명 모드 또는 라우티드 모드), 인라인 집합, 패시브 인터페이스 또는 페일오버 링크에 대해서는 공유 인터페이스가 지원되지 않습니다.
- Mgmt(관리) - 관리 인터페이스를 사용하여 애플리케이션 인스턴스를 관리합니다. 하나 이상의 논리적 디바이스가 외부 호스트에 액세스하기 위해 이러한 인터페이스를 공유할 수 있습니다. 논리적 디바이스가 인터페이스를 공유하는 다른 논리적 디바이스와 이 인터페이스를 통해 통신할 수는 없습니다. 논리적 디바이스당 관리 인터페이스 1개만 할당할 수 있습니다. 개별 섀시 관리 인터페이스에 대한 내용은 섀시 관리 인터페이스, 167 페이지 섹션을 참조하십시오.
- Firepower-eventing(Firepower 이벤트) - 이 인터페이스는 FTD 디바이스의 보조 관리 인터페이스입니다. 이 인터페이스를 사용하려면 FTD CLI에서 해당 IP 주소 및 기타 매개변수를 구성해야 합니다. 예를 들면 관리 트래픽을 이벤트(예: 웹 이벤트)에서 분리할 수 있습니다. Firepower Management Center 구성 가이드 시스템 구성 장의 "관리 인터페이스" 섹션을 참조하십시오. 하나 이상의 논리적 디바이스가 외부 호스트에 액세스하기 위해 Firepower 이벤트 인터페이스를 공유할 수 있습니다. 논리적 디바이스가 인터페이스를 공유하는 다른 논리적 디바이스와 이 인터페이스를 통해 통신할 수는 없습니다.
- Cluster(클러스터) - 클러스터된 논리적 디바이스에 사용되는 특수 인터페이스 유형입니다. 이 유형은 유닛 클러스터 간 통신을 지원하는 클러스터 제어 링크에 자동으로 할당됩니다. 기본적으로, 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다.

섀시와 애플리케이션의 독립 인터페이스 상태

관리를 위해 섀시와 애플리케이션에서 인터페이스를 활성화하고 비활성화할 수 있습니다. 인터페이스는 두 운영 체제에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로 섀시와 애플리케이션에서 상태가 일치하지 않을 수도 있습니다.

논리적 디바이스 정보

논리적 디바이스를 사용하면 애플리케이션 인스턴스 하나(ASA 또는 Firepower Threat Defense)와 선택적 데코레이터 애플리케이션(Radware DefensePro)을 실행하여 서비스 체인을 만들 수 있습니다 .

논리적 디바이스를 추가할 때는 애플리케이션 인스턴스 유형 및 버전 정의, 인터페이스 할당, 애플리케이션 구성으로 푸시되는 부트스트랩 설정 작업도 수행합니다.

참고 Firepower 9300의 경우에는 섀시 내의 모든 모듈에 동일한 애플리케이션 인스턴스 유형(ASA 또는 FTD)을 설치해야 합니다. 다른 유형은 현재 지원되지 않습니다. 모듈은 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수 있습니다.

독립형 논리적 디바이스와 클러스터형 논리적 디바이스

다음의 논리적 디바이스 유형을 추가할 수 있습니다.

- 독립형 - 독립형 유닛으로 또는 고가용성 쌍의 유닛으로 작동하는 독립형 논리적 디바이스입니다.
- 클러스터 - 클러스터형 논리적 디바이스에서는 여러 유닛을 함께 그룹화할 수 있으므로 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. Firepower 9300과 같은 다중 모듈 디바이스는 인트라 섀시 클러스터링(intra-chassis clustering)을 지원합니다. Firepower 9300에서는 3개의 모듈 애플리케이션 인스턴스가 모두 단일 논리적 디바이스에 속합니다.

  참고 Firepower 9300에서는 모든 모듈이 클러스터에 속해야 합니다. 한 보안 모듈에서 독립형 논리적 디바이스를 생성한 다음에 나머지 2개의 보안 모듈을 사용하는 클러스터를 생성할 수는 없습니다.

논리적 디바이스 관련 지침 및 제한 사항

지침 및 제한 사항은 다음 섹션을 참조하십시오.

Firepower 인터페이스에 대한 지침 및 제한 사항

인라인 집합 **FTD**

기본 **MAC** 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- EtherChannel - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터

페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.

일반 지침 및 제한 사항

방화벽 모드

FTD 및 ASA의 부트스트랩 구성에서 방화벽 모드를 라우팅 또는 투명으로 설정할 수 있습니다.

고가용성

- 애플리케이션 구성 내에서 고가용성을 구성합니다.
- 모든 데이터 인터페이스를 페일오버 및 상태 링크로 사용할 수 있습니다.
- 자세한 내용은 장애 조치 시스템 요구 사항, 268 페이지을 참조하십시오.

컨텍스트 모드

- 다중 상황 모드는 ASA에서만 지원됩니다.
- 구축 후에 ASA에서 다중 컨텍스트 모드를 활성화합니다.

인터페이스 구성

기본적으로 물리적 인터페이스는 비활성화되어 있습니다. 인터페이스 활성화, EtherChannels 추가, 인터페이스 속성 수정 구성 작업을 수행할 수 있습니다.

참고 네트워크 모듈/EtherChannel을 제거하거나 EtherChannel에 인터페이스를 재할당하는 등 FXOS에서 인터페이스를 제거하면 ASA 구성에서 원래 명령이 유지되므로 필요한 조정을 수행할 수 있습니다. 구성에서 인터페이스를 제거하면 그 영향이 광범위하게 미칠 수 있습니다. ASA OS에서 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.

실제 인터페이스 구성

인터페이스를 물리적으로 활성화 및 비활성화할 뿐만 아니라 인터페이스 속도 및 듀플렉스를 설정할 수 있습니다. 인터페이스를 사용하려면 FXOS에서 인터페이스를 물리적으로 활성화하고 애플리케이션에서 논리적으로 활성화해야 합니다.

시작하기 전에

- 이미 EtherChannel의 멤버인 인터페이스는 개별적으로 수정할 수 없습니다. EtherChannel에 인터페이스를 추가하기 전에 설정을 구성하십시오.

프로시저

단계 **1** 인터페이스 모드를 시작합니다.

scope eth-uplink

scope fabric a

단계 **2** 인터페이스를 활성화합니다.

enter interface *interface_id*

enable

예제:

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

참고 이미 포트 채널의 멤버인 인터페이스는 개별적으로 수정할 수 없습니다. 포트 채널의 멤버인 인터페이스에서 **enter interface** 또는 **scope interface** 명령을 사용하는 경우 개체가 없음을 알리는 오류가 표시됩니다. 포트 채널에 인터페이스를 추가하기 전에 **enter interface** 명령을 사용하여 인터페이스를 수정해야 합니다.

단계 **3** (선택 사항) 인터페이스 유형을 설정합니다.

set port-type {**data** | **mgmt** | **cluster**}

예제:

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data 키워드는 기본 유형입니다. **cluster** 키워드는 선택하지 마십시오. 기본적으로 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다.

단계 **4** 자동 협상이 인터페이스에 대해 지원되는 경우 이를 활성화하거나 비활성화합니다.

set auto-negotiation {**on** | **off**}

예제:

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

단계 **5** 인터페이스 속도를 설정합니다.

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

예제:

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

단계 **6** 인터페이스 듀플렉스 모드를 설정합니다.

set admin-duplex {**fullduplex** | **halfduplex**}

예제:

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

단계 **7** 기본 플로우 제어 정책을 수정한 경우 인터페이스에 정책이 이미 적용되어 있습니다. 새 정책을 생성한 경우에는 인터페이스에 정책을 적용합니다.

set flow-control-policy *name*

예제:

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

단계 **8** 구성을 저장합니다.

commit-buffer

예제:

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

EtherChannel(포트 채널) 추가

EtherChannel(포트 채널)은 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다. LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 데이터 인터페이스를 다음과 같이 구성할 수 있습니다.

- 액티브 — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- 켜짐 — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

비 데이터 인터페이스는 액티브 모드만 지원합니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 구성이 확인되지 않습니다.

Firepower 4100/9300 섀시에서 EtherChannel을 만들면, 물리적 링크가 가동 중이더라도 EtherChannel은 물리적 디바이스에 할당될 때까지 **Suspended(**일시 중단**)** 상태로 유지됩니다. 다음의 상황에서는 EtherChannel의 **Suspended(**일시 중단**)** 상태가 해제됩니다.

- EtherChannel이 독립형 논리적 디바이스에 대한 데이터 인터페이스 또는 관리 인터페이스로 추가됩니다.
- EtherChannel이 클러스터의 일부인 논리적 디바이스에 대한 관리 인터페이스 또는 클러스터 제어 링크로 추가됩니다.
- EtherChannel이 클러스터의 일부이며 유닛 하나 이상이 클러스터에 조인된 논리적 디바이스에 대한 데이터 인터페이스로 추가됩니다.

EtherChannel은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. EtherChannel을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, EtherChannel은 **Suspended** 상태로 전환됩니다.

프로시저

단계 **1** 인터페이스 모드를 입력합니다.

scope eth-uplink

scope fabric a

단계 **2** 포트 채널을 생성합니다.

create port-channel *id*

enable

단계 **3** 멤버 인터페이스를 할당합니다.

create member-port *interface_id*

예제**:**

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

단계 **4** (선택 사항) 인터페이스 유형을 설정합니다.

set port-type {**data** | **mgmt** | **cluster**}

예제**:**

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data 키워드는 기본 유형입니다. 이 포트 채널을 기본값 대신 클러스터 제어 링크로 사용하려는 경우가 아니라면 **cluster** 키워드를 선택하지 마십시오.

단계 **5** (선택 사항) 포트 채널의 모든 멤버에 대해 인터페이스 속도를 설정합니다.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

예제:

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

단계 **6** (선택 사항) 포트 채널의 모든 멤버에 대해 듀플렉스를 설정합니다.

set duplex {**fullduplex** | **halfduplex**}

예제:

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

단계 **7** 자동 협상이 인터페이스에 대해 지원되는 경우 이를 활성화하거나 비활성화합니다.

set auto-negotiation {**on** | **off**}

예제:

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

단계 **8** 데이터 인터페이스에 대해 LACP 포트 채널 모드를 설정합니다.

비 데이터 인터페이스의 경우 모드는 항상 액티브입니다.

set port-channel-mode {**active** | **on**}

예제:

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

단계 **9** 기본 플로우 제어 정책을 수정한 경우 인터페이스에 정책이 이미 적용되어 있습니다. 새 정책을 생성한 경우에는 인터페이스에 정책을 적용합니다.

set flow-control-policy *name*

예제:

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

단계 **10** 구성을 커밋합니다.

commit-buffer

논리적 디바이스 구성

Firepower 4100/9300 섀시에서 독립형 논리적 디바이스 또는 고가용성 쌍을 추가합니다.

클러스터링에 대해서는 ASA 클러스터 - Firepower 4100/9300 섀시, 469 페이지의 내용을 참조하십시오.

독립형 ASA 추가

독립형 논리적 디바이스는 단독으로 작동하거나 고가용성 쌍으로 작동합니다. Firepower 9300과 같이 모듈이 여러 개인 디바이스에서는 클러스터 또는 독립형 디바이스를 구축할 수 있습니다. 클러스터는 모든 모듈을 사용해야 하므로 모듈이 2개인 클러스터와 단일 독립형 디바이스를 혼용하는 방식은 사용할 수 없습니다.

Firepower 4100/9300 섀시에서 라우팅된 방화벽 모드 또는 투명 방화벽 모드 ASA를 구축할 수 있습니다.

다중 컨텍스트 모드의 경우 먼저 논리적 디바이스를 구축한 다음 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화해야 합니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음 해당 이미지를 Firepower 4100/9300 섀시에 다운로드합니다.

  참고 Firepower 9300의 경우에는 섀시 내의 모든 모듈에 동일한 애플리케이션 인스턴스 유형(ASA 또는 FTD)을 설치해야 합니다. 다른 유형은 현재 지원되지 않습니다. 모듈은 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수 있습니다.

- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 인터페이스(FXOS에서 MGMT, management0 또는 기타 유사한 이름으로 표시될 수 있으며와는 다릅니다.

프로시저

단계 **1** Security Services(보안 서비스) 모드를 설정합니다.

scope ssa

예제**:**

```
Firepower# scope ssa
Firepower /ssa #
```

단계 **2** 애플리케이션 인스턴스 이미지 버전을 설정합니다.

a) 사용 가능한 이미지를 확인합니다. 사용하려는 버전 번호를 적어 둡니다.

show app

예제:

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) 보안 모듈/엔진 슬롯에 범위를 설정합니다.

scope slot *slot_id*

*slot_id*는 Firepower 4100의 경우 항상 1이고 Firepower 9300의 경우 1, 2 또는 3입니다.

예제:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) 애플리케이션 인스턴스를 생성합니다.

enter app-instance asa *device_name*

*device_name*은 1~64자로 입력할 수 있습니다. 이 인스턴스에 대해 논리적 디바이스를 생성할 때 이 디바이스 이름을 사용합니다.

예제:

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) ASA 이미지 버전을 설정합니다.

set startup-version *version*

예제:

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) 슬롯 모드를 종료합니다.

exit

예제:

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) SSA 모드를 종료합니다.

exit

예제:

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

예제:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

단계 **3** 논리적 디바이스를 생성합니다.

enter logical-device *device_name* **asa** *slot_id* **standalone**

앞에서 추가한 애플리케이션 인스턴스와 같은 *device_name*을 사용합니다.

예제:

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

단계 **4** 논리적 디바이스에 관리 및 데이터 인터페이스를 할당합니다. 각 인터페이스에 대해 이 작업을 반복합니다.

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name(*이름*)* - ASA 구성에서 사용되는 인터페이스 이름이 아닌 Firepower 4100/9300 섀시 수퍼바이저가 사용하는 이름입니다.
- *description(*설명*)* - 공백이 있는 구는 따옴표(")로 묶습니다.

예제:

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

단계 **5** 관리 부트스트랩 정보를 구성합니다.

a) 부트스트랩 개체를 생성합니다.

create mgmt-bootstrap asa

예제:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 방화벽 모드(라우팅 또는 투명)를 지정합니다.

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 관리자 및 비밀번호 활성화를 지정합니다.

create bootstrap-key-secret PASSWORD

set value

password 값을 입력합니다.

password 값을 확인합니다.

exit

예제:

비밀번호를 복구할 때는 사전 구성된 ASA 관리자 및 비밀번호 활성화를 사용하면 유용합니다. FXOS 액세스 권한이 있다면 관리자 비밀번호를 잊어버린 경우 재설정할 수 있습니다.

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) IPv4 관리 인터페이스 설정을 구성합니다.

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

setgateway *gateway_address*

exit

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) IPv6 관리 인터페이스 설정을 구성합니다.

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 관리 부트스트랩 모드를 종료합니다.

exit

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

단계 **6** 구성을 저장합니다.

commit-buffer

예제:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device #
```

예

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
```

```
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

고가용성 쌍 추가

ASA 고가용성(페일오버라고도 함)은 FXOS가 아닌 애플리케이션 내에 구성됩니다. 그러나 고가용성을 사용할 수 있도록 섀시를 준비하려는 경우 다음 단계를 참조하십시오.

시작하기 전에

- 고가용성을 위한 시스템 요구 사항은 장애 조치 시스템 요구 사항, 268 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 각 논리적 디바이스는 별도의 섀시에 있어야 합니다. Firepower 9300의 경우 섀시 내 고가용성은 지원되지 않을 수 있으며 사용하지 않는 것이 좋습니다.

단계 **2** 각 논리적 디바이스에 동일한 인터페이스를 할당합니다.

단계 **3** 페일오버 및 상태 링크용으로 데이터 인터페이스 1~2개를 할당합니다.

이러한 인터페이스는 두 섀시 간의 고가용성 트래픽을 교환합니다. 페일오버 및 상태 링크를 함께 사용하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다. 사용 가능한 인터페이스가 있다면 페일오버 및 상태 링크를 각각 별도로 사용할 수 있습니다. 상태 링크에는 최대 대역폭이 필요합니다. 관리 유형 인터페이스는 페일오버 또는 상태 링크용으로 사용할 수 없습니다. 페일오버 인터페이스와 같은 네트워크 세그먼트에 다른 디바이스가 없는 상태로 섀시 간에 스위치를 사용하는 것이 좋습니다.

단계 **4** 논리적 디바이스에서 고가용성을 활성화합니다. 고가용성을 위한 장애 조치, 267 페이지 섹션을 참조하십시오.

단계 5 고가용성을 활성화한 후에 인터페이스를 변경해야 하는 경우에는 먼저 스탠바이 유닛에서 변경을 수행한 다음 액티브 유닛에서 변경을 수행합니다.

참고 ASA의 경우 네트워크 모듈/EtherChannel을 제거하거나 EtherChannel에 인터페이스를 재할당하는 등 FXOS에서 인터페이스를 제거하면 ASA 구성에서 원래 명령이 유지되므로 필요한 조정을 수행할 수 있습니다. 구성에서 인터페이스를 제거하는 경우에는 구성 전반에 걸쳐 영향을 줄 수 있습니다. ASA OS에서 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.

ASA 논리적 디바이스에서 인터페이스 변경

ASA 논리적 디바이스에서 관리 인터페이스를 할당, 할당 해제 또는 교체할 수 있습니다. ASDM은 새 인터페이스를 자동으로 검색합니다.

시작하기 전에

- 실제 인터페이스 구성, 170 페이지 및 EtherChannel(포트 채널) 추가, 172 페이지에 따라 인터페이스를 구성하고 EtherChannel을 추가합니다.
- 논리적 디바이스에 영향을 주지 않고 할당된 EtherChannel의 멤버십을 수정할 수 있습니다.
- 모든 인터페이스가 기본적으로 클러스터에 할당된 경우와 같이 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우에는 먼저 논리적 디바이스에서 인터페이스 할당을 해제한 다음 EtherChannel에 인터페이스를 추가해야 합니다. 새 EtherChannel의 경우 이렇게 한 후에 디바이스에 EtherChannel을 할당할 수 있습니다.
- 네트워크 모듈/EtherChannel을 제거하거나 EtherChannel에 할당된 인터페이스를 재할당하는 등 FXOS에서 인터페이스를 제거하면 ASA 구성에서 원래 명령이 유지되므로 필요한 조정을 수행할 수 있습니다. 구성에서 인터페이스를 제거하는 경우에는 구성 전반에 걸쳐 영향을 줄 수 있습니다. ASA OS에서 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.
- 클러스터링 또는 페일오버의 경우 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 먼저 슬레이브/스탠바이 유닛에서 인터페이스를 변경한 후에 마스터/액티브 유닛에서 변경하는 것이 좋습니다. 새 인터페이스는 관리를 위해 다운된 상태로 추가되므로 인터페이스 모니터링에는 영향을 주지 않습니다.

프로시저

단계 1 보안 서비스 모드를 입력합니다.

Firepower# **scope ssa**

단계 2 논리적 디바이스를 편집합니다.

Firepower /ssa # **scope logical-device** *device_name*

단계 **3** 논리적 디바이스에서 인터페이스를 할당 해제합니다.

Firepower /ssa/logical-device # **delete external-port-link** *name*

show external-port-link 명령을 입력하여 인터페이스 이름을 확인합니다.

관리 인터페이스의 경우 새 관리 인터페이스를 추가하기 전에 현재 인터페이스를 삭제한 다음 **commit-buffer** 명령을 사용하여 변경 사항을 커밋합니다.

단계 **4** 논리적 디바이스에 새 인터페이스를 할당합니다.

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

단계 **5** 구성을 커밋합니다.

commit-buffer

시스템 구성에 트랜잭션을 커밋합니다.

애플리케이션 콘솔에 연결

다음 절차를 수행하여 애플리케이션의 콘솔에 연결합니다.

프로시저

단계 **1** 콘솔 연결 또는 텔넷 연결을 사용하여 모듈 CLI에 연결합니다.

connect module *slot_number* {**console** | **telnet**}

여러 보안 모듈을 지원하지 않는 디바이스의 보안 엔진에 연결하려면 항상 **1**을 *slot_number*로 사용합니다.

텔넷 연결 사용 시에는 동시에 여러 세션을 모듈에 연결할 수 있으며 연결 속도가 더 빠르다는 이점이 있습니다.

예제**:**

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

단계 **2** 애플리케이션 콘솔에 연결합니다.

connect asa

예제**:**

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

단계 **3** 애플리케이션 콘솔을 FXOS 모듈 CLI로 종료합니다.

- ASA - **Ctrl-a, d**를 입력합니다.

문제 해결을 위해 FXOS 모듈 CLI를 사용할 수 있습니다.

단계 **4** FXOS CLI의 Supervisor(관리자) 수준으로 돌아갑니다.

콘솔을 종료합니다**.**

a) ~를 입력합니다.

텔넷 애플리케이션을 종료합니다.

b) 텔넷 애플리케이션을 종료하려면 다음을 입력합니다.

telnet>**quit**

텔넷 세션을 종료합니다**.**

a) **Ctrl-], .**를 입력합니다.

예시

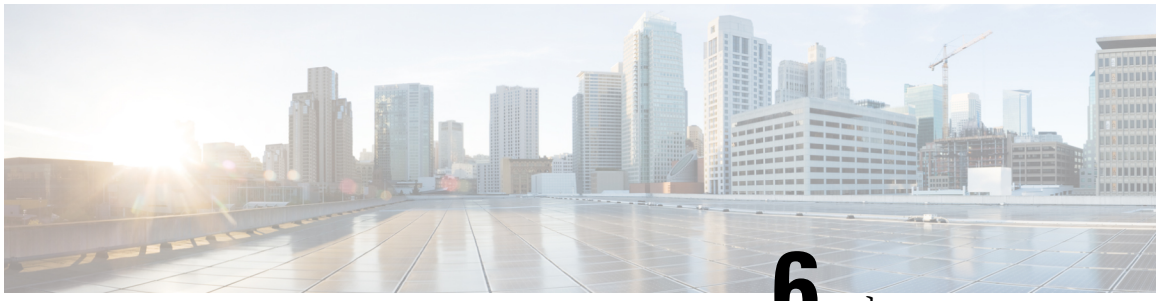
다음 예시에서는 보안 모듈 1에 있는 ASA에 연결한 다음 FXOS CLI의 수퍼바이저 레벨로 다시 종료합니다.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

논리적 디바이스의 기록

기능	버전	세부 사항
Firepower 4100/9300에 대한 클러스터 제어 링크의 맞춤화 가능한 IP 주소	9.10.1	기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 이제 FXOS에서 클러스터를 구축하는 경우 네트워크를 설정할 수 있습니다. 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 따라서 이제 FXOS에서 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외하고 클러스터 제어 링크의 맞춤형 /16 서브넷을 설정할 수 있습니다. 신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리적 디바이스**)** > **Add Device(**디바이스 추가**)** > **Cluster Information(**클러스터 정보**)** > **CCL Subnet IP(CCL** 서브넷 **IP)** 필드 신규/수정된 FXOS 명령: **set cluster-control-link network**
On(켜기) 모드에서 데이터 EtherChannel 지원	9.10.1	이제 데이터 및 데이터 공유 EtherChannel을 Active LACP(액티브 LACP) 모드 또는 On(켜기) 모드로 설정할 수 있습니다. 다른 유형의 Etherchannel은 Active(액티브) 모드만 지원합니다. 신규/수정된 명령: **set port-channel-mode**

기능	버전	세부 사항
Firepower 4100/9300 섀시에서 ASA에 대한 사이트 간 클러스터링 개선	9.7(1)	이제 ASA 클러스터를 구축할 때 각 Firepower 4100/9300 섀시에 대한 사이트 ID를 구성할 수 있습니다. 전에는 ASA 애플리케이션 내에서 사이트 ID를 구성해야 했습니다. 이 기능 덕분에 초기 구축이 수월해졌습니다. 더 이상 ASA 구성 내에서 사이트 ID를 설정할 수 없습니다. 또한 사이트 간 클러스터링과의 호환성을 최대한 활용하려면 안정성과 성능이 개선된 ASA 9.7(1) 및 FXOS 2.1.1로 업그레이드하는 것이 좋습니다. 다음 명령을 수정했습니다. **site-id**
지원 - Firepower 4100 Series	9.6(1)	FXOS 1.1.4를 활용하여 ASA에서는 Firepower 4100 Series에서 섀시 간 클러스터링을 지원합니다. 명령은 수정하지 않았습니다.
6개 모듈을 위한 섀시 간 클러스터링 및 Firepower 9300 ASA 애플리케이션을 위한 사이트 간 클러스터링	9.5(2.1)	이제 FXOS 1.1.3에서 사이트 간 클러스터링을 확장하여 섀시 간 클러스터링을 활성화할 수 있습니다. 최대 6개의 섀시에 최대 6개의 모듈을 포함할 수 있습니다. 명령은 수정하지 않았습니다.
Firepower 9300을 위한 인트라 섀시 클러스터링(intra-chassis clustering)	9.4(1.150)	Firepower 9300 섀시 내부에서 최대 3개의 보안 모듈을 클러스터링할 수 있습니다. 섀시의 모든 모듈은 클러스터에 속해야 합니다. 다음 명령을 도입했습니다. **cluster replication delay, debug service-module, management-only individual, show cluster chassis**



6 장

투명한 또는 라우팅된 방화벽 모드

이 장에서는 방화벽 모드를 라우팅 또는 투명 모드로 설정하는 방법 및 각 방화벽 모드에서 방화벽이 어떻게 작동하는지에 대해 설명합니다.

다중 컨텍스트 모드의 각 컨텍스트에 방화벽 모드를 개별적으로 설정할 수 있습니다.

방화벽 모드 정보

ASA에서는 두 가지 방화벽 모드(라우팅 방화벽 모드 및 투명 방화벽 모드)를 지원합니다.

라우팅 방화벽 모드 정보

라우팅 모드에서 ASA는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 상황 간에 Layer 3 인터페이스를 공유할 수 있습니다.

통합 라우팅 및 브리징을 통해 네트워크에서 여러 인터페이스를 그룹화하는 "브리지 그룹"을 사용할 수 있으며, ASA에서는 브리징 기술을 사용하여 인터페이스 간에 트래픽을 통과시킵니다. 각 브리지 그룹에는 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)가 있습니다. ASA에서는 BVI와 일반 라우팅 인터페이스 간을 라우팅합니다. 여러 상황 모드, 클러스터링, EtherChannel, 이중 또는 VNI 멤버 인터페이스가 필요하지 않은 경우, 투명 모드 대신 라우팅 모드를 사용하는 것을 고려할 수 있습니다. 라우팅 모드에서는 투명 모드에서와 같이 하나 이상의 격리된 브리지 그룹을 가질 수 있지만, 혼합 구축을 위한 일반적인 라우팅 인터페이스도 가집니다.

투명 방화벽 모드 정보

일반적으로 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다. 그러나 다른 방화벽과 마찬가지로 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다.

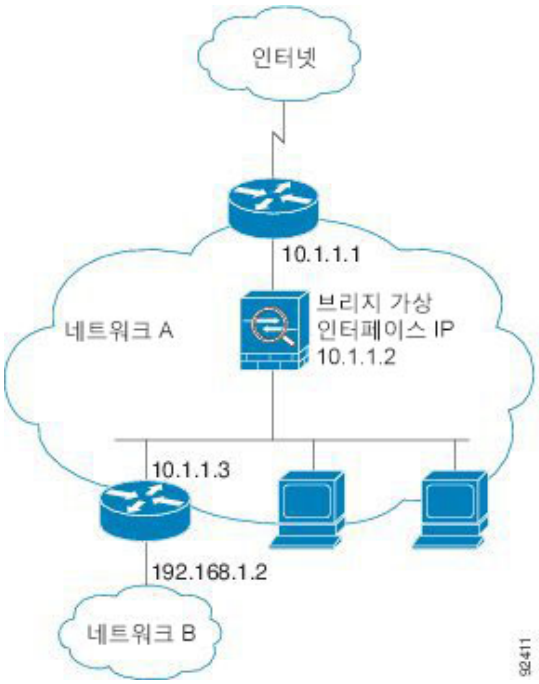
Layer 2 연결성은 네트워크의 내부 및 외부 인터페이스를 그룹화하는 "브리지 그룹"을 사용하여 획득할 수 있으며, ASA에서는 브리징 기술을 사용하여 인터페이스 간에 트래픽을 통과시킵니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 여러 네트워크에 대해 여러 개의 브리지 그룹을 사용할 수 있습니다. 투명 모드에서 이러한 브리지 그룹은 서로 통신할 수 없습니다.

네트워크에서 투명 방화벽 사용

ASA에서는 인터페이스 간의 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로, 투명 모드를 기존 네트워크에서 쉽게 도입할 수 있습니다.

다음 그림에는 외부 디바이스가 내부 디바이스와 동일한 서브넷에 존재하는 일반적인 투명 방화벽 네트워크가 나와 잇습니다. 내부 라우터와 호스트는 외부 라우터에 직접 연결되어 있는 것으로 표시됩니다.

그림 ***17:*** 투명 방어벽 네트워크



관리 인터페이스

각 BVI(Bridge Virtual Interface) IP 주소 이외에도 브리지 그룹에 속하지 않은 별도의 관리 슬롯/포트 인터페이스를 추가할 수 있으며, 이렇게 하면 ASA에는 관리 트래픽만 허용됩니다. 자세한 내용은 관리 인터페이스, 556 페이지을 참조하십시오.

라우팅 모드 기능의 트래픽 전달

투명 방화벽에서 직접 지원되지 않는 기능의 경우, 업스트림 및 다운스트림 라우터를 통해 트래픽이 전달되도록 허용하여 해당 기능을 지원할 수 있습니다. 예를 들어, 액세스 규칙을 사용하여 DHCP 트래픽(지원되지 않는 DHCP 릴레이 기능 대신) 또는 IP/TV에서 생성된 것과 같은 멀티캐스트 트래픽을 허용할 수 있습니다. 또한 투명 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수도 있습니다. 액세스 규칙을 기반으로 OSPF, RIP, EIGRP 또는 BGP 트래픽의 통과를 허용할 수 있습니다. 마찬가지로, HSRP 또는 VRRP와 같은 프로토콜이 ASA를 통과할 수 있습니다.

브리지 그룹 정보

브리지 그룹은 ASA에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 그룹은 투명 방화벽 모드와 라우팅 방화벽 모드에서 지원됩니다. 다른 방화벽 인터페이스와 마찬가지로 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다.

BVI(Bridge Virtual Interface)

각 브리지 그룹에는 BVI(Bridge Virtual Interface)가 있습니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 BVI IP 주소를 사용합니다. BVI IP 주소는 브리지 그룹 멤버 인터페이스와 동일한 서브넷에 있어야 합니다. BVI는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

투명 모드에서는 브리지 그룹 멤버 인터페이스만 이름이 지정되고 인터페이스 기반 기능과 함께 사용될 수 있습니다.

라우팅 모드에서는 BVI가 브리지 그룹 및 기타 라우팅 인터페이스 간에 게이트웨이 역할을 합니다. 브리지 그룹/라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다. 일부 인터페이스 기반 기능에는 BVI 자체를 사용할 수 있습니다.

- 액세스 규칙 — 브리지 그룹 멤버 인터페이스와 BVI 둘 다에 대한 액세스 규칙을 구성할 수 있습니다. 인바운드 규칙의 경우 멤버 인터페이스가 먼저 확인됩니다. 아웃바운드 규칙의 경우 BVI가 먼저 확인됩니다.
- DHCPv4 서버 — BVI에서만 DHCPv4 서버 구성을 지원합니다.
- 고정 경로 — BVI에 대한 고정 경로는 구성할 수 있지만, 멤버 인터페이스에 대한 고정 경로는 구성할 수 없습니다.
- ASA에서 시작되는 기타 트래픽 및 syslog 서버 — syslog 서버(또는 SNMP 서버나 ASA에서 트래픽이 시작되는 기타 서비스)를 지정하는 경우 BVI 또는 멤버 인터페이스를 지정할 수 있습니다.

라우팅 모드에서 BVI 이름을 지정하지 않는 경우 ASA에서는 브리지 그룹 트래픽을 라우팅하지 않습니다. 이 구성을 사용하면 브리지 그룹에 대한 투명 방화벽 모드가 복제됩니다. 여러 상황 모드, 클

러스터링, EtherChannel, 이중 또는 VNI 멤버 인터페이스가 필요하지 않은 경우, 라우팅 모드를 대신 사용하는 것을 고려할 수 있습니다. 라우팅 모드에서는 투명 모드에서와 같이 하나 이상의 격리된 브리지 그룹을 가질 수 있지만 혼합 구축을 위한 일반적인 라우팅 인터페이스도 사용할 수 있습니다.

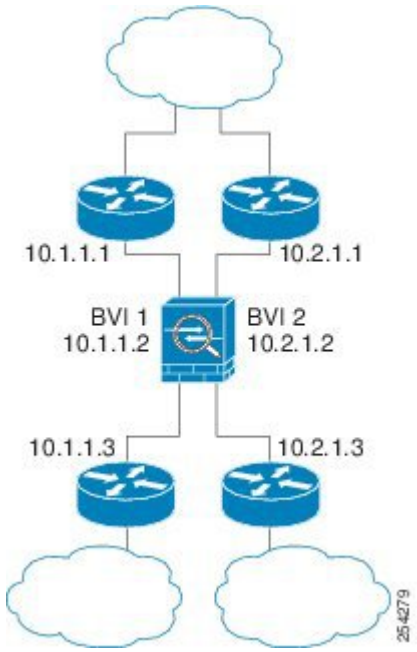
투명 방화벽 모드의 브리지 그룹

브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 트래픽은 ASA 내의 다른 브리지 그룹으로 라우팅되지 않으며, 트래픽은 외부 라우터에 의해 ASA의 다른 브리지 그룹으로 다시 라우팅되기 전에 ASA에서 나가야 합니다. 브리지 기능은 브리지 그룹마다 따로 있지만, 다른 여러 기능은 모든 브리지 그룹이 공유합니다. 예를 들어, 모든 브리지 그룹은 syslog 서버 또는 AAA 서버 컨피그레이션을 공유합니다. 완전한 보안 정책 분리를 위해서는 각 컨텍스트에서 한 브리지 그룹의 보안 컨텍스트를 사용합니다.

브리지 그룹당 여러 인터페이스를 포함할 수 있습니다. 지원되는 브리지 그룹 및 인터페이스의 정확한 수는 방화벽 모드에 대한 지침, 197 페이지의 내용을 참조하십시오. 브리지 그룹당 3개 이상의 인터페이스를 사용하는 경우, 동일한 네트워크에 있는 여러 세그먼트 간의 통신은 제어할 수 있지만 내부 및 외부 간의 통신은 제어할 수 없습니다. 예를 들어, 서로 통신하는 것을 허용하지 않을 내부 세그먼트가 3개 있는 경우, 각 세그먼트를 개별 인터페이스에 두고 외부 인터페이스하고만 통신하도록 허용할 수 있습니다. 또는 원하는 만큼만 액세스하는 것을 허용하기 위해 인터페이스 간에 액세스 규칙을 맞춤화할 수 있습니다.

다음 그림에는 2개의 브리지 그룹이 있는 ASA에 연결된 2개의 네트워크가 나와 있습니다.

그림 ***18: 2***개의 브리지 그룹이 있는 투명 방화벽 네트워크



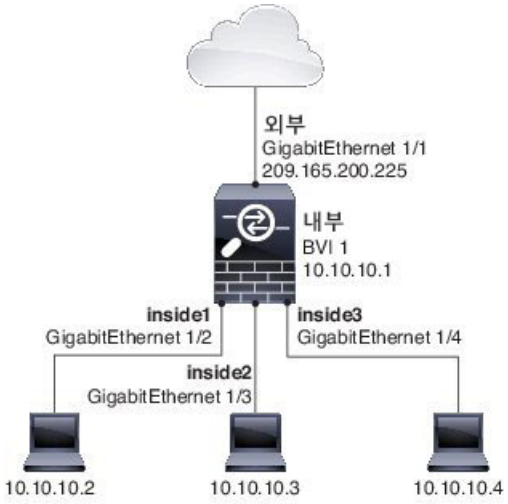
라우팅 방화벽 모드의 브리지 그룹

브리지 그룹 트래픽은 다른 브리지 그룹 또는 라우팅 인터페이스로 라우팅될 수 있습니다. 브리지 그룹의 BVI 인터페이스에 이름을 할당하지 않는 방법을 통해 브리지 그룹 트래픽을 격리하도록 선택

할 수 있습니다. BVI에 이름을 지정하면 BVI에서는 다른 일반 인터페이스와 마찬가지로 라우팅에 참여합니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 ASA에서 추가 인터페이스를 사용하는 것입니다. 예를 들어 일부 디바이스에 대한 기본 구성에서는 외부 인터페이스를 일반 인터페이스로 포함한 다음, 내부 브리지 그룹에 할당된 기타 모든 인터페이스를 포함합니다. 이 브리지 그룹의 목적이 외부 스위치를 교체하는 것이므로 모든 브리지 그룹 인터페이스가 자유롭게 통신할 수 있도록 액세스 정책을 구성해야 합니다. 예를 들어, 기본 구성에서와 마찬가지로 모든 인터페이스를 동일한 보안 수준으로 설정한 다음, 동일한 보안 인터페이스 통신을 활성화합니다. 액세스 규칙은 필요하지 않습니다.

그림 ***19:*** 내부 브리지 그룹 및 외부 라우팅 인터페이스를 사용하는 라우팅 방화벽 네트워크



라우팅 모드에서 허용되지 않는 트래픽 전달

라우팅 모드에서는 일부 트래픽 유형이 ASA를 통과하지 못할 수 있으며, 이는 액세스 규칙에서 허용한 경우에도 마찬가지입니다. 그러나 브리지 그룹은 액세스 규칙(IP 트래픽용) 또는 이더 타입 규칙(비 IP 트래픽)을 사용하여 거의 모든 트래픽이 통과하도록 허용할 수 있습니다.

- IP 트래픽 — 라우팅 방화벽 모드에서는 액세스 규칙에서 허용하더라도 브로드캐스트 및 멀티캐스트 트래픽이 차단됩니다. 지원되지 않는 동적 라우팅 프로토콜과 DHCP도 마찬가지입니다(DHCP 릴레이를 구성하지 않는 한). 브리지 그룹 내에서 액세스 규칙을 사용하여 이 트래픽을 허용할 수 있습니다(확장된 ACL 사용).
- 비 IP 트래픽 — 이더 타입 규칙을 사용하여 예를 들어, AppleTalk, IPX, BPDU, MPLS가 통과되도록 구성할 수 있습니다.

참고 브리지 그룹은 CDP 패킷 또는 0x600 이상의 유효한 이더 타입이 없는 패킷은 전달하지 않습니다. 예외적으로 BPDU 및 IS-IS는 지원됩니다.

Layer 3 트래픽 허용

- 액세스 규칙 없이도 유니캐스트 IPv4 및 IPv6 트래픽은 상위 보안 인터페이스에서 하위 보안 인터페이스까지 브리지 그룹을 자동으로 통과할 수 있습니다.
- 하위 보안 인터페이스에서 상위 보안 인터페이스로 이동하는 Layer 3 트래픽의 경우, 하위 보안 인터페이스에 액세스 규칙이 필요합니다.
- ARP는 액세스 규칙 없이도 양방향에서 브리지 그룹을 통과할 수 있습니다. ARP 트래픽은 ARP 감시로 제어할 수 있습니다.
- IPv6 네이버 검색 및 라우터 요청 패킷은 액세스 규칙을 사용하여 전달될 수 있습니다.
- 액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽을 전달할 수 있습니다.

허용되는 MAC 주소

액세스 정책에서 허용하는 경우 다음과 같은 대상 MAC 주소가 브리지 그룹을 통과할 수 있습니다 (Layer 3 트래픽 허용, 192 페이지 참조). 이 목록에 없는 모든 MAC 주소는 손실됩니다.

- FFFF.FFFF.FFFF와 같은 TRUE 브로드캐스트 목적지 MAC 주소
- 0100.5E00.0000에서 0100.5EFE.FFFF 사이의 IPv4 멀티캐스트 MAC 주소
- 3333.0000.0000에서 3333.FFFF.FFFF 사이의 IPv6 멀티캐스트 MAC 주소
- 0100.0CCC.CCCD와 같은 BPDU 멀티캐스트 주소
- 0900.0700.0000에서 0900.07FF.FFFF 사이의 AppleTalk 멀티캐스트 MAC 주소

BPDU 처리

Spanning Tree Protocol을 사용하여 루프를 방지하기 위해 BPDU가 기본적으로 전달됩니다. BPDU를 차단하려면 이더 타입 규칙이 이를 거부하도록 구성해야 합니다. 장애 조치를 사용할 경우, 토폴로지가 변경될 때 BPDU를 차단하여 스위치 포트가 차단 상태가 되는 것을 방지하고자 할 수 있습니다. 자세한 내용은 장애 조치를 위한 브리지 그룹 요구 사항, 282 페이지를 참조하십시오.

MAC 주소 대 경로 조회 비교

브리지 그룹 내 트래픽의 경우 패킷의 발신 인터페이스는 경로 조회 대신 대상 MAC 주소 조회를 수행하여 확인할 수 있습니다.

그러나 다음과 같은 상황에는 경로 조회가 필요합니다.

- ASA에서 시작되는 트래픽 — 예를 들어, syslog 서버가 위치한 원격 네트워크로 향하는 트래픽을 위해 ASA에서 기본/고정 경로를 추가합니다.
- 검사가 활성화되어 있는 VoIP(Voice over IP) 및 TFTP 트래픽, 1홉 이상 떨어져 있는 엔드포인트 — 보조 연결에 성공하도록 원격 엔드포인트로 향하는 트래픽을 위해 ASA에서 고정 경로를 추가합니다. ASA에서는 보조 연결을 허용하기 위해 액세스 제어 정책에서 임시 "핀홀"을 생성합

니다. 연결에서 기본 연결보다 다양한 IP 주소 집합을 사용할 수 있기 때문에, ASA에서는 올바른 인터페이스에서 핀홀을 설치하기 위해 경로 조회를 수행해야 합니다.

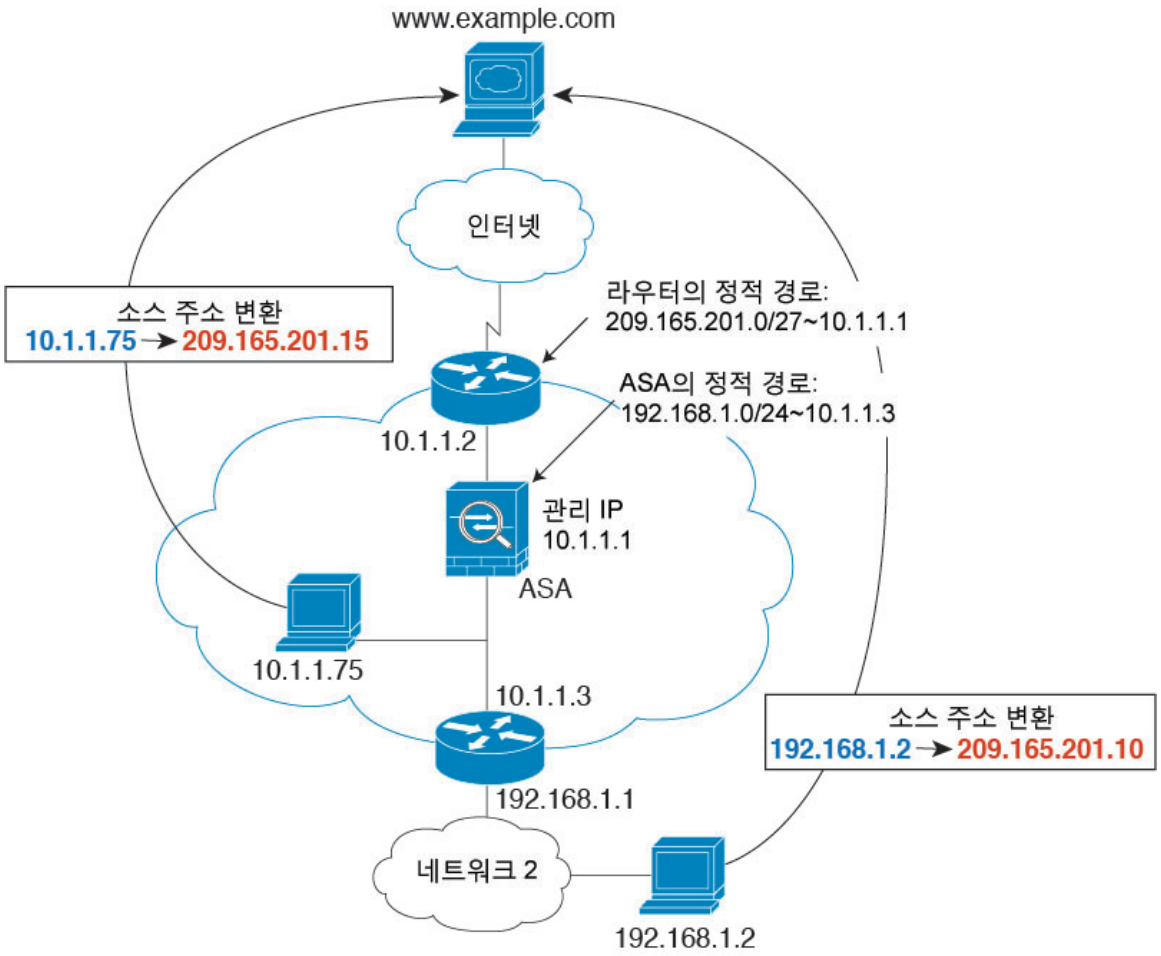
영향을 받는 애플리케이션은 다음과 같습니다.

- CTIQBE
- GTP
- H.323
- MGCP
- RTSP
- SIP
- Skinny(SCCP)
- SQL*Net
- SunRPC
- TFTP

- ASA에서 NAT를 수행하는 1홉 이상 떨어져 있는 트래픽 — 원격 네트워크로 향하는 트래픽을 위해 ASA에서 고정 경로를 구성합니다. 또한 ASA로 전송될 매핑된 주소로 향하는 트래픽을 위해 업스트림 라우터에 고정 경로가 필요합니다.

  이 라우팅 요구 사항은 검사 및 NAT가 활성화되어 있는 DNS 및 VoIP용 임베디드 IP 주소에도 마찬가지로 적용되며, 임베디드 IP 주소는 1홉 이상 떨어져 있습니다. ASA에서는 올바른 이그레스 인터페이스를 식별해야 변환을 수행할 수 있습니다.

그림 *20: NAT* 예: 브리지 그룹 내부의 *NAT*



투명 모드의 브리지 그룹에 대해 지원되지 않는 기능

다음 표에는 투명 모드의 브리지 그룹에서 지원되지 않는 기능이 나와 있습니다.

표 *3:* 투명 모드에서 지원되지 않는 기능

기능	설명
동적 DNS	—
DHCPv6 스테이트리스 서버	DHCPv4 서버만 브리지 그룹 멤버 인터페이스에서 지원됩니다.

기능	설명
DHCP 릴레이	투명 방화벽에서는 DHCPv4 서버 역할을 수행할 수 있으나, DHCP 릴레이를 지원하지는 않습니다. 2개의 액세스 규칙을 사용하여 DHCP 트래픽이 통과되도록 할 수 있으므로 DHCP 릴레이가 필요하지 않습니다. 이러한 액세스 규칙 중 하나는 DHCP 요청이 내부 인터페이스에서 외부 인터페이스로 전달되도록 하고, 나머지 하나는 서버의 응답을 다른 방향으로 전달할 수 있도록 합니다.
동적 라우팅 프로토콜	그러나 브리지 그룹 멤버 인터페이스의 ASA에서 시작된 트래픽에 대한 고정 경로를 추가할 수 있습니다. 또한 액세스 규칙을 사용하여 동적 라우팅 프로토콜이 ASA를 통과하도록 할 수 있습니다.
멀티캐스트 IP 라우팅	액세스 규칙에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 ASA를 통과하도록 할 수 있습니다.
QoS	—
통과 트래픽의 VPN 종료	투명 방화벽에서는 브리지 그룹 멤버 인터페이스에서만 관리 연결에 Site-to-Site VPN 터널을 지원합니다. 그러나 이로 인해 ASA를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 액세스 규칙을 사용하여 VPN 트래픽이 ASA를 통과하도록 할 수 있으나, 이로 인해 관리 이외 연결이 종료되지는 않습니다. 클라이언트리스 SSL VPN이 지원되지 않습니다.
통합 통신	—

라우팅 모드의 브리지 그룹에 대해 지원되지 않는 기능

다음 표에는 라우팅 모드의 브리지 그룹에서 지원되지 않는 기능이 나와 있습니다.

표 ***4:*** 라우팅 모드에서 지원되지 않는 기능

기능	설명
EtherChannel 또는 VNI 멤버 인터페이스	물리적 인터페이스, 이중 인터페이스 및 하위 인터페이스만 브리지 그룹 멤버 인터페이스로 지원됩니다. 관리 인터페이스도 지원되지 않습니다.

기능	설명
클러스터링	브리지 그룹은 클러스터링에서 지원되지 않습니다.
동적 DNS	—
DHCPv6 스테이트리스 서버	DHCPv4 서버만 BVI에서 지원됩니다.
DHCP 릴레이	라우팅 방화벽은 DHCPv4 서버로 작동할 수 있지만, BVI 또는 브리지 그룹 멤버 인터페이스에서 DHCP 릴레이를 지원하지는 않습니다.
동적 라우팅 프로토콜	그러나 BVI에 고정 경로를 추가할 수 있습니다. 또한 액세스 규칙을 사용하여 동적 라우팅 프로토콜이 ASA를 통과하도록 할 수 있습니다. 비 브리지 그룹 인터페이스에서는 동적 라우팅을 지원합니다.
멀티캐스트 IP 라우팅	액세스 규칙에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 ASA를 통과하도록 할 수 있습니다. 비 브리지 그룹 인터페이스에서는 멀티캐스트 라우팅을 지원합니다.
다중 상황 모드	브리지 그룹은 다중 상황 모드에서 지원되지 않습니다.
QoS	비 브리지 그룹 인터페이스에서는 QoS를 지원합니다.
통과 트래픽의 VPN 종료	BVI에서 VPN 연결을 종료할 수 없습니다. 비 브리지 그룹 인터페이스에서는 VPN을 지원합니다. 브리지 그룹 멤버 인터페이스에서는 관리 연결에만 Site-to-Site VPN 터널을 지원합니다. 그러나 이로 인해 ASA를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 액세스 규칙을 사용하여 VPN 트래픽이 브리지 그룹을 통과하도록 할 수 있으나, 이로 인해 관리 이외 연결이 종료되지는 않습니다. 클라이언트리스 SSL VPN이 지원되지 않습니다.
통합 통신	비 브리지 그룹 인터페이스에서는 Unified Communications를 지원합니다.

기본 설정

기본 모드

기본 모드는 라우팅 모드입니다.

브리지 그룹 기본값

기본적으로 모든 ARP 패킷은 브리지 그룹 내에서 전달됩니다.

방화벽 모드에 대한 지침

상황 모드 지침

컨텍스트당 방화벽 모드를 설정합니다.

모델 지침

- ASAv50의 경우, 브리지 그룹이 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.

브리지 그룹 지침(투명 모드 및 라우팅 모드)

- 브리지 그룹당 64개의 인터페이스가 있는 최대 250개의 브리지 그룹을 생성할 수 있습니다.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.
- IPv4에서는 관리 트래픽과 ASA를 거칠 트래픽 모두 브리지 그룹마다 BVI용 IP 주소가 필요합니다. IPv6 주소는 지원되지만 BVI에는 필요하지 않습니다.
- IPv6 주소만 수동으로 구성할 수 있습니다.
- BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다.
- 관리 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 투명 모드에서는 1개 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 투명 모드에서는 BVI IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 ASA의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.

- 투명 모드에서는 관리 트래픽의 반환 경로를 제공하는 데 필요한 기본 경로가 하나의 브리지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브리지 그룹의 인터페이스 및 브리지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브리지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 일반 고정 경로를 지정해야 합니다.
- 투명 모드에서 PPPoE는 관리 인터페이스에 대해 지원되지 않습니다.
- 라우팅 모드에서 브리지 그룹 및 기타 라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다.
- 라우팅 모드에서 EtherChannel 및 VNI 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 브리지 그룹 멤버를 사용할 때 ASA를 통과하는 것이 허용되지 않습니다. BFD를 실행하는 ASA의 양쪽 측면에 두 개의 네이버가 있는 경우, ASA는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

추가 지침 및 제한

- 방화벽 모드를 변경할 경우, 두 모드에 모두 여러 명령이 지원되지 않으므로 ASA에서는 실행 중인 구성을 지웁니다. 시작 컨피그레이션은 변경되지 않고 유지됩니다. 저장하지 않고 다시 로드할 경우 시작 컨피그레이션이 로드되며 모드가 원래 설정으로 다시 전환됩니다. 구성 파일 백업에 대한 자세한 내용은 방화벽 모드, 198 페이지을 참조하십시오.
- **firewall transparent** 명령으로 모드를 변경하는 텍스트 구성을 ASA에 다운로드할 경우, 구성의 맨 위에 해당 명령을 입력해야 합니다. ASA에서는 이 명령을 읽는 즉시 모드를 변경한 다음, 다운로드된 구성을 계속 읽습니다. 명령이 구성의 뒤에 표시될 경우 ASA에서는 구성의 앞에 있는 모든 행을 지웁니다.텍스트 파일 다운로드에 대한 자세한 내용은 ASA 이미지, ASDM 및 시작 구성설정, 1174 페이지을 참조하십시오.

방화벽 모드

이 섹션에서는 하여 방화벽 모드를 변경하는 방법에 대해 설명합니다.

참고 방화벽 모드를 변경하면 실행 중인 컨피그레이션이 지워지므로 다른 컨피그레이션을 수행하기 전에 방화벽 모드를 설정하는 것이 좋습니다.

시작하기 전에

모드를 변경하면 ASA에서는 실행 중인 구성을 지웁니다(자세한 내용은 방화벽 모드에 대한 지침, 197 페이지 참조).

- 컨피그레이션이 이미 채워져 있는 경우 모드를 변경하기 전에 해당 컨피그레이션을 백업하십시오. 새 컨피그레이션을 생성할 때 이러한 백업을 참조할 수 있습니다. 구성 또는 기타 파일 백업 및 복원, 1176 페이지을 참조하십시오.
- 모드를 변경하려면 콘솔 포트에서 CLI를 사용합니다. ASDM 명령줄 인터페이스 툴이나 SSH를 비롯한 다른 유형의 세션을 사용할 경우, 구성이 지워지면 연결이 끊어지며 콘솔 포트를 사용하여 ASA에 다시 연결해야 합니다.
- 컨텍스트 내에서 모드를 설정합니다.

참고 구성이 지워진 후에 방화벽 모드를 투명 모드로 설정하고 ASDM 관리 액세스를 구성하려면 ASDM 액세스 구성, 23 페이지를 참조하십시오.

프로시저

방화벽을 투명 모드로 설정합니다.

firewall transparent

예제:

```
ciscoasa(config)# firewall transparent
```

모드를 라우팅 모드로 변경하려면 **no firewall transparent** 명령을 입력합니다.

참고 방화벽 모드 변경을 확인하는 메시지가 표시되지 않으며, 변경이 즉시 이루어집니다.

방화벽 모드의 예

이 섹션에는 트래픽이 라우팅 및 투명 방화벽 모드에서 어떻게 ASA를 통과하여 이동하는지에 대한 예가 포함되어 있습니다.

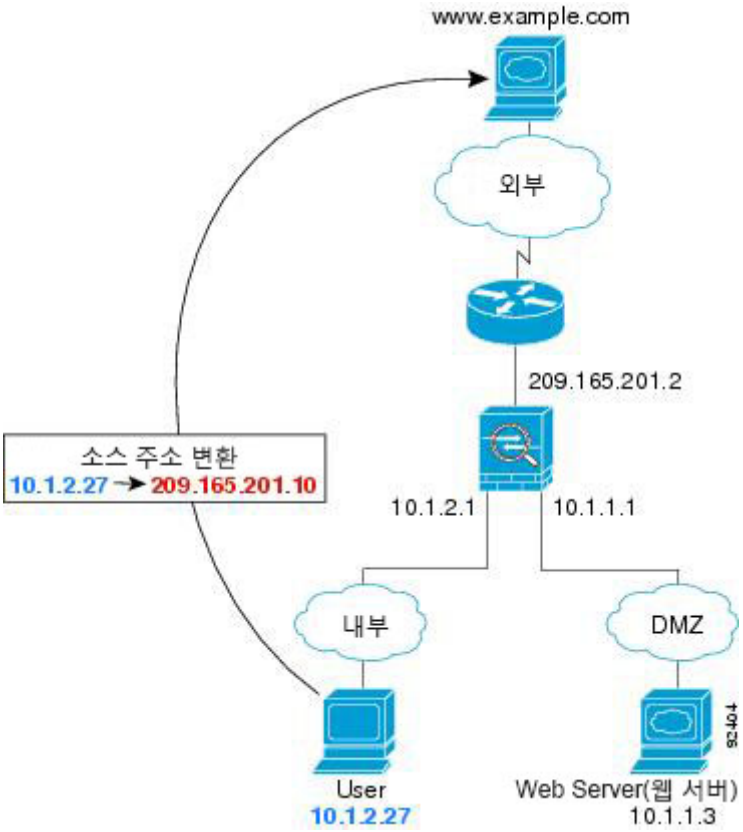
라우팅 방화벽 모드에서 데이터가 ASA를 통과하여 이동하는 방식

다음 섹션에서는 여러 시나리오의 라우팅 방화벽 모드에서 데이터가 ASA를 통과하여 이동하는 방식에 대해 설명합니다.

웹 서버를 방문하는 내부 사용자

다음 그림에는 외부 웹 서버에 액세스하는 내부 사용자가 나와 있습니다.

그림 *21:* 내부 대 외부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하는데, 해당 패킷은 새 세션이기 때문에 ASA에서는 보안 정책의 조건에 따라 해당 패킷이 허용되는지 확인합니다.

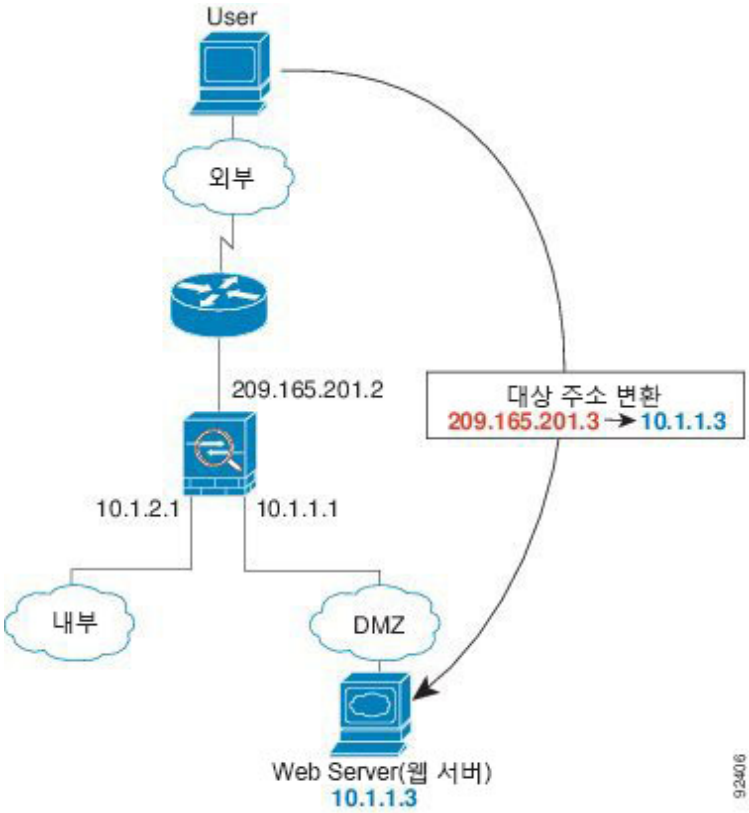
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 실제 주소(10.1.2.27)를 매핑된 주소(209.165.201.10)(외부 인터페이스 서브넷에 있음)로 변환합니다.

   매핑된 주소는 어느 서브넷에나 있을 수 있지만, 외부 인터페이스 서브넷에 있을 경우 라우팅이 간소화됩니다.
4. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 외부 인터페이스에서 패킷을 전달합니다.
5. www.example.com에서 요청에 응답할 경우 패킷이 ASA를 통해 이동하며, 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다. ASA에서는 전역 목적지 주소를 로컬 사용자 주소인 10.1.2.27로 변환하지 않고 NAT를 수행합니다.
6. ASA에서는 패킷을 내부 사용자에게 전달합니다.

DMZ의 웹 서버를 방문하는 외부 사용자

다음 그림에는 DMZ 웹 서버에 액세스하는 외부 사용자가 나와 있습니다.

그림 *22:* 외부 대 *DMZ*



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

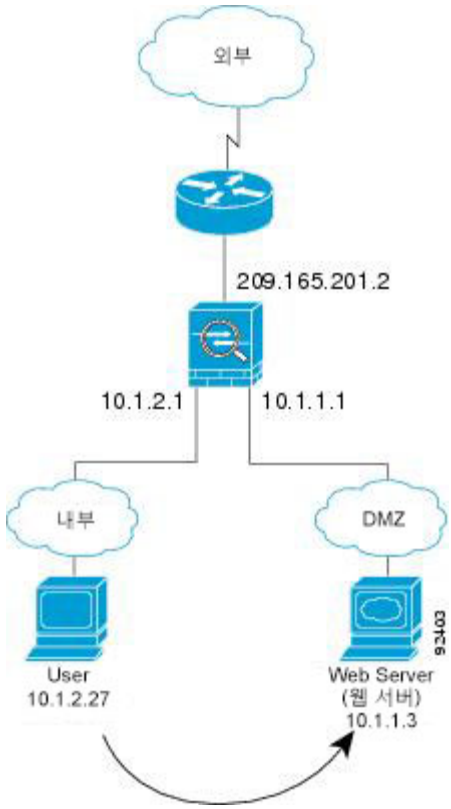
1. 외부 네트워크의 사용자가 외부 인터페이스 서브넷에 있는 매핑된 주소(209.165.201.3)를 사용하여 DMZ 웹 서버의 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 매핑된 주소를 실제 주소 10.1.1.3으로 변환 취소합니다.
3. 이 패킷은 새 세션이므로 ASA에서는 보안 정책의 조건에 따라 해당 패킷이 허용되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
4. 그런 다음 ASA에서는 세션 항목을 빠른 경로에 추가하고 DMZ 인터페이스에서 패킷을 전달합니다.
5. DMZ 웹 서버에서 요청에 응답할 경우 패킷이 ASA를 통해 이동하며, 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다. ASA에서는 실제 주소를 209.165.201.3으로 변환하여 NAT를 수행합니다.
6. ASA에서는 패킷을 외부 사용자에게 전달합니다.

DMZ의 웹 서버를 방문하는 외부 사용자

다음 그림에는 DMZ 웹 서버에 액세스하는 내부 사용자가 나와 있습니다.

그림 ***23:*** 내부 대 ***DMZ***



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

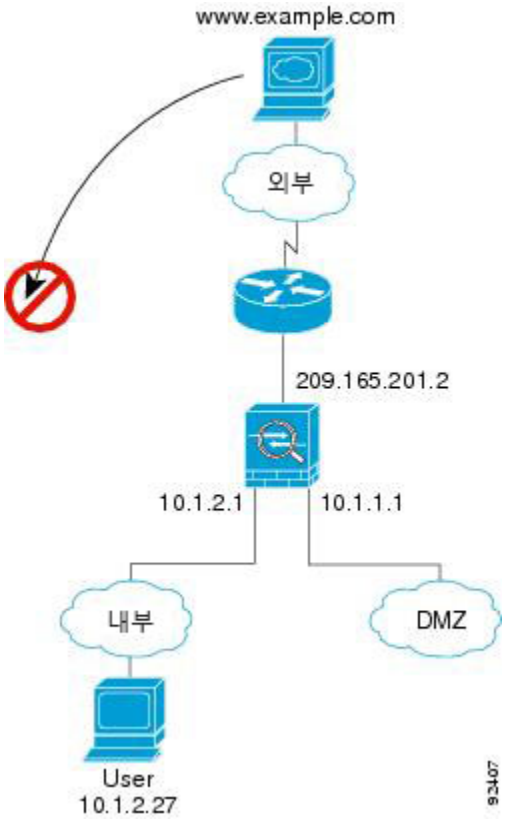
1. 내부 네트워크의 사용자가 목적지 주소(10.1.1.3)를 사용하여 DMZ 웹 서버의 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하는데, 해당 패킷은 새 세션이기 때문에 ASA에서는 보안 정책의 조건에 따라 해당 패킷이 허용되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 DMZ 인터페이스에서 패킷을 전달합니다.
4. DMZ 웹 서버에서 요청에 응답할 경우 패킷이 빠른 경로를 통해 이동하며, 이에 따라 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회할 수 있습니다.
5. ASA에서는 패킷을 내부 사용자에게 전달합니다.

내부 호스트에 액세스를 시도하는 외부 사용자

다음 그림에는 내부 네트워크에 액세스를 시도하는 외부 사용자가 나와 있습니다.

그림 *24:* 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

1. 외부 네트워크의 사용자가 내부 호스트에 연결하기 위해 시도합니다(해당 호스트에 라우팅 가능한 IP 주소가 있는 것으로 가정).

   내부 네트워크에서 사설 주소를 사용할 경우, 외부 사용자는 NAT 없이 내부 네트워크에 연결할 수 없습니다. 외부 사용자는 기존 NAT 세션을 사용하여 내부 사용자에게 연결을 시도하려고 할 수 있습니다.

2. ASA에서 패킷을 수신하는데, 해당 패킷은 새 세션이기 때문에 ASA에서는 보안 정책에 따라 해당 패킷이 허용되는지 확인합니다.

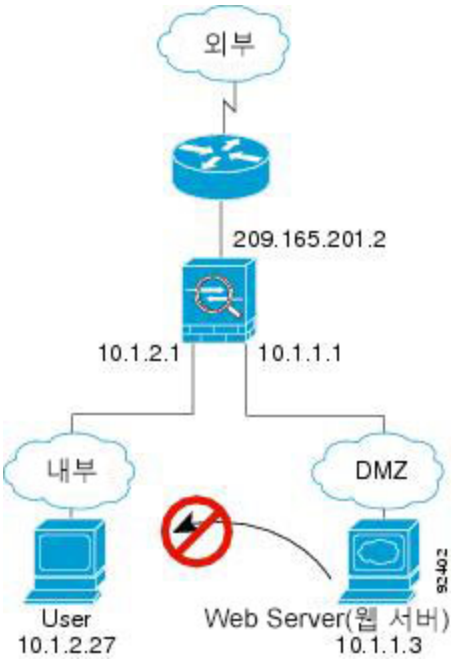
3. 패킷이 거부되며 ASA에서 해당 패킷을 누락시키고 연결 시도를 기록합니다.

   외부 사용자가 내부 네트워크에 공격을 시도할 경우, ASA에서는 다양한 기술을 사용하여 패킷이 기존에 설정된 세션에 사용할 수 있는 유효한 패킷인지 확인합니다.

내부 호스트에 액세스를 시도하는 DMZ 사용자

다음 그림에는 내부 네트워크에 액세스를 시도하는 DMZ의 사용자가 나와 있습니다.

그림 ***25: DMZ*** 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

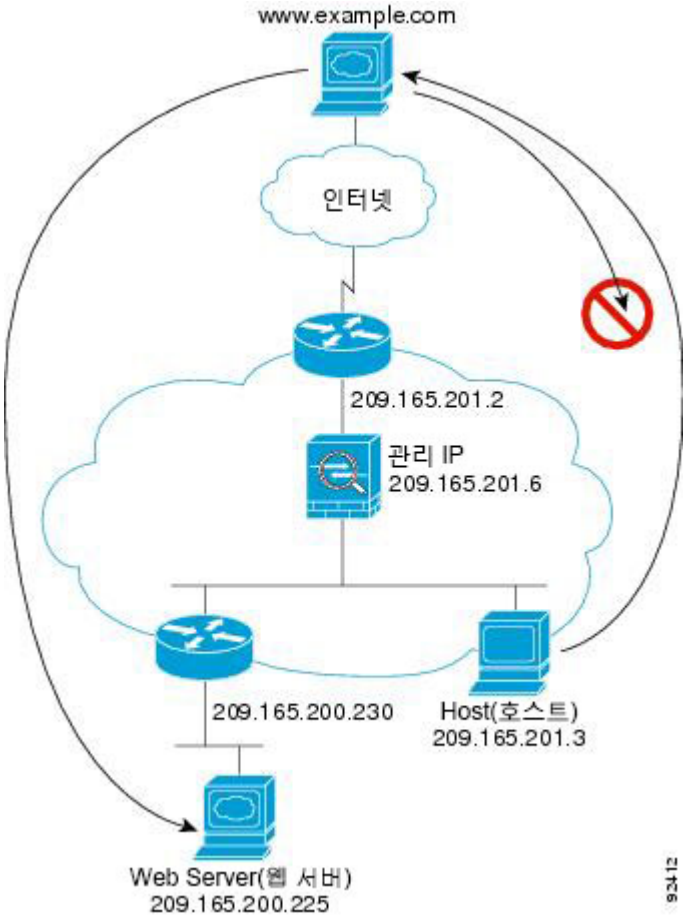
1. DMZ 네트워크 사용자가 내부 호스트에 연결하기 위해 시도합니다. DMZ에서는 인터넷의 트래픽을 라우팅해야 할 필요가 없으므로, 사설 주소 지정 체계로 라우팅을 방지할 수 없습니다.
2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 보안 정책에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   패킷이 거부되며 ASA에서 해당 패킷을 누락시키고 연결 시도를 기록합니다.

데이터가 투명 방화벽을 통해 이동하는 방식

다음 그림에는 공용 웹 서버가 포함된 내부 네트워크에 투명 방화벽을 구현한 일반적인 예가 나와 있습니다. ASA에는 액세스 규칙이 있어 내부 사용자가 인터넷 리소스에 액세스할 수 있습니다. 또 다른 액세스 규칙은 외부 사용자가 내부 네트워크의 웹 서버에만 액세스할 수 있도록 합니다.

그림 *26:* 일반적인 투명 방화벽 데이터 경로

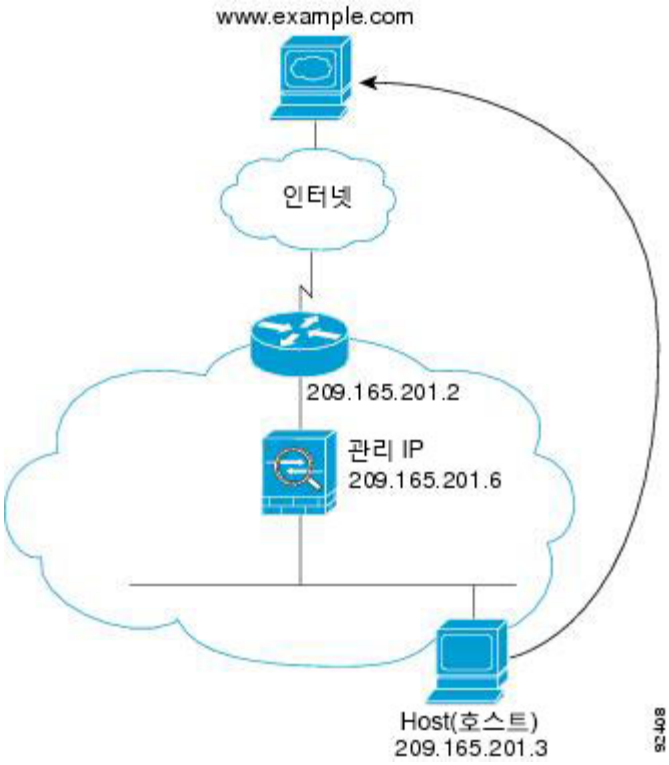


다음 섹션에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

웹 서버를 방문하는 내부 사용자

다음 그림은 외부 웹 서버에 액세스하는 내부 사용자를 보여줍니다.

그림 *27:* 내부 대 외부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이기 때문에 ASA에서는 보안 정책의 조건에 따라 해당 패킷이 허용되는지 확인합니다.

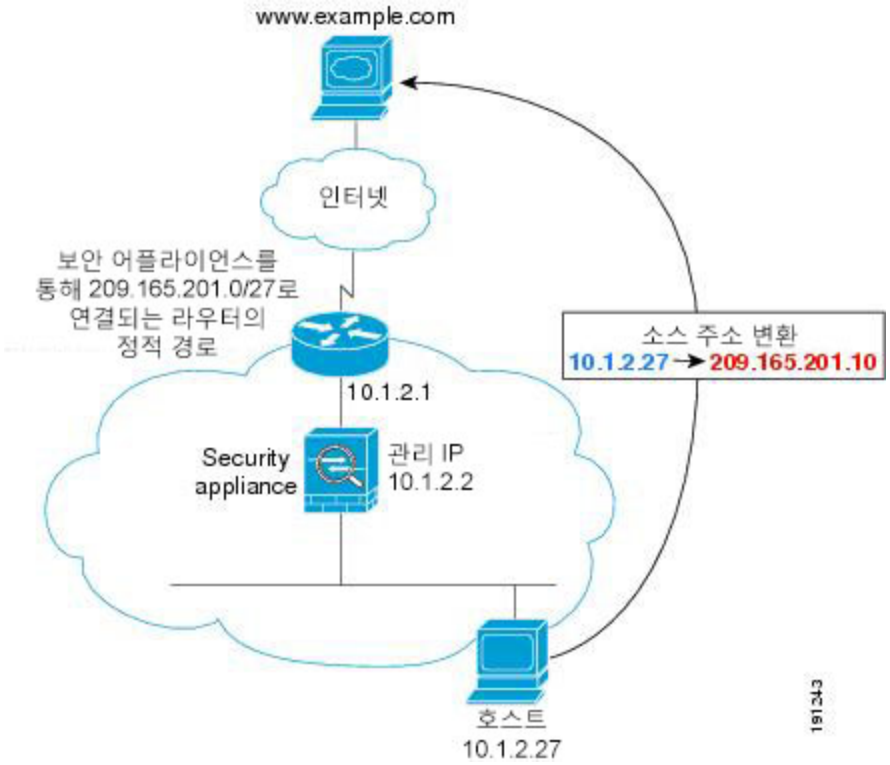
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 세션이 설정되었음을 기록합니다.
4. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 외부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 209.165.201.2입니다.

   대상 MAC 주소가 ASA 테이블에 없는 경우, ASA에서는 ARP 요청 또는 Ping을 전송하여 MAC 주소를 찾으려고 합니다. 첫 번째 패킷은 손실됩니다.
5. 웹 서버에서 요청에 응답합니다. 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다.
6. ASA에서는 패킷을 내부 사용자에게 전달합니다.

NAT를 사용하여 웹 서버를 방문하는 내부 사용자

다음 그림은 외부 웹 서버에 액세스하는 내부 사용자를 보여줍니다.

그림 *28:* 내부 대 외부*(NAT* 사용*)*



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 보안 정책의 조건에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 우선 고유한 인터페이스에 따라 패킷을 분류합니다.
3. ASA에서는 실제 주소(10.1.2.27)를 매핑된 주소 209.165.201.10으로 변환합니다.

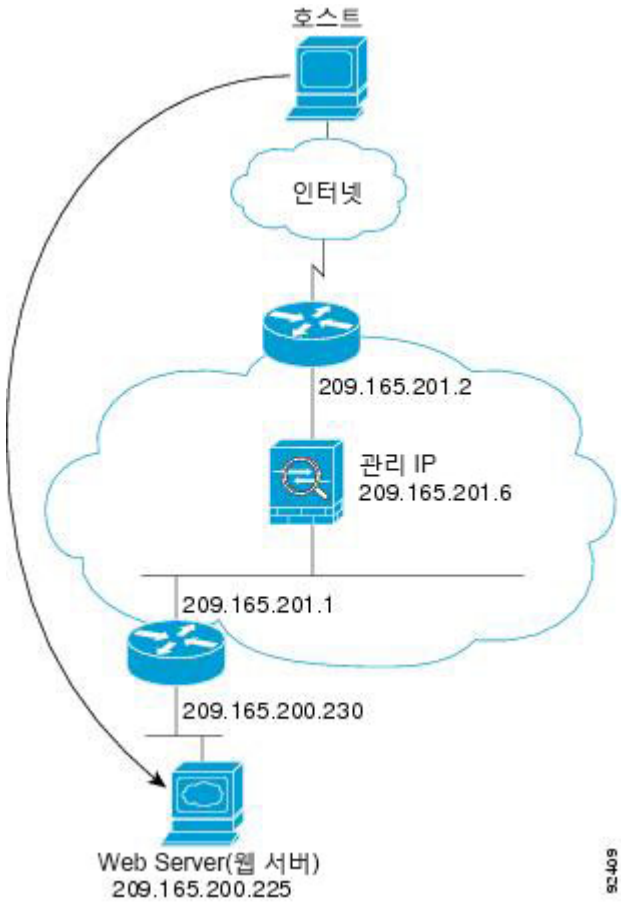
   매핑된 주소는 외부 인터페이스와 같은 네트워크에 있지 않으므로, ASA를 가리키는 매핑된 네트워크에 대한 고정 경로가 업스트림 라우터에 있어야 합니다.
4. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 외부 인터페이스에서 패킷을 전달합니다.
5. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 외부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 10.1.2.1입니다.

   대상 MAC 주소가 ASA 테이블에 없는 경우, ASA에서는 ARP 요청 및 ping을 전송하여 MAC 주소를 찾으려고 합니다. 첫 번째 패킷은 손실됩니다.
6. 웹 서버에서 요청에 응답합니다. 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다.
7. ASA에서는 매핑된 주소를 실제 주소(10.1.2.27)로 변환하지 않고 NAT를 수행합니다.

내부 네트워크의 웹 서버를 방문하는 외부 사용자

다음 그림에는 내부 웹 서버에 액세스하는 외부 사용자가 나와 있습니다.

그림 ***29:*** 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

1. 외부 네트워크의 사용자가 내부 웹 서버의 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 보안 정책의 조건에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 세션이 설정되었음을 기록합니다.
4. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 내부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 209.165.201.1입니다.

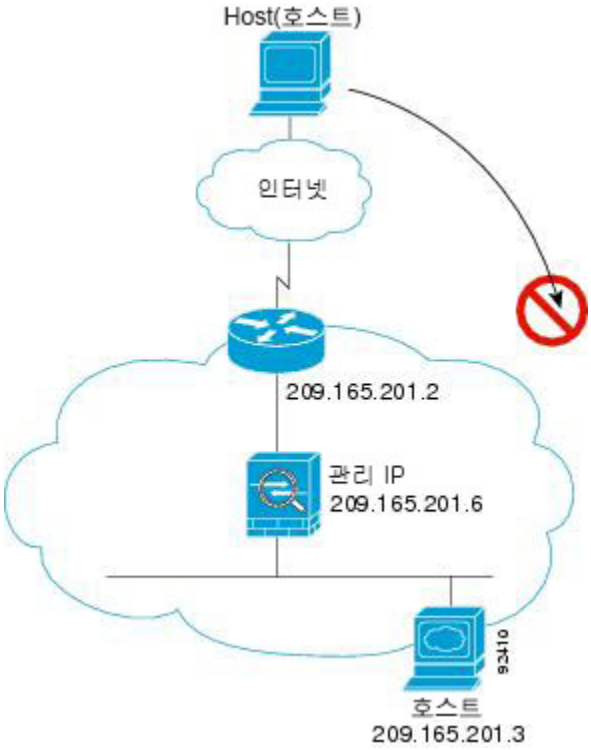
   대상 MAC 주소가 ASA 테이블에 없는 경우, ARP 요청 및 ping을 전송하여 MAC 주소를 찾으려고 합니다. 첫 번째 패킷은 손실됩니다.

5. 웹 서버에서 요청에 응답합니다. 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다.
6. ASA에서는 패킷을 외부 사용자에게 전달합니다.

내부 호스트에 액세스를 시도하는 외부 사용자

다음 그림에는 내부 네트워크의 호스트에 액세스를 시도하는 외부 사용자가 나와 있습니다.

그림 ***30:*** 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

1. 외부 네트워크 사용자가 내부 호스트에 연결하기 위해 시도합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 ASA에서는 보안 정책의 조건에 따라 해당 패킷이 허용되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. 외부 호스트를 허용하는 액세스 규칙이 없으므로 패킷이 거부되며 ASA에서 패킷을 누락시킵니다.
4. 외부 사용자가 내부 네트워크에 공격을 시도할 경우, ASA에서는 다양한 기술을 사용하여 패킷이 기존에 설정된 세션에 사용할 수 있는 유효한 패킷인지 확인합니다.

방화벽 모드 내역

표 *5:* 방화벽 모드의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
투명 방화벽 모드	7.0(1)	투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다. 다음 명령을 도입했습니다. **firewall transparent**, **show firewall**
투명 방화벽 브리지 그룹	8.4(1)	보안 컨텍스트의 오버헤드를 원치 않을 경우 또는 보안 컨텍스트 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 단일 모드 또는 다중 모드의 컨텍스트당 최대 8개의 브리지 그룹을 구성할 수 있으며, 브리지 그룹당 최대 4개의 인터페이스가 포함됩니다. 참고 ASA 5505에서 여러 개의 브리지 그룹을 구성할 수는 있으나, ASA 5505의 투명 모드에서 데이터 인터페이스가 2개로 제한된다는 것은 실제로 사용 가능한 브리지 그룹은 1개라는 의미입니다. 다음 명령을 도입했습니다. **interface bvi**, **bridge-group**, **show bridge-group**
다중 컨텍스트 모드에서 혼합 방화벽 모드 지원	8.5(1), 9.0(1)	다중 컨텍스트 모드에서 각 보안 컨텍스트에 방화벽 모드를 개별적으로 설정할 수 있으므로, 일부는 투명 모드에서 실행되는 동시에 다른 나머지는 라우팅 모드에서 실행될 수 있습니다. 다음 명령을 수정했습니다. **firewall transparent**

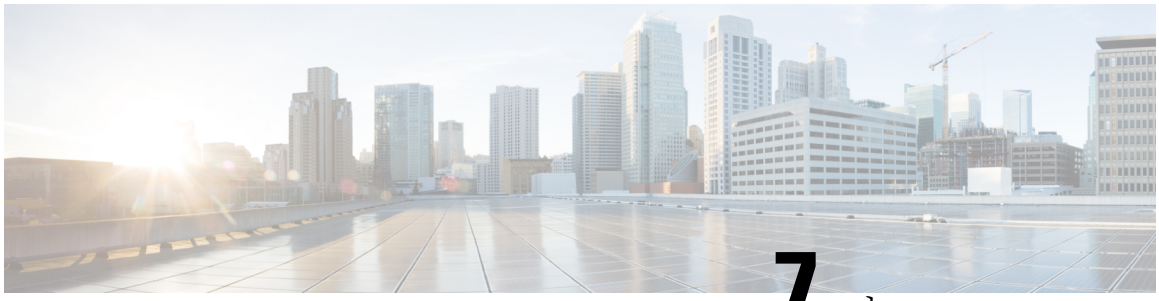
기능 이름	플랫폼 릴리스	기능 정보
투명 모드 브리지 그룹 최대 개수 250개로 증가	9.3(1)	브리지 그룹의 최대 개수가 8개에서 250개로 늘어났습니다. 단일 모드에서 또는 다중 모드의 각 컨텍스트에서 최대 250개의 브리지 그룹을 구성할 수 있으며, 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 다음 명령을 수정했습니다. **interface bvi**, **bridge-group**
브리지 그룹당 투명 모드 최대 인터페이스 개수 64개로 증가	9.6(2)	브리지 그룹당 최대 인터페이스 개수가 4개에서 64개로 증가되었습니다. 명령은 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
통합 라우팅 및 브리징	9.7(1)	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 ASA에서 경로 대신 브리징하는 인터페이스 그룹입니다. ASA는 실제 브리지가 아닙니다. ASA는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이전에는 브리지 그룹 간에 라우팅할 수 없는 투명 방화벽 모드에서만 브리지 그룹을 구성할 수 있었습니다. 이 기능을 사용하면 라우팅 방화벽 모드에서 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 ASA에 있는 경우에는 외부 Layer 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. 라우팅 모드에서 BVI는 명명된 인터페이스가 될 수 있으며 액세스 규칙 및 DHCP 서버 같은 일부 기능에서 멤버 인터페이스와 별도로 참여할 수 있습니다. 투명 모드에서 지원되는 다음 기능은 라우팅 모드에서는 지원되지 않습니다. 다중 상황 모드, ASA 클러스터링. 동적 라우팅 및 멀티캐스트 라우팅 기능은 BVI에서도 지원되지 않습니다. 다음 명령을 수정했습니다. **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**

기능 이름	플랫폼 릴리스	기능 정보
Firepower 4100/9300 ASA 논리적 디바이스에 대한 투명 모드 구축 지원	9.10(1)	이제 Firepower 4100/9300에 ASA를 구축할 때 투명 또는 라우티드 모드를 지정할 수 있습니다. 신규/수정된 FXOS 명령: **enter bootstrap-key FIREWALL_MODE**, **set value routed**, **set value transparent**

II 부

우수한 가용성 및 확장성



7 장

다중 상황 모드

이 장에서는 Cisco ASA에서 다중 보안 상황을 구성하는 방법을 설명합니다.

보안 상황 정보

단일 ASA를 보안 컨텍스트라고 하는 다중 가상 장치로 분할할 수 있습니다. 각 컨텍스트는 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스의 역할을 합니다. 다중 상황은 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 다중 상황 모드에서 지원되지 않는 기능에 대해서는 다중 상황 모드를 위한 지침, 230 페이지를 참조하십시오.

이 섹션에서는 보안 상황의 개요를 제공합니다.

보안 상황의 일반적인 용도

다음과 같은 상황에서 다중 보안 상황을 사용할 수 있습니다.

- 많은 고객에게 보안 서비스를 판매하려는 서비스 공급자라면 ASA에서 다중 보안 상황을 활성화함으로써 모든 고객의 트래픽을 분리하여 안전하게 지키면서 구성하기도 쉬운 경제적인 공간 절약형 솔루션을 구현할 수 있습니다.
- 각 부서/학과를 완전히 분리된 상태로 유지하려는 대기업 또는 대학 캠퍼스

- 부서별로 각기 다른 보안 정책을 제공하려는 기업
- 두 개 이상의 ASA가 필요한 네트워크가 있음

상황 구성 파일

이 섹션에서는 ASA에서 다중 상황 모드 구성을 구현하는 방법을 설명합니다.

상황 구성

각 상황에서 ASA는 보안 정책, 인터페이스 그리고 독립형 디바이스에서 구성 가능한 모든 옵션을 나타내는 구성을 갖추고 있습니다. 상황 컨피그레이션을 플래시 메모리에 저장하거나 TFTP, FTP 또는 HTTP(S) 서버에서 다운로드할 수 있습니다.

시스템 구성

시스템 관리자는 시스템 구성에서 각 상황 컨피그레이션 위치, 할당된 인터페이스, 기타 상황 운영 매개 변수를 컨피그레이션함으로써 상황을 추가하고 관리합니다. 이는 단일 모드 컨피그레이션처럼 시작 컨피그레이션이 됩니다. 시스템 구성은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 구성은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 상황 다운로드) 관리 상황으로 지정된 상황 중 하나를 사용합니다. 시스템 구성은 장애 조치 트래픽만을 위한 전용 장애 조치 인터페이스를 포함합니다.

관리 상황 구성

관리 상황은 여느 상황과 비슷하지만, 사용자가 관리 상황에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 컨텍스트에 액세스할 수 있다는 점이 다릅니다. 관리 상황은 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 상황에 로그인하면 모든 상황에 대한 관리자 권한이 부여되므로, 관리 상황 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다. 관리 상황은 원격 위치가 아닌 플래시 메모리에 항상 있어야 합니다.

시스템이 이미 다중 상황 모드인 경우 또는 단일 모드에서 전환한 경우, 관리 상황이 내부 플래시 메모리에 admin.cfg라는 파일로 자동 생성됩니다. 이 상황의 이름은 “admin”입니다. admin.cfg를 관리 상황으로 사용하고 싶지 않다면 관리 상황을 변경할 수 있습니다.

ASA의 패킷 분류

ASA에 들어오는 각 패킷은 분류되어야 합니다. 그래야 ASA에서 어떤 상황에 패킷을 보낼지 판단할 수 있습니다.

참고 목적지 MAC 주소가 멀티캐스트 또는 브로드캐스트 MAC 주소인 경우 패킷이 복제되어 각 상황에 배포됩니다.

유효한 분류자 기준

이 섹션에서는 분류자에서 사용하는 기준에 대해 설명합니다.

참고 인터페이스로 갈 관리 트래픽에서는 인터페이스 IP 주소가 분류에 사용됩니다.

라우팅 테이블은 패킷 분류에 사용되지 않습니다.

고유 인터페이스

단 하나의 상황이 인그레스 인터페이스와 연결된 경우 ASA에서는 패킷을 해당 상황으로 분류합니다. 투명 방화벽 모드에서는 상황에 대한 고유 인터페이스가 필요합니다. 따라서 항상 패킷 분류에 이 방법이 사용됩니다.

고유 **MAC** 주소

여러 상황에서 하나의 인터페이스를 공유할 경우, 분류자는 각 상황에서 인터페이스에 할당된 고유 MAC 주소를 사용합니다. 업스트림 라우터는 고유 MAC 주소가 없으면 상황에 곧바로 라우팅할 수 없습니다. MAC 주소의 자동 생성을 활성화할 수 있습니다. 또한 각 인터페이스를 구성할 때 직접 MAC 주소를 설정할 수도 있습니다.

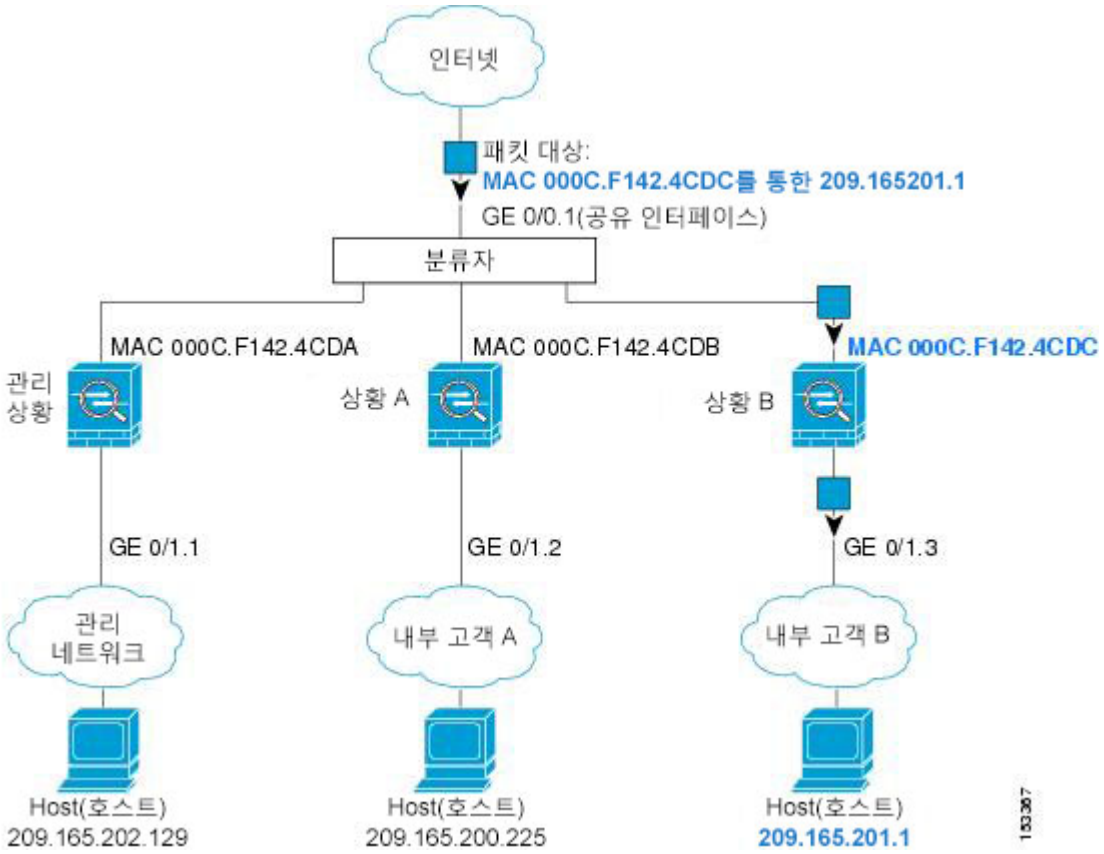
NAT 구성

고유 MAC 주소의 사용을 활성화하지 않는 경우 ASA에서는 NAT 구성의 매핑된 주소를 사용하여 패킷을 분류합니다. NAT 대신 MAC 주소를 사용하는 것이 좋습니다. 그러면 NAT 컨피그레이션의 완전성과 상관없이 트래픽 분류가 가능해집니다.

분류의 예

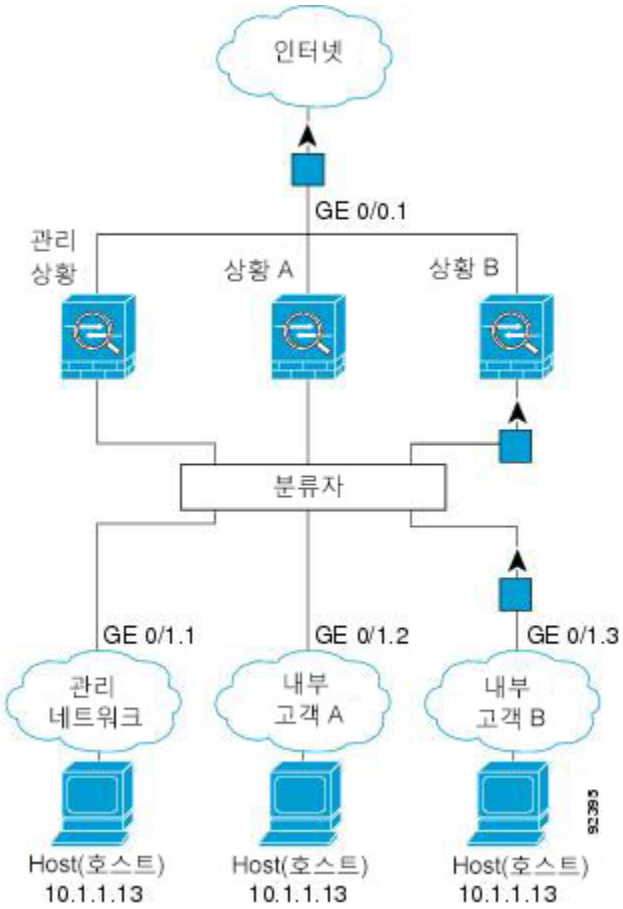
다음 그림에는 외부 인터페이스를 공유하는 여러 상황이 나와 있습니다. 분류자는 상황 B에 패킷을 지정합니다. 상황 B가 라우터에서 패킷을 보내는 패킷을 수신하는 MAC 주소를 포함하기 때문입니다.

그림 ***31: MAC*** 주소를 사용하는 공유 인터페이스를 통한 패킷 분류



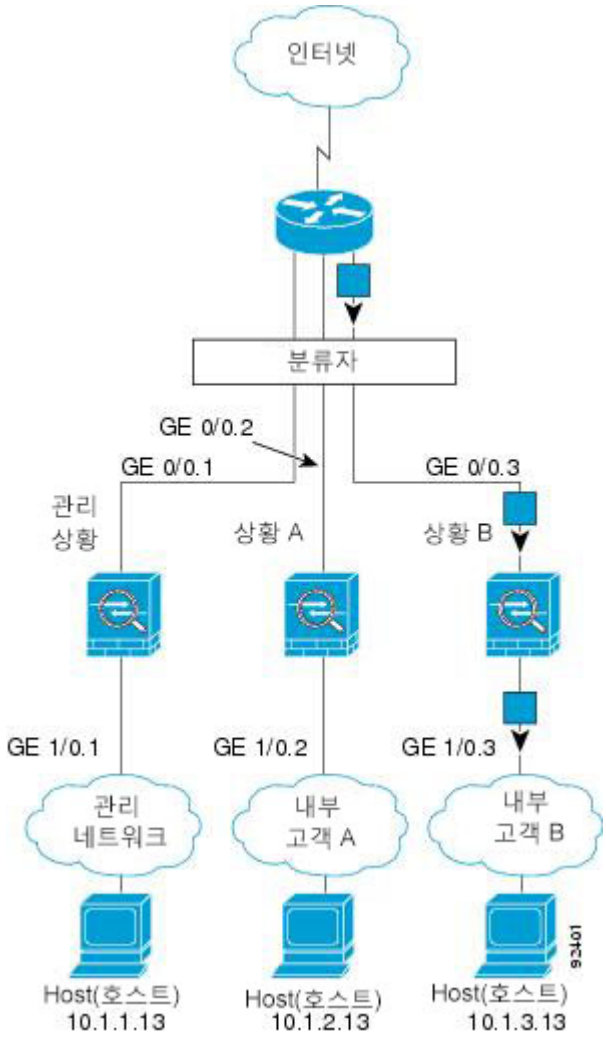
내부 네트워크에서 보낸 것을 비롯하여 모든 신규 수신 트래픽은 분류되어야 합니다. 다음 그림에는 인터넷에 액세스하는 네트워크 내부 상황 B에 있는 호스트가 나와 있습니다. 분류자는 상황 B에 패킷을 지정합니다. 인그레스 인터페이스가 상황 B에 지정되는 기가비트 이더넷 0/1.3이기 때문입니다.

그림 **32:** 내부 네트워크로부터 수신하는 트래픽



투명 방화벽의 경우 고유한 인터페이스를 사용해야 합니다. 다음 그림에는 인터넷의 네트워크 내부 상황 B에 있는 호스트로 향하는 패킷이 나와 있습니다. 분류자는 상황 B에 패킷을 지정합니다. 인그레스 인터페이스가 상황 B에 지정되는 기가비트 이더넷 1/0.3이기 때문입니다.

그림 ***33:*** 투명 방화벽 상황



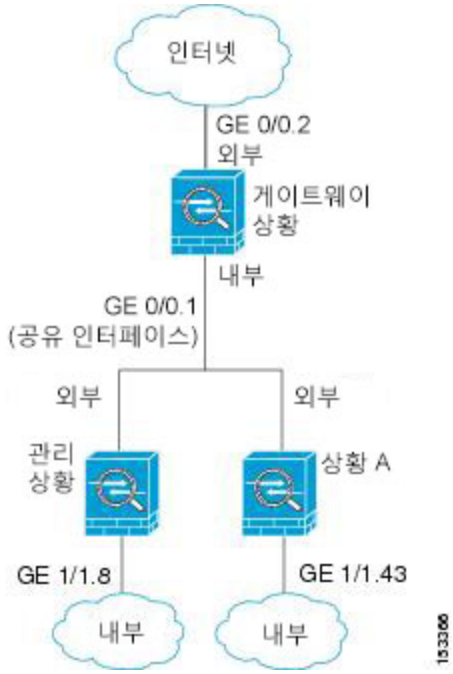
보안 상황 캐스케이딩

어떤 상황의 바로 앞에 다른 상황을 놓는 것을 상황 캐스케이딩이라고 합니다. 한 상황의 외부 인터페이스가 다른 상황의 내부 인터페이스가 됩니다. 최상위 상황에서 공유 매개 변수를 컨피그레이션함으로써 일부 상황의 컨피그레이션을 간소화하고 싶다면 상황 캐스케이딩이 유용할 수 있습니다.

참고 상황을 캐스케이딩하려면 상황 인터페이스별로 고유한 MAC 주소가 필요합니다. MAC 주소 없이 공유 인터페이스에서 패킷을 분류하면 여러 제약이 따라므로, 고유한 MAC 주소 없이 상황을 캐스케이딩하는 것은 권장되지 않습니다.

다음 그림에는 게이트웨이 뒤에 2개의 상황이 있는 게이트웨이 상황이 나와 있습니다.

그림 **34:** 상황 캐스케이딩



보안 상황에 대한 관리 액세스

ASA에서는 다중 상황 모드에서 시스템 관리자 액세스를 제공할 뿐만 아니라 개별 상황 관리자를 위한 액세스도 제공합니다. 다음 섹션에서는 시스템 관리자나 상황 관리자로 로그인하는 것에 대해 설명합니다.

시스템 관리자 액세스

다음과 같은 2가지 방법으로 ASA에 시스템 관리자로 액세스할 수 있습니다.

- ASA 콘솔에 액세스합니다.

  콘솔에서 시스템 실행 영역에 액세스합니다. 여기서 입력하는 모든 명령은 시스템 구성 또는 시스템 실행(런타임 명령의 경우)에만 영향을 줍니다.

- 텔넷, SSH 또는 ASDM을 사용하여 관리 상황에 액세스합니다.

시스템 관리자로서 모든 상황에 액세스할 수 있습니다.

시스템 실행 영역은 AAA 명령을 지원하지 않으므로, 로컬 데이터베이스에 자체 enable 비밀번호와 사용자 이름을 구성하여 개별 로그인을 제공할 수 있습니다.

상황 관리자 액세스

텔넷, SSH 또는 ASDM을 사용하여 상황에 액세스할 수 있습니다. 비 admin 상황으로 로그인한 경우 그 상황의 컨피그레이션만 액세스 가능합니다. 상황에 개별 로그인을 제공할 수 있습니다.

리소스 관리 정보

기본적으로 모든 보안 상황은 상황별 최대 제한이 적용되는 경우는 제외하고 ASA의 리소스에 무제한으로 액세스할 수 있습니다. 유일한 예외가 VPN 리소스인데, 이는 기본적으로 비활성화되어 있습니다. 하나 이상의 상황에서 너무 많은 리소스를 사용하고 있으며 그로 인해 다른 상황의 연결이 거부되는 것과 같은 상황이 벌어진다면, 컨텍스트별 리소스 사용을 제한하는 리소스 관리를 구성할 수 있습니다. VPN 리소스의 경우 임의의 VPN 터널을 허용하도록 리소스 관리를 구성해야 합니다.

리소스 클래스

ASA에서는 상황을 리소스 클래스에 할당하는 방법으로 리소스를 관리합니다. 각 컨텍스트는 해당 클래스에서 설정한 리소스 제한을 적용합니다. 어떤 클래스의 설정을 사용하려면 컨텍스트를 정의할 때 해당 클래스에 컨텍스트를 지정합니다. 모든 컨텍스트는 별도의 클래스에 지정되지 않는 한 기본 클래스에 속해 있습니다. 직접 기본 클래스에 컨텍스트를 지정할 필요는 없습니다. 하나의 컨텍스트는 하나의 리소스 클래스에만 지정할 수 있습니다. 이 규칙의 예외는 멤버 클래스에 정의되지 않은 제한이 기본 클래스로부터 상속되는 것입니다. 즉 컨텍스트는 기본 클래스와 또 다른 클래스의 멤버가 될 수 있습니다.

리소스 제한

개별 리소스에 대한 제한을 백분율(명시적 시스템 제한이 있는 경우) 또는 절대값으로 설정할 수 있습니다.

대부분의 리소스의 경우, ASA에서는 클래스에 할당된 각 상황에 어느 정도의 리소스를 따로 고려해 두지 않습니다. 오히려 ASA에서 상황의 최대 제한을 설정합니다. 리소스를 오버서브스크립션하거나 일부 리소스가 무제한이 되는 것을 허용할 경우, 몇몇 컨텍스트에서 이 리소스를 "소진"하여 다른 컨텍스트에 대한 서비스에 영향을 줄 수 있습니다. 오버서브스크립션할 수 없는 VPN 리소스 유형은 예외입니다. 즉 각 컨텍스트에 할당된 리소스가 보장됩니다. VPN 세션이 일시적으로 급증하여 할당량을 넘어서는 상황에 대비하여 ASA에서는 "버스트(burst)" VPN 리소스 유형을 지원합니다. 이는 할당되지 않은 나머지 VPN 세션과 같습니다. 버스트 세션은 오버서브스크립션될 수 있으며, 선착순으로 컨텍스트에 제공됩니다.

기본 클래스

모든 컨텍스트는 별도의 클래스에 지정되지 않는 한 기본 클래스에 속해 있습니다. 직접 기본 클래스에 컨텍스트를 지정할 필요는 없습니다.

어떤 컨텍스트가 기본 클래스가 아닌 클래스에 속할 경우, 항상 이 클래스의 설정이 기본 클래스의 설정에 우선합니다. 그러나 그 클래스에서 어떤 설정이 정의되지 않았다면 멤버 컨텍스트는 기본 클래스의 해당 제한을 적용합니다. 예를 들어, 모든 동시 연결에 대한 2% 제한이 있지만 그 밖의 어떤 제한도 없는 클래스를 만든다면 그 밖의 제한은 기본 클래스로부터 상속됩니다. 이와 달리 모든 리소스에 대해 제한이 있는 클래스를 만들 경우 이 클래스는 기본 클래스의 어떤 설정도 사용하지 않습니다.

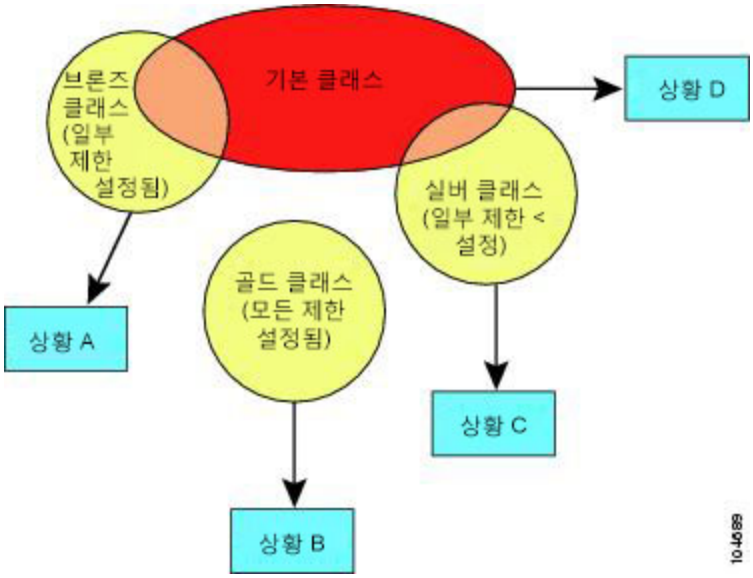
대부분의 리소스에서 기본 클래스는 다음 제한을 제외하고 모든 컨텍스트에 무제한적인 리소스 액세스를 제공합니다.

- 텔넷 세션 - 5개 세션 (컨텍스트당 최대 제한)

- SSH 세션 - 5개 세션 (컨텍스트당 최대 제한)
- IPsec 세션 - 5개 세션 (컨텍스트당 최대 제한)
- MAC 주소—65,535개 항목 (시스템의 최댓값)
- AnyConnect 피어 — 0개 세션 (AnyConnect 피어를 허용하려면 직접 클래스를 구성해야 함)
- VPN 사이트 대 사이트 터널 - 0개 세션 (VPN 세션을 허용하려면 직접 클래스를 구성해야 함)

다음 그림에는 기본 클래스와 다른 클래스의 관계가 나와 있습니다. 컨텍스트 A와 C는 몇 가지 제한이 설정된 클래스에 속해 있습니다. 다른 제한은 기본 클래스로부터 상속됩니다. 컨텍스트 B는 기본 클래스에서 어떤 제한도 상속하지 않습니다. 모든 제한이 설정되어 있는 골드 클래스에 속해 있기 때문입니다. 컨텍스트 D는 클래스에 지정되지 않았으므로, 기본적으로 기본 클래스의 멤버입니다.

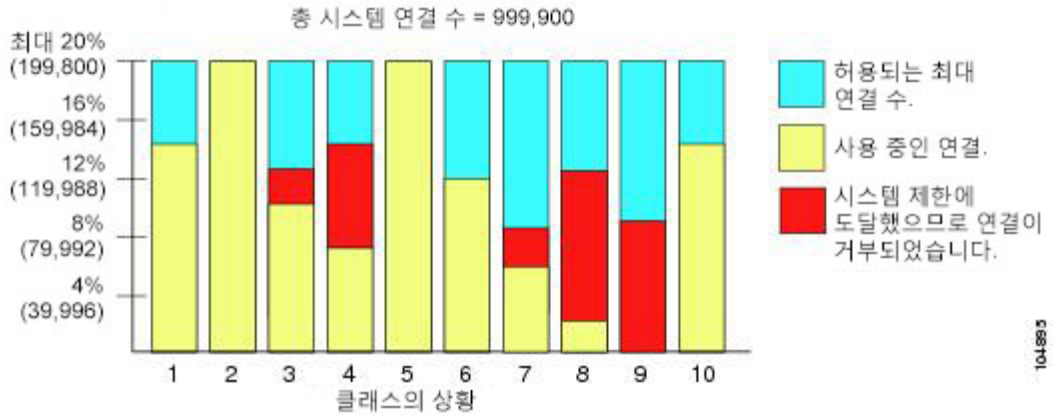
그림 ***35:*** 리소스 클래스



오버서브스크립션된 리소스 사용

모든 상황을 통틀어 100%가 넘는 리소스를 할당함으로써 ASA를 오버서브스크립션할 수 있습니다 (버스트 이외 VPN 리소스는 제외). 이를테면 컨텍스트당 20%로 연결을 제한하도록 Bronze 클래스를 설정한 다음 이 클래스에 10개의 컨텍스트를 지정하여 총 200%가 되게 할 수 있습니다. 컨텍스트가 동시에 시스템 제한을 초과하여 사용할 경우 각 컨텍스트는 원래 의도했던 20%보다 적게 받습니다.

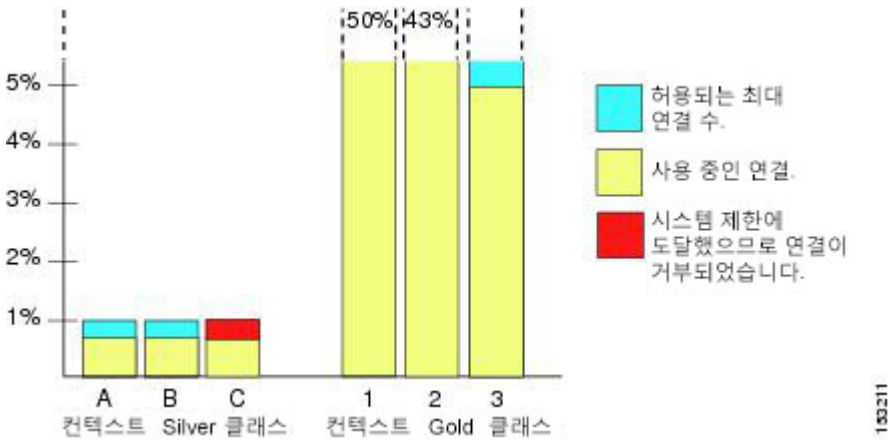
그림 ***36:*** 리소스 오버서브스크립션



무제한 리소스 사용

ASA를 통해 클래스의 하나 이상의 리소스에 백분율이나 절대값이 아닌 무제한 액세스 권한을 할당할 수 있습니다. 어떤 리소스가 무제한이 되면 컨텍스트는 시스템의 가용 제한에서 그 리소스를 최대한 많이 사용할 수 있습니다. 이를테면 컨텍스트 A, B, C는 실버 클래스인데, 이 클래스는 각 멤버를 연결의 1%로 제한하므로 총 3%가 됩니다. 그러나 이 세 컨텍스트는 현재 모두 합쳐 2%만 사용하고 있습니다. 골드 클래스는 무제한으로 연결에 액세스합니다. 골드 클래스의 컨텍스트는 "할당되지 않은" 연결을 97% 넘게 사용할 수 있습니다. 또한 현재 컨텍스트 A, B, C에서 사용하지 않는 1% 연결도 사용 가능합니다. 그러면 컨텍스트 A, B, C는 주어진 제한(총 3%)만큼 사용할 수 없게 됩니다. 무제한 액세스 설정은 ASA의 오버서브스크립션과 비슷하지만, 시스템의 오버서브스크립션 용량을 그만큼 제어하지는 않습니다.

그림 ***37:*** 무제한 리소스



MAC 주소 정보

MAC 주소를 수동으로 할당하여 기본값을 재정의할 수 있습니다. 다중 컨텍스트 모드의 경우 특정컨텍스트에 할당된 모든 인터페이스에 대해 고유한 MAC 주소를 자동으로 생성할 수 있습니다.

참고 ASA에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있어 ASA의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

다중 컨텍스트 모드의 **MAC** 주소

이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다. 어떤 인터페이스를 공유하지만 각 컨텍스트에서 그 인터페이스에 대한 고유한 MAC 주소가 없을 경우, 다른 분류 방법을 시도하는데 전 범위를 포괄하지 못할 수도 있습니다.

컨텍스트가 인터페이스를 공유할 수 있도록 하려면 각 공유 컨텍스트 인터페이스에 대해 가상 MAC 주소 자동 생성을 활성화해야 합니다. ASASM에서만 자동 생성이 다중 컨텍스트 모드에서 기본적으로 활성화됩니다.

자동 **MAC** 주소

다중 컨텍스트 모드에서는 자동 생성 기능이 특정 컨텍스트에 할당된 모든 인터페이스에 고유한 MAC 주소를 할당합니다.

직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우 직접 지정한 수동 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 제거하면 자동 생성 주소가 사용됩니다(활성화된 경우).

드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 해당 인터페이스의 MAC 주소를 직접 설정할 수 있습니다.

자동 생성 주소는 (접두사 사용 시) A2로 시작하므로, 자동 생성도 사용하려는 경우 수동 MAC 주소가 A2로 시작해서는 안 됩니다.

ASA에서는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx.yyzz.zzzz*

여기서 *xx.yy*는 사용자가 정의한 접두사이거나 인터페이스 MAC 주소의 마지막 2바이트에 근거하여 자동 생성된 접두사이며, *zz.zzzz*는 ASA에서 생성한 내부 카운터입니다. 스탠바이 MAC 주소는 동일하지만, 내부 카운터가 1만큼 증가합니다.

접두사 사용 방식의 예를 들자면, 접두사를 77로 설정한 경우 ASA에서는 77을 16진수 값인 004D(*yyxx*)로 변환합니다. 접두사를 MAC 주소에서 사용하는 경우 다음과 같이 ASA 기본 형식에 부합하도록 역전됩니다(*xxyy*).

A2**4D.00***zz.zzzz*

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2**F1.03***zz.zzzz*

참고 접두사가 없는 MAC 주소 형식은 레거시 버전입니다. 레거시 형식에 대한 자세한 내용은 명령 참조에서 **mac-address auto** 명령을 참조하십시오.

VPN 지원

VPN 리소스의 경우 임의의 VPN 터널을 허용하도록 리소스 관리를 구성해야 합니다.

다중 상황 모드에서 Site-to-Site VPN을 사용할 수 있습니다.

원격 액세스 VPN의 경우 SSL VPN 및 IKEv2 프로토콜에 AnyConnect 3.x 이상 버전을 사용해야 합니다. 모든 상황을 통틀어 공유 플래시 메모리를 사용할 뿐만 아니라 AnyConnect 이미지 및 맞춤화를 위해 상황별로 플래시 스토리지를 맞춤화할 수 있습니다. 지원되지 않는 기능은 다중 상황 모드를 위한 지침, 230 페이지의 내용을 참조하십시오. ASA 릴리스별로 지원되는 VPN 기능의 상세 목록은 다중 상황 모드의 내역, 260 페이지의 내용을 참조하십시오.

참고 다중 상황 모드에서 AnyConnect Apex 라이선스가 필요합니다. 기본 라이선스 또는 레거시 라이선스는 사용할 수 없습니다.

다중 상황 모드를 위한 라이센싱

모델	라이센스 요건
ASA 5506-X	지원 안 함
ASA 5508-X	Security Plus 라이센스: 2개 컨텍스트 선택적 라이센스: *5*개 컨텍스트
ASA 5512-X	• Base 라이센스: 지원 안 함 • Security Plus 라이센스: 2개 컨텍스트 선택적 라이센스: *5*개 컨텍스트
ASA 5515-X	Base 라이센스: 2개 컨텍스트 선택적 라이센스: *5*개 컨텍스트
ASA 5516-X	Security Plus 라이센스: 2개 컨텍스트 선택적 라이센스: *5*개 컨텍스트
ASA 5525-X	Base 라이센스: 2개 컨텍스트 선택적 라이센스: *5, 10* 또는 *20*개 컨텍스트

모델	라이센스 요건
ASA 5545-X	Base 라이센스: 2개 컨텍스트 선택적 라이센스*: 5, 10, 20* 또는 *50*개 컨텍스트
ASA 5555-X	Base 라이센스: 2개 컨텍스트 선택적 라이센스*: 5, 10, 20* 또는 *50*개 컨텍스트
ASA 5585-X(SSP-10 포함)	Base 라이센스: 2개 컨텍스트 선택적 라이센스*: 5, 10, 20* 또는 *50*개 컨텍스트
ASA 5585-X(SSP-20, -40 및 -60 포함)	Base 라이센스: 2개 컨텍스트 선택적 라이센스*: 5, 10, 20, 50, 100* 또는 *250*개 컨텍스트
ASASM	Base 라이센스: 2개 컨텍스트 선택적 라이센스*: 5, 10, 20, 50, 100* 또는 *250*개 컨텍스트
Firepower 2100의 ASA	Base 라이센스: 2개 컨텍스트 선택적 라이선스, 증가 시 최대값은 *5* 또는 *10*입니다. *Firepower 2110: 25*개 *Firepower 2120: 25*개 *Firepower 2130: 30*개 *Firepower 2140: 40*개
Firepower 4100의 ASA	Base 라이선스: 10개 상황 *(*선택 사항*)* 라이선스*:* 최대 *250*개의 상황*, 10*씩 증가
Firepower 9300의 ASA	Base 라이선스: 10개 상황 선택적 라이선스*:* 최대 *250*개의 상황*, 10*씩 증가
ISA 3000	지원 안 함
ASAv	지원 안 함

참고 다중 상황 모드에서 AnyConnect Apex 라이선스가 필요합니다. 기본 라이선스 또는 레거시 라이선스는 사용할 수 없습니다.

다중 상황 모드의 사전 요구 사항

다중 상황 모드에 들어온 다음 시스템 또는 관리 상황에 연결하여 시스템 구성에 액세스합니다. 비 관리 상황에서 시스템을 구성할 수 없습니다. 기본적으로 다중 상황 모드를 활성화한 다음에는 기본 관리 IP 주소를 사용하여 관리 상황에 연결할 수 있습니다.

다중 상황 모드를 위한 지침

페일오버

활성/활성(Active/Active) 모드 장애 조치는 다중 상황 모드에서만 지원됩니다.

IPv6

교차 상황 IPv6 라우팅은 지원되지 않습니다.

지원되지 않는 기능

다중 상황 모드는 다음 기능을 지원하지 않습니다.

- RIP
- OSPFv3. (OSPFv2는 지원)
- 멀티캐스트 라우팅
- 위협 탐지
- 통합 통신
- QoS

다중 상황 모드는 현재 원격 액세스 VPN에 대해 다음 기능을 지원하지 않습니다.

- AnyConnect 2.x 이하 버전
- IKEv1
- WebLaunch
- VLAN 매핑
- HostScan
- VPN 로드 밸런싱
- 맞춤 설정
- L2TP/IPsec

추가 지침

- (단일 또는 다중) 상황 모드는 재부팅할 때 유지되더라도 컨피그레이션 파일에 저장되지 않습니다. 컨피그레이션을 다른 디바이스에 복사하려면 새 디바이스의 모드를 일치하게 설정합니다.
- 플래시 메모리의 루트 디렉터리에 컨텍스트 컨피그레이션을 저장할 경우, 일부 모델에서는 가용 메모리가 있더라도 이 디렉터리의 공간이 부족해질 수 있습니다. 그러한 경우 컨피그레이션 파일을 위한 하위 디렉터리를 만듭니다. 배경 정보: ASA 5585-X와 같은 일부 모델에서는 내부 플래시 메모리에 FAT 16 파일 시스템을 사용합니다. 그리고 8.3 규격의 짧은 이름을 사용하지 않거나 대문자를 사용할 경우, 저장 가능한 파일 및 폴더는 512개보다 적습니다. 파일 시스템에서 긴 파일 이름을 저장하는 데 슬롯을 사용하기 때문입니다 (http://support.microsoft.com/kb/120138/en-us 참조).

다중 상황 모드에 대한 기본값

- 기본적으로 ASA는 단일 상황 모드입니다.
- 기본 클래스, 224 페이지를 참조하십시오.

다중 상황 구성

프로시저

단계 **1** 다중 상황 모드 활성화 또는 비활성화, 232 페이지.

단계 **2** (선택 사항) 리소스 관리를 위한 클래스 구성, 233 페이지

참고 VPN을 지원하려면 리소스 클래스에 VPN 리소스를 구성해야 합니다. 기본 클래스는 VPN을 허용하지 않습니다.

단계 **3** 시스템 실행 영역에서 인터페이스를 구성합니다.

- ASA 5500-X — 기본 인터페이스 구성, 555 페이지
- ASASM — ASASM 빠른 시작 가이드입니다.

단계 **4** 보안 상황 구성, 237 페이지.

단계 **5** (선택 사항) 상황 인터페이스에 자동으로 MAC 주소 할당, 242 페이지.

단계 **6** 컨텍스트에서 인터페이스 컨피그레이션을 완료합니다. 라우팅 및 투명 모드 인터페이스, 609 페이지를 참조하십시오.

다중 상황 모드 활성화 또는 비활성화

Cisco에 주문한 내용에 따라 ASA에서 이미 다중 보안 상황이 구성되었을 수도 있습니다. 단일 모드에서 다중 모드로 전환하려면 이 섹션의 절차를 따르십시오.

다중 상황 모드 활성화

단일 모드에서 다중 모드로 전환할 때 ASA에서는 실행 중인 구성을 2개 파일, 즉 시스템 구성을 이루는 새 시작 구성과 관리 상황을 이루는 admin.cfg(내부 플래시 메모리의 루트 디렉터리에서)로 변환합니다. 원래의 실행 중 컨피그레이션은 old_running.cfg로 (내부 플래시 메모리의 루트 디렉터리에) 저장됩니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. ASA에서는 관리 상황 항목을 "admin"이라는 이름으로 시스템 구성에 자동 추가합니다.

시작하기 전에

시작 컨피그레이션을 백업합니다. 단일 모드에서 다중 모드로 전환할 때 ASA에서는 실행 중인 구성을 2개 파일로 변환합니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. 구성 또는 기타 파일 백업 및 복원, 1176 페이지을 참조하십시오.

프로시저

다중 상황 모드로 변경:

mode multiple

예제**:**

```
ciscoasa(config)# mode multiple
```

ASA를 재부팅하라는 프롬프트가 나타납니다.

단일 상황 모드 복원

기존의 실행 중 컨피그레이션을 시작 컨피그레이션에 복사하고 모드를 단일 모드로 변경하려면 다음 단계를 수행합니다.

시작하기 전에

시스템 실행 영역에서 이 절차를 수행합니다.

프로시저

단계 **1** 원래 실행 중 구성의 백업 버전을 현재 시작 구성에 복사합니다.

copy disk0:old_running.cfg startup-config

예제:

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

단계 **2** 모드를 단일 모드로 설정:

mode single

예제:

```
ciscoasa(config)# mode single
```

ASA를 재부팅하라는 메시지가 나타납니다.

리소스 관리를 위한 클래스 구성

시스템 구성에서 클래스를 컨피그레이션하려면 다음 단계를 수행합니다. 새 값으로 명령을 다시 입력하여 특정 리소스 제한의 값을 변경할 수 있습니다.

시작하기 전에

- 시스템 실행 영역에서 이 절차를 수행합니다.
- 다음 표에는 리소스 유형과 제한이 나와 있습니다. **show resource types** 명령도 참조하십시오.

참고 시스템 제한이 N/A이면 해당 리소스에 대한 명시적 시스템 제한이 없으므로 리소스의 비율을 설정할 수 없습니다.

표 ***6:*** 리소스 이름 및 제한

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한	설명
asdm	동시	최소 1 최대 20개	32	ASDM 관리 세션입니다. ASDM 세션에서는 2개의 HTTPS 연결을 사용합니다. 하나는 모니터링용으로 항상 실행되며 다른 하나는 구성 변경용으로, 변경할 때만 실행됩니다. 예를 들어, 시스템 제한이 32개의 ASDM 세션이라면 64개의 HTTPS 세션을 의미합니다.

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한	설명
conns	동시 또는 비율	해당 없음	동시 연결: 해당 모델의 연결 제한은 모델당 지원되는 기능 라이센스, 76 페이지를 참조하십시오. 비율: N/A	임의의 두 호스트 간의 TCP 또는 UDP 연결입니다(단일 호스트와 여러 다른 호스트 간의 연결 포함). 참고 xlate 또는 conn 중 제한이 더 낮은 하나에 대해 syslog 메시지가 생성됩니다. 예를 들어, xlate 제한을 7로, conn을 9로 설정한 경우 ASA에서는 syslog message 321001("Resource 'xlates' limit of 7 reached for context 'ctx1'")만 생성합니다. 321002("Resource 'conn rate' limit of 5 reached for context 'ctx1'")는 생성하지 않습니다.
호스트	동시	해당 없음	해당 없음	ASA를 통해 연결할 수 있는 호스트입니다.
inspects	비율	해당 없음	해당 없음	초당 애플리케이션 검사 수입니다.
mac-addresses	동시	해당 없음	65,535	투명 방화벽 모드의 경우 MAC 주소 테이블에서 허용되는 MAC 주소의 수입니다.
routes	동시	해당 없음	해당 없음	동적 경로입니다.
vpn burst anyconnect	동시	해당 없음	사용 중인 모델의 AnyConnect Premium 피어에서 **vpn anyconnect**에 대한 모든 상황에 할당된 합계를 뺀 값입니다.	**vpn anyconnect**을 통해 상황에 할당된 양을 초과하는 허용된 AnyConnect 세션의 수입니다. 예를 들어, 모델이 5000개의 피어를 지원하고 **vpn anyconnect**를 통해 모든 상황에서 4000개의 피어를 할당하면 나머지 1,000개의 세션을 **vpn burst anyconnect**에 사용할 수 있습니다. 상황에 대한 세션을 보장하는 **vpn anyconnect**와 달리 **vpn burst anyconnect**에서는 오버서브스크립션이 가능합니다. 버스트 풀은 모든 상황에서 선착순으로 사용할 수 있습니다.

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한	설명
vpn anyconnect	동시	해당 없음	사용 중인 모델에 사용할 수 있는 AnyConnect Premium 피어에 대해서는 모델당 지원되는 기능 라이센스, 76 페이지의 내용을 참조하십시오.	AnyConnect 피어입니다. 이 리소스는 오버서브스크립션할 수 없습니다. 모든 컨텍스트의 할당량 합계가 모델의 제한을 초과할 수 없습니다. 이 리소스에 대해 할당하는 피어는 해당 상황에 보장됩니다.
vpn burst other	동시	해당 없음	해당 모델의 기타 VPN 세션의 양에서 에 할당된 세션의 합계를 뺀 값입니다.	로 상황에 할당된 양을 초과하는 허용된 Site-to-Site VPN 세션 수입니다. 예를 들어, 모델에서 세션 5,000개를 지원하는데 **vpn other**으로 상황 전체에 세션 4,000개를 할당한 경우 나머지 1,000개 세션은 **vpn burst other**에서 사용 가능합니다. 상황에 대한 세션을 보장하는 **vpn other**와 달리, **vpn burst other**에서는 오버서브스크립션이 가능합니다. 버스트 풀은 모든 상황에서 선착순으로 사용할 수 있습니다.
vpn other	동시	해당 없음	해당 모델에서 사용 가능한 기타 VPN 세션은 모델당 지원되는 기능 라이센스, 76 페이지를 참조하십시오.	사이트 대 사이트 VPN 세션. 이 리소스는 오버서브스크립션할 수 없습니다. 모든 컨텍스트의 할당량 합계가 모델의 제한을 초과할 수 없습니다. 이 리소스에 대해 할당하는 세션은 해당 컨텍스트에 보장됩니다.
ikev1 in-negotiation	동시(백분율만 해당)	해당 없음	이 상황에 할당된 기타 VPN 세션의 백분율입니다. 세션을 상황에 할당하려면 **vpn other** 리소스를 참조하십시오.	수신 IKEv1 SA 협상입니다(상황 기타 VPN 제한의 백분율로 사용됨).
ssh	동시	최소 1 최대 5	100	SSH 세션입니다.
스토리지	MB	최댓값은 지정된 플래시 메모리 드라이브에 따라 달라집니다.	최대값은 지정된 플래시 메모리 드라이브에 따라 달라집니다.	상황 디렉터리의 스토리지 제한입니다(MB 단위). **storage-url** 명령을 사용하여 드라이브를 지정합니다.
syslogs	비율	해당 없음	해당 없음	초당 syslog 메시지 수입니다.

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한	설명
telnet	동시	최소 1 최대 5	100	텔넷 세션입니다.
xlates	동시	해당 없음	해당 없음	네트워크 주소 변환입니다.

프로시저

단계 **1** 클래스 이름을 지정하고 클래스 구성 모드를 입력합니다.

class *name*

예제**:**

```
ciscoasa(config)# class gold
```

*name*은 최대 20자의 문자열입니다. 기본 클래스에 대해 이 제한을 설정하려면 **default**를 이름으로 입력합니다.

단계 **2** 리소스 유형에 대한 리소스 제한을 설정합니다.

limit-resource [**rate**] *resource_name number*[**%**]

예제**:**

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- 리소스 유형의 목록은 앞의 표를 참조하십시오. **all**을 지정하면 모든 리소스가 동일한 값으로 구성됩니다. 특정 리소스에 대해 값을 지정할 경우 그 제한이 **all**에 설정된 제한에 우선합니다.
- **rate** 인수를 입력하여 특정 리소스에 대해 초당 비율을 설정할 수 있습니다.
- 대부분의 리소스는 *number*에 **0**을 지정하여 리소스를 무제한으로 설정하거나 시스템 제한(있는 경우)까지 사용하게 합니다. VPN 리소스의 경우 **0**은 제한을 none으로 설정합니다.
- 시스템 제한이 없는 리소스는 백분율(**%**)을 설정할 수 없습니다. 절대값만 설정 가능합니다.

예

이를테면 conns의 기본 클래스 제한을 무제한 대신 10%로 설정하고 5개의 사이트 대 사이트 VPN 터널을 허용하되 VPN 버스트로 2개 터널을 허용하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

```
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

다른 모든 리소스는 무제한으로 유지됩니다.

gold라는 클래스를 추가하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

상황이 리소스 클래스로 구성된 경우, 검사가 수행됩니다. VPN 원격 액세스 연결을 시도하기 전에 적절한 라이선스가 설치되지 않은 경우 경고가 생성됩니다. 그러면 관리자는 AnyConnect Apex 라이선스를 확보해야 합니다. 예를 들어, 다음과 같은 경고가 표시될 수 있습니다.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

보안 상황 구성

시스템 구성의 보안 컨텍스트 정의는 상황 이름, 컨피그레이션 파일 URL, 컨텍스트에서 사용할 수 있는 인터페이스 및 기타 설정을 나타냅니다.

시작하기 전에

- 시스템 실행 영역에서 이 절차를 수행합니다.
- ASASM의 경우, ASASM 빠른 시작 가이드에 따라 스위치의 ASASM에 VLAN을 할당합니다.
- ASA 5500-X의 경우 기본 인터페이스 구성, 555 페이지에 따라 물리적 인터페이스 파라미터, VLAN 하위 인터페이스, EtherChannel, 이중 인터페이스를 구성합니다.
- 관리 상황이 없는 경우(예: 이 컨피그레이션을 지웠음) 먼저 다음 명령을 입력하여 관리 상황 이름을 지정해야 합니다.

```
ciscoasa(config)# admin-context name
```

이 컨텍스트는 아직 컨피그레이션에 없지만, 그 다음에 **context** *name* 명령을 입력하여 관리 상황 컨피그레이션을 계속할 수 있습니다.

프로시저

단계 **1** 상황 추가 또는 수정:

context *name*

예제**:**

```
ciscoasa(config)# context admin
```

*name*은 최대 32자의 문자열입니다. 이 이름은 대/소문자를 구분합니다. 즉 "customerA"와 "CustomerA"는 2개의 컨텍스트입니다. 문자, 숫자 또는 하이픈을 사용할 수 있으나 하이픈으로 이름을 시작하거나 끝내서는 안 됩니다.

참고 "System"과 "Null"(대문자 및 소문자 모두 해당)은 예약된 이름이므로 사용할 수 없습니다.

단계 **2** (선택 사항) 이 상황에 대한 설명을 추가합니다.

description 텍스트

예제**:**

```
ciscoasa(config-ctx)# description Admin Context
```

단계 **3** 상황에서 사용할 수 있는 인터페이스를 지정합니다.

인터페이스를 할당하려면

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

하나 이상의 하위 인터페이스를 할당하려면

allocate-interface *interface_id***.***subinterface* [**-***interface_id***.***subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**]

예제**:**

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

참고 인터페이스 유형과 포트 번호 사이에 공백을 넣지 마십시오.

- 여러 범위를 지정하려면 이 명령을 여러 번 입력합니다. 이 명령의 **no** 형식을 사용하여 할당을 삭제한 경우 이 인터페이스를 포함한 모든 상황 명령이 실행 중인 구성에서 삭제됩니다.
- 투명 방화벽 모드에서는 제한된 수의 인터페이스에서 트래픽을 전달하는 것이 허용됩니다. 그러나 전용 관리 인터페이스인 관리 슬롯/포트(물리적, 하위 인터페이스, 이중 또는 EtherChannel)

를 추가 관리 트래픽 인터페이스로 사용할 수 있습니다. ASASM을 위한 별도의 관리 인터페이스는 제공되지 않습니다.

- 라우팅 모드에서는 원한다면 여러 컨텍스트에 동일한 인터페이스를 지정할 수 있습니다. 투명 모드에서는 공유 인터페이스를 허용하지 않습니다.
- *mapped_name*은 인터페이스의 영숫자 별칭으로, 상황 내에서 인터페이스 ID 대신 사용할 수 있습니다. 매핑된 이름을 지정하지 않으면 인터페이스 ID가 컨텍스트 내에서 사용됩니다. 보안상의 이유로, 컨텍스트에서 어떤 인터페이스를 사용하고 있는지 컨텍스트 관리자에게 알리고 싶지 않을 수 있습니다. 매핑된 이름은 문자로 시작하고 문자 또는 숫자로 끝나며, 나머지 자리에는 문자, 숫자, 밑줄만 사용할 수 있습니다. 예를 들어 **int0**, **inta**, **int_0** 등의 이름을 사용할 수 있습니다.
- 하위 인터페이스의 이름을 지정할 경우 매핑된 이름의 매칭 범위를 지정할 수 있습니다. 범위에 대한 다음 지침을 따르십시오.
  - 매핑된 이름은 영문자 다음에 숫자가 와야 합니다. 매핑된 이름에서 영문자 부분은 범위의 양쪽 경계에 매칭해야 합니다. 예를 들어, **int0-int10** 등의 범위를 입력합니다. 예를 들어, gig0/1.1-gig0/1.5 **happy**1-**sad**5라고 입력하면 명령은 실패합니다.
  - 매핑된 이름의 숫자 부분은 하위 인터페이스 범위와 동일한 개수의 숫자를 포함해야 합니다. 예를 들어, 두 범위 모두 100개의 인터페이스를 포함합니다 (**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**). 예를 들어, gig0/0.**100**-gig0/0.**199** int**1**-int**15**라고 입력하면 명령은 실패합니다.
- 매핑된 이름을 설정한 경우 **show interface** 명령에서 실제 인터페이스 ID를 보려면 **visible**을 지정합니다. 기본 **invisible** 키워드를 사용하면 매핑된 이름만 표시됩니다.

단계 **4** 시스템이 상황 구성을 다운로드할 URL을 나타냅니다.

config-url *url*

예제**:**

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

단계 **5** (선택 사항) 각 상황에서 플래시 메모리를 사용하여 VPN 패키지(예: AnyConnect)를 저장하도록 허용하면서, AnyConnect 및 클라이언트리스 SSL VPN 포털 맞춤화를 위해 스토리지를 제공합니다. 예를 들어, 다중 상황 모드를 사용하여 Dynamic Access Policies를 포함하는 AnyConnect 프로필을 구성하는 경우 상황별 프라이빗 스토리지를 계획해야 합니다. 각 상황에서 공유 읽기 전용 스토리지 공간뿐만 아니라 프라이빗 스토리지 공간을 사용할 수 있습니다. 참고**: mkdir** 명령을 사용하여 대상 디렉터리가 지정된 디스크에 이미 있는지 확인하십시오.

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

예제**:**

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
```

```
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

상황별로 1개의 **private** 스토리지 공간을 지정할 수 있습니다. 상황 내에서 이 디렉터리를 읽기/쓰기/삭제할 수 있습니다(시스템 실행 공간에서도 가능). 디스크 수를 지정하지 않으면 기본값은 disk0입니다. 지정된 경로에서 ASA는 상황의 이름을 따서 하위 디렉터리를 생성합니다. 예를 들어, contextA에서 경로에 **disk1:/private-storage**를 지정하는 경우 ASA에서는 **disk1:/private-storage/contextA/**에서 이 상황에 대해 하위 디렉터리를 생성합니다. 또한 원하는 경우 파일 시스템이 상황 관리자에게 노출되지 않도록 *context_label*을 사용하여 상황 내에서 경로의 이름을 지정할 수 있습니다. 예를 들어, *context_label*을 **context**로 지정하는 경우, 상황 내부에서 이 디렉터리를 **context:**라고 부릅니다. 상황별로 얼마나 많은 디스크 공간이 허용되는지 제어하려면 리소스 관리를 위한 클래스 구성, 233 페이지의 내용을 참조하십시오.

상황별로 읽기 전용 **shared** 스토리지 공간을 지정할 수 있지만 여러 공유 디렉터리를 생성할 수 있습니다. AnyConnect 패키지와 같이 모든 상황에서 공유 가능한 일반적인 큰 파일의 중복을 줄이기 위해 공유 스토리지 공간을 사용할 수 있습니다. 이 스토리지 공간은 다중 상황에 대한 공유 공간이므로 ASA에서는 이에 대해 상황의 하위 디렉터리를 생성하지 않습니다. 시스템 실행 영역만 공유 디렉터리에서 작성 및 삭제할 수 있습니다.

단계 **6** (선택 사항) 리소스 클래스에 상황을 할당합니다.

member *class_name*

예제**:**

```
ciscoasa(config-ctx)# member gold
```

클래스를 지정하지 않으면 컨텍스트는 기본 클래스에 속합니다. 하나의 컨텍스트는 하나의 리소스 클래스에만 지정할 수 있습니다.

단계 **7** (선택 사항) IPS 모듈이 설치된 경우 이 상황에 IPS 가상 센서를 할당합니다.

allocate-ips *sensor_name* [*mapped_name*] [**default**]

예제**:**

```
ciscoasa(config-ctx)# allocate-ips sensor1 highsec
```

가상 센서에 대한 자세한 내용은 IPS 빠른 시작 가이드를 참조하십시오.

- 컨텍스트 URL을 추가하면, 해당 컨피그레이션이 사용 가능한 경우 시스템에서 즉시 컨텍스트를 로드하므로 실행 중이 됩니다.
- allocate-interface 명령을 **config-url** 명령보다 먼저 입력합니다. **config-url** 명령을 먼저 입력하면 ASA에서는 즉시 상황 구성을 로드합니다. 컨텍스트에 (아직 구성되지 않은) 인터페이스를 참조하는 명령이 있을 경우 그 명령은 실패합니다.
- 파일 이름에서 확장자가 필요하지는 않지만 ".cfg"를 사용하는 것이 좋습니다. 서버는 관리 상황에서 액세스할 수 있어야 합니다. 구성 파일을 사용할 수 없는 경우 다음 경고 메시지가 표시됩니다.

```
WARNING: Could not fetch the URL url
```

```
INFO: Creating context with default config
```

- 비 HTTP(S) URL 위치의 경우, URL을 지정한 다음 상황으로 바꾸고 CLI에서 구성할 수 있습니다. 그리고 **write memory** 명령을 입력하여 URL 위치에 파일을 쓸 수 있습니다. HTTP(S)는 읽기 전용입니다.
- 관리 상황 파일은 내부 플래시 메모리에 저장해야 합니다.
- 사용 가능한 URL 유형으로는 **disk***number*(플래시 메모리의 경우), **ftp**, **http**, **https** 또는 **tftp** 등이 있습니다.
- URL을 변경하려면 새 URL과 함께 config-url 명령을 다시 입력합니다.

단계 **8** (선택 사항) 액티브/액티브 장애 조치에서 장애 조치 그룹에 상황을 할당합니다.
join-failover-group {**1** | **2**}

예제**:**

```
ciscoasa(config-ctx)# join-failover-group 2
```

기본적으로 컨텍스트는 그룹 1에 있습니다. 관리 상황은 항상 그룹 1에 있어야 합니다.

단계 **9** (선택 사항) 이 상황에서 Cloud Web Security를 활성화합니다.
scansafe [**license** *key*]

예제**:**

```
ciscoasa(config-ctx)# scansafe
```

license를 지정하지 않으면 상황은 시스템 구성에 구성된 라이선스를 사용합니다. ASA에서는 Cloud Web Security 프록시 서버에 인증 키를 보내 어떤 조직에서 요청을 보냈는지 알립니다. 인증 키는 16바이트 16진수입니다.

ScanSafe에 대한 자세한 내용은 방화벽 구성 가이드를 참조하십시오.

예

다음 예에서는 관리 상황을 "administrator"가 되게 설정하고 내부 플래시 메모리에 "administrator"라는 컨텍스트를 만든 다음 FTP 서버에서 2개의 컨텍스트를 추가합니다.

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
```

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

상황 인터페이스에 자동으로 **MAC** 주소 할당

이 섹션에서는 MAC 주소의 자동 생성을 구성하는 방법을 설명합니다. 이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다.

시작하기 전에

- 상황에서 인터페이스에 대해 **nameif** 명령을 구성하면 새 MAC 주소가 즉시 생성됩니다. 컨텍스트 인터페이스를 구성한 다음 이 기능을 활성화한 경우, 활성화한 직후에 모든 인터페이스에 대해 MAC 주소가 생성됩니다. 이 기능을 비활성화한 경우 각 인터페이스의 MAC 주소가 기본 MAC 주소로 돌아갑니다. 예를 들어, GigabitEthernet 0/1의 하위 인터페이스는 다시 GigabitEthernet 0/1의 MAC 주소를 사용하게 됩니다.
- 드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 컨텍스트 내에서 그 인터페이스의 MAC 주소를 직접 설정할 수 있습니다.

프로시저

각 상황 인터페이스에 사설 MAC 주소를 자동으로 할당합니다.

mac-address auto [**prefix** *prefix*]

예제**:**

```
ciscoasa(config)# mac-address auto prefix 19
```

접두사를 입력하지 않으면 ASA에서 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동으로 생성합니다.

직접 접두사를 입력할 경우 *prefix*는 0 ~ 65535 범위의 십진수입니다. 이 접두사가 4자리 16진수로 변환되어 MAC 주소의 일부로 사용됩니다.

상황과 시스템 실행 영역 간 전환

시스템 실행 영역(또는 관리 상황)에 로그인한 경우 여러 컨텍스트로 전환하면서 각 컨텍스트에서 컨피그레이션 및 모니터링 작업을 수행할 수 있습니다. 구성 모드에서 수정하거나 **copy** 또는 **write** 명령에서 사용되는 실행 중인 구성은 위치에 따라 달라집니다. 시스템 실행 영역이라면 실행 중 컨피그레이션은 시스템 구성으로만 이루어집니다. 컨텍스트에 있을 경우 실행 중 컨피그레이션은 그 컨텍스트로만 이루어집니다. 예를 들어, **show running-config** 명령을 입력할 때 모든 실행 중 구성(시스템 및 모든 상황)을 볼 수는 없습니다. 현재 컨피그레이션만 표시됩니다.

프로시저

단계 **1** 상황으로 변경:

changeto context *name*

프롬프트가 ciscoasa/*name*#으로 변경됨

단계 **2** 시스템 실행 영역으로 변경:

changeto system

프롬프트가 ciscoasa#으로 변경됨

보안 상황 관리

이 섹션에서는 보안 컨텍스트를 관리하는 방법을 설명합니다.

보안 상황 제거

현재 관리 상황을 삭제할 수 없습니다. **clear context** 명령을 사용하여 모든 컨텍스트를 삭제하는 것만 가능합니다.

참고 장애 조치를 사용하는 경우, 액티브 유닛에서 컨텍스트를 삭제하는 시점과 스탠바이 유닛에서 컨텍스트가 삭제되는 시점 간에 지연이 발생합니다. 액티브 유닛과 스탠바이 유닛의 인터페이스 수가 일치하지 않는다는 오류 메시지가 나타날 수 있으나, 이는 일시적인 것이므로 무시해도 됩니다.

시작하기 전에

시스템 실행 영역에서 이 절차를 수행합니다.

프로시저

단계 **1** 단일 상황을 제거합니다.

no context *name*

모든 컨텍스트 명령도 삭제됩니다. 컨텍스트 컨피그레이션 파일은 config URL 위치에서 삭제되지 않습니다.

단계 **2** (관리 상황을 포함하여) 모든 상황을 제거합니다.

clear context

컨텍스트 컨피그레이션 파일은 컨피그레이션 URL 위치에서 삭제되지 않습니다.

관리 상황 변경

시스템 구성은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 컨텍스트 다운로드) 관리 상황으로 지정된 컨텍스트 중 하나를 사용합니다.

관리 상황은 여느 상황과 비슷하지만, 사용자가 관리 상황에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 컨텍스트에 액세스할 수 있다는 점이 다릅니다. 관리 상황은 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 상황에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 상황 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다.

시작하기 전에

- 어떤 컨텍스트도 관리 상황으로 설정할 수 있습니다. 단, 컨피그레이션 파일이 내부 플래시 메모리에 저장되어 있어야 합니다.
- 시스템 실행 영역에서 이 절차를 수행합니다.

프로시저

관리 상황 설정:

admin-context *context_name*

예제**:**

```
ciscoasa(config)# admin-context administrator
```

텔넷, SSH, HTTPS와 같이 관리 상황에 연결되어 있는 원격 관리 세션은 모두 종료됩니다. 새 관리 상황에 다시 연결해야 합니다.

ntp server와 같이 몇 가지 시스템 구성 명령은 관리 상황에 속한 인터페이스 이름을 지정합니다. 관리 상황을 변경하는 경우, 그 인터페이스 이름이 새 관리 상황에 없다면 그 이름을 참조하는 모든 시스템 명령을 업데이트해야 합니다.

보안 상황 URL 변경

이 섹션에서는 컨텍스트 URL을 변경하는 방법을 설명합니다.

시작하기 전에

- 새 URL에서 컨피그레이션을 다시 로드하지 않고는 보안 컨텍스트 URL을 변경할 수 없습니다. ASA에서는 새 구성을 현재 실행 중인 구성과 병합합니다.
- 동일한 URL을 다시 입력하면 역시 저장된 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다.
- 병합은 새 컨피그레이션의 새로운 명령을 실행 중인 컨피그레이션에 추가합니다.
  - 컨피그레이션이 동일할 경우 어떤 변경도 없습니다.
  - 명령이 충돌하거나 명령이 상황 실행에 영향을 줄 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다. 실행 중인 컨피그레이션이 비어 있을 경우(예: 서버가 사용할 수 없는 상태이고 컨피그레이션이 다운로드된 적이 없는 경우) 새로운 컨피그레이션이 사용됩니다.
- 컨피그레이션의 병합을 원치 않는다면 실행 중인 컨피그레이션을 지운 다음(해당 컨텍스트를 통한 모든 통신이 중지됨) 새 URL에서 컨피그레이션을 다시 로드하면 됩니다.
- 시스템 실행 영역에서 이 절차를 수행합니다.

프로시저

단계 **1** (선택 사항, 병합을 수행하지 않으려는 경우) 상황으로 변경 및 구성 지우기:

changeto context *name*

clear configure all

예제**:**

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

병합을 하려면 2단계로 진행합니다.

단계 **2** 시스템 실행 영역으로 변경:

changeto system

예제:

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

단계 **3** 변경할 상황의 상황 구성 모드로 들어갑니다.

context *name*

예제:

```
ciscoasa(config)# context ctx1
```

단계 **4** 새 URL을 입력합니다. 시스템에서 즉시 컨텍스트를 로드하므로 실행 중이 됩니다.

config-url *new_url*

예제:

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

보안 상황 다시 로드

2가지 방법으로 컨텍스트를 다시 로드할 수 있습니다.

- 실행 중인 컨피그레이션을 지운 다음 시작 컨피그레이션을 가져옵니다.

  그러면 컨텍스트와 연결된 대부분의 특성(연결, NAT 테이블 등)이 사라집니다.

- 시스템 구성에서 컨텍스트를 삭제합니다.

  그러면 문제 해결에 유용할 수 있는 추가 특성(예: 메모리 할당)이 사라집니다. 그러나 컨텍스트를 다시 시스템에 추가하려면 URL과 인터페이스를 다시 지정해야 합니다.

구성을 지워 다시 로드

프로시저

단계 **1** 다시 로드할 상황으로 변경:

changeto context *name*

예제:

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

단계 **2** 실행 중인 구성 지우기:

clear configure all

이 명령은 모든 연결을 끊습니다.

단계 **3** 구성 다시 로드:

copy startup-config running-config

예제**:**

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA에서는 시스템 구성에 지정된 URL에서 구성을 복사합니다. 컨텍스트 내에서 URL을 변경할 수 없습니다.

상황을 제거하고 다시 추가하여 다시 로드

상황을 삭제한 다음 다시 추가하는 방법으로 상황을 다시 로드하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 보안 상황 제거, 243 페이지. **Also delete config URL file from the disk(**디스크에서 구성 **URL** 파일도 삭제**)**

단계 **2** 보안 상황 구성, 237 페이지

보안 상황 모니터링

이 섹션에서는 컨텍스트 정보를 보고 모니터링하는 방법을 설명합니다.

상황 정보 보기

시스템 실행 영역에서 이름, 할당된 인터페이스, 컨피그레이션 파일 URL이 포함된 컨텍스트 목록을 볼 수 있습니다.

프로시저

모든 상황을 표시합니다.

show context [*name* | **detail**| **count**]

특정 컨텍스트에 대한 정보를 표시하려면 *name*을 지정합니다.

detail 옵션은 추가 정보를 표시합니다. 자세한 내용은 아래에 있는 샘플 출력을 참조하십시오.

count 옵션은 총 컨텍스트 수를 표시합니다.

예

다음은 **show context** 명령의 샘플 출력입니다. 다음 샘플 출력은 3개의 컨텍스트를 보여줍니다.

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

다음 표는 각 필드 설명을 보여줍니다.

표 ***7: show context Fields***

필드	설명
상황 이름	모든 상황 이름을 나열합니다. 별표(*)로 표시된 상황 이름이 관리 상황입니다.
Interfaces	컨텍스트에 지정된 인터페이스입니다.
URL	ASA에서 상황 구성을 로드하는 URL입니다.

다음은 **show context detail** 명령의 샘플 출력입니다.

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
```

```
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

detail 출력에 대한 자세한 내용은 명령 참조를 참조하십시오.

다음은 **show context count** 명령의 샘플 출력입니다.

```
ciscoasa# show context count
Total active contexts: 2
```

리소스 할당 보기

시스템 실행 영역에서 모든 클래스 및 클래스 멤버를 포괄하여 각 리소스의 할당을 볼 수 있습니다.

프로시저

리소스 할당 표시:

show resource allocation [**detail**]

이 명령은 리소스 할당을 표시하지만 사용 중인 실제 리소스는 표시하지 않습니다. 실제 리소스 사용량에 대한 자세한 내용은 리소스 사용량 보기, 252 페이지를 참조하십시오.

detail 인수는 추가 정보를 표시합니다. 자세한 내용은 아래에 있는 샘플 출력을 참조하십시오.

예

다음 샘플 출력에서는 각 리소스의 총 할당량을 절대값 및 가용 시스템 리소스 기준 백분율로 표시합니다.

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
```

```
AnyConnect                  1000           10%
AnyConnectBurst              200           2%
Other VPN Sessions            20           2.66%
Other VPN Burst               20           2.66%
All                       unlimited
```

다음 표는 각 필드 설명을 보여줍니다.

표 ***8: show resource allocation Fields***

필드	설명
리소스	제한할 수 있는 리소스의 이름입니다.
합계	모든 컨텍스트에 할당된 리소스의 총량입니다. 이는 동시 인스턴스 또는 초당 인스턴스의 개수(절대값)입니다. 클래스 정의에 백분율을 지정한 경우 ASA에서는 백분율을 절대값으로 환산하여 여기에 표시합니다.
% of Avail	리소스에 명시적 시스템 제한이 있을 경우, 모든 컨텍스트에 할당된 전체 시스템 리소스의 백분율입니다. 리소스에 시스템 제한이 없는 경우에는 이 열에 N/A가 표시됩니다.

다음은 **show resource allocation detail** 명령의 샘플 출력입니다.

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%
```

```
Hosts             default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      26214      26214      N/A
                  bronze             0      CA      13107
                  All Contexts:      3                         26214      N/A

SSH               default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%

Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%

Routes            default          all       C  unlimited                 N/A
                  gold               1       D  unlimited          5      N/A
                  silver             1      CA         10         10      N/A
                  bronze             0      CA          5                 N/A
                  All Contexts:      3                             20      N/A

Xlates            default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      23040      23040     N/A
                  bronze             0      CA      11520
                  All Contexts:      3                         23040     N/A

mac-addresses     default          all       C      65535
                  gold               1       D      65535      65535    100.00%
                  silver             1      CA       6553       6553      9.99%
                  bronze             0      CA       3276
                  All Contexts:      3                        137623    209.99%
```

다음 표는 각 필드 설명을 보여줍니다.

표 ***9: show resource allocation detail Fields***

필드	설명
리소스	제한할 수 있는 리소스의 이름입니다.
클래스	기본 클래스를 비롯한 각 클래스의 이름입니다. All contexts 필드는 모든 클래스를 포괄한 총계를 표시합니다.
Mmbrs	각 클래스에 지정된 컨텍스트의 수입니다.

필드	설명
근원	다음과 같은 리소스 제한의 출처입니다. • A—개별 리소스가 아닌 **all** 옵션과 함께 이 제한을 설정합니다. • C - 이 제한은 멤버 클래스에서 파생됩니다. • D - 이 제한은 멤버 클래스에 정의되지 않고 기본 클래스에서 파생됩니다. 기본 클래스에 지정된 컨텍스트의 경우 값은 “D”가 아니라 "C"가 됩니다. ASA에서는 "A"를 "C" 또는 "D"와 조합할 수 있습니다.
Limit(제한)	컨텍스트별 리소스 제한이며 절대값입니다. 클래스 정의에 백분율을 지정한 경우 ASA는 백분율을 절대값으로 환산하여 여기에 표시합니다.
합계	클래스의 모든 컨텍스트에 할당된 리소스의 총량입니다. 이는 동시 인스턴스 또는 초당 인스턴스의 개수(절대값)입니다. 리소스가 무제한일 경우 이 필드는 비어 있습니다.
% of Avail	클래스의 모든 컨텍스트에 할당된 전체 시스템 리소스의 백분율입니다. 리소스가 무제한일 경우 이 필드는 비어 있습니다. 리소스에 시스템 제한이 없을 경우 이 열에는 N/A가 표시됩니다.

리소스 사용량 보기

시스템 실행 영역에서 각 컨텍스트의 리소스 사용량을 보고 시스템 리소스 사용량을 표시할 수 있습니다.

프로시저

각 상황에 대한 리소스 사용량 보기:

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- 기본적으로 모든 컨텍스트 사용량이 표시됩니다. 각 컨텍스트는 개별적으로 표시됩니다.
- **top** *n* 키워드를 입력하면 지정된 리소스의 상위 사용자 *n*명의 컨텍스트를 표시합니다. 이 옵션을 사용하는 경우 **resource all**이 아니라 단일 리소스 유형을 지정해야 합니다.

- **summary** 옵션은 모든 컨텍스트 사용량의 합계를 표시합니다.
- **system** 옵션은 모든 컨텍스트 사용량의 합계를 표시하되 총 컨텍스트 제한이 아니라 리소스의 시스템 제한을 표시합니다.
- **resource** *resource_name*에 사용 가능한 리소스 이름은 리소스 관리를 위한 클래스 구성, 233 페이지를 참조하십시오. **show resource type** 명령도 참조하십시오. 모든 유형에는 **all**(기본 설정)을 지정합니다.
- **detail** 옵션은 관리할 수 없는 것을 포함한 모든 리소스의 리소스 사용량을 표시합니다. 예를 들어, TCP 인터셉트의 수를 볼 수 있습니다.
- **counter** *counter_name*은 다음 키워드 중 하나입니다.
  - **current** - 액티브 동시 인스턴스 또는 리소스의 현재 비율을 표시합니다.
  - **denied** - Limit 열에 표시된 리소스 제한을 초과했기 때문에 거부된 인스턴스 수를 표시합니다.
  - **peak**—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최다 동시 인스턴스 수 또는 최고 리소스 비율을 표시합니다.
  - **all**—(기본 설정) 모든 통계를 표시합니다.
- *count_threshold*에서 설정하는 값을 초과하면 리소스가 표시됩니다. 기본값은 1입니다. 리소스 사용량이 설정된 값보다 적을 경우 리소스가 표시되지 않습니다. 카운터 이름에 대해 **all**을 지정한 경우 *count_threshold*는 현재 사용량에 적용됩니다.
- 모든 리소스를 표시하려면 *count_threshold*를 **0**으로 설정합니다.

예

다음은 **show resource usage context** 명령의 샘플 출력입니다. 여기서는 관리 상황의 리소스 사용량을 보여줍니다.

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

다음은 **show resource usage summary** 명령의 샘플 출력입니다. 여기서는 모든 컨텍스트와 모든 리소스의 리소스 사용량을 보여줍니다. 이 샘플은 6개 컨텍스트의 제한을 표시합니다.

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
```

```
Xlates                  8526         8966      N/A           0 Summary
Hosts                    254          254      N/A           0 Summary
Conns [rate]             270          535      N/A        1704 Summary
Inspects [rate]          270          535      N/A           0 Summary
AnyConnect                 2           25     1000           0 Summary
AnyConnectBurst            0            0      200           0 Summary
Other VPN Sessions         0           10       10         740 Summary
Other VPN Burst            0           10       10         730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

다음은 **show resource usage summary** 명령의 샘플 출력입니다. 여기서는 25개 컨텍스트의 제한을 보여줍니다. 텔넷 및 SSH 연결의 컨텍스트 제한이 컨텍스트당 5이므로 총 제한은 125입니다. 시스템 제한은 100에 불과하므로 시스템 제한이 표시됩니다.

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

다음은 **show resource usage system** 명령의 샘플 출력입니다. 여기서는 모든 컨텍스트의 리소스 사용량을 보여주지만, 전체 컨텍스트 제한이 아니라 시스템 제한을 표시합니다. **counter all 0** 옵션은 현재 사용 중이 아닌 리소스를 표시하는 데 사용합니다. Denied statistics는 시스템 제한이 있을 경우 그로 인해 리소스가 거부된 횟수를 나타냅니다.

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit        Denied    Context
Telnet                      0            0        100             0    System
SSH                         0            0        100             0    System
ASDM                        0            0         32             0    System
Routes                      0            0        N/A             0    System
IPSec                       0            0          5             0    System
Syslogs [rate]              1           18        N/A             0    System
Conns                       0            1     280000             0    System
Xlates                      0            0        N/A             0    System
Hosts                       0            2        N/A             0    System
Conns [rate]                1            1        N/A             0    System
Inspects [rate]             0            0        N/A             0    System
AnyConnect                  2           25      10000             0    System
AnyConnectBurst             0            0        200             0    System
Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

상황의 **SYN** 공격 모니터링

ASA에서는 TCP 인터셉트를 사용하여 SYN 공격을 차단합니다. TCP 인터셉트는 SYN 쿠키 알고리즘을 통해 TCP SYN 플러딩 공격을 막아냅니다. SYN 플러딩 공격은 일반적으로 스푸핑된 IP 주소에서 시작되는 일련의 SYN 패킷으로 구성됩니다. SYN 패킷의 지속적인 플러드로 인해 서버 SYN 큐가 계속해서 꽉 차기 때문에 연결 요청을 처리하지 못하게 됩니다. 어떤 연결의 최초 연결 임계값을 초과

하면 ASA는 서버의 프록시 역할을 하면서 클라이언트 SYN 요청에 대해 SYN-ACK 응답을 생성합니다. ASA에서 클라이언트로부터 다시 ACK를 받으면 클라이언트를 인증하고 서버와의 연결을 허용합니다.

프로시저

단계 **1** 개별 상황의 공격 비율을 모니터링합니다.

show perfmon

단계 **2** 개별 상황에서 TCP 인터셉트가 사용 중인 리소스의 양을 모니터링합니다.

show resource usage detail

단계 **3** 전체 시스템에서 TCP 가로채기가 사용 중인 리소스를 모니터링합니다.

show resource usage summary detail

예

다음은 **show perfmon** 명령의 샘플 출력이며, admin이라는 컨텍스트의 TCP 인터셉트 비율을 보여줍니다.

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s      322779/s
```

다음은 **show resource usage detail** 명령의 샘플 출력이며, 개별 컨텍스트에서 TCP 인터셉트가 사용 중인 리소스의 양을 보여줍니다. (굵게 표시된 샘플 텍스트는 TCP 인터셉트 정보)

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
```

```
chunk:list-elem            21           21  unlimited            0 admin
chunk:list-hdr              3            4  unlimited            0 admin
chunk:route                 2            2  unlimited            0 admin
chunk:static                1            1  unlimited            0 admin
tcp-intercepts         328787       803610  unlimited            0 admin
np-statics                  3            3  unlimited            0 admin
statics                     1            1  unlimited            0 admin
ace-rules                   1            1  unlimited            0 admin
console-access-rul          2            2  unlimited            0 admin
fixup-rules                14           15  unlimited            0 admin
memory                 959872       960000  unlimited            0 c1
chunk:channels             15           16  unlimited            0 c1
chunk:dbgtrace              1            1  unlimited            0 c1
chunk:fixup                15           15  unlimited            0 c1
chunk:global                1            1  unlimited            0 c1
chunk:hole                  2            2  unlimited            0 c1
chunk:ip-users             10           10  unlimited            0 c1
chunk:udp-ctrl-blk          1            1  unlimited            0 c1
chunk:list-elem            24           24  unlimited            0 c1
chunk:list-hdr              5            6  unlimited            0 c1
chunk:nat                   1            1  unlimited            0 c1
chunk:route                 2            2  unlimited            0 c1
chunk:static                1            1  unlimited            0 c1
tcp-intercept-rate      16056        16254  unlimited            0 c1
globals                     1            1  unlimited            0 c1
np-statics                  3            3  unlimited            0 c1
statics                     1            1  unlimited            0 c1
nats                        1            1  unlimited            0 c1
ace-rules                   2            2  unlimited            0 c1
console-access-rul          2            2  unlimited            0 c1
fixup-rules                14           15  unlimited            0 c1
memory              232695716    232020648  unlimited            0 system
chunk:channels             17           20  unlimited            0 system
chunk:dbgtrace              3            3  unlimited            0 system
chunk:fixup                15           15  unlimited            0 system
chunk:ip-users              4            4  unlimited            0 system
chunk:list-elem          1014         1014  unlimited            0 system
chunk:list-hdr              1            1  unlimited            0 system
chunk:route                 1            1  unlimited            0 system
block:16384               510          885  unlimited            0 system
block:2048                 32           34  unlimited            0 system
```

다음 샘플 출력은 전체 시스템에서 TCP 인터셉트가 사용 중인 리소스를 보여줍니다. (굵게 표시된 샘플 텍스트는 TCP 인터셉트 정보)

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited            0 Summary
chunk:channels             46           48  unlimited            0 Summary
chunk:dbgtrace              4            4  unlimited            0 Summary
chunk:fixup                45           45  unlimited            0 Summary
chunk:global                1            1  unlimited            0 Summary
chunk:hole                  3            3  unlimited            0 Summary
chunk:ip-users             24           24  unlimited            0 Summary
chunk:udp-ctrl-blk          1            1  unlimited            0 Summary
chunk:list-elem          1059         1059  unlimited            0 Summary
chunk:list-hdr             10           11  unlimited            0 Summary
chunk:nat                   1            1  unlimited            0 Summary
chunk:route                 5            5  unlimited            0 Summary
chunk:static                2            2  unlimited            0 Summary
block:16384               510          885  unlimited            0 Summary
block:2048                 32           35  unlimited            0 Summary
```

```
tcp-intercept-rate      341306        811579  unlimited             0 Summary
globals                      1             1  unlimited             0 Summary
np-statics                   6             6  unlimited             0 Summary
statics                      2             2        N/A             0 Summary
nats                         1             1        N/A             0 Summary
ace-rules                    3             3        N/A             0 Summary
console-access-rul           4             4        N/A             0 Summary
fixup-rules                 43            44        N/A             0 Summary
```

할당된 **MAC** 주소 보기

시스템 구성 내에서 또는 컨텍스트 내에서 자동 생성된 MAC 주소를 볼 수 있습니다.

시스템 구성에서 **MAC** 주소 보기

이 단원에서는 시스템 구성에서 MAC 주소를 보는 방법을 설명합니다.

시작하기 전에

직접 인터페이스에 MAC 주소를 지정하지만 자동 생성도 활성화한 경우, 수동 MAC 주소가 사용되지만 자동 생성 주소도 계속 컨피그레이션에 표시됩니다. 나중에 수동 MAC 주소를 삭제하면, 여기에 표시되었던 자동 생성 주소가 사용됩니다.

프로시저

시스템 실행 영역에서 할당된 MAC 주소를 표시합니다.

show running-config all context [*name*]

지정된 MAC 주소를 보려면 **all** 옵션이 필요합니다. **mac-address auto** 명령은 전역 컨피그레이션 모드에서만 사용자 컨피그레이션이 가능하지만, 이 명령은 컨텍스트 컨피그레이션 모드에서 지정된 MAC 주소와 함께 읽기 전용 항목으로 표시됩니다. 컨텍스트 내에서 **nameif** 명령으로 구성된, 할당된 인터페이스만 MAC 주소를 받습니다.

예

다음은 **show running-config all context admin** 명령의 출력이며, Management0/0 인터페이스에 지정된 기본 및 스탠바이 MAC 주소를 보여줍니다.

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

다음은 **show running-config all context** 명령의 출력이며, 모든 컨텍스트 인터페이스의 모든 MAC 주소(기본 및 스탠바이)를 보여줍니다. GigabitEthernet0/0 및 GigabitEthernet0/1 기본 인터페이스는 컨텍스트 내에서 **nameif** 명령으로 구성되지 않았으므로, 어떤 MAC 주소도 생성되지 않았습니다.

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

상황 내 **MAC** 주소 보기

이 섹션에서는 컨텍스트 내에서 MAC 주소를 보는 방법을 설명합니다.

프로시저

상황 내에서 각 인터페이스가 사용 중인 MAC 주소를 표시합니다.

show interface | include (Interface)|(MAC)

예

예를 들면 다음과 같습니다.

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

참고 **show interface** 명령은 사용 중인 MAC 주소를 보여줍니다. 직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우, 시스템 구성 내에서는 사용되지 않은 자동 생성 주소만 볼 수 있습니다.

다중 상황 모드의 예

다음 예에서는

- 사용자 지정 접두사를 사용하여 컨텍스트에서 MAC 주소를 자동으로 설정합니다.
- conn의 기본 클래스 제한은 무제한이 아닌 10%로 설정하고, VPN 기타 세션을 10으로, 버스트는 5로 설정합니다.
- gold 리소스 클래스를 만듭니다.
- 관리 상황을 “administrator”가 되게 설정합니다.
- 내부 플래시 메모리에 “administrator”라는 이름으로 기본 리소스 클래스의 멤버가 될 컨텍스트를 만듭니다.
- FTP 서버에서 2개의 컨텍스트를 gold 리소스 클래스의 멤버로 추가합니다.

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
```

```
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

다중 상황 모드의 내역

표 ***10:*** 다중 상황 모드의 내역

기능 이름	플랫폼 릴리스	기능 정보
다중 보안 컨텍스트	7.0(1)	다중 상황 모드를 도입했습니다. 다음 명령을 도입했습니다. **context**, **mode**, **class**
자동 MAC 주소 지정	7.2(1)	컨텍스트 인터페이스에 MAC 주소를 자동으로 지정하는 기능을 도입했습니다. 다음 명령을 도입했습니다. **mac-address auto**
리소스 관리	7.2(1)	리소스 관리를 도입했습니다. 다음 명령을 도입했습니다. **class**, **limit-resource**, **member**

기능 이름	플랫폼 릴리스	기능 정보
IPS 가상 센서	8.0(2)	IPS 소프트웨어 버전 6.0 이상을 실행하는 AIP SSM에서 여러 가상 센서를 실행할 수 있습니다. 즉 AIP SSM에서 다중 보안 정책을 구성할 수 있습니다. 각 상황 또는 단일 모드 ASA를 하나 이상의 가상 센서에 할당하거나 여러 보안 상황을 동일한 가상 센서에 지정할 수 있습니다. 다음 명령을 도입했습니다. **allocate-ips**
자동 MAC 주소 지정 확장	8.0(5)/8.2(2)	MAC 주소 형식이 접두사를 사용하고, 고정 시작 값(A2)을 사용하고, 장애 조치 쌍에서는 기본 유닛 MAC 주소와 보조 유닛 MAC 주소에 서로 다른 체계를 사용하도록 변경되었습니다. 또한 MAC 주소는 다시 로드하더라도 유지됩니다. 명령 구문 분석기에서 자동 생성 활성화 여부를 확인합니다. 직접 MAC 주소를 지정하는 것도 원할 경우 수동 MAC 주소는 A2로 시작할 수 없습니다. 다음 명령을 수정했습니다. **mac-address auto prefix**
ASA 5550 및 5580에서 최대 컨텍스트 증가	8.4(1)	ASA 5550의 최대 보안 컨텍스트 수가 50에서 100으로 늘어났습니다. ASA 5580의 최대 보안 컨텍스트 수가 50에서 250으로 늘어났습니다.
자동 MAC 주소 지정 기본적으로 활성화	8.5(1)	자동 MAC 주소 지정이 기본적으로 활성화되어 있습니다. 다음 명령을 수정했습니다. **mac-address auto prefix**

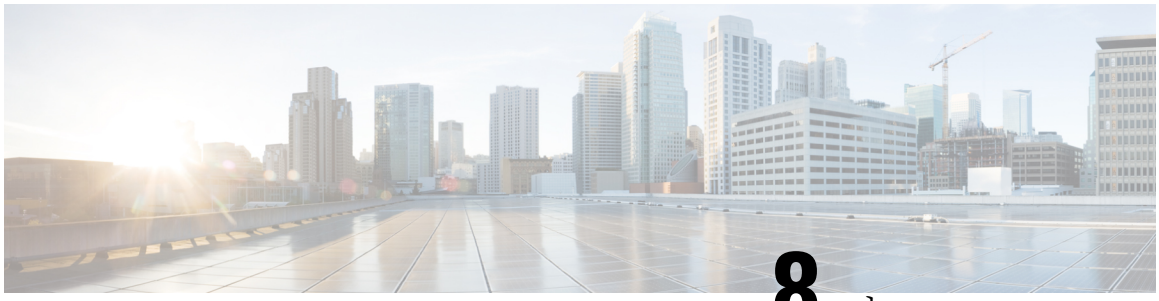
기능 이름	플랫폼 릴리스	기능 정보
MAC 주소 접두사 자동 생성	8.6(1)	다중 상황 모드에서 ASA의 자동 MAC 주소 생성 구성은 기본 접두사를 사용하도록 변환됩니다. ASA에서는 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동 생성합니다. 다시 로드할 때 또는 MAC 주소 생성을 다시 활성화할 경우 이 변환이 자동으로 이루어집니다. 이러한 접두사 생성 방식은 세그먼트에서 더 확실하게 고유한 MAC 주소를 보장하는 등 여러 가지 이점을 제공합니다.**show running-config mac-address** 명령을 입력하여 자동 생성된 접두사를 확인할 수 있습니다. 접두사를 변경하려는 경우 사용자 지정 접두사로 기능을 재구성할 수 있습니다. 기존의 MAC 주소 생성 방식은 더 이상 사용되지 않습니다. 참고 장애 조치 쌍의 히트리스 업그레이드를 유지하고자 ASA에서는 장애 조치가 활성화된 경우 다시 로드할 때 기존 구성의 MAC 주소 방식을 변환하지 않습니다. 그러나 특히 ASASM의 경우에는 장애 조치를 사용할 때 직접 접두사 생성 방법으로 바꾸는 것이 좋습니다. 접두사 방법을사용하지 않으면 서로 다른 슬롯 번호에 설치된 ASASM에서 장애 조치 시 MAC 주소가 바뀌어 트래픽이 중단될 수 있습니다. 업그레이드한 다음 MAC 주소 생성에 접두사 방법을 사용하려면 MAC 주소 자동 생성에서 다시 접두사를 사용할 수 있게 합니다. 다음 명령을 수정했습니다. **mac-address auto prefix**

기능 이름	플랫폼 릴리스	기능 정보
ASASM을 제외한 모든 모델에서 기본적으로 비활성화되어 있는 자동 MAC 주소 할당	9.0(1)	이제 자동 MAC 주소 할당은 ASASM을 제외하고 기본적으로 비활성화되어 있습니다. 다음 명령을 수정했습니다. **mac-address auto prefix**
보안 컨텍스트의 동적 라우팅	9.0(1)	EIGRP 및 OSPFv2 동적 라우팅 프로토콜이 다중 상황 모드에서 지원됩니다. OSPFv3, RIP, 멀티캐스트 라우팅은 지원되지 않습니다.
라우팅 테이블 항목의 새로운 리소스 유형	9.0(1)	각 컨텍스트에서 라우팅 테이블 항목의 최대값을 설정하기 위해 새로운 리소스 유형인 routes를 개발했습니다. 다음 명령을 수정했습니다. **limit-resource, show resource types, show resource usage, show resource allocation**
다중 상황 모드의 사이트 대 사이트 VPN	9.0(1)	사이트 대 사이트 VPN 터널이 다중 상황 모드에서 지원됩니다.
사이트 대 사이트 VPN 터널을 위한 새로운 리소스 유형	9.0(1)	각 컨텍스트에서 사이트 대 사이트 VPN 터널의 최대값을 설정하기 위해 새로운 리소스 유형인 vpn other와 vpn burst other를 개발했습니다. 다음 명령을 수정했습니다. **limit-resource, show resource types, show resource usage, show resource allocation**
IKEv1 SA 협상의 새로운 리소스 유형	9.1(2)	새로운 리소스 유형인 ikev1 in-negotiation이 CPU 및 암호화 엔진이 가득차는 것을 방지하기 위해 각 상황에서 IKEv1 SA 협상의 최대 백분율을 설정하도록 생성되었습니다. 특정한 조건(대형 인증서, CRL 확인)에서 이 리소스를 제한하는 것이 좋습니다. 다음 명령을 수정했습니다. **limit-resource, show resource types, show resource usage, show resource allocation**

기능 이름	플랫폼 릴리스	기능 정보
다중 상황 모드에서의 원격 액세스 VPN 지원	9.5(2)	이제 다중 상황 모드에서 다음 원격 액세스 기능을 사용할 수 있습니다. • AnyConnect 3.x 이상(SSL VPN만 해당, IKEv2는 지원되지 않음) • 중앙 집중식 AnyConnect 이미지 구성 • AnyConnect 이미지 업그레이드 • AnyConnect 연결을 위한 상황 리소스 관리 참고 다중 상황 모드에서 AnyConnect Apex 라이선스가 필요합니다. 기본 라이선스 또는 레거시 라이선스는 사용할 수 없습니다. 다음 명령을 도입했습니다. **limit-resource vpn anyconnect, limit-resource vpn burst anyconnect**
다중 상황 모드에 대한 Pre-fill/Username-from-cert 기능	9.6(2)	AnyConnect SSL 지원은 이전에는 단일 모드에서만 사용 가능했던 pre-fill/username-from-certificate 기능 CLI가 다중 상황 모드에서도 활성화되는 것을 허용하도록 확장되었습니다. 명령은 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
원격 액세스 VPN에 대한 플래시 가상화	9.6(2)	이제 다중 상황 모드에서 원격 액세스 VPN이 플래시 가상화를 지원합니다. 각 상황은 프라이빗 스토리지 공간과 사용 가능한 총 플래시 기반 공유 스토리지 위치를 보유할 수 있습니다. • 프라이빗 스토리지 — 해당 사용자와 연결된 파일만 저장하며 해당 사용자용으로 원하는 콘텐츠로만 한정됩니다. • 공유 스토리지 — 이 공간에 파일을 업로드하고 일단 활성화하면 읽기/쓰기 액세스에 대한 모든 사용자 상황에 액세스할 수 있게 합니다. 다음 명령을 도입했습니다. **limit-resource storage, storage-url**
다중 상황 디바이스에서의 AnyConnect 클라이언트 프로필 지원	9.6(2)	AnyConnect 클라이언트 프로필은 다중 상황 디바이스에서 지원됩니다. ASDM을 사용하여 새 프로필을 추가하려면 AnyConnect Secure Mobility Client 릴리스 4.2.00748 또는 4.3.03013 이상 버전을 사용 중이어야 합니다.
다중 상황 모드에서의 AnyConnect 연결에 대한 스테이트풀 장애 조치	9.6(2)	이제 다중 상황 모드에서 AnyConnect 연결에 대한 스테이트풀 장애 조치가 지원됩니다. 명령은 수정하지 않았습니다.
다중 상황 모드에서의 원격 액세스 VPN(Dynamic Access Policy) 지원	9.6(2)	이제 다중 상황 모드에서 상황별로 DAP를 구성할 수 있습니다. 명령은 수정하지 않았습니다.
다중 상황 모드에서의 원격 액세스 VPN CoA(Change of Authorization) 지원	9.6(2)	이제 다중 상황 모드에서 상황별로 CoA를 구성할 수 있습니다. 명령은 수정하지 않았습니다.
다중 상황 모드에서의 원격 액세스 VPN 현지화 지원	9.6(2)	현지화는 글로벌 지원입니다. 다양한 상황 전반에서 공유되는 현지화 파일의 집합은 하나만 있습니다. 명령은 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
다중 상황 모드에서의 IKEv2용 원격 액세스 VPN 지원	9.9(2)	IKEv2를 위한 다중 상황 모드에서 원격 액세스 VPN을 구성할 수 있습니다.



8 장

고가용성을 위한 장애 조치

이 장에서는 Cisco ASA의 고가용성을 실현하기 위해 액티브/스탠바이 또는 액티브/액티브 페일오버를 구성하는 방법에 대해 설명합니다.

장애 조치 정보

장애 조치를 구성하려면 2개의 동일한 ASA가 전용 장애 조치 링크 또는 선택에 따라 상태 링크를 통해 서로 연결되어 있어야 합니다. 액티브 유닛 및 인터페이스의 상태를 모니터링하여 특정한 장애 조치 조건을 충족하는지 판단합니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다.

장애 조치 모드

ASA에서는 액티브/액티브 장애 조치 및 액티브/스탠바이 장애 조치로 된 2가지 장애 조치 모드를 지원합니다. 각 장애 조치 모드에서는 고유한 방법을 통해 장애 조치를 확인하고 수행합니다.

- 액티브/스탠바이 장애 조치에서는 하나의 유닛이 액티브 유닛입니다. 이 유닛에서 트래픽을 전달합니다. 스탠바이 유닛에서는 트래픽을 능동적으로 전달하지 않습니다. 장애 조치가 일어나면 액티브 유닛은 스탠바이 유닛으로 장애 조치를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다. 단일 또는 다중 상황 모드에서는 ASA에 액티브/스탠바이 장애 조치를 사용할 수 있습니다.

- 액티브/액티브 장애 조치 구성에서는 두 ASA가 모두 네트워크 트래픽을 전달할 수 있습니다. 액티브/액티브 장애 조치는 다중 상황 모드의 ASA에만 사용할 수 있습니다. 액티브/액티브 장애 조치에서 ASA의 보안 상황은 2개의 장애 조치 그룹으로 나뉩니다. 장애 조치 그룹은 단순히 하나 이상의 보안 상황으로 구성된 논리적 그룹입니다. 한 그룹은 기본 ASA에서 액티브 상태로 할당되고 다른 그룹은 보조 ASA에서 액티브 상태로 할당됩니다. 장애 조치는 장애 조치 그룹 수준에서 수행됩니다.

두 장애 조치 모드 모두 스테이트풀 및 스테이트리스 장애 조치를 지원합니다.

장애 조치 시스템 요구 사항

이 섹션에서는 장애 조치 구성에서 ASA의 하드웨어, 소프트웨어 및 라이선스 요구 사항에 대해 설명합니다.

하드웨어 요구 사항

장애 조치 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 모델이어야 합니다.
- 인터페이스 개수와 유형이 같아야 합니다.

  Firepower 2100 및 Firepower 4100/9300 섀시의 경우, 장애 조치 기능을 활성화하기 전에 FXOS에서 동일하게 모든 인터페이스를 사전에 구성해야 합니다. 장애 조치 기능을 활성화한 후에 인터페이스를 변경하는 경우, 스탠바이 유닛의 FXOS에서 인터페이스를 변경한 후 액티브 유닛에서 동일하게 변경을 수행합니다. 네트워크 모듈/EtherChannel을 제거하거나 EtherChannel에 인터페이스를 재할당하는 등 FXOS에서 인터페이스를 제거하면 ASA 구성에서 원래 명령이 유지되므로 필요한 조정을 수행할 수 있습니다. 구성에서 인터페이스를 제거하면 그 영향이 광범위하게 미칠 수 있습니다. ASA OS에서 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.
- 같은 모듈을 설치해야 합니다(있을 경우).
- 같은 RAM을 설치해야 합니다.

장애 조치 구성에서 플래시 메모리 크기가 다른 유닛을 사용 중인 경우, 플래시 메모리 용량이 작은 유닛에 소프트웨어 이미지 파일 및 구성 파일을 수용할 수 있는 충분한 공간이 있는지 확인해야 합니다. 그렇지 않을 경우 플래시 메모리 용량이 큰 유닛에서 플래시 메모리 용량이 작은 유닛으로 컨피그레이션을 동기화할 수 없습니다.

소프트웨어 요구 사항

장애 조치 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 방화벽 모드에 있어야 합니다(라우팅 또는 투명).
- 같은 상황 모드에 있어야 합니다(단일 또는 다중).
- 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 같아야 합니다. 그러나 업그레이드 과정에서 일시적으로 여러 소프트웨어 버전을 사용할 수 있습니다. 예를 들어, 버전 8.3(1)에서 버

전 8.3(2)으로 업그레이드하고 장애 조치를 활성 상태로 유지할 수 있습니다. 장기적으로 호환성을 보장하려면 두 유닛을 모두 같은 버전으로 업그레이드하는 것이 좋습니다.

- 같은 AnyConnect 이미지가 있어야 합니다. 무중단 업그레이드를 수행할 때 장애 조치 쌍에 불일치하는 이미지가 있을 경우, 업그레이드 프로세스의 마지막 재부팅 단계에서 클라이언트리스 SSL VPN 연결이 종료되고 데이터베이스에 Orphan 세션이 표시되며 IP 풀에는 클라이언트에 할당된 IP 주소가 "사용 중"인 것으로 표시됩니다.
- 동일한 FIPS 모드에 있어야 합니다.

라이선스 요건

장애 조치 컨피그레이션의 유닛 2개는 라이센스가 동일하지 않아도 됩니다. 이러한 라이센스는 통합되어 장애 조치 클러스터 라이센스를 생성합니다.

페일오버 및 스테이트풀 페일오버 링크

장애 조치 링크 및 스테이트풀 장애 조치 링크(선택 사항)는 2개 유닛 간의 전용 연결입니다.

⚠

주의 IPsec 터널이나 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(사전 공유 키)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 IPsec 터널이나 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

페일오버 링크

장애 조치 쌍의 유닛 2개에서는 장애 조치 링크를 통해 지속적으로 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.

장애 조치 링크 데이터

다음 정보는 페일오버 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이)
- Hello 메시지(keep-alives)
- 네트워크 링크 상태
- MAC 주소 교환
- 컨피그레이션 복제 및 동기화

장애 조치 링크에 대한 인터페이스

사용되지 않는 데이터 인터페이스(물리적, 하위 인터페이스, 이중화 또는 EtherChannel)는 모두 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. 장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능). 대부분의 모델에서 아래와 같이 명시적으로 설명되어 있지 않은 경우, 장애 조치에 관리 인터페이스를 사용할 수 없습니다.

ASA에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.또한 데이터와 장애 조치 링크에 대해 동일한 상위에서 별도의 하위 인터페이스를 사용할 수 없습니다.

장애 조치 링크에 대한 다음 지침을 참조하십시오.

- 5506-X~5555-X — 관리 인터페이스를 장애 조치 링크로 사용할 수 없습니다. 데이터 인터페이스를 사용해야 합니다. 유일한 예외는 5506H-X인데, 이 경우에는 관리 인터페이스를 장애 조치 링크로 사용할 수 있습니다.
- 5506H-X — Management 1/1 인터페이스를 장애 조치 링크로 사용할 수 있습니다. 이 제품에서 장애 조치를 구성하는 경우, 구성을 적용하려면 디바이스를 다시 로드해야 합니다. 이 경우 관리 인터페이스가 관리 목적으로 필요하기 때문에 ASA Firepower 모듈은 사용할 수 없습니다.
- 5585-X — Management 0/0 인터페이스는 데이터 인터페이스로 사용할 수 있더라도 사용하지 마십시오. 이 제품은 이 용도에 필요한 성능을 지원하지 않습니다.
- Firepower 9300 및 Firepower 4100의 ASA — 장애 조치 및 상태 링크를 통합하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다. 관리 유형 인터페이스는 장애 조치 링크용으로 사용할 수 없습니다.
- 기타 모델 — 1GB 인터페이스는 통합된 장애 조치 및 상태 링크에 충분한 크기입니다.

장애 조치 링크로 사용된 이중 인터페이스의 경우, 추가된 이중성에 대한 다음 이점을 참조하십시오.

- 장애 조치 유닛이 부팅될 때, 활성 유닛을 검색하기 위해 멤버 인터페이스 간에 교체를 수행합니다.
- 장애 조치 유닛이 멤버 인터페이스 중 하나에서 피어로부터 keepalive 메시지 수신을 중지하는 경우, 다른 멤버 인터페이스로 전환합니다.

장애 조치 링크로 사용된 EtherChannel의 경우, EtherChannel의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

장애 조치 링크 연결

다음 2가지 방법 중 하나를 사용하여 장애 조치 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 ASA의 장애 조치 인터페이스로 사용합니다.
- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다.

유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

ASA에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through 케이블을 사용할 수 있습니다. 다이렉트 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

스테이트풀 페일오버 링크

스테이트풀 장애 조치를 사용하려면 연결 상태 정보를 전달할 스테이트풀 장애 조치 링크(상태 링크라고도 함)를 구성해야 합니다.

참고 스테이트풀 장애 조치 링크의 대역폭은 데이터 인터페이스의 최소 대역폭과 일치하는 것이 좋습니다.

장애 조치 링크 공유

장애 조치 링크를 공유하는 방법은 인터페이스를 보호하는 가장 좋은 방법입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다.

전용 인터페이스

상태 링크에 전용 데이터 인터페이스(물리적, 이중 또는 EtherChannel)를 사용할 수 있습니다. 상태 링크로 사용된 EtherChannel의 경우, EtherChannel의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다.

다음 두 가지 방법 중 하나를 사용하여 전용 상태 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 ASA 디바이스의 장애 조치 인터페이스로 사용합니다.
- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 어플라이언스를 직접 연결합니다.

  유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

  ASA에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through 케이블을 사용할 수 있습니다. 다이렉트 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

장거리 페일오버를 사용할 경우 최적의 성능을 보장하려면 페일오버 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 페일오버 메시지의 재전송으로 인해 성능이 다소 저하됩니다.

페일오버 및 데이터 링크 중단 방지

페일오버 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 장애 조치 링크가 중단될 경우 ASA에서는 데이터 인터페이스를 사용하여 장애 조치가 필요한지 여부를 확인합니다. 그런 다음 장애 조치 링크 상태가 복원될 때까지는 장애 조치 작업이 보류됩니다.

복원력이 뛰어난 페일오버 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 **1** — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 ASA 간의 장애 조치 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 ASA 모두 액티브 상태가 됩니다. 따라서 아래 그림에 표시된 다음 2가지 연결 방법은 권장되지 않습니다.

그림 ***38:*** 단일 스위치로 연결 - 권장하지 않음

그림 ***39:*** 이중 스위치로 연결 - 권장하지 않음

시나리오 **2** — 권장

장애 조치 링크에서는 같은 스위치를 데이터 인터페이스로 사용하지 않는 것이 좋습니다. 대신 다음 그림에 나와 있는 것처럼 다른 스위치를 사용하거나 다이렉트 케이블을 사용하여 페일오버 링크에 연결합니다.

그림 ***40:*** 다른 스위치로 연결

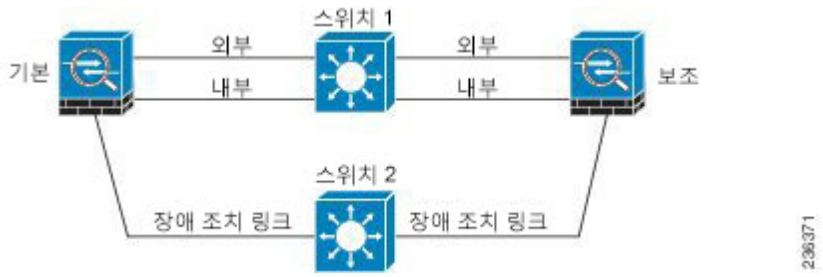
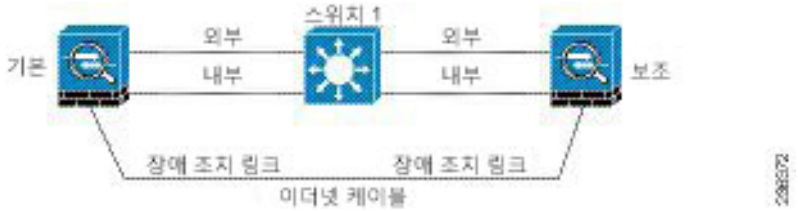


그림 ***41:*** 케이블로 연결



시나리오 **3** — 권장

ASA 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 페일오버 링크는 이러한 스위치 중 하나에 연결될 수 있으며 다음 그림에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 ***42:*** 보안 스위치로 연결

시나리오 **4** — 권장

가장 안정적인 페일오버 컨피그레이션에서는 다음 그림에 나와 있는 것처럼 페일오버 링크에서 이중 인터페이스를 사용합니다.

그림 ***43:*** 이중 인터페이스로 연결

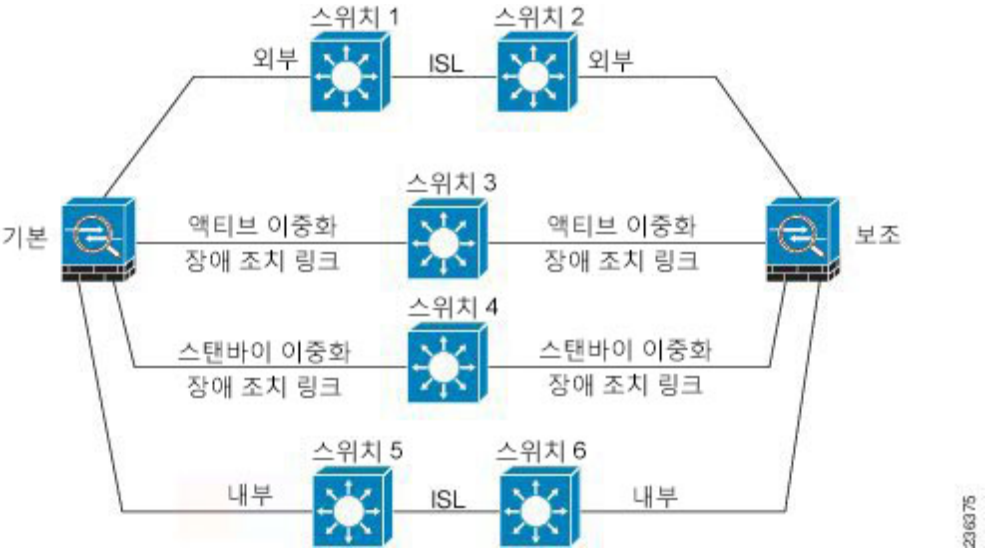
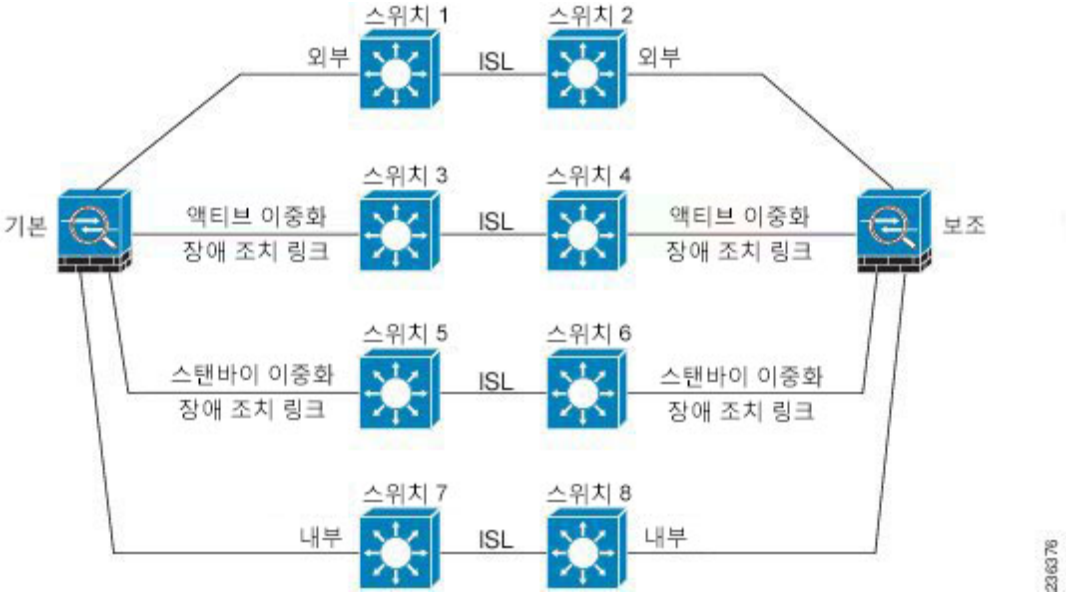


그림 *44:* 스위치 간 링크로 연결



MAC 주소와 IP 주소 - 장애 조치

인터페이스를 구성할 때는 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정할 수 있습니다. 일반적으로 페일오버가 발생할 때는 활성 IP 주소와 MAC 주소가 새 액티브 유닛에 승계됩니다. 네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

참고 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다. 관리 목적으로 해당 인터페이스에서 스탠바이 유닛에 연결할 수도 없습니다.

상태 링크의 IP 주소와 MAC 주소는 장애 조치 시 변경되지 않습니다.

액티브/스탠바이 IP 주소와 MAC 주소

액티브/스탠바이 장애 조치의 경우 페일오버 이벤트가 발생하는 동안의 IP 주소 및 MAC 주소 사용법은 다음 설명을 참조하십시오.

1. 액티브 유닛은 항상 기본 유닛의 IP 주소와 MAC 주소를 사용합니다.
2. 액티브 유닛에서 장애 조치가 수행될 때 스탠바이 유닛에서는 장애 발생 유닛의 IP 주소와 MAC 주소를 사용해 트래픽 전달을 시작합니다.
3. 장애 발생 유닛은 다시 온라인으로 설정되면 스탠바이 상태가 되며 스탠바이 IP 주소와 MAC 주소를 승계합니다.

하지만 기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 기본 유닛이 사용 가능해지면 보조(액티브) 유닛이 MAC 주소를 기본 유닛의 주소로 변경하므로 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다.

시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 ASA에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

액티브/액티브 IP 주소와 MAC 주소

액티브/액티브 페일오버의 경우 페일오버 이벤트가 발생하는 동안의 IP 주소 및 MAC 주소 사용법은 다음 설명을 참조하십시오.

1. 기본 유닛이 페일오버 그룹 1 및 2 컨텍스트에서 모든 인터페이스에 대해 액티브 및 스탠바이 MAC 주소를 자동 생성합니다. MAC 주소가 충돌하는 경우 등 필요 시에는 MAC 주소를 수동으로 구성할 수도 있습니다.
2. 각 유닛은 활성 페일오버 그룹에 대해 활성 IP 주소 및 MAC 주소를 사용하며 스탠바이 페일오버 그룹에 대해 스탠바이 주소를 사용합니다. 예를 들어 기본 유닛은 페일오버 그룹 1에 대해서는 액티브 상태이므로, 페일오버 그룹 1의 컨텍스트에 대해서는 액티브 주소를 사용합니다. 그리고 페일오버 그룹 2의 컨텍스트에 대해서는 스탠바이 상태이므로 스탠바이 주소를 사용합니다.
3. 유닛에서 장애 조치가 수행될 때 다른 유닛에서는 장애 발생 장애 조치 그룹의 액티브 IP 주소와 MAC 주소를 사용해 트래픽 전달을 시작합니다.
4. 선점 옵션을 활성화한 상태에서 장애 발생 유닛이 다시 온라인 상태가 되면 해당 유닛의 페일오버 그룹이 다시 시작됩니다.

가상 MAC 주소

ASA에서는 여러 가지 방법으로 가상 MAC 주소를 구성할 수 있습니다. 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다. 아래에서 설명하는 자동 생성 방법 외에도 인터페이스 모드 **mac-address** 명령, **failover mac address** 명령 및 액티브/액티브 페일오버를 위한 페일오버 그룹 모드 **mac address** 명령 등의 수동 방법도 있습니다.

다중 컨텍스트 모드에서는 공유 인터페이스에 대해 가상 액티브 및 스탠바이 MAC 주소를 자동으로 생성하도록 ASA를 구성할 수 있습니다. 이러한 할당은 보조 유닛으로 동기화됩니다(**mac-address auto** 명령 참조). 비공유 인터페이스의 경우 액티브/스탠바이 모드에 대해 MAC 주소를 수동으로 설정할 수 있습니다. 액티브/액티브 모드에서는 모든 인터페이스에 대해 MAC 주소를 자동 생성합니다.

액티브/액티브 페일오버의 경우에는 항상 기본값 또는 사용자가 인터페이스당 설정할 수 있는 값이 포함된 가상 MAC 주소가 사용됩니다.

ASA 서비스 모듈을 위한 섀시 내 모듈 및 섀시 간 모듈 배치

기본 및 보조 ASASM을 같은 스위치 또는 두 개의 개별 스위치 내에 배치할 수 있습니다.

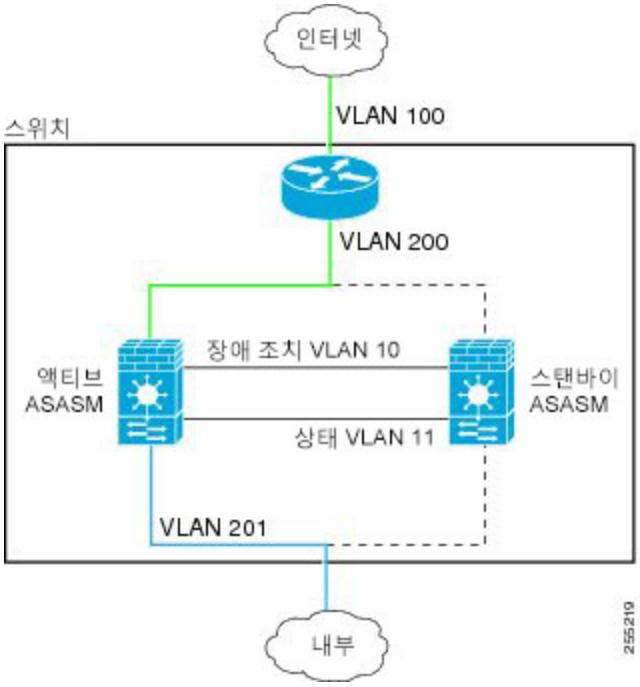
섀시 내 장애 조치

기본 ASASM과 동일한 스위치에서 보조 ASASM을 설치할 경우 모듈 수준 장애를 방지할 수 있습니다.

두 ASASM이 모두 같은 VLAN에 할당된 경우에도 액티브 모듈만 네트워킹에 참여합니다. 스탠바이 모듈에서는 어떠한 트래픽도 전달하지 않습니다.

다음 그림은 일반적인 스위치 내 구성을 보여줍니다.

그림 ***45: Intra-Switch*** 장애 조치



섀시 간 장애 조치

스위치 수준 장애를 방지하기 위해 별도의 스위치에 보조 ASASM을 설치할 수 있습니다. ASASM에서는 스위치와 직접 장애 조치를 조정하지 않으나 스위치 장애 조치 작업과 원활하게 연동됩니다. 스위치의 장애 조치를 구성하는 방법에 대한 내용은 스위치 설명서를 참조하십시오.

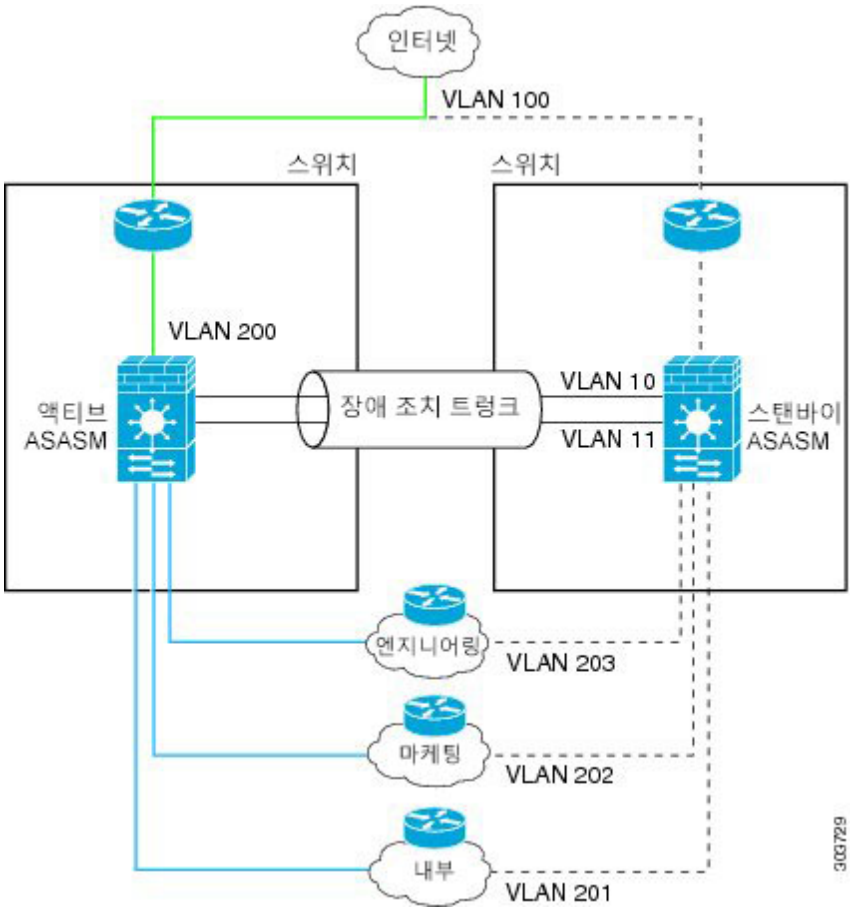
ASASM 간의 장애 조치 통신을 최대한 안정적으로 수행하려면 두 스위치 사이에 EtherChannel 트렁크 포트를 구성하여 장애 조치 및 상태 VLAN을 전송하는 것이 좋습니다.

기타 VLAN의 경우 두 스위치에 모든 방화벽 VLAN에 대한 액세스 권한이 있고, 모니터링된 VLAN에서 두 스위치 간에 hello 패킷을 올바르게 전달할 수 있는지 확인해야 합니다.

다음 그림에는 일반적인 스위치 및 ASASM 이중화 구성이 나와 있습니다. 두 스위치 간의 트렁크에서는 장애 조치 ASASM VLAN(VLAN 10 및 11)을 전송합니다.

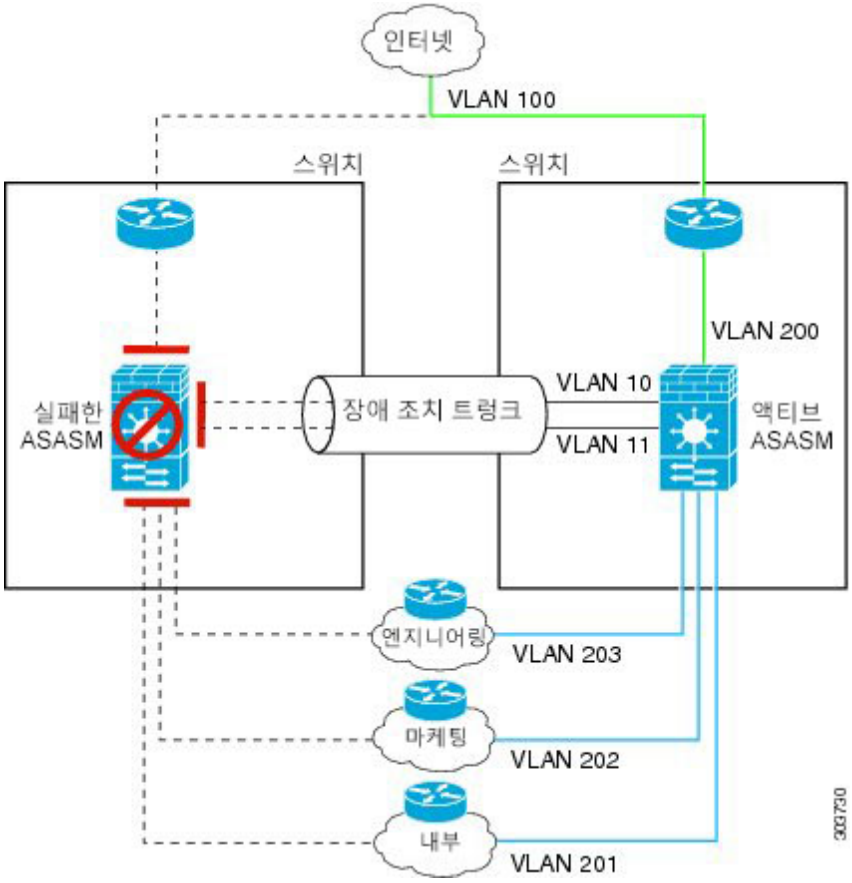
참고 ASASM 장애 조치는 스위치 장애 조치 작업과는 무관하지만, ASASM의 경우 모든 스위치 장애 조치 시나리오에서 작동합니다.

그림 **46:** 정상 가동



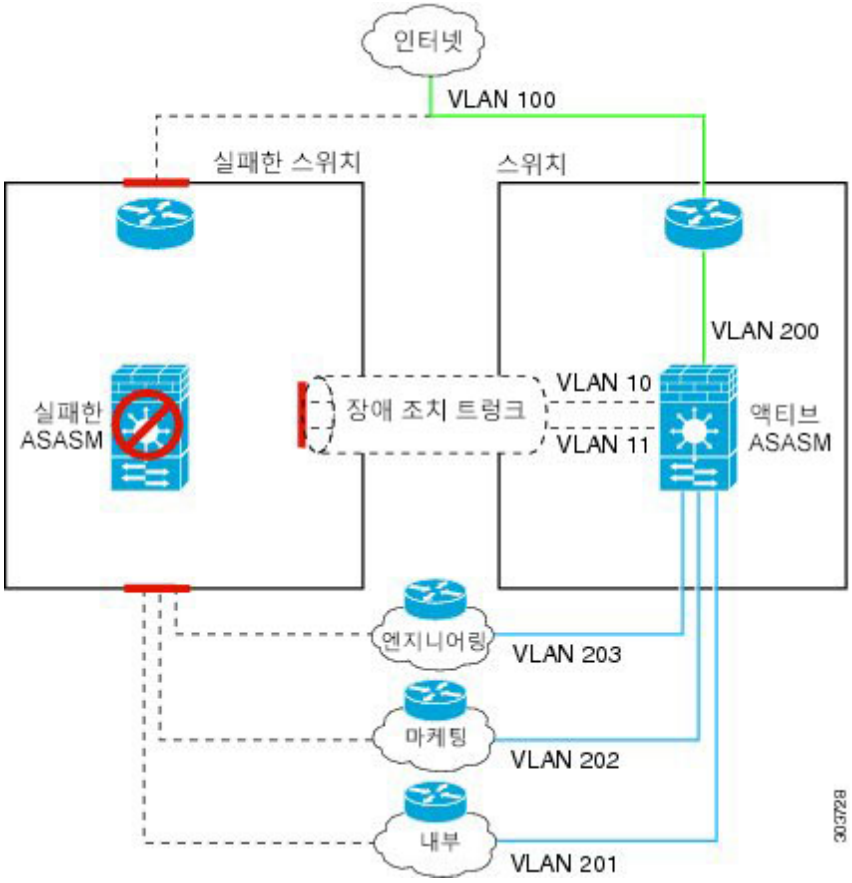
기본 ASASM에 장애가 발생하면 보조 ASASM이 액티브 상태가 되고 방화벽 VLAN을 성공적으로 통과합니다.

그림 ***47: ASASM*** 장애



ASASM을 비롯한 전체 스위치에 장애가 발생할 경우(예: 정전), 두 스위치 및 ASASM에서는 해당 보조 유닛으로 장애 조치를 시작합니다.

그림 **48:** 스위치 오류



상태 비저장 및 상태 저장 장애 조치

ASA에서는 액티브/스탠바이 및 액티브/액티브 모드에 대해 두 가지 유형의 장애 조치(스테이트리스 및 스테이트풀)를 지원합니다.

참고 클라이언트리스 SSL VPN의 일부 컨피그레이션 요소(예: 책갈피 및 맞춤화)에서는 스테이트풀 장애 조치의 일부분인 VPN 장애 조치 하위 시스템을 사용합니다. 스테이트풀 장애 조치를 사용하여 상태 조치 쌍의 멤버 간에 이러한 요소를 동기화해야 합니다. 클라이언트리스 SSL VPN에는 스테이트리스 장애 조치를 권장하지 않습니다.

스테이트리스 장애 조치

장애 조치가 일어나면 모든 활성 연결이 손실됩니다. 새 액티브 유닛을 인계받을 경우 클라이언트에서는 연결을 다시 설정해야 합니다.

참고 클라이언트리스 SSL VPN의 일부 컨피그레이션 요소(예: 책갈피 및 맞춤화)에서는 스테이트풀 장애 조치의 일부분인 VPN 장애 조치 하위 시스템을 사용합니다. 스테이트풀 장애 조치를 사용하여 상태 조치 쌍의 멤버 간에 이러한 요소를 동기화해야 합니다. 클라이언트리스 SSL VPN에는 스테이트리스(일반) 장애 조치를 권장하지 않습니다.

스테이트풀 페일오버

스테이트풀 장애 조치를 스테이트풀 장애 조치 동안액티브 유닛에서는 연결당 상태 정보를 스탠바이 유닛으로 전달하거나 액티브/액티브 장애 조치에서 액티브 및 스탠바이 장애 조치 그룹 간에 지속적으로 전달합니다. 장애 조치가 일어난 후에는 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션이 없어도 다시 연결하여 동일한 통신 세션을 그대로 유지할 수 있습니다.

지원 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 ASA로 전달됩니다.

- NAT 변환 테이블.
- TCP 및 UDP 연결과 상태(). 다른 유형의 IP 프로토콜과 ICMP는 새 패킷이 도착하면 새 액티브 유닛에서 설정되므로 액티브 유닛에서 구문 분석되지 않습니다.
- HTTP 연결 테이블(HTTP 복제를 활성화하지 않는 경우).
- HTTP 연결 상태(HTTP 복제가 활성화된 경우) - 기본적으로 ASA에서는 스테이트풀 페일오버가 활성화된 경우 HTTP 세션 정보를 복제하지 않습니다. 보통 HTTP 클라이언트에서는 오류가 발생한 연결을 다시 수행하려고 시도하기 때문에 HTTP 세션은 짧은 것이 일반적입니다. 따라서 HTTP 세션을 복제하지 않을 경우 중요한 데이터 또는 연결이 손실되지 않으면서 시스템 성능이 향상됩니다.
- SCTP 연결 상태. 그러나 SCTP 검사 스테이트풀 페일오버가 최상의 결과입니다. 페일오버 중에 SACK 패킷이 손실되면 새 액티브 유닛은 누락된 패킷이 수신될 때까지 대기열에서 문제가 있는 기타 모든 패킷을 삭제합니다.
- ARP 테이블
- 레이어 2 브리지 테이블(브리지 그룹용)
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 시그널링 세션 및 핀홀.
- ICMP 연결 상태 — ICMP 연결 복제는 해당 인터페이스가 비대칭 라우팅 그룹에 할당된 경우에만 활성화됩니다.
- 정적 및 동적 라우팅 테이블 - 스테이트풀 페일오버는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 확인한 경로는 스탠바이 유닛

의 RIB(Routing Information Base) 테이블에 유지됩니다. 페일오버 이벤트 발생 시 액티브 보조 유닛에서는 초기 규칙에 따라 기본 유닛을 미러링하므로 트래픽 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 페일오버가 끝난 직후에는 새 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP 경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.

참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스탠바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적이고 정상적인 동작입니다.

- DHCP 서버 - DHCP 주소 임대는 복제되지 않습니다. 그러나 인터페이스에 구성된 DHCP 서버는 ping을 전송하여 특정 주소가 사용 중이지 않음을 확인한 후에 DHCP 클라이언트에 해당 주소를 부여하므로 서비스에는 영향이 없습니다. 상태 정보는 DHCP 릴레이 또는 DDNS와 관련이 없습니다.
- Cisco IP SoftPhone 세션 — 액티브 Cisco IP SoftPhone 세션 도중 페일오버가 일어날 경우, 통화 세션 상태 정보가 스탠바이 유닛에 복제되므로 통화는 활성 상태로 유지됩니다. 통화가 종료되면 IP SoftPhone 클라이언트와 Cisco Call Manager의 연결이 해제됩니다. 이러한 연결 손실이 일어나는 이유는 스탠바이 유닛에 CTIQBE 끊기 메시지에 대한 세션 정보가 없기 때문입니다. Call Manager에서 다시 보내는 응답이 특정 시간 내에 IP SoftPhone 클라이언트에 수신되지 않을 경우, 해당 Call Manager는 전달 불가능 상태로 간주되며 자체적으로 등록이 해제됩니다.
- RA VPN - 원격 액세스 VPN 최종 사용자는 페일오버 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 페일오버 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.

지원되지 않는 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 ASA로 전달되지 않습니다.

- 사용자 인증(uauth) 테이블
- TCP 상태 우회 연결
- 멀티캐스트 라우팅.
- ASA FirePOWER 모듈과 같은 모듈을 위한 상태 정보.
- 선택한 클라이언트 리스 SSL VPN 기능:
  - 스마트 터널
  - 포트 포워딩
  - 플러그인

- Java 애플릿
- IPv6 클라이언트리스 또는 AnyConnect 세션
- Citrix 인증(Citrix 사용자는 페일오버 후 다시 인증을 수행해야 함)

장애 조치를 위한 브리지 그룹 요구 사항

브리지 그룹 사용 시 장애 조치에 대해 특별히 고려해야 할 사항이 있습니다.

어플라이언스, ASAv에 대한 브리지 그룹 요구 사항

액티브 유닛에서 스탠바이 유닛으로 장애 조치를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하려면 스위치 포트 모드에 따라 다음 해결 방법 중 하나를 구성하십시오.

- 액세스 모드—스위치에서 STP PortFast 기능을 활성화합니다.

```
interface interface_id
  spanning-tree portfast
```

  PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 트렁크 모드 — 이더 타입 액세스 규칙이 있는 브리지 그룹의 멤버 인터페이스에서 ASA의 BPDU를 차단합니다.

```
access-list id ethertype deny bpdu
access-group id in interface name1
access-group id in interface name2
```

  BPDU를 차단하면 스위치의 STP가 비활성화됩니다. 네트워크 레이아웃에 ASA와 관련된 루프가 없도록 해야 합니다.

위의 옵션이 모두 가능하지 않을 경우, 다음 해결 방법 중 하나를 사용할 수 있으며 이 경우 장애 조치 기능 또는 STP 안정성에 다소 영향을 미치게 됩니다.

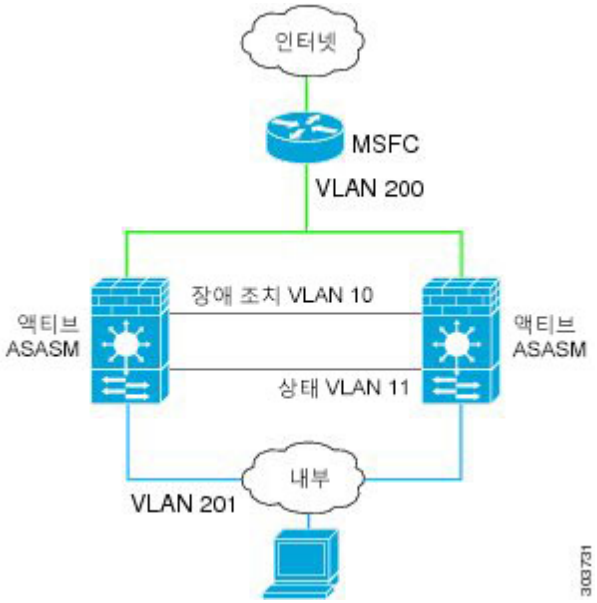
- 인터페이스 모니터링을 비활성화합니다.
- 인터페이스 대기 시간을 큰 값으로 늘려 ASA에서 장애 조치를 수행하기 전에 STP가 통합될 수 있도록 합니다.
- STP 타이머를 줄여 STP가 인터페이스 대기 시간보다 빨리 통합될 수 있도록 합니다.

ASA Services Module에 대한 브리지 그룹 요구 사항

브리지 그룹에서 장애 조치를 사용할 경우 루프를 방지하려면 BPDU가 전달되도록 해야 하며(기본값), BPDU 전달을 지원하는 스위치 소프트웨어를 사용해야 합니다.

두 모듈이 동시에 활성 상태이거나(예: 두 모듈에서 서로의 존재를 인지할 경우) 장애 조치 링크에 오류가 발생한 경우 루프가 발생할 수 있습니다. ASASM에서는 동일한 두 VLAN 간에 패킷을 연결하므로 브리지 그룹 멤버 인터페이스 간의 패킷이 두 ASASM에 의해 끊임없이 복제되는 경우 루프가 발생할 수 있습니다. BPDU가 적시에 교환되는 경우 Spanning Tree Protocol에서는 이러한 루프를 끊을 수 있습니다. 루프를 끊으려면 VLAN 200과 VLAN 201 간에 전송된 BPDU를 연결해야 합니다.

그림 ***49:*** 브리지 그룹 루프



장애 조치 상태 모니터링

ASA에서는 각 유닛의 전체 상태 및 인터페이스 상태를 모니터링합니다. 이 섹션에는 ASA에서 각 유닛의 상태를 확인하기 위해 테스트를 수행하는 방법에 대한 정보가 포함되어 있습니다.

유닛 상태 모니터링

ASA에서는 hello 메시지가 있는 장애 조치 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 장애 조치 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 장애 조치 링크를 비롯한 각 데이터 인터페이스에 LANTEST 메시지를 전송하여 피어의 응답 여부를 확인합니다. Firepower 9300 및 4100 Series에서 BFD(Bidirectional Forwarding Detection) 모니터링을 활성화할 수 있으며 이러한 모니터링은 hello 메시지보다 훨씬 안정적인 방법입니다. ASA에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다. 아래의 가능한 조치를 참조하십시오.

- ASA에서 장애 조치 링크에 대한 응답을 수신하지 못할 경우 장애 조치가 이루어지지 않습니다.

- ASA에서 장애 조치 링크에 대한 응답은 수신하지 못했으나 데이터 인터페이스에 대한 응답은 수신한 경우, 유닛에서 장애 조치를 수행하지 않습니다. 페일오버 링크가 실패한 것으로 표시됩니다. 페일오버 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버할 수 없으므로 최대한 빨리 페일오버 링크를 복원해야 합니다.
- ASA에서 인터페이스에 대한 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 실패한 것으로 분류합니다.

인터페이스 모니터링

최대 1025개의 인터페이스를 모니터링할 수 있습니다(다중 모드에서 해당되며 모든 상황 간에 분할됨). 중요한 인터페이스를 모니터링해야 합니다. 예를 들어 다중 모드에서 하나의 공유 인터페이스를 모니터링하기 위해 단일 상황을 구성할 수 있습니다. 인터페이스가 공유되므로, 모든 상황은 모니터링을 활용합니다.

2번의 폴링 기간 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 인터페이스 테스트가 실행됩니다. 인터페이스에 대한 모든 인터페이스 테스트가 실패하였으나 다른 유닛에 있는 이 동일한 인터페이스에서는 지속적으로 트래픽을 전달할 수 있는 경우, 해당 인터페이스는 오류가 발생한 것으로 간주합니다. 오류가 발생한 인터페이스의 임계값이 충족될 경우 장애 조치가 실행됩니다. 다른 유닛 인터페이스에서도 모든 네트워크 테스트가 실패할 경우, 두 인터페이스 모두 "Unknown" 상태가 되며 장애 조치 한도에 대해 가산되지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 장애 임계값이 더 이상 충족되지 않을 경우 장애가 발생한 ASA는 스탠바이 모드로 돌아갑니다.

ASA FirePOWER SSP 등의 서비스 모듈이 없는 경우 ASA에서는 백플레인 인터페이스에서 모듈의 상태를 모니터링합니다. 모듈의 오류를 유닛 오류로 간주하고 장애 조치를 시작합니다. 이 설정은 구성 가능합니다.

인터페이스에 구성된 IPv4 및 IPv6 주소가 없는 경우 ASA에서는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다.

인터페이스에 IPv6 주소만 구성되어 있으면 ASA에서는 ARP 대신 IPv6 네이버 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 ping 테스트의 경우 ASA에서는 IPv6 모든 노드 주소를 사용합니다(FE02::1).

참고 오류가 발생한 유닛에서 복구가 이루어지지 않고 오류가 발생해서는 안 되는 유닛일 경우 **failover reset** 명령을 입력하여 상태를 재설정할 수 있습니다. 그러나 장애 조치 상태가 지속되면 유닛에 다시 오류가 발생합니다.

인터페이스 테스트

ASA에서는 다음과 같은 인터페이스 테스트를 사용합니다.

1. 링크 작동/중단 테스트 - 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 중단되었는지 여부를 나타내며 ASA에서는 이 상태를 실패로 간주합니다. 작동 상태일 경우 ASA에서는 네트워크 활동 테스트를 수행합니다.

2. 네트워크 활동 테스트 - 수신된 네트워크 활동 테스트입니다. 이 테스트의 목적은 LANTEST 메시지를 사용하는 네트워크 트래픽을 생성하여 어떤 유닛에서 오류가 발생했는지 확인하는 것입니다. 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 유닛에서 테스트 동안(최대 5초) 임의의 패킷을 수신하는 즉시, 인터페이스는 작동 중으로 간주됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않을 경우, 트래픽이 수신되지 않은 유닛은 오류가 발생한 것으로 간주합니다. 유닛에서 트래픽을 수신하지 못한 경우, ASA에서는 ARP 테스트를 시작합니다.
3. ARP 테스트 - 최근에 얻은 항목 2개의 유닛 ARP 캐시를 읽는 테스트입니다. 유닛에서는 한 번에 하나씩 ARP 요청을 이러한 시스템에 전송하여 네트워크 트래픽의 시뮬레이션을 시도합니다. 각 요청 후 유닛에서는 최대 5초 동안 수신된 모든 트래픽의 수를 셉니다. 트래픽이 수신된 경우 해당 인터페이스는 제대로 작동 중인 것으로 간주합니다. 트래픽이 수신되지 않은 경우, ARP 요청이 다음 시스템에 전송됩니다. 목록 마지막에 트래픽이 수신되지 않은 경우 ASA에서는 ping 테스트를 시작합니다.
4. 브로드캐스트 ping 테스트 - 브로드캐스트 ping 요청을 전송하는 작업으로 이루어진 ping 테스트입니다. 그런 다음 유닛에서는 최대 5초 동안 수신된 모든 패킷의 수를 셉니다. 이 간격 동안 언제라도 수신된 패킷이 있을 경우 인터페이스가 작동 중인 것으로 간주되며 테스트가 중지됩니다. 모든 트래픽이 수신되지 않으면, 테스트는 ARP 테스트와 함께 다시 시작됩니다.

인터페이스 상태

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- No Link - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

장애 조치 시간

다음 표에는 최소, 기본 및 최대 장애 조치 시간이 나와 있습니다.

참고 CLI 또는 ASDM을 사용하여 수동으로 장애 조치하는 경우, 또는 ASA를 다시 로드하는 경우 장애 조치가 즉시 시작되고 아래에 나열된 타이머의 영향을 받지 않습니다.

표 ***11: ASA***

장애 조치 조건	최소	기본	최대
액티브 유닛의 전원이 중단되거나 정상적인 작동이 중지됩니다.	800밀리초	15초	45초
액티브 유닛 메인 보드 인터페이스 의 연결이 해제됩니다.	500밀리초	5초	15초
액티브 유닛 4GE 모듈 인터페이스 링크가 중단됩니다.	2초	5초	15초
액티브 유닛 FirePOWER 모듈에 장애가 발생합니다.	2초	2초	2초
액티브 유닛 인터페이스가 작동하지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

구성 동기화

장애 조치에는 다양한 유형의 구성 동기화가 포함됩니다.

실행 중인 구성 복제

하나 또는 두 디바이스가 모두 장애 조치 쌍 부팅 중일 경우 실행 중인 구성이 복제됩니다.

액티브/스탠바이 장애 조치에서 구성은 항상 액티브 유닛에서 스탠바이 유닛으로 동기화됩니다.

액티브/액티브 장애 조치에서 부팅 유닛의 기존 또는 보조 지정에 관계없이 두 번째로 부팅하는 유닛이 먼저 부팅하는 유닛에서 실행 중인 구성을 획득합니다. 두 유닛이 작동되면 시스템 실행 영역 공간에 입력되는 명령이 장애 조치 그룹 1이 액티브 상태인 유닛으로부터 복제됩니다.

스탠바이/두 번째 유닛에서 초기 시작을 완료하면 실행 중인 구성이 지워지며(**failover** 명령과 액티브 유닛이 통신을 수행해야 하는 경우는 예외), 액티브 유닛에서는 전체 구성을 스탠바이/두 번째 유닛으로 보냅니다. 복제가 시작되면 액티브 유닛의 ASA 콘솔에는 "Beginning configuration replication: Sending to mate"(구성 복제 시작: 짝으로 전송)이라는 메시지가 표시되며, 이 작업이 완료되면 ASA에서는 "End Configuration Replication to mate"(짝으로의 구성 복제 종료)라는 메시지가 표시됩니다. 구성의 크기에 따라 복제가 완료되기까지 몇 초에서 몇 분이 걸릴 수 있습니다.

구성을 수신하는 유닛에서 구성은 실행 중인 메모리에만 존재합니다. 에 따라 구성을 플래시 메모리 구성 변경사항 저장, 43 페이지에 저장해야 합니다. 예를 들어 액티브/액티브 장애 조치를 위해 유닛에서 액티브 상태인 장애 조치 그룹 1을 지닌 유닛의 시스템 실행 영역에 **write memory all** 명령을 입력합니다. 이 명령은 피어 유닛으로 복제되며 피어 유닛은 플래시 메모리에 구성을 작성합니다.

참고 복제가 실행되는 동안 구성을 전송하는 유닛에 입력된 명령은 피어 유닛에 제대로 복제되지 않을 수 있으며, 구성을 수신하는 유닛에 입력된 명령은 수신되는 구성으로 덮어씌워질 수 있습니다. 구성 복제 프로세스가 진행되는 동안에는 장애 조치 쌍의 유닛에 명령을 입력하지 마십시오.

참고 **crypto ca server** 명령 및 관련된 하위 명령은 장애 조치에서 지원되지 않습니다. **no crypto ca server** 명령을 사용하여 제거해야 합니다.

파일 복제

컨피그레이션 동기화 시 다음 파일 및 컨피그레이션 요소는 복제되지 않으므로, 이러한 파일을 수동으로 복사하여 일치시켜야 합니다.

- AnyConnect 이미지
- CSD 이미지
- AnyConnect 프로필

  ASA에서는 cache:/stc/profiles에 저장된 AnyConnect 클라이언트 프로필에 대해 캐시된 파일을 사용하며 플래시 파일 시스템에 저장된 파일은 사용하지 않습니다. 대기 유닛에서 AnyConnect 클라이언트 프로파일을 복제하려면, 다음 중 하나를 수행합니다.

  - 활성 유닛에서 **write standby** 명령을 입력합니다.
  - 활성 유닛에서 프로파일을 다시 적용합니다.
  - 대기 유닛을 다시 로드합니다.

- 로컬 CA(Certificate Authority)
- ASA 이미지
- ASDM 이미지

명령 복제

시작 후 활성 유닛에 입력하는 메시지는 대기 유닛에 즉시 복제됩니다. 활성 구성을 플래시 메모리에 저장하여 명령을 복제하지 않아도 됩니다.

액티브/액티브 장애 조치의 경우 시스템 실행 영역에 입력되는 명령은 장애 조치 그룹 1이 액티브 상태인 유닛으로부터 복제됩니다.

명령 복제를 실행할 해당 유닛에 명령을 입력하지 못할 경우 구성이 동기화되지 않습니다. 이러한 변경 사항은 다음번에 초기 컨피그레이션 동기화가 실행될 때 사라질 수 있습니다.

다음과 같은 명령이 스탠바이 ASA에 복제됩니다.

- **mode**, **firewall** 및 **failover lan unit**를 제외한 모든 구성 명령
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

다음과 같은 명령은 스탠바이 ASA에 복제되지 않습니다.

- 모든 형태의 **copy** 명령(**copy running-config startup-config** 제외)
- 모든 형태의 **write** 명령(**write memory** 제외)
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** 및 **pager**

액티브/스탠바이 페일오버 정보

액티브/스탠바이 페일오버에서는 스탠바이 ASA를 사용해 장애가 발생한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하는 경우 스탠바이 유닛이 액티브 유닛이 됩니다.

참고 다중 컨텍스트 모드의 경우 ASA는 전체 유닛(모든 컨텍스트 포함)에 대해 페일오버를 실행할 수 있으나 개별 컨텍스트를 대상으로 별도로 페일오버를 수행할 수는 없습니다.

기본/보조 역할 및 액티브/스탠바이 상태

페일오버 쌍의 두 유닛의 주된 차이점은 어느 유닛이 액티브 유닛이고 어느 유닛이 스탠바이 유닛인지와 관련 있습니다. 즉, 어떤 IP 주소를 사용하고 어떤 유닛이 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.

- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 페일오버 링크를 통해 기본 유닛의 MAC 주소를 획득할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

페일오버 이벤트

액티브/스탠바이 페일오버 시 페일오버는 유닛을 기준으로 실행됩니다. 다중 컨텍스트 모드에서 실행 중인 시스템에서도 개별 또는 컨텍스트 그룹으로는 페일오버를 수행할 수 없습니다.

다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 페일오버 이벤트에 적용되는 페일오버 정책(페일오버 실행 또는 페일오버 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 페일오버 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 ***12:*** 페일오버 이벤트

오류 이벤트	정책	액티브 그룹 조치	스탠바이 그룹 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 페일오버 링크에 대한 hello 메시지가 수신되지 않음
이전 액티브 유닛 복구	페일오버 없음	스탠바이 상태가 됨	작업 없음	없음
스탠바이 유닛 오류(전력 또는 하드웨어)	페일오버 없음	스탠바이가 실패한 것으로 표시됨	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

오류 이벤트	정책	액티브 그룹 조치	스탠바이 그룹 조치	참고
작동 중 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	페일오버 링크가 실패한 것으로 표시됨	페일오버가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버를 시작하지 못하므로 최대한 빨리 페일오버 링크를 복구해야 합니다.
시작 시 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	액티브 상태가 됨	시작 시 페일오버 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	페일오버가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	페일오버	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	페일오버 없음	작업 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

활성/활성 장애 조치 정보

이 섹션에서는 액티브/액티브 장애 조치에 대해 설명합니다.

활성/활성 장애 조치 개요

액티브/액티브 장애 조치 구성에서는 두 ASA가 모두 네트워크 트래픽을 전달할 수 있습니다. 액티브/액티브 장애 조치는 다중 상황 모드의 ASA에만 사용할 수 있습니다. 액티브/액티브 장애 조치에서 ASA의 보안 상황은 최대 2개의 장애 조치 그룹으로 나뉩니다.

장애 조치 그룹은 단순히 하나 이상의 보안 상황으로 구성된 논리적 그룹입니다. 기본 ASA에서 액티브 상태가 되는 장애 조치 그룹을 할당하고 보조 ASA에서 액티브 상태가 되는 장애 조치 그룹 2를 할당할 수 있습니다. 장애 조치는 장애 조치 그룹 수준에서 수행됩니다. 예를 들어, 인터페이스 장애 패턴에 따라 장애 조치 그룹 1에서 보조 ASA로 장애 조치를 실행하고, 그 후 장애 조치 그룹 2에서 기본

ASA로 장애 조치를 실행할 수 있습니다. 장애 조치 그룹 1의 인터페이스가 기본 ASA에서 중단되었으나 보조 ASA에서 작동 중이고, 장애 조치 그룹 2의 인터페이스가 보조 ASA에서는 중단되었으나 기본 ASA에서 작동 중인 경우 이러한 이벤트가 발생할 수 있습니다.

관리자 상황은 항상 장애 조치 그룹 1의 멤버입니다. 또한 할당되지 않은 모든 보안 상황도 기본적으로 장애 조치 그룹 1의 멤버입니다. 액티브/액티브 장애 조치만 수행하고 다중 상황은 사용하지 않으려는 경우, 가장 간단한 컨피그레이션 방법은 추가 상황 1개를 추가하고 이를 장애 조치 그룹 2에 할당하는 것입니다.

참고 액티브/액티브 장애 조치를 구성할 경우 두 유닛의 통합된 트래픽이 각 유닛의 용량 내에 있는지 확인해야 합니다.

참고 원하는 경우 두 장애 조치 그룹을 하나의 ASA에 할당할 수 있지만, 이렇게 하면 두 액티브 ASA의 장점을 활용할 수 없게 됩니다.

장애 조치 그룹의 기본/보조 역할 및 활성/대기 상태

활성/대기 장애 조치와 마찬가지로, 활성/활성 장애 조치 쌍에서 한 유닛은 기본 유닛으로 지정되고 다른 유닛은 보조 유닛으로 지정됩니다. 그러나 액티브/스탠바이 장애 조치와 달리, 기본 유닛과 보조 유닛이 지정되어도 두 유닛이 동시에 시작될 때 어느 유닛이 액티브 유닛이 되는지를 나타내지는 않습니다. 그 대신 기본/보조 유닛을 지정하는 작업에서는 다음 두 가지 역할을 수행합니다.

- 동시에 부팅이 시작될 경우 기본 유닛에서는 실행 중인 컨피그레이션을 해당하는 쌍에 제공합니다.
- 컨피그레이션의 각 장애 조치 그룹은 기본 또는 보조 유닛 기본 설정으로 컨피그레이션됩니다. 사전 대응 방식으로 사용하는 경우 이 환경 설정에서는 장애 조치가 시작된 이후에 올바른 유닛에서 장애 조치가 실행되고 있는지 확인합니다. 사전 조치 없이 두 그룹이 첫 번째 유닛에서 실행되어 부팅됩니다.

시작 시 장애 조치 그룹에 대한 액티브 유닛 결정

장애 조치 그룹에서 액티브 유닛이 되는 유닛은 다음에 따라 결정됩니다.

- 피어 유닛이 제공되지 않을 때 유닛이 부팅될 경우, 두 장애 조치 그룹은 유닛에서 활성 상태가 됩니다.
- 피어 유닛이 액티브 상태일 때(두 장애 조치 그룹이 모두 활성 상태일 때) 유닛이 부팅될 경우, 장애 조치 그룹의 기본 또는 보조 기본 설정에 상관없이 장애 조치 그룹은 액티브 유닛에서 활성 상태를 유지하며 이는 다음 중 한 가지 상황이 발생하지 않는 한 유효합니다.
  - 장애 조치가 발생할 경우
  - 장애 조치를 수동으로 강제 실행할 경우

- 장애 조치 그룹의 사전 대응 방식을 구성한 경우. 이 경우 유닛이 사용 가능한 상태가 되었을 때 장애 조치 그룹이 기본 유닛에서 자동으로 액티브 상태가 됨

페일오버 이벤트

액티브/액티브 장애 조치 컨피그레이션에서 장애 조치는 시스템이 아닌 장애 조치 그룹을 기준으로 실행됩니다. 예를 들어, 기본 유닛에서 두 장애 조치 그룹을 모두 액티브로 지정할 경우 장애 조치 그룹 1에 오류가 발생하면 장애 조치 그룹 2는 기본 유닛에서 액티브 상태를 유지하는 반면 장애 조치 그룹 1은 보조 유닛에서 액티브 상태가 됩니다.

장애 조치 그룹에는 다중 상황을 포함할 수 있고 각 상황에는 여러 인터페이스가 포함될 수 있으므로, 관련된 장애 조치 그룹에 오류가 발생하는 대신 단일 상황 내의 모든 인터페이스에 오류가 발생할 수 있습니다.

다음 표에는 각 장애 조치 이벤트에 대한 장애 조치가 나와 있습니다. 이 표에는 각 오류 이벤트에 대한 정책(장애 조치의 실행 여부 결정), 액티브 장애 조치 그룹에 대한 조치, 스탠바이 장애 조치 그룹에 대한 조치가 나와 있습니다.

표 ***13:*** 페일오버 이벤트

오류 이벤트	정책	액티브 그룹 조치	스탠바이 그룹 조치	참고
유닛에 전원 또는 소프트웨어 오류가 발생함	장애 조치	스탠바이가 실패한 것으로 표시됨	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	장애 조치 쌍의 유닛 1개에 오류가 발생할 경우, 해당 유닛의 액티브 장애 조치 그룹은 실패한 것으로 표시되며 피어 유닛에서 액티브 상태가 됩니다.
임계값을 넘은 액티브 장애 조치 그룹에서 인터페이스 오류 발생	장애 조치	액티브 그룹이 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 장애 조치 그룹에서 인터페이스 오류 발생	장애 조치 없음	작업 없음	스탠바이 그룹이 실패한 것으로 표시됨	스탠바이 장애 조치 그룹이 실패한 것으로 표시될 경우, 액티브 장애 조치 그룹에서는 장애 조치를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

오류 이벤트	정책	액티브 그룹 조치	스탠바이 그룹 조치	참고
이전 액티브 장애 조치 그룹 복구	장애 조치 없음	작업 없음	작업 없음	장애 조치 그룹 사전 대응 방식이 구성되지 않는 한 장애 조치 그룹은 해당 유닛에서 액티브 상태를 유지합니다.
시작 시 장애 조치 링크에 오류 발생	장애 조치 없음	액티브 상태가 됨	액티브 상태가 됨	시작 시 장애 조치 링크가 중단되면 두 유닛의 두 장애 조치 그룹 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	장애 조치가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
작동 중 장애 조치 링크에 오류 발생	장애 조치 없음	해당 없음	해당 없음	각 유닛에서 장애 조치 링크가 실패한 것으로 표시됨 장애 조치가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치를 시작하지 못하므로 최대한 빨리 장애 조치 링크를 복구해야 합니다.

장애 조치 라이센스

장애 조치 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다. 이 규칙에도 몇 가지 예외가 있습니다. 장애 조치에 대한 올바른 라이센싱 요건은 다음 표를 참조하십시오.

모델	라이센스 요건
ASA 5506-X 및 ASA 5506W-X	• 활성/대기 — Security Plus 라이센스. • 활성/활성 — 지원되지 않음. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.

모델	라이센스 요건
ASA 5512-X - ASA 5555-X	• ASA 5512 X — Security Plus 라이센스. • 기타 모델 — 기본 라이센스. 참고 • 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다. • 다중 상황 모드에서 각 유닛에는 동일한 AnyConnect Apex 라이선스가 있어야 합니다. • 각 유닛에는 동일한 IPS 모듈 라이선스가 있어야 합니다. 또한 두 유닛의 IPS에는 IPS 서명 서브스크립션이 필요합니다. 다음 지침을 참조하십시오. • 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다. • 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이선스가 아니므로 장애 조치에서 공유되지 않습니다. • IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이선스와 마찬가지로, IPS 모듈 라이선스는 장애 조치 클러스터 라이선스 내에서 기술적으로 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
ASAv	ASAv의 장애 조치 라이선스, 124 페이지을 참조하십시오.
Firepower 2100의 ASA	Firepower 2100의 장애 조치 라이선스, 125 페이지을 참조하십시오.
ASA - Firepower 4100/9300 섀시	ASA의 장애 조치 라이선스 - Firepower 4100/9300 섀시, 126 페이지을 참조하십시오.

모델	라이센스 요건
기타 모든 모델	Base 라이선스 또는 Standard 라이선스. 참고 • 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다. • 다중 상황 모드에서 각 유닛에는 동일한 AnyConnect Apex 라이선스가 있어야 합니다.

참고 유효한 영구 키가 필요합니다. 드문 경우지만 PAK 인증 키를 제거할 수 있습니다. 키가 모두 0으로 구성되어 있으면 장애 조치를 활성화하기 전에 유효한 인증 키를 다시 설치해야 합니다.

장애 조치 지침

상황 모드

- 액티브/액티브 모드는 다중 상황 모드에서만 지원됩니다.
- 다중 상황 모드의 경우, 달리 명시되지 않는 한 모든 단계가 시스템 실행 영역에서 수행됩니다.

모델 지원

- ASA 5506W-X — 내부 GigabitEthernet 1/9 인터페이스에 대해 인터페이스 모니터링을 비활성화해야 합니다. 이 인터페이스는 기본값 인터페이스 모니터링 확인을 수행하기 위해 통신할 수 없습니다. 그 결과 예상된 인터페이스 통신 오류 때문에 활성에서 대기 모드로 전환되며 다시 되돌아 갑니다.
- Firepower 9300의 ASA — 섀시 간 장애 조치를 사용하여 최상의 이중화를 수행하는 것이 좋습니다.
- Microsoft Azure 및 Amazon Web Services와 같은 퍼블릭 클라우드 네트워크에 있는 ASAv에서는 Layer 2 연결이 필요하기 때문에 장애 조치를 통해 지원되지 않습니다. 퍼블릭 클라우드의 고가용성을 위한 장애 조치, 329 페이지 섹션을 참조하십시오.
- ASA FirePOWER 모듈에서는 장애 조치를 직접 지원하지 않습니다. ASA 장애 조치가 끝나면 기존 ASA FirePOWER 플로우는 새로운 ASA에 전송됩니다. 새 ASA의 ASA FirePOWER 모듈은 해당 시점부터 트래픽을 검사하기 시작합니다. 이전 검사 상태는 전송되지 않습니다.

  일관된 장애 조치 동작을 보장하려면 고가용성 ASA 쌍의 ASA FirePOWER 모듈에 대해 일관된 정책을 유지 관리해야 합니다.

참고 ASA FirePOWER 모듈을 구성하기 전에 장애 조치 쌍을 생성합니다. 이 모듈이 두 디바이스에서 이미 구성된 경우, 장애 조치 쌍을 생성하기 전에 스탠바이 디바이스에서 인터페이스 구성을 지웁니다. 스탠바이 디바이스의 CLI에서 **clear configure interface** 명령을 입력합니다.

고가용성을 위한 **ASAv** 장애 조치

ASAv와 장애 조치 쌍을 생성할 때 동일한 순서로 각 ASAv에 데이터 인터페이스를 추가해야 합니다. 각 ASAv에 동일한 인터페이스를 추가했지만 순서가 다른 경우 ASAv 콘솔에서 오류가 나타날 수 있습니다. 장애 조치 기능도 영향을 받을 수 있습니다.

추가 지침

- 액티브 유닛에서 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하기 위해 스위치에서 STP PortFast 기능을 활성화할 수 있습니다.

  interface *interface_id* **spanning-tree portfast**

  이 해결 방법은 라우팅 모드 및 브리지 그룹 인터페이스에 모두 연결된 스위치에 적용됩니다. PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 로컬 CA 서버가 구성된 경우 장애 조치를 활성화할 수 없습니다. **no crypto ca server** 명령을 사용하여 CA 구성을 제거합니다.

- ASA 장애 조치 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 장애 조치 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확보한 보안 MAC 주소가 다른 보안 포트로 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.

- 한 유닛에서 모든 상황 전반에 걸쳐 최대 1025개의 인터페이스를 모니터링할 수 있습니다.

- 액티브/스탠바이 장애 조치 및 VPN IPsec 터널의 경우, VPN 터널을 통해 SNMP를 사용하여 액티브 유닛과 스탠바이 유닛을 모두 모니터링할 수는 없습니다. 스탠바이 유닛에는 활성 VPN 터널이 없으며 NMS로 전송되는 트래픽은 삭제됩니다. 암호화 기능이 있는 SNMPv3을 대신 사용하면 IPsec 터널을 사용하지 않아도 됩니다.

- 액티브/액티브 장애 조치의 경우 같은 ASR 그룹의 같은 상황에서 2개의 인터페이스를 구성할 수 없습니다.

- 액티브/액티브 장애 조치의 경우 최대 2개의 장애 조치 그룹을 정의할 수 있습니다.

- 액티브/액티브 장애 조치의 경우 장애 조치 그룹을 제거할 때 장애 조치 그룹 1을 마지막에 제거해야 합니다. 장애 조치 그룹 1에는 관리자 상황이 항상 포함됩니다. 장애 조치 그룹에 할당되지

않은 모든 상황은 장애 조치 그룹 1에 기본 설정됩니다. 상황이 명시적으로 할당된 장애 조치 그룹은 제거할 수 없습니다.

장애 조치 기본값

기본적으로 장애 조치 정책은 다음과 같이 구성됩니다.

- HTTP 복제가 없는 스테이트풀 장애 조치
- 단일 인터페이스 오류 시 장애 조치 발생
- 인터페이스 폴링 시간 5초
- 인터페이스 대기 시간 25초
- 유닛 폴링 시간 1초
- 유닛 대기 시간 15초
- 가상 MAC 주소는 기본적으로 활성화되어 있는 ASASM을 제외하고 다중 상황 모드에서 비활성화되어 있습니다.
- 모든 물리적 인터페이스 또는 ASASM, 모든 VLAN 인터페이스에 대한 모니터링

활성/대기 장애 조치 구성

액티브/스탠바이 장애 조치를 구성하려면 기본 유닛과 보조 유닛 모두에서 기본 장애 조치 설정을 구성합니다. 다른 모든 구성은 기본 유닛에서만 수행된 다음, 보조 유닛에 동기화됩니다.

활성/대기 장애 조치를 위한 기본 유닛 구성

이 섹션의 단계에 따라 활성/대기 장애 조치 구성에서 기본 유닛을 구성하십시오. 이러한 단계에서는 기본 유닛에서 장애 조치를 사용하는 데 필요한 최소 구성을 제공합니다.

시작하기 전에

- 장애 조치 및 상태 링크를 제외한 모든 인터페이스에 사용할 스탠바이 IP 주소를 구성하는 것이 좋습니다. 지점 간 연결을 위해 31비트 서브넷 마스크를 사용하는 경우, 스탠바이 IP 주소를 구성하지 마십시오.
- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 이 유닛을 기본 유닛으로 지정합니다.

failover lan unit primary

단계 **2** 장애 조치 링크로 사용할 인터페이스를 지정합니다.

failover lan interface *if_name interface_id*

예제:

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

이 인터페이스는 다른 용도로 사용할 수 없습니다(선택에 따라 상태 링크의 경우는 제외).

if_name 인수를 사용하면 인터페이스에 이름이 할당됩니다.

interface_id 인수는 데이터 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*를 사용하면 VLAN ID가 지정됩니다. 이제 ASA 5506H-X에서만 장애 조치 링크로 Management 1/1 인터페이스를 지정할 수 있습니다. 이 작업을 수행하면 **write memory**로 구성을 저장하고 디바이스를 **reload**해야 합니다. 그런 다음에는 장애 조치에 이 인터페이스를 사용할 수 없으며 ASA Firepower 모듈은 사용할 수 있습니다. 이 모듈에는 관리를 위해 인터페이스가 필요하며 한 가지 기능에만 사용할 수 있습니다. Firepower 9300 ASA 보안 모듈에서 데이터 또는 관리 유형 인터페이스를 사용할 수 있습니다.

단계 **3** 활성 및 대기 IP 주소를 장애 조치 링크에 할당합니다.

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

예제:

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

또는

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

이 주소는 사용되지 않는 서브넷에 있어야 합니다. 이 서브넷은 두 개의 IP 주소만 사용하며 31비트(255.255.255.254)가 될 수 있습니다.

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다.

단계 **4** 장애 조치 링크를 활성화합니다.

interface *failover_interface_id*

no shutdown

예제:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

단계 **5** (선택사항) 상태 링크로 사용하려는 인터페이스를 지정합니다.

failover link *if_name interface_id*

예제**:**

```
ciscoasa(config)# failover link folink gigabitethernet0/3
```

장애 조치 링크는 상태 링크와 함께 공유할 수 있습니다.

if_name 인수는 인터페이스에 이름을 할당합니다.

interface_id 인수는 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

단계 **6** 별도의 상태 링크를 지정한 경우 상태 링크에 활성 및 대기 IP 주소를 할당합니다.

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

예제**:**

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

또는

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

이 주소는 장애 조치 링크와 다른 사용되지 않는 서브넷에 있어야 합니다. 이 서브넷은 두 개의 IP 주소만 사용하며 31비트(255.255.255.254)가 될 수 있습니다.

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다.

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

단계 **7** 별도의 상태 링크를 지정한 경우 해당 상태 링크를 활성화합니다.

interface*state_interface_id*

no shutdown

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

단계 **8** (선택사항) 다음 중 하나를 수행하여 장애 조치 및 상태 링크에 대한 통신을 암호화합니다.

- (권장) 유닛 간의 장애 조치 및 상태 링크에 대한 IPsec LAN-LAN 터널을 설정하여 모든 장애 조치 통신을 암호화합니다.

  failover ipsec pre-shared-key [**0** | **8**] *key*

  예:

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  키의 최대 길이는 128자입니다. 두 유닛의 동일한 키를 식별합니다. IKEv2에서는 이 키를 사용하여 터널을 설정합니다.

  마스터 패스프레이즈(마스터 패스프레이즈 구성, 689 페이지 참조)를 사용할 경우 구성에서 키가 암호화됩니다. 구성에서(예: **more system:running-config** 출력에서) 복사할 경우 **8** 키워드를 사용하여 키가 암호화되는지 지정합니다. 기본적으로 **0**이 사용되며 암호화되지 않은 비밀번호를 지정합니다.

  failover ipsec pre-shared-key는 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다.

  장애 조치 및 상태 링크 암호화를 구성하지 않을 경우, 명령을 복제하는 동안 전송되는 장애 조치 통신(구성의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

  IPsec 암호화와 기존 **failover key** 암호화를 함께 사용할 수는 없습니다. 두 방법을 모두 구성할 경우 IPsec가 사용됩니다. 그러나 마스터 패스프레이즈를 사용할 경우, IPsec 암호화를 구성하기 전에 **no failover key** 명령을 사용하여 장애 조치 키를 제거해야 합니다.

  장애 조치 LAN-LAN 터널의 경우 IPsec(기타 VPN) 라이센스는 계산에 포함하지 않습니다.

- (선택사항) 장애 조치 및 상태 링크에 대한 장애 조치 통신을 암호화합니다.

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  예:

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1~63자로 된 *shared_secret* 또는 32자로 된 **hex** *key*를 사용합니다. *shared_secret*의 경우 숫자, 문자 또는 구두점을 조합하여 사용할 수 있습니다. 공유 비밀 또는 16진수 키는 암호화 키를 생성하는 데 사용됩니다. 두 유닛의 동일한 키를 식별합니다.

  마스터 패스프레이즈(마스터 패스프레이즈 구성, 689 페이지 참조)를 사용할 경우 구성에서 공유 비밀 또는 16진수 키가 암호화됩니다. 구성에서(예: **more system:running-config** 출력에서) 복사할 경우 **8** 키워드를 사용하여 공유 암호 또는 16진수 키가 암호화되는지 지정합니다. 기본적으로 **0**이 사용되며 암호화되지 않은 비밀번호를 지정합니다.

  failover key shared secret은 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다.

  장애 조치 및 상태 링크 암호화를 구성하지 않을 경우, 명령을 복제하는 동안 전송되는 장애 조치 통신(구성의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

단계 **9** 장애 조치를 사용하도록 설정합니다.

failover

단계 **10** 플래시 메모리에 시스템 구성을 저장합니다.

write memory

예

다음 예에서는 기본 유닛의 장애 조치 파라미터를 구성합니다.

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

활성/대기 장애 조치를 위한 보조 유닛 구성

보조 유닛에 필요한 유일한 구성은 장애 조치 링크에 대한 구성입니다. 보조 유닛에서 기본 유닛과 처음 통신을 수행하려면 이러한 명령이 필요합니다. 기본 유닛에서 해당 구성을 보조 유닛으로 전송하면 두 구성 간의 유일한 영구적인 차이점은 **failover lan unit** 명령이며, 이 명령에서는 각 유닛을 기본 또는 보조 유닛으로 식별합니다.

시작하기 전에

- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** **failover lan unit primary** 명령을 제외하고 기본 유닛과 동일한 명령을 다시 입력합니다. 선택에 따라 이를 **failover lan unit secondary** 명령으로 대체할 수도 있으나, **secondary**가 기본 설정이므로 필수 사항은 아닙니다. 활성/대기 장애 조치를 위한 기본 유닛 구성, 297 페이지를 참조하십시오.

예를 들면 다음과 같습니다.

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config-ifc)# failover link folink gigabitethernet0/3
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

단계 **2** 장애 조치 구성을 동기화한 후 구성을 플래시 메모리에 저장합니다.

```
ciscoasa(config)# write memory
```

활성/활성 장애 조치 구성

이 섹션에서는 액티브/액티브 장애 조치를 구성하는 방법을 설명합니다.

활성/활성 장애 조치를 위한 기본 유닛 구성

이 섹션의 단계에 따라 활성/활성 장애 조치 구성에서 기본 유닛을 구성하십시오. 이러한 단계에서는 기본 유닛에서 장애 조치를 사용하는 데 필요한 최소 구성을 제공합니다.

시작하기 전에

- 다중 상황 모드 활성화 또는 비활성화, 232 페이지에 따라 다중 상황 모드를 활성화합니다.
- 라우팅 및 투명 모드 인터페이스, 609 페이지에 따라 장애 조치 및 상태 링크를 제외한 모든 인터페이스에 사용할 스탠바이 IP 주소를 구성하는 것이 좋습니다. 지점 간 연결을 위해 31비트 서브넷 마스크를 사용하는 경우, 스탠바이 IP 주소를 구성하지 마십시오.
- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 이 유닛을 기본 유닛으로 지정합니다.

failover lan unit primary

단계 **2** 장애 조치 링크로 사용할 인터페이스를 지정합니다.

failover lan interface *if_name interface_id*

예제:

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

이 인터페이스는 다른 용도로 사용할 수 없습니다(선택에 따라 상태 링크의 경우는 제외).

if_name 인수는 인터페이스에 이름을 할당합니다.

interface_id 인수는 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

단계 **3** 활성 및 대기 IP 주소를 장애 조치 링크에 할당합니다.

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

예제:

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

또는

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

이 주소는 사용되지 않는 서브넷에 있어야 합니다. 이 서브넷은 두 개의 IP 주소만 사용하며 31비트(255.255.255.254)가 될 수 있습니다.

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다.

단계 **4** 장애 조치 링크를 활성화합니다.

interface *failover_interface_id*

no shutdown

예제:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

단계 **5** (선택사항) 상태 링크로 사용하려는 인터페이스를 지정합니다.

failover link *if_name interface_id*

예제:

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

장애 조치 링크 또는 데이터 인터페이스와 별도의 인터페이스를 지정하는 것이 좋습니다.

if_name 인수는 인터페이스에 이름을 할당합니다.

interface_id 인수는 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

단계 **6** 별도의 상태 링크를 지정한 경우 상태 링크에 활성 및 대기 IP 주소를 할당합니다.

이 주소는 장애 조치 링크와 다른 사용되지 않는 서브넷에 있어야 합니다. 이 서브넷은 두 개의 IP 주소만 사용하며 31비트(255.255.255.254)가 될 수 있습니다.

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다.

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

예제:

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

또는

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

단계 **7** 별도의 상태 링크를 지정한 경우 해당 상태 링크를 사용합니다.

interface*state_interface_id*

no shutdown

예제:

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

단계 **8** (선택사항) 다음 중 하나를 수행하여 장애 조치 및 상태 링크에 대한 통신을 암호화합니다.

- (권장) 유닛 간의 장애 조치 및 상태 링크에 대한 IPsec LAN-LAN 터널을 설정하여 모든 장애 조치 통신을 암호화합니다.

  failover ipsec pre-shared-key [**0** | **8**] *key*

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  키의 최대 길이는 128자입니다. 두 유닛의 동일한 키를 식별합니다. IKEv2에서는 이 키를 사용하여 터널을 설정합니다.

  마스터 패스프레이즈(마스터 패스프레이즈 구성, 689 페이지 참조)를 사용할 경우 구성에서 키가 암호화됩니다. 구성에서(예: **more system:running-config** 출력에서) 복사할 경우 **8** 키워드를 사용하여 키가 암호화되었는지 지정합니다. 기본적으로 **0**이 사용되며 암호화되지 않은 비밀번호를 지정합니다.

  failover ipsec pre-shared-key는 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다.

  장애 조치 및 상태 링크 암호화를 구성하지 않을 경우, 명령을 복제하는 동안 전송되는 장애 조치 통신(구성의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

IPsec 암호화와 기존 **failover key** 암호화를 함께 사용할 수 없습니다. 두 방법을 모두 구성할 경우 IPsec가 사용됩니다. 그러나 마스터 패스프레이즈를 사용할 경우, IPsec 암호화를 구성하기 전에 우선 **no failover key** 명령을 사용하여 장애 조치 키를 제거해야 합니다.

장애 조치 LAN-LAN 터널의 경우 IPsec(기타 VPN) 라이센스는 계산에 포함하지 않습니다.

- (선택사항) 장애 조치 및 상태 링크에 대한 장애 조치 통신을 암호화합니다.

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1~63자로 된 *shared_secret* 또는 32자로 된 **hex** *key*를 사용합니다.

  *shared_secret*의 경우 숫자, 문자 또는 구두점을 조합하여 사용할 수 있습니다. 공유 비밀 또는 16진수 키는 암호화 키를 생성하는 데 사용됩니다. 두 유닛의 동일한 키를 식별합니다.

  마스터 패스프레이즈(마스터 패스프레이즈 구성, 689 페이지 참조)를 사용할 경우 구성에서 공유 비밀 또는 16진수 키가 암호화됩니다. 구성에서(예: **more system:running-config** 출력에서) 복사할 경우 **8** 키워드를 사용하여 공유 비밀 또는 16진수 키가 암호화되었는지 지정합니다. 기본적으로 **0**이 사용되며 암호화되지 않은 비밀번호를 지정합니다.

  failover key shared secret은 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다.

  장애 조치 및 상태 링크 암호화를 구성하지 않을 경우, 명령을 복제하는 동안 전송되는 장애 조치 통신(구성의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

단계 **9** 장애 조치 그룹 1을 생성합니다.

failover group 1

primary

preempt [*delay*]

예제**:**

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

일반적으로 그룹 1은 기본 유닛에 할당하고 그룹 2는 보조 유닛에 할당합니다. 그룹에 대한 기본 설정 또는 보조 설정과 관계없이 장애 조치 그룹은 먼저 부팅되는 유닛에서 액티브 상태가 됩니다(동시에 부팅되는 것처럼 보이지만 한 유닛이 먼저 액티브 상태가 됨). **preempt** 명령을 사용하면 유닛이 사용 가능한 상태가 되었을 때 지정된 유닛에서 장애 조치 그룹이 자동으로 활성 상태가 됩니다.

지연 값(선택 사항)을 입력할 수 있으며, 이 값은 지정된 유닛에서 자동으로 액티브 상태가 되기 전에 장애 조치 그룹이 현재 유닛에서 액티브 상태로 유지되는 시간(초 단위)을 지정합니다. 유효한 값은 1 ~ 1200입니다.

스테이트풀 장애 조치를 사용할 경우, 장애 조치 그룹이 현재 액티브 상태로 있는 유닛에서 연결이 복제될 때까지 사전 대응이 지연됩니다.

수동으로 장애 조치를 수행하는 경우 **preempt** 명령은 무시됩니다.

단계 **10** 장애 조치 그룹 2를 생성하고 이를 보조 유닛에 할당합니다.

failover group 2

secondary

preempt [*delay*]

예제**:**

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

단계 **11** 제공된 상황에 대한 상황 컨피그레이션 모드로 들어간 다음 장애 조치 그룹에 상황을 할당합니다.

context *name*

join-failover-group{**1** | **2**}

예제**:**

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

각 상황에 이 명령을 반복합니다.

할당되지 않은 모든 상황은 장애 조치 그룹 1에 자동으로 할당됩니다. 관리자 상황은 항상 장애 조치 그룹 1의 멤버이며 이를 그룹 2에 할당할 수 없습니다.

단계 **12** 장애 조치를 사용하도록 설정합니다.

failover

단계 **13** 플래시 메모리에 시스템 구성을 저장합니다.

write memory

예

다음 예에서는 기본 유닛의 장애 조치 파라미터를 구성합니다.

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
```

```
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

활성/활성 장애 조치를 위한 보조 유닛 구성

보조 유닛에 필요한 유일한 구성은 장애 조치 링크에 대한 구성입니다. 보조 유닛에서 기본 유닛과 처음 통신을 수행하려면 이러한 명령이 필요합니다. 기본 유닛에서 해당 구성을 보조 유닛으로 전송하면, 두 구성 간의 유일한 영구적인 차이점은 **failover lan unit** 명령이며 이 명령은 각 유닛을 기본 또는 보조 유닛으로 식별합니다.

시작하기 전에

- 다중 상황 모드 활성화 또는 비활성화, 232 페이지에 따라 다중 상황 모드를 활성화합니다.
- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** **failover lan unit primary** 명령을 제외하고 기본 유닛과 동일한 명령을 다시 입력합니다. 선택에 따라 이를 **failover lan unit secondary** 명령으로 대체할 수도 있으나, **secondary**가 기본 설정이므로 필수 사항은 아닙니다. **failover group** 및 **join-failover-group** 명령은 기본 유닛에서 복제되므로 이러한 명령은 입력하지 않아도 됩니다. 활성/활성 장애 조치를 위한 기본 유닛 구성, 302 페이지를 참조하십시오.

예를 들면 다음과 같습니다.

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

단계 **2** 기본 유닛에서 장애 조치 구성을 동기화한 후 구성을 플래시 메모리에 저장합니다.

ciscoasa(config)# **write memory**

단계 **3** 필요한 경우, 장애 조치 그룹 2가 보조 유닛에서 활성 상태가 되도록 강제 설정합니다.

failover active group 2

선택적 장애 조치 파라미터 구성

원하는 경우 장애 조치 설정을 맞춤화할 수 있습니다.

장애 조치 기준 및 기타 설정 구성

이 섹션에서 변경할 수 있는 다양한 매개변수에 대한 기본 설정은 장애 조치 기본값, 297 페이지를 참조하십시오. 액티브/액티브 모드에서는 장애 조치 그룹당 가장 많은 기준을 설정합니다.

시작하기 전에

- 다중 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.
- 유닛 상태 모니터링을 위한 BFD(Bidirectional Forwarding Detection)에 대한 내용은 다음 제한 사항을 참조하십시오.
  - Firepower 9300 및 4100만 해당합니다.
  - 액티브/스탠바이만 해당합니다.
  - 라우팅 모드만 해당합니다.

프로시저

단계 **1** 유닛 폴링 및 대기 시간을 변경합니다.

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

예제:

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

polltime 범위는 1~15초 또는 200~999밀리초입니다. **holdtime** 범위는 1~ 45초 또는 800~999밀리초입니다. 유닛 폴링 시간의 3배보다 작은 보류 시간 값은 입력할 수 없습니다. 폴링 시간이 빠를수록 ASA에서 더욱 신속하게 장애를 탐지하고 장애 조치를 시행할 수 있습니다. 그러나 감지 기능이 빨라지면 네트워크에 일시적으로 정체 현상이 일어났을 때 불필요한 전환이 발생할 수 있습니다.

한 차례의 폴링 기간 동안 장애 조치 통신 인터페이스에 대한 hello 패킷이 유닛에 수신되지 않을 경우, 나머지 인터페이스 전체에 추가 테스트가 이루어집니다. 대기 시간에도 피어 유닛의 응답이 없을 경우 그 유닛에 오류가 발생한 것으로 간주하며, 오류가 발생한 유닛이 활성 유닛이었다면 대기 유닛이 활성 유닛으로 전환합니다.

활성/활성 모드에서 시스템에 대한 이러한 속도를 설정합니다. 이러한 속도는 장애 조치 그룹당 설정할 수 없습니다.

단계 **2** 유닛 상태 모니터링을 위해 BFD를 구성합니다.

정기적인 유닛 모니터링으로 인해 CPU 사용량이 많을 때 잘못된 알람이 발생할 수 있습니다. 높은 CPU가 작업에 영향을 주지 않으므로 BFD 방법이 배포됩니다.

a) 장애 조치 상태 탐지에 사용할 BFD 템플릿을 정의합니다.

bfd-template single-hop*template_name*

bfd interval min-tx *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier_value*

예제**:**

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

min-tx를 사용하면 BFD 제어 패킷이 장애 조치 피어로 전송되는 속도가 지정됩니다. 범위는 50~999밀리초입니다. **min-rx**를 사용하면 BFD 제어 패킷이 장애 조치 피어에서 수신될 것으로 예상되는 속도가 지정됩니다. 범위는 50~ 999밀리초입니다. **multiplier** 를 사용하면 BFD에서 피어를 사용할 수 없는 것으로 선언하기 전에 장애 조치 피어에서 누락되어야 하는 연속 BFD 제어 패킷의 수가 지정됩니다. 범위는 3~50개입니다.

이 템플릿에 대한 에코 및 인증을 구성할 수도 있습니다. BFD 템플릿 생성, 850 페이지의 내용을 참조하십시오.

b) 상태 모니터링을 위해 BFD를 활성화합니다.

failover health-check bfd *template_name*

예제**:**

```
ciscoasa(config)# failover health-check bfd failover-temp
```

단계 **3** 인터페이스 링크 상태 폴링 시간을 변경합니다.

failover polltime link-state msec *poll_time*

예제**:**

```
ciscoasa(config)# failover polltime link-state msec 300
```

범위는 300~799밀리초입니다. 기본적으로 장애 조치 쌍의 각 ASA는 해당 인터페이스의 링크 상태를 500밀리초마다 확인합니다. 이제 폴링 시간을 맞춤화할 수 있습니다. 예를 들어, 폴링 시간을 300밀리초로 설정하면 ASA에서 인터페이스 장애를 탐지하고 더 빨리 장애 조치를 트리거할 수 있습니다.

활성/활성 모드에서 시스템에 대한 이러한 속도를 설정합니다. 이러한 속도는 장애 조치 그룹당 설정할 수 없습니다.

단계 **4** 초당 연결의 세션 복제 속도를 설정합니다.

failover replication rate *conns*

예제**:**

```
ciscoasa(config)# failover replication rate 20000
```

최소 및 최대 속도는 모델에 따라 결정됩니다. 기본값은 최대 속도입니다. 활성/활성 모드에서 시스템에 대한 이러한 속도를 설정합니다. 이러한 속도는 장애 조치 그룹당 설정할 수 없습니다.

단계 **5** 스탠바이 유닛 또는 상황에서 컨피그레이션을 직접 변경하려면 이 기능을 비활성화합니다.

failover standby config-lock

기본적으로 스탠바이 유닛/상황에서 컨피그레이션을 수행하는 작업은 경고 메시지와 함께 허용됩니다.

단계 **6** (활성/활성 모드에만 해당) 사용자 지정하려는 장애 조치 그룹을 지정합니다.

failover group {**1** | **2**}

예제**:**

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

단계 **7** HTTP 상태 복제를 사용하도록 설정합니다.

- 활성/대기 모드의 경우:

  failover replication http

- 활성/활성 모드의 경우:

  replication http

HTTP 연결이 상태 정보 복제에 포함될 수 있도록 하려면 HTTP 복제를 사용하도록 설정해야 합니다. 보통 HTTP 클라이언트에서는 오류가 발생한 연결을 다시 수행하려고 시도하기 때문에 HTTP 연결은 짧은 것이 일반적입니다. HTTP 연결은 복제된 상태 정보에 자동으로 포함되지 않습니다.

참고 장애 조치를 사용할 때 스탠바이 유닛에서 HTTP 플로우를 삭제하면서 지연이 발생하므로 **show conn count** 출력은 액티브 유닛과 스탠바이 유닛에서 다른 수를 표시할 수 있습니다. 수 초간 기다리는 경우 명령을 재발행하면 두 유닛에 동일한 수가 표시됩니다.

단계 **8** 인터페이스에 오류가 발생할 경우에 대한 장애 조치의 임계값을 설정합니다.

- 활성/대기 모드의 경우:

  failover interface-policy *num* [%]

  예:

```
ciscoasa (config)# failover interface-policy 20%
```

- 활성/활성 모드의 경우:

  interface-policy *num* [%]

  예:

```
ciscoasa(config-fover-group)# interface-policy 20%
```

기본적으로 하나의 인터페이스에 오류가 발생하면 장애 조치가 실행됩니다.

인터페이스의 특정 개수를 지정할 경우, *num* 인수의 지원되는 범위는 1에서 1025까지입니다.

인터페이스의 백분율을 지정할 경우, *num* 인수의 지원되는 범위는 1에서 100까지입니다.

단계 **9** 인터페이스 폴링 및 대기 시간을 변경합니다.

- 활성/대기 모드의 경우:

  failover polltime interface [**msec**] *time* [**holdtime** *time*]

  예:

```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

- 활성/활성 모드의 경우:

  polltime interface [**msec**] *time* [**holdtime***time*]

  예:

```
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
```

폴링 시간의 올바른 값의 범위는 1~15초입니다. **msec** 키워드(선택 사항)가 사용될 경우, 범위는 500~999 밀리초입니다. 대기 시간은 인터페이스가 실패한 것으로 표시될 때 hello 패킷이 손실되는 데 소요된 시간을 결정합니다. 대기 시간의 올바른 값은 5~75초입니다. 대기 시간은 폴링 시간보다 5배 적게 입력할 수 없습니다.

인터페이스 링크가 중단되면 인터페이스 테스트가 시행되지 않으며, 오류가 발생한 인터페이스의 개수가 구성된 장애 조치 기준과 일치하거나 이를 초과할 경우 한 차례의 인터페이스 폴링 기간 동안에만 대기 유닛이 활성 상태가 됩니다.

단계 **10** 인터페이스에 가상 MAC 주소를 구성합니다.

- 활성/대기 모드의 경우:

  failover mac address *phy_if active_mac standby_mac*

  예:

```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- 활성/활성 모드의 경우:

  mac address *phy_if active_mac standby_mac*

  예:

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

phy_if 인수는 gigabitethernet0/1와 같은 인터페이스의 물리적인 이름입니다.

active_mac 및 *standby_mac* 인수는 H.H.H 형식으로 된 MAC 주소이며 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다.

active_mac 주소는 인터페이스의 액티브 IP 주소와 연결되며, *standby_mac*은 인터페이스의 스탠바이 IP 주소와 연결됩니다.

다른 명령이나 방법을 사용하여 MAC 주소를 설정할 수도 있으나, 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

show interface 명령을 사용하여 인터페이스에서 사용되는 MAC 주소를 표시합니다.

단계 **11** (액티브/액티브 모드에만 해당) 다른 장애 조치 그룹에 이 절차를 반복합니다.

인터페이스 모니터링

기본적으로 모니터링은 모든 물리적 인터페이스 또는 ASASM, 모든 VLAN 인터페이스, ASA에 설치된 모든 하드웨어 또는 소프트웨어 모듈(예: ASA FirePOWER 모듈)에서 사용됩니다. 중요도가 낮은 네트워크에 연결된 인터페이스를 제외하여 장애 조치 정책에 영향을 미치지 않도록 하고자 할 수 있습니다.

시작하기 전에

- 한 유닛에서 최대 1025개의 인터페이스를 모니터링할 수 있습니다(다중 상황 모드의 전체 상황 전반에 걸쳐).
- 다중 상황 모드에서 각 상황 내에 인터페이스를 구성합니다.

프로시저

인터페이스에 대한 상태 모니터링을 활성화하거나 비활성화합니다.

[**no**] **monitor-interface** {*if_name* | **service-module**}

예제:

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

ASA FirePOWER 모듈과 같은 하드웨어 또는 소프트웨어 모듈 장애로 인해 장애 조치가 일어나지 않도록 하려는 경우 **no monitor-interface service-module** 명령을 사용하여 모듈 모니터링을 비활성화할 수 있습니다. ASA 5585-X에서 서비스 모듈 모니터링을 비활성화하는 경우 개별적으로 모니터링되는 모듈의 인터페이스 모니터링도 비활성화할 수 있습니다.

비대칭 라우팅 패킷을 위한 지원 구성(활성/활성 모드)

활성/활성 장애 조치에서 실행 중인 경우, 유닛의 피어 유닛을 통해 시작된 연결에 대한 반환 패킷이 유닛에 수신될 수 있습니다. 패킷을 수신하는 ASA에 패킷에 대한 연결 정보가 없으므로 패킷이 손실됩니다. 액티브/액티브 장애 조치 쌍에 있는 두 ASA가 서로 다른 서비스 공급자에 연결되어 있고, 아웃바운드 연결에서 NAT 주소를 사용하지 않을 경우 이러한 손실 현상이 자주 일어납니다.

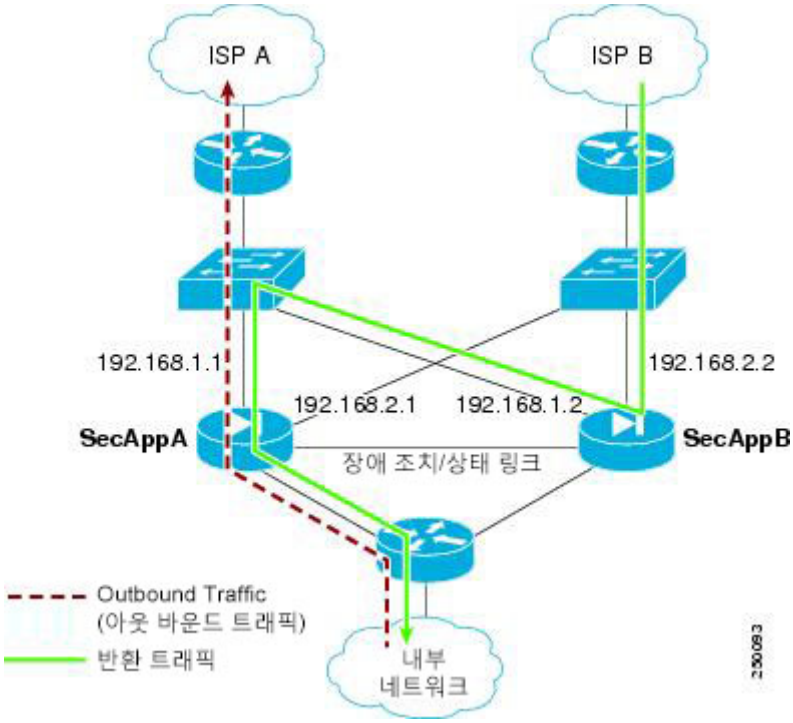
비대칭 라우팅 패킷을 사용하여 반환 패킷이 손실되는 것을 방지할 수 있습니다. 이렇게 하려면 각 ASA의 유사한 인터페이스를 동일한 ASR 그룹에 할당합니다. 예를 들어, 두 ASA는 모두 내부 인터페이스의 내부 네트워크에 연결되지만 외부 인터페이스의 별도의 ISP에 연결됩니다. 기본 유닛에서는 ASR 그룹 1에 활성 상황 외부 인터페이스를 할당하고, 보조 유닛에서는 동일한 ASR 그룹 1에 활성 상황 외부 인터페이스를 할당합니다. 기본 유닛의 외부 인터페이스에 세션 정보가 없는 패킷이 수신될 경우, 동일한 그룹(이 경우에는 ASR 그룹 1)에 있는 스탠바이 상황의 다른 인터페이스에 대한 세션 정보를 검사합니다. 일치하는 정보가 없을 경우 해당 패킷은 손실됩니다. 일치하는 정보가 있을 경우 다음 작업 중 하나가 실행됩니다.

- 수신 트래픽이 피어 유닛에서 시작된 경우, 레이어 2 헤더의 일부 또는 전체가 다시 작성되고 패킷이 다른 유닛에 리디렉션됩니다. 이러한 리디렉션은 세션이 활성화되어 있는 동안 지속합니다.
- 수신 트래픽이 동일한 유닛의 다른 인터페이스에서 시작된 경우, 레이어 2 헤더의 일부 또는 전체가 다시 작성되고 패킷이 스트림으로 다시 삽입됩니다.

참고 이 기능에서는 비대칭 라우팅을 제공하지 않으며, 비대칭 라우팅 패킷을 올바른 인터페이스로 복원하는 역할을 합니다.

다음 그림에는 비대칭 라우팅 패킷의 예가 나와 있습니다.

그림 ***50: ASR*** 예



1. 아웃바운드 세션이 액티브 SecAppA 상황이 포함된 ASA를 통해 전달됩니다. 이 상황은 외부 ISP-A(192.168.1.1)에 있습니다.
2. 비대칭 라우팅이 업스트림에서 구성되었으므로, 액티브 SecAppB 상황이 포함된 ASA에서 반환 트래픽이 인터페이스 outsideISP-B(192.168.2.2)를 통해 다시 전달됩니다.
3. 인터페이스 192.168.2.2의 트래픽에 대한 세션 정보가 없으므로 일반적으로 반환 트래픽은 손실됩니다. 그러나 인터페이스는 ASR 그룹 1의 일부로 구성됩니다. 유닛에서는 동일한 ASR 그룹 ID로 구성된 다른 인터페이스의 세션을 찾습니다.
4. 세션 정보가 인터페이스 outsideISP-A(192.168.1.2)에 있으며, 이 인터페이스는 SecAppB가 포함된 유닛에서 스탠바이 상태로 존재합니다. 스테이트풀 장애 조치를 통해 세션 정보가 SecAppA에서 SecAppB로 복제됩니다.
5. 손실되는 대신 레이어 2 헤더가 인터페이스 192.168.1.1에 대한 정보로 다시 작성되며 트래픽이 192.168.1.2 밖으로 리디렉션됩니다. 그런 다음에는 트래픽이 시작된 유닛(SecAppA의 192.168.1.1)의 인터페이스를 통해 트래픽을 반환할 수 있습니다. 이러한 전달 작업은 세션이 끝날 때까지 계속 진행되어야 합니다.

시작하기 전에

- 스테이트풀 장애 조치 — 액티브 장애 조치 그룹에 있는 인터페이스의 세션에 대한 상태 정보를 스탠바이 장애 조치 그룹으로 전달합니다.

- 복제 HTTP — HTTP 세션 상태 정보는 스탠바이 장애 조치 그룹으로 전달되지 않으므로, 스탠바이 인터페이스에 존재하지 않습니다. ASA에서 비대칭 라우팅 HTTP 패킷을 다시 라우팅할 수 있도록 하려면 HTTP 상태 정보를 복제해야 합니다.
- 기본 및 보조 유닛의 각 활성 상황에서 이 절차를 수행합니다.
- 한 상황 내에서 두 ASR 그룹 및 트래픽 영역을 모두 구성할 수 없습니다. 상황의 영역을 구성할 경우 상황 인터페이스는 ASR 그룹의 일부가 될 수 없습니다.

프로시저

단계 **1** 기본 유닛에서 사용자가 비대칭으로 라우팅된 패킷을 허용할 인터페이스를 지정합니다.

interface *phy_if*

예제:

```
primary/admin(config)# interface gigabitethernet 0/0
```

단계 **2** 인터페이스에 대한 ASR 그룹 번호를 설정합니다.

asr-group *num*

예제:

```
primary/admin(config-ifc)# asr-group 1
```

num 범위의 올바른 값은 1~32입니다.

단계 **3** 보조 유닛에서 사용자가 비대칭으로 라우팅된 패킷을 허용할 유사한 인터페이스를 지정합니다.

interface *phy_if*

예제:

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

단계 **4** 인터페이스의 ASR 그룹 번호를 기본 유닛 인터페이스와 일치하도록 설정합니다.

asr-group *num*

예제:

```
secondary/ctx1(config-ifc)# asr-group 1
```

예

두 개의 유닛에 다음과 같은 구성이 포함됩니다(구성에는 관련 명령만 표시됨). 다이어그램에 SecAppA로 표시된 디바이스는 장애 조치 쌍의 기본 유닛입니다.

기본 유닛 시스템 구성

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

SecAppA Context Configuration

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

SecAppB Context Configuration

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
```

```
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

장애 조치 관리

이 섹션에서는 장애 조치를 활성화한 다음, 장애 조치 유닛을 관리하는 방법을 설명합니다. 장애 조치 설정을 변경하고 한 유닛에서 다른 유닛으로의 장애 조치를 강제로 수행하는 방법도 알아봅니다.

장애 조치 적용

스탠바이 유닛을 강제로 액티브 유닛으로 만들려면 다음 절차를 수행합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

프로시저

단계 **1** *standby* 유닛이 되면 장애 조치를 강제로 실행합니다. 대기 유닛이 활성 유닛이 됩니다.

group *group_id*를 지정하면 이 명령에서는 지정된 액티브/액티브 장애 조치 그룹이 *standby* 유닛이 될 때 장애 조치를 강제로 실행합니다. 대기 유닛은 장애 조치 그룹의 활성 유닛이 됩니다.

- 대기 유닛에서 활성/대기 모드의 경우:

  failover active

- 대기 유닛에서 활성/활성 모드의 경우:

  failover active [**group** *group_id*]

  예:

  ```
  standby# failover active group 1
  ```

단계 **2** *active*유닛이 되면 장애 조치를 강제로 실행합니다. 활성 유닛은 대기 유닛이 됩니다.

group *group_id*를 지정하면 이 명령에서는 지정된 장애 조치 그룹이 *active* 유닛이 될 때 장애 조치를 강제로 실행합니다. 활성 유닛은 장애 조치 그룹의 대기 유닛이 됩니다.

- 활성 유닛에서 활성/대기 모드의 경우:

  no failover active

- 활성 유닛에서 활성/활성 모드의 경우:

  no failover active [**group** *group_id*]

예:

```
active# no failover active group 1
```

장애 조치 비활성화

하나 또는 두 개의 유닛에서 장애 조치를 비활성화하면 사용자가 다시 로드하기 전까지는 각 유닛의 활성 및 대기 상태가 유지됩니다. 활성/활성 장애 조치 쌍의 경우 장애 조치 그룹은 활성 상태에 있는 어느 유닛에서든, 그리고 기본으로 구성하는 어떤 유닛에서든 활성 상태를 유지합니다.

장애 조치를 비활성화하는 경우 다음 특징을 참조하십시오.

- 두 유닛 모두 트래픽 전달을 시작하지 않도록 대기 유닛/상황은 대기 상태로 남아 있습니다(의사 대기 상태라고 함).
- 더 이상 활성 유닛/상황에 연결 되지 않지만 대기 유닛/상황은 대기 IP 주소를 계속 사용할 수 있습니다.
- 대기 유닛/상황은 장애 조치 링크 연결을 계속해서 수신 대기합니다. 장애 조치가 활성 유닛/상황에 다시 활성화되는 경우, 다음 대기 유닛/상황은 구성의 나머지 부분을 재동기화한 후 일반적인 대기 상태를 다시 시작합니다.
- 스탠바이 유닛을 액티브 유닛으로 설정하기 위해 스탠바이 유닛에서 수동으로 장애 조치를 활성화하지 마십시오. 대신 장애 조치 적용, 317 페이지의 내용을 참조하십시오. 스탠바이 유닛에서 장애 조치를 활성화하는 경우 IPv6 트래픽을 중단시킬 수 있는 MAC 주소 충돌이 표시됩니다.
- 장애 조치를 비활성화하려면 시작 구성에 장애 조치 구성을 저장하지 않고 다시 로드합니다.

시작하기 전에

다중 상황 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

프로시저

단계 **1** 장애 조치를 비활성화합니다.

no failover

단계 **2** 장애 조치를 완전히 비활성화하려면 구성을 저장하고 다시 로드합니다.

write memory

reload

오류가 발생한 유닛 복원

오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원하려면 다음 절차를 수행합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

프로시저

단계 **1** 오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원합니다.

- 활성/대기 모드의 경우:

  failover reset

- 활성/활성 모드의 경우:

  failover reset [**group** *group_id*]

  예:

```
ciscoasa(config)# failover reset group 1
```

오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원한다고 해서 자동으로 활성 유닛이 되지는 않습니다. 복원된 유닛은 장애 조치를 통해(강제로 또는 자연적으로) 활성 유닛이 되기 전까지는 대기 상태로 유지됩니다. 한 가지 예외는 장애 조치 사전 대응 방식으로 구성된 장애 조치 그룹(활성/활성 모드에만 해당)입니다. 이전의 활성 장애 조치 그룹이 활성 상태가 되고, 사전 대응 방식으로 구성되었으며, 유닛에 오류가 발생한 경우 해당 유닛이 기본 유닛입니다.

group *group_id*를 지정하는 경우, 이 명령을 사용하면 장애가 발생한 액티브/액티브 장애 조치 그룹이 장애가 발생하지 않은 상태로 복원됩니다.

단계 **2** (액티브/액티브 모드만) 장애 조치 그룹 수준에서 장애 조치를 재설정하려면

a) **Monitoring(**모니터링**) > Failover(**장애 조치**) > Failover Group(**장애 조치 그룹**)** #이 선택되며 # 은 제어하려는 장애 조치 그룹의 개수입니다.

b) **Reset Failover(**장애 조치 재설정**)**를 클릭합니다.

구성 다시 동기화

활성 유닛에 write standby 명령을 입력할 경우, 대기 유닛의 실행 중인 구성(활성 유닛과의 통신에 사용되는 장애 조치 명령은 제외)이 지워지며, 활성 유닛에서는 전체 구성을 대기 유닛으로 전송합니다.

다중 상황 모드에서 시스템 실행 영역에 **write standby** 명령을 입력하면 모든 상황이 복제됩니다. 상황 내에서 **write standby** 명령을 입력하면 해당 명령에서는 상황 컨피그레이션만 복제합니다.

복제된 명령은 실행 중인 구성에 저장됩니다.

장애 조치 기능 테스트

장애 조치 기능을 테스트하려면 다음 절차를 수행합니다.

프로시저

단계 **1** 활성 유닛에서 FTP(예)를 사용하여 정상적으로 트래픽을 전달하여 다른 인터페이스의 호스트 간에 파일을 전송하는지 테스트합니다.

단계 **2** 활성 유닛에 다음 명령을 입력하여 장애 조치를 강제로 실행합니다.

활성/대기 모드:

ciscoasa(config)# **no failover active**

활성/활성 모드:

ciscoasa (config) # **no failover active group** *group_id*

단계 **3** FTP를 사용하여 동일한 두 호스트 간에 다른 파일을 전송합니다.

단계 **4** 테스트에 성공하지 못할 경우, **show failover** 명령을 입력하여 장애 조치 상태를 확인합니다.

단계 **5** 완료되면 다음 명령을 새 활성 유닛에 입력하여 유닛을 활성 상태로 복원할 수 있습니다.

활성/대기 모드:

ciscoasa(config)# **no failover active**

활성/활성 모드:

ciscoasa(config)# **failover active group** *group_id*

참고 ASA 인터페이스가 중단되면 장애 조치에 대해 이는 계속 유닛 문제로 간주됩니다. ASA에서 인터페이스 중단이 감지될 경우, 인터페이스 대기 시간을 기다리지 않고 장애 조치가 즉시 이루어집니다. 인터페이스 대기 시간은 피어에서 hello 패킷이 수신되지 않는 경우에도 ASA에서 상태가 괜찮은 것으로 간주하는 경우에만 유용합니다. 인터페이스 대기 시간을 시뮬레이션하려면 스위치에서 VLAN을 종료하여 각 피어에서 보내는 hello 패킷이 피어에 수신되지 않도록 합니다.

원격 명령 실행

원격 명령 실행을 사용하면 명령줄에 입력한 명령을 특정 장애 조치 피어에 보낼 수 있습니다.

명령 전송

구성 명령은 활성 유닛 또는 상황에서 스탠바이 유닛이나 상황으로 복제되므로, 어떤 유닛에 로그인해도 **failover exec** 명령을 사용하여 올바른 유닛에 구성 명령을 입력할 수 있습니다. 예를 들어, 스탠

바이 유닛에 로그인한 경우 **failover exec active** 명령을 사용하여 구성 변경 사항을 액티브 유닛에 보낼 수 있습니다. 그런 다음 이러한 변경사항은 대기 유닛에 복제됩니다. **failover exec** 명령을 사용하여 구성 명령을 스탠바이 유닛이나 상황에 보내지 마십시오. 이러한 구성 명령은 액티브 유닛에 복제되지 않으며 두 개의 구성이 더 이상 동기화되지 않습니다.

configuration, exec, **show** 명령의 결과가 현재 터미널 세션에 표시되므로, **failover exec** 명령을 사용하여 **show** 명령을 피어 유닛에 제공하고 현재 터미널에서 결과를 볼 수 있습니다.

피어 유닛에 명령을 실행하려면 로컬 유닛에 명령을 실행할 충분한 권한이 있어야 합니다.

프로시저

단계 **1** 다중 상황 모드에 있을 경우, **changeto context***name* 명령을 사용하여 구성하려는 상황을 변경합니다. **failover exec** 명령으로는 장애 조치 피어에서 상황을 변경할 수 없습니다.

단계 **2** 다음 명령을 사용하여 지정된 장애 조치 유닛에 명령을 전송합니다.

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

지정된 유닛에서 명령을 실행하려면 **active** 또는 **standby** 키워드를 사용합니다. 해당 유닛이 현재 유닛인 경우에도 마찬가지입니다. 장애 조치 피어에서 명령을 실행하려면 **mate** 키워드를 사용합니다.

명령 모드를 변경하는 명령을 사용해도 현재 세션의 프롬프트가 변경되지는 않습니다. 명령이 실행되는 명령 모드를 표시하려면 **show failover exec** 명령을 사용해야 합니다. 자세한 내용은 명령 모드 변경를 참조하십시오.

명령 모드 변경

failover exec 명령은 터미널 세션의 명령 모드와 별개인 명령 모드 상태를 유지합니다. 기본적으로 **failover exec** 명령 모드는 지정된 디바이스에 대한 전역 구성 모드에서 시작됩니다. **failover exec** 명령을 사용하면 적절한 명령(예: **interface** 명령)을 전송하여 명령 모드를 변경할 수 있습니다. **failover exec**를 사용하여 모드를 변경할 경우 세션 프롬프트가 변경되지 않습니다.

예를 들어, 장애 조치 쌍에 있는 액티브 유닛의 전역 구성 모드에 로그인되어 있고 **failover exec active** 명령을 사용하여 인터페이스 구성 모드를 변경할 경우, 터미널 프롬프트는 전역 구성 모드로 유지되지만 **failover exec**를 사용하여 입력한 명령은 인터페이스 구성 모드에 입력됩니다.

다음 예에는 터미널 세션 모드와 **failover exec** 명령 모드의 차이점이 나와 있습니다. 이 예에서 관리자는 활성 유닛의 **failover exec** 모드를 인터페이스 GigabitEthernet0/1를 위한 인터페이스 구성 모드로 변경합니다. 그 후에는 **failover exec active**를 사용하여 입력한 모든 명령이 GigabitEthernet0/1 인터페이스에 대한 인터페이스 구성 모드로 전송됩니다. 관리자는 장애 조치 exec active를 사용하여 해당 인터페이스에 IP 주소를 할당할 수 있습니다. 프롬프트는 전역 구성 모드를 나타내지만, 인터페이스 구성 모드에 **failover exec active** 모드가 있습니다.

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
```

```
ciscoasa(config-router)#
```

디바이스의 현재 세션에 대한 명령 모드 변경은 **failover exec** 명령에서 사용하는 명령 모드에 영향을 주지 않습니다. 예를 들어, 액티브 유닛에서 인터페이스 구성 모드를 사용 중이고 **failover exec** 명령 모드를 변경한 경우, 다음 명령이 전역 구성 모드에서 실행됩니다. 그 결과 디바이스에 대한 세션은 인터페이스 구성 모드에서 유지되는 반면, **failover exec active**를 사용하여 입력한 명령은 지정된 라우팅 프로세스의 라우터 구성 모드로 전송됩니다.

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

show failover exec 명령을 사용하여 지정된 디바이스(**failover exec** 명령으로 전송된 명령이 실행됨)에 명령 모드를 표시합니다. **show failover exec** 명령에서는 **failover exec** 명령과 동일한 키워드인 **active**, **mate** 또는 **standby**를 사용합니다. 각 디바이스의 **failover exec** 모드는 개별적으로 추적됩니다.

예를 들어, 다음은 스탠바이 유닛에 입력된 **show failover exec** 명령의 샘플 출력입니다.

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

보안 문제

failover exec 명령에서는 장애 조치 링크를 사용하여 명령을 전송하고 피어 유닛에서 명령 실행 결과를 수신합니다. 장애 조치 링크에 암호화를 활성화하여 도청이나 끼어들기 공격을 방지해야 합니다.

원격 명령 실행의 제한사항

원격 명령을 사용할 경우 다음과 같은 제한사항이 발생할 수 있습니다.

- 무중단 업그레이드 절차를 사용하여 유닛 하나를 업그레이드하고 다른 유닛은 업그레이드하지 않을 경우, 두 유닛에서는 명령을 가동하는 데 필요한 **failover exec** 명령을 지원하는 소프트웨어를 실행해야 합니다.
- *cmd_string* 인수의 명령에서 명령 완료 및 상황 도움말이 제공되지 않습니다.
- 다중 상황 모드의 경우, 피어 유닛에 있는 피어 상황에 명령을 전송하는 것만 가능합니다. 다른 상황에 명령을 전송하려면 우선 유닛의 해당 상황을 로그인한 상황으로 변경해야 합니다.
- 다음 명령은 **failover exec** 명령과 함께 사용할 수 없습니다.
  - **changeto**
  - **debug (undebug)**

- 스탠바이 유닛에 장애가 발생한 상태이고 장애의 원인이 서비스 카드 장애인 경우 **failover exec** 명령에서 명령을 계속 수신할 수 있습니다. 그렇지 않을 경우에는 원격 명령을 실행할 수 없습니다.
- **failover exec** 명령을 사용하여 장애 조치 피어의 특권 EXEC 모드를 전역 구성 모드로 전환할 수 없습니다. 예를 들어, 현재 유닛이 EXEC 모드에 있고 **failover exec mate configure terminal**을 입력할 경우 **show failover exec mate** 출력에는 장애 조치 exec 세션이 전역 구성 모드에 있는 것으로 표시됩니다. 그러나 현재 유닛이 전역 구성 모드가 되지 않는 한 **failover exec**를 사용하여 피어 유닛에 구성 명령을 입력할 경우 장애가 발생합니다.
- **failover exec mate failover exec mate** 명령과 같은 재귀적 장애 조치 exec 명령은 입력할 수 없습니다.
- 사용자 입력 또는 확인이 필요한 명령에는 **noconfirm** 옵션을 사용해야 합니다. 예를 들어, 짝을 다시 로드하려면 다음을 입력합니다.

  failover exec mate reload noconfirm

모니터링 장애 조치

이 섹션에서는 장애 조치 상태를 모니터링할 수 있습니다.

장애 조치 메시지

장애 조치가 발생할 경우, ASA에서는 시스템 메시지를 전송합니다.

장애 조치 **Syslog** 메시지

ASA에서는 심각한 상황을 의미하는 우선순위 등급 2에 해당하는 장애 조치와 관련된 여러 가지 syslog 메시지를 전달합니다. 이러한 메시지를 보려면 syslog 메시지 가이드를 참조하십시오. 페일오버와 관련된 메시지 ID의 범위는 101xxx, 102xxx, 103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx, 727xxx입니다. 예를 들어 105032 및 105043은 페일오버 링크의 문제를 나타냅니다.

참고 장애 조치가 실행되는 동안에는 ASA가 논리적으로 종료되고 인터페이스를 호출하여 syslog 메시지 411001 및 411002를 생성합니다. 이는 정상적인 동작입니다.

장애 조치 디버그 메시지

디버그 메시지를 보려면 **debug fover** 명령을 입력합니다. 자세한 내용은 명령 참조를 참조하십시오.

참고 디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되므로 시스템 성능에 큰 영향을 미칠 수 있습니다. 따라서 **debug fover** 명령은 특정 문제를 트러블슈팅하거나 Cisco TAC를 통해 세션 문제를 트러블슈팅하는 동안에만 사용해야 합니다.

SNMP 장애 조치 트랩

장애 조치를 위한 SNMP syslog 트랩을 수신하려면 SNMP 에이전트에서 SNMP 트랩을 SNMP 관리 스테이션으로 전송하도록 구성하고, syslog 호스트를 정의하고, Cisco syslog MIB를 SNMP 관리 스테이션으로 컴파일합니다.

장애 조치 상태 모니터링

장애 조치 상태를 모니터링하려면 다음 명령 중 하나를 입력합니다.

- **show failover**

  유닛의 장애 조치 상태에 대한 정보를 표시합니다.

- **show failover group**

  장애 조치 그룹의 장애 조치 상태에 대한 정보를 표시합니다. 표시되는 정보는 **show failover** 명령의 내용과 유사하지만 지정된 그룹에 한정됩니다.

- **show monitor-interface**

  모니터링된 인터페이스에 대한 정보를 표시합니다.

- **show running-config failover**

  실행 중인 구성의 장애 조치 명령을 표시합니다.

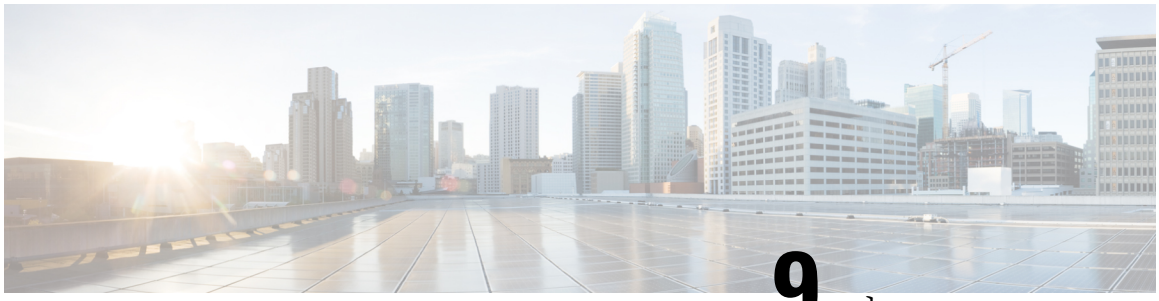
장애 조치 내역

기능 이름	릴리스	기능 정보
액티브/스탠바이 장애 조치	7.0(1)	이 기능을 도입했습니다.
액티브/액티브 장애 조치	7.0(1)	이 기능을 도입했습니다.
장애 조치 키에 16진수 값 지원	7.0(4)	장애 조치 링크 암호화에 16진수 값을 지정할 수 있습니다. 수정된 명령: **failover key hex**

기능 이름	릴리스	기능 정보
장애 조치 키에 마스터 패스프레이즈 지원	8.3(1)	장애 조치 키에서 마스터 암호를 지원하며, 이 기능은 실행 중인 컨피그레이션과 시작 컨피그레이션의 공유 키를 암호화합니다. ASA에서 다른 ASA로 공유 암호를 복사할 경우(예: **more system:running-config** 명령에서) 암호화된 공유 키를 복사하여 붙여넣을 수 있습니다. 참고 **failover key** shared secret은 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다. 수정된 명령: **failover key** [**0** | **8**]
장애 조치에 IPv6 지원이 추가되었습니다.	8.2(2)	수정된 명령: **failover interface ip**, **show failover**, **ipv6 address**, **show monitor-interface**
"동시" 부팅하는 동안 장애 조치 그룹 유닛 환경 설정을 변경합니다.	9.0(1)	이전 소프트웨어 버전에서는 "동시" 부팅을 허용했습니다. 따라서 장애 조치 그룹은 기본 유닛에서 액티브 상태가 되기 위해 **preempt** 명령을 필요로 하지 않았습니다. 하지만, 이 기능 설정은 이제 부팅하는 첫 번째 유닛에서 두 장애 조치 그룹이 활성 상태가 되는 것으로 변경되었습니다.
장애 조치 및 상태 링크 통신을 암호화하는 IPsec LAN-LAN 터널 지원	9.1(2)	장애 조치 키(**failover key** 명령)에 전용 암호화를 사용하는 대신, 이제 장애 조치 및 상태 링크 암호화를 위한 IPsec LAN-LAN 터널을 사용할 수 있습니다. 참고 장애 조치 LAN-LAN 터널은 IPsec(기타 VPN) 라이센스 계산에 포함되지 않습니다. 도입 또는 수정된 명령: **failover ipsec pre-shared-key**, **show vpn-sessiondb**

기능 이름	릴리스	기능 정보
하드웨어 모듈의 상태 모니터링 비활성화	9.3(1)	기본적으로 ASA에서는 ASA FirePOWER 모듈과 같은 설치된 하드웨어 모듈의 상태를 모니터링합니다. 하드웨어 모듈 오류 때문에 장애 조치가 수행되는 것을 원치 않을 경우 모듈 모니터링을 비활성화할 수 있습니다. 다음 명령을 수정했습니다. **monitor-interface service-module**
장애 조치 쌍에 있는 스탠바이 유닛 또는 스탠바이 상황의 컨피그레이션 변경 잠금	9.3(2)	이제 스탠바이 유닛(액티브/스탠바이 장애 조치) 또는 스탠바이 상황(액티브/액티브 장애 조치)의 컨피그레이션 변경을 잠글 수 있으므로, 정상적인 컨피그레이션 동기화에서 벗어난 스탠바이 유닛의 변경 사항을 적용할 수 없습니다. 다음 명령을 도입했습니다. **failover standby config-lock**
ASA 5506H에서 장애 조치 링크로 Management 1/1 인터페이스 사용 활성화	9.5(1)	이제 ASA 5506H에서만 장애 조치 링크로 Management 1/1 인터페이스를 구성할 수 있습니다. 이 기능을 통해 디바이스에서 다른 모든 인터페이스를 데이터 인터페이스로 사용할 수 있습니다. 이 기능을 사용하면 Management 1/1 인터페이스를 일반 관리 인터페이스로 계속 유지하도록 요구하는 ASA Firepower 모듈을 사용할 수 없습니다. 다음 명령을 수정했습니다. **failover lan interface, failover link**
장애 조치 및 ASA 클러스터링에서의 통신 사업자급 NAT 개선 사항 지원	9.5(2)	통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 이 기능은 이제 장애 조치 및 ASA 클러스터 구축에서 지원됩니다. 다음 명령을 수정했습니다. **show local-host**

기능 이름	릴리스	기능 정보
액티브/스탠바이 장애 조치 사용 시 AnyConnect에서 동적 ACL에 대해 향상된 동기화 시간	9.6(2)	이제 장애 조치 쌍에서 AnyConnect를 사용할 경우, 스탠바이 유닛에 연결된 동적 ACL(dACL)에 대한 동기화 시간이 향상되었습니다. 이전에는 큰 dACL을 사용하는 경우 스탠바이 유닛이 고가용성 백업을 제공하는 대신 동기화로 바쁜 동안 동기화에 오랜 시간이 걸릴 수 있었습니다. 명령은 수정하지 않았습니다.
다중 상황 모드에서의 AnyConnect 연결에 대한 스테이트풀 장애 조치	9.6(2)	이제 다중 상황 모드에서 AnyConnect 연결에 대한 스테이트풀 장애 조치가 지원됩니다. 명령은 수정하지 않았습니다.
장애 조치에 대한 인터페이스 링크 상태 모니터링 폴링을 더 빠른 탐지를 위해 구성 가능	9.7(1)	기본적으로 장애 조치 쌍의 각 ASA는 해당 인터페이스의 링크 상태를 500밀리초마다 확인합니다. 이제 폴링 간격을 300msec와 799msec 사이로 구성할 수 있습니다. 예를 들어 폴링 시간을 300msec로 설정하면 ASA에서 인터페이스 오류를 탐지하고 더 빨리 장애 조치를 트리거할 수 있습니다. 다음 명령을 도입했습니다. **failover polltime link-state**
Firepower 9300 및 4100에서 액티브/스탠바이 장애 조치 상태 모니터링에 대한 BFD(Bidirectional Forwarding Detection) 지원	9.7(1)	Firepower 9300 및 4100에서 액티브/스탠바이 쌍의 두 유닛 간의 장애 조치 상태 확인을 위해 BFD(Bidirectional Forwarding Detection)를 활성화할 수 있습니다. 상태 확인에 BFD를 사용하면 기본 상태 확인 방법보다 더 신뢰할 수 있으며 CPU를 덜 사용합니다. 다음 명령을 도입했습니다. **failover health-check bfd**



9 장

퍼블릭 클라우드의 고가용성을 위한 장애 조치

이 장에서는 Microsoft Azure와 같은 퍼블릭 클라우드 환경에서 Cisco ASAv의 고가용성을 확보하기 위해 액티브/백업 장애 조치를 구성하는 방법을 설명합니다.

퍼블릭 클라우드의 장애 조치 정보

이중화를 보장하기 위해 액티브/백업 고가용성(HA) 구성에서 퍼블릭 클라우드 환경에 ASAv를 구축할 수 있습니다. 퍼블릭 클라우드에서 HA는 액티브 ASAv 장애 때문에 백업 ASAv로 시스템의 자동 장애 조치를 트리거하게 만들 수 있는 스테이트리스 액티브/백업 솔루션을 구현합니다.

다음 목록에서는 HA 퍼블릭 클라우드 솔루션의 주요 구성 요소를 설명합니다.

- 활성 **ASAv** — HA 피어에 대한 방화벽 트래픽을 처리하기 위해 설정된 HA 쌍에 있는 ASAv입니다.
- 백업 **ASAv** — 방화벽 트래픽을 처리하지 않고 액티브 ASAv 장애 발생 시 액티브 ASAv로 대체하는 HA 쌍의 ASAv입니다. 장애 조치 발생 시 피어 식별을 수행하지 않으므로 이를 스탠바이보다는 백업이라고 부릅니다.
- **HA** 에이전트 — ASAv에서 실행되고 ASAv의 HA 역할(액티브/백업)을 결정하고, HA 피어의 장애를 탐지하며, HA 역할을 기반으로 작업을 수행하는 경량 프로세스입니다.

물리적 ASA 및 비 퍼블릭 클라우드 가상 ASA에서는 액티브 IP 및 MAC 주소와 현재 연결되어 있음을 나타내는 Gratuitous ARP를 백업 ASA에서 전송하는 Gratuitous ARP 요청을 사용하여 장애 조치 상태가 처리됩니다. 대부분의 퍼블릭 클라우드 환경에서는 이 특성의 브로드캐스트 트래픽을 허용하지 않습니다. 이러한 이유로, 퍼블릭 클라우드에서 HA 구성할 때는 장애 조치가 발생하는 경우 진행 중인 연결을 다시 시작해야 합니다.

액티브 유닛의 상태는 특정한 장애 조치 조건을 충족하는지 판단하기 위해 백업 유닛에서 모니터링됩니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다. 장애 조치 시간은 퍼블릭 클라우드 인프라의 응답성에 따라 몇 초에서 몇 분까지 다양할 수 있습니다.

액티브/백업 장애 조치 정보

액티브/백업 장애 조치에서는 하나의 유닛이 액티브 유닛입니다. 이 유닛에서 트래픽을 전달합니다. 백업 유닛에서는 트래픽을 능동적으로 전달하거나 액티브 유닛 없이 구성 정보를 교환하지 않습니다. 액티브/백업 장애 조치에서는 백업 ASAv 디바이스를 사용해 실패한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛이 실패하면 백업 상태로 변경되며, 백업 유닛은 액티브 상태로 변경됩니다.

기본/보조 역할 및 액티브/백업 상태

액티브/백업 장애 조치를 설정할 때는 한 유닛을 기본 유닛으로, 다른 유닛을 보조 유닛으로 구성합니다. 이 시점에서 두 개의 유닛은 디바이스 및 정책 구성뿐만 아니라 이벤트, 대시보드, 보고서 및 상태 모니터링에 대한 두 개의 개별 디바이스 역할을 합니다.

장애 조치 쌍에서 두 유닛 간의 주요 차이점은 어느 유닛이 액티브 유닛에 연결되어 있고 어느 유닛이 백업 유닛에 연결되어 있는지, 즉 어떤 유닛에서 트래픽을 능동적으로 전달하는지와 관련되어 있습니다. 두 유닛에서는 모두 트래픽을 전달할 수 있지만, 기본 유닛에서만 로드 밸런서 프로브에 응답하고 이를 경로 대상으로 사용하여 모든 구성된 경로를 프로그래밍합니다. 백업 유닛의 기본 기능은 기본 유닛의 상태를 모니터링하는 것입니다. 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.

장애 조치 연결

백업 ASAv에서는 TCP를 통해 설정되는 장애 조치 연결을 사용하여 액티브 ASAv의 상태를 모니터링합니다.

- 액티브 ASAv는 수신 대기 포트를 열어 연결 서버로 작동합니다.
- 백업 ASAv에서는 연결 포트를 사용하여 액티브 ASAv에 연결합니다.
- 일반적으로 구성에서 ASAv 유닛 간에 네트워크 주소 변환의 일부 유형을 요구하지 않는 한 수신 대기 포트와 연결 포트는 동일합니다.

장애 조치 연결 상태는 액티브 ASAv의 장애를 탐지합니다. 백업 ASAv에서는 장애 조치 연결이 중단된 것을 발견하면 액티브 ASAv가 실패한 것으로 간주합니다. 마찬가지로, 백업 ASAv에서는 액티브 유닛으로 전송된 keepalive 메시지에 대한 응답을 수신하지 않는 경우 액티브 ASAv가 실패한 것으로 간주합니다.

관련 주제

설문 조사 및 Hello 메시지

백업 ASAv에서는 장애 조치 연결을 통해 Hello 메시지를 액티브 ASAv에 전송하며 Hello 응답이 반환될 것으로 기대합니다. 메시지 타이밍은 폴링 간격 즉, 백업 ASAv 유닛에서의 Hello 응답을 수신하고 다음 Hello 메시지를 보내는 사이의 시간을 사용합니다. 응답 수신에는 보류 시간이라고 하는 수신 시간 제한이 적용됩니다. Hello 응답 수신 시간이 초과되면 액티브 ASAv가 실패한 것으로 간주됩니다.

폴링 및 보류 시간 간격은 구성 가능한 파라미터입니다. 장애 조치 기준 및 기타 설정 구성, 339 페이지의 내용을 참조하십시오.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 백업 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 백업 유닛이 됩니다.

페일오버 이벤트

액티브/백업 장애 조치 시 장애 조치는 유닛을 기준으로 실행됩니다. 다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 장애 조치 이벤트에 적용되는 장애 조치 정책(장애 조치 실행 또는 장애 조치 없음), 액티브 유닛에서 시행한 조치, 백업 유닛에서 시행한 조치, 장애 조치 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 ***14:*** 페일오버 이벤트

오류 이벤트	정책	액티브 조치	백업 작업	**Notes**(참고)
백업 유닛에서 장애 조치 연결이 종료된 것을 확인	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	이는 표준 장애 조치 사용 사례입니다.
액티브 유닛에서 장애 조치 연결이 종료된 것을 확인	페일오버 없음	백업을 실패로 표시	해당 없음	액티브 상태가 아닌 유닛에 대한 장애 조치는 발생하지 않아야 합니다.

오류 이벤트	정책	액티브 조치	백업 작업	**Notes**(참고)
액티브 유닛에서 장애 조치 링크의 TCP 시간 제한 확인	페일오버 없음	백업을 실패로 표시	작업 없음	액티브 유닛이 백업 유닛에서 응답을 수신하지 않고 있는 경우 장애 조치는 발생하지 않아야 합니다.
백업 유닛에서 장애 조치 링크의 TCP 시간 제한 확인	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨 액티브 유닛에 장애 조치 명령을 전송하려고 시도함	백업 유닛은 액티브 유닛이 작업을 계속할 수 없으며 인수한다고 가정합니다. 액티브 유닛이 계속 작동 중이지만 제 시간 이내에 응답을 전송하지 못하는 경우, 백업 유닛에서 액티브 유닛에 장애 조치 명령을 전송합니다.
활성 인증에 실패함	페일오버 없음	작업 없음	작업 없음	백업 유닛이 경로 테이블을 변경하고 있으므로 Azure에서 인증받아야 하는 유일한 유닛입니다. 액티브 유닛이 Azure에서 인증을 받았는지 여부는 중요하지 않습니다.
백업 인증에 실패함	페일오버 없음	백업을 인증되지 않음으로 표시	작업 없음	백업 유닛이 Azure에서 인증되지 않은 경우 장애 조치가 발생할 수 없습니다.
액티브 유닛에서 의도적인 장애 조치를 시작함	페일오버	백업 상태가 됨	액티브 상태가 됨	액티브 유닛에서는 장애 조치 링크 연결을 종료하여 장애 조치를 시작합니다. 백업 유닛은 연결이 종료된 것을 확인하고 액티브 유닛이 됩니다.

오류 이벤트	정책	액티브 조치	백업 작업	**Notes**(참고)
백업 유닛에서 의도적인 장애 조치를 시작함	페일오버	백업 상태가 됨	액티브 상태가 됨	백업 유닛에서 장애 조치 메시지를 액티브 유닛에 전송하여 장애 조치를 시작합니다. 액티브 유닛이 이 메시지를 확인하면 연결을 종료하고 백업 유닛이 됩니다. 백업 유닛은 연결이 종료된 것을 확인하고 액티브 유닛이 됩니다.
이전 액티브 유닛 복구	페일오버 없음	백업 상태가 됨	짝을 백업으로 표시	절대적으로 필수적인 경우를 제외하고 장애 조치는 발생하지 않아야 합니다.
액티브 유닛에서 백업 유닛의 장애 조치 메시지 확인	페일오버	백업 상태가 됨	액티브 상태가 됨	사용자가 수동 장애 조치를 시작한 경우 또는 백업 유닛이 TCP 시간이 초과되었지만 액티브 유닛에서 백업 유닛의 메시지를 수신할 수 있는 상태임을 확인한 경우 발생 가능합니다.

지침 및 제한 사항

이 섹션에는 이 기능을 위한 지침 및 제한 사항이 포함되어 있습니다.

퍼블릭 클라우드의 고가용성을 위한 **ASAv** 장애 조치

이중화를 보장하기 위해 액티브/백업 고가용성(HA) 구성에서 퍼블릭 클라우드 환경에 ASAv를 구축할 수 있습니다.

- Standard D3_v2 인스턴스를 사용하여 Microsoft Azure 퍼블릭 클라우드에서만 지원됩니다.
- 액티브 ASAv 장애 때문에 백업 ASAv로 시스템의 자동 장애 조치를 트리거하게 만들 수 있는 스테이트리스 액티브/백업 솔루션을 구현합니다.

제한 사항

- 장애 조치는 밀리초 보다는 초 순서로 진행됩니다.

- HA 역할 결정 및 HA 유닛으로 참여하기 위한 기능은 HA 피어와 HA 유닛, Azure 인프라 간의 TCP 연결성에 따라 달라집니다. ASAv가 HA 유닛으로 참여할 수 없는 다음과 같은 여러 가지 상황이 있습니다.
  - HA 피어에 장애 조치 연결을 설정할 수 없음
  - Azure에서 인증 토큰을 검색할 수 없음
  - Azure를 통해 인증 받을 수 없음
- 액티브 유닛에서 백업 유닛으로 구성 동기화 불가능 각 유닛은 장애 조치 트래픽을 처리하기 위해 유사한 구성을 사용하여 개별적으로 구성되어야 합니다.
- ASDM은 지원되지 않습니다.
- IPSec 원격 액세스 VPN은 지원되지 않습니다.

참고 퍼블릭 클라우드에서 지원되는 VPN 토폴로지에 대한 내용은 Cisco ASAv(Adaptive Security Virtual Appliance) 빠른 시작 가이드를 참조하십시오.

- ASAv 가상 머신 인스턴스는 동일한 가용성 집합에 속해야 합니다. Azure에서 현재 ASAv 사용자인 경우 기존 구축에서 HA로 업그레이드할 수 없습니다. 인스턴스를 삭제하고 Azure Marketplace의 ASAv 4 NIC HA 오퍼링을 구축해야 합니다.

퍼블릭 클라우드의 장애 조치에 대한 라이선싱

ASAv에서는 Cisco Smart Software Licensing을 사용합니다. 스마트 라이센스는 일반적인 운영에 필요합니다. 각 ASAv는 ASAv 플랫폼 라이선스와 별개로 라이선스를 부여받아야 합니다. 라이센스를 설치할 때까지 예비 연결 테스트를 수행할 수 있도록 처리량이 100Kbps로 제한됩니다. ASAv에 대한 정확한 라이선싱 요구 사항을 확인하려면 Cisco ASA Series 기능 라이선스 페이지를 참조하십시오.

퍼블릭 클라우드의 장애 조치에 대한 기본값

기본적으로 장애 조치 정책은 다음과 같이 구성됩니다.

- 스테이트리스 장애 조치만 해당합니다.
- 각 유닛은 장애 조치 트래픽을 처리하기 위해 유사한 구성을 사용하여 개별적으로 구성되어야 합니다.
- 장애 조치 TCP 제어 포트 번호는 44442입니다.
- Azure 로드 밸런서 상태 프로브 포트 번호는 44441입니다.
- 유닛 폴링 시간은 5초입니다.

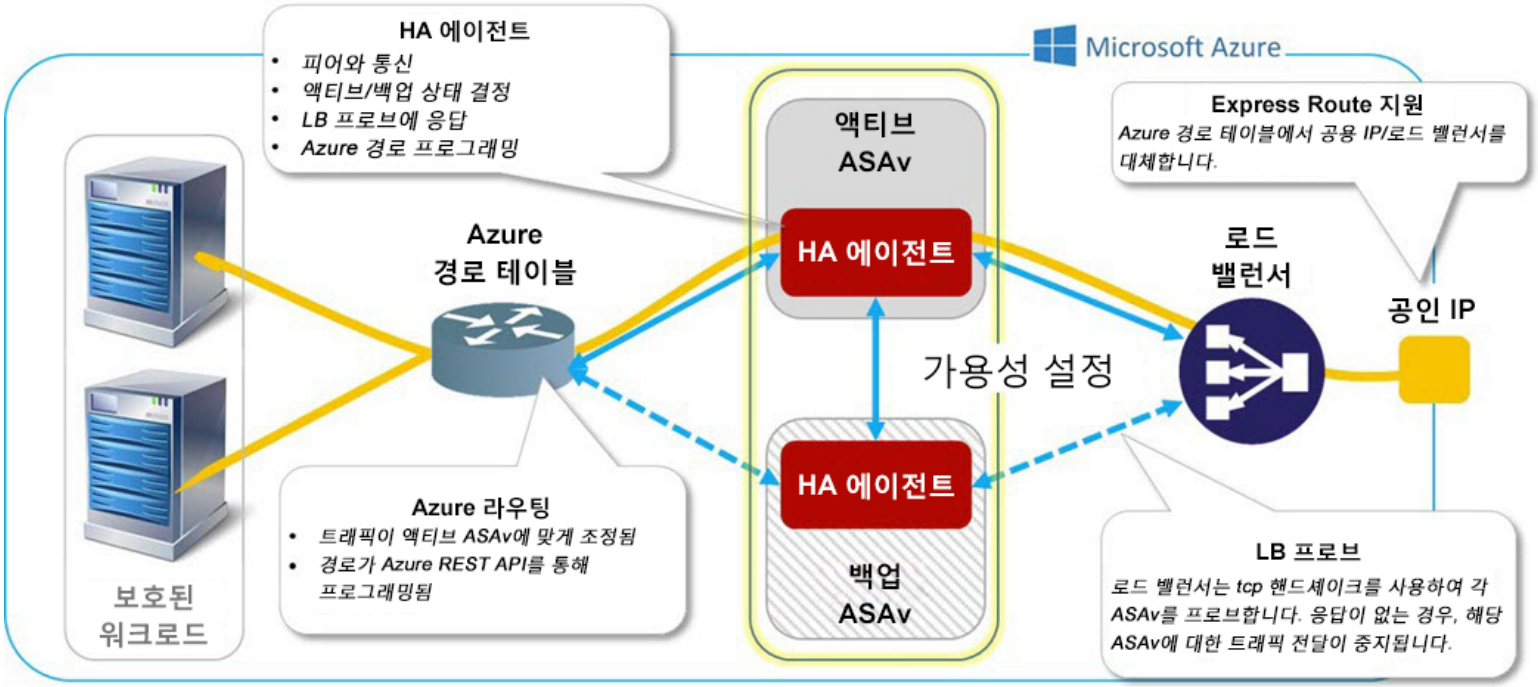
• 유닛 대기 시간 15초

Microsoft Azure의 ASAv 고가용성 정보

다음 그림에는 Azure 내 ASAv HA 구축에 대한 상위 수준 보기가 나와 있습니다. 보호 대상인 워크로드는 액티브/백업 장애 조치 구성에서 2개의 ASAv 인스턴스 뒤에 있습니다. Azure 로드 밸런서는 3방향 TCP 핸드셰이크를 사용하여 ASAv 유닛을 프로브합니다. 액티브 ASAv는 상태가 양호한지 표시하는 3방향 핸드셰이크를 완료하고 백업 ASAv는 의도적으로 응답하지 않습니다. 로드 밸런서에 응답하지 않으면 백업 ASAv가 로드 밸런서에 상태가 양호하지 않은 것으로 표시됨에 따라 트래픽이 전송되지 않습니다.

장애 조치 시 액티브 ASAv는 로드 밸런서의 프로브에 대한 응답을 중지하고 백업 ASAv는 응답을 시작하는데, 이로 인해 새로운 모든 연결이 백업 ASAv에 전송됩니다. 백업 ASAv는 API 요청을 Azure 패브릭에 전송하여 경로 테이블을 수정하고, 이때 액티브 유닛에서 백업 유닛으로 트래픽이 리디렉션됩니다. 이 시점에서 백업 ASAv는 액티브 유닛이 되고 액티브 유닛은 백업 유닛이 되거나 장애 조치 이유에 따라 오프라인 상태가 됩니다.

그림 ***51: Azure***에서 ***ASAv HA*** 구축



Azure 경로 테이블을 수정하기 위해 API 통화를 자동으로 할 수 있으려면 ASAv HA 유닛에는 Azure Active Directory 크리덴셜이 필요합니다. Azure는 서비스 주체라는 개념을 적용하는데, 이는 간단히 말해 서비스 어카운트입니다. 서비스 주체를 사용하면 충분한 권한이 있는 어카운트만 프로비저닝할 수 있으며 Azure 리소스의 미리 정의된 집합 내에서 작업을 실행하도록 범위를 정할 수 있습니다.

서비스 주체를 사용하여 Azure 서브스크립션을 관리하기 위해 ASAv HA 구축을 활성화하는 두 가지 단계는 다음과 같습니다.

1. Azure Active Directory 애플리케이션 및 서비스 주체를 생성합니다. Azure 서비스 주체 정보, 336 페이지의 내용을 참조하십시오.
2.

관련 주제

로드 밸런서에 대한 자세한 내용은 Azure 설명서를 참조하십시오.

Azure 서비스 주체 정보

경로 테이블과 같은 Azure 리소스에 액세스하거나 수정해야 하는 애플리케이션을 사용 중인 경우, Azure AD(Active Directory) 애플리케이션을 설치하고 필요한 권한을 할당해야 합니다. 이 방법은 고유한 크리덴셜로 애플리케이션을 실행하는 것보다 더 좋은 방법입니다. 그 이유는 다음과 같습니다.

- 고유한 권한과 다른 애플리케이션 ID에 권한을 할당할 수 있습니다. 일반적으로 이러한 권한은 정확히 애플리케이션이 수행해야 할 작업으로 제한됩니다.
- 사용자 역할이 변경되는 경우 애플리케이션의 크리덴셜을 변경할 필요가 없습니다.
- 무인 스크립트를 실행할 때 인증서를 사용하여 인증을 자동화할 수 있습니다.

Azure 포털에서 Azure AD 애플리케이션을 등록하는 경우, Azure AD 테넌트에서 애플리케이션 개체와 서비스 주체 개체라는 두 개의 개체가 생성됩니다.

- 애플리케이션 개체 — Azure AD 애플리케이션은 유일한 하나의 애플리케이션 개체를 사용하여 정의되며 이 개체는 애플리케이션이 등록된 위치인 Azure AD 테넌트(애플리케이션의 "홈" 테넌트로 알려져 있음)에 상주합니다.
- 서비스 주체 개체 — 서비스 주체 개체는 특정 테넌트에서 애플리케이션을 사용하기 위한 정책 및 권한을 정의합니다. 이때 런타임 시 애플리케이션을 나타내는 보안 주체에 대한 기본 요소를 제공합니다.

Azure에서는 *Azure Resource Manager* 설명서에서 Azure AD 애플리케이션 및 서비스 주체를 생성하는 방법에 대한 지침을 제공합니다. 자세한 지침은 다음 항목을 참조하십시오.

- 포털을 사용하여 리소스에 액세스할 수 있는 Azure Active Directory 애플리케이션 및 서비스 주체를 생성합니다.
- Azure PowerShell을 사용하여 서비스 주체를 생성하여 리소스에 액세스합니다.

참고 서비스 주체를 설정한 후 **Directory ID**(디렉터리 **ID**), **Application ID**(애플리케이션 **ID**)**Secret key**(비밀 키)를 얻습니다. 이러한 요소들은 Azure 인증 크리덴셜을 구성하는 데 필요합니다. Azure 서비스 주체에 대한 인증 크리덴셜 구성, 341 페이지의 내용을 참조하십시오.

Azure에서의 ASAv 고가용성 구축을 위한 구성 요구 사항

그림 51: Azure에서 ASAv HA 구축, 335 페이지에 설명된 구성과 유사한 구성을 구축하려면 다음과 같은 요소가 필요합니다.

- Azure 인증 정보(Azure 서비스 주체 정보, 336 페이지 참조):
  - 디렉터리 ID
  - 애플리케이션 ID
  - 암호 키
- Azure 경로 정보(Azure 경로 테이블 구성, 342 페이지 참조):
  - Azure 서브스크립션 ID
  - 경로 테이블 리소스 그룹
  - 테이블 이름
  - 주소 접두사
  - 다음 홉 주소
- ASA 구성(액티브/백업 장애 조치 구성, 337 페이지, 퍼블릭 클라우드의 장애 조치에 대한 기본값, 334 페이지 참조):
  - 액티브/백업 IP 주소
  - HA 에이전트 통신 포트
  - 로드 밸런서 프로브 포트
  - 폴링 간격

참고 기본 유닛과 보조 유닛 모두에서 기본 장애 조치 설정을 구성합니다. 기본 유닛에서 보조 유닛으로 구성이 동기화되지 않습니다. 각 유닛은 장애 조치 트래픽을 처리하기 위해 유사한 구성을 사용하여 개별적으로 구성되어야 합니다.

액티브/백업 장애 조치 구성

액티브/백업 장애 조치를 구성하려면 기본 유닛과 보조 유닛 모두에서 기본 장애 조치 설정을 구성합니다. 기본 유닛에서 보조 유닛으로 구성이 동기화되지 않습니다. 각 유닛은 장애 조치 트래픽을 처리하기 위해 유사한 구성을 사용하여 개별적으로 구성되어야 합니다.

시작하기 전에

- ASAv HA 쌍을 Azure 가용성 집합에 구축합니다.
- 서비스 주체용 Azure 서브스크립션 ID 및 Azure 인증 크리덴셜을 포함하여 사용 가능한 Azure 환경 정보를 확보합니다.

액티브/백업 장애 조치를 위한 기본 유닛 구성

이 섹션의 단계에 따라 액티브/백업 장애 조치 구성에서 기본 유닛을 구성합니다. 이러한 단계에서는 기본 유닛에서 장애 조치를 사용하는 데 필요한 최소 구성을 제공합니다.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

예

다음 예에는 기본/액티브 유닛의 장애 조치 파라미터를 구성하는 방법이 나와 있습니다.

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

다음에 수행할 작업

필요에 따라 추가 파라미터를 구성합니다.

- 백업 유닛을 구성합니다. 액티브/백업 장애 조치를 위한 보조 유닛 구성, 338 페이지의 내용을 참조하십시오.
- Azure 인증을 구성합니다. Azure 서비스 주체에 대한 인증 크리덴셜 구성, 341 페이지의 내용을 참조하십시오.
- Azure 경로 정보를 구성합니다. Azure 경로 테이블 구성, 342 페이지의 내용을 참조하십시오.
- 추가 파라미터를 검토합니다. 장애 조치 기준 및 기타 설정 구성, 339 페이지의 내용을 참조하십시오.

액티브/백업 장애 조치를 위한 보조 유닛 구성

이 섹션의 단계에 따라 액티브/백업 장애 조치 구성에서 보조 유닛을 구성합니다. 이러한 단계에서는 보조 유닛에서 장애 조치를 활성화하는 데 필요한 최소 구성을 제공합니다.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

프로시저

단계 **1** 이 유닛을 백업 유닛으로 지정합니다.

failover cloud unit secondary

단계 **2** 액티브 IP 주소를 장애 조치 링크에 할당합니다.

failover cloud peer ip *ip-address* [**port** *port-number*]

이 IP 주소는 HA 피어에 대한 TCP 장애 조치 제어 연결을 설정하는 데 사용됩니다. 이미 액티브 유닛이 되었을 수 있는 HA 피어에 대한 장애 조치 연결을 열려고 시도 중일 때 포트가 사용됩니다. NAT가 HA 피어 간에 발생하는 경우 포트를 여기에서 구성해야 할 수 있습니다. 대부분의 경우 포트를 구성할 필요가 없습니다.

예

다음 예에는 보조/백업 유닛의 장애 조치 파라미터를 구성하는 방법이 나와 있습니다.

```
failover cloud unit secondary
failover cloud peer ip 10.4.3.4 port 4444
```

다음에 수행할 작업

필요에 따라 추가 파라미터를 구성합니다.

- Azure 인증을 구성합니다. Azure 서비스 주체에 대한 인증 크리덴셜 구성, 341 페이지.
- Azure 경로 정보를 구성합니다. Azure 경로 테이블 구성, 342 페이지의 내용을 참조하십시오.
- 추가 파라미터를 검토합니다. 장애 조치 기준 및 기타 설정 구성, 339 페이지의 내용을 참조하십시오.

선택적 장애 조치 파라미터 구성

필요에 따라 장애 조치 설정을 맞춤화할 수 있습니다.

장애 조치 기준 및 기타 설정 구성

이 섹션에서 변경할 수 있는 다양한 매개변수에 대한 기본 설정은 퍼블릭 클라우드의 장애 조치에 대한 기본값, 334 페이지를 참조하십시오.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

- 기본 유닛과 보조 유닛 모두에서 이러한 설정을 구성합니다. 기본 유닛에서 보조 유닛으로 구성이 동기화되지 않습니다.

프로시저

단계 **1** HA 피어와의 통신에 사용할 TCP 포트를 지정합니다.

failover cloud port control *port-number*

예제**:**

```
ciscoasa(config)# failover cloud port control 4444
```

port-number 인수는 피어-투-피어 통신에 사용되는 TCP 포트 번호를 할당합니다.

이를 통해 액티브 유닛 역할일 때 연결을 수락하는 장애 조치 연결 TCP 포트가 구성됩니다. 이는 백업 ASAv가 연결할 액티브 ASAv에서 열려 있는 포트입니다.

참고 기본값인 44442를 유지하는 것이 좋습니다. 이 값은 HA 피어 둘 다에서 기본값입니다. 하나의 HA 피어에 대한 기본값을 변경하는 경우 다른 HA 유닛에서도 동일하게 변경하는 것이 가장 좋습니다.

단계 **2** 유닛 폴링 및 대기 시간을 변경합니다.

failover cloud polltime *poll_time* [**holdtime** *time*]

예제**:**

```
ciscoasa(config)# failover cloud polltime 10 holdtime 30
```

polltime 범위는 1~15초입니다. 보류 시간은 유닛이 실패한 것으로 표시될 때 hello 패킷이 손실되는 데 소요된 시간을 결정합니다. **holdtime** 범위는 3~60초입니다. 유닛 폴링 시간의 3배보다 작은 보류 시간 값은 입력할 수 없습니다. 폴링 시간이 빠를수록 ASA에서 더욱 신속하게 오류를 감지하고 장애 조치를 시행할 수 있습니다. 그러나 감지 기능이 빨라지면 네트워크에 일시적으로 정체 현상이 일어났을 때 불필요한 전환이 발생할 수 있습니다.

단계 **3** Azure 로드 밸런서 상태 프로브에 사용되는 TCP 포트를 지정합니다.

failover cloud port probe *port-number*

예제**:**

```
ciscoasa(config)# failover cloud port probe 4443
```

구축 시 Azure 로드 밸런서를 사용하는 경우 수신 연결이 액티브 유닛에 바로 전달될 수 있도록 액티브 ASAv에서는 로드 밸런서의 TCP 프로브에 응답해야 합니다.

Azure 서비스 주체에 대한 인증 크리덴셜 구성

Azure 서비스 주체를 사용하여 ASAv HA 피어가 경로 테이블과 같은 Azure 리소스에 액세스하거나 이를 수정하도록 활성화할 수 있습니다. Azure AD(Active Directory) 애플리케이션을 설치하고 필요한 권한을 할당해야 합니다. 다음과 같은 명령을 사용하면 ASAv에서 서비스 주체를 사용하여 Azure로 인증할 수 있습니다. Azure 서비스 주체에 대한 자세한 내용은 ASAv 빠른 시작 가이드의 Azure 장을 참조하십시오.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.
- 기본 유닛과 보조 유닛 모두에서 이러한 설정을 구성합니다. 기본 유닛에서 보조 유닛으로 구성이 동기화되지 않습니다.

프로시저

단계 **1** Azure 서비스 주체의 Azure 서브스크립션 ID를 구성합니다.

failover cloud subscription-id *subscription-id*

예제:

```
(config)# failover cloud subscription-id ab2fe6b2-c2bd-44
```

Azure 경로 테이블을 수정하려면 Azure 서브스크립션 ID가 필요합니다. 클라우드 HA 사용자가 내부 경로를 액티브 유닛으로 향하도록 지시하려는 경우를 예로 들 수 있습니다.

단계 **2** Azure 서비스 주체 크리덴셜 정보를 구성합니다.

failover cloud authentication {**application-id** | **directory-id** | **key**}

장애 조치 중에 Azure 경로 테이블을 변경하려면 경로 테이블에 액세스하기 전에 Azure 인프라에서 액세스 키를 얻어야 합니다. HA 쌍을 제어하는 Azure 서비스 주체용 비밀 키, 애플리케이션 ID, 디렉터리 ID를 사용하여 액세스 키를 얻습니다.

단계 **3** Azure 서비스 주체의 애플리케이션 ID를 구성합니다.

failover cloud authentication application-id *appl-id*

예제:

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e4201
```

Azure 인프라에서 액세스 키를 요청할 때 이 애플리케이션 ID가 필요합니다.

단계 **4** Azure 서비스 주체의 디렉터리 ID를 구성합니다.

failover cloud authentication directory-id *dir-id*

예제:

```
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
```

Azure 인프라에서 액세스 키를 요청할 때 이 디렉터리 ID가 필요합니다.

단계 **5** Azure 서비스 주체의 비밀 키 ID를 구성합니다.

failover cloud authentication key *secret-key* [**encrypt**]

예제:

```
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
```

Azure 인프라에서 액세스 키를 요청할 때 이 비밀 키가 필요합니다. **encrypt** 키워드가 있는 경우 **running-config**에서 비밀 키가 암호화됩니다.

Azure 경로 테이블 구성

경로 테이블 구성은 ASAv가 액티브 유닛 역할을 수행할 때 업데이트해야 하는 Azure 사용자 정의 경로에 대한 정보로 이루어집니다. 장애 조치 시 내부 경로를 액티브 유닛으로 향하도록 지시할 수 있습니다. 이때 액티브 유닛에서는 구성된 경로 테이블 정보를 사용하여 경로가 자신에게 향하도록 자동으로 지시합니다.

참고 액티브 유닛과 백업 유닛 모두에서 Azure 경로 테이블 정보를 구성해야 합니다.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.
- 기본 유닛과 보조 유닛 모두에서 이러한 설정을 구성합니다. 기본 유닛에서 보조 유닛으로 구성이 동기화되지 않습니다.
- 서비스 주체용 Azure 서브스크립션 ID 및 Azure 인증 크리덴셜을 포함하여 사용 가능한 Azure 환경 정보를 확보합니다.

프로시저

단계 **1** 장애 조치 중에 업데이트해야 하는 Azure 경로 테이블을 구성합니다.

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

예제:

```
ciscoasa(config)# failover cloud route-table inside-rt
```

(선택 사항) 둘 이상의 Azure 서브스크립션에서 사용자 정의 경로를 업데이트하려면 **subscription-id** 파라미터를 포함합니다.

예제:

```
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
```

route-table 명령 수준의 **subscription-id** 파라미터는 전역 수준에 지정된 Azure 서브스크립션 ID를 재정의합니다. Azure 서브스크립션 ID를 지정하지 않고 **route-table** 명령을 입력하는 경우, 전역 **subscription-id** 파라미터가 사용됩니다. Azure 서브스크립션 ID에 대한 내용은 Azure 서비스 주체에 대한 인증 크리덴셜 구성, 341 페이지을 참조하십시오.

참고 **route-table** 명령을 입력하면 ASAv는 **cfg-fover-cloud-rt** 모드로 전환됩니다.

단계 **2** 경로 테이블에 대해 Azure 리소스 그룹을 구성합니다.

rg *resource-group*

예제:

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
```

Azure 내 경로 테이블 업데이트 요청을 위해서는 리소스 그룹이 필요합니다.

단계 **3** 장애 조치 시 업데이트해야 하는 경로를 구성합니다.

route name *route-name* **prefix** *address-prefix* **nexthop** *ip-address*

예제:

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

주소 접두사는 IP 주소 접두사, 슬래시('/') 및 숫자 넷마스크로 구성됩니다. 예를 들어 *192.120.0.0/16* 입니다.

예

전체 구성의 예:

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4
```

액티브/백업 장애 조치 활성화

기본 유닛과 보조 유닛 모두에서 설정을 구성한 후에 액티브/백업 장애 조치를 활성화합니다. 기본 유닛에서 보조 유닛으로 구성이 동기화되지 않습니다. 각 유닛은 장애 조치 트래픽을 처리하기 위해 유사한 구성을 사용하여 개별적으로 구성되어야 합니다.

액티브/백업 장애 조치를 위한 기본 유닛 활성화

이 섹션의 단계에 따라 액티브/백업 장애 조치 구성에서 기본 유닛을 활성화합니다.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

프로시저

단계 **1** 장애 조치를 사용하도록 설정합니다.

ciscoasa(config)# failover

단계 **2** 플래시 메모리에 시스템 구성을 저장합니다.

ciscoasa(config)# write memory

예

다음 예에는 기본 유닛에 대한 전체 구성이 나와 있습니다.

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.4

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

다음에 수행할 작업

보조 유닛을 활성화합니다.

액티브/백업 장애 조치를 위한 보조 유닛 활성화

이 섹션의 단계에 따라 액티브/백업 장애 조치 구성에서 보조 유닛을 활성화합니다.

시작하기 전에

- 단일 상황 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

프로시저

단계 **1** 장애 조치를 사용하도록 설정합니다.

ciscoasa(config)# **failover**

단계 **2** 플래시 메모리에 시스템 구성을 저장합니다.

ciscoasa(config)# **write memory**

예

다음 예에는 보조 유닛에 대한 전체 구성이 나와 있습니다.

```
ciscoasa(config)# failover cloud unit secondary
ciscoasa(config)# failover cloud peer ip 10.4.3.5

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

퍼블릭 클라우드의 장애 조치 관리

이 섹션에서는 장애 조치를 활성화한 후 클라우드에서 장애 조치 유닛을 관리하는 방법 및 한 유닛에서 다른 유닛으로 장애 조치를 강제로 수행하도록 변경하는 방법에 대해 설명합니다.

장애 조치 적용

스탠바이 유닛을 강제로 액티브 유닛으로 만들려면 다음 명령을 수행합니다.

시작하기 전에

단일 상황 모드의 시스템 실행 영역에서 이 명령을 사용합니다.

프로시저

단계 **1** 스탠바이 유닛에서 입력하는 경우 장애 조치를 강제로 실행합니다.

failover active

예제**:**

```
ciscoasa# failover active
```

대기 유닛이 활성 유닛이 됩니다.

단계 **2** 액티브 유닛에서 입력하는 경우 장애 조치를 강제로 실행합니다.

no failover active

예제**:**

```
ciscoasa# no failover active
```

활성 유닛은 대기 유닛이 됩니다.

경로 업데이트

Azure에서 경로의 상태가 액티브 역할의 ASAv와 일치하지 않는 경우, 다음과 같은 EXEC 명령을 사용하여 ASAv에서 경로 업데이트를 강제로 실행할 수 있습니다.

시작하기 전에

단일 상황 모드의 시스템 실행 영역에서 이 명령을 사용합니다.

프로시저

액티브 유닛에서 경로를 업데이트합니다.

failover cloud update routes

예제:

```
ciscoasa# failover cloud update routes
Beginning route-table updates
Routes changed
```

이 명령은 액티브 역할의 ASAv에서만 유효합니다. 인증이 실패하는 경우 명령 출력이 `Route changes failed`가 됩니다.

Azure 인증 확인

Azure에서 ASAv HA 구축에 성공하려면 서비스 주체 구성을 정확하게 완료해야 합니다. 적절한 Azure 권한을 부여받지 못하면 ASAv 유닛에서는 장애 조치를 처리하고 경로 업데이트를 수행하기 위해 리소스에 액세스할 수 없습니다. 장애 조치 구성을 테스트하여 Azure 서비스 주체의 다음 요소와 관련된 오류를 탐지할 수 있습니다.

- 디렉터리 ID
- 애플리케이션 ID
- 인증 키

시작하기 전에

단일 상황 모드의 시스템 실행 영역에서 이 명령을 사용합니다.

프로시저

ASAv HA 구성에서 Azure 인증 요소를 테스트합니다.

test failover cloud authentication

예제:

```
ciscoasa(config)# test failover cloud authentication
Checking authentication to cloud provider
Authentication Succeeded
```

인증이 실패하는 경우 명령 출력이 `Authentication Failed`가 됩니다.

디렉터리 ID 또는 애플리케이션 ID가 적절하게 구성되지 않은 경우, Azure에서는 인증 토큰을 얻기 위한 REST 요청에서 주소가 지정된 리소스를 인식하지 못합니다. 이 조건 항목에 대한 이벤트 기록은 다음과 같이 작성됩니다.

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

디렉터리 ID 또는 애플리케이션 ID가 올바르지만 인증 키가 적절하게 구성되지 않은 경우, Azure에서는 인증 토큰을 생성하기 위한 권한을 부여하지 않습니다. 이 조건 항목에 대한 이벤트 기록은 다음과 같이 해석됩니다.

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

퍼블릭 클라우드의 장애 조치 모니터링

이 섹션에서는 장애 조치 상태를 모니터링하는 방법에 대해 설명합니다.

장애 조치 상태

장애 조치 상태를 모니터링하려면 다음 명령 중 하나를 입력합니다.

- **show failover**

  유닛의 페일오버 상태에 대한 정보를 표시합니다. 구성하지 않은 구성 요소의 값은 *not configured* 로 표시됩니다.

  경로 업데이트 정보는 액티브 유닛에 대해서만 제공됩니다.

- **show failover history**

  타임스탬프, 심각도 수준, 이벤트 유형 및 이벤트 텍스트와 함께 장애 조치 이벤트 기록을 표시합니다.

장애 조치 메시지

장애 조치 **Syslog** 메시지

ASA에서는 심각한 상황을 의미하는 우선순위 등급 2에 해당하는 장애 조치와 관련된 여러 가지 syslog 메시지를 전달합니다. 이러한 메시지를 보려면 syslog 메시지 가이드를 참조하십시오. Syslog 메시지는 1045xx 및 1055xx 범위에 있습니다.

참고 장애 조치 시에는 ASA에서 인터페이스를 논리적으로 종료했다가 작동하므로 syslog 메시지가 생성됩니다. 이는 정상적인 동작입니다.

전환 시 생성되는 샘플 syslog는 다음과 같습니다.

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error: Unknown
 error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
Active unit
```

```
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

퍼블릭 클라우드 구축과 관련된 각 syslog에는 앞에 (기본) 또는 (보조) 유닛 역할이 적혀 있습니다.

장애 조치 디버그 메시지

디버그 메시지를 보려면 **debug fover** 명령을 입력합니다. 자세한 내용은 명령 참조를 참조하십시오.

참고 디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되므로 시스템 성능에 큰 영향을 미칠 수 있습니다. 따라서 **debug fover** 명령은 특정 문제를 트러블슈팅하거나 Cisco TAC를 통해 세션 문제를 트러블슈팅하는 동안에만 사용해야 합니다.

SNMP 장애 조치 트랩

장애 조치를 위한 SNMP syslog 트랩을 수신하려면 SNMP 에이전트에서 SNMP 트랩을 SNMP 관리 스테이션으로 전송하도록 구성하고, syslog 호스트를 정의하고, Cisco syslog MIB를 SNMP 관리 스테이션으로 컴파일합니다.

퍼블릭 클라우드의 장애 조치에 대한 기록

기능 이름	릴리스	기능 정보
Microsoft Azure에서의 액티브/백업 장애 조치	9.8(200)	이 기능을 도입했습니다.

10 장

ASA 클러스터

클러스터링을 사용하면 여러 개의 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. 클러스터링으로 지원되지 않는 기능, 362 페이지를 참조하십시오.

ASA 클러스터링 정보

이 섹션에서는 클러스터링 아키텍처 및 이러한 아키텍처의 작동 방식에 대해 설명합니다.

ASA 클러스터를 네트워크에 맞게 활용하는 방법

클러스터는 단일 유닛으로 작동하는 여러 개의 ASA로 구성됩니다. 클러스터로 작동하려면 ASA에는 다음과 같은 인프라가 필요합니다.

- 클러스터 내 커뮤니케이션을 위한 분리된 고속 백플레인 네트워크(또는 클러스터 제어 링크라고 함)
- 구성 및 모니터링을 위한 각 ASA에 대한 관리 액세스

네트워크에 클러스터를 배치할 경우, 업스트림 및 다운스트림 라우터에서는 다음 중 한 가지 방법을 사용하여 클러스터로 들어오고 나가는 데이터의 로드 밸런싱을 수행할 수 있어야 합니다.

- 스팬 EtherChannel(권장) — 클러스터의 여러 멤버에 대한 인터페이스는 단일 EtherChannel로 그룹화되며, EtherChannel은 유닛 간의 로드 밸런싱을 수행합니다.
- 정책 기반 라우팅(라우팅 방화벽 모드 전용) — 업스트림 및 다운스트림 라우터에서는 경로 맵 및 ACL을 사용하여 유닛 간의 로드 밸런싱을 수행합니다.
- Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용) — 업스트림 및 다운스트림 라우터에서는 Equal Cost 고정 또는 동적 라우팅을 사용하여 유닛 간의 로드 밸런싱을 수행합니다.

성능 확장 요소

클러스터에 여러 유닛을 결합할 경우 성능을 대략 다음과 같이 예측할 수 있습니다.

- 통합 처리량의 70%
- 최대 연결 수의 60%
- 초당 연결 수의 50%

예를 들어 처리량의 경우 ASA 5585-X(SSP-40 포함)를 단독 실행하면 실제 방화벽 트래픽 중 약 10Gbps를 처리할 수 있습니다. 8개 유닛으로 구성된 클러스터의 경우 최대 통합 처리량은 80Gbps의 약 70%(유닛 8개 x 10Gbps), 즉 56Gbps에 해당합니다.

클러스터 멤버

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다. 이 섹션에서는 각 멤버 역할의 특성을 설명합니다.

부트스트랩 컨피그레이션

각 디바이스에서 클러스터 이름, 클러스터 제어 링크 인터페이스, 기타 클러스터 설정 등을 비롯한 최소 부트스트랩 컨피그레이션을 구성합니다. 클러스터링을 사용하는 첫 번째 유닛이 일반적으로 마스터 유닛이 됩니다. 후속 유닛에서 클러스터링을 사용하도록 설정할 경우, 해당 유닛은 클러스터에 슬레이브로 참가합니다.

마스터 및 슬레이브 유닛 역할

클러스터의 멤버 중 하나는 마스터 유닛입니다. 마스터 유닛은 부트스트랩 컨피그레이션의 우선순위 설정에 따라 결정됩니다. 우선순위는 1에서 100까지 1이 가장 높은 우선순위입니다. 기타 모든 멤버는 슬레이브 유닛입니다. 클러스터를 처음 생성할 경우, 추가되는 첫 번째 유닛은 해당 단계에서 클러스터의 유일한 유닛이므로 마스터 유닛이 됩니다.

마스터 유닛에서만 모든 컨피그레이션(부트스트랩 컨피그레이션 제외)을 수행해야 하며, 그 후 이러한 컨피그레이션은 슬레이브 유닛에 복제됩니다. 인터페이스와 같은 물리적 자산의 경우 마스터 유닛의 컨피그레이션은 모든 슬레이브 유닛에 미러링됩니다. 예를 들어, GigabitEthernet 0/1을 내부 인

터페이스로 구성하고 GigabitEthernet 0/0을 외부 인터페이스로 구성할 경우 이러한 인터페이스는 슬레이브 유닛에서도 내부 및 외부 인터페이스로 사용됩니다.

일부 기능은 클러스터에서 확장되지 않으며 마스터 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다.

마스터 유닛 선택

클러스터의 멤버는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 마스터 유닛을 선택합니다.

1. 유닛에 클러스터링을 사용할 경우(또는 이미 사용 설정된 클러스터링을 처음 시작할 경우), 선택 요청이 3초마다 전송됩니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 1에서 100까지 설정되며 1이 가장 높은 우선순위입니다.
3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 마스터 유닛이 됩니다.

참고 가장 우선순위가 높은 유닛이 공동으로 여러 개인 경우, 클러스터 유닛 이름과 일련 번호를 사용하여 마스터 유닛을 결정합니다.

4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 마스터 유닛이 되는 것은 아닙니다. 기존 마스터 유닛은 응답이 중지되지 않는 한 항상 마스터 유닛으로 유지되며 응답이 중지될 때에 새 마스터 유닛이 선택됩니다.

참고 유닛을 수동으로 강제 변경하여 마스터 유닛이 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

클러스터 인터페이스

데이터 인터페이스를 스팬 EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 클러스터의 모든 데이터 인터페이스는 1가지 유형만 가능합니다. 자세한 내용은 클러스터 인터페이스 정보, 380 페이지를 참조하십시오.

클러스터 제어 링크

각 유닛에서는 최소 1개의 하드웨어 인터페이스를 클러스터 제어 링크로 지정해야 합니다. 자세한 내용은 클러스터 제어 링크 정보, 380 페이지를 참조하십시오.

ASA 클러스터 내의 고가용성

ASA 클러스터링에서는 유닛과 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

유닛 상태 모니터링

마스터 유닛에서는 클러스터 제어 링크를 통해 하트비트 메시지를 주기적으로 전송하여 모든 슬레이브 유닛을 모니터링합니다(기간은 구성 가능함). 각 슬레이브 유닛에서는 동일한 메커니즘을 사용하여 마스터 유닛을 모니터링합니다. 유닛 상태 검사에 장애가 발생하는 경우 클러스터에서 유닛이 제거됩니다.

인터페이스 모니터링

각 유닛에서는 명명되어 있고 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 마스터 유닛에 보고합니다.

- 스팬 EtherChannel — 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 유닛에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인합니다. 상태가 마스터 유닛에 보고됩니다.
- 개별 인터페이스(라우팅 모드 전용) — 각 유닛에서는 인터페이스를 스스로 모니터링하고 인터페이스 상태를 마스터 유닛에 보고합니다.

상태 모니터링을 활성화하면 모든 물리적 인터페이스(주요 EtherChannel 및 중복 인터페이스 유형 포함)가 기본적으로 모니터링됩니다. 선택적으로 인터페이스별 모니터링을 비활성화할 수 있습니다. 명명된 인터페이스만 모니터링될 수 있습니다. 예를 들어, 명명된 EtherChannel은 장애가 발생한 것으로 간주되지 않아야 합니다. 즉, EtherChannel의 모든 멤버 포트가 클러스터 제거를 트리거하지 못해야 합니다(최소 포트 번들 설정에 따라).

유닛의 모니터링된 인터페이스에 장애가 발생하면 클러스터에서 해당 유닛이 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. EtherChannel(Spanned 또는 일반)의 경우, 설정된 멤버에 대한 인터페이스가 중지되면 ASA에서는 9초 후에 해당 멤버를 제거합니다. ASA에서는 유닛이 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 ASA가 클러스터에서 제거되지 않습니다. 비 EtherChannel의 경우, 멤버 상태와 관계없이 500ms 후에 유닛이 제거됩니다.

실패 이후 상태

클러스터의 유닛에 오류가 발생할 경우, 해당 유닛에서 호스팅하는 연결이 다른 유닛으로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 클러스터 링크를 통해 공유됩니다.

마스터 유닛에 장애가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 마스터 유닛이 됩니다.

ASA는 실패 이벤트에 따라 클러스터에 다시 참가하려고 시도합니다.

참고 ASA가 비활성화되고 클러스터에 자동으로 다시 조인하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우 관리 인터페이스가 비활성화됩니다. 추가 구성을 위해서는 콘솔 포트를 사용해야 합니다.

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 처음 참가 시 클러스터 제어 링크 장애 — 클러스터 제어 링크의 문제를 해결한 후에는 콘솔 포트에서 **cluster group** *name*을 입력한 다음 **enable**을 입력하여 클러스터링을 다시 활성화함으로써 클러스터에 수동으로 다시 참가해야 합니다.
- 클러스터 참가 후 클러스터 제어 링크 장애 — ASA에서는 자동으로 5분마다 무기한으로 다시 참가하려고 시도합니다. 이 동작은 구성 가능합니다.
- 데이터 인터페이스 장애 — ASA에서는 자동으로 5분, 10분, 마지막으로 20분 후에 다시 참가하도록 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 ASA에서는 클러스터링을 비활성화합니다. 데이터 인터페이스 문제를 해결한 후에는 콘솔 포트에서 **cluster group** *name*을 입력한 다음 **enable**을 입력하여 클러스터링을 수동으로 활성화해야 합니다. 이 동작은 구성 가능합니다.
- ASA 5585-X의 ASA FirePOWER 모듈 장애 — ASA에서는 자동으로 5분 후에 다시 참가하도록 시도합니다.
- ASA FirePOWER 소프트웨어 모듈 장애 — 모듈 문제를 해결한 후에는 콘솔 포트에서 **cluster group** *name*을 입력한 다음 **enable**을 입력하여 클러스터링을 수동으로 활성화해야 합니다.
- 유닛 오류 — 유닛 상태 검사 오류로 인해 클러스터에서 유닛이 제거된 경우, 클러스터에 다시 가입할 수 있을지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한 경우 클러스터 제어 링크가 활성 상태이고 **enable** 명령이 계속 활성화되어 있으면 전원을 다시 가동할 때 유닛이 클러스터에 다시 가입할 수 있습니다. ASA에서는 5초마다 클러스터에 다시 참가하도록 시도합니다.
- 내부 오류 — 내부 장애 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등이 있습니다. 유닛에서는 자동으로 5분, 10분, 20분 간격으로 클러스터에 다시 참가하도록 시도합니다. 이 동작은 구성 가능합니다.

마스터 유닛 부트스트랩 설정 구성, 400 페이지을 참조하십시오.

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 장애 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다. 백업 소유자는 일반적으로 관리자이기도 합니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 ***15:*** 클러스터 전반에 걸쳐 복제된 기능

트래픽	상태 지원	**Notes**(참고)
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	—
MAC 주소 테이블	예	—
사용자 ID	Yes(예)	AAA 규칙(uauth)을 포함하고 방화벽을 식별합니다.
IPv6 네이버 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—
중앙 집중식 VPN(사이트 대 사이트)	아니요	마스터 유닛에 오류가 발생할 경우 VPN 세션의 연결이 끊어집니다.
분산 VPN(사이트 대 사이트)	Yes(예)	백업 세션이 활성 세션이 되며 새 백업 세션이 생성됩니다.

구성 복제

클러스터의 모든 유닛에서는 단일 구성을 공유합니다. 마스터 유닛에서는 구성만 변경할 수 있으며 변경 사항은 클러스터의 모든 다른 유닛에 자동으로 동기화됩니다.

ASA 클러스터 관리

ASA 클러스터링을 사용하는 데 따른 여러 장점 중 하나는 관리하기가 쉽다는 점입니다. 이 섹션에서는 클러스터를 관리하는 방법에 대해 설명합니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결할 것을 권장합니다. 이 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

관리 인터페이스의 경우 전용 관리 인터페이스 중 하나를 사용하는 것이 좋습니다. 관리 인터페이스를 개별 인터페이스(라우팅 및 투명 모드용 모두 해당) 또는 스팬 EtherChannel 인터페이스로 구성할 수 있습니다.

데이터 인터페이스에 스팬 EtherChannel을 사용 중인 경우에도, 관리용으로는 개별 인터페이스를 사용하는 것이 좋습니다. 개별 인터페이스를 사용하면 필요한 경우 각 유닛에 직접 연결할 수 있는 반면, 스팬 EtherChannel 인터페이스의 경우에는 현재 마스터 유닛에 원격 연결만 가능합니다.

참고 스팬 EtherChannel 인터페이스 모드를 사용 중이고 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 경로를 사용해야 합니다.

개별 인터페이스의 경우, 기본 클러스터 IP 주소는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 각 인터페이스에는 주소의 범위를 구성하여 현재 마스터를 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 마스터 유닛이 변경될 경우 주요 클러스터 IP 주소는 새 마스터 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 로컬 IP 주소는 라우팅에 사용되며 문제 해결에도 도움이 됩니다.

예를 들어, 현재 마스터 유닛에 항상 연결되어 있는 기본 클러스터 IP 주소에 연결하여 클러스터를 관리할 수 있습니다. 로컬 IP 주소에 연결하여 개별 멤버를 관리할 수 있습니다.

TFTP 또는 syslog 같은 아웃바운드 관리 트래픽의 경우 마스터 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

스팬 EtherChannel 인터페이스에는 하나의 IP 주소만 구성할 수 있으며, 해당 IP 주소는 항상 마스터 유닛에 연결됩니다. EtherChannel 인터페이스를 사용할 경우 슬레이브 유닛에 직접 연결할 수 없으며, 관리 인터페이스는 개별 인터페이스로 구성하는 것이 좋습니다. 이렇게 하면 각 유닛에 연결할 수 있습니다. 디바이스-로컬 EtherChannel을 관리용으로 사용할 수 있습니다.

마스터 유닛 관리와 슬레이브 유닛 관리 비교

모든 관리 및 모니터링은 마스터 유닛에서 수행할 수 있습니다. 마스터 유닛에서 런타임 통계, 리소스 사용량 또는 모든 유닛의 기타 모니터링 정보를 확인할 수 있습니다. 또한 클러스터 내의 모든 유닛에 명령을 배포하고, 슬레이브 유닛의 콘솔 메시지를 마스터 유닛으로 복제할 수 있습니다.

필요한 경우 슬레이브 유닛을 직접 모니터링할 수 있습니다. 마스터 유닛에서도 사용 가능하지만 슬레이브 유닛에서 파일 관리를 수행할 수 있습니다(구성 백업 및 이미지 업데이트 포함). 다음 기능은 마스터 유닛에서 사용할 수 없습니다.

- 유닛당 클러스터별 통계 모니터링
- 유닛당 Syslog 모니터링(콘솔 복제가 활성화된 경우 콘솔로 전송되는 syslog 제외).
- SNMP
- NetFlow

RSA 키 복제

마스터 유닛에서 RSA 키를 생성할 경우, 해당 키는 모든 슬레이브 유닛에 복제됩니다. 기본 클러스터 IP 주소에 대한 SSH 세션이 있는 경우 마스터 유닛에 오류가 발생하면 연결이 끊어집니다. 새 마스터 유닛에서는 SSH 연결에 동일한 키를 사용하므로, 새 마스터 유닛에 다시 연결할 때 캐시된 SSH 호스트 키를 업데이트하지 않아도 됩니다.

ASDM 연결 인증서 IP 주소 불일치

기본적으로, 자체 서명된 인증서는 로컬 IP 주소를 기준으로 ASDM 연결에 사용됩니다. ASDM을 사용하여 기본 클러스터 IP 주소를 연결할 경우, 인증서에서는 기본 클러스터 IP 주소가 아닌 로컬 IP 주소를 사용하므로 IP 주소가 일치하지 않는다는 경고 메시지가 표시됩니다. 이 메시지를 무시하고 ASDM 연결을 설정할 수 있습니다. 그러나 이러한 유형의 경고를 방지하려면 기본 클러스터 IP 주소 및 IP 주소 풀의 모든 로컬 IP 주소가 포함된 인증서를 등록하면 됩니다. 그런 다음 이 인증서를 각 클러스터 멤버에 사용할 수 있습니다.

사이트 간 클러스터링

사이트 간 설치 시 권장 지침을 준수하면 ASA 클러스터링을 활용할 수 있습니다.

각 클러스터 섀시를 별도의 사이트 ID에 속하도록 구성할 수 있습니다.

사이트 ID는 사이트별 MAC 주소 및 IP 주소와 작동합니다. 클러스터에서 온 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면, 클러스터가 수신한 패킷은 전역 MAC 주소 및 IP 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지 못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다. 사이트별 MAC 주소 및 IP 주소는 Spanned EtherChannel만을 사용하는 라우팅 모드에서 지원됩니다.

사이트 ID는 LISP 검사를 사용한 플로우 모빌리티 활성화, 데이터 센터의 사이트 간 클러스터링에 대해 왕복 시간 레이턴시를 줄이고 성능을 개선하기 위한 관리자 지역화, 그리고 트래픽 플로우의 백업 소유자가 항상 소유자와 다른 사이트에 있는 연결에 대한 사이트 이중화에도 사용됩니다.

사이트 간 클러스터링에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 데이터 센터 인터커넥트 크기 조정 -ASA 클러스터링의 요구 사항 및 사전 요구 사항, 372 페이지
- 사이트 간 지침 -ASA 클러스터링 지침, 374 페이지
- 클러스터 플로우 모빌리티 구성 —클러스터 플로우 모빌리티 구성, 414 페이지
- 관리자 현지화 활성화 —관리자 현지화 활성화, 413 페이지
- 사이트 이중화 활성화 —관리자 현지화 활성화, 413 페이지
- 사이트 간 예시 -사이트 간 클러스터링 예시, 450 페이지

ASA 클러스터의 연결 관리 방법

클러스터의 여러 멤버에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

연결 역할

각 연결에 대해 정의된 다음 역할을 참조하십시오.

- 소유자 - 일반적으로 연결을 가장 처음 수신하는 유닛입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다. 원래 소유자가 실패하고 새 유닛이 연결에서 패킷을 수신하면, 관리자는 해당 유닛으로부터 새 소유자를 선택합니다.
- 백업 소유자 - 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있도록 소유자로부터 수신한 TCP/UDP 상태 정보를 저장하는 유닛입니다. 백업 소유자는 장애 발생 시 연결을 승계할 수 없습니다. 소유자를 사용할 수 없을 경우, 연결에서 패킷을 받을(로드 밸런싱을 기준으로) 첫 번째 유닛이 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

  관리자(아래 설명 참조)는 소유자와 같은 유닛이 아니라면 백업 소유자로도 사용됩니다. 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  Firepower 9300의 섀시 간 클러스터링(섀시 하나에 클러스터 유닛이 3개까지 포함될 수 있음)에서 백업 소유자가 소유자와 같은 섀시에 있으면 섀시 장애로부터 플로우를 보호하기 위해 다른 섀시에서 추가 백업 소유자가 선택됩니다.

  사이트 간 클러스터링에 대한 관리자 지역화를 활성화하는 경우에는 두 가지 백업 소유자 역할, 즉 로컬 백업 및 글로벌 백업이 있습니다. 소유자는 항상 자신과 동일한 사이트의 로컬 백업을 선택합니다(사이트 ID 기반). 글로벌 백업은 어느 사이트에든 있을 수 있으며, 로컬 백업과 동일한 유닛일 수도 있습니다. 소유자는 연결 상태 정보를 두 백업에 모두 전송합니다.

  사이트 이중화를 활성화하는 경우 백업 소유자가 소유자와 같은 사이트에 있으면 사이트 장애로부터 플로우를 보호하기 위해 다른 사이트에서 추가 백업 소유자가 선택됩니다. 섀시 백업 및 사이트 백업은 서로 독립적이므로 경우에 따라서는 플로우에 섀시 백업과 사이트 백업이 모두 포함됩니다.
- 관리자 - 전달자의 소유자 조회 요청을 처리하는 유닛입니다. 소유자가 새 연결을 수신할 경우, 소유자 유닛에서는 소스/대상 IP 주소와 포트의 해시를 기준으로 관리자 유닛을 선택하며 관리자 유닛에 메시지를 전송하여 새 연결을 등록합니다. 패킷이 소유자 유닛이 아닌 다른 유닛에 전달될 경우, 해당 유닛에서는 관리자 유닛에 어떤 유닛이 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다. 관리자가 실패하면 소유자는 새 관리자를 선택합니다.

  관리자는 소유자와 같은 유닛이 아니라면 백업 소유자로도 사용됩니다(위의 설명 참조). 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  사이트 간 클러스터링에 대한 관리자 지역화를 활성화하는 경우에는 두 가지 관리자 역할, 즉 로컬 관리자와 전역 관리자가 있습니다. 소유자는 항상 자신과 동일한 사이트의 로컬 관리자를 선택합니다(사이트 ID 기반). 전역 관리자는 어느 사이트에든 있을 수 있으며, 로컬 관리자와 동일

한 유닛일 수도 있습니다. 원래 소유자가 실패하면 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다.

- 전달자 — 패킷을 소유자 유닛에 전달하는 유닛입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 흐름을 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 관리자 지역화를 활성화하면, 전달자는 항상 로컬 관리자를 쿼리합니다. 전달자는 로컬 관리자가 소유자를 모르는 경우에만 전역 관리자를 쿼리합니다. 클러스터 멤버가 다른 사이트의 소유인 연결에 대한 패킷을 수신하는 경우를 예로 들 수 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 시퀀스 임의 설정을 비활성화한 경우 SYN 쿠키는 사용되지 않으며, 책임자에게 쿼리해야 합니다.) DNS 및 ICMP 같이 짧은 흐름의 경우 쿼리 대신 전달자가 책임자에게 패킷을 즉시 전송하고 책임자가 소유자에게 전송합니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.

연결에 PAT(Port Address Translation)가 사용되는 경우, PAT 유형(per-session 또는 multi-session)이 클러스터의 어떤 멤버가 새 연결의 소유자가 될지에 영향을 미칩니다.

- Per-session PAT(세션 단위 PAT) - 연결에서 초기 패킷을 수신하는 유닛이 소유자입니다.

  기본적으로 TCP 및 DNS UDP 트래픽은 per-session PAT를 사용합니다.

- Multi-session PAT(다중 세션 PAT) - 항상 마스터 유닛이 소유자입니다. Multi-session PAT 연결이 초기에 슬레이브 유닛에서 수신되면 슬레이브 유닛은 해당 연결을 마스터 유닛으로 전달합니다.

  기본적으로 UDP(DNS UDP 제외) 및 ICMP 트래픽은 multi-session PAT를 사용하므로, 항상 마스터 유닛에서 해당 연결을 소유합니다.

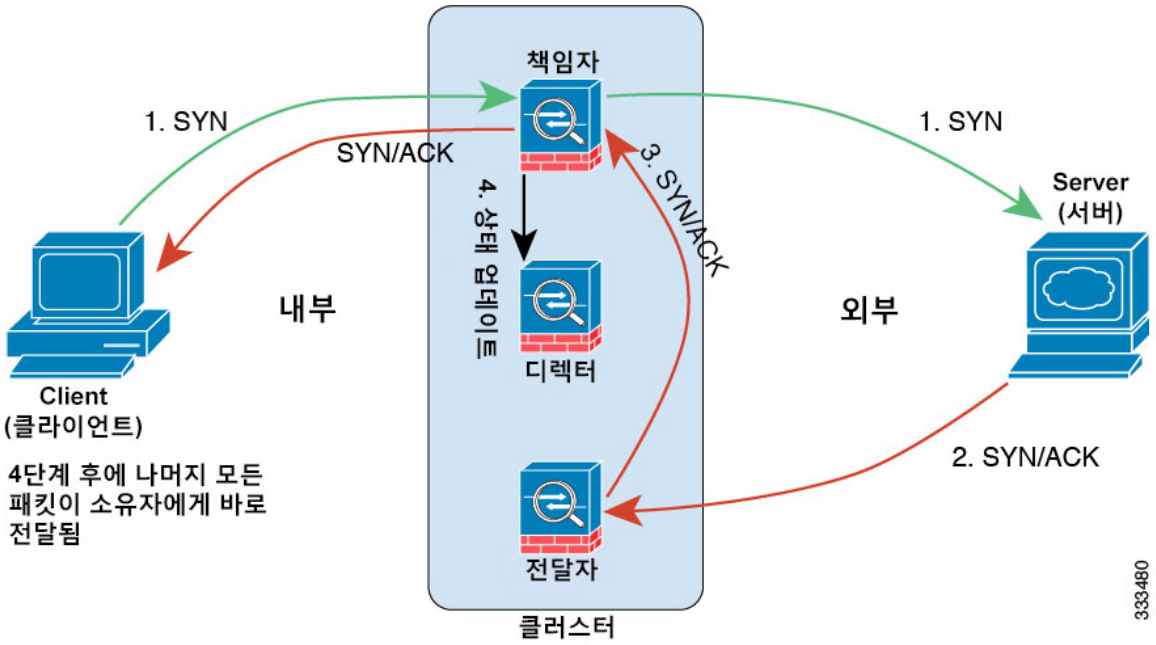
TCP 및 UDP에 대한 per-session PAT 기본값을 변경하여, 이러한 프로토콜에 대한 연결이 구성에 따라 세션 단위 또는 다중 세션으로 처리되도록 할 수 있습니다. ICMP의 경우 기본 multi-session PAT에서 변경할 수 없습니다. 세션당 PAT에 대한 자세한 내용은 방화벽 설정 가이드를 참조하십시오.

새 연결 소유권

로드 밸런싱을 통해 클러스터의 멤버에 새 연결이 전송될 경우, 해당 유닛에서는 연결의 양방향을 모두 소유합니다. 다른 유닛에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 유닛에 전달됩니다. 최상의 성능을 실현하려면, 같은 유닛에 전송될 수 있도록 흐름의 양방향에 적절한 외부 로드 밸런싱이 필요합니다. 또한 흐름은 유닛 간에 균일하게 분산되어야 합니다. 다른 유닛에 반대 방향의 흐름이 전송될 경우, 이는 원래 유닛으로 다시 리디렉션됩니다.

샘플 데이터 흐름

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.



1. SYN 패킷은 클라이언트에서 시작되고 ASA에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 ASA에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 ASA는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.
5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 흐름을 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 유닛에 전달된 경우, 소유자 유닛에 관리자를 쿼리하고 흐름을 설정합니다.
8. 흐름 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

클러스터 전반에 걸쳐 새 **TCP** 연결 리밸런싱

업스트림 또는 다운스트림 라우터의 로드 밸런싱 기능을 사용하는 도중 흐름이 균일하게 분산되지 않을 경우, 오버로드된 유닛에서 새 TCP 흐름을 다른 유닛에 리디렉션하도록 구성할 수 있습니다. 기존 흐름은 다른 유닛으로 이동되지 않습니다.

ASA 기능 및 클러스터링

일부 ASA 기능은 ASA 클러스터링이 지원되지 않으며, 일부 기능은 마스터 유닛에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

클러스터링으로 지원되지 않는 기능

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.

- TLS 프록시를 사용하는 Unified Communication 기능
- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- 다음과 같은 애플리케이션 감시:
  - CTIQBE
  - H323, H225, RAS
  - IPsec 통과
  - MGCP
  - MMP
  - RTSP
  - SCCP(Skinny)
  - WAAS
  - WCCP
- 봇네트 트래픽 필터
- Auto Update Server
- DHCP 클라이언트, 서버, 프록시 DHCP 릴레이가 지원됩니다.
- VPN 로드 밸런싱
- 장애 조치
- ASA CX 모듈
- 통합 라우팅 및 브리징
- DCD(데드 연결 탐지)

클러스터링을 위한 중앙 집중식 기능

다음 기능은 마스터 유닛에서만 지원되며 클러스터에 확장되지 않습니다. 예를 들어, 8개 유닛으로 구성된 클러스터(SSP-60이 포함된 5585-X)가 있는 경우를 가정해 보겠습니다. 기타 VPN 라이센스에서는 하나의 ASA 5585-X(SSP-60 포함)에 사이트 대 사이트 IPsec 터널을 최대 10,000개까지 허용합니

다. 8개 유닛으로 구성된 전체 클러스터에는 터널을 10,000개까지만 사용할 수 있으며 이 기능은 확장되지 않습니다.

참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 유닛에서 마스터 유닛으로 전달됩니다.

리밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 마스터 유닛으로 리밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 마스터 유닛으로 다시 전송됩니다.

중앙 집중식 기능의 경우 마스터 유닛에 오류가 발생하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

- Site-Site VPN
- 다음과 같은 애플리케이션 감시:
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- 동적 라우팅(스팬 EtherChannel 모드 전용)
- 멀티캐스트 라우팅(개별 인터페이스 모드 전용)
- 고정 경로 모니터링
- IGMP 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- PIM 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)

- 네트워크 액세스에 대한 인증 및 권한 부여. 어카운팅이 분산됨
- 필터링 서비스

개별 유닛에 적용되는 기능

이러한 기능은 전체 클러스터 또는 마스터 유닛이 아닌 각 ASA 유닛에 적용됩니다.

- QoS — QoS 정책은 구성 복제의 일부로 클러스터 전체와 동기화됩니다. 그러나 정책은 각 유닛에서 독립적으로 시행됩니다. 예를 들어, 출력에 대한 정책 시행을 구성할 경우 특정 ASA에 있는 트래픽에서 적응 속도 및 적응 버스트 값이 시행됩니다. 3개 유닛으로 구성되고 트래픽이 균일하게 분산된 클러스터의 경우, 적응 속도는 클러스터 속도의 3배가 됩니다.
- 위협 감지 — 위협 감지는 각 유닛에 개별적으로 작동됩니다. 예를 들어, 상위 통계는 유닛별로 적용됩니다. 이를테면 포트 검사 감지 기능의 경우, 검사 트래픽이 모든 유닛 간에 로드 밸런싱되고 한 유닛에 모든 트래픽이 표시되지 않으므로 이 기능은 작동하지 않습니다.
- 리소스 관리 — 다중 상황 모드에서 리소스 관리는 로컬 사용량을 기준으로 각 유닛에 개별적으로 시행됩니다.
- LISP 트래픽 — UDP 포트 4342의 LISP 트래픽은 각각의 수신 유닛에서 검사되지만, 관리자는 할당되지 않습니다. 각 유닛은 EDI 테이블에 추가되어 클러스터 전체에서 공유되지만, LISP 트래픽 자체는 클러스터 상태 공유에 참여하지 않습니다.
- ASA Firepower 모듈 — ASA Firepower 모듈 간에는 구성 동기화 또는 상태 공유 기능이 없습니다. Firepower Management Center를 사용하여 클러스터의 ASA Firepower 모듈에 대해 일관된 정책을 유지 관리해야 합니다. 클러스터의 디바이스에 다른 ASA 인터페이스 기반 영역 정의를 사용하지 마십시오.
- ASA IPS 모듈 — IPS 모듈 간에는 컨피그레이션 동기화 또는 상태 공유 기능이 없습니다. 일부 IPS 서명의 경우 여러 연결 전반의 상태를 유지하기 위한 IPS가 필요합니다. 예를 들어, 누군가 다른 포트로 하나의 서버에 여러 개의 연결을 열고 있는 것이 IPS 모듈에 감지된 경우 포트 검사 서명이 사용됩니다. 클러스터링에서 이러한 연결은 여러 ASA 디바이스 간에 균형이 유지됩니다. 각 디바이스에는 고유한 IPS 모듈이 있습니다. 이러한 IPS 모듈에서는 상태 정보를 공유하지 않으므로, 클러스터에서 포트 검사를 결과로 감지하지 못할 수 있습니다.

네트워크 액세스 및 클러스터링용 **AAA**

네트워크 액세스용 AAA는 인증, 권한 부여, 어카운팅이라는 세 가지 구성 요소로 이루어져 있습니다. 인증 및 권한 부여는 클러스터 슬레이브에 대한 데이터 구조의 복제를 통해 클러스터링 마스터에서 중앙 집중식 기능으로 구현됩니다. 마스터 유닛이 선택된 경우, 새 마스터에서는 설정된 인증 완료 사용자 및 관련 인증 작업을 중단 없이 계속 가동하는 데 필요한 모든 정보를 보유하게 됩니다. 사용자 인증의 유휴 및 절대 시간 제한은 마스터 유닛이 변경될 경우 유지됩니다.

어카운팅은 클러스터에서 분산된 기능으로 구현됩니다. 어카운팅은 흐름 하나의 단위로 수행되므로, 흐름에 대한 어카운팅이 구성되면 흐름을 소유한 클러스터에서는 어카운팅 시작 및 중지 메시지를 AAA 서버에 보냅니다.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 흐름을 소유한 경우, 데이터 채널 소유자 유닛에서는 유휴 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유휴 시간 제한 값을 업데이트합니다. 그러나 제어 흐름 소유자가 다시 로드되고 제어 흐름이 다시 호스팅된 경우, 부모/자식 흐름 관계가 더 이상 유지되지 않으며 제어 흐름 유휴 시간 제한도 업데이트되지 않습니다.
- FTP 액세스용 AAA를 사용할 경우 마스터 유닛에서는 제어 채널 흐름을 중앙 집중화합니다.

방화벽 및 클러스터링 식별

마스터 유닛만이 AD에서 사용자-그룹을 검색하고 AD 에이전트에서 사용자-IP 매핑을 검색합니다. 그런 다음 마스터 유닛에서는 사용자 정보를 슬레이브에 제공하며, 슬레이브에서는 보안 정책을 기준으로 사용자 ID의 일치 여부를 결정할 수 있습니다.

멀티캐스트 라우팅 및 클러스터링

멀티캐스트 라우팅은 인터페이스 모드에 따라 다르게 작동합니다.

스팬 **EtherChannel** 모드의 멀티캐스트 라우팅

스팬 EtherChannel 모드에서 마스터 유닛은 빠른 경로(fast-path) 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 처리합니다. 연결이 설정되면 각 슬레이브에서 멀티캐스트 데이터 패킷을 전달할 수 있습니다.

개별 인터페이스 모드의 멀티캐스트 라우팅

개별 인터페이스 모드에서 유닛은 멀티캐스트와 별개로 작동하지 않습니다. 모든 데이터 및 라우팅 패킷은 마스터 유닛을 통해 처리되고 전달되므로, 패킷 복제가 방지됩니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 ASA에 전송할 수 있습니다. 패킷이 NAT 소유자가 아닌 ASA에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다. 보안 및 정책 확인 결과에 따라 NAT 소유자가 패킷에 대해 연결을 생성하지 않을 수도 있으므로 수신 유닛은 소유자에 대한 전달 플로우를 생성하지 않습니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

- 프록시 ARP 없음 — 개별 인터페이스에서 프록시 ARP 응답은 매핑된 주소에 전송되지 않습니다. 이렇게 되면 인접한 라우터가 클러스터에 더 이상 존재하지 않을 수 있는 ASA와 피어 관계를 유지하지 못하게 됩니다. 업스트림 라우터에는 기본 클러스터 IP 주소를 나타내는 매핑된 주소에 대한 고정 경로 또는 PBR(Object Tracking 포함)이 필요합니다. 스팬 EtherChannel의 경우에는 하나의 IP 주소만 클러스터 인터페이스에 연결되므로 이것이 문제가 되지 않습니다.

- 개별 인터페이스에 인터페이스 PAT 없음 — 개별 인터페이스에는 인터페이스 PAT가 지원되지 않습니다.
- 포트 블록 할당이 있는 PAT 없음 - 이 기능은 클러스터에서 지원되지 않습니다.
- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
  - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 유닛에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서, 호스트의 트래픽이 3개 유닛 모두에 부하 분산되는 경우 각 유닛에 하나씩 3개의 블록이 할당될 수 있습니다.
  - 백업 풀의 백업 유닛에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
  - PAT IP 주소 소유자가 다운되면 백업 유닛이 PAT IP 주소, 해당 포트 블록 및 xlate를 소유하게 됩니다. 그러나 새로운 요청을 처리하는 데 이러한 블록을 사용하지는 않습니다. 연결은 결국 시간 초과되고 블록은 해제됩니다.
  - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 새 풀이 작동하게 되는 동안 여전히 전환 중이던 xlate 백업 요청에 대해 xlate 백업 생성이 실패하게 됩니다. 이러한 동작은 포트 블록 할당 기능과 관련이 없으며, 풀이 분산되고 트래픽이 클러스터 유닛 전체에서 부하 분산되는 클러스터 구축 과정에서만 발생하는 일시적인 PAT 풀 문제입니다.
- 동적 PAT에 NAT 풀 주소 분산 — 마스터 유닛은 클러스터 전체에 걸쳐 주소를 사전에 균일하게 분산시킵니다. 멤버에 주소가 없는 연결이 전달된 경우 해당 연결이 끊어지며, 다른 멤버는 유효한 주소를 보유한 경우에도 마찬가지입니다. 각 유닛에 주소가 전달되도록 하려면 NAT 주소는 최소한 클러스터의 유닛에 있는 수만큼 추가해야 합니다. **show nat pool cluster** 명령을 사용하여 주소 할당을 확인합니다.
- 라운드 로빈 없음 — 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 마스터 유닛에 의해 관리되는 동적 NAT xlate — 마스터 유닛에서는 xlate 테이블을 유지하고 이를 슬레이브 유닛에 복제합니다. 동적 NAT가 필요한 연결이 슬레이브 유닛에 전달되고 xlate가 테이블에 없을 경우, 슬레이브 유닛에서는 마스터 유닛에서 xlate를 요청합니다. 슬레이브 유닛에서는 이 연결을 소유합니다.
- 세션당 PAT 기능 — 클러스터링에만 해당되는 것은 아니지만, 세션당 PAT 기능을 사용하면 PAT의 확장성이 개선되며 클러스터링을 수행할 때 각 슬레이브 유닛에서 고유한 PAT 연결을 소유할 수 있게 됩니다. 이와 달리 다중 세션 PAT 연결은 마스터 유닛에 전달해야 하며 마스터 유닛에서 해당 연결을 소유하게 됩니다. 기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽은 세션 단위 PAT xlate를 사용하며, 여기서 ICMP 및 기타 모든 UDP 트래픽은 멀티 세션을 사용합니다. TCP 및 UDP에 대해 이러한 기본값을 변경하도록 세션 단위 NAT 규칙을 구성할 수 있지만, ICMP에 대해서는 세션 단위 PAT를 구성할 수 없습니다. H.323, SIP, Skinny 등과 같이 다중 세션 PAT가 도움이 되는 트래픽의 경우 연결된 TCP 포트에 대해 세션 단위 PAT를 비활성화할 수 있습니다(이러한 H.323 및 SIP에 대한 UDP 포트는 기본적으로 이미 다중 세션임). 세션당 PAT에 대한 자세한 내용은 방화벽 설정 가이드를 참조하십시오.
- 다음을 검사할 수 있는 고정 PAT 없음

- FTP
- PPTP
- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

동적 라우팅 및 클러스터링

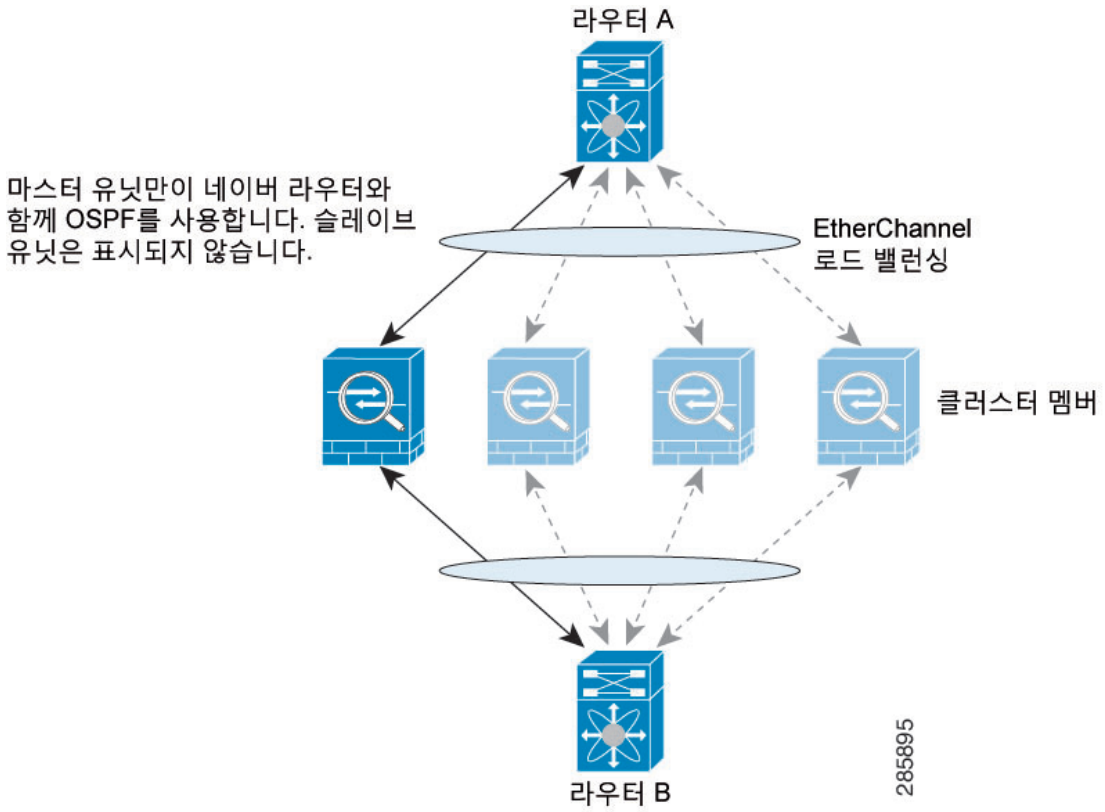
이 섹션에서는 클러스터링을 통해 동적 라우팅을 사용하는 방법에 대해 설명합니다.

Spanned EtherChannel 모드의 동적 라우팅

참고 IS-IS는 Spanned EtherChannel 모드에서 지원되지 않습니다.

스팬 EtherChannel 모드의 경우 라우팅 프로세스는 마스터 유닛에서만 실행되며, 마스터 유닛을 통해 경로가 파악되고 슬레이브에 복제됩니다. 라우팅 패킷이 슬레이브에 전송되면 해당 패킷은 마스터 유닛에 리디렉션됩니다.

그림 ***52: Spanned EtherChannel*** 모드의 동적 라우팅



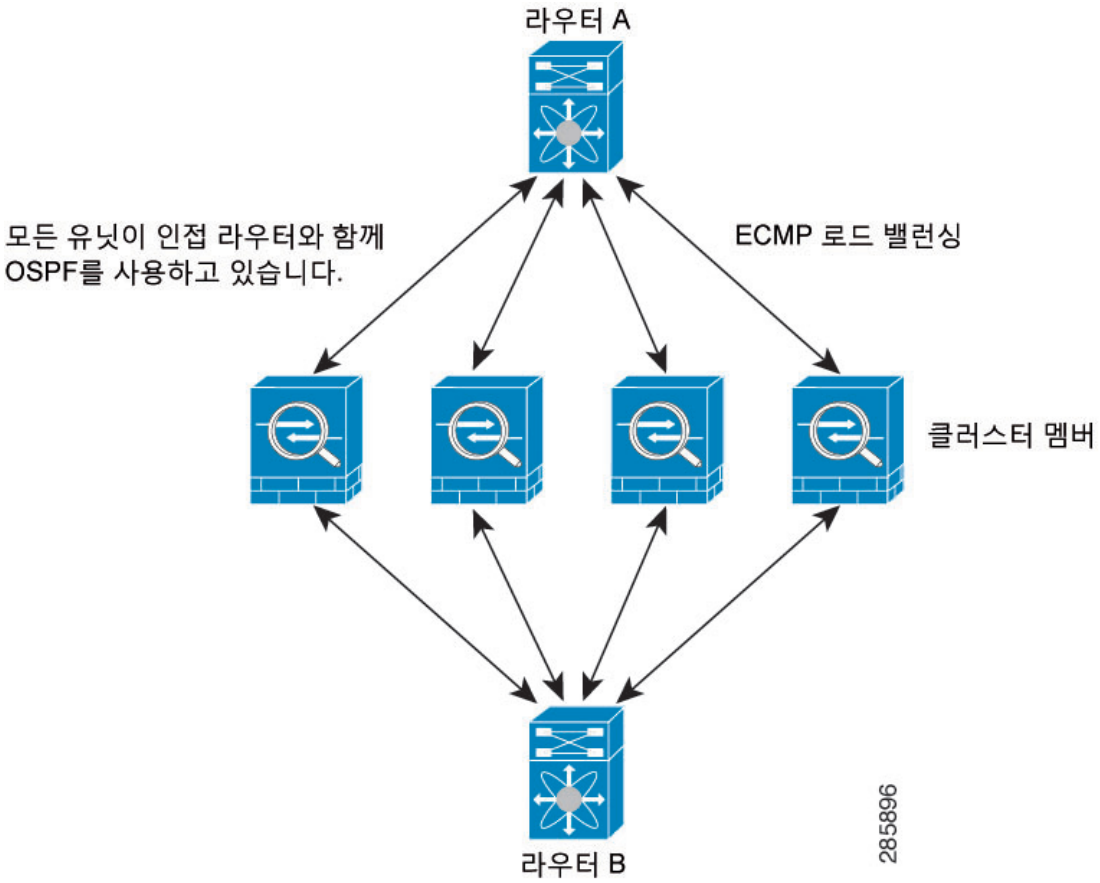
슬레이브 멤버가 마스터 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 마스터 유닛에서 슬레이브 유닛으로 동기화되지 않습니다. 마스터 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

개별 인터페이스 모드의 동적 라우팅

개별 인터페이스 모드의 경우 각 유닛에서는 라우팅 프로토콜을 독립형 라우터로 실행하며, 경로에 대한 정보 파악은 각 유닛에서 개별적으로 수행합니다.

그림 *53:* 개별 인터페이스 모드의 동적 라우팅



위 다이어그램에서 라우터 A는 라우터 B에 각각 ASA를 통한 4개의 Equal-Cost 경로가 있다는 정보를 파악합니다. ECMP는 4개 경로 간의 트래픽을 로드 밸런싱하는 데 사용됩니다. 각각의 ASA는 외부 라우터와 통신할 경우 다른 라우터 ID를 선택합니다.

라우터 ID에 대한 클러스터 풀을 구성하여 유닛마다 개별 라우터 ID를 보유하도록 해야 합니다.

EIGRP는 개별 인터페이스 모드에서 클러스터 피어와 네이버 관계를 형성하지 않습니다.

참고 클러스터가 이중화를 위해 동일한 라우터의 여러 위치에 인접하는 경우 비대칭 라우팅으로 인해 트래픽이 너무 많이 손실될 수 있습니다. 비대칭 라우팅을 피하려면 모든 ASA 인터페이스를 동일한 트래픽 영역으로 그룹화하십시오. 트래픽 영역 구성, 670 페이지을 참조하십시오.

SCTP 및 클러스터링

로드 밸런싱으로 인해 모든 유닛에서 SCTP 연결을 만들 수 있습니다. 멀티호밍 연결은 동일한 유닛에 있어야 합니다.

SIP 검사 및 클러스터링

로드 밸런싱으로 인해 모든 디바이스에서 제어 흐름을 만들 수 있지만 자식 데이터 흐름은 동일한 디바이스에 상주해야 합니다.

TLS 프록시 구성은 지원되지 않습니다.

SNMP 및 클러스터링

SNMP 에이전트에서는 로컬 IP 주소로 각각의 개별 ASA를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 마스터가 선택된 경우, 새 마스터 유닛에 대한 폴링이 이루어지지 않습니다.

STUN 및 클러스터링

STUN 검사는 핀홀이 복제될 때 장애 조치 및 클러스터 모드에서 지원됩니다. 그러나 트랜잭션 ID는 유닛 간에 복제되지 않습니다. STUN Request를 수신한 후 유닛이 실패하고 다른 유닛이 STUN Response를 수신한 경우, STUN Response는 삭제됩니다.

Syslog와 NetFlow 및 클러스터링

- Syslog - 클러스터의 각 유닛에서는 고유한 syslog 메시지를 생성합니다. 각 유닛에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 구성은 클러스터의 모든 유닛에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 유닛에서는 단일 유닛에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 구성에 할당된 로컬-유닛 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, syslog 메시지는 다른 유닛에서 생성된 것처럼 보입니다.
- NetFlow — 클러스터의 각 유닛에는 고유한 NetFlow 스트림이 있습니다. NetFlow 컬렉터에서는 각각의 ASA를 별도의 NetFlow 내보내기 장치로만 처리할 수 있습니다.

Cisco TrustSec 및 클러스터링

마스터 유닛에서만 SGT(security group tag) 정보를 파악합니다. 그런 다음 마스터 유닛에서는 SGT를 슬레이브에 제공하며, 슬레이브에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

VPN 및 클러스터링

사이트 대 사이트 VPN은 중앙 집중식 기능이며, 마스터 유닛에서만 VPN 연결을 지원합니다.

참고 원격 액세스 VPN은 클러스터링으로 지원되지 않습니다.

VPN 기능은 마스터 유닛에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 마스터 유닛에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 마스터가 선택되면 VPN 연결을 다시 설정해야 합니다.

VPN 터널을 스팬 EtherChannel 주소에 연결할 경우 연결이 마스터 유닛에 자동으로 전달됩니다. PBR 또는 ECMP를 사용할 경우 개별 인터페이스에 연결하려면 항상 로컬 주소가 아닌 기본 클러스터 IP 주소에 연결해야 합니다.

VPN 관련 키 및 인증서는 모든 유닛에 복제됩니다.

ASA 클러스터링용 라이선스

클러스터 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 일반적으로 마스터 유닛에만 라이센스를 구매하며, 슬레이브 유닛에서는 마스터 라이센스를 상속합니다. 여러 유닛에 라이센스가 있는 경우, 해당 라이센스는 단일하게 실행되는 ASA 클러스터 라이센스로 통합됩니다.

이 규칙에는 예외가 있습니다. 클러스터링에 대한 올바른 라이센스 요건은 다음 표를 참조하십시오.

모델	라이센스 요건
ASA 5585-X	클러스터 라이센스, 최대 16개까지 지원. 참고 각 유닛에 동일한 암호화 라이센스가 있어야 합니다. 각 유닛에 동일한 10개의 GE I/O/Security Plus 라이센스(SSP-10 및 -20이 포함된 ASA 5585-X)가 있어야 합니다.
ASA 5516-X	Base 라이선스, 유닛 2개 지원. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
ASA 5512-X	Security Plus 라이센스, 유닛 2개 지원. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Base 라이센스, 유닛 2개 지원. 참고 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
ASA Firepower 4100/9300 섀시	ASA의 ASA 클러스터 라이선스 - Firepower 4100/9300 섀시, 127 페이지을 참조하십시오.
다른 모든 모델	지원 안 함

ASA 클러스터링의 요구 사항 및 사전 요구 사항

모델 요구 사항

- ASA 5516-X — 최대 2개의 유닛
- ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X — 최대 2개의 유닛
- ASA 5585-X — 최대 16개의 유닛

  10기가비트 이더넷 인터페이스 2개가 내장된 SSP-10 및 SSP-20이 포함된 ASA 5585-X의 경우, 클러스터 제어 링크에는 하나의 인스턴스를 사용하고 데이터에는 나머지를 사용하는 것이 좋습니다. 이러한 설치 과정에서는 클러스터 제어 링크의 이중화를 수용하지 않으나, 클러스터 제어 링크의 크기를 데이터 인터페이스의 크기와 일치시켜야 하는 요구 사항은 충족합니다.

- ASA FirePOWER 모듈 — ASA FirePOWER 모듈에서 클러스터링을 직접 지원하지는 않지만 클러스터에서 이러한 모듈을 사용할 수 있습니다. 클러스터의 ASA FirePOWER 모듈에 대해 일관된 정책을 유지 관리해야 합니다.

  참고 ASA FirePOWER 모듈을 구성하기 전에 클러스터를 생성합니다. 모듈이 슬레이브 디바이스에서 이미 구성된 경우, 이러한 모듈을 클러스터에 추가하기 전에 디바이스에서 인터페이스 구성을 지웁니다. CLI에서 **clear configure interface** 명령을 입력합니다.

ASA 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 유닛은 다음과 같아야 합니다.

- 동일한 DRAM과 같은 모델이어야 합니다. 플래시 메모리는 동일하지 않아도 됩니다.
- 이미지 업그레이드 시간을 제외하고는 동일한 소프트웨어를 실행해야 합니다. 무중단 업그레이드가 지원됩니다.
- 동일한 보안 상황 모드(단일 또는 다중)에 있어야 합니다.
- (단일 상황 모드) 동일한 방화벽 모드(라우팅 또는 투명 모드)여야 합니다.
- 새 클러스터 멤버는 컨피그레이션을 복제하기 전에 맨 처음 클러스터 제어 링크 통신을 수행할 경우 마스터 유닛과 동일한 SSL 암호화 설정(**ssl encryption** 명령)을 사용해야 합니다.
- 클러스터, 암호화 그리고 ASA 5585-X의 경우 10GE I/O 라이센스가 동일해야 합니다.

스위치 요구 사항

- ASA에서 클러스터링을 구성하기 전에 스위치 구성을 완료해야 합니다.
- 지원되는 스위치 목록의 경우, Cisco ASA 호환성을 참조하십시오.

ASA 요구 사항

- 각 유닛이 관리 네트워크에 참가하기 전에 각 유닛에 고유한 IP 주소를 제공해야 합니다.
  - ASA에 연결하고 관리 IP 주소를 설정하는 방법에 대한 자세한 내용은 시작하기 장을 참조하십시오.
  - 마스터 유닛(일반적으로 클러스터에 추가하는 첫 번째 유닛)에서 사용하는 IP 주소를 제외하고, 이러한 관리 IP 주소는 일시적으로만 사용됩니다.
  - 슬레이브가 클러스터에 참가하면 관리 인터페이스 컨피그레이션이 마스터 유닛에서 복제된 컨피그레이션으로 교체됩니다.
- 클러스터 제어 링크에 점보 프레임을 사용하려면(권장), 클러스터링을 사용하기 전에 점보 프레임 예약(Jumbo Frame Reservation)을 사용하도록 설정해야 합니다.

사이트 간 클러스터링을 위한 **Data Center Interconnect** 크기 조정

클러스터 제어 링크 트래픽을 처리하기 위한 DCI(data center interconnect) 대역폭을 다음 계산과 같이 예약해야 합니다.

$$\frac{\text{사이트당 클러스터 멤버의 수}}{2} \times \text{멤버당 클러스터 제어 링크 크기}$$

각 사이트의 멤버 수가 다를 경우, 더 큰 숫자를 계산에 사용합니다. DCI의 최소 대역폭은 한 멤버에 대한 클러스터 제어 링크의 크기보다 작으면 안 됩니다.

예를 들면 다음과 같습니다.

- 2개 사이트에 멤버가 4개인 경우:
  - 총 클러스터 멤버 4개
  - 각 사이트당 멤버 2개
  - 멤버당 5Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 5Gbps(2/2 x 5Gbps)
- 3개 사이트에 멤버가 6개인 경우 크기가 다음과 같이 증가함:
  - 총 클러스터 멤버 6개
  - 사이트 1에 멤버 3개, 사이트 2에 멤버 2개, 사이트 3에 멤버 1개
  - 멤버당 10Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 15Gbps(3/2 x 10Gbps)
- 2개 사이트에 멤버가 2개인 경우:
  - 총 클러스터 멤버 2개
  - 사이트당 멤버 1개

- 멤버당 10Gbps 클러스터 제어 링크

예약된 DCI 대역폭 = 10Gbps(1/2 x 10Gbps = 5Gbps). 그러나 최소 대역폭은 클러스터 제어 링크의 크기(10Gbps)보다 작으면 안 됩니다.

기타 요구 사항

모든 클러스터 멤버 유닛 콘솔 포트에 액세스하려면 터미널 서버를 사용하는 것이 좋습니다. 초기 설치 및 지속적인 관리(예: 유닛이 중지될 경우)를 위해서는 터미널 서버를 사용하는 것이 원격 관리에 유용합니다.

ASA 클러스터링 지침

상황 모드

모드는 각 멤버 유닛과 일치해야 합니다.

방화벽 모드

단일 모드의 경우 방화벽 모드는 모든 유닛과 일치해야 합니다.

페일오버

클러스터링에서는 장애 조치가 지원되지 않습니다.

IPv6

클러스터 제어 링크는 IPv4를 사용하는 경우에만 지원됩니다.

스위치

- ASR 9006의 경우 기본이 아닌 MTU를 설정하려면 ASR 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면, **mtu-ignore** 옵션을 사용하지 않는 경우 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 ASR *IPv4* MTU와 일치해야 합니다.
- 클러스터 제어 링크 인터페이스용 스위치의 경우, 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP를 지원하지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조).

로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 디바이스에 트래픽이 균일하지 않게 분산될 수 있습니다. 클러스터 디바이스에서 로드 밸런싱 알고리즘의 기본값을 변경하지 마십시오.

- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 비활성화하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 클러스터 제어 링크 경로의 스위치에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다.
- Supervisor 2T EtherChannel에서 기본 해시 분산 알고리즘은 적응형입니다. VSS 설계에서 비대칭 트래픽을 방지하려면 클러스터 디바이스에 연결된 포트 채널의 해시 알고리즘을 다음과 같이 변경하여 수정합니다.

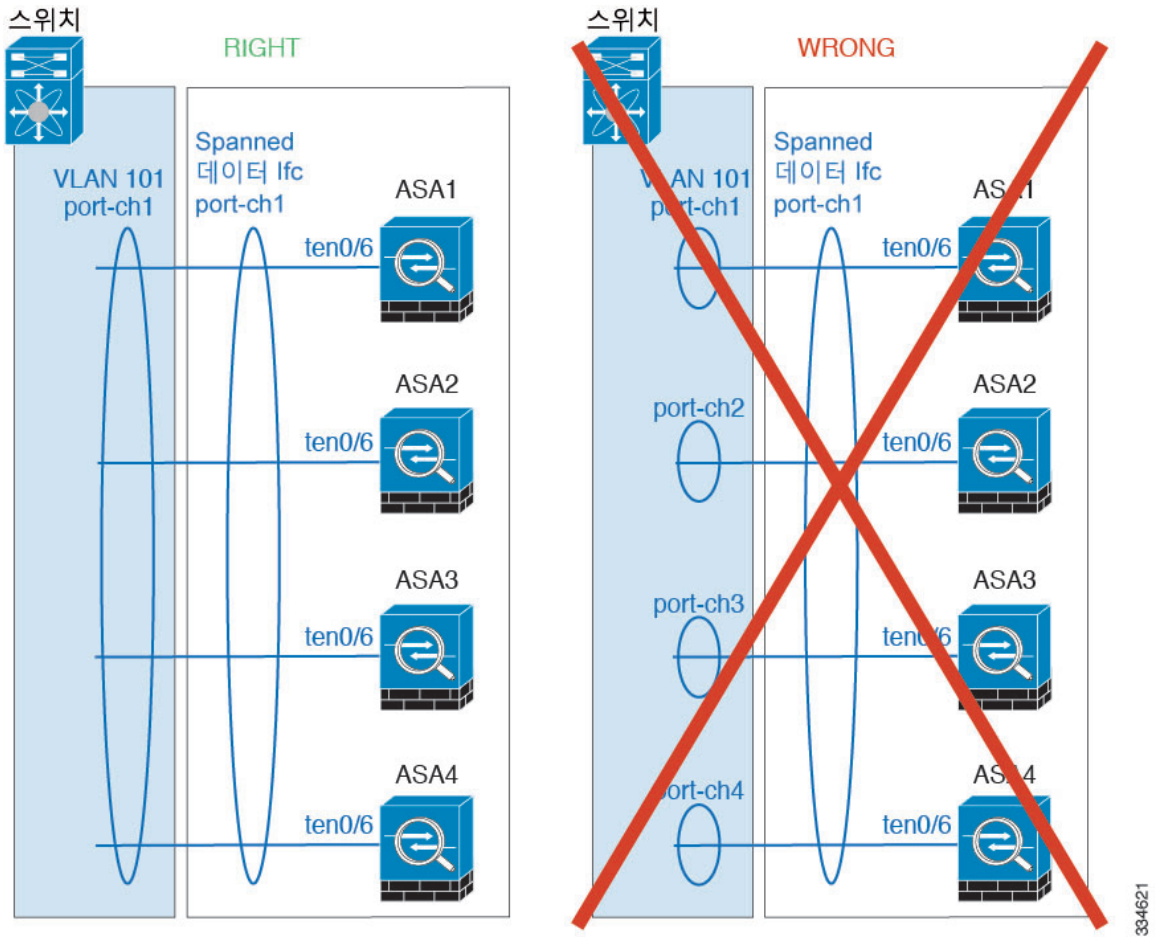
  router(config) # **port-channel** *id* **hash-distribution fixed**

  VSS 피어 링크의 적응형 알고리즘을 활용할 때가 있을 수 있으므로 알고리즘을 전역으로 변경하지 마십시오.

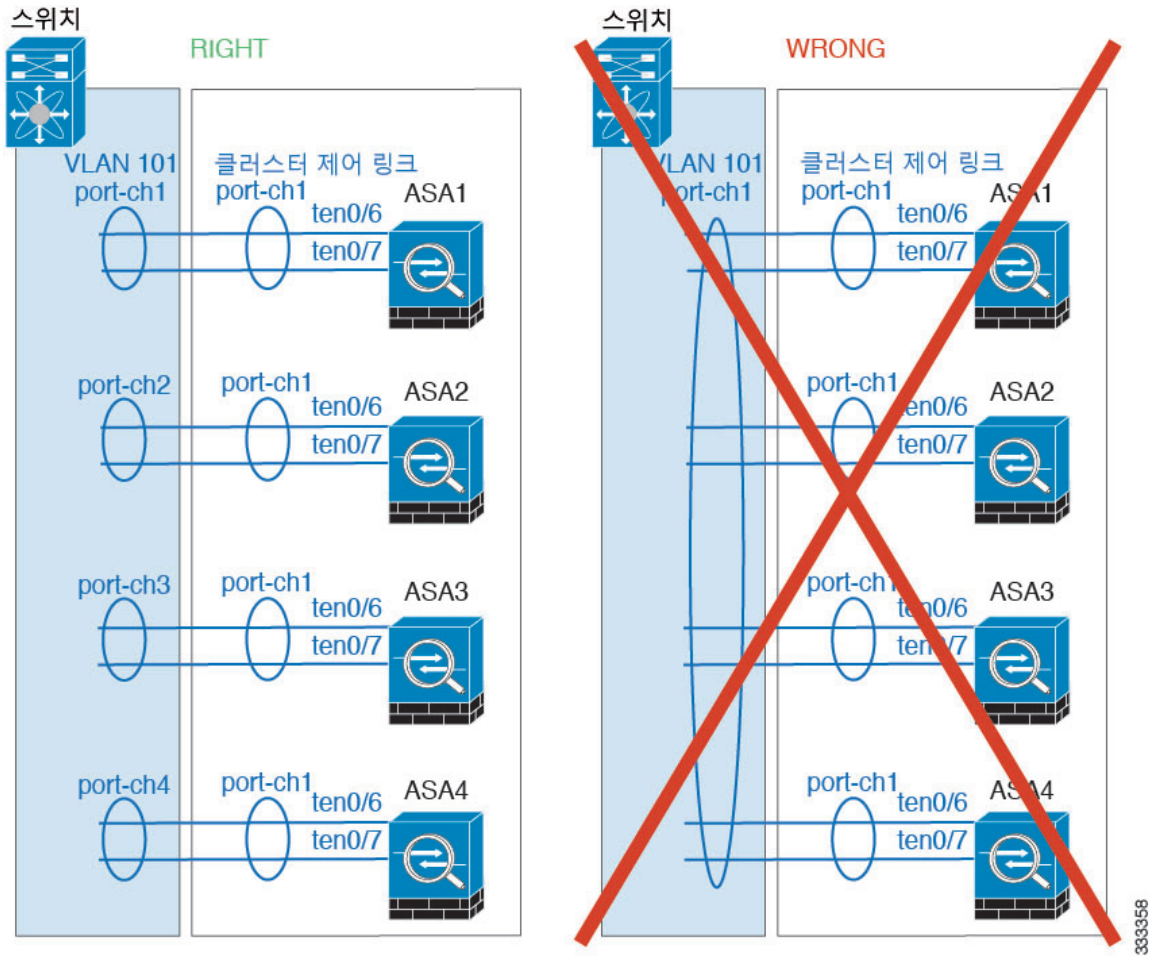
- Cisco Nexus 스위치의 경우 모든 클러스터용 EtherChannel 인터페이스에서 LACP Graceful Convergence 기능을 사용하지 않도록 설정해야 합니다.

EtherChannel

- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.
- Spanned EtherChannel 구성과 디바이스-로컬 EtherChannel 구성 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에서 각각 알맞게 스위치를 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 *Spanned* EtherChannels의 경우, 인터페이스가 스위치의 단일 EtherChannel에 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



- 디바이스-로컬 EtherChannel - 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 클러스터 유닛 디바이스-로컬 EtherChannel의 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 클러스터 유닛 EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



사이트 간 지침

사이트 간 클러스터링에 대한 다음 지침을 참조하십시오.

- 다음과 같은 인터페이스 및 방화벽 모드에서는 사이트 간 클러스터링을 지원합니다.

인터페이스 모드	방화벽 모드	
	라우팅됨	투명
개별 인터페이스	예	해당 없음
스팬 EtherChannel	예	예

- 개별 인터페이스 모드의 경우 멀티캐스트 RP(Rendezvous Point)를 향해 ECMP를 사용할 때 기본 클러스터 IP 주소를 next hop으로 사용하는 RP IP 주소에 대한 고정 경로를 사용하는 것이 좋습니다. 이 고정 경로는 유니캐스트 PIM 등록 패킷이 슬레이브 유닛으로 전송되는 것을 방지합니다. 슬레이브 유닛이 PIM 등록 패킷을 수신한 다음 이 패킷이 삭제되는 경우, 멀티캐스트 스트림을 등록할 수 없습니다.

- 클러스터 제어 링크 레이턴시는 RTT(왕복 시간)가 20ms 이하여야 합니다.
- 클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 전용 링크를 사용해야 합니다.
- 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 연결이 리밸런싱됩니다.
- 클러스터를 구현할 경우 들어오는 연결에 대한 여러 사이트에 있는 멤버가 구분되지 않습니다. 따라서 하나의 특정한 연결의 연결 역할은 사이트 전체를 포괄하게 될 수 있습니다. 이는 정상적인 동작입니다. 그러나 관리자 지역화를 활성화하는 경우 항상 연결 소유자와 동일한 사이트에서 로컬 관리자 역할이 선택됩니다(사이트 ID에 따라). 원래 소유자가 실패하면 로컬 관리자는 동일한 사이트에서 새 소유자를 선택합니다. (참고: 트래픽이 사이트 간에 비동기 상태이고 원래 소유자가 실패한 이후 원격 사이트로부터 계속해서 트래픽이 발생하면, 원격 사이트의 유닛이 재호스팅 기간 내에 데이터 패킷을 수신하는 경우 새로운 소유자가 될 수 있습니다.)
- 관리자 지역화의 경우 NAT 또는 PAT 트래픽, SCTP에서 검사된 트래픽, 단편화 소유자 쿼리 등의 트래픽 유형은 지역화를 지원하지 않습니다.
- 투명 모드에서, 클러스터가 내부 및 외부 라우터(north-south 삽입이라고도 함) 쌍 사이에 위치하면 내부 라우터 모두에서 MAC 주소를 공유해야 하며 외부 라우터 모두에서도 MAC 주소를 공유해야 합니다. 사이트 1의 클러스터 멤버가 사이트 2의 멤버에 연결을 전달할 경우, 목적지 MAC 주소가 유지됩니다. MAC 주소가 사이트 1의 라우터와 동일할 경우 패킷은 사이트 2의 라우터에만 도달합니다.
- 투명 모드에서 클러스터가 내부 네트워크(East-West 삽입이라고 함) 사이에서 방화벽을 위해 각 사이트에서 데이터 네트워크 및 게이트웨이 라우터 사이에 위치하면 각 게이트웨이 라우터는 HSRP와 같은 첫 번째 홉 이중화 프로토콜(FHRP)을 사용하여 각 사이트에서 동일한 가상 IP 및 MAC 주소 대상을 제공해야 합니다. 데이터 VLAN은 OTV(오버레이 전송 가상화) 또는 유사한 기능을 사용하는 사이트 전체로 확장됩니다. DCI를 통해 다른 사이트로 전송 중인 로컬 게이트웨이 라우터에 예약된 트래픽을 방지하려면 필터를 생성해야 합니다. 게이트웨이 라우터가 1개의 사이트에 연결할 수 없게 되면, 모든 필터를 제거해야 트래픽이 성공적으로 다른 사이트의 게이트웨이에 연결할 수 있습니다.
- Spanned EtherChannel을 사용하는 라우팅 모드의 경우 사이트별 MAC 주소를 구성하십시오. OTV 또는 유사한 것을 사용하여 사이트 전체로 데이터 VLAN을 확장하십시오. 전역 MAC 주소로 향하는 트래픽이 DCI를 통해 다른 사이트에 가지 않도록 필터를 생성해야 합니다. 어떤 사이트에서 클러스터가 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 유닛에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. 사이트 간 클러스터가 확장 세그먼트의 FHR(First Hop Router)로 작동하는 경우에는 동적 라우팅이 지원되지 않습니다.

추가 지침

- 중요한 토폴로지 변경 사항(예: EtherChannel 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 구성 변경 사항이 모든 유닛과 동기화되면 인터페이스 상태 검사 기능을 다시 활성화할 수 있습니다.

- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel에 연결된 Windows 2003 Server를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않으며, 이렇게 되면 대량의 ICMP 메시지가 ASA 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 ASA 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능이 영향을 받을 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.
- 개별 인터페이스 모드에서 VXLAN을 지원하지 않습니다. 스팬 EtherChannel 모드만 VXLAN을 지원합니다.
- Spanned EtherChannel 모드에서는 IS-IS가 지원되지 않습니다. 개별 인터페이스 모드만 IS-IS를 지원합니다.

ASA 클러스터의 기본값

- 스팬 EtherChannel을 사용할 경우, cLACP 시스템 ID가 자동 생성되며 시스템 우선순위는 기본적으로 1입니다.
- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 장애가 발생한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도됩니다.
- 장애가 발생한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도됩니다.
- 연결 리밸런싱은 기본적으로 비활성화되어 있습니다. 연결 리밸런싱을 활성화할 경우 로드 정보를 교환하는 데 걸리는 기본 시간은 5초입니다.
- 5초의 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

ASA 클러스터링 구성

클러스터링을 구성하려면 다음 작업을 수행합니다.

참고 클러스터링을 활성화하거나 비활성화하려면 콘솔 연결(CLI용) 또는 ASDM 연결을 사용해야 합니다.

유닛 케이블 연결 및 인터페이스 구성

클러스터링을 구성하기 전에 클러스터 제어 링크 네트워크, 관리 네트워크, 데이터 네트워크의 케이블을 연결합니다. 그런 다음 인터페이스를 구성합니다.

클러스터 인터페이스 정보

데이터 인터페이스를 스팬 EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 클러스터의 모든 데이터 인터페이스는 1가지 유형만 가능합니다. 또한 각 유닛에서는 최소 1개의 하드웨어 인터페이스를 클러스터 제어 링크로 지정해야 합니다.

클러스터 제어 링크 정보

각 유닛에서는 최소 1개의 하드웨어 인터페이스를 클러스터 제어 링크로 지정해야 합니다.

클러스터 제어 링크 트래픽 개요

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 마스터 선택
- 구성 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

클러스터 제어 링크 인터페이스 및 네트워크

클러스터 제어 링크에는 모든 데이터 인터페이스를 사용할 수 있으나 다음 경우는 제외입니다.

- VLAN 하위 인터페이스는 클러스터 제어 링크로 사용할 수 없습니다.
- 관리 *x/x* 인터페이스는 단독으로든 EtherChannel로든 클러스터 제어 링크로 사용할 수 없습니다.
- ASA FirePOWER 모듈을 사용하는 ASA 5585-X의 경우 ASA FirePOWER 모듈의 인터페이스가 아닌 클러스터 제어 링크의 ASA 인터페이스를 사용하는 것이 좋습니다. 모듈 인터페이스에서는 소프트웨어 업그레이드 중 다시 로드하게 되는 경우 등 모듈을 다시 로드하는 경우에 최대 30초 동안 트래픽을 삭제할 수 있습니다. 그러나, 필요한 경우 모듈 인터페이스와 ASA 인터페이스를 동일한 클러스터 제어 링크 EtherChannel에서 사용할 수 있습니다. 모듈 인터페이스가 삭제되는 경우, EtherChannel의 나머지 인터페이스는 여전히 작동합니다. ASA 5585-X 네트워크 모듈은 별도의 운영 체제를 실행하지 않으므로 이 문제의 영향을 받지 않습니다.

  모듈의 데이터 인터페이스도 다시 로드하는 것으로 인한 삭제의 영향을 받는다는 점에 유의하십시오. 항상 ASA 인터페이스를 EtherChannel의 모듈 인터페이스와 함께 중복으로 사용하는 것이 좋습니다.

10기가비트 이더넷 인터페이스 2개가 내장된 SSP-10 및 SSP-20이 포함된 ASA 5585-X의 경우, 클러스터 제어 링크에는 하나의 인스턴스를 사용하고 데이터에는 나머지를 사용하는 것이 좋습니다. 이러한 설치 과정에서는 클러스터 제어 링크의 이중화를 수용하지 않으나, 클러스터 제어 링크의 크기를 데이터 인터페이스의 크기와 일치시켜야 하는 요구 사항은 충족합니다.

EtherChannel 또는 이중 인터페이스를 사용할 수 있습니다.

각 클러스터 제어 링크는 동일한 서브넷에 IP 주소가 있습니다. 이 서브넷은 모든 다른 트래픽과 분리되어 있어야 하며, ASA 클러스터 제어 링크 인터페이스만 포함해야 합니다.

2-멤버 클러스터의 경우 클러스터 제어 링크를 한 ASA에서 다른 ASA로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

을 위한 클러스터 제어 링크 크기 조정

가능한 경우, 각 섀시의 예상 처리량에 맞게 클러스터 제어 링크의 크기를 조정하여 클러스터 제어 링크가 최악의 시나리오를 처리할 수 있게 해야 합니다. 예를 들어, 클러스터에 있는 유닛당 최대 14Gbps를 전달할 수 있는 ASA 5585-X(SSP-60 포함)를 보유한 경우, 최소 14Gbps를 전달할 수 있는 클러스터 제어 링크에 대한 인터페이스 또한 할당해야 합니다. 이 경우 클러스터 제어 링크의 EtherChannel에 10기가비트 이더넷 인터페이스 2개를 사용할 수 있으며, 데이터 링크에 필요한 경우 나머지 인터페이스를 사용합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예를 들면 다음과 같습니다.

- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.
- 네트워크 액세스용 AAA는 중앙 집중식 기능이므로 모든 트래픽이 마스터 유닛으로 전달됩니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

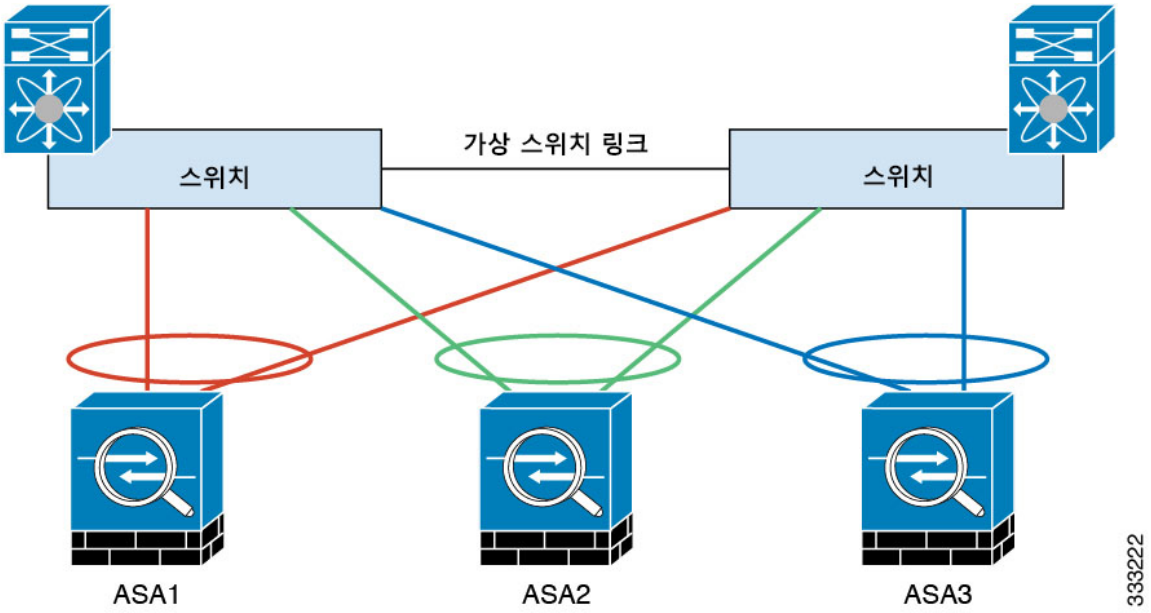
대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

을 위한 클러스터 제어 링크 이중화

클러스터 제어 링크에는 EtherChannel을 사용하는 편이 바람직하며, 이렇게 할 경우 EtherChannel 내의 여러 링크에 트래픽을 전달하는 동시에 이중화를 실현할 수 있습니다.

다음 다이어그램에는 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel) 환경에서 EtherChannel을 클러스터 제어 링크로 사용하는 방법이 나와 있습니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 VSS 또는 vPC의 일부일 경우 동일한 EtherChannel 내에 있는 ASA 인터페이스를 연결하여 VSS 또는 vPC의 스위치를 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스팬 EtherChannel입니다.



을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(round-trip time)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

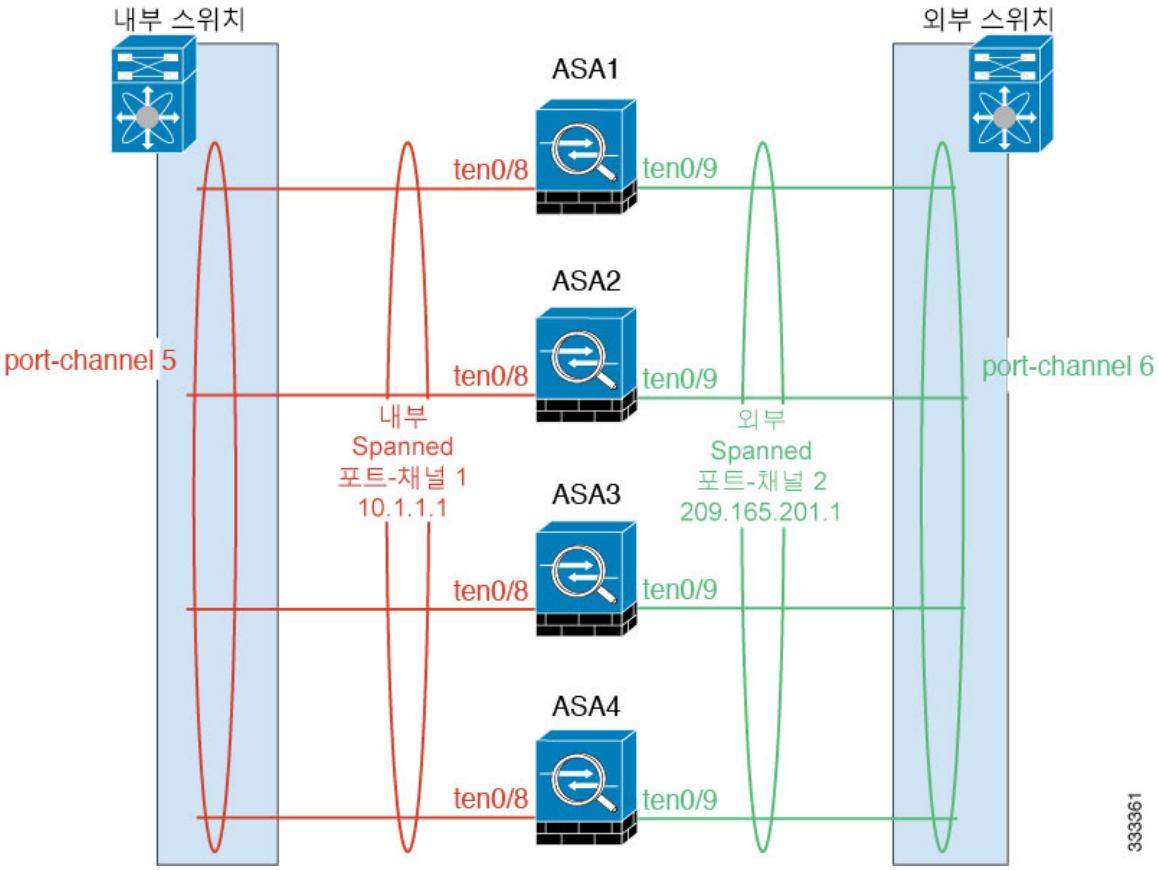
클러스터 제어 링크 오류

유닛의 클러스터 제어 링크 라인 프로토콜이 작동되지 않을 경우, 클러스터링을 사용할 수 없게 되며 데이터 인터페이스가 종료됩니다. 클러스터 제어 링크를 해결한 후 클러스터링을 다시 사용하도록 설정하여 클러스터에 수동으로 다시 참가해야 합니다.

참고 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드한 후에도 유닛이 클러스터 내에서 비활성 상태일 경우, 관리 인터페이스에서는 마스터 유닛과 동일한 기본 IP 주소를 사용하므로 관리 인터페이스에 액세스할 수 없습니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

Spanned EtherChannels(권장)

섀시당 하나 이상의 인터페이스를 클러스터 내의 모든 섀시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 스팬 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스가 아닌 BVI에 IP 주소가 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.



스팬 *EtherChannel* 이점

EtherChannel 로드 밸런싱 방식을 다른 방법보다 권장하는 이유는 다음과 같은 이점 때문입니다.

- 신속한 오류 발견
- 빠른 통합 시간 개별 인터페이스에서는 라우팅 프로토콜을 기반으로 트래픽의 로드 밸런싱을 수행하며, 라우팅 프로토콜은 링크 오류 발생 시 통합 속도가 느려지는 경우가 많습니다.
- 컨피그레이션의 용이성

최대 처리량에 대한 지침

최대 처리량을 달성하기 위해서는 다음 사항을 권장합니다.

- "대칭"을 이루는 로드 밸런싱 해시 알고리즘을 사용합니다. 이는 즉, 양방향의 패킷의 해시가 동일하며 패킷이 Spanned EtherChannel 내의 동일한 ASA로 전송됨을 의미합니다. 소스와 목적지 IP 주소(기본값) 또는 소스와 목적지 포트를 해싱 알고리즘으로 사용하는 것이 좋습니다.
- ASA를 스위치에 연결할 경우 동일한 유형의 라인 카드를 사용하여 모든 패킷에 동일한 해싱 알고리즘이 적용되도록 합니다.

부하 균형

소스 또는 목적지 IP 주소 및 TCP, UDP 포트 번호를 기준으로 전용 해시 알고리즘을 사용하여 EtherChannel 링크를 선택합니다.

참고 ASA에서는 로드 밸런싱 알고리즘을 기본값에서 변경하지 마십시오. 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 또는 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 ASA에 트래픽이 균일하지 않게 분산될 수 있습니다.

EtherChannel의 링크 수는 로드 밸런싱에 영향을 미칩니다.

경우에 따라 대칭 로드 밸런싱이 가능하지 않을 수 있습니다. NAT를 구성할 경우, 전달 및 반환 패킷의 IP 주소 및/또는 포트는 서로 다릅니다. 반환 트래픽은 해시에 따라 서로 다른 유닛에 전송되며, 클러스터에서는 가장 많이 반환되는 트래픽을 현재 유닛에 리디렉션하게 됩니다.

EtherChannel 이중화

EtherChannel에는 이중화 기능이 내장되어 있으며, 모든 링크의 라인 프로토콜 상태를 모니터링합니다. 링크 하나에 오류가 발생하면 나머지 링크 간의 트래픽이 리밸런싱됩니다. 특정 유닛에서 EtherChannel의 모든 링크에 오류가 발생했으나 다른 유닛은 아직 가동 중인 경우, 클러스터에서 특정 유닛이 제거됩니다.

VSS 또는 *vPC*에 연결

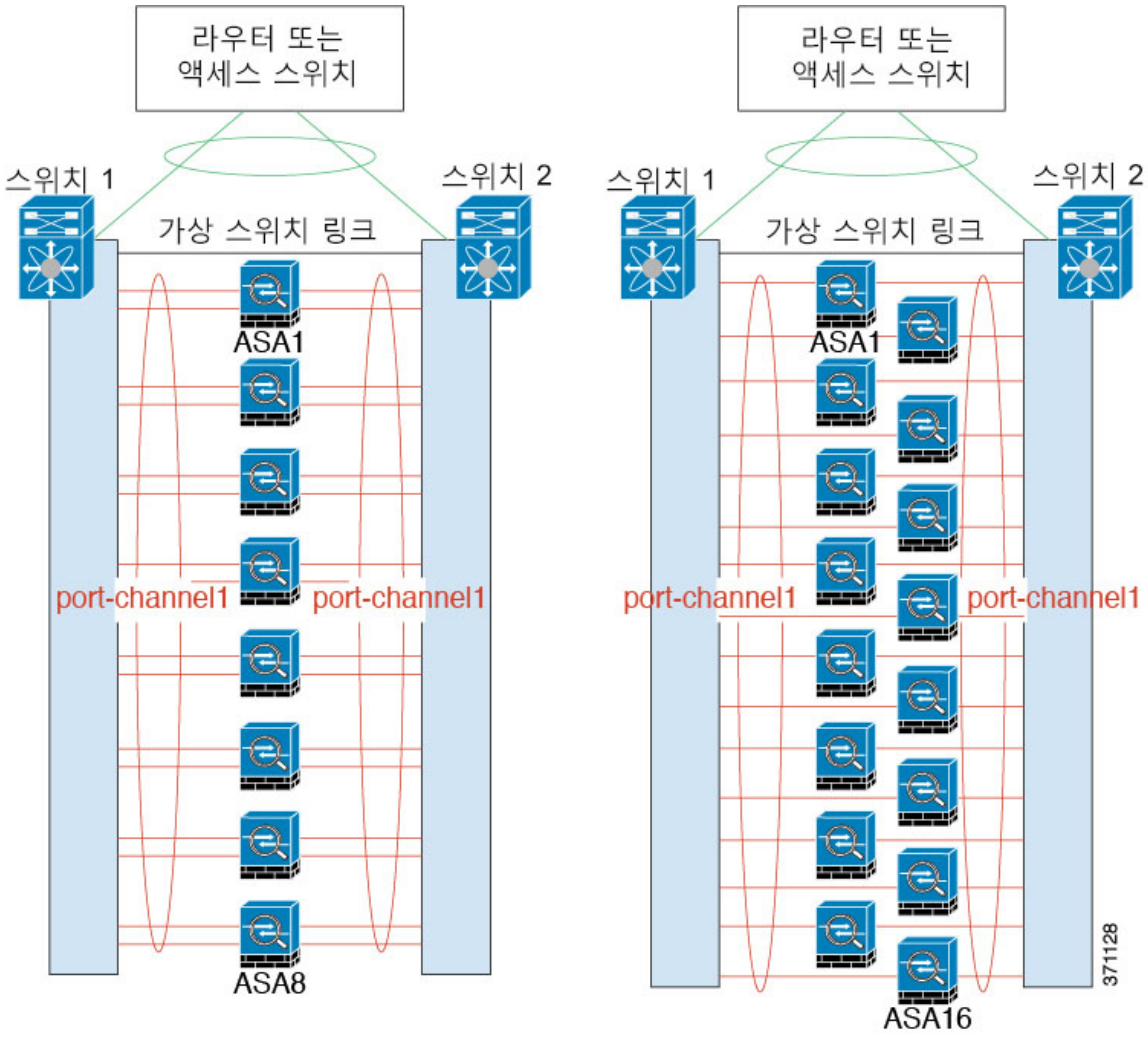
Spanned EtherChannel에서 ASA당 여러 인터페이스를 포함할 수 있습니다. ASA당 여러 인터페이스를 포함하는 것은 VSS 또는 vPC에서 두 스위치에 모두 연결하는 경우에 특히 유용합니다.

스위치에 따라 스팬 EtherChannel에서 활성 링크를 최대 32개까지 구성할 수 있습니다. 이 기능을 사용하려면 각각 16개의 활성 링크가 포함된 EtherChannel(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000)을 지원하는 vPC의 두 스위치가 필요합니다.

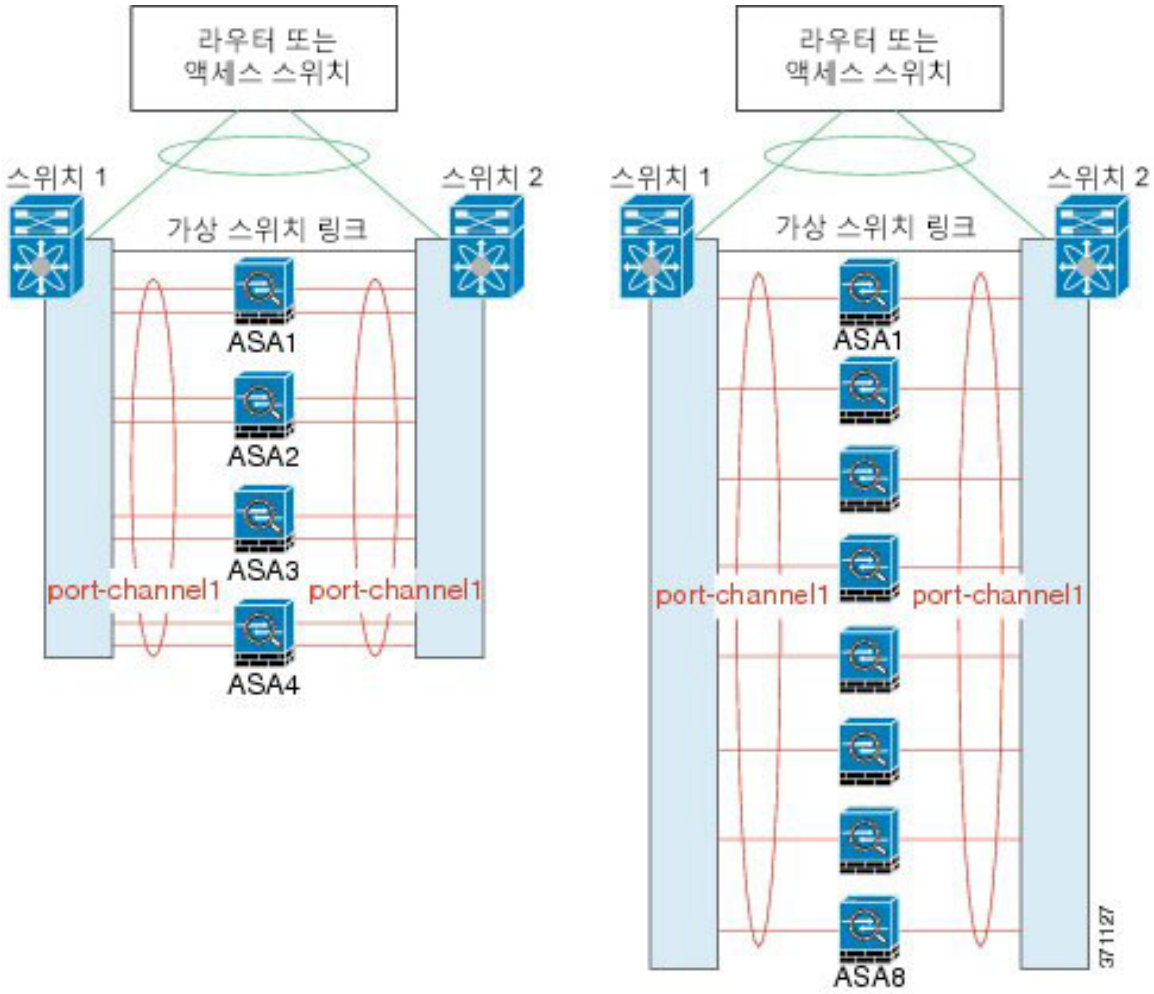
EtherChannel에서 8개의 활성 링크를 지원하는 스위치를 사용하려면, VSS/vPC에서 2개의 스위치에 연결할 때 스팬 EtherChannel에 최대 16개의 활성 링크를 구성하면 됩니다.

스팬 EtherChannel에서 활성 링크를 8개 이상 사용하려는 경우 스탠바이 링크까지 보유할 수는 없습니다. 활성 링크를 9~32개까지 지원하려면 스탠바이 링크의 사용을 허용하는 cLACP 동적 포트 우선순위를 비활성화해야 합니다. 단일 스위치에 연결하는 경우와 같이, 필요한 경우에는 활성 링크 8개와 스탠바이 링크 8개를 계속 사용할 수 있습니다.

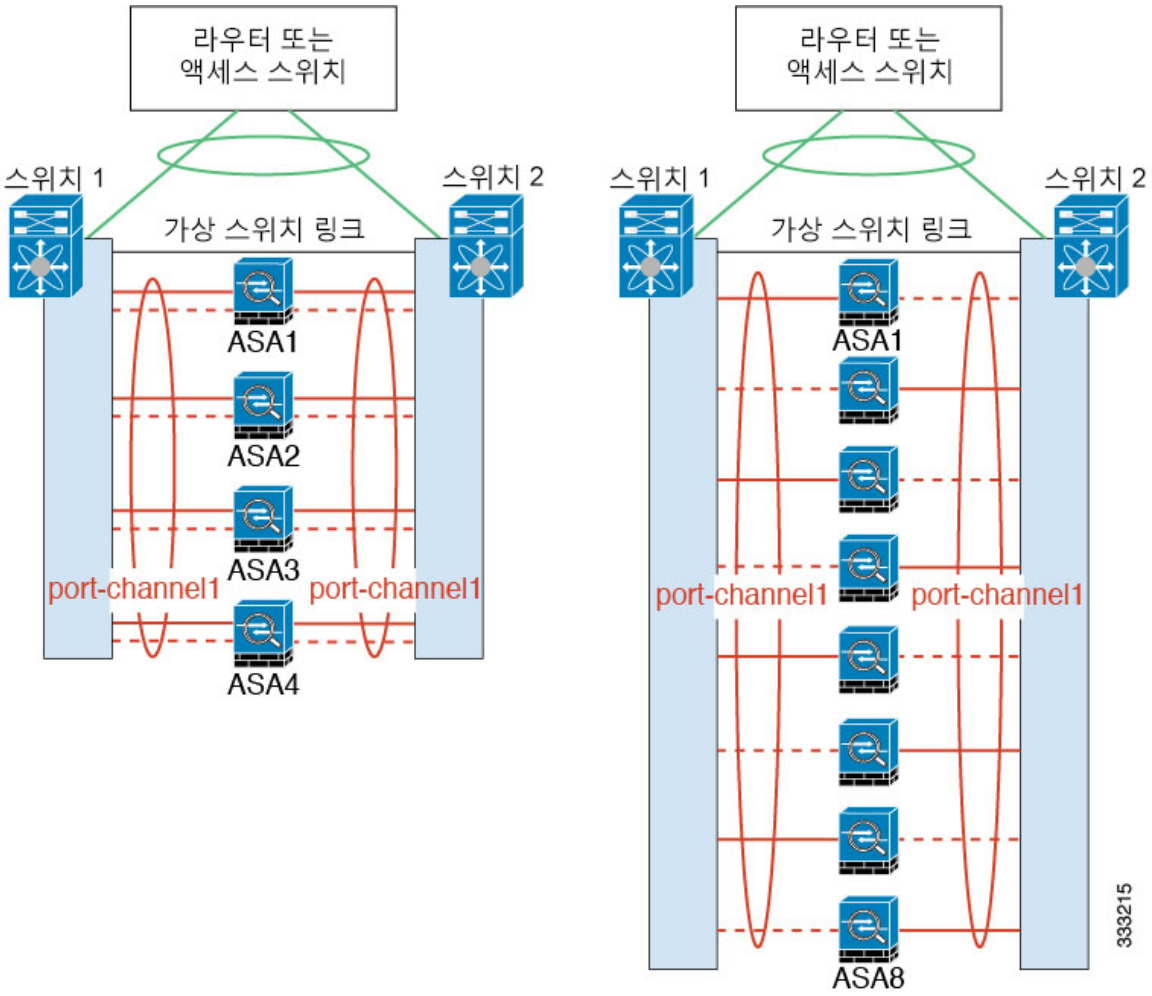
다음 그림에는 8-ASA 클러스터 및 16-ASA 클러스터의 32개 액티브 링크 Spanned EtherChannel이 나와 있습니다.



다음 그림에는 4-ASA 클러스터 및 8-ASA 클러스터의 16개 액티브 링크 Spanned EtherChannel이 나와 있습니다.



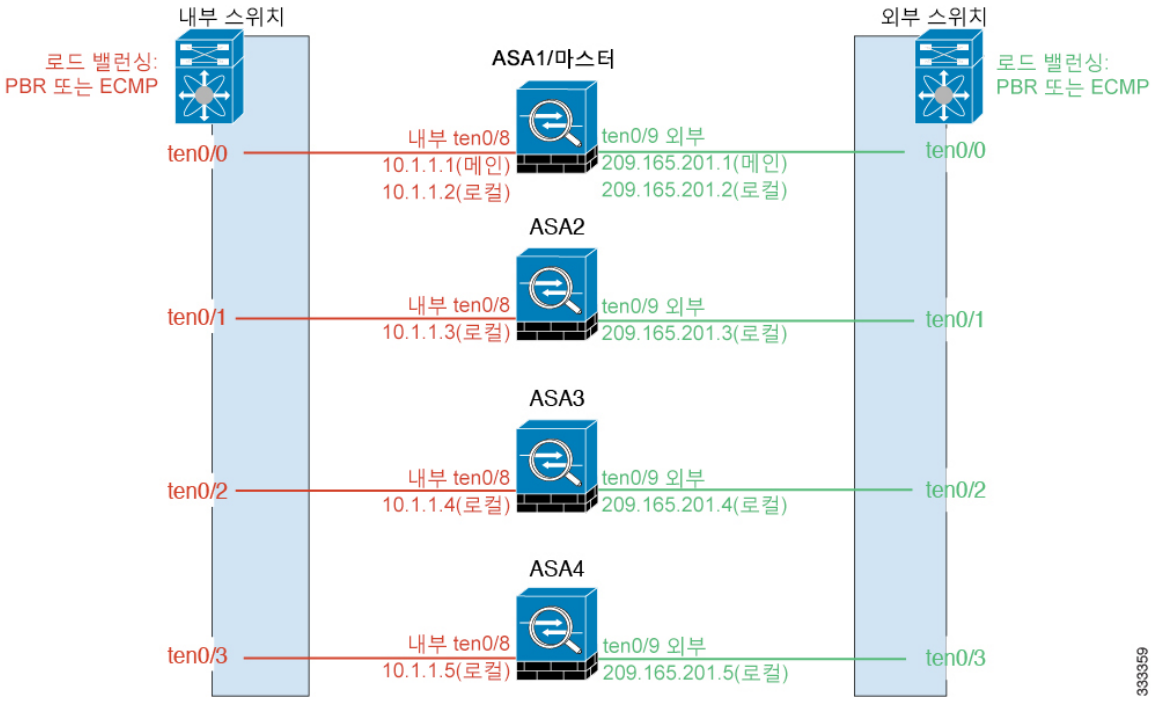
다음 그림에는 4-ASA 클러스터 및 8-ASA 클러스터의 8개 액티브/8개 스탠바이 링크 Spanned EtherChannel이 나와 있습니다. 활성 링크는 실선으로 표시되며 비활성 링크는 점으로 표시됩니다. cLACP 로드 밸런싱은 EtherChannel에서 활성화할 최상의 8가지 링크를 자동으로 선택할 수 있습니다. 그림과 같이, cLACP를 사용하면 링크 수준에서 로드 밸런싱을 실현하는 데 도움이 됩니다.



개별 인터페이스(라우팅 방화벽 모드 전용)

개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 로컬 *IP* 주소가 있습니다. 인터페이스 컨피그레이션은 마스터 유닛에서만 구성해야 하므로, 인터페이스 컨피그레이션을 사용하면 클러스터 멤버에 대해 지정된 인터페이스에 사용할 IP 주소 풀을 설정할 수 있습니다. 기본 클러스터 *IP* 주소는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 기본 클러스터 IP 주소는 마스터 유닛의 슬레이브 IP 주소이며, 로컬 IP 주소는 항상 라우팅의 마스터 주소입니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 마스터 유닛이 변경될 경우 주요 클러스터 IP 주소는 새 마스터 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 그러나 이 경우 로드 밸런싱은 업스트림 스위치에서 별도로 구성해야 합니다.

참고 개별 인터페이스보다는 스팬 EtherChannel을 권장합니다. 그 이유는 개별 인터페이스의 경우 라우팅 프로토콜을 기반으로 트래픽의 로드 밸런싱을 수행하며, 라우팅 프로토콜은 링크 오류 발생 시 통합 속도가 느려지는 경우가 많습니다.



정책 기반 라우팅(라우팅 방화벽 모드 전용)

개별 인터페이스를 사용할 경우, 각 ASA 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. 로드 밸런싱 방법 중 하나는 PBR(Policy-Based Routing)입니다.

이미 PBR을 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다. 이 방법은 추가 조정 옵션과 스팬 EtherChannel을 비교하여 제공할 수도 있습니다.

PBR 방법의 경우 경로 맵 및 ACL을 기준으로 라우팅을 결정합니다. 클러스터에 있는 모든 ASA 간의 트래픽을 수동으로 나누어야 합니다. PBR은 고정이므로 매번 최적의 로드 밸런싱 결과를 달성할 수 있는 것은 아닙니다. 최상의 성능을 실현하려면 연결의 전달 및 반환 패킷이 동일한 물리적 ASA에 전달되도록 PBR 정책을 구성하는 것이 좋습니다. 예를 들어, Cisco 라우터가 있는 경우 Cisco IOS PBR with Object Tracking을 사용하여 이중화를 구현할 수 있습니다. Cisco IOS Object Tracking에서는 ICMP Ping을 사용하여 각 ASA를 모니터링합니다. 그러면 PBR에서 특정 ASA의 도달 범위를 기준으로 경로 맵을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

참고 이 로드 밸런싱 방법을 사용할 경우 디바이스-로컬 EtherChannel을 개별 인터페이스로 사용할 수 있습니다.

Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용)

개별 인터페이스를 사용할 경우, 각각의 ASA 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. 로드 밸런싱 방법 중 하나는 ECMP(Equal-Cost Multi-Path) 라우팅입니다.

이미 ECMP를 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다. 이 방법은 추가 조정 옵션과 스팬 EtherChannel을 비교하여 제공할 수도 있습니다.

ECMP 라우팅을 사용하면 라우팅 메트릭에서 가장 순위가 높은 여러 가지 "최상의 경로"를 통해 패킷을 전달할 수 있습니다. EtherChannel과 마찬가지로, 소스와 목적지 IP 주소 및/또는 소스와 목적지 포트의 해시를 사용하여 다음 홉 중 하나로 패킷을 보낼 수 있습니다. ECMP 라우팅을 위한 고정 경로를 사용할 경우, ASA 장애가 발생하면 문제를 초래할 수 있습니다. 경로는 계속 사용되며 장애가 발생한 ASA에 대한 트래픽은 손실됩니다. 고정 경로를 사용할 경우 Object Tracking 같은 고정 경로 모니터링 기능을 사용할 수 있는지 확인하십시오. 동적 라우팅 프로토콜을 사용하여 경로를 추가 및 제거하는 것이 좋으며, 이 경우 동적 라우팅에 참여하도록 각 ASA를 구성해야 합니다.

참고 이 로드 밸런싱 방법을 사용할 경우 디바이스-로컬 EtherChannel을 개별 인터페이스로 사용할 수 있습니다.

Nexus Intelligent Traffic Director(라우팅 방화벽 모드 전용)

개별 인터페이스를 사용할 경우, 각각의 ASA 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. ITD(Intelligent Traffic Director)는 Nexus 5000, 6000, 7000 및 9000 스위치 시리즈용 고속 하드웨어 로드 밸런싱 솔루션입니다. 여기서는 기존 PBR의 작동 기능을 완전히 다룰 뿐만 아니라 더 세분화된 로드 분배를 위해 간소화된 구성 워크플로 및 여러 추가적인 기능을 제공합니다.

ITD에서는 IP 고착성, 양방향 플로우 대칭을 위한 일관된 해싱, 가상 IP 주소 지정, 상태 모니터링, N+M 이중화를 통한 정교한 장애 처리 정책, 가중화된 로드 밸런싱, DNS를 포함하는 애플리케이션 IP SLA 프로브를 지원합니다. 로드 밸런싱의 동적인 특성으로 인해 ITD에서는 PBR과 비교하여 모든 클러스터 멤버에서 더 균일한 트래픽 배포를 수행할 수 있습니다. 양방향 플로우 대칭을 달성하기 위해 동일한 물리적 ASA로 향하는 연결의 패킷을 전달하고 반환하는 ITD를 구성하는 것이 좋습니다. 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

클러스터 유닛 케이블 연결 및 업스트림/다운스트림 장비 구성

클러스터링을 구성하기 전에 클러스터 제어 링크 네트워크, 관리 네트워크, 데이터 네트워크의 케이블을 연결합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	클러스터 제어 링크 네트워크, 관리 네트워크, 데이터 네트워크의 케이블을 연결합니다.	참고 클러스터에 참가할 유닛을 구성하기 전에 최소한 활성 클러스터 제어 링크 네트워크가 있어야 합니다. 또한 업스트림 및 다운스트림 장비도 구성해야 합니다. 예를 들어, EtherChannel을 사용할 경우 EtherChannel에 대한 업스트림 및 다운스트림 장비를 구성해야 합니다.

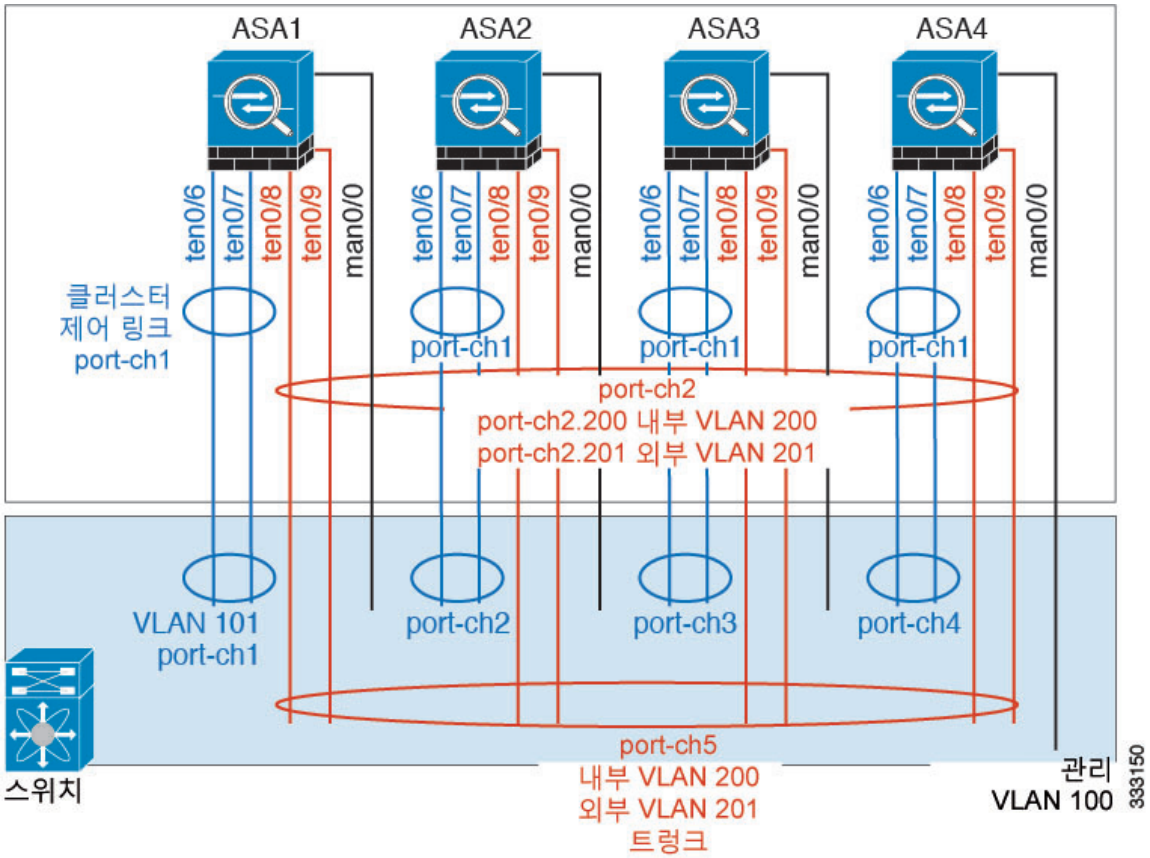
예

참고 이 예에서는 로드 밸런싱에 EtherChannel을 사용합니다. PBR 또는 ECMP를 사용할 경우 스위치 컨피그레이션이 달라집니다.

예를 들어, 4개의 각 ASA 5585-X에서 다음과 같은 기능을 사용할 수 있습니다.

- 클러스터 제어 링크에 대한 디바이스-로컬 EtherChannel에서 10기가비트 이더넷 인터페이스 2개
- 내부 및 외부 네트워크에 대한 스팬 EtherChannel에서 10기가비트 이더넷 인터페이스 2개. 각 인터페이스는 EtherChannel의 VLAN 하위 인터페이스입니다. 하위 인터페이스를 사용하면 내부 및 외부 인터페이스에서 모두 EtherChannel의 이점을 활용할 수 있습니다.
- 관리 인터페이스 1개.

내부 및 외부 네트워크의 스위치는 1개입니다.



목적	각 **4**개의 **ASA**에 인터페이스 연결	포트 전환
클러스터 제어 링크	TenGigabitEthernet 0/6 및 TenGigabitEthernet 0/7	총 8개 포트 각 TenGigabitEthernet 0/6 및 TenGigabitEthernet 0/7 쌍에 대해 EtherChannel 4개를 구성합니다(각 ASA당 EC 1개). 이러한 EtherChannel은 모두 동일한 별도의 클러스터 제어 VLAN에 있어야 합니다(예: VLAN 101).
내부 및 외부 인터페이스	TenGigabitEthernet 0/8 및 TenGigabitEthernet 0/9	총 8개 포트 단일 EtherChannel을 구성합니다(모든 ASA에 대해). 스위치에서 이러한 VLAN 및 네트워크를 구성합니다(예: 내부용 VLAN 200 및 외부용 VLAN 201을 포함하는 트렁크).
관리 인터페이스	Management 0/0	총 4개 포트 동일한 별도의 관리 VLAN에 모든 인터페이스를 배치합니다(예: VLAN 100).

각 유닛에서 클러스터 인터페이스 모드 구성

클러스터링의 인터페이스 유형은 스팬 EtherChannel 또는 개별 인터페이스 중 한 가지로만 구성할 수 있으며, 클러스터에서 여러 인터페이스 유형을 함께 사용할 수 없습니다.

시작하기 전에

- 클러스터에 추가할 각 ASA에 모드를 개별적으로 설정해야 합니다.
- 관리 전용 인터페이스는 항상 개별 인터페이스로 구성할 수 있으며(권장), 스팬 EtherChannel 모드에서도 마찬가지입니다. 투명 방화벽 모드에서도 관리 인터페이스는 개별 인터페이스가 될 수 있습니다.
- 스팬 EtherChannel 모드에서 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 경로를 사용해야 합니다.
- 다중 상황 모드에서는 모든 상황에 한 가지 인터페이스 유형을 선택해야 합니다. 예를 들어, 투명 및 라우팅 모드 상황을 함께 선택한 경우 투명 모드에는 한 가지 인터페이스 유형만 허용되므로 모든 상황에 스팬 EtherChannel 모드를 사용해야 합니다.

프로시저

단계 **1** 호환되지 않는 모든 컨피그레이션을 표시하여 인터페이스 모드를 강제로 시행하여 나중에 컨피그레이션을 수정할 수 있습니다. 다음 명령을 사용할 경우 모드는 변경되지 않습니다.

cluster interface-mode {**individual** | **spanned**} **check-details**

예제**:**

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

단계 **2** 클러스터링에 대한 인터페이스 모드를 설정합니다.

cluster interface-mode {**individual** | **spanned**} **force**

예제**:**

```
ciscoasa(config)# cluster interface-mode spanned force
```

기본 설정은 없으며, 모드를 명시적으로 선택해야 합니다. 모드를 설정하지 않을 경우 클러스터링을 사용할 수 없습니다.

force 옵션을 사용하면 컨피그레이션에 호환되지 않는 설정이 있는지 확인하지 않고 모드를 변경합니다. 모드를 변경한 후에는 수동으로 컨피그레이션 문제를 수정해야 합니다. 모드를 설정한 후에는 인터페이스 컨피그레이션을 수정하는 것만 가능하므로, **force** 옵션을 사용하여 최소한 기존 컨피그레이션에서 시작하는 방법을 권장합니다. 자세한 지침을 보려면 모드를 설정한 후 **check-details** 옵션을 다시 실행합니다.

force 옵션을 사용하지 않을 경우 호환되지 않는 컨피그레이션 문제가 발생하면 컨피그레이션을 지우고 다시 로드하겠는지 묻는 메시지가 표시됩니다. 이 경우 콘솔 포트에 연결하여 관리 액세스를 다시 구성해야 합니다. 드물게 컨피그레이션이 호환되는 경우 모드가 변경되며 해당 컨피그레이션이 유지됩니다. 컨피그레이션을 지우지 않으려면 **n**을 입력하여 명령 창에서 나옵니다.

인터페이스 모드를 제거하려면 **no cluster interface-mode** 명령을 입력합니다.

마스터 유닛의 인터페이스 구성

클러스터링을 활성화하기 전에, 현재 IP 주소가 구성된 모든 인터페이스가 클러스터링을 수행할 준비가 되도록 수정해야 합니다. 그 외의 기타 인터페이스는 클러스터링을 활성화하기 전에 또는 활성화한 후에 구성할 수 있습니다. 그러나 모든 인터페이스를 사전에 구성하여 전체 컨피그레이션을 새 클러스터 멤버와 동기화하는 것이 좋습니다.

이 섹션에서는 클러스터링과 호환되는 인터페이스를 구성하는 방법에 대해 설명합니다. 데이터 인터페이스를 스팬 EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 각 방법에서는 다양한 로드 밸런싱 메커니즘을 사용합니다. 스팬 EtherChannel 모드에서도 개별 인터페이스가 될 수 있는 관리 인터페이스를 제외하고는 같은 컨피그레이션에 두 가지 유형을 모두 컨피그레이션할 수 없습니다.

개별 인터페이스 구성(관리 인터페이스 권장 사항)

개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 IP 주소 풀에서 가져온 고유한 IP 주소가 있습니다. 기본 클러스터 IP 주소는 현재 기본 유닛에 항상 속해 있는 클러스터를 위한 고정 주소입니다.

스팬 EtherChannel 모드의 경우 관리 인터페이스를 개별 인터페이스로 구성하는 방법을 권장합니다. 개별 관리 인터페이스를 사용하면 필요한 경우 각 유닛에 직접 연결할 수 있는 반면, Spanned EtherChannel 인터페이스의 경우에는 현재 기본 유닛에 대한 연결만 가능합니다.

시작하기 전에

- 관리 전용 인터페이스를 제외하고, 개별 인터페이스 모드를 사용해야 합니다.
- 다중 상황 모드의 경우, 각 상황에서 이러한 절차를 수행합니다. 현재 상황 구성 모드가 아닌 경우, **changeto context***name* 명령을 입력합니다.
- 개별 인터페이스는 네이버 디바이스의 로드 밸런싱을 구성해야 합니다. 관리 인터페이스에는 외부 로드 밸런싱이 필요하지 않습니다.
- (선택 사항) 인터페이스를 디바이스-로컬 EtherChannel, 이중 인터페이스로 구성하거나 하위 인터페이스로 구성합니다.
  - EtherChannel의 경우 이러한 EtherChannel은 유닛에 대해 로컬이며 스팬 EtherChannel이 아닙니다.
  - 관리 전용 인터페이스는 이중 인터페이스가 될 수 없습니다.

프로시저

단계 **1** 로컬 IP 주소(IPv4 및/또는 IPv6)를 구성합니다. 이 중 하나는 인터페이스의 각 클러스터 유닛에 할당됩니다.

(IPv4)

ip local pool *poolname first-address — last-address* [**mask** *mask*]

(IPv6)

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

예제**:**

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8::1002/32 8
```

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 기본 유닛에 속하는 기본 클러스터 IP 주소는 이러한 풀에 속하지 않습니다. 따라서 동일한 네트워크에서 기본 클러스터 IP 주소에 대한 IP 주소를 예약해 두어야 합니다.

각 유닛에 정확히 어떤 로컬 주소가 할당되는지 미리 확인할 수는 없습니다. 각 유닛에 사용된 주소를 보려면 **show ip**[v6] **local pool** *poolname* 명령을 입력하십시오. 각 클러스터 멤버는 클러스터에 참가할 때 멤버 ID가 할당됩니다. ID는 풀에서 사용되는 로컬 IP를 결정합니다.

단계 **2** 인터페이스 구성 모드로 들어갑니다.

interface *interface_id*

예제:

```
ciscoasa(config)# interface tengigabitethernet 0/8
```

단계 **3** (관리 인터페이스 전용) 인터페이스를 관리 전용 모드로 설정하여 트래픽을 통해 전달되지 않도록 합니다.

management-only

기본적으로 관리 유형 인터페이스는 관리 전용으로 구성됩니다. 투명 모드에서 이 명령은 관리 유형 인터페이스에 항상 사용됩니다.

클러스터 인터페이스 모드가 스팬인 경우 이 설정이 필요합니다.

단계 **4** 인터페이스 이름을 지정합니다.

nameif *name*

예제:

```
ciscoasa(config-if)# nameif inside
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다.

단계 **5** 기본 클러스터 IP 주소를 설정하고 클러스터 풀을 확인합니다.

(IPv4)

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

(IPv6)

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

예제:

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8::1002/32 cluster-pool insipv6
```

이 IP 주소는 같은 네트워크의 클러스터 풀 주소로 있어야 하지만 풀의 일부는 아닙니다. IPv4 및/또는 IPv6 주소를 구성할 수 있습니다.

DHCP, PPPoE, IPv6 자동 구성은 지원되지 않습니다. 수동으로 IP 주소를 구성해야 합니다.

단계 **6** 보안 수준을 설정합니다. 입력할 숫자는 0(가장 낮음)에서 100(가장 높음) 사이의 정수입니다.

security-level *number*

예제:

```
ciscoasa(config-if)# security-level 100
```

단계 7 인터페이스를 활성화합니다.

no shutdown

예

다음 예에서는 Management 0/0 및 Management 0/1 인터페이스를 디바이스-로컬 EtherChannel로 구성하고, EtherChannel을 개별 인터페이스로 구성합니다.

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8
interface management 0/0

channel-group 1 mode active
no shutdown

interface management 0/1

channel-group 1 mode active
no shutdown

interface port-channel 1

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1001/64 cluster-pool mgmtipv6
security-level 100
management-only
```

스팬 EtherChannel 구성

Spanned EtherChannel은 클러스터의 모든 ASA를 포괄하며, EtherChannel이 실행되는 과정의 일환으로 로드 밸런싱을 제공합니다.

시작하기 전에

- 스팬 EtherChannel 인터페이스 모드에 있어야 합니다.
- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 시작합니다. 현재 시스템 구성 모드가 아닌 경우 Configuration(구성) > Device List(디바이스 목록) 창의 활성 디바이스 IP 주소에서 **System(**시스템**)**을 두 번 클릭하여 **changeto system** 명령.
- 투명 모드의 경우 브리지 그룹을 구성합니다. BVI(Bridge Virtual Interface) 구성, 618 페이지을 참조하십시오.

- EtherChannel에서는 최대 및 최소 링크 수를 지정하지 마십시오. ASA 또는 스위치의 EtherChannel에서는 최대 및 최소 링크 수를 지정하지 않는 것이 좋습니다(**lacp max-bundle** 및 **port-channel min-bundle** 명령). 사용해야 하는 경우 다음 사항을 주의하십시오.
  - ASA에 설정된 최대 링크 수는 전체 클러스터의 총 액티브 포트 수입니다. 스위치에 구성된 최대 링크 수 값이 ASA 값보다 크지 않은지 확인하십시오.
  - ASA에 설정된 최소 링크 수는 유닛당 포트 채널 인터페이스를 가져오는 최소 액티브 포트 수입니다. 스위치에서 최소 링크 수는 클러스터 전체의 최소 링크 수이므로 이 값은 ASA 값과 일치하지 않습니다.
- 로드 밸런싱 알고리즘의 기본값을 변경하지 마십시오(**port-channel load-balance** 명령의 경우). 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 ASA에 트래픽이 균일하지 않게 분산될 수 있습니다.
- **lacp port-priority** 및 **lacp system-priority** 명령은 스팬 EtherChannel에 사용되지 않습니다.
- 스팬 EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 작동하지 않습니다. 이러한 요건으로 인해 클러스터의 활성 유닛이 아닌 유닛에는 트래픽이 전달되지 않습니다.

프로시저

단계 **1** 채널 그룹에 추가할 인터페이스를 지정합니다.

interface *physical_interface*

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID에는 유형, 슬롯, 포트 번호가 유형 슬롯/ 포트로 포함되어 있습니다. 채널 그룹의 첫 번째 인터페이스는 그룹에 있는 모든 기타 인터페이스의 유형과 속도를 결정합니다.

단계 **2** 이 인터페이스를 EtherChannel에 할당합니다.

channel-group *channel_id* **mode active** [**vss-id** {**1** | **2**}]

예제**:**

```
ciscoasa(config-if)# channel-group 1 mode active
```

*channel_id*는 1에서 48까지의 숫자입니다. 이 채널 ID의 포트 채널 인터페이스가 아직 구성에 없는 경우, 자동으로 추가됩니다.

interface port-channel *channel_id*

스팬 EtherChannel에는 액티브 모드만 지원됩니다.

ASA를 VSS 또는 vPC에 있는 두 개의 스위치에 연결할 경우, **vss-id** 키워드를 구성하여 이 인터페이스를 어느 스위치(1 또는 2)에 연결할지 식별합니다. 또한 6단계의 포트 채널 인터페이스에 **port-channel span-cluster vss-load-balance** 명령을 사용해야 합니다.

단계 **3** 인터페이스를 활성화합니다.

no shutdown

단계 **4** (선택 사항) 프로세스를 반복하여 EtherChannel에 인터페이스를 추가합니다.

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

유닛당 EtherChannel의 다중 인터페이스는 VSS 또는 vPC의 스위치에 연결할 때 유용합니다. 기본적으로 스팬 EtherChannel의 경우 클러스터의 모든 멤버 전체의 최대 16개 인터페이스 중 활성 인터페이스를 8개까지만 보유할 수 있습니다. 나머지 8개 인터페이스는 링크 오류에 대비하여 스탠바이 상태로 유지됩니다. 대기 인터페이스는 그대로 두고 8개 이상의 활성 인터페이스를 사용하려면, **clacp static-port-priority** 명령을 사용하여 동적 포트 우선순위를 비활성화합니다. 동적 포트 우선순위를 비활성화하면 클러스터 전체에 걸쳐 최대 32개의 활성 링크를 사용할 수 있습니다. 예를 들어, 16개의 ASA로 구성된 클러스터의 경우 각 ASA에 최대 2개의 인터페이스를 사용할 수 있으므로 스팬 EtherChannel의 인터페이스는 총 32개입니다.

단계 **5** 포트 채널 인터페이스를 지정합니다.

interface port-channel *channel_id*

예제**:**

```
ciscoasa(config)# interface port-channel 1
```

이 인터페이스는 채널 그룹에 인터페이스를 추가할 경우 자동으로 생성된 것입니다.

단계 **6** 이 EtherChannel을 스팬 EtherChannel로 설정합니다.

port-channel span-cluster [**vss-load-balance**]

예제**:**

```
ciscoasa(config-if)# port-channel span-cluster
```

ASA를 VSS 또는 vPC에 있는 두 개의 스위치에 연결할 경우, **vss-load-balance** 키워드를 사용하여 VSS 로드 밸런싱을 활성화해야 합니다. 이 기능은 VSS(또는 vPC) 쌍에 대한 ASA 간의 물리적 링크 연결이 균형을 이루도록 합니다. 로드 밸런싱을 활성화하기 전에 **channel-group** 명령에서 **vss-id** 키워드를 각 멤버 인터페이스에 대해 구성해야 합니다(2단계 참조).

단계 **7** (선택사항) 포트 채널 인터페이스에 대한 이더넷 속성을 설정하여 개별 인터페이스의 속성 설정을 재정의할 수 있습니다.

이러한 매개변수는 채널 그룹의 모든 인터페이스와 일치해야 하므로, 이 방법을 사용하면 이러한 매개변수를 빠르게 설정할 수 있습니다.

단계 **8** (선택사항) 이러한 EtherChannel에 VLAN 하위 인터페이스를 생성하려면 지금 수행하십시오.

예제**:**

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

이 절차의 나머지는 하위 인터페이스에 적용됩니다.

단계 **9** (다중 상황 모드) 상황에 인터페이스를 할당합니다. 그리고 다음과 같이 입력합니다.

changeto context *name*
interface port-channel *channel_id*

예제**:**

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

다중 상황 모드의 경우, 각 상황에서 인터페이스 컨피그레이션의 나머지 부분이 이루어집니다.

단계 **10** 인터페이스 이름을 지정합니다.

nameif *name*

예제**:**

```
ciscoasa(config-if)# nameif inside
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다.

단계 **11** 방화벽 모드에 따라 다음 중 하나를 수행합니다.

- 라우팅 모드—IPv4 및/또는 IPv6 주소를 설정합니다.

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

  예:

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

DHCP, PPPoE, IPv6 자동 구성은 지원되지 않습니다. 포인트 투 포인트 연결을 위해 31비트 서브넷 마스크(255.255.255.254)를 지정할 수 있습니다. 이 경우 IP 주소가 네트워크 또는 브로드캐스트 주소에 대해 예약되어 있습니다.

- 투명 모드 — 브리지 그룹에 인터페이스를 할당합니다.

  bridge-group *number*

  예:

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  *number*는 1에서 100까지의 정수입니다. 최대 64개의 인터페이스를 하나의 브리지 그룹에 할당할 수 있습니다. 동일한 인터페이스를 둘 이상의 브리지 그룹에 할당할 수 없습니다. BVI 구성에는 IP 주소가 포함되어 있습니다.

단계 **12** 보안 수준을 설정합니다.

security-level *number*

예제**:**

```
ciscoasa(config-if)# security-level 50
```

*number*는 0(최저) ~ 100(최고) 범위의 정수입니다.

단계 **13** 잠재적인 네트워크 연결 문제를 방지하기 위해 Spanned EtherChannel에 대한 전역 MAC 주소를 구성합니다.

mac-address *mac_address*

예제**:**

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

수동 구성된 MAC 주소를 사용할 경우, 해당 MAC 주소가 현재 마스터 유닛에 유지됩니다. MAC 주소를 구성하지 않은 상태에서 마스터 유닛을 변경하는 경우 새 마스터 유닛에서는 인터페이스의 새 MAC 주소를 사용하며, 이로 인해 임시 네트워크가 중단될 수 있습니다.

다중 상황 모드에서 상황 간에 인터페이스를 공유할 경우, MAC 주소를 수동으로 설정할 필요가 없도록 MAC 주소의 자동 생성을 활성화해야 합니다. 공유되지 않는 인터페이스에 이 명령을 사용하여 MAC 주소를 수동으로 구성해야 합니다.

*mac_address*는 H.H.H 형식이며, 여기서 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다.

자동 생성된 MAC 주소도 사용하려는 경우 수동 MAC 주소의 처음 2바이트는 A2가 될 수 없습니다.

단계 **14** (라우팅 모드) 사이트 간 클러스터링을 위해 각 사이트의 사이트별 MAC 주소 및 IP 주소를 구성합니다.

mac-address *mac_address* **site-id** *number*

예제:

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

사이트별 IP 주소는 전역 IP 주소와 동일한 서브넷에 있어야 합니다. 유닛에서 사용한 사이트별 MAC 주소 및 IP 주소는 각 유닛의 부트스트랩 구성에서 지정하는 사이트 ID에 따라 달라집니다.

부트스트랩 구성 생성

클러스터의 각 유닛은 클러스터에 참가하려면 부트스트랩 컨피그레이션이 필요합니다.

마스터 유닛 부트스트랩 설정 구성

클러스터의 각 유닛은 클러스터에 참가하려면 부트스트랩 컨피그레이션이 필요합니다. 일반적으로 클러스터에 참가하기 위해 구성하는 첫 번째 유닛이 마스터 유닛이 됩니다. 클러스터링이 활성화되고 선택 기간이 지나면 클러스터에서 마스터 유닛을 선택합니다. 맨 처음 클러스터에 유닛이 하나밖에 없을 경우, 해당 유닛이 마스터 유닛이 됩니다. 클러스터에 추가되는 후속 유닛은 슬레이브 유닛이 됩니다.

시작하기 전에

- 향후 클러스터에서 벗어나려는 경우 구성을 백업한 후 해당 구성을 복원해야 합니다.
- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 완료하십시오. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.
- 클러스터 제어 링크에 사용하려면 점보 프레임 예약을 활성화하는 것이 좋습니다.
- 클러스터링을 활성화하거나 비활성화하려면 콘솔 포트를 사용해야 합니다. 텔넷이나 SSH는 사용할 수 없습니다.
- 클러스터 제어 링크를 제외하고, 컨피그레이션의 모든 인터페이스는 클러스터링을 활성화하기 전에 인터페이스 모드에 따라 클러스터 IP 풀 또는 스팬 EtherChannel로 컨피그레이션해야 합니다. 기존의 인터페이스 구성이 있는 경우, 클러스터링을 활성화하기 전에 해당 인터페이스 구성을 지우거나(**clear configure interface**) 인터페이스를 클러스터 인터페이스로 변환할 수 있습니다.
- 실행 중인 클러스터에 유닛을 추가할 경우, 일시적이고 제한적으로 패킷/연결이 드롭될 수 있으며 이는 정상적인 동작입니다.
- 클러스터 제어 링크의 크기를 사전에 결정합니다. 을 위한 클러스터 제어 링크 크기 조정, 381 페이지을 참조하십시오.

프로시저

단계 **1** 클러스터에 참가하기 전에 클러스터 제어 링크 인터페이스를 활성화합니다.

클러스터링을 활성화할 경우 나중에 이 인터페이스를 클러스터 제어 링크로 확인합니다.

인터페이스가 충분한 경우 여러 개의 클러스터 제어 링크 인터페이스를 하나의 EtherChannel로 통합하는 편이 좋습니다. EtherChannel은 ASA에 대해 로컬이며 Spanned EtherChannel이 아닙니다.

클러스터 제어 링크 인터페이스 구성은 마스터 유닛에서 슬레이브 유닛으로 복제되지 않지만, 각 유닛에는 동일한 구성을 사용해야 합니다. 이 구성은 복제되지 않으므로, 각 유닛에 클러스터 제어 링크 인터페이스를 별도로 구성해야 합니다.

- VLAN 하위 인터페이스는 클러스터 제어 링크로 사용할 수 없습니다.
- 관리 *x/x* 인터페이스는 단독으로든 EtherChannel로든 클러스터 제어 링크로 사용할 수 없습니다.
- ASA FirePOWER 모듈을 사용하는 ASA 5585-X의 경우 ASA FirePOWER 모듈의 인터페이스가 아닌 클러스터 제어 링크의 ASA 인터페이스를 사용하는 것이 좋습니다. 모듈 인터페이스는 소프트웨어 업그레이드 중에 발생하는 다시 로드를 포함하여 모듈 다시 로드 중에 최대 30초 동안 트래픽을 삭제할 수 있습니다. 그러나, 필요한 경우 모듈 인터페이스와 ASA 인터페이스를 동일한 클러스터 제어 링크 EtherChannel에서 사용할 수 있습니다. 모듈 인터페이스가 삭제되는 경우, EtherChannel의 나머지 인터페이스는 여전히 작동합니다. ASA 5585-X 네트워크 모듈은 별도의 운영 체제를 실행하지 않으므로 이 문제의 영향을 받지 않습니다.

a) 인터페이스 컨피그레이션 모드를 시작합니다.

interface *interface_id*

예제**:**

```
ciscoasa(config)# interface tengigabitethernet 0/6
```

b) (EtherChannel의 선택사항) 이 물리적 인터페이스를 EtherChannel에 할당합니다.

channel-group *channel_id* **mode on**

예제**:**

```
ciscoasa(config-if)# channel-group 1 mode on
```

*channel_id*는 1에서 48까지의 숫자입니다. 이 채널 ID의 포트 채널 인터페이스가 아직 구성에 없는 경우, 자동으로 추가됩니다.

interface port-channel *channel_id*

클러스터 제어 링크 멤버 인터페이스에 On 모드를 사용하여 클러스터 제어 링크의 불필요한 트래픽을 줄이는 것이 좋습니다. 클러스터 제어 링크는 분리된 안정적인 네트워크이므로 LACP 트래픽의 오버헤드가 필요하지 않습니다. 참고**:** 활성 모드에 데이터 EtherChannel을 설정하는 것이 좋습니다.

c) 인터페이스를 활성화합니다.

no shutdown

인터페이스를 활성화하기만 하면 되며 인터페이스의 이름이나 기타 매개변수는 구성하지 마십시오.

d) (EtherChannel에 해당) EtherChannel에 추가할 각 추가 인터페이스를 반복합니다.

예제:

```
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

단계 **2** (선택사항) 클러스터 제어 링크 인터페이스의 최대 전송 유닛을 지정합니다.

mtu cluster 바이트

예제:

```
ciscoasa(config)# mtu cluster 9000
```

MTU를 1400~9198바이트 범위에서 설정합니다. 기본 MTU는 1500바이트입니다.

MTU는 1600바이트 이상으로 설정하는 것이 좋습니다. 이 경우 이 절차를 계속 진행하기 전에 점보 프레임 예약을 활성화해야 합니다. 점보 프레임 예약을 수행하려면 ASA를 다시 로드해야 합니다.

이 명령은 전역 구성 명령일 뿐만 아니라 유닛 간에 복제되지 않은 부트스트랩 구성의 일부입니다.

단계 **3** 클러스터의 이름을 지정하고 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제:

```
ciscoasa(config)# cluster group pod1
```

이름은 1~38자로 된 ASCII 문자열이어야 합니다. 유닛당 클러스터 그룹은 하나만 구성할 수 있습니다. 클러스터의 모든 멤버는 동일한 이름을 사용해야 합니다.

단계 **4** 이 클러스터 멤버의 이름을 지정하십시오.

local-unit *unit_name*

1~38자로 된 고유한 ASCII 문자열을 사용합니다. 각 유닛에는 고유한 이름이 있어야 합니다. 이름이 중복된 유닛은 클러스터에서 사용할 수 없습니다.

예제:

```
ciscoasa(cfg-cluster)# local-unit unit1
```

단계 **5** 클러스터 제어 링크 인터페이스를 지정하며, EtherChannel이 권장됩니다.

cluster-interface *interface_id* **ip** *ip_address mask*

예제:

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

하위 인터페이스 및 관리 인터페이스는 허용되지 않습니다.

IP 주소의 IPv4 주소를 지정합니다. 이 인터페이스에는 IPv6가 지원되지 않습니다. 이 인터페이스에는 **nameif**가 구성될 수 없습니다.

각 유닛의 IP 주소는 동일한 네트워크상에 있되 서로 다르게 지정하십시오.

단계 **6** 사이트 간 클러스터링을 사용하는 경우 이 유닛에 대한 사이트 ID가 사이트별 MAC 주소를 사용하도록 설정합니다.

site-id *number*

예제**:**

```
ciscoasa(cfg-cluster)# site-id 1
```

*number*는 1~8 범위의 수입니다.

단계 **7** 마스터 유닛 선택을 위해 이 유닛의 우선순위를 설정합니다.

priority *priority_number*

예제**:**

```
ciscoasa(cfg-cluster)# priority 1
```

우선순위는 1에서 100까지이며 1이 가장 높은 우선순위입니다.

단계 **8** (선택사항) 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 설정합니다.

key *shared_secret*

예제**:**

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

공유 비밀은 1자 ~ 63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 명령은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

단계 **9** (선택사항) LACP의 동적 포트 우선순위를 비활성화합니다.

clacp static-port-priority

일부 스위치에서는 동적 포트 우선순위를 지원하지 않으므로, 이 명령을 사용하면 스위치 호환성이 개선됩니다. 또한 이 명령을 사용하면 8개 이상의 활성 스팬 EtherChannel 멤버를 지원하는 것이 허용되므로 최대 32개의 멤버를 지원할 수 있습니다. 이 명령을 사용하지 않을 경우 8개의 활성 멤버 및 8개의 대기 멤버만 지원됩니다. 이 명령을 활성화할 경우 대기 멤버를 사용할 수 없으며 모든 멤버가 활성 상태로 됩니다.

단계 **10** (선택사항) cLACP 시스템 ID 및 시스템 우선순위를 수동으로 지정합니다.

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

예제**:**

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

Spanned EtherChannel을 사용할 경우 ASA에서는 cLACP를 사용하여 EtherChannel과 네이버 스위치의 협상을 수행합니다. 클러스터의 ASA는 cLACP 협상 과정에서 협업을 수행하므로 스위치에 단일(가상) 디바이스로 표시됩니다. cLACP 협상의 한 가지 매개변수는 MAC 주소 형식으로 된 시스템 ID입니다. 클러스터의 모든 ASA에서는 동일한 시스템 ID를 사용합니다. 이는 마스터 유닛에서 자동 생성되고(기본값) 모든 보조 유닛에 복제됩니다. 또는 *H.H.H* 형식으로 이러한 명령을 통해 수동으로 지정됩니다. 여기서 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0A-00-00-AA-AA는 000A.0000.AAAA로 입력됩니다. 문제 해결을 위해 MAC 주소를 수동으로 구성할 수도 있습니다. 예를 들어 식별하기 쉬운 MAC 주소를 사용하기 위해 수동으로 구성할 수 있습니다. 일반적으로 자동 생성된 MAC 주소를 사용하게 됩니다.

1에서 65535 사이의 시스템 우선순위는 번들링 결정을 담당할 유닛을 지정하는 데 사용됩니다. 기본적으로 ASA에서는 우선순위가 가장 높은 우선순위 1을 사용합니다. 우선순위는 스위치의 우선순위보다 높아야 합니다.

이 명령은 부트스트랩 구성의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다. 그러나 클러스터링을 활성화한 후에는 이 값을 변경할 수 없습니다.

단계 **11** 클러스터링을 활성화합니다.

enable [**noconfirm**]

예제**:**

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

enable 명령을 입력하면 ASA에서는 실행 중인 구성을 스캔하여 클러스터링에서 지원되지 않는 기능에 대한 호환되지 않는 명령을 확인하며, 여기에는 기본 구성에 있을 수 있는 명령이 포함됩니다. 비호환 명령을 삭제할지 묻습니다. **No**를 선택하면 클러스터링이 활성화되지 않습니다. 확인을 건너뛰고 비호환 명령을 자동으로 삭제하려면 **noconfirm** 키워드를 사용합니다.

활성화된 1번째 유닛에서 마스터 유닛 선택이 일어납니다. 1번째 유닛이 지금까지는 클러스터의 유일한 멤버이므로 마스터 유닛이 됩니다. 이 기간에는 어떤 구성 변경도 하지 마십시오.

클러스터링을 비활성화하려면 **no enable** 명령을 입력합니다.

참고 클러스터링을 비활성화할 경우, 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스만 활성 상태가 됩니다.

예

다음 예에서는 관리 인터페이스를 구성하고, 클러스터 제어 링크에 대한 디바이스-로컬 EtherChannel을 구성한 후 ASA에 대해 "unit1"라는 이름의 클러스터링을 활성화합니다. 이는 클러스터에 가장 처음 추가되었으므로 마스터 유닛이 됩니다.

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 0/0
   nameif management
   ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
   ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
   security-level 100
   management-only
   no shutdown

interface tengigabitethernet 0/6
   channel-group 1 mode on
   no shutdown

interface tengigabitethernet 0/7
   channel-group 1 mode on
   no shutdown

cluster group pod1
   local-unit unit1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
   priority 1
   key chuntheunavoidable
   enable noconfirm
```

슬레이브 유닛 부트스트랩 설정 구성

슬레이브 유닛을 구성하려면 다음 절차를 수행합니다.

시작하기 전에

- 클러스터링을 활성화하거나 비활성화하려면 콘솔 포트를 사용해야 합니다. 텔넷이나 SSH는 사용할 수 없습니다.
- 향후 클러스터에서 벗어나려는 경우 구성을 백업한 후 해당 구성을 복원해야 합니다.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.
- 클러스터 제어 링크에 사용하려면 점보 프레임 예약을 활성화하는 것이 좋습니다.

- 구성에 클러스터링이 구성되지 않은 인터페이스가 있는 경우(예: 기본 구성 Management 0/0 인터페이스), 해당 클러스터를 슬레이브 유닛으로 참가하도록 할 수 있습니다(현재 선택 상태에서 마스터 유닛이 될 가능성은 없음).
- 실행 중인 클러스터에 유닛을 추가할 경우, 일시적이고 제한적으로 패킷/연결이 드롭될 수 있으며 이는 정상적인 동작입니다.

프로시저

단계 **1** 마스터 유닛에 설정한 것과 동일한 클러스터 제어 링크 인터페이스를 구성합니다.

예제**:**

```
ciscoasa(config)# interface tengigabitethernet 0/6
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

단계 **2** 마스터 유닛에 구성한 것과 동일한 MTU를 지정합니다.

예제**:**

```
ciscoasa(config)# mtu cluster 9000
```

단계 **3** 마스터 유닛에 구성한 것과 동일한 클러스터 이름을 식별합니다.

예제**:**

```
ciscoasa(config)# cluster group pod1
```

단계 **4** 고유한 문자열로 이 클러스터 멤버의 이름을 지정합니다.

local-unit *unit_name*

예제**:**

```
ciscoasa(cfg-cluster)# local-unit unit2
```

1~38자로 된 ASCII 문자열을 지정합니다.

각 유닛에는 고유한 이름이 있어야 합니다. 이름이 중복된 유닛은 클러스터에서 사용할 수 없습니다.

단계 **5** 마스터 유닛에 구성된 동일한 클러스터 제어 링크 인터페이스를 지정합니다. 단, 각 유닛의 IP 주소는 동일한 네트워크상에 있되 서로 다르게 지정해야 합니다.

cluster-interface *interface_id* **ip** *ip_address mask*

예제**:**

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

IP 주소의 IPv4 주소를 지정합니다. 이 인터페이스에는 IPv6가 지원되지 않습니다. 이 인터페이스에는 **nameif**가 구성될 수 없습니다.

각 유닛에는 고유한 이름이 있어야 합니다. 이름이 중복된 유닛은 클러스터에서 사용할 수 없습니다.

단계 **6** 사이트 간 클러스터링을 사용하는 경우 이 유닛에 대한 사이트 ID가 사이트별 MAC 주소를 사용하도록 설정합니다.

site-id *number*

예제**:**

```
ciscoasa(cfg-cluster)# site-id 1
```

number는 1~8 범위의 수입니다.

단계 **7** 마스터 유닛 선택을 위해 이 유닛의 우선순위를 지정합니다. 일반적으로 마스터 유닛보다 숫자가 커야 합니다.

priority *priority_number*

예제**:**

```
ciscoasa(cfg-cluster)# priority 2
```

우선순위를 1에서 100까지 설정하며, 1의 우선순위가 가장 높습니다.

단계 **8** 마스터 유닛에 설정한 동일한 인증 키를 설정합니다.

예제**:**

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

단계 **9** 클러스터링을 활성화합니다.

enable as-slave

enable as-slave 명령을 사용하여 구성 비호환(아직 클러스터링이 구성되지 않은 모든 인터페이스에서 주로 발생함) 문제를 방지할 수 있습니다. 이 명령을 사용하면 현재 선택 상태에서 마스터 유닛이 될 가능성이 없는 클러스터에 슬레이브가 참가하도록 할 수 있습니다. 이 구성은 마스터 유닛에서 동기화된 구성이 덮어씁니다.

클러스터링을 비활성화하려면 **no enable** 명령을 입력합니다.

참고 클러스터링을 비활성화할 경우 모든 데이터 인터페이스가 종료되고 관리 인터페이스만 활성 상태가 됩니다.

예

다음 예에는 슬레이브 유닛인 unit2에 대한 구성이 포함됩니다.

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

cluster group pod1

local-unit unit2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

클러스터링 운영 맞춤화

클러스터링 상태 모니터링, TCP 연결 복제 지연, 플로우 모빌리티 및 기타 최적화를 맞춤화할 수 있습니다.

마스터 유닛에서 다음 절차를 수행합니다.

기본 **ASA** 클러스터 파라미터 구성

마스터 유닛에서 클러스터 설정을 맞춤화할 수 있습니다.

시작하기 전에

- 다중 상황 모드에서는 마스터 유닛의 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

단계 **2** (선택 사항) 슬레이브 유닛에서 마스터 유닛으로의 콘솔 복제를 활성화합니다.

console-replicate

이 기능은 기본적으로 비활성화되어 있습니다. ASA에서는 중요한 특정 이벤트 발생 시 일부 메시지를 콘솔에 직접 출력합니다. 콘솔 복제를 활성화할 경우, 슬레이브 유닛에서는 콘솔 메시지를 마스터 유닛에 전송하므로 클러스터의 콘솔 포트 하나만 모니터링하면 됩니다.

단계 **3** 클러스터링 이벤트의 최소 추적 수준을 설정합니다

trace-level 수준

원하는 대로 최소 수준을 설정합니다.

- **critical**— 중요 이벤트(심각도=1)
- **warning**— 경고(심각도=2)
- **informational**— 정보 이벤트(심각도=3)
- **debug**— 디버깅 이벤트(심각도=4)

상태 모니터링 및 자동 다시 참가 설정 구성

이 절차에서는 유닛 및 인터페이스 상태 모니터링을 구성합니다.

필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다. 포트 채널 ID, 중복 ID 또는 단일 물리적 인터페이스 ID 또는 ASA Firepower 모듈과 같은 소프트웨어 또는 하드웨어 모듈을 모니터링할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

단계 **2** 클러스터 유닛 상태 검사 기능을 맞춤화합니다.

health-check [**holdtime** *timeout*] [**vss-enabled**]

유닛 상태를 확인하기 위해 ASA 클러스터 유닛에서는 다른 유닛에 대한 클러스터 제어 링크에서 하트비트 메시지를 보냅니다. 유닛이 피어 유닛의 하트비트 메시지를 대기 시간 내에 수신하지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주됩니다.

- **holdtime** *timeout(*시간 제한*)* — 유닛 하트비트 상태 메시지 간의 시간 간격을 0.3~45초 범위에서 지정합니다(기본값은 3초).

- **vss-enabled** — 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 하트비트 메시지를 플러딩하여 하나 이상의 스위치에서 해당 메시지를 수신할 수 있도록 합니다. 클러스터 제어 링크를 EtherChannel로 구성하고(권장) 이를 VSS 또는 vPC 쌍에 연결한 경우, **vss-enabled** 옵션을 활성화해야 할 수 있습니다. 일부 스위치의 경우 VSS/vPC에서 유닛 하나가 중단되거나 부팅하면 해당 스위치에 연결된 EtherChannel 멤버 인터페이스가 ASA에 대해 가동되는 것으로 표시되지만, 스위치 측의 트래픽을 통과하지 않습니다. ASA 보류 시간 제한을 낮은 값(0.8초)으로 설정한 경우 클러스터에서 ASA가 잘못 제거될 수 있으며, ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다(**no health-check monitor-interface**). 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.

예제**:**

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

단계 **3** 인터페이스에서 인터페이스 상태 검사를 비활성화합니다.

no health-check monitor-interface [*interface_id* | **service-module]**

인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 유닛에서 오류가 발생했지만 다른 유닛에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 유닛은 클러스터에서 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. 상태 선택은 모든 인터페이스에 대해 기본적으로 활성화됩니다. 이 명령의 **no** 형식을 사용하여 이를 인터페이스별로 비활성화할 수 있습니다. 필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다.

- *interface_id* — 모든 포트 채널 ID, 중복 ID 또는 단일 물리적 인터페이스 ID의 모니터링을 비활성화합니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.
- **service-module**— 하드웨어 또는 소프트웨어 모듈(예: ASA FirePOWER 모듈)의 모니터링을 비활성화합니다. ASA 5585-X에서 서비스 모듈 모니터링을 비활성화하는 경우 개별적으로 모니터링되는 모듈의 인터페이스 모니터링도 비활성화할 수 있습니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능(**no health-check**)을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.

예제**:**

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
```

단계 **4** 상태 검사에 실패한 후에 자동 다시 참가 클러스터 설정을 맞춤화합니다.

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**— 내부 오류에 대한 자동 다시 참가 설정을 지정합니다. 내부 오류 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등
- **unlimited** — (**cluster-interface**의 기본값) 다시 참가 시도 횟수를 제한하지 않습니다.
- *auto-rejoin-max* — 다시 참가 시도 횟수를 0~65535 범위에서 설정합니다. **0**을 사용하면 자동 다시 참가가 비활성화됩니다. **data-interface** 및 **system**에 대한 기본값은 3입니다.
- *auto_rejoin_interval* — 다시 참가 시도 간의 간격 기간(분)을 2~60분 범위에서 정의합니다. 기본값은 5분입니다. 유닛이 클러스터에 다시 참가하려고 시도하는 최대 총 시간은 마지막 장애 시간으로부터 14400분(10일)으로 제한됩니다.
- *auto_rejoin_interval_variation* — 간격 기간이 증가하는지 여부를 정의합니다. 1~3 범위의 값 설정합니다(**1**(변경 없음), **2**(2 x 이전 기간) 또는 **3**(3 x 이전 기간)). 예를 들어, 간격 기간을 5분으로 설정하고 변수를 2로 설정하면 첫 번째 시도가 5분 후에 일어나고 두 번째 시도는 10분(2 x 5), 세 번째 시도는 20분(2 x 10) 후에 일어납니다. 기본값은 클러스터 인터페이스의 경우 **1**이며 데이터 인터페이스 및 시스템의 경우 **2**입니다.

예제**:**

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

단계 **5** ASA에서 인터페이스를 실패 상태로 간주하고 유닛이 클러스터에서 제거되기 전에 디바운스 시간을 구성합니다.

health-check monitor-interface debounce-time 밀리초

예제**:**

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

디바운스 시간을 300~9000밀리초 범위에서 설정합니다. 기본값은 500밀리초입니다. 값이 낮을수록 인터페이스 장애 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 지정되어 있는 밀리초 동안 대기합니다. 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다.

예

다음 예에서는 상태 확인 보류 시간을 0.3초로 구성하고 VSS를 활성화하며 관리에 사용되는 Ethernet 1/2 인터페이스에서 모니터링을 비활성화합니다. 데이터 인터페이스에 대한 자동 다시 참가를 2분에 시작하는 4회 시도로 설정하고 기간을 3 x 이전 간격으로 늘리며 클러스터 제어 링크에 대한 자동 다시 참가를 2분마다 6회 시도로 설정합니다.

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3 vss-enabled
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/2
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

연결 리밸런싱 및 클러스터 **TCP** 복제 지연 구성

연결 리밸런싱을 구성할 수 있습니다. 자세한 내용은 클러스터 전반에 걸쳐 새 TCP 연결 리밸런싱, 361 페이지을 참조해 주십시오.

관리자/백업 플로우 생성을 지연시켜 짧은 수명의 플로우와 관련된 "불필요한 작업"을 제거하는 데 도움을 주기 위해 TCP 연결에 대해 클러스터 복제 지연을 활성화합니다. 관리자/백업 플로우가 생성되기 전에 유닛에서 장애가 발생하는 경우, 이러한 플로우는 복구될 수 없습니다. 마찬가지로 플로우가 생성되기 전에 트래픽이 다른 유닛으로 리밸런싱되며 플로우는 복구될 수 없습니다. TCP 임의 설정을 비활성화한 트래픽에 대해 TCP 복제 지연을 활성화하지 않아야 합니다.

프로시저

단계 **1** TCP 연결에 대해 클러스터 복제 지연을 활성화합니다.

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

예제**:**

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

1~15 범위의 초를 설정합니다. **http** 지연은 기본적으로 5초 동안 활성화됩니다.

다중 상황 모드에서 상황 내에 이 설정을 구성합니다.

단계 **2** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

단계 **3** (선택 사항) TCP 트래픽을 위해 연결 재밸런싱을 활성화합니다.

conn-rebalance [**frequency** *seconds*]

예제**:**

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

이 명령은 기본적으로 비활성화되어 있습니다. 활성화할 경우 ASA에서는 로드 정보를 주기적으로 교환하며, 로드가 과중한 디바이스에서 적은 디바이스로 새 연결을 오프로드합니다. 빈도는 1에서 360초 사이이며, 로드 정보를 교환하는 빈도를 지정합니다. 기본값은 5일입니다.

사이트 간 토폴로지에 대한 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 대한 연결이 리밸런싱됩니다.

사이트 간 기능 구성

사이트 간 클러스터링의 경우, 구성을 맞춤화하여 이중화 및 안정성을 개선할 수 있습니다.

관리자 현지화 활성화

데이터 센터에 대한 사이트 간 클러스터링을 위해 성능을 개선하고 왕복 시간 레이턴시를 줄이기 위해 관리자 현지화를 활성화할 수 있습니다. 새로운 연결은 일반적으로 로드 밸런싱 상태이며 지정된 사이트 내부의 클러스터 멤버가 소유합니다. 그러나 ASA는 모든 사이트에서 멤버에 관리자 역할을 할당합니다. 관리자 현지화를 사용하면 추가 관리자 역할이 활성화됩니다. 즉, 소유자와 동일한 사이트의 로컬 관리자와 모든 사이트의 전역 관리자 역할이 활성화됩니다. 소유자와 관리자를 동일한 사이트에서 유지하면 성능이 향상됩니다. 또한 원래 소유자가 실패할 경우, 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다. 전역 관리자는 클러스터 멤버가 다른 사이트에서 소유하는 연결에 대한 패킷을 수신하는 경우 사용됩니다.

시작하기 전에

- 부트스트랩 구성에서 클러스터 멤버에 대한 사이트 ID를 설정합니다.
- NAT 또는 PAT 트래픽, SCTP에서 검사된 트래픽, 단편화 소유자 쿼리 등의 트래픽 유형은 현지화를 지원하지 않습니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

단계 **2** 관리자 현지화를 활성화합니다.

director-localization

사이트 이중화 활성화

사이트 장애로부터 플로우를 보호하기 위해 사이트 이중화를 활성화할 수 있습니다. 연결 백업 소유자가 소유자와 같은 사이트에 있으면 사이트 장애로부터 플로우를 보호하기 위해 다른 사이트에서 추가 백업 소유자가 선택됩니다.

시작하기 전에

- 부트스트랩 구성에서 클러스터 멤버에 대한 사이트 ID를 설정합니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

단계 **2** 사이트 이중화를 활성화합니다.

site-redundancy

클러스터 플로우 모빌리티 구성

서버가 사이트 간에 이동하는 경우 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

LISP 검사 정보

사이트 간에 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

LISP 정보

VMware VMotion과 같은 데이터 센터 가상 머신 모빌리티를 통해 서버는 클라이언트에 대한 연결을 유지하면서 데이터 센터 간에 데이터를 마이그레이션할 수 있습니다. 그러한 데이터 센터 서버 모빌리티를 지원하려면 라우터는 이동 시 서버에 대한 인그레스 경로를 업데이트할 수 있어야 합니다. Cisco LISP(Locator/ID Separation Protocol) 아키텍처는 디바이스 ID 또는 EDI(endpoint identifier)를 해당 위치 또는 RLOC(routing locator)에서 두 개의 서로 다른 숫자 공간으로 분리하여, 서버 마이그레이션을 클라이언트에 투명하게 만듭니다. 예를 들어 서버가 새 사이트로 이동하고 클라이언트가 서버로 트래픽을 전송하면, 라우터가 트래픽을 새 위치로 리디렉션합니다.

LISP에는 LISP ETR(egress tunnel router), ITR(ingress tunnel router), FHR(first hop router), MR(map resolver), MS(map server) 같은 특정 역할의 라우터 및 서버가 필요합니다. 서버에 대한 FHR(first hop router)은 서버가 다른 라우터에 연결된 것을 감지하면, 클라이언트에 연결된 ITR이 트래픽을 가로채고 캡슐화하여 새로운 서버 위치로 전송할 수 있도록 다른 모든 라우터 및 데이터베이스를 업데이트합니다.

ASA LISP 지원

ASAASAASA는 LISP 자체를 실행하지 않습니다. 그러나 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작동을 위해 이 정보를 사용할 수 있습니다. LISP 통합이 없으면 서버가 새 사이트로 이전할 경우, 원래의 플로우 소유자 대신 새 사이트의 ASA 클러스터 멤버로 트래픽이 전달됩니다. 새 ASA가 트래픽을 이전 사이트의 ASA로 전달하면, 이전 ASA는 서버에 도달하기 위해 트래픽을 다시 새 사이트로 전송합니다. 이 트래픽 플로우는 차선책이며, "tromboning" 또는 hair-pinning"으로 알려져 있습니다.

LISP 통합 시 ASA 클러스터 멤버는 FHR(first hop router)과 ETR 또는 ITR 간에 전달되는 LISP 트래픽을 검사할 수 있으며, 그런 다음 플로우 소유자가 새 사이트에 있도록 변경할 수 있습니다.

LISP 지침

- ASA 클러스터 멤버는 FHR과 사이트의 ITR 또는 ETR 사이에 상주해야 합니다. ASA 클러스터 자체는 확장 세그먼트의 FHR이 될 수 없습니다.
- 완전히 분산된 플로우만 지원됩니다. 중앙 집중식 플로우, 반 분산 플로우 또는 개별 유닛에 속한 플로우는 새 소유자로 이동하지 않습니다. 반 분산 플로우에는, 상위 플로우를 소유하는 동일한 ASA가 모든 하위 플로우도 소유하는 SIP 같은 애플리케이션이 포함됩니다.
- 클러스터는 계층 3 및 4 플로우 상태만 이동하므로, 일부 애플리케이션 데이터가 손실될 수 있습니다.
- 수명이 짧은 플로우 또는 비즈니스 크리티컬 플로우의 경우 소유자를 이동하는 것이 의미가 없을 수 있습니다. 검사 정책을 구성할 때 이 기능으로 지원되는 트래픽의 유형을 제어할 수 있으며, 플로우 모빌리티를 필수 트래픽으로 제한해야 합니다.

ASA LISP 구현

이 기능에는 몇 가지 상호 연결된 구성이 포함됩니다(모두 이 장에서 설명).

1. (선택 사항) Limit inspected EIDs based on the host or server IP address(호스트 또는 서버 IP 주소를 기반으로 검사된 EID 제한) - FHR(first hop router)은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EDI를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개뿐이지만 LISP가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다.
2. LISP traffic inspection(LISP 트래픽 검사) - ASA는 FHR(first hop router)과 ITR 또는 ETR 간에 EID-notify 메시지를 보낼 수 있도록 UDP 포트 4342에서 LISP 트래픽을 검사합니다. ASA는 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 보수합니다. 예를 들면, FHR(first hop router)의 소스 IP 주소 및 ITR 또는 ETR의 목적지 주소로 LISP 트래픽을 검사해야 합니다. LISP 트래픽에는 관리자가 할당되지 않으며, LISP 트래픽 자체는 클러스터 상태 공유에 참여하지 않습니다.

3. Service Policy to enable flow mobility on specified traffic(지정된 트래픽에서 플로우 모빌리티 활성화를 위한 서비스 정책) - 비즈니스 크리티컬 트래픽에서 플로우 모빌리티를 활성화해야 합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다.
4. Site IDs(사이트 ID) - ASA는 각 클러스터 유닛에 대해 사이트 ID를 사용하여 새로운 소유자를 확인합니다.
5. Cluster-level configuration to enable flow mobility(플로우 모빌리티 활성화를 위한 클러스터 레벨 구성) - 또한 클러스터 레벨에서 플로우 모빌리티를 활성화해야 합니다. 이 켜기/끄기 토글을 사용하면 특정 클래스의 트래픽 또는 애플리케이션에 대한 플로우 모빌리티를 손쉽게 활성화 또는 비활성화할 수 있습니다.

LISP 검사 구성

서버가 사이트 간에 이동하는 경우 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

시작하기 전에

- 마스터 유닛 부트스트랩 설정 구성, 400 페이지 및 슬레이브 유닛 부트스트랩 설정 구성, 405 페이지에 따라 각 클러스터 유닛을 사이트 ID에 할당합니다.
- LISP 트래픽은 기본 검사 트래픽 클래스에 포함되지 않으므로 이 절차를 수행하는 중에 LISP 트래픽에 대해 별도의 클래스를 구성해야 합니다.

프로시저

단계 **1** (선택 사항) IP 주소를 기반으로 하는 검사된 EID로 제한하고 LISP 사전 공유 키를 구성하려면 다음과 같이 LISP 검사 맵을 구성합니다.

a) 확장된 ACL을 생성합니다. 대상 IP 주소만 EID 임베디드 주소와 일치합니다.

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

IPv4 및 IPv6 ACL이 모두 허용됩니다. 정확한 **access-list extended** 구문에 대한 명령 참조를 참고합니다.

b) LISP 검사 맵을 생성하고 파라미터 모드로 진입합니다.

policy-map type inspect lisp *inspect_map_name*

parameters

c) 생성한 ACL을 식별하여 허용되는 EID를 정의합니다.

allowed-eid access-list *eid_acl_name*

FHR(first hop router) 또는 ITR/ETR은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EID를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개뿐이지만 LISP

가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다.

d) 필요한 경우, 사전 공유 키를 입력합니다.

validate-key *key*

예제:

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

단계 **2** 포트 4342에서 FHR(first hop router) 및 ITR/ETR 간에 UDP 트래픽에 대한 LISP 검사를 구성합니다.

a) LISP 트래픽을 식별하기 위해 확장된 ACL을 구성합니다.

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

UDP 포트 4342를 지정해야 합니다. IPv4 및 IPv6 ACL이 모두 수락됩니다. 정확한 **access-list extended** 구문에 대한 명령 참조를 참고합니다.

b) ACL에 대한 클래스 맵을 생성합니다.

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) 정책 맵, 클래스 맵을 지정하고 선택적 LISP 검사 맵을 사용하여 검사를 활성화하고 인터페이스(새 인터페이스인 경우)에 서비스 정책을 적용합니다.

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

기존 서비스 정책이 있으면 기존 정책 맵 이름을 지정합니다. 기본적으로 ASA에는 **global_policy**라고 하는 전역 정책이 포함되어 있으므로 전역 정책에 해당 이름을 지정합니다. 정책을 전역적으로 적용하지 않으려는 경우 인터페이스별로 하나의 서비스 정책을 생성할 수도 있습니다. LISP 검사는 트래픽에 양방향으로 적용되므로 소스 및 대상 인터페이스 모두에서 서비스 정책을 적용할 필요가 없습니다. 트래픽이 양쪽 방향의 클래스 맵과 일치할 경우 정책 맵을 적용하는 인터페이스로 들어가거나 나가는 모든 트래픽이 영향을 받습니다.

예제:

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
```

```
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASA에서는 FHR(first hop router)과 ITR/ETR 간에 EID-notify 메시지를 보낼 수 있도록 LISP 트래픽을 검사합니다. ASA는 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 관리합니다.

단계 **3** 트래픽 클래스에 대한 플로우 모빌리티를 활성화합니다.

a) 서버에서 사이트를 변경하는 경우 가장 최적의 사이트에 다시 할당하려는 비즈니스 크리티컬 트래픽을 식별하기 위해 확장된 ACL을 구성합니다.

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

IPv4 및 IPv6 ACL이 모두 수락됩니다. 정확한 **access-list extended** 구문에 대한 명령 참조를 참고합니다. 비즈니스 크리티컬 트래픽에서 플로우 모빌리티를 활성화해야 합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다.

b) ACL에 대한 클래스 맵을 생성합니다.

class-map *flow_map_name*

match access-list *flow_acl_name*

c) LISP 검사가 활성화되어 있는 동일한 정책 맵인 플로우 클래스 맵을 지정하고 플로우 모빌리티를 활성화합니다.

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

예제:

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

단계 **4** 클러스터 그룹 구성 모드로 들어가고 클러스터에 대한 플로우 모빌리티를 활성화합니다.

cluster group *name*

flow-mobility lisp

이 켜기/끄기 토글을 사용하면 플로우 모빌리티를 손쉽게 활성화 또는 비활성화할 수 있습니다.

예

다음 예에서는

- 10.10.10.0/24 네트워크에서의 EID 제한

- 192.168.50.89(내부)에서의 LISP 라우터와 192.168.10.8에서 다른 ASA 인터페이스에 있는 ITR/ETR 라우터 간의 LISP 트래픽(UDP 4342) 검사
- 10.10.10.0/24에서 HTTPS를 사용하여 서버로 이동하는 모든 내부 트래픽에 대한 플로우 모빌리티를 활성화합니다.
- 클러스터에 대한 플로우 모빌리티를 활성화합니다.

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

클러스터 멤버 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 멤버를 관리할 수 있습니다.

멤버 비활성화

클러스터의 멤버를 비활성화하려면, 클러스터링 컨피그레이션은 그대로 유지한 상태로 유닛의 클러스터링을 비활성화합니다.

참고 수동으로 또는 상태 확인 장애를 통해 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 유닛을 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우(예를 들어, 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

- 콘솔 포트를 사용해야 합니다. 원격 CLI 연결에서는 클러스터링을 활성화하거나 비활성화할 수 없습니다.
- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group pod1
```

단계 **2** 클러스터링을 비활성화합니다.

no enable

이 유닛이 마스터 유닛이었던 경우, 새 마스터가 선택되며 다른 멤버가 마스터 유닛이 됩니다.

클러스터 컨피그레이션은 그대로 유지되므로 클러스터링을 나중에 다시 활성화할 수 있습니다.

마스터 유닛의 멤버

유닛에서 멤버를 비활성화하려면 다음 단계를 수행합니다.

참고 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 유닛을 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우(예를 들어, 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.

프로시저

클러스터에서 유닛을 제거합니다.

cluster remove unit *unit_name*

예제**:**

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

부트스트랩 구성과 마스터 유닛에서 동기화한 마지막 구성도 그대로 유지되므로 나중에 구성을 잃지 않고 다시 유닛을 추가할 수 있습니다. 슬레이브 유닛에 이 명령을 입력하여 마스터 유닛을 제거할 경우 새 마스터 유닛이 선택됩니다.

멤버 이름을 보려면 **cluster remove unit ?**을 입력하거나 **show cluster info** 명령을 입력합니다.

클러스터 다시 참가

유닛이 클러스터에서 제거된 경우, 예를 들어 실패한 인터페이스의 경우 또는 멤버를 수동으로 비활성화한 경우, 클러스터를 수동으로 다시 조인해야 합니다.

시작하기 전에

- 클러스터링을 다시 활성화하려면 콘솔 포트를 사용해야 합니다. 다른 인터페이스는 종료됩니다.
- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.
- 클러스터를 다시 조인하기 전에 장애가 해결되었는지 확인하십시오.

프로시저

단계 **1** 콘솔에서 클러스터 구성 모드를 시작합니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group pod1
```

단계 **2** 클러스터링을 활성화합니다.

enable

클러스터 벗어나기

클러스터를 모두 벗어나려는 경우, 전체 클러스터 부트스트랩 컨피그레이션을 제거해야 합니다. 각 멤버에 대한 현재 구성이 동일하므로(기본 유닛에서 동기화됨), 클러스터를 벗어날 경우 백업에서 사전 클러스터링 구성을 복원하거나, IP 주소 충돌을 피하기 위해 구성을 지우고 처음부터 다시 시작하게 됩니다.

시작하기 전에

콘솔 포트를 사용해야 합니다. 클러스터 구성을 제거하면 관리 인터페이스 및 클러스터 제어 링크를 비롯한 모든 인터페이스가 종료됩니다. 또한 원격 CLI 연결에서는 클러스터링을 활성화하거나 비활성화할 수 없습니다.

프로시저

단계 **1** 보조 유닛의 클러스터링을 비활성화합니다.

cluster group *cluster_name* **no enable**

예제**:**

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

보조 유닛에 클러스터링이 활성화되어 있는 동안에는 구성을 변경할 수 없습니다.

단계 **2** 클러스터 컨피그레이션을 지웁니다.

clear configure cluster

ASA에서는 관리 인터페이스 및 클러스터 제어 링크를 비롯한 모든 인터페이스를 종료합니다.

단계 **3** 클러스터 인터페이스 모드를 비활성화합니다.

no cluster interface-mode

모드는 컨피그레이션에 저장되지 않으며 수동으로 재설정해야 합니다.

단계 **4** 백업 컨피그레이션이 있을 경우, 실행 중인 컨피그레이션에 백업 컨피그레이션을 복사합니다.

copy *backup_cfg* **running-config**

예제**:**

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?
```

```
Destination filename [running-config]?
ciscoasa(config)#
```

단계 **5** 시작에 컨피그레이션을 저장합니다.

write memory

단계 **6** 백업 컨피그레이션이 없는 경우 관리 액세스를 다시 컨피그레이션합니다. 인터페이스 IP 주소를 변경하고 이를테면 올바른 호스트 이름을 복원해야 합니다.

마스터 유닛 변경

주의 마스터 유닛을 변경하는 가장 좋은 방법은 마스터 유닛의 클러스터링을 비활성화한 후 새 마스터가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 마스터 유닛이 될 정확한 유닛을 지정해야 할 경우, 이 섹션을 절차를 사용하십시오. 그러나 중앙 집중식 기능의 경우 이 절차를 통해 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

마스터 유닛을 변경하려면 다음 단계를 수행합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.

프로시저

새 유닛을 마스터 유닛으로 설정합니다.

cluster master unit *unit_name*

예제**:**

```
ciscoasa(config)# cluster master unit asa2
```

기본 클러스터 IP 주소에 다시 연결해야 합니다.

멤버 이름을 보려면 **cluster master unit ?**을 입력하거나 (현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.

클러스터 전체에서 명령 실행

클러스터의 모든 멤버 또는 특정 멤버에 명령을 보내려면 다음 단계를 수행합니다. 모든 멤버에 **show** 명령을 보내면 모든 출력이 수집되고 해당 내용이 현재 유닛의 콘솔에 표시됩니다. **capture** 및 **copy** 같은 다른 명령의 경우 클러스터 전체 실행을 활용할 수도 있습니다.

프로시저

모든 멤버 또는 유닛 이름을 지정한 경우 특정 멤버에 명령을 전송합니다.

cluster exec [**unit** *unit_name*] *command*

예제**:**

```
ciscoasa# cluster exec show xlate
```

멤버 이름을 보려면 **cluster exec unit ?**을 입력하거나 (현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.

예

클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 다음 명령을 마스터 유닛에 입력합니다.

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일의 이름 뒤에는 유닛 이름이 자동으로 연결되며 capture1_asa1.pcap, capture1_asa2.pcap 같은 형식이 됩니다. 이 예에서 asa1 및 asa2는 클러스터 유닛 이름 입니다.

cluster exec show port-channel 요약 명령에 대한 다음 샘플 출력에는 클러스터의 각 멤버에 대한 EtherChannel 정보가 나와 있습니다.

```
ciscoasa# cluster exec show port-channel summary
master(LOCAL):**************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

ASA 클러스터 모니터링

클러스터의 상태 및 연결을 모니터링하고 문제를 해결할 수 있습니다.

클러스터 상태 모니터링

클러스터 상태 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show cluster info** [**health** [**details**]]

  키워드가 없는 경우 **show cluster info** 명령을 사용하면 클러스터의 모든 멤버 상태가 표시됩니다.

  show cluster info health 명령을 사용하면 인터페이스, 유닛, 클러스터 전반의 현재 상태가 표시됩니다. **details** 키워드를 사용하면 숫자 하트비트 메시지 장애가 표시됩니다.

  show cluster info 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
```

```
Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  시간 지연 이후에 클러스터 유닛이 자동으로 클러스터에 다시 참가하는지 여부 및 장애 상태(예: 라이선스 대기 중, 섀시 상태 검사 장애)가 해결되었는지 여부를 표시합니다. 유닛이 영구적으로 비활성화된 경우 또는 유닛이 이미 클러스터에 있는 경우, 이 명령을 사용해도 출력이 표시되지 않습니다.

  show cluster info auto-join 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport** {**asp** | **cp** [**detail**]}

  다음에 대한 전송 관련 통계를 표시합니다.

  - **asp** — 데이터 평면 전송 통계입니다.
  - **cp** — 제어 평면 전송 통계입니다.

    detail 키워드를 입력하는 경우, 클러스터의 신뢰할 수 있는 전송 프로토콜 사용량을 볼 수 있어 버퍼가 제어 평면에서 가득 찬 경우 패킷 삭제 문제를 식별할 수 있습니다. **show cluster info transport cp detail** 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
```

```
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
--------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0
```

```
    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

```
MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  클러스터 내역을 표시합니다.

클러스터 전체 패킷 캡처

클러스터의 패킷을 캡처하는 방법에 대한 내용은 다음 명령을 참조하십시오.

cluster exec capture

클러스터 전체의 문제를 해결하기 위해 **cluster exec capture** 명령을 사용하여 마스터 유닛에서 클러스터별 트래픽의 캡처를 활성화할 수 있습니다. 이 경우 클러스터의 모든 슬레이브 유닛에서 캡처가 자동으로 활성화됩니다.

클러스터 리소스 모니터링

클러스터 리소스 모니터링에 대한 내용은 다음 명령을 참조하십시오.

show cluster {**cpu** | **memory** | **resource**} [*options*]

전체 클러스터에 대한 집계된 데이터를 표시합니다. 사용 가능한 옵션은 데이터 유형에 따라 달라집니다.

클러스터 트래픽 모니터링

클러스터 트래픽 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show conn [detail], cluster exec show conn**

  show conn 명령을 사용하면 흐름이 관리자, 백업 또는 전달자 흐름인지 보여 줍니다. 유닛에 **cluster exec show conn** 명령을 사용하여 모든 연결을 볼 수 있습니다. 이 명령을 사용하면 클러스터의 다른 ASA에 단일 플로우에 대한 트래픽이 어떤 방식으로 도착하는지가 표시될 수 있습니다. 클러스터의 처리량은 로드 밸런싱의 효율성과 구성에 따라 달라집니다. 이 명령을 사용하면 연결에 대한 트래픽 흐름이 클러스터를 통해 어떻게 이루어지는지 손쉽게 볼 수 있으며, 로드 밸런서가 이 흐름의 성능에 어떤 영향을 미치는지 파악하는 데 유용합니다.

  show conn detail 명령을 사용하면 플로우 모빌리티의 영향을 받는 플로우도 표시됩니다.

  다음은 **show conn detail** 명령의 샘플 출력입니다.

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

연결 흐름 문제를 해결하려면, 유닛에 **cluster exec show conn** 명령을 입력하여 모든 유닛에 대한 연결을 우선 확인해야 합니다. 디렉터(Y), 백업(y) 및 전달자(z) 플래그가 있는 흐름을 확인합니다. 다음 예는 세 ASA 모두에 대한 172.18.124.187:22와 192.168.103.131:44727 간의 SSH 연결을 보여 줍니다. ASA 1에는 연결의 전달자임을 나타내는 z 플래그가 있고, ASA3에는 연결의 디렉터임을 나타내는 Y 플래그가 있으며, ASA2에는 특별한 플래그가 없어 소유자임을 나타냅니다. 아웃바운드 방향에서 이 연결의 패킷은 ASA2의 내부 인터페이스로 들어가 외부 인터페이스를 나갑니다. 인바운드 방향에서 이 연결의 패킷은 ASA1 및 ASA3의 외부 인터페이스로 들어가 클러스터 제어 링크를 통해 ASA2로 전달된 다음 ASA2의 내부 인터페이스를 나갑니다.

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:************************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
```

```
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution 및 **show cluster info packet-distribution** 명령을 사용하면 모든 클러스터 유닛 전체의 트래픽 분포가 표시됩니다. 이러한 명령은 외부 로드 밸런서를 평가하고 조정하는 데 유용합니다.

  show cluster info loadbalance 명령을 사용하면 연결 리밸런싱 통계가 표시됩니다.

  show cluster info flow-mobility counters 명령을 사용하면 EID 이동과 플로우 소유자 이동 정보가 표시됩니다. **show cluster info flow-mobility counters** 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  전체 클러스터에 대한 집계된 데이터를 표시합니다. 사용 가능한 옵션은 데이터 유형에 따라 달라집니다.

  show cluster access-list 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
```

```
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

모든 디바이스에서 사용 중인 연결의 집계된 수를 표시하려면 다음을 입력합니다.

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*****************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:*************************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  이 명령은 데이터 경로 문제를 해결하는 데 유용합니다.

클러스터 라우팅 모니터링

클러스터 라우팅에 대한 내용은 다음 명령을 참조하십시오.

- **show route cluster**
- **debug route cluster**

  라우팅에 대한 클러스터 정보를 표시합니다.

- **show lisp eid**

  EID 및 사이트 ID를 보여주는 ASA EID 테이블을 표시합니다.

  cluster exec show lisp eid 명령의 다음 출력을 참조하십시오.

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):*************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
```

```
11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  이 명령은 트러블슈팅에 유용합니다.

클러스터링의 로깅 구성

클러스터링의 로깅 구성에 대한 내용은 다음 명령을 참조하십시오.

logging device-id

클러스터의 각 유닛에서는 syslog 메시지를 독립적으로 생성합니다. **logging device-id** 명령을 사용하면 디바이스 ID가 동일하거나 다른 syslog 메시지를 생성하여 클러스터의 동일한 또는 다른 유닛에서 메시지가 표시되도록 할 수 있습니다.

클러스터 인터페이스 모니터링

클러스터 인터페이스 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show cluster interface-mode**

  클러스터 인터페이스 모드를 표시합니다.

- **show port-channel**

  포트 채널이 스팬인지 여부에 대한 정보가 포함됩니다.

- **show lacp cluster {system-mac | system-id}**

  cLACP 시스템 ID 및 우선순위가 표시됩니다.

- **debug lacp cluster [all | ccp | misc | protocol]**

  cLACP에 대한 디버그 메시지가 표시됩니다.

- **show interface**

  사용 중인 사이트 MAC 주소의 사용법을 표시합니다.

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

클러스터링 디버깅

클러스터링 디버깅에 대한 내용은 다음 명령을 참조하십시오.

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  클러스터링에 대한 디버그 메시지가 표시됩니다.

- **debug cluster flow-mobility**

  클러스터링 플로우 모빌리티와 관련된 이벤트를 표시합니다.

- **debug lisp eid-notify-intercept**

  eid-notify 메시지가 차단된 경우 이벤트를 표시합니다.

- **show cluster info trace**

  show cluster info trace 명령을 사용하면 추가적인 문제 해결을 위한 디버깅 정보가 표시됩니다.

  show cluster info trace 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

ASA 클러스터링의 예

이러한 예에는 일반적인 구축을 위한 모든 클러스터 관련 ASA 구성이 포함되어 있습니다.

샘플 ASA 및 스위치 구성

다음 샘플 컨피그레이션에서는 ASA와 스위치 간에 다음과 같은 인터페이스를 연결합니다.

ASA 인터페이스	스위치 인터페이스
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

ASA 컨피그레이션

각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 컨피그레이션

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 슬레이브 부트스트랩 컨피그레이션

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-slave
```

마스터 인터페이스 컨피그레이션

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
```

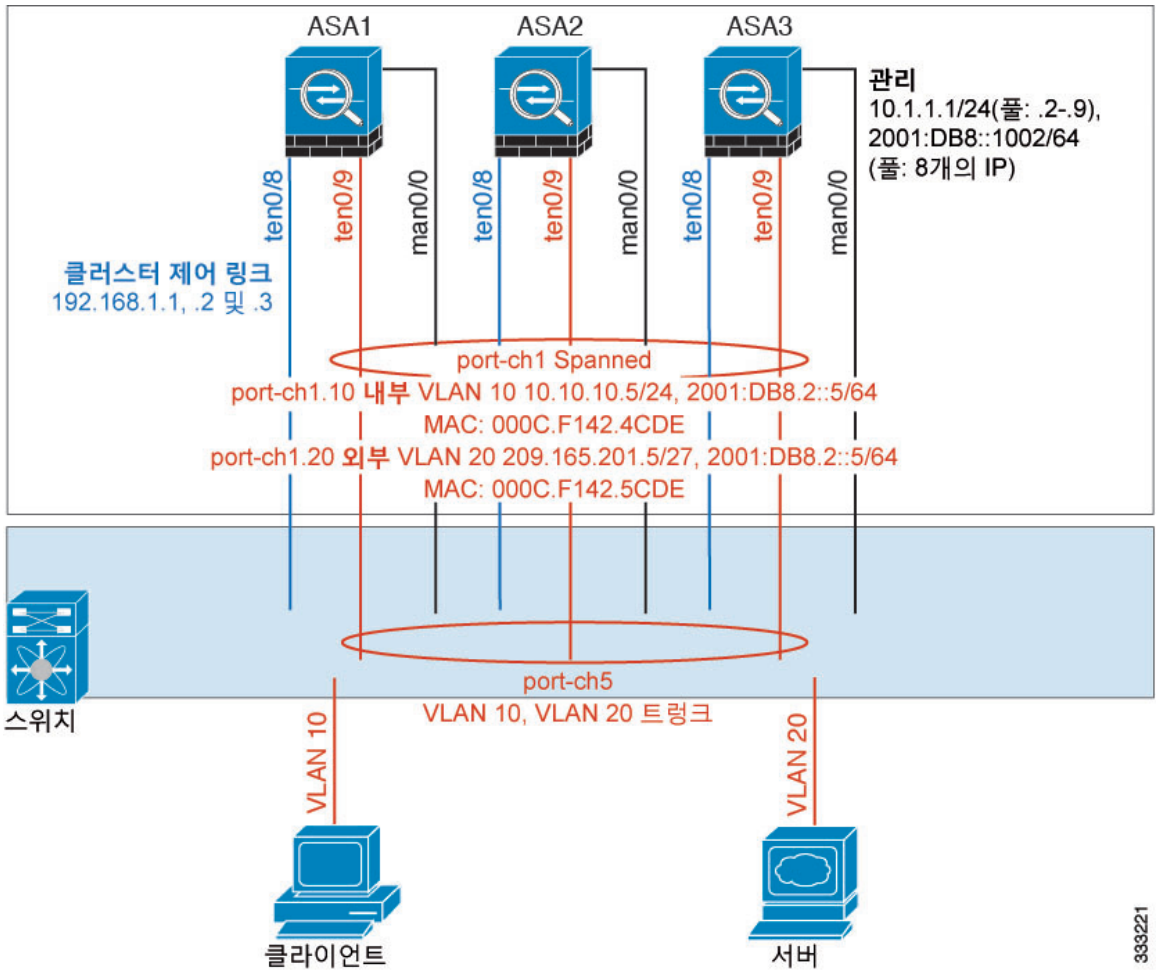
```
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 11 mode active
 no shutdown
!
interface Management0/0
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Cisco IOS 스위치 구성

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access
```

```
interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

단일화된 방화벽



서로 다른 보안 도메인의 데이터 트래픽은 서로 다른 VLAN에 연결됩니다. 예를 들어, VLAN 10은 내부 네트워크용이고 VLAN 20은 외부 네트워크용입니다. 각 ASA에는 외부 스위치 또는 라우터에 연결된 하나의 물리적 포트가 있습니다. 트렁킹이 활성화되어 있으므로 물리적 링크의 모든 패킷은 캡슐화된 802.1q입니다. ASA는 VLAN 10과 VLAN 20 사이의 방화벽입니다.

스팬 EtherChannel을 사용할 경우, 모든 데이터 링크가 스위치 측의 단일한 EtherChannel로 그룹화됩니다. ASA를 사용할 수 없게 될 경우, 스위치에서 나머지 유닛 간의 트래픽을 리밸런싱합니다.

각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa1
cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 슬레이브 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa2
cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ASA3 슬레이브 부트스트랩 컨피그레이션

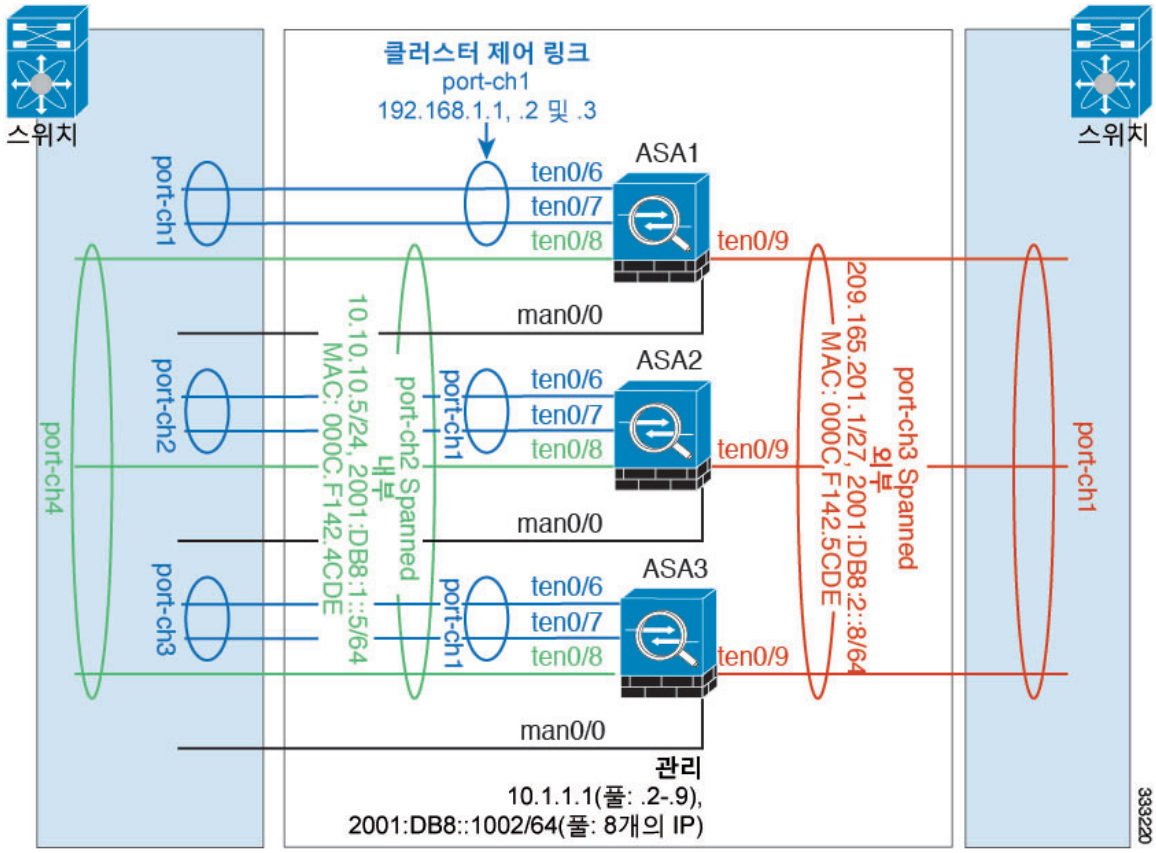
```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa3
cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

마스터 인터페이스 컨피그레이션

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8
interface management 0/0

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
```

```
no shutdown

interface tengigabitethernet 0/9

channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

트래픽 분리



내부 네트워크와 외부 네트워크 간의 트래픽을 물리적으로 분리하려는 경우가 있습니다.

위의 다이어그램에 표시된 것과 같이, 왼쪽에는 내부 스위치에 연결되는 스팬 EtherChannel이 하나 있고 오른쪽에는 외부 스위치에 연결되는 스팬 EtherChannel이 있습니다. 필요한 경우 각 EtherChannel에 VLAN 하위 인터페이스를 생성할 수도 있습니다.

각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 슬레이브 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ASA3 슬레이브 부트스트랩 컨피그레이션

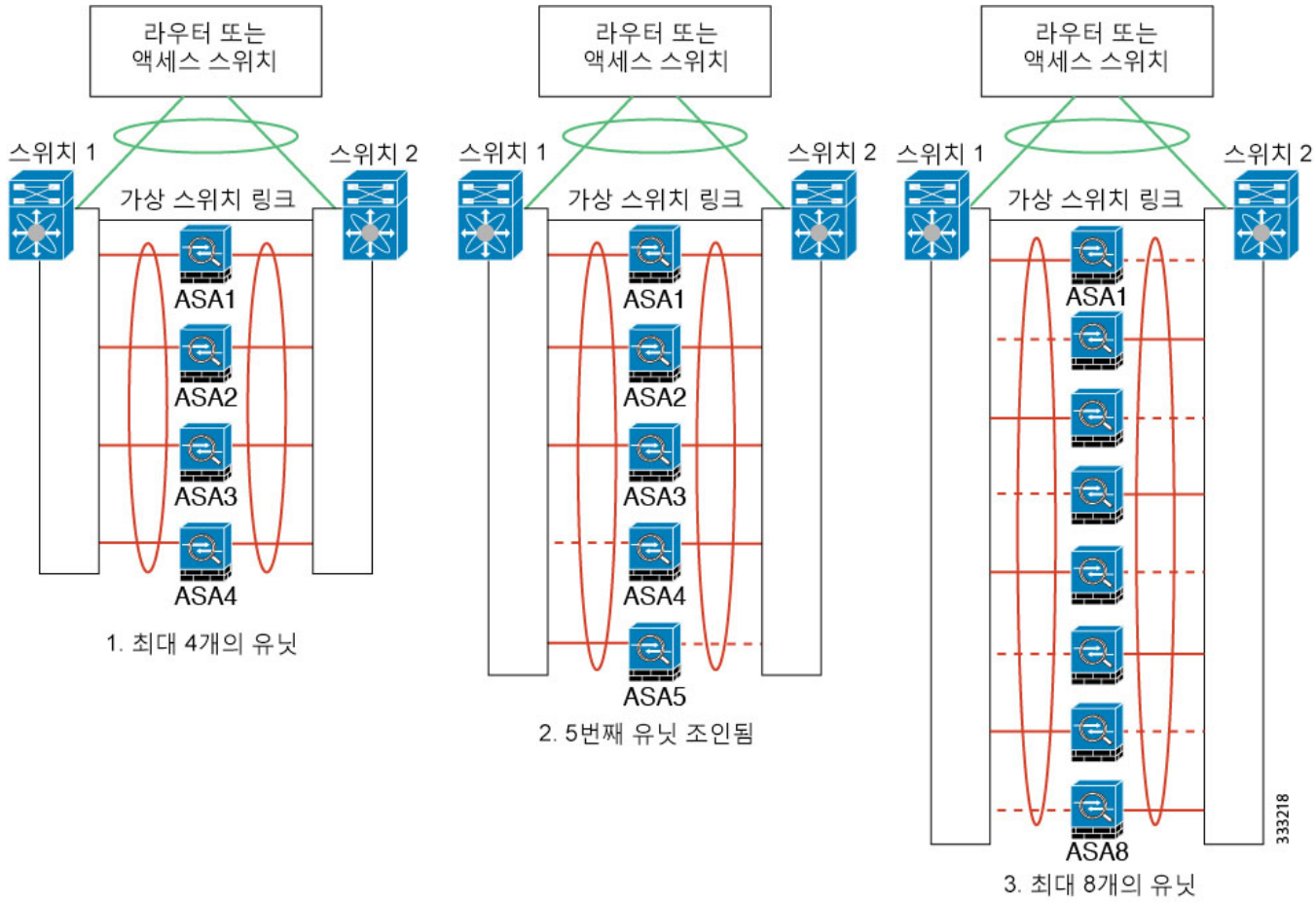
```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

마스터 인터페이스 컨피그레이션

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8
interface management 0/0

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface tengigabitethernet 0/8

channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9

channel-group 3 mode active
no shutdown
interface port-channel 3
port-channel span-cluster
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

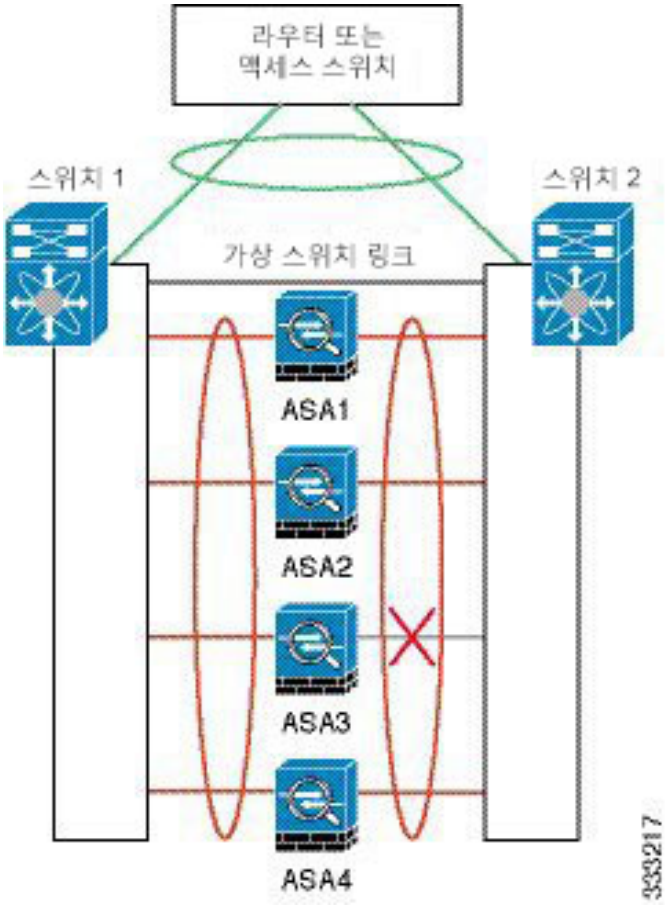
백업 링크가 포함된 스팬 EtherChannel(기존 8 액티브 포트/8 스탠바이)

기존 EtherChannel에서 활성 포트의 최대 개수는 스위치 측에서 8개로 제한됩니다. 8-ASA 클러스터가 있는 경우 유닛당 2개의 포트를 EtherChannel에 할당하며, 이렇게 하면 총 16개의 전체 포트 중 8개는 스탠바이 모드가 되어야 합니다. ASA에서는 LACP를 사용하여 어떤 링크를 액티브 또는 스탠바이 상태로 설정해야 하는지 협상을 수행합니다. VSS 또는 vPC를 사용하여 다중 스위치 EtherChannel을 활성화할 경우 스위치 간 이중화를 실현할 수 있습니다. ASA에서 모든 물리적 포트는 우선 슬롯 번호를 기준으로 순서가 지정된 다음 포트 번호를 기준으로 순서가 지정됩니다. 다음 그림에서 순서가 낮은 포트가 "마스터" 포트(예: GigabitEthernet 0/0)이고, 다른 포트가 "슬레이브" 포트(예: GigabitEthernet 0/1)입니다. 하드웨어 연결은 대칭을 이루어야 합니다. 모든 마스터 링크는 하나의 스위치에서 종료되어야 하며, 모든 슬레이브 링크는 VSS/vPC가 사용된 경우 다른 스위치에서 종료되어야 합니다. 다음 다이어그램에서는 클러스터에 참가하는 유닛의 수가 증가하여 링크의 총 개수가 증가할 경우 어떤 상황이 발생하는지 보여 줍니다.

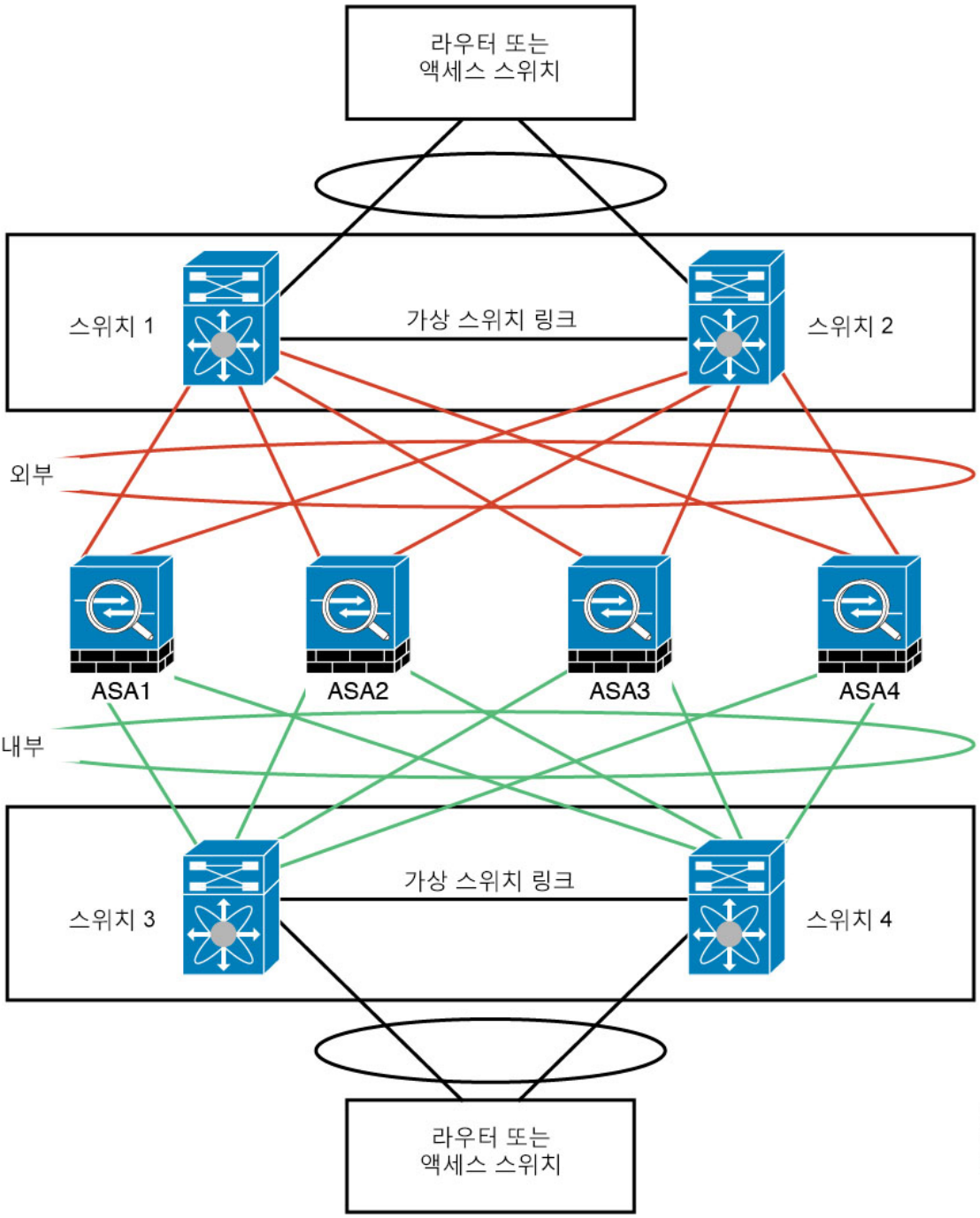


원칙은 우선 채널에 있는 액티브 포트의 수를 최대화하고, 그다음에는 액티브 마스터 포트의 수와 액티브 슬레이브 포트의 수가 균형을 이루도록 유지하는 것입니다. 클러스터에 5번째 유닛이 참가할 경우 모든 유닛 간의 트래픽이 균일하게 조정되지 않습니다.

링크 또는 디바이스 오류는 이와 동일한 원칙에 따라 처리됩니다. 또한 완벽하지 않은 로드 밸런싱 상황에 처하게 될 수 있습니다. 다음 그림에는 유닛 중 하나에 단일 링크 오류가 발생한 4-유닛 클러스터가 나와 있습니다.



네트워크에는 여러 개의 EtherChannel이 구성될 수 있습니다. 다음 다이어그램에는 내부의 EtherChannel과 외부의 EtherChannel이 나와 있습니다. 한쪽 EtherChannel의 마스터 및 슬레이브 링크에 모두 장애가 발생할 경우 클러스터에서 ASA가 제거됩니다. 이렇게 되면 외부 네트워크와 내부 네트워크의 연결이 이미 끊긴 경우, 외부 네트워크의 트래픽이 ASA에 전달되지 않습니다.



각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 슬레이브 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
```

```
key chuntheunavoidable
enable as-slave
```

ASA3 슬레이브 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

ASA4 슬레이브 부트스트랩 컨피그레이션

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL
```

```
cluster group cluster1

local-unit asa4
cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
priority 4
key chuntheunavoidable
enable as-slave
```

마스터 인터페이스 컨피그레이션

```
ip local pool mgmt 10.1.1.2-10.1.1.9
interface management 0/0

channel-group 2 mode active
no shutdown

interface management 0/1

channel-group 2 mode active
no shutdown
interface port-channel 2
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
security-level 100
management-only

interface tengigabitethernet 1/6

channel-group 3 mode active vss-id 1
no shutdown

interface tengigabitethernet 1/7

channel-group 3 mode active vss-id 2
no shutdown
interface port-channel 3
port-channel span-cluster vss-load-balance
nameif inside
ip address 10.10.10.5 255.255.255.0
mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8

channel-group 4 mode active vss-id 1
no shutdown

interface tengigabitethernet 1/9

channel-group 4 mode active vss-id 2
no shutdown
interface port-channel 4
port-channel span-cluster vss-load-balance
nameif outside
ip address 209.165.201.1 255.255.255.224
mac-address 000C.F142.5CDE
```

라우팅 모드 사이트 간 클러스터링을 위한 **OTV** 구성

Spanned EtherChannel의 라우팅 모드에 대한 사이트 간 클러스터링의 성공 여부는 적절한 구성 및 OTV의 모니터링에 달려 있습니다. OTV는 DCI를 통해 패킷을 전달함으로써 중요한 역할을 수행합니다. OTV는 전달 테이블에서 MAC 주소를 학습하는 경우에만 DCI를 통해 유니캐스트 패킷을 전달합니다. OTV 전달 테이블에서 MAC 주소를 학습하지 못하면 유니캐스트 패킷을 삭제합니다.

샘플 **OTV** 구성

```
//Sample OTV config:
//3151 – Inside VLAN, 3152 – Outside VLAN, 202 – CCL VLAN
//aaaa.1111.1234 – ASA inside interface global vMAC
//0050.56A8.3D22 – Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown
```

```
interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

사이트 장애 때문에 **OTV** 필터 수정 필요

사이트가 다운되면, 전역 MAC 주소를 더 이상 차단하지 않을 것이기 때문에 OTV에서 필터를 제거해야 합니다 몇 가지 추가 구성이 필요합니다.

작동하는 사이트의 OTV 스위치에서 ASA 전역 MAC 주소에 대한 정적 항목을 추가해야 합니다. 정적 항목을 추가하면 다른 쪽의 OTV는 오버레이 인터페이스에서 이러한 항목을 추가할 수 있습니다. 서버 및 클라이언트가 ASA에 대한 ARP 항목을 이미 가지고 있으면(기존 연결의 경우 그러함) ARP를 다시 전송하지 않을 것이므로 이 단계가 필요합니다. 따라서 OTV는 전달 테이블에서 ASA 전역 MAC 주소를 학습할 수 없게 됩니다. OTV는 전달 테이블에 전역 MAC 주소를 가지고 있지 않으며 OTV 설계 단위로 오버레이 인터페이스를 통해 유니 캐스트 패킷을 플러드하지 않을 것이므로, 서버에서 전역 MAC 주소로 보내는 유니캐스트 패킷이 삭제되고 기존 연결이 끊어집니다.

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

다른 사이트가 복원되면 필터를 다시 추가하고 OTV에서 이 정적 항목을 제거해야 합니다. 전역 MAC 주소에 대한 오버레이 항목을 지우려면 두 OTV에서 동적 MAC 주소 테이블을 지우는 것이 매우 중요합니다.

MAC 주소 테이블 지우기

사이트가 다운되고 전역 MAC 주소의 정적 항목이 OTV에 추가되면, 다른 OTV가 오버레이 인터페이스의 전역 MAC 주소를 학습하도록 해야 합니다. 다른 사이트가 나타나면 이러한 항목을 지워야 합니다. OTV의 전달 테이블에 이러한 항목이 없는지 확인하려면 MAC 주소 테이블을 지우십시오.

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP 캐시 모니터링

OTV는 OTV 인터페이스를 통해 학습한 IP 주소의 프록시 ARP에 대한 ARP 캐시를 유지 관리합니다.

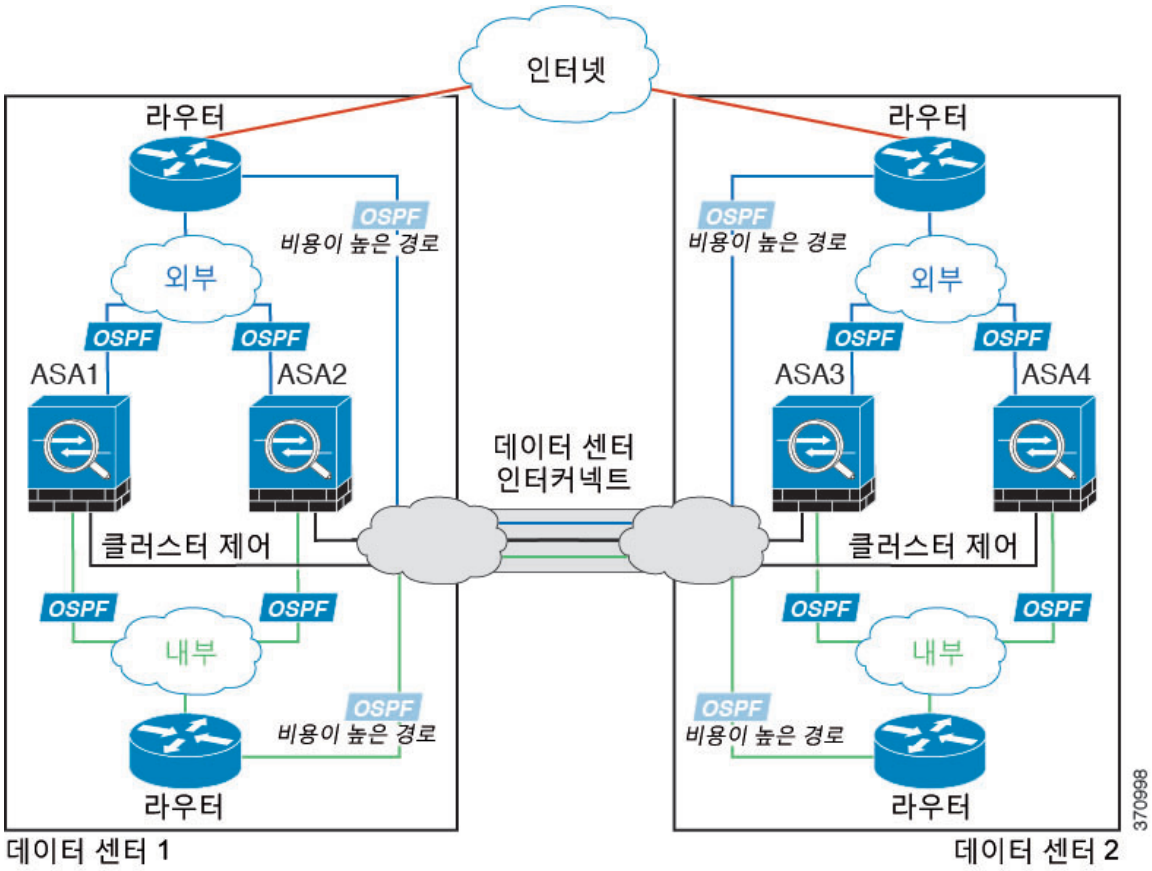
```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

사이트 간 클러스터링 예시

다음 예에는 지원되는 클러스터 구축에 대한 내용이 나와 있습니다.

개별 인터페이스 라우팅 모드 **North-South** 사이트 간 예

다음 예에서는 내부 라우터와 외부 라우터의 사이에 위치한(노스-사우스 삽입) 2개 데이터 센터 각각에 2개의 ASA 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 데이터 센터의 내부 및 외부 라우터에서는 OSPF와 PBR 또는 ECMP를 사용하여 클러스터 멤버 간의 트래픽을 로드 밸런싱합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 ASA 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. 어느 한 사이트의 모든 클러스터 멤버에 장애가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 ASA 클러스터 멤버로 이동합니다.



사이트별 MAC 및 IP 주소가 있는 Spanned EtherChannel 라우팅 모드의 예

다음 예에서는 게이트웨이 라우터와 각 사이트의 내부 네트워크 사이에 위치한(이스트-웨스트 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버를 보여줍니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부 네트워크용 Spanned EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 섀시를 포괄합니다.

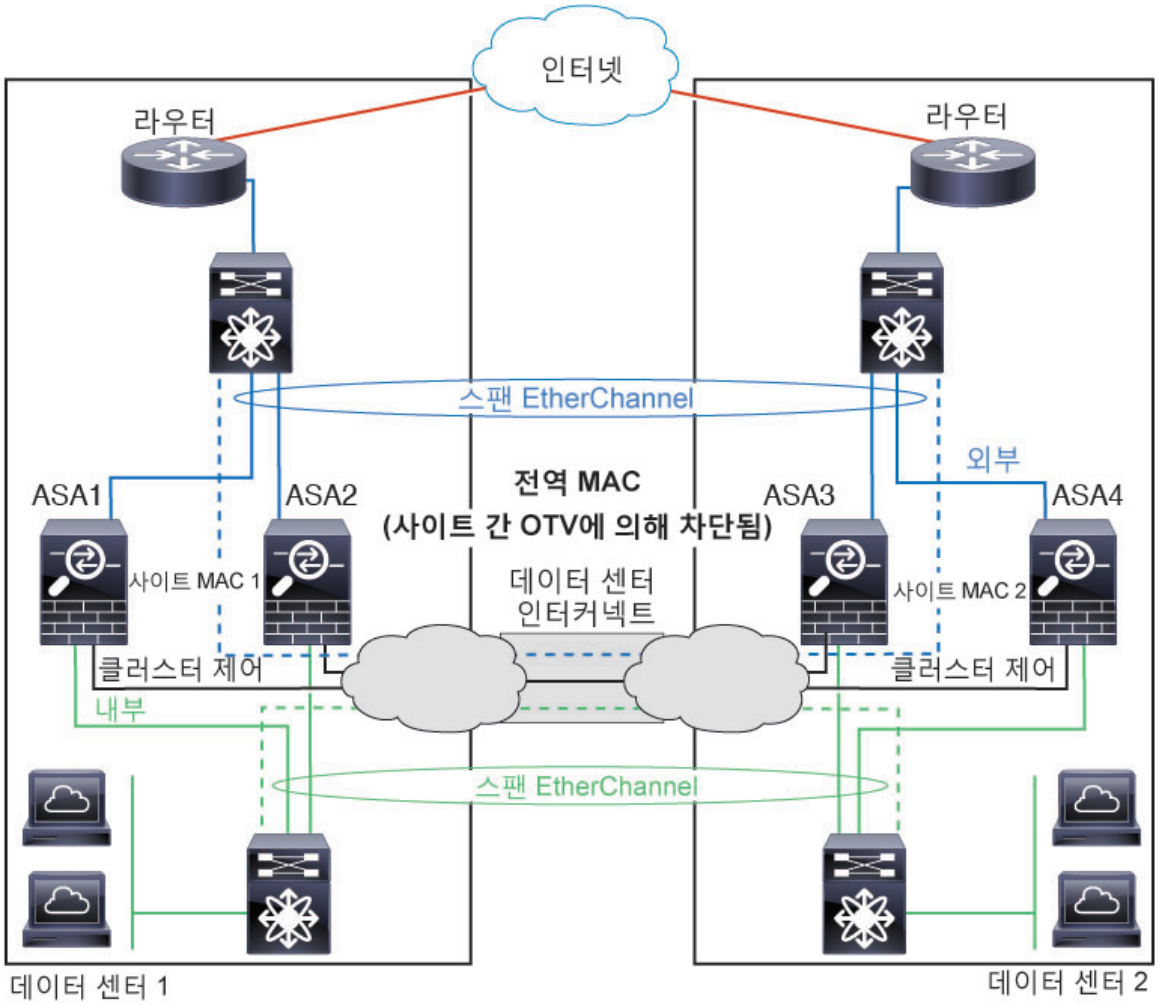
OTV(Overlay Transport Virtualization) 또는 이와 유사한 방법으로 데이터 VLAN이 사이트 전반에 확장됩니다. 트래픽이 클러스터로 향할 때 DCI를 통과하여 반대쪽 사이트에 가지 않도록 전역 MAC 주소를 차단하는 필터를 추가해야 합니다. 어떤 사이트의 클러스터 유닛이 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 유닛에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. VACL을 사용하여 전역 MAC 주소를 필터링해야 합니다.F3-Series 라인 카드가 포함된 Nexus 등 일부 스위치의 경우 전역 MAC 주소에서 ARP 패킷을 차단하려면 ARP 검사도 사용해야 합니다. ARP 검사를 수행하려면 ASA에서 사이트 MAC 주소와 사이트 IP 주소를 모두 설정해야 합니다. 사이트 MAC 주소만 구성하는 경우ARP 검사를 비활성화해야 합니다. 자세한 내용은 라우팅 모드 사이트 간 클러스터링을 위한 OTV 구성, 448 페이지를 참조하십시오.

클러스터는 내부 네트워크의 게이트웨이 역할을 합니다. 모든 클러스터 유닛에서 공유되는 전역 가상 MAC은 패킷 수신에만 사용됩니다. 발신 패킷은 각 DC 클러스터의 사이트별 MAC 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지

못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다.

이 시나리오에서:

- 클러스터에서 전송한 모든 이그레스(egress) 패킷은 사이트 MAC 주소를 사용하며 데이터 센터에서 지역화됩니다.
- 클러스터에 대한 모든 인그레스(ingress) 패킷은 전역 MAC 주소를 사용하여 전송되므로, 양 사이트의 어느 유닛에서나 수신할 수 있습니다. OTV의 필터는 데이터 센터 내에서 트래픽을 지역화합니다.



샘플 OTV 구성 및 모범 사례는 라우팅 모드 사이트 간 클러스터링을 위한 OTV 구성, 448 페이지 섹션을 참조하십시오.

Spanned EtherChannel 투명 모드 노스-사우스 사이트 간의 예

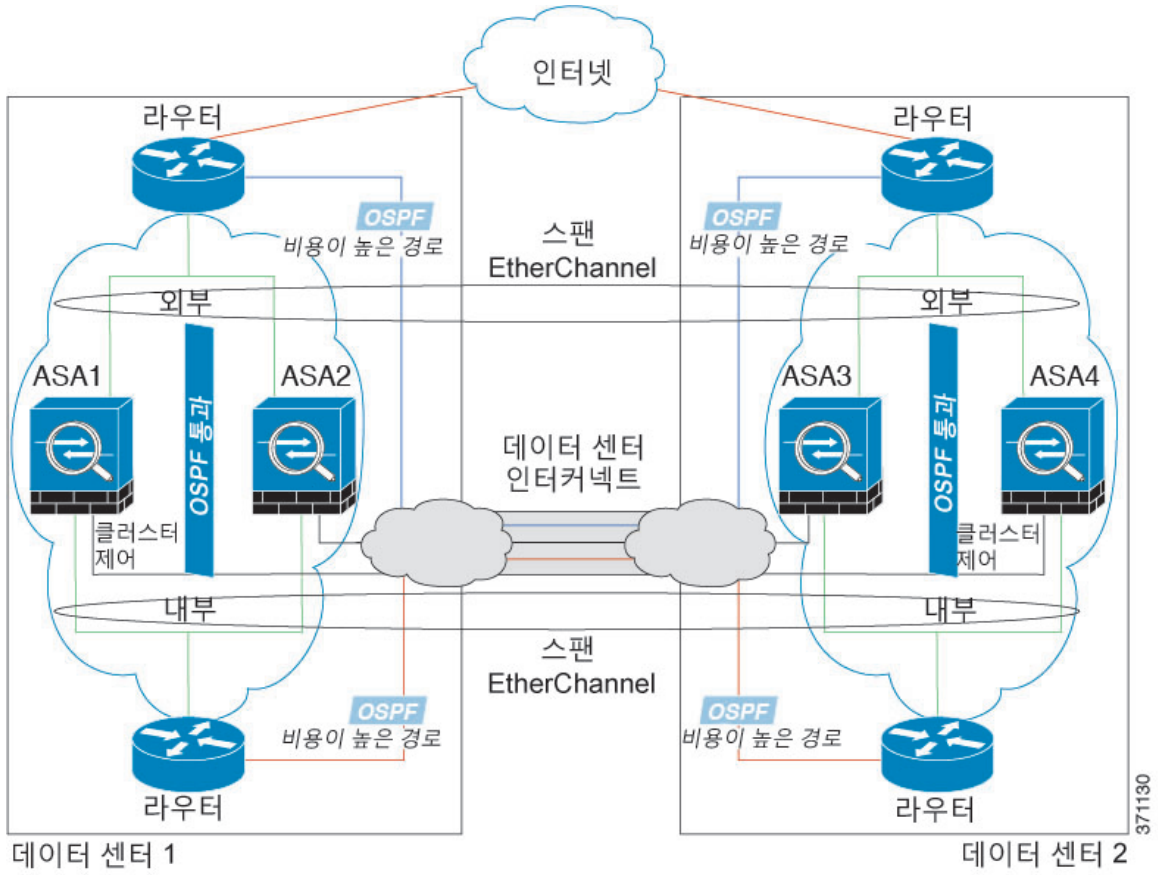
다음 예에서는 내부 라우터와 외부 라우터의 사이에 위치한(노스-사우스 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다.

각 사이트의 클러스터 멤버는 내부 및 외부용 스팬 EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 섀시를 포괄합니다.

각 데이터 센터의 내부 및 외부 라우터에서는 투명 ASA를 통과하는 OSPF를 사용합니다. MAC과 달리 라우터 IP는 모든 라우터마다 고유합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. ASA를 통과하는 비용이 낮은 경로의 경우, 클러스터의 각 사이트에 있는 같은 브리지 그룹을 거쳐 비대칭 연결을 유지해야 합니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 클러스터 멤버로 이동합니다.

각 사이트의 스위치 구현 과정에는 다음 사항이 포함될 수 있습니다.

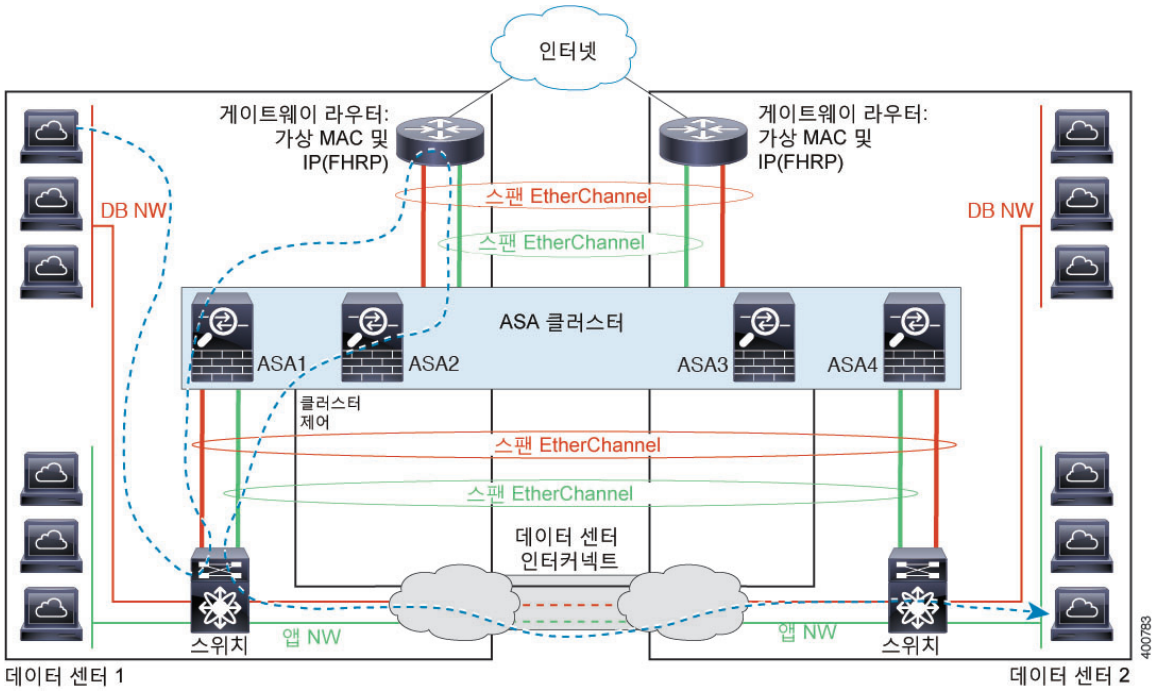
- 사이트 간 VSS/vPC — 이 시나리오의 경우 데이터 센터 1에 하나의 스위치를 설치하고, 나머지 하나는 데이터 센터 2에 설치합니다. 각 데이터 센터의 클러스터 유닛에 사용할 수 있는 한 가지 옵션은 로컬 스위치에만 연결하는 반면, VSS/vPC 트래픽이 DCI를 통해 통과하도록 하는 것입니다. 이 경우 연결의 대부분은 각 데이터 센터에 로컬로 저장됩니다. DCI에서 추가 트래픽을 처리할 수 있는 경우, 선택에 따라 각 유닛을 DCI 전반의 스위치에 연결할 수 있습니다. 이 경우 트래픽이 데이터 센터 전반에 분산되므로 DCI의 성능이 매우 뛰어나야 합니다.
- 각 사이트의 로컬 VSS/vPC — 스위치 이중화를 개선하기 위해 각 사이트에 별도의 VSS/vPC 쌍을 2개씩 설치할 수 있습니다. 이 경우 여전히 클러스터 유닛의 Spanned EtherChannel은 두 로컬 스위치에만 연결된 데이터 센터 1 섀시 및 이러한 로컬 스위치에 연결된 데이터 센터 2 섀시로 이루어져 있으나, 사실상 Spanned EtherChannel은 "분리"되어 있습니다. 각 로컬 VSS/vPC에서는 Spanned EtherChannel을 사이트-로컬 EtherChannel로 간주합니다.



Spanned EtherChannel 투명 모드 이스트-웨스트 사이트 간의 예

다음 예에서는 게이트웨이 라우터와 각 사이트의 두 내부 네트워크, 즉 애플리케이션 네트워크 및 DB 네트워크의 사이에 위치한(이스트-웨스트 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부에 있는 애플리케이션 및 DB 네트워크에 대한 스팬 EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 섀시를 포괄합니다.

각 사이트의 게이트웨이 라우터는 HSRP와 같은 FHRP를 사용하여 각 사이트에 동일한 목적지 가상 MAC 및 IP 주소를 제공합니다. 의도치 않은 MAC 주소 플래핑(flapping)을 피하는 좋은 방법은 **mac-address-table static** *outside_interface mac_address* 명령을 사용하여 게이트웨이 라우터 실제 MAC 주소를 ASA MAC 주소 테이블에 정적으로 추가하는 것입니다. 이러한 항목이 없으면, 사이트 1의 게이트웨이가 사이트 2의 게이트웨이와 통신할 경우 해당 트래픽이 ASA를 통과해 내부 인터페이스에서 사이트 2에 도달하려고 시도하여 문제를 일으킬 수 있습니다. OTV(Overlay Transport Virtualization) 또는 이와 유사한 방법으로 데이터 VLAN이 사이트 전반에 확장됩니다. 트래픽이 게이트웨이 라우터로 예정된 경우 트래픽에서 다른 사이트에 DCI를 전달하는 것을 방지하려면 필터를 추가해야 합니다. 한 개의 사이트에서 게이트웨이 라우터에 연결할 수 없는 경우, 필터를 제거해야 트래픽이 다른 사이트의 게이트웨이 라우터에 전송될 수 있습니다.



vPC/VSS 옵션에 대한 자세한 내용은 Spanned EtherChannel 투명 모드 노스-사우스 사이트 간의 예, 452 페이지를 참조하십시오.

ASA 클러스터링에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
이제 클러스터 인터페이스 디바운스 시간이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다.	9.10(1)	인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 **health-check monitor-interface debounce-time** 명령 또는 ASDM **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** 화면에 지정되어 있는 밀리초 동안 대기합니다. 이제 이 기능이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다. 예를 들어 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다. 명령은 수정하지 않았습니다.
내부 장애 발생 후 클러스터에 자동으로 다시 참가	9.9(2)	이전에는 많은 오류 상태로 인해 클러스터에서 클러스터 유닛이 제거되었으며 문제를 해결한 후에 클러스터에 수동으로 다시 참가해야 했습니다. 이제 유닛에서는 기본적으로 5분, 10분, 20분 간격으로 자동으로 클러스터에 다시 참가하려고 시도합니다. 이러한 값은 구성할 수 있습니다. 내부 오류 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등 신규 또는 수정된 명령: **health-check system auto-rejoin, show cluster info auto-join**

기능 이름	플랫폼 릴리스	기능 정보
클러스터의 신뢰할 수 있는 전송 프로토콜 메시지에 대해 전송 관련 통계 표시	9.9(2)	이제 유닛당 클러스터의 신뢰할 수 있는 전송 버퍼 사용량을 볼 수 있어 버퍼가 제어 평면에서 가득 찬 경우 패킷 삭제 문제를 식별할 수 있습니다. 신규 또는 수정된 명령: **show cluster info transport cp detail**
ASA 5000-X Series에서 인터페이스를 실패 상태로 표시하기 위해 구성 가능한 디바운스 시간	9.9(2)	이제 ASA에서 인터페이스를 실패 상태로 간주하고 유닛이 ASA 5500-X Series의 클러스터에서 제거되기 전에 디바운스 시간을 구성할 수 있습니다. 이 기능을 통해 인터페이스 오류 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 지정되어 있는 밀리초 동안 대기합니다. 기본 디바운스 시간은 500ms이며 범위는 300ms~9초입니다. 이 기능은 Firepower 4100/9300에서 이전에 사용 가능했습니다. 신규 또는 수정된 명령: **health-check monitor-interface debounce-time**
클러스터링을 위한 사이트 간 이중화	9.9 (1)	사이트 간 이중화를 통해 트래픽 플로우의 백업 소유자는 항상 소유자의 다른 사이트에 있습니다. 이 기능은 사이트 오류로부터 보호합니다. 신규 또는 수정된 명령: **site-redundancy, show asp cluster counter change, showasp table cluster chash-table, show conn flag**

기능 이름	플랫폼 릴리스	기능 정보
향상된 클러스터 유닛 상태 검사 장애 탐지	9.8(1)	이제 유닛 상태 검사의 보류 시간을 더 낮게 0.3초(최솟값)로 구성할 수 있습니다. 이전에는 최소값이 0.8초였습니다. 이 기능은 유닛 상태 검사 메시징 체계를 제어 평면의 *keepalives*에서 데이터 평면의 하트비트로 변경합니다. 하트비트를 사용하면 제어 평면 CPU 과다 사용 및 예약 지연의 영향을 받지 않으므로 클러스터링의 신뢰성과 응답성이 개선됩니다. 대기 시간을 낮게 구성하면 클러스터 제어 링크 메시징 활동이 증가합니다. 낮은 대기 시간을 구성하기 전에 네트워크를 분석하는 것이 좋습니다. 예를 들어, 한 번의 대기 시간 간격 동안 3개의 하트비트 메시지가 있으므로 클러스터 제어 링크를 통과하는 한 유닛에서 다른 유닛으로의 핑이 *holdtime*/3 이내에 반환되는지 확인하십시오. 대기 시간을 0.3 - 0.7초로 설정한 후에 ASA 소프트웨어를 다운그레이드하는 경우, 새로운 설정이 지원되지 않으므로 이 설정은 3초의 기본값으로 되돌아갑니다. 수정된 명령: **health-check holdtime, show asp drop clustercounter, show cluster info health details**

기능 이름	플랫폼 릴리스	기능 정보
관리자 현지화: 데이터 센터에 대한 사이트 간 클러스터링 개선 사항	9.7(1)	성능을 개선하고 데이터 센터에 대한 사이트 간 클러스터링을 위해 사이트 내부에서 트래픽을 유지하기 위해 관리자 현지화를 활성화할 수 있습니다. 새로운 연결은 일반적으로 로드 밸런싱 상태이며 지정된 사이트 내부의 클러스터 멤버가 소유합니다. 그러나 ASA는 모든 사이트에서 멤버에 관리자 역할을 할당합니다. 관리자 현지화를 사용하면 추가 관리자 역할이 활성화됩니다. 즉, 소유자와 동일한 사이트의 로컬 관리자와 모든 사이트의 전역 관리자 역할이 활성화됩니다. 소유자와 관리자를 동일한 사이트에서 유지하면 성능이 향상됩니다. 또한 원래 소유자가 실패할 경우, 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다. 전역 관리자는 클러스터 멤버가 다른 사이트에서 소유하는 연결에 대한 패킷을 수신하는 경우 사용됩니다. 도입 또는 수정된 명령: **director-localization, show asp tablecluster chash, show conn, show conn detail**
라우팅 모드, Spanned EtherChannel 모드에서 사이트별 IP 주소에 대한 지원	9.6(1)	Spanned EtherChannel을 사용하는 라우팅 모드에서 사이트 간 클러스터링을 위해 이제 사이트별 MCA 주소에 추가하여 사이트별 IP 주소를 구성할 수 있습니다. 사이트의 IP 주소를 추가하면 라우팅 문제를 일으킬 수 있는 전역 MAC 주소의 ARP 응답이 DCI(Data Center Interconnect)를 통해 이동하는 것을 방지하기 위해 OTV(Overlay Transport Virtualization) 디바이스에서 ARP 검사를 사용할 수 있습니다. ARP 검사는 VACL을 사용하여 MAC 주소를 필터링할 수 없는 일부 스위치에 필요합니다. 수정된 명령: **mac-address, show interface**

기능 이름	플랫폼 릴리스	기능 정보
클러스터링에 대한 ASA 5516-X 지원	9.5(2)	이제 ASA 5516-X는 2-유닛 클러스터를 지원합니다. 유닛 2개의 클러스터링은 Base 라이선스에서 기본적으로 활성화되어 있습니다. 어떤 명령도 수정하지 않았습니다.
사이트 간 플로우 모빌리티에 대한 LISP 검사	9.5(2)	Cisco LISP(Locator/ID Separation Protocol) 아키텍처는 디바이스 ID를 해당 위치에서 두 개의 서로 다른 숫자 공간으로 분리하여, 서버 마이그레이션을 클라이언트에 투명하게 만듭니다. ASA는 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작업을 위해 이 정보를 사용할 수 있습니다. ASA 클러스터 멤버는 첫 번째 홉 라우터와 ETR(Egress Tunnel Router) 또는 ITR(Ingress Tunnel Router) 사이를 통과하는 LISP 트래픽을 검사할 수 있으며 플로우 소유자가 새로운 사이트에 있도록 변경할 수 있습니다. 도입 또는 수정된 명령: **allowed-eid, clear cluster info flow-mobility counters, clear lisp eid, cluster flow-mobility lisp, debug cluster flow-mobility, debuglisp eid-notify-intercept, flow-mobility lisp, inspect lisp, policy-map type inspect lisp, site-id, show asp table classify domain inspect-lisp, show cluster info flow-mobility counters, showconn, show lisp eid, show service-policy, validate-key**
장애 조치 및 ASA 클러스터링에서의 통신 사업자급 NAT 개선 사항 지원	9.5(2)	통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 이 기능은 이제 장애 조치 및 ASA 클러스터 구축에서 지원됩니다. 수정된 명령: **show local-host**

기능 이름	플랫폼 릴리스	기능 정보
추적 항목 클러스터링의 구성 가능한 레벨	9.5(2)	기본적으로 클러스터링 이벤트의 모든 레벨이 많은 낮은 레벨의 이벤트를 포함하여 추적 버퍼에 포함되어 있습니다. 더 높은 레벨의 이벤트로 추적을 제한하기 위해 클러스터에 대해 최소한의 추적 레벨을 설정할 수 있습니다. 도입된 명령: **trace-level**
라우팅 방화벽 모드에서 Spanned EtherChannel에 대한 사이트 간 클러스터링 지원을 위한 사이트별 MAC 주소	9.5(1)	이제 라우팅 모드에서 Spanned EtherChannel에 대한 사이트 간 클러스터링을 사용할 수 있습니다. MAC 주소 플래핑을 방지하려면 각 인터페이스에 대한 사이트별 MAC 주소를 사이트의 유닛 간에 공유할 수 있도록 각 클러스터 멤버에 대한 사이트 ID를 구성합니다. 도입 또는 수정된 명령: **site-id, mac-address site-id, showcluster info, show interface**
인터페이스 또는 클러스터 제어 링크 작동 실패 시 자동 다시 참가 동작의 ASA 클러스터 맞춤화	9.5(1)	이제 인터페이스 또는 클러스터 제어 링크 작동이 실패할 경우 자동 다시 참가 동작을 맞춤화할 수 있습니다. 도입된 명령: **health-check auto-rejoin**
ASA 클러스터의 GTPv1 및 GTPv2 지원	9.5(1)	이제 ASA 클러스터는 GTPv1 및 GTPv2 검사를 지원합니다. 명령은 수정하지 않았습니다.
ASA 클러스터링에서 하드웨어 모듈의 상태 모니터링 비활성화	9.5(1)	기본적으로 클러스터링 사용 시 ASA에서는 ASA FirePOWER 모듈과 같은 설치된 하드웨어 모듈의 상태를 모니터링합니다. 하드웨어 모듈 오류 때문에 장애 조치가 수행되는 것을 원치 않을 경우 모듈 모니터링을 비활성화할 수 있습니다. 수정된 명령: **health-check monitor-interface service-module**

기능 이름	플랫폼 릴리스	기능 정보
TCP 연결에 대한 클러스터 복제 지연	9.5(1)	이 기능은 관리자/백업 플로우 생성을 지연시켜 짧은 수명의 플로우와 관련된 "불필요한 작업"을 제거하는 데 도움이 됩니다. 도입된 명령: **cluster replication delay**
인터페이스당 ASA 클러스터 상태 모니터링 활성화 및 비활성화	9.4(1)	현재 인터페이스당 상태 모니터링을 활성화하거나 비활성화할 수 있습니다. 상태 모니터링은 모든 포트 채널, 이중 및 단일 물리적 인터페이스에서 기본적으로 활성화되어 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다. 필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다. 도입된 명령: **health-check monitor-interface**
DHCP 릴레이에 대한 ASA 클러스터링 지원	9.4(1)	현재 ASA 클러스터에서 DHCP 릴레이를 구성할 수 있습니다. 클라이언트 DHCP 요청이 클라이언트 MAC 주소의 해시를 사용하는 클러스터 멤버에 대해 로드 밸런싱 상태가 됩니다. DHCP 클라이언트 및 서버 기능은 아직 지원되지 않습니다. 어떤 명령도 수정하지 않았습니다.
ASA 클러스터링에서의 SIP 검사 지원	9.4(1)	현재 ASA 클러스터에서 SIP 검사를 구성할 수 있습니다. 부하 균형으로 인해 모든 디바이스에서 제어 흐름을 만들 수 있지만 자식 데이터 흐름은 동일한 디바이스에 상주해야 합니다. TLS 프록시 컨피그레이션은 지원되지 않습니다. 다음 명령을 도입했습니다. **show cluster service-policy**

기능 이름	플랫폼 릴리스	기능 정보
내부 네트워크 간에 ASA 클러스터링 방화벽이 구성된 투명 모드의 사이트 간 구축	9.3(2)	이제 각 사이트(East-West 삽입)에서 내부 네트워크와 게이트웨이 라우터 간에 투명 모드에서 클러스터를 구축하고 사이트 간에 내부 VLAN을 확장할 수 있습니다. OTV(오버레이 전송 가상화)를 사용할 것을 권장하지만 게이트웨이 라우터의 겹치는 MAC 주소 및 IP 주소가 사이트에서 유출되지 않도록 하는 모든 방법을 사용할 수 있습니다. 게이트웨이 라우터에 동일한 가상 MAC 및 IP 주소를 제공하기 위해 HSRP 등의 첫 번째 홉 이중화 프로토콜(FHRP)을 사용하십시오.
ASA 클러스터링을 위한 BGP 지원	9.3(1)	ASA 클러스터링에서 BGP 지원을 추가했습니다. 도입된 명령: **bgp router-id clusterpool**
투명 모드의 경우 지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버 지원	9.2(1)	이제 투명 방화벽 모드에서 스팬 EtherChannel 모드를 사용할 경우 지리적으로 다른 위치에 클러스터 멤버를 배치할 수 있습니다. 라우팅 방화벽 모드에서 스팬 EtherChannel을 사용한 사이트 간 클러스터링은 지원되지 않습니다. 어떤 명령도 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
클러스터링을 위한 고정 LACP 포트 우선순위 지원	9.2(1)	일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 이제 동적 포트 우선순위를 사용하지 않도록 설정하여 스팬 EtherChannel과의 호환성을 향상할 수 있습니다. 또한 다음 지침을 따라야 합니다. • 클러스터 제어 링크 경로의 네트워크 요소에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다. • 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다. 다음 명령을 도입했습니다. **clacp static-port-priority**

기능 이름	플랫폼 릴리스	기능 정보
스팬 EtherChannel에서 32개의 활성 링크 지원	9.2(1)	ASA EtherChannel에서는 최대 16개의 활성 링크를 지원합니다. 스팬 EtherChannel까지 활용하면 vPC에서 2개의 스위치를 함께 사용할 경우, 그리고 동적 포트 우선순위를 비활성화할 경우 클러스터 전체에서 최대 32개의 활성 링크를 지원하도록 이 기능을 확장할 수 있습니다. 스위치에서는 16개의 활성 링크가 포함된 EtherChannel(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000)을 지원해야 합니다. VSS 또는 vPC에서 8개의 활성 링크를 지원하는 스위치를 사용하려는 경우, 이제 스팬 EtherChannel에 16개의 활성 링크를 구성하면 됩니다(각 스위치에 8개씩 연결됨). 이전에는 VSS/vPC와 함께 사용해도 스팬 EtherChannel에서 8개의 활성 링크, 8개의 스탠바이 링크만 지원되었습니다. 참고 스팬 EtherChannel에서 활성 링크를 8개 이상 사용하려는 경우 스탠바이 링크까지 보유할 수는 없습니다. 활성 링크를 9~32개까지 지원하려면 스탠바이 링크의 사용을 허용하는 cLACP 동적 포트 우선순위를 비활성화해야 합니다. 다음 명령을 도입했습니다. **clacp static-port-priority**
ASA 5585-X에 클러스터 멤버 16개 지원	9.2(1)	이제 ASA 5585-X에서는 16유닛 클러스터를 지원합니다. 어떤 명령도 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
ASA 5500-X support for clustering	9.1(4)	이제 ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X에서는 2-유닛 클러스터를 지원합니다. 유닛 2개의 클러스터링은 기본 라이센스에서 기본적으로 활성화되어 있으며, ASA 5512-X의 경우 Security Plus 라이센스가 필요합니다. 어떤 명령도 수정하지 않았습니다.
VSS 및 vPC의 상태 검사 모니터링 지원 개선	9.1(4)	클러스터 제어 링크를 EtherChannel로 구성하고(권장) 이를 VSS 또는 vPC 쌍에 연결한 경우, 이제 상태 검사 모니터링 기능을 통해 안정성을 높일 수 있습니다. Cisco Nexus 5000과 같은 일부 스위치의 경우 VSS/vPC에서 유닛 하나가 중단되거나 부팅되면 해당 스위치에 연결된 EtherChannel 멤버 인터페이스가 ASA에 대해 가동되는 것으로 표시될 수 있지만, 스위치 측의 트래픽을 통과하지는 않습니다. ASA 대기 시간 제한을 낮은 값으로 설정한 경우(에: 0.8초) 클러스터에서 ASA가 잘못 제거될 수 있으며 ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다. VSS/vPC 상태 검사 기능을 활성화할 경우, ASA에서는 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 keepalive 메시지를 플러딩하여 하나 이상의 스위치에 해당 메시지가 전송되도록 합니다. 수정된 명령: **health-check** [**vss-enabled**]
지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버 지원(개별 인터페이스 모드 전용)	9.1(4)	이제 개별 인터페이스 모드를 사용할 경우 지리적으로 다른 위치에 클러스터 멤버를 배치할 수 있습니다.@@ 어떤 명령도 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
ASA 5580 및 5585-X를 위한 ASA 클러스터링	9.0(1)	ASA 클러스터링을 사용하면 최대 8개의 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. ASA 클러스터링은 ASA 5580 및 ASA 5585-X를 지원합니다. 클러스터의 모든 유닛은 동일한 하드웨어 사양을 갖춘 동일한 모델이어야 합니다. 클러스터링이 활성화된 경우, 지원되지 않는 기능에 대한 목록은 컨피그레이션 설명서를 참조하십시오. 도입 또는 수정된 명령: **channel-group**, **clacp system-mac**, **clear cluster info**, **clear configure cluster**, **cluster exec**, **cluster group**, **cluster interface-mode**, **cluster-interface**, **conn-rebalance, console-replicate**, **cluster master unit**, **cluster remove unit**, **debug cluster**, **debug lacp cluster**, **enable**(클러스터 그룹),**health-check**, **ip address**, **ipv6 address**, **key**(클러스터 그룹), **local-unit, mac-address** (인터페이스), **mac-address pool**, **mtu cluster, port-channel span-cluster, priority**(클러스터 그룹), **prompt cluster-unit**, **show asp cluster counter**, **show asp table cluster chash-table**, **show cluster**, **show cluster info**, **show cluster user-identity**, **show lacp cluster**, **show running-config cluster**

11 장

ASA 클러스터 - Firepower 4100/9300 섀시

클러스터링을 사용하면 여러 개의 Firepower 4100/9300 섀시 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. Firepower 4100/9300 섀시 Series에는 Firepower 9300 및 Firepower 4100 Series이(가) 포함되어 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. 클러스터링으로 지원되지 않는 기능, 476 페이지를 참조하십시오.

클러스터링 정보 Firepower 4100/9300 섀시

클러스터는 단일 논리적 유닛으로 작동하는 여러 개의 디바이스로 구성됩니다. Firepower 4100/9300 섀시에서 클러스터를 구축할 때는 다음 작업이 수행됩니다.

- 유닛 간 통신에 사용되는 클러스터 제어 링크(기본값: port-channel 48)를 생성합니다. 인트라 섀시 클러스터링(intra-chassis clustering)(Firepower 9300 전용)의 경우, 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 섀시 간 클러스터링의 경우, 섀시 간의 통신을 위해 물리적 인터페이스를 이 EtherChannel에 수동으로 할당해야 합니다.

- 애플리케이션 내부에 클러스터 부트스트랩 구성을 생성합니다.

  클러스터를 구축할 때, Firepower 4100/9300 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다. 클러스터링 환경을 사용자 정의하려는 경우, 사용자가 일부 부트스트랩 구성을 애플리케이션 내부에 구성할 수 있습니다.

- 데이터 인터페이스를 *Spanned* 인터페이스로 클러스터에 할당합니다.

  섀시 내 클러스터링의 경우, 스팬 인터페이스는 섀시 간 클러스터링과 마찬가지로 EtherChannel에 국한되지 않습니다. Firepower 9300 수퍼바이저는 EtherChannel 기술을 내부에 사용하여 트래픽을 공유 인터페이스의 다중 모듈에 로드 밸런싱하므로 모든 데이터 인터페이스 유형이 Spanned(스팬) 모드에서 작동합니다. 섀시 간 클러스터링의 경우, 모든 데이터 인터페이스에 Spanned EtherChannel을 사용해야 합니다.

  참고 개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

- 관리 인터페이스를 클러스터의 모든 유닛에 할당합니다.

다음 섹션에서는 클러스터링 개념 및 구현에 대한 자세한 정보를 제공합니다. 클러스터링에 대한 참조, 537 페이지 섹션도 참조하십시오.

부트스트랩 컨피그레이션

클러스터를 구축할 때, Firepower 4100/9300 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다. 클러스터링 환경을 맞춤화하려는 경우, 일부 부트스트랩 구성은 사용자가 구성할 수 있습니다.

클러스터 멤버

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다.

클러스터의 멤버 중 하나는 마스터 유닛입니다. 마스터 유닛은 자동으로 결정됩니다. 기타 모든 멤버는 슬레이브 유닛입니다.

모든 컨피그레이션은 마스터 유닛에서만 수행해야 하며, 이후 컨피그레이션이 슬레이브 유닛에 복제됩니다.

일부 기능은 클러스터에서 확장되지 않으며 마스터 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다. 클러스터링을 위한 중앙 집중식 기능, 477 페이지의 내용을 참조하십시오.의 내용을 참조하십시오.

마스터 및 슬레이브 유닛 역할

클러스터의 멤버 1개는 마스터 유닛입니다. 마스터 유닛은 자동으로 결정됩니다. 기타 모든 멤버는 슬레이브 유닛입니다.

모든 컨피그레이션은 마스터 유닛에서만 수행해야 하며, 이후 컨피그레이션이 슬레이브 유닛에 복제됩니다.

일부 기능은 클러스터에서 확장되지 않으며 마스터 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다. 클러스터링을 위한 중앙 집중식 기능, 477 페이지의 내용을 참조하십시오.의 내용을 참조하십시오.

클러스터 제어 링크

유닛 간 통신에 사용되는 클러스터 제어 링크는 EtherChannel(port-channel 48)입니다. 섀시 내 클러스터링을 위해 이 링크에서는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 섀시 간 클러스터링의 경우 섀시 간의 통신을 위해 물리적 인터페이스를 Firepower 4100/9300 섀시의 이 EtherChannel에 수동으로 할당해야 합니다.

2-섀시의 섀시 간 클러스터의 경우 클러스터 제어 링크를 한 섀시에서 다른 섀시로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 마스터 선택
- 구성 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

을 위한 클러스터 제어 링크 크기 조정

가능한 경우, 각 섀시의 예상 처리량에 맞게 클러스터 제어 링크의 크기를 조정하여 클러스터 제어 링크가 최악의 시나리오를 처리할 수 있게 해야 합니다. 예를 들어, 클러스터에 있는 유닛당 최대 14Gbps를 전달할 수 있는 ASA 5585-X(SSP-60 포함)를 보유한 경우, 최소 14Gbps를 전달할 수 있는 클러스터 제어 링크에 대한 인터페이스 또한 할당해야 합니다. 이 경우 클러스터 제어 링크의 EtherChannel에 10기가비트 이더넷 인터페이스 2개를 사용할 수 있으며, 데이터 링크에 필요한 경우 나머지 인터페이스를 사용합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예를 들면 다음과 같습니다.

- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.

- 네트워크 액세스용 AAA는 중앙 집중식 기능이므로 모든 트래픽이 마스터 유닛으로 전달됩니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

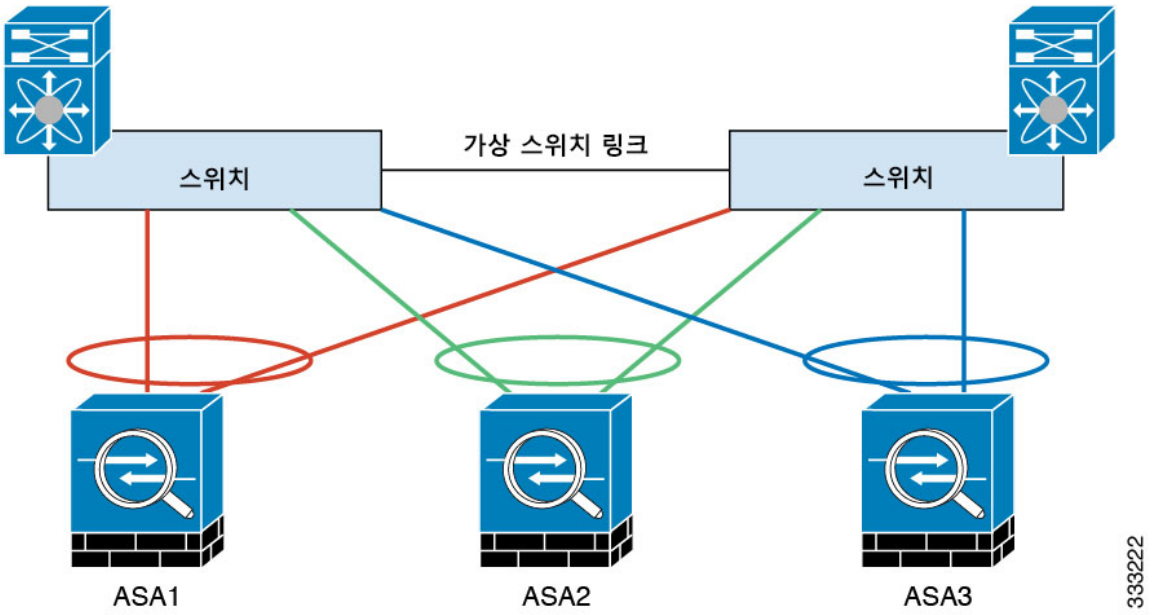
대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

을 위한 클러스터 제어 링크 이중화

클러스터 제어 링크에는 EtherChannel을 사용하는 편이 바람직하며, 이렇게 할 경우 EtherChannel 내의 여러 링크에 트래픽을 전달하는 동시에 이중화를 실현할 수 있습니다.

다음 다이어그램에는 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel) 환경에서 EtherChannel을 클러스터 제어 링크로 사용하는 방법이 나와 있습니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 VSS 또는 vPC의 일부일 경우 동일한 EtherChannel 내에 있는 ASA 인터페이스를 연결하여 VSS 또는 vPC의 스위치를 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스팬 EtherChannel입니다.



을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(round-trip time)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

클러스터 제어 링크 네트워크

Firepower 4100/9300 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.클러스터를 구축할 때 이 IP 주소를 맞춤 설정할 수 있습니다. 클러스터 제어 링크 네트워크는 유닛 간에 라우터를 포함할 수 없으며 레이어 2 스위칭만 허용됩니다. 사이트 간 트래픽의 경우에는 OTV(Overlay Transport Virtualization)를 사용하는 것이 좋습니다.

클러스터 인터페이스

섀시 내 클러스터링의 경우 클러스터에 물리적 인터페이스 또는 EtherChannel(포트 채널이라고도 함)을 둘 다 할당할 수 있습니다. 클러스터에 할당된 인터페이스는 클러스터의 모든 멤버 전체에서 트래픽의 로드 밸런싱을 수행하는 Spanned 인터페이스입니다.

섀시 간 클러스터링의 경우 데이터 EtherChannel만 클러스터에 할당할 수 있습니다. 이러한 Spanned EtherChannel에는 각 섀시의 동일한 멤버 인터페이스가 포함되어 있습니다. 업스트림 스위치에서 이러한 인터페이스는 모두 단일 EtherChannel에 포함되어 있습니다. 따라서 스위치에서는 여러 디바이스에 연결되어 있는지 알지 못합니다.

개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

VSS 또는 **vPC**에 연결

인터페이스에 대한 이중화를 제공하기 위해 EtherChannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.

구성 복제

클러스터의 모든 유닛에서는 단일 구성을 공유합니다. 마스터 유닛에서는 구성만 변경할 수 있으며 변경 사항은 클러스터의 모든 다른 유닛에 자동으로 동기화됩니다.

ASA클러스터 관리

ASA 클러스터링을 사용하는 데 따른 여러 장점 중 하나는 관리하기가 쉽다는 점입니다. 이 섹션에서는 클러스터를 관리하는 방법에 대해 설명합니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결할 것을 권장합니다. 이 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

클러스터에 관리 유형 인터페이스를 할당해야 합니다. 이 인터페이스는 Spanned 인터페이스와는 다른 특수 개별 인터페이스입니다. 관리 인터페이스를 사용하면 각 유닛에 직접 연결할 수 있습니다.

기본 클러스터 IP 주소는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 주소의 범위를 구성하여 현재 마스터를 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 마스터 유닛이 변경될 경우 주요 클러스터 IP 주소는 새 마스터 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다.

예를 들어, 현재 마스터 유닛에 항상 연결되어 있는 기본 클러스터 IP 주소에 연결하여 클러스터를 관리할 수 있습니다. 로컬 IP 주소에 연결하여 개별 멤버를 관리할 수 있습니다.

TFTP 또는 syslog 같은 아웃바운드 관리 트래픽의 경우 마스터 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

마스터 유닛 관리와 슬레이브 유닛 관리 비교

모든 관리 및 모니터링은 마스터 유닛에서 수행할 수 있습니다. 마스터 유닛에서 런타임 통계, 리소스 사용량 또는 모든 유닛의 기타 모니터링 정보를 확인할 수 있습니다. 또한 클러스터 내의 모든 유닛에 명령을 배포하고, 슬레이브 유닛의 콘솔 메시지를 마스터 유닛으로 복제할 수 있습니다.

필요한 경우 슬레이브 유닛을 직접 모니터링할 수 있습니다. 마스터 유닛에서도 사용 가능하지만 슬레이브 유닛에서 파일 관리를 수행할 수 있습니다(구성 백업 및 이미지 업데이트 포함). 다음 기능은 마스터 유닛에서 사용할 수 없습니다.

- 유닛당 클러스터별 통계 모니터링
- 유닛당 Syslog 모니터링(콘솔 복제가 활성화된 경우 콘솔로 전송되는 syslog 제외).
- SNMP
- NetFlow

RSA 키 복제

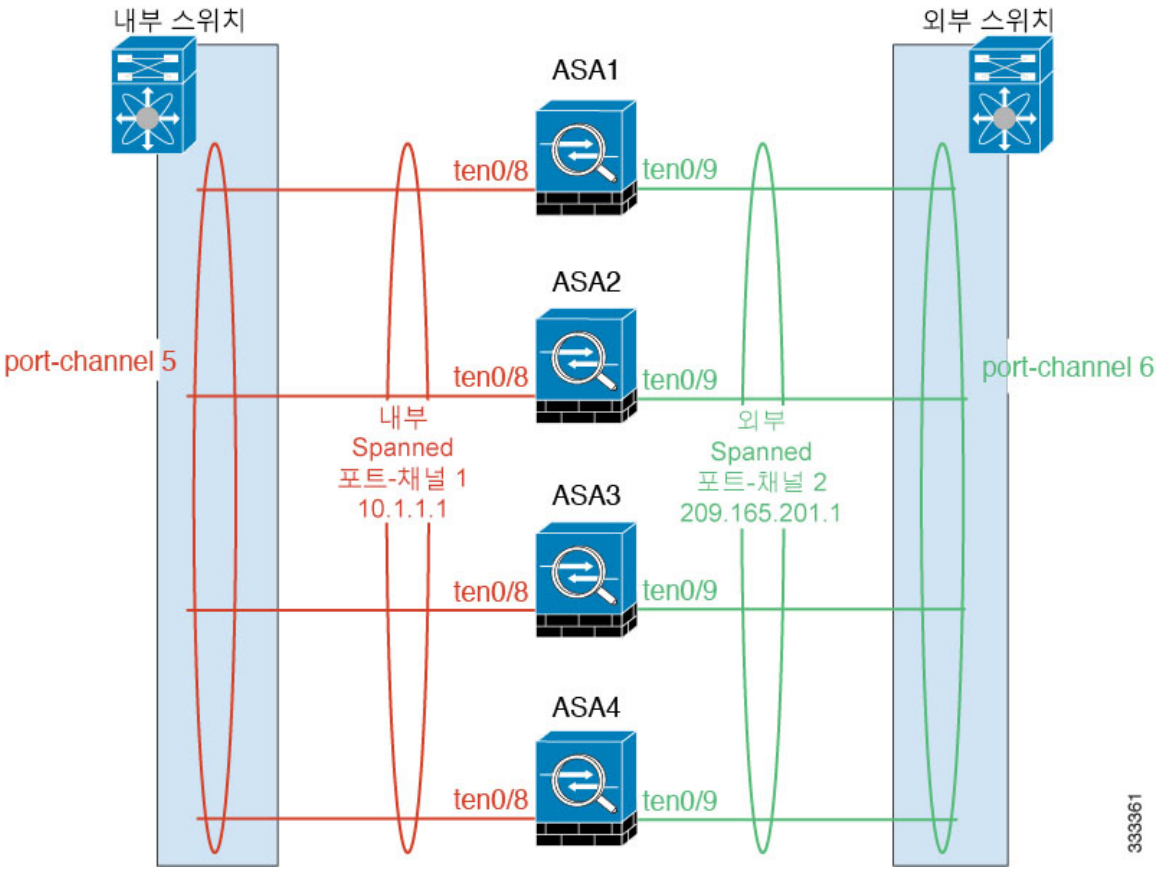
마스터 유닛에서 RSA 키를 생성할 경우, 해당 키는 모든 슬레이브 유닛에 복제됩니다. 기본 클러스터 IP 주소에 대한 SSH 세션이 있는 경우 마스터 유닛에 오류가 발생하면 연결이 끊어집니다. 새 마스터 유닛에서는 SSH 연결에 동일한 키를 사용하므로, 새 마스터 유닛에 다시 연결할 때 캐시된 SSH 호스트 키를 업데이트하지 않아도 됩니다.

ASDM 연결 인증서 IP 주소 불일치

기본적으로, 자체 서명된 인증서는 로컬 IP 주소를 기준으로 ASDM 연결에 사용됩니다. ASDM을 사용하여 기본 클러스터 IP 주소를 연결할 경우, 인증서에서는 기본 클러스터 IP 주소가 아닌 로컬 IP 주소를 사용하므로 IP 주소가 일치하지 않는다는 경고 메시지가 표시됩니다. 이 메시지를 무시하고 ASDM 연결을 설정할 수 있습니다. 그러나 이러한 유형의 경고를 방지하려면 기본 클러스터 IP 주소 및 IP 주소 풀의 모든 로컬 IP 주소가 포함된 인증서를 등록하면 됩니다. 그런 다음 이 인증서를 각 클러스터 멤버에 사용할 수 있습니다.

Spanned EtherChannels(권장)

섀시당 하나 이상의 인터페이스를 클러스터 내의 모든 섀시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 스팬 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스가 아닌 BVI에 IP 주소가 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.



사이트 간 클러스터링

사이트 간 설치 시 다음 권장 지침을 준수하면 ASA 클러스터링을 활용할 수 있습니다.

각 클러스터 섀시를 별도의 사이트 ID에 속하도록 구성할 수 있습니다.

사이트 ID는 사이트별 MAC 주소 및 IP 주소와 작동합니다. 클러스터에서 온 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면, 클러스터가 수신한 패킷은 전역 MAC 주소 및 IP 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지 못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다. 사이트별 MAC 주소 및 IP 주소는 Spanned EtherChannel만을 사용하는 라우팅 모드에서 지원됩니다.

사이트 ID는 LISP 검사를 사용한 플로우 모빌리티 활성화, 데이터 센터의 사이트 간 클러스터링에 대해 왕복 시간 레이턴시를 줄이고 성능을 개선하기 위한 관리자 지역화, 그리고 트래픽 플로우의 백업 소유자가 항상 소유자와 다른 사이트에 있는 연결에 대한 사이트 이중화에도 사용됩니다.

사이트 간 클러스터링에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 클러스터 플로우 모빌리티 구성 —클러스터 플로우 모빌리티 구성, 511 페이지
- 관리자 현지화 활성화 —관리자 현지화 활성화, 510 페이지
- 사이트 이중화 활성화 —관리자 현지화 활성화, 510 페이지

ASA 기능 및 클러스터링

일부 ASA 기능은 ASA 클러스터링이 지원되지 않으며, 일부 기능은 마스터 유닛에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

클러스터링으로 지원되지 않는 기능

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.

- TLS 프록시를 사용하는 Unified Communication 기능
- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- IS-IS 라우팅
- 다음과 같은 애플리케이션 감시:
  - CTIQBE
  - H323, H225, RAS
  - IPsec 통과
  - MGCP
  - MMP

  - RTSP
  - SCCP(Skinny)
  - WAAS
  - WCCP
- 봇네트 트래픽 필터
- Auto Update Server
- DHCP 클라이언트, 서버, 프록시 DHCP 릴레이가 지원됩니다.
- VPN 로드 밸런싱
- 장애 조치
- 통합 라우팅 및 브리징
- DCD(데드 연결 탐지)

클러스터링을 위한 중앙 집중식 기능

다음 기능은 마스터 유닛에서만 지원되며 클러스터에 확장되지 않습니다.

참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 유닛에서 마스터 유닛으로 전달됩니다.

리밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 마스터 유닛으로 리밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 마스터 유닛으로 다시 전송됩니다.

중앙 집중식 기능의 경우 마스터 유닛에 오류가 발생하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

- 다음과 같은 애플리케이션 감시:
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP

  - XDMCP

- 동적 라우팅
- 고정 경로 모니터링
- IGMP 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- PIM 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- 네트워크 액세스에 대한 인증 및 권한 부여. 어카운팅이 분산됨
- 필터링 서비스
- Site-to-Site IKEv1/IKEv2 VPN

  중앙 집중식 모드에서 VPN 연결은 클러스터의 마스터로만 설정됩니다. VPN 클러스터링의 기본 모드입니다. Site-to-Site VPN은 S2S IKEv2 VPN 연결이 멤버 전체에 분산되어 있는 분산 VPN 모드에서도 구축될 수 있습니다.

개별 유닛에 적용되는 기능

이러한 기능은 전체 클러스터 또는 마스터 유닛이 아닌 각 ASA 유닛에 적용됩니다.

- QoS — QoS 정책은 구성 복제의 일부로 클러스터 전체와 동기화됩니다. 그러나 정책은 각 유닛에서 독립적으로 시행됩니다. 예를 들어, 출력에 대한 정책 시행을 구성할 경우 특정 ASA에 있는 트래픽에서 적응 속도 및 적응 버스트 값이 시행됩니다. 3개 유닛으로 구성되고 트래픽이 균일하게 분산된 클러스터의 경우, 적응 속도는 클러스터 속도의 3배가 됩니다.
- 위협 감지 — 위협 감지는 각 유닛에 개별적으로 작동됩니다. 예를 들어, 상위 통계는 유닛별로 적용됩니다. 이를테면 포트 검사 감지 기능의 경우, 검사 트래픽이 모든 유닛 간에 로드 밸런싱되고 한 유닛에 모든 트래픽이 표시되지 않으므로 이 기능은 작동하지 않습니다.
- 리소스 관리 — 다중 상황 모드에서 리소스 관리는 로컬 사용량을 기준으로 각 유닛에 개별적으로 시행됩니다.
- LISP 트래픽 — UDP 포트 4342의 LISP 트래픽은 각각의 수신 유닛에서 검사되지만, 관리자는 할당되지 않습니다. 각 유닛은 EDI 테이블에 추가되어 클러스터 전체에서 공유되지만, LISP 트래픽 자체는 클러스터 상태 공유에 참여하지 않습니다.

네트워크 액세스 및 클러스터링용 **AAA**

네트워크 액세스용 AAA는 인증, 권한 부여, 어카운팅이라는 세 가지 구성 요소로 이루어져 있습니다. 인증 및 권한 부여는 클러스터 슬레이브에 대한 데이터 구조의 복제를 통해 클러스터링 마스터에서 중앙 집중식 기능으로 구현됩니다. 마스터 유닛이 선택된 경우, 새 마스터에서는 설정된 인증 완료 사용자 및 관련 인증 작업을 중단 없이 계속 가동하는 데 필요한 모든 정보를 보유하게 됩니다. 사용자 인증의 유휴 및 절대 시간 제한은 마스터 유닛이 변경될 경우 유지됩니다.

어카운팅은 클러스터에서 분산된 기능으로 구현됩니다. 어카운팅은 흐름 하나의 단위로 수행되므로, 흐름에 대한 어카운팅이 구성되면 흐름을 소유한 클러스터에서는 어카운팅 시작 및 중지 메시지를 AAA 서버에 보냅니다.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 흐름을 소유한 경우, 데이터 채널 소유자 유닛에서는 유휴 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유휴 시간 제한 값을 업데이트합니다. 그러나 제어 흐름 소유자가 다시 로드되고 제어 흐름이 다시 호스팅된 경우, 부모/자식 흐름 관계가 더 이상 유지되지 않으며 제어 흐름 유휴 시간 제한도 업데이트되지 않습니다.
- FTP 액세스용 AAA를 사용할 경우 마스터 유닛에서는 제어 채널 흐름을 중앙 집중화합니다.

방화벽 및 클러스터링 식별

마스터 유닛만이 AD에서 사용자-그룹을 검색하고 AD 에이전트에서 사용자-IP 매핑을 검색합니다. 그런 다음 마스터 유닛에서는 사용자 정보를 슬레이브에 제공하며, 슬레이브에서는 보안 정책을 기준으로 사용자 ID의 일치 여부를 결정할 수 있습니다.

멀티캐스트 라우팅 및 클러스터링

마스터 유닛에서는 fast-path 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 처리합니다. 연결이 설정되면 각 슬레이브에서 멀티캐스트 데이터 패킷을 전달할 수 있습니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 ASA에 전송할 수 있습니다. 패킷이 NAT 소유자가 아닌 ASA에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다. 보안 및 정책 확인 결과에 따라 NAT 소유자가 패킷에 대해 연결을 생성하지 않을 수도 있으므로 수신 유닛은 소유자에 대한 전달 플로우를 생성하지 않습니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

- 포트 블록 할당이 있는 PAT 없음 - 이 기능은 클러스터에서 지원되지 않습니다.
- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
  - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 유닛에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서, 호스트의 트래픽이 3개 유닛 모두에 부하 분산되는 경우 각 유닛에 하나씩 3개의 블록이 할당될 수 있습니다.

  - 백업 풀의 백업 유닛에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
  - PAT IP 주소 소유자가 다운되면 백업 유닛이 PAT IP 주소, 해당 포트 블록 및 xlate를 소유하게 됩니다. 그러나 새로운 요청을 처리하는 데 이러한 블록을 사용하지는 않습니다. 연결은 결국 시간 초과되고 블록은 해제됩니다.
  - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 새 풀이 작동하게 되는 동안 여전히 전환 중이던 xlate 백업 요청에 대해 xlate 백업 생성이 실패하게 됩니다. 이러한 동작은 포트 블록 할당 기능과 관련이 없으며, 풀이 분산되고 트래픽이 클러스터 유닛 전체에서 부하 분산되는 클러스터 구축 과정에서만 발생하는 일시적인 PAT 풀 문제입니다.

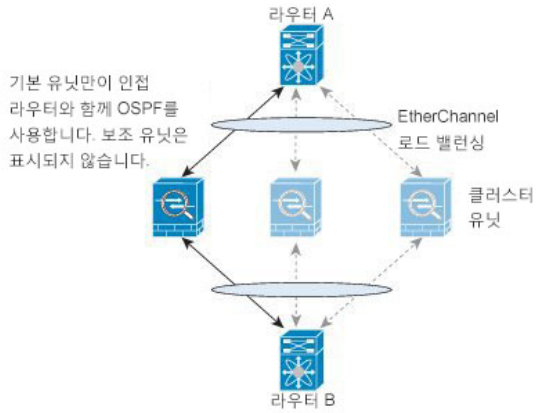
- 동적 PAT에 NAT 풀 주소 분산 — 마스터 유닛은 클러스터 전체에 걸쳐 주소를 사전에 균일하게 분산시킵니다. 멤버에 주소가 없는 연결이 전달된 경우 해당 연결이 끊어지며, 다른 멤버는 유효한 주소를 보유한 경우에도 마찬가지입니다. 각 유닛에 주소가 전달되도록 하려면 NAT 주소는 최소한 클러스터의 유닛에 있는 수만큼 추가해야 합니다. **show nat pool cluster** 명령을 사용하여 주소 할당을 확인합니다.
- 라운드 로빈 없음 — 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 마스터 유닛에 의해 관리되는 동적 NAT xlate — 마스터 유닛에서는 xlate 테이블을 유지하고 이를 슬레이브 유닛에 복제합니다. 동적 NAT가 필요한 연결이 슬레이브 유닛에 전달되고 xlate가 테이블에 없을 경우, 슬레이브 유닛에서는 마스터 유닛에서 xlate를 요청합니다. 슬레이브 유닛에서는 이 연결을 소유합니다.
- 세션당 PAT 기능 — 클러스터링에만 해당되는 것은 아니지만, 세션당 PAT 기능을 사용하면 PAT의 확장성이 개선되며 클러스터링을 수행할 때 각 슬레이브 유닛에서 고유한 PAT 연결을 소유할 수 있게 됩니다. 이와 달리 다중 세션 PAT 연결은 마스터 유닛에 전달해야 하며 마스터 유닛에서 해당 연결을 소유하게 됩니다. 기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽은 세션 단위 PAT xlate를 사용하며, 여기서 ICMP 및 기타 모든 UDP 트래픽은 멀티 세션을 사용합니다. TCP 및 UDP에 대해 이러한 기본값을 변경하도록 세션 단위 NAT 규칙을 구성할 수 있지만, ICMP에 대해서는 세션 단위 PAT를 구성할 수 없습니다. H.323, SIP, Skinny 등과 같이 다중 세션 PAT가 도움이 되는 트래픽의 경우 연결된 TCP 포트에 대해 세션 단위 PAT를 비활성화할 수 있습니다(이러한 H.323 및 SIP에 대한 UDP 포트는 기본적으로 이미 다중 세션임). 세션당 PAT에 대한 자세한 내용은 방화벽 설정 가이드를 참조하십시오.
- 다음을 검사할 수 있는 고정 PAT 없음
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP

- SIP

동적 라우팅 및 클러스터링

라우팅 프로세스는 마스터 유닛에서만 실행되며, 경로는 마스터 유닛을 통해 파악되고 보조 유닛에 복제됩니다. 라우팅 패킷이 슬레이브에 전송되면 해당 패킷은 마스터 유닛에 리디렉션됩니다.

그림 ***54:*** 동적 라우팅



슬레이브 멤버가 마스터 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 마스터 유닛에서 슬레이브 유닛으로 동기화되지 않습니다. 마스터 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

SCTP 및 클러스터링

로드 밸런싱으로 인해 모든 유닛에서 SCTP 연결을 만들 수 있습니다. 멀티호밍 연결은 동일한 유닛에 있어야 합니다.

SIP 검사 및 클러스터링

로드 밸런싱으로 인해 모든 디바이스에서 제어 흐름을 만들 수 있지만 자식 데이터 흐름은 동일한 디바이스에 상주해야 합니다.

TLS 프록시 구성은 지원되지 않습니다.

SNMP 및 클러스터링

SNMP 에이전트에서는 로컬 IP 주소로 각각의 개별 ASA를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 마스터가 선택된 경우, 새 마스터 유닛에 대한 폴링이 이루어지지 않습니다.

STUN 및 클러스터링

STUN 검사는 핀홀이 복제될 때 장애 조치 및 클러스터 모드에서 지원됩니다. 그러나 트랜잭션 ID는 유닛 간에 복제되지 않습니다. STUN Request를 수신한 후 유닛이 실패하고 다른 유닛이 STUN Response를 수신한 경우, STUN Response는 삭제됩니다.

Syslog와 NetFlow 및 클러스터링

- Syslog - 클러스터의 각 유닛에서는 고유한 syslog 메시지를 생성합니다. 각 유닛에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 구성은 클러스터의 모든 유닛에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 유닛에서는 단일 유닛에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 구성에 할당된 로컬-유닛 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, syslog 메시지는 다른 유닛에서 생성된 것처럼 보입니다.
- NetFlow — 클러스터의 각 유닛에는 고유한 NetFlow 스트림이 있습니다. NetFlow 컬렉터에서는 각각의 ASA를 별도의 NetFlow 내보내기 장치로만 처리할 수 있습니다.

Cisco TrustSec 및 클러스터링

마스터 유닛에서만 SGT(security group tag) 정보를 파악합니다. 그런 다음 마스터 유닛에서는 SGT를 슬레이브에 제공하며, 슬레이브에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

FXOS 섀시에서의 VPN 및 클러스터링

ASA FXOS 클러스터는 중앙 집중식 또는 분산 S2S VPN에 함께 사용할 수 없는 다음 두 가지 모드 중 하나를 지원합니다.

- 중앙 집중식 VPN 모드. 기본 모드. 중앙 집중식 모드에서 VPN 연결은 클러스터의 마스터로만 설정됩니다.

  VPN 기능은 마스터 유닛에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 마스터 유닛에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN에 연결된 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 마스터가 선택되면 VPN 연결을 다시 설정해야 합니다.

VPN 터널을 스팬 인터페이스 주소에 연결할 경우 연결이 마스터 유닛에 자동으로 전달됩니다. VPN 관련 키 및 인증서는 모든 유닛에 복제됩니다.

- 분산 VPN 모드. 이 모드에서 S2S IPsec IKEv2 VPN 연결은 확장성을 제공하는 ASA 클러스터의 멤버 전체에서 분산됩니다. 클러스터 멤버 전체에서 VPN 연결을 분산시키면 클러스터의 용량 및 처리량 모두를 완전히 활용하며 특히 중앙 집중식 VPN 기능 이상으로 VPN 지원을 크게 확장합니다.

참고 중앙 집중식 VPN 클러스터링 모드는 S2S IKEv1 및 S2S IKEv2를 지원합니다.

분산 VPN 클러스터링 모드는 S2S IKEv2만 지원합니다.

분산 VPN 클러스터링 모드는 Firepower 9300에서만 지원됩니다.

원격 액세스 VPN은 중앙 집중식 또는 분산 VPN 클러스터링 모드에서 지원되지 않습니다.

클러스터링의 요구 사항 및 사전 요구 사항 - **Firepower 4100/9300** 섀시

모델별 최대 클러스터링 유닛 수

- Firepower 4100 — 16개 섀시
- Firepower 9300 — 최대 16개 섀시의 16개 모듈

섀시 간 클러스터링을 위한 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 섀시:

- Firepower 4100 Series의 경우: 모든 섀시가 동일한 모델이어야 합니다. Firepower 9300의 경우: 모든 보안 모듈이 동일한 유형이어야 합니다. 빈 슬롯을 포함하여 섀시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 섀시에 설치된 보안 모듈의 수는 다를 수 있습니다.
- 이미지 업그레이드 시 동일한 FXOS 소프트웨어 예외를 실행해야 합니다.
- 클러스터에 할당하는 인터페이스에 대한 것과 동일한 인터페이스 구성을 포함해야 합니다(예: EtherChannel, 활성 인터페이스, 속도 및 이중 등). 동일한 인터페이스 ID에 대해 용량이 일치하고 동일한 Spanned EtherChannel에서 성공적인 인터넷 번들링이 가능한 한 섀시에서 서로 다른 네트워크 모듈 유형을 사용할 수 있습니다. 모든 데이터 인터페이스는 섀시 간 클러스터링에서 EtherChannel이어야 합니다. 인터페이스 모듈을 추가 또는 제거하거나 EtherChannel을 구성하는 등의 방법을 통해 클러스터링을 활성화한 후 FXOS에서 인터페이스를 변경하는 경우에는 각 섀시에서 슬레이브 유닛부터 시작하여 마지막으로 마스터까지 같은 변경을 수행합니다. FXOS에서 인터페이스를 제거하는 경우 ASA 구성에서는 관련 명령을 유지하므로 필요한 조정을 수행

할 수 있습니다. 구성에서 인터페이스를 제거하는 경우에는 구성 전반에 걸쳐 영향을 줄 수 있습니다. 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.

- 동일한 NTP 서버를 사용해야 합니다. 시간을 수동으로 설정해서는 안 됩니다.
- ASA: 각 FXOS 섀시를 License Authority 또는 Satellite Server에 등록해야 합니다. 슬레이브 유닛에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 섀시용으로 별도의 라이선스를 구매해야 합니다. Firepower Threat Defense의 경우 모든 라이선싱이 Firepower Management Center에서 처리됩니다.

스위치 요구 사항

- Firepower 4100/9300 섀시에서 클러스터링을 구성하기 전에 스위치 구성을 완료하고 섀시의 모든 EtherChannel을 스위치에 성공적으로 연결하십시오.
- 지원되는 스위치의 목록은 Cisco FXOS 호환성을 참고하십시오.

클러스터링에 대한 라이선스 - Firepower 4100/9300 섀시

각 Firepower 4100/9300 섀시를 License Authority 또는 Satellite 서버에 등록해야 합니다. 슬레이브 유닛에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 섀시용으로 별도의 라이선스를 구매해야 합니다.

각 ASA에는 동일한 암호화 라이선스가 있어야 합니다. 일반 Smart Software Manager 사용자의 경우 Firepower 4100/9300 섀시에서 등록 토큰을 적용할 때 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화됩니다. 이전 Cisco Smart Software Manager Satellite 구축에 대해서는 아래 내용을 참조하십시오.

ASA 라이선스 구성에서는 마스터 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 구성은 슬레이브 유닛에 복제됩니다. 하지만 일부 라이선스의 경우 구성을 사용하지 않고 캐시된 상태로 남으며, 마스터 유닛만 라이선스를 요청합니다. 라이선스는 클러스터 유닛에서 공유된 단일 클러스터 라이선스로 집계되고, 이 집계된 라이선스는 슬레이브 유닛 중 하나가 나중에 마스터 유닛이 되면 사용할 슬레이브 유닛에서도 캐시됩니다. 각 라이선스 유형은 다음과 같이 관리됩니다.

- Standard — 마스터 유닛만 서버에서 Standard 라이선스를 요청합니다. 슬레이브 유닛에서는 기본적으로 Standard 라이선스가 활성화되어 있으므로 이를 사용하기 위해 서버에 등록할 필요가 없습니다.
- Context — 마스터 유닛만 서버에서 Context 라이선스를 요청합니다. Standard 라이선스는 기본적으로 10개의 상황을 포함하며 모든 클러스터 멤버에 있습니다. 각 유닛의 Standard 라이선스 값과 마스터 유닛의 Context 라이선스 값은 집계된 클러스터 라이선스에서 플랫폼 한도에 도달할 때까지 통합됩니다. 예를 들면 다음과 같습니다.
  - 클러스터에 6개의 Firepower 9300 모듈을 갖고 있습니다. Standard 라이선스는 10개의 상황을 포함하고 이러한 라이선스는 6개 유닛에 최대 60개의 상황을 추가합니다. 마스터 유닛에서 20개의 추가 Context 라이선스를 구성합니다. 따라서 집계된 클러스터 라이선스에서는 80개의 상황을 포함합니다. 모듈 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 80개의 상황은 제한을 초과하지 않습니다. 따라서

마스터 유닛에서 최대 80개의 상황을 구성할 수 있습니다. 각 슬레이브 유닛에서도 구성 복제를 통해 80개의 상황을 포함할 수 있습니다.

- 클러스터에 3개의 Firepower 4110 유닛을 갖고 있습니다. Standard 라이선스는 10개의 상황을 포함하고 이러한 라이선스는 3개 유닛에 최대 30개의 상황을 추가합니다. 마스터 유닛에서 250개의 추가 Context 라이선스를 구성합니다. 따라서 집계된 클러스터 라이선스에서는 280개의 상황을 포함합니다. 유닛 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 280개의 상황은 제한을 초과합니다. 따라서 마스터 유닛에서는 최대 250개의 상황만 구성할 수 있습니다. 각 슬레이브 유닛에서도 구성 복제를 통해 250개의 상황을 포함할 수 있습니다. 이 경우 마스터 Context 라이선스만 220개의 상황으로 구성해야 합니다.

- 통신 사업자 — 분산 S2S VPN에 필요합니다. 이 라이선스는 유닛당 엔타이틀먼트이며 각 유닛은 서버에서 고유한 라이선스를 요청합니다. 이 라이선스 구성은 슬레이브 유닛에 복제됩니다.
- 강력한 암호화(3DES)(2.3.0 이전 Cisco Smart Software Manager Satellite 구축에만 해당) — 이 라이선스는 유닛당 엔타이틀먼트이며 각 유닛은 서버에서 고유한 라이선스를 요청합니다. Smart Software Manager Satellite 구축의 경우 ASDM 및 기타 강력한 암호화 기능을 사용하려면 클러스터를 구축한 후에 ASA CLI를 사용하여 마스터 유닛에서 강력한 암호화(3DES) 라이선스를 활성화해야 합니다. 이 라이선스 구성은 슬레이브 유닛에 복제됩니다. 강력한 암호화(3DES) 라이선스는 어떤 유형의 평가 라이선스하고도 함께 사용할 수 없습니다.

새 마스터 유닛이 선택되면 새 마스터 유닛은 집계된 라이선스를 계속해서 사용합니다. 또한 마스터 라이선스를 다시 요청하기 위해 캐시된 라이선스 구성을 사용합니다. 이전 마스터 유닛이 클러스터를 슬레이브 유닛으로 다시 조인하는 경우, 마스터 유닛 라이선스 엔타이틀먼트를 릴리스합니다. 슬레이브 유닛이 라이선스를 릴리스하기 전에 어카운트에서 사용 가능한 라이선스가 없는 경우 마스터 유닛의 라이선스는 비준수 상태일 수 있습니다. 유지된 라이선스는 30일 동안 유효하지만 유예 기간이 지난 후에도 계속해서 비준수 상태인 경우 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다. 새 액티브 유닛은 라이선스 준수 상태가 될 때까지 12시간마다 엔타이틀먼트 권한 부여 갱신 요청을 보냅니다. 라이선스 요청이 완전히 처리될 때까지 구성을 변경하지 않아야 합니다. 유닛이 클러스터를 떠나는 경우, 캐시된 마스터 구성은 제거되는 반면, 유닛당 엔타이틀먼트는 유지됩니다. 특히, 비클러스터 유닛에서 Context 라이선스를 다시 요청해야 합니다.

분산 **S2S VPN**에 대한 라이선스

클러스터의 각 멤버에 있는 분산 S2S VPN에 통신 사업자 라이선스가 필요합니다.

각 VPN 연결에는 두 개의 기타 *VPN* 라이선스 세션(기타 *VPN* 라이선스는 기본 라이선스의 일부임)이 필요합니다. 하나는 액티브 세션용이고 하나는 백업 세션용입니다. 각 세션에 두 개의 라이선스를 사용하기 때문에 클러스터의 최대 VPN 세션 용량은 라이선스가 부여된 용량의 절반을 초과할 수 없습니다.

클러스터링 지침 및 제한 사항

섀시 간 클러스터링을 위한 스위치

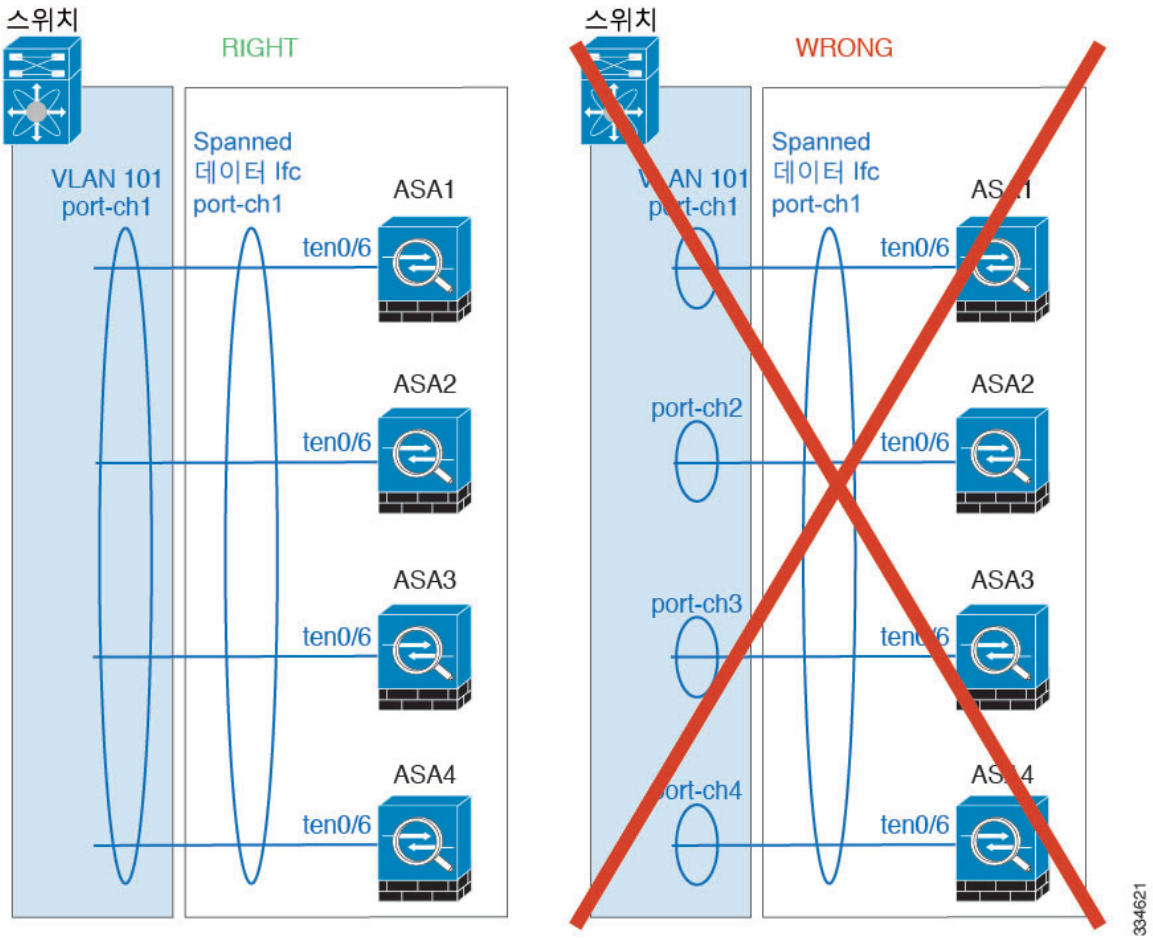
- ASR 9006의 경우 기본이 아닌 MTU를 설정하려면 ASR 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면, **mtu-ignore** 옵션을 사용하지 않는 경우 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 ASR *IPv4* MTU와 일치해야 합니다.
- 클러스터 제어 링크 인터페이스용 스위치의 경우, 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP를 지원하지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 디바이스에 트래픽이 균일하지 않게 분산될 수 있습니다. 클러스터 디바이스에서 로드 밸런싱 알고리즘의 기본값을 변경하지 마십시오.
- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 비활성화하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 클러스터 제어 링크 경로의 스위치에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다.
- Supervisor 2T EtherChannel에서 기본 해시 분산 알고리즘은 적응형입니다. VSS 설계에서 비대칭 트래픽을 방지하려면 클러스터 디바이스에 연결된 포트 채널의 해시 알고리즘을 다음과 같이 변경하여 수정합니다.

  router(config) # **port-channel** *id* **hash-distribution fixed**

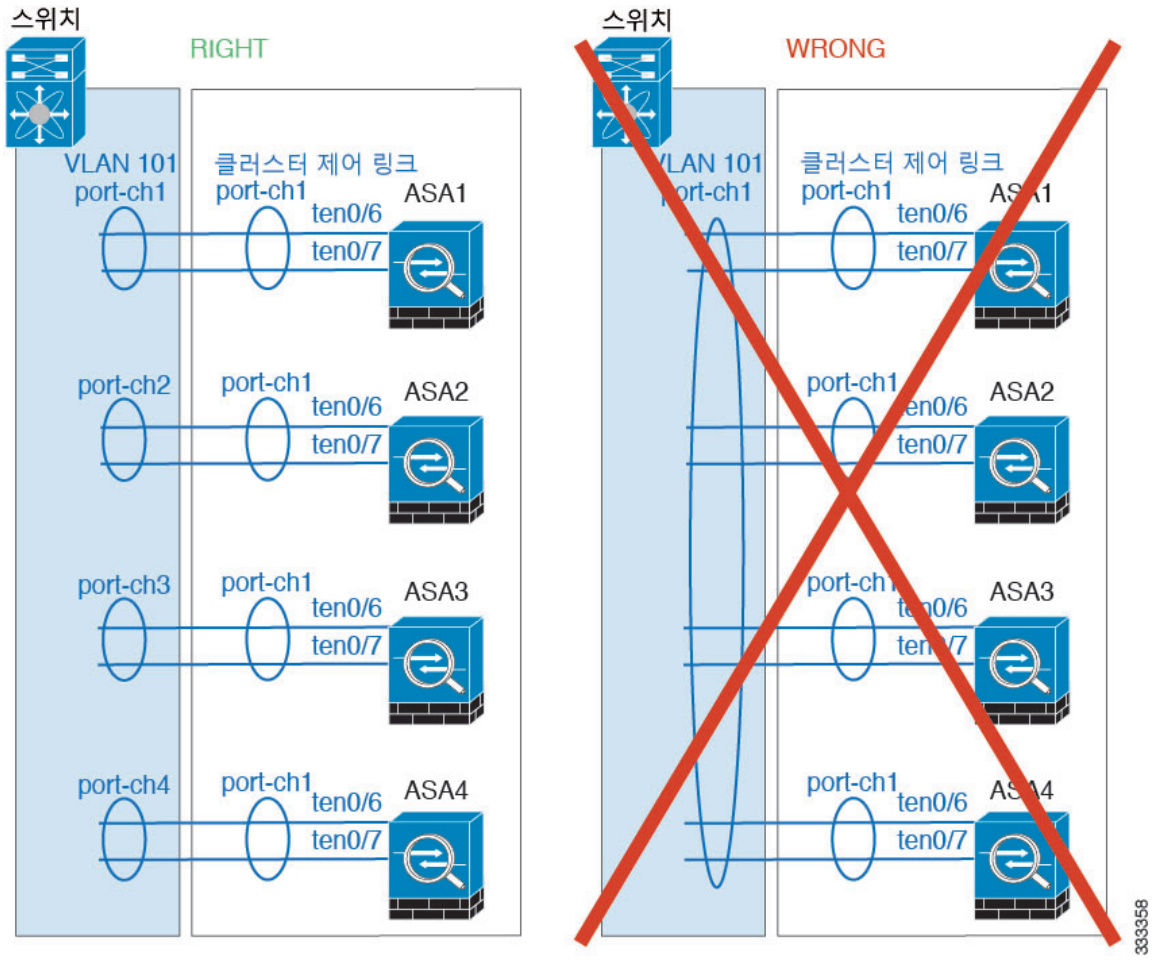
  VSS 피어 링크의 적응형 알고리즘을 활용할 때가 있을 수 있으므로 알고리즘을 전역으로 변경하지 마십시오.

섀시 간 클러스터링을 위한 **EtherChannel**

- 연결 스위치의 경우, EtherChannel 모드를 활성으로 설정합니다. On(켜기) 모드는 Firepower 4100/9300 섀시에서 지원되지 않으며 클러스터 제어 링크에서도 지원되지 않습니다.
- FXOS EtherChannel에서는 기본적으로 LACP 속도가 fast(고속)로 설정됩니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP가 지원되지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.
- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.
- Spanned EtherChannel 구성과 디바이스-로컬 EtherChannel 구성 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에서 각각 알맞게 스위치를 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 *Spanned* EtherChannels의 경우, 인터페이스가 스위치의 단일 EtherChannel에 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



- 디바이스-로컬 EtherChannel - 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 클러스터 유닛 디바이스-로컬 EtherChannel의 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 클러스터 유닛 EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



사이트 간 클러스터링

사이트 간 클러스터링에 대한 다음 지침을 참조하십시오.

- 클러스터 제어 링크 레이턴시는 RTT(왕복 시간)가 20ms 이하여야 합니다.
- 클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 전용 링크를 사용해야 합니다.
- 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 연결이 리밸런싱됩니다.
- 클러스터를 구현할 경우 들어오는 연결에 대한 여러 사이트에 있는 멤버가 구분되지 않습니다. 따라서 하나의 특정한 연결의 연결 역할은 사이트 전체를 포괄하게 될 수 있습니다. 이는 정상적인 동작입니다. 그러나 관리자 지역화를 활성화하는 경우 항상 연결 소유자와 동일한 사이트에서 로컬 관리자 역할이 선택됩니다(사이트 ID에 따라). 원래 소유자가 실패하면 로컬 관리자는 동일한 사이트에서 새 소유자를 선택합니다. (참고: 트래픽이 사이트 간에 비동기 상태이고 원래 소유자가 실패한 이후 원격 사이트로부터 계속해서 트래픽이 발생하면, 원격 사이트의 유닛이 재호스팅 기간 내에 데이터 패킷을 수신하는 경우 새로운 소유자가 될 수 있습니다.)

- 관리자 지역화의 경우 NAT 또는 PAT 트래픽, SCTP에서 검사된 트래픽, 단편화 소유자 쿼리 등의 트래픽 유형은 지역화를 지원하지 않습니다.
- 투명 모드에서, 클러스터가 내부 및 외부 라우터(north-south 삽입이라고도 함) 쌍 사이에 위치하면 내부 라우터 모두에서 MAC 주소를 공유해야 하며 외부 라우터 모두에서도 MAC 주소를 공유해야 합니다. 사이트 1의 클러스터 멤버가 사이트 2의 멤버에 연결을 전달할 경우, 목적지 MAC 주소가 유지됩니다. MAC 주소가 사이트 1의 라우터와 동일할 경우 패킷은 사이트 2의 라우터에만 도달합니다.
- 투명 모드에서 클러스터가 내부 네트워크(East-West 삽입이라고 함) 사이에서 방화벽을 위해 각 사이트에서 데이터 네트워크 및 게이트웨이 라우터 사이에 위치하면 각 게이트웨이 라우터는 HSRP와 같은 첫 번째 홉 이중화 프로토콜(FHRP)을 사용하여 각 사이트에서 동일한 가상 IP 및 MAC 주소 대상을 제공해야 합니다. 데이터 VLAN은 OTV(오버레이 전송 가상화) 또는 유사한 기능을 사용하는 사이트 전체로 확장됩니다. DCI를 통해 다른 사이트로 전송 중인 로컬 게이트웨이 라우터에 예약된 트래픽을 방지하려면 필터를 생성해야 합니다. 게이트웨이 라우터가 1개의 사이트에 연결할 수 없게 되면, 모든 필터를 제거해야 트래픽이 성공적으로 다른 사이트의 게이트웨이에 연결할 수 있습니다.
- Spanned EtherChannel을 사용하는 라우팅 모드의 경우 사이트별 MAC 주소를 구성하십시오. OTV 또는 유사한 것을 사용하여 사이트 전체로 데이터 VLAN을 확장하십시오. 전역 MAC 주소로 향하는 트래픽이 DCI를 통해 다른 사이트에 가지 않도록 필터를 생성해야 합니다. 어떤 사이트에서 클러스터가 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 유닛에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. 사이트 간 클러스터가 확장 세그먼트의 FHR(First Hop Router)로 작동하는 경우에는 동적 라우팅이 지원되지 않습니다.

추가 지침

- 중요한 토폴로지 변경 사항(예: EtherChannel 인터페이스 추가 또는 제거, Firepower 4100/9300 섀시 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대해 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.
- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel 인터페이스에 연결된 Windows 2003 서버를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않아 대량의 ICMP 메시지가 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.
- 이중화를 위해 EtherChannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.
- 섀시 내에서 일부 보안 모듈을 클러스터하여 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.

기본값

- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 연결 리밸런싱은 기본적으로 비활성화되어 있습니다. 연결 리밸런싱을 활성화할 경우 로드 정보를 교환하는 데 걸리는 기본 시간은 5초입니다.
- 실패한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도하도록 설정됩니다.
- 실패한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도하도록 설정됩니다.
- 5초의 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

클러스터링 구성 - Firepower 4100/9300 섀시

Firepower 4100/9300 섀시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다. 이 섹션에서는 ASA에서 수행할 수 있는 기본 부트스트랩 구성 및 맞춤화(선택 사항)에 대해 설명합니다. 이 섹션에서는 ASA 내에서 클러스터 멤버를 관리하는 방법에 대해서도 설명합니다. Firepower 4100/9300 섀시에서 클러스터 멤버십을 관리할 수도 있습니다. 자세한 내용은 Firepower 4100/9300 섀시 설명서를 참조하십시오.

프로시저

단계 **1** FXOS: ASA 클러스터 추가, 491 페이지
단계 **2** ASA: 방화벽 모드 및 상황 모드 변경, 500 페이지
단계 **3** ASA: 데이터 인터페이스 구성, 501 페이지
단계 **4** ASA: 클러스터 구성 맞춤화, 504 페이지
단계 **5** ASA: 클러스터 멤버 관리, 523 페이지

FXOS: ASA 클러스터 추가

단일 Firepower 9300 섀시를 섀시 내 클러스터로 추가하거나 섀시 간 클러스터링용으로 여러 섀시를 추가할 수 있습니다. 섀시 간 클러스터링의 경우 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 추가한 다음 대부분의 동일 설정을 다음 섀시에 입력합니다.

ASA 클러스터 생성

Firepower 4100/9300 섀시에서 클러스터를 구축합니다.

다중 컨텍스트 모드의 경우 먼저 논리적 디바이스를 구축한 다음 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화해야 합니다.

Firepower 4100/9300 섀시에서 라우팅된 방화벽 모드 또는 투명 방화벽 모드 ASA를 구축할 수 있습니다.

클러스터를 구축할 때 Firepower 4100/9300 섀시 수퍼바이저는 다음 부트스트랩 구성을 사용하여 각 ASA 애플리케이션을 구성합니다. 필요한 경우 나중에 ASA에서 일부 부트스트랩 구성을 수정할 수 있습니다(굵은 텍스트로 표시됨).

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

참고 **local-unit** 이름은 클러스터링을 비활성화하는 경우에만 변경할 수 있습니다.

시작하기 전에

- 모듈을 설치하지 않은 경우에도 Firepower 9300 섀시의 3개 모듈 슬롯 모두에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.
- 멤버 인터페이스가 포함되지 않은 경우, **Interfaces(**인터페이스**)** 탭에서 port-channel 48 클러스터 유형 인터페이스에 **Operation State(**운영 상태**)**가 **failed(**실패**)**로 표시됩니다. 인트라 섀시 클러스터링(intra-chassis clustering)의 경우 이 EtherChannel에는 멤버 인터페이스가 필요하지 않으므로 이 Operation State(운영 상태)를 무시할 수 있습니다.

프로시저

단계 1 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(포트 채널)을 최소 1개 구성합니다. EtherChannel(포트 채널) 추가, 172 페이지 또는 실제 인터페이스 구성, 170 페이지를 참조하십시오.

모든 인터페이스는 클러스터에 기본적으로 할당되어 있습니다. 또한 데이터 인터페이스를 구축한 후에 클러스터에 추가할 수 있습니다.

섀시 간 클러스터링의 경우, 모든 데이터 인터페이스는 멤버 인터페이스가 최소 1개 있는 EtherChannel이어야 합니다. 각 섀시에 EtherChannel을 추가합니다.

단계 2 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. EtherChannel(포트 채널) 추가, 172 페이지 또는 실제 인터페이스 구성, 170 페이지를 참조하십시오.

관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 인터페이스(FXOS에서 MGMT, management0 또는 기타 유사한 이름으로 표시되는 섀시 관리 인터페이스 확인 가능)와는 다릅니다.

단계 3 Port-channel 48은 클러스터 제어 링크로 예약됩니다. 섀시 간 클러스터링의 경우, 멤버 인터페이스 최소 1개를 port-channel 48에 추가합니다.

단계 4 보안 서비스 모드를 입력합니다.

scope ssa

예제:

```
Firepower # scope ssa
Firepower /ssa #
```

단계 5 클러스터를 생성합니다.

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name* - Firepower 4100/9300 섀시 수퍼바이저가 클러스터링 설정을 구성하고 인터페이스를 할당할 때 사용합니다. 이는 보안 모듈 구성에 사용되는 클러스터 이름이 아닙니다. 하드웨어를 아직 설치하지 않은 경우에도 보안 모듈 3개를 모두 지정해야 합니다.
- *slots* - 섀시 모듈을 클러스터에 할당합니다. Firepower 4100의 경우 **1**을 지정합니다. Firepower 9300의 경우 **1,2,3**을 지정합니다. 모듈을 설치하지 않은 경우에도 Firepower 9300 섀시의 3개 모듈 슬롯 모두에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.

예제:

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

단계 6 관리 부트스트랩 개체를 생성합니다.

enter mgmt-bootstrap asa

예제:

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

단계 **7** 논리적 디바이스가 작동할 모드(Routed(라우팅됨) 또는 Transparent(투명))를 지정합니다.

enter bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

단계 **8** 관리자 비밀번호를 지정합니다.

enter bootstrap-key-secret PASSWORD

set value

exit

exit

비밀번호를 복구할 때는 사전 구성된 ASA 관리자가 있으면 유용합니다. FXOS 액세스 권한이 있다면 관리자 비밀번호를 잊어버린 경우 재설정할 수 있습니다.

예제:

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: happytuesday
Confirm the value: happytuesday
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

단계 **9** 클러스터 매개변수를 구성합니다.

enter cluster-bootstrap

예제:

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

단계 **10** 보안 모듈 구성에서 클러스터 그룹 이름을 설정합니다.

set service-type *cluster_name*

예제:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

이름은 1자 ~ 38자로 된 ASCII 문자열이어야 합니다.

단계 **11** 클러스터 인터페이스 모드를 설정합니다.

set mode spanned-etherchannel

예제**:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

Spanned EtherChannel 모드는 유일하게 지원되는 모드입니다.

단계 **12** 관리 IP 주소 정보를 구성합니다.

이 정보는 보안 모듈 구성의 관리 인터페이스를 구성하는 데 사용됩니다.

a) 로컬 IP 주소의 풀을 구성합니다. 이 중 하나는 인터페이스의 각 클러스터 유닛에 할당됩니다.

set ipv4 pool*start_ip end_ip*

set ipv6 pool *start_ip end_ip*

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. Firepower 9300에서는 모든 모듈 슬롯을 채우지 않은 경우에도 새시당 3개 주소를 포함해야 합니다. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 마스터 유닛에 속하는 가상 IP 주소(기본 클러스터 IP 주소)는 이러한 풀에 속하지 않습니다. 따라서 동일한 네트워크에서 기본 클러스터 IP 주소에 대한 IP 주소를 예약해 두어야 합니다. IPv4 및/또는 IPv6 주소를 사용할 수 있습니다.

b) 관리 인터페이스의 기본 클러스터 IP 주소를 구성합니다.

set virtual ipv4 *ip_address* **mask** *mask*

set virtual ipv6 *ip_address* **prefix-length** *prefix*

이 IP 주소는 같은 네트워크의 클러스터 풀 주소로 있어야 하지만 풀의 일부는 아닙니다.

c) 네트워크 게이트웨이 주소를 입력합니다.

set ipv4 gateway *ip_address*

set ipv6 gateway *ip_address*

예제**:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1 prefix-length
 64
```

단계 **13** 섀시 ID를 설정합니다.

set chassis-id *id*

클러스터의 각 섀시에는 고유한 ID가 필요합니다.

예제:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

단계 **14** 사이트 간 클러스터링의 경우 1~8의 사이트 ID를 설정합니다.

set site-id *number*.

예제:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

단계 **15** 클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 구성합니다.

set key

예제:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

공유 비밀을 입력하라는 프롬프트가 표시됩니다.

공유 비밀은 1자 ~ 63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 옵션은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

단계 **16** (선택 사항) 클러스터 제어 링크 IP 네트워크를 설정합니다.

set cluster-control-link network ***a*.*b*.0.0**

기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 이 경우 클러스터용 고유 네트워크에서 /16 주소를 지정할 수 있습니다.

- ***a*.*b*.0.0** - 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외한 모든 /16 네트워크 주소를 지정합니다. 값을 0.0.0.0으로 설정하는 경우 기본 네트워크(127.2.0.0)가 사용됩니다.

섀시에서는 섀시 ID 및 슬롯 ID *a.b.chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.

예제:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network 10.10.0.0
```

단계 **17** 클러스터 부트스트랩 모드 및 논리적 디바이스 모드를 종료합니다.

exit

exit

단계 **18** 사용 가능한 소프트웨어 버전을 확인한 다음 사용할 버전을 설정합니다.

a) 사용 가능한 버전을 표시합니다.

show app

예제:

```
/ssa # show app

Application:
    Name       Version    Description Author     Deploy Type  CSP Type    Is Default App

    ---------- ---------- ----------- ---------- -----------  ----------- --------------

    asa        9.1.4.152  N/A         cisco      Native       Application Yes
    asa        9.4.2      N/A         cisco      Native       Application No
    asa        9.5.2.1    N/A         cisco      Native       Application No
```

b) 사용할 버전의 앱 모드를 입력합니다.

scope app asa*version_number*

c) 이 버전을 기본값으로 설정합니다.

set-default

d) 앱 모드를 종료합니다.

exit

예제:

```
/ssa* # scope app asa 9.5.2.1
/ssa/app* # set-default
/ssa/app* # exit
/ssa* #
```

단계 **19** 구성을 커밋합니다.

commit-buffer

Firepower 4100/9300 섀시 관리자(supervisor)는 기본 보안 모듈 소프트웨어 버전을 다운로드하고 클러스터 부트스트랩 구성 및 관리 인터페이스 설정을 각 보안 모듈에 입력하여 클러스터를 구축합니다.

단계 **20** 클러스터에 다른 섀시를 추가하려면 고유한 **chassis-id** 및 올바른 **site-id**를 구성해야 하는 경우를 제외하고 이 절차를 반복합니다. 아니면 두 섀시 모두에 동일한 구성을 사용합니다.

인터페이스 구성은 새 섀시에서 동일해야 합니다. FXOS 섀시 구성 내보내기와 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.

단계 **21** 마스터 유닛 ASA에 연결하여 클러스터링 구성을 맞춤 설정합니다.

예

섀시 1의 경우:

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
```

```
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

섀시 2의 경우:

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
```

```
    set ipv4 pool 10.1.1.11 10.1.1.15
    set ipv6 gateway 2001:DB8::AA
    set ipv6 pool 2001:DB8::11 2001:DB8::19
    set key
    Key: f@rscape
    set mode spanned-etherchannel
    set service-type cluster1
    set virtual ipv4 10.1.1.1 mask 255.255.255.0
    set virtual ipv6 2001:DB8::1 prefix-length 64
    exit
  exit
scope app asa 9.5.2.1
  set-default
  exit
commit-buffer
```

클러스터 멤버 더 추가

ASA 클러스터 멤버를 추가하거나 교체합니다.

참고 이 절차는 새시 추가 또는 교체 시에만 적용됩니다. 클러스터링이 이미 활성화된 Firepower 9300에 모듈을 추가하거나 교체하는 경우에는 모듈이 자동으로 추가됩니다.

시작하기 전에

- 기존 클러스터에서 이 새 멤버의 관리 IP 주소 풀에 충분한 IP 주소가 있는지 확인하십시오. IP 주소가 충분하지 않은 경우, 이 새 멤버를 추가하기 전에 각 새시에서 기존 클러스터 부트스트랩 구성을 수정해야 합니다. 이러한 변경으로 인해 논리적 디바이스가 재시작됩니다.
- 인터페이스 구성은 새 새시에서 동일해야 합니다. FXOS 새시 구성 내보내기와 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.
- 다중 컨텍스트 모드의 경우 첫 번째 클러스터 멤버의 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화합니다. 그러면 추가 클러스터 멤버가 다중 컨텍스트 모드 구성을 자동으로 상속합니다.

프로시저

클러스터에 다른 새시를 추가하려면 고유한 **chassis-id** 및 올바른 **site-id**를 구성해야 하는 경우를 제외하고 ASA 클러스터 생성, 491 페이지의 절차를 반복합니다. 아니면 새 새시에 동일한 구성을 사용합니다.

ASA: 방화벽 모드 및 상황 모드 변경

기본적으로 FXOS 새시에서는 라우팅 방화벽 모드와 단일 상황 모드에서 클러스터를 구축합니다.

- 방화벽 모드 변경 — 구축한 후에 모드를 변경하려면 마스터 유닛에서 모드를 변경합니다. 모드는 일치시킬 모든 슬레이브 유닛에서 자동으로 변경됩니다. 방화벽 모드, 198 페이지의 내용을 참조하십시오. 다중 상황 모드에서는 상황별로 방화벽 모드를 설정합니다.
- 여러 상황 모드로 변경 — 구축한 후에 여러 상황 모드로 변경하려면 마스터 유닛에서 모드를 변경합니다. 모드는 일치시킬 모든 슬레이브 유닛에서 자동으로 변경됩니다. 다중 상황 모드 활성화, 232 페이지을 참조하십시오.

ASA: 데이터 인터페이스 구성

이 절차에서는 FXOS에서 클러스터를 구축할 때 클러스터에 할당한 각 데이터 인터페이스의 기본 파라미터를 구성합니다. 섀시 간 클러스터링의 경우, 데이터 인터페이스는 항상 Spanned EtherChannel 인터페이스입니다.

참고 관리 인터페이스는 클러스터를 구축할 때 사전 구성되어 있습니다. ASA에서 관리 인터페이스 파라미터를 변경할 수도 있지만 이 절차에서는 데이터 인터페이스에 중점을 두고 있습니다. 관리 인터페이스는 Spanned 인터페이스와는 달리 개별 인터페이스입니다. 자세한 내용은 관리 인터페이스, 474 페이지를 참조하십시오.

시작하기 전에

- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 시작합니다. 현재 시스템 구성 모드가 아닌 경우 Configuration(구성) > Device List(디바이스 목록) 창의 활성 디바이스 IP 주소에서 **System(시스템)**을 두 번 클릭하여 **changeto system** 명령.
- 투명 모드의 경우 브리지 그룹을 구성합니다.
- 섀시 간 클러스터링을 위해 Spanned EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 나타나지 않습니다. 이러한 요구 사항으로 인해 클러스터의 활성 유닛이 아닌 유닛에는 트래픽이 전달되지 않습니다.

프로시저

단계 **1** 인터페이스 ID를 지정합니다.

interface *id*

이 클러스터에 할당된 인터페이스에 대해서는 FXOS 섀시를 참조하십시오. 인터페이스 ID는 다음 값이 가능합니다.

- **port-channel** *integer*
- **ethernet** *slot/port*

예제:

```
ciscoasa(config)# interface port-channel 1
```

단계 **2** 인터페이스를 활성화합니다.

no shutdown

단계 **3** (선택 사항) 이 인터페이스에 VLAN 하위 인터페이스를 생성 중인 경우, 해당 작업을 지금 수행합니다.

예제**:**

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

이 절차의 나머지는 하위 인터페이스에 적용됩니다.

단계 **4** (다중 상황 모드) 인터페이스를 상황에 할당한 다음, 상황으로 변경하고 인터페이스 모드로 들어갑니다.

예제**:**

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

다중 상황 모드의 경우, 각 상황에서 인터페이스 컨피그레이션의 나머지 부분이 이루어집니다.

단계 **5** 인터페이스 이름을 지정합니다.

nameif *name*

예제**:**

```
ciscoasa(config-if)# nameif inside
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다.

단계 **6** 방화벽 모드에 따라 다음 중 하나를 수행합니다.

- 라우팅 모드—IPv4 및/또는 IPv6 주소를 설정합니다.

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

  예:

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ```

```
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
```

DHCP, PPPoE, IPv6 자동 구성은 지원되지 않습니다. 포인트 투 포인트 연결을 위해 31비트 서브넷 마스크(255.255.255.254)를 지정할 수 있습니다. 이 경우 IP 주소가 네트워크 또는 브로드캐스트 주소에 대해 예약되어 있습니다.

- 투명 모드 — 브리지 그룹에 인터페이스를 할당합니다.

  bridge-group *number*

  예:

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  *number*는 1에서 100까지의 정수입니다. 최대 64개의 인터페이스를 하나의 브리지 그룹에 할당할 수 있습니다. 동일한 인터페이스를 둘 이상의 브리지 그룹에 할당할 수 없습니다. BVI 구성에는 IP 주소가 포함되어 있습니다.

단계 **7** 보안 수준을 설정합니다.

security-level *number*

예제**:**

```
ciscoasa(config-if)# security-level 50
```

*number*는 0(최저) ~ 100(최고) 범위의 정수입니다.

단계 **8** (섀시 간 클러스터링) 잠재적인 네트워크 연결 문제를 방지하기 위해 Spanned EtherChannel에 대한 전역 MAC 주소를 구성합니다.

mac-address *mac_address*

- *mac_address* — MAC 주소는 H.H.H 형식이며, 여기서 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. 자동 생성된 MAC 주소도 사용하려는 경우 수동 MAC 주소의 처음 2바이트는 A2가 될 수 없습니다.

수동 구성된 MAC 주소를 사용할 경우, 해당 MAC 주소가 현재 마스터 유닛에 유지됩니다. MAC 주소를 구성하지 않은 상태에서 마스터 유닛을 변경하는 경우, 새 마스터 유닛은 인터페이스의 새 MAC 주소를 사용하며 이로 인해 임시 네트워크가 중단될 수 있습니다.

다중 상황 모드에서 상황 간에 인터페이스를 공유할 경우, 대신 MAC 주소의 자동 생성을 활성화해야 하며 이렇게 해야 MAC 주소를 수동으로 설정할 필요가 없습니다. 공유되지 않는 인터페이스에 이 명령을 사용하여 MAC 주소를 수동으로 구성해야 합니다.

예제**:**

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

단계 **9** (사이트 간 클러스터링) 사이트별 MAC 주소 및 각 사이트의 IP 주소(라우팅 모드의 경우)를 구성합니다.

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

예제:

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

사이트별 IP 주소는 전역 IP 주소와 동일한 서브넷에 있어야 합니다. 유닛에서 사용한 사이트별 MAC 주소 및 IP 주소는 각 유닛의 부트스트랩 구성에서 지정한 사이트 ID에 따라 달라집니다.

ASA: 클러스터 구성 맞춤화

클러스터를 구축한 후에 부트스트랩 설정을 변경하거나 추가 옵션을 구성하려는 경우(예: 클러스터링 상태 모니터링, TCP 연결 복제 지연, 플로우 모빌리티 및 기타 최적화), 마스터 유닛에서 해당 작업을 수행할 수 있습니다.

기본 ASA 클러스터 파라미터 구성

마스터 유닛에서 클러스터 설정을 맞춤화할 수 있습니다.

시작하기 전에

- 다중 상황 모드에서는 마스터 유닛의 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.
- 로컬 유닛의 name(이름) 및 기타 여러 옵션은 FXOS 섀시에서만 설정될 수 있습니다. 또는 이러한 옵션은 클러스터링을 비활성화하는 경우, ASA에서만 변경될 수 있습니다. 따라서 다음 절차에는 포함되지 않습니다.

프로시저

단계 **1** 이 유닛이 마스터 유닛인지 확인합니다.

show cluster info

예제:

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
```

```
        CCL MAC    : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID         : 4
        Version    : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP     : 127.2.1.3
        CCL MAC    : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID         : 1
        Version    : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP     : 127.2.1.1
        CCL MAC    : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID         : 3
        Version    : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP     : 127.2.2.1
        CCL MAC    : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

다른 유닛이 마스터 유닛인 경우, 연결을 종료하고 올바른 유닛에 연결합니다. Firepower 4100용 Cisco ASA 빠른 시작 가이드 또는 ASA 콘솔 액세스에 대한 내용은 Firepower 9300용 Cisco ASA 빠른 시작 가이드를 참조하십시오.

단계 **2** 클러스터 제어 링크 인터페이스의 MTU(Maximum Transmission Unit)를 지정합니다.

mtu cluster 바이트

예제:

```
ciscoasa(config)# mtu cluster 9000
```

MTU를 최댓값인 9184바이트로 설정하는 것이 좋습니다. 최솟값은 1400바이트입니다.

단계 **3** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

단계 **4** (선택 사항) 슬레이브 유닛에서 마스터 유닛으로의 콘솔 복제를 활성화합니다.

console-replicate

이 기능은 기본적으로 비활성화되어 있습니다. ASA에서는 중요한 특정 이벤트 발생 시 일부 메시지를 콘솔에 직접 출력합니다. 콘솔 복제를 활성화할 경우, 슬레이브 유닛에서는 콘솔 메시지를 마스터 유닛에 전송하므로 클러스터의 콘솔 포트 하나만 모니터링하면 됩니다.

단계 **5** 클러스터링 이벤트의 최소 추적 레벨을 설정합니다

trace-level 레벨

원하는 대로 최소 레벨을 설정합니다.

- **critical**— 중요 이벤트(심각도=1)
- **warning**— 경고(심각도=2)
- **informational**— 정보 이벤트(심각도=3)
- **debug**— 디버깅 이벤트(심각도=4)

단계 **6** (선택 사항) LACP의 동적 포트 우선순위를 비활성화합니다.

clacp static-port-priority

일부 스위치에서는 동적 포트 우선순위를 지원하지 않으므로, 이 명령을 사용하면 스위치 호환성이 개선됩니다. 또한 이 명령을 사용하면 8개 이상의 활성 스팬 EtherChannel 멤버를 지원하는 것이 허용되므로 최대 32개의 멤버를 지원할 수 있습니다. 이 명령을 사용하지 않을 경우 8개의 활성 멤버 및 8개의 대기 멤버만 지원됩니다. 이 명령을 활성화할 경우 대기 멤버를 사용할 수 없으며 모든 멤버가 활성 상태로 됩니다.

단계 **7** (선택 사항) (Firepower 9300만 해당) 트래픽이 모듈 간에 고르게 분산되도록 섀시에서 보안 모듈이 클러스터에 동시에 참가하는지 확인합니다. 모듈이 다른 모듈보다 훨씬 먼저 참가하는 경우, 다른 모듈이 로드를 아직 공유할 수 없기 때문에 이 모듈은 원하는 트래픽보다 더 많은 트래픽을 받을 수 있습니다.

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

- *num_of_units* — 모듈이 클러스터에 참가하기 전에 준비해야 하는 동일한 섀시의 최소 모듈 수를 1~3 범위에서 지정합니다. 기본값은 1인데, 이는 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하지 않는다는 것을 의미합니다. 예를 들어, 값을 3으로 설정하는 경우, 각 모듈이 클러스터에 참가하기 전에 *max_delay_time*동안 대기하거나 3개의 모듈이 모두 준비 상태가 될 때까지 대기합니다. 3개 모듈 모두 클러스터에 거의 동시에 참가하도록 요청하며 비슷한 시간에 트래픽을 수신하기 시작합니다.
- *max_delay_time* — 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하는 것을 중지하기 전의 최대 지연 시간(분)을 0~30분 범위에서 지정합니다. 기본값은 0인데, 이는 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하지 않는다는 것을 의미합니다. *num_of_units*을 1로 설정하는 경우 이 값은 0이어야 합니다. *num_of_units*을 2 또는 3으로 설정하는 경우 이 값은 1 이상이어야 합니다. 이 타이머는 모듈별로 할당되지만 첫 번째 모듈이 클러스터에 참가하면 다른 모든 모듈 타이머가 종료되고 나머지 모듈은 클러스터에 참가합니다.

예를 들어, *num_of_units*을 3으로 설정하고 *max_delay_time*을 5분으로 설정합니다. 모듈 1이 나타나면 5분 타이머가 시작됩니다. 2분 후에 모듈 2가 나타나고 5분 타이머가 시작됩니다. 1분 후에 모듈 3이 나타나므로 4분으로 표시될 때는 이제 모든 모듈이 클러스터에 참가하게 되며, 모든 모듈은 타이머가 완료될 때까지 대기하지 않습니다. 모듈 3이 나타나지 않으면 모듈 1이 5분 타이머 종료 시 클러스터에 참가하게 되고, 모듈 2 또한 참가하게 되는데(타이머에 아직 2분이 남아 있는 경우에도) 이는 타이머가 완료할 때까지 대기하지 않습니다.

상태 모니터링 및 자동 재참가 설정 구성

이 절차에서는 유닛 및 인터페이스 상태 모니터링을 구성합니다.

필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다. 모든 포트 채널 ID 또는 단일 물리적 인터페이스 ID를 모니터링할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

단계 **2** 클러스터 유닛 상태 검사 기능을 맞춤화합니다.

health-check [**holdtime** *timeout*]

예제**:**

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

대기 시간은 유닛 하트비트 상태 메시지 간의 시간 간격을 0.3~45초 범위에서 지정합니다(기본값은 3초).

유닛 상태를 확인하기 위해 ASA 클러스터 유닛에서는 다른 유닛에 대한 클러스터 제어 링크에서 하트비트 메시지를 보냅니다. 유닛이 피어 유닛의 하트비트 메시지를 대기 시간 내에 수신하지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주됩니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, ASA, Firepower 4100/9300 섀시 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능을 비활성화하고 비활성화된 인터페이스(**no health-check monitor-interface**)에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.

단계 **3** 인터페이스에서 인터페이스 상태 검사를 비활성화합니다.

no health-check monitor-interface [*interface_id* | **service-application**]

예제**:**

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 유닛에서 오류가 발생했지만 다른 유닛에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 유닛은 클러스터에서 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다.

상태 선택은 모든 인터페이스에 대해 기본적으로 활성화됩니다. 이 명령의 **no** 형식을 사용하여 인터페이스별로 비활성화할 수 있습니다. 필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다. 데코레이터 애플리케이션의 모니터링을 비활성화하려면 **service-application**을 지정합니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, ASA, Firepower 4100/9300 섀시 또는 스위치에서 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능(**no health-check**)을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.

단계 **4** 상태 검사에 실패한 후에 자동 다시 참가 클러스터 설정을 맞춤화합니다.

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**— 내부 오류에 대한 자동 다시 참가 설정을 지정합니다. 내부 오류 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등
- **unlimited** — (**cluster-interface**의 기본값) 다시 참가 시도 횟수를 제한하지 않습니다.
- *auto-rejoin-max* — 다시 참가 시도 횟수를 0~65535 사이로 설정합니다. **0**은 자동 다시 참가를 비활성화합니다. **data-interface** 및 **system**에 대한 기본값은 3입니다.
- *auto_rejoin_interval* — 다시 참가 시도 간의 간격 기간(분)을 2~60분 사이로 정의합니다. 기본값은 5분입니다. 유닛이 클러스터에 다시 참가하려고 시도하는 최대 총 시간은 마지막 장애 시간으로부터 14400분(10일)으로 제한됩니다.
- *auto_rejoin_interval_variation* — 간격 기간이 증가하는지 여부를 정의합니다. 1~3 사이의 값 설정: **1**(변경 없음), **2**(2 x 이전 기간) 또는 **3**(3 x 이전 기간)입니다. 예를 들어, 간격 기간을 5분으로 설정하고 변수를 2로 설정하면 첫 번째 시도가 5분 후에 일어나고 두 번째 시도는 10분(2 x 5), 세 번째 시도는 20분(2 x 10) 후에 일어납니다. 기본값은 클러스터 인터페이스의 경우 **1**이며 데이터 인터페이스 및 시스템의 경우 **2**입니다.

예제**:**

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

단계 **5** ASA가 인터페이스를 실패 상태로 간주하고 유닛이 클러스터에서 제거되기 전에 디바운스 시간을 구성합니다.

health-check monitor-interface debounce-time 밀리초

예제**:**

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

디바운스 시간을 300~9000밀리초 범위에서 설정합니다. 기본값은 500ms입니다. 값이 낮을수록 인터페이스 오류 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 지정되어 있는 밀리초 동안 대기합니다. 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다.

단계 **6** 섀시 상태 검사 간격을 구성합니다.

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

예제**:**

```
ciscoasa(config)# app-agent heartbeat interval 300
```

ASA에서는 호스트인 Firepower 섀시와 백플레인을 통해 통신할 수 있는지 확인합니다.

- **interval** *ms* — 하트비트 사이의 시간을 100의 배수인 100~6000밀리초 범위에서 설정합니다. 기본값은 1000ms입니다.
- **retry-count** *number* —- 재시도 횟수를 1~30 범위에서 설정합니다. 기본값은 3회입니다.

최소 결합 시간(간격 x 재시도 횟수)은 600밀리초보다 적을 수 없습니다. 예를 들어, 간격을 100으로 설정하고 재시도 횟수를 3으로 설정하는 경우 총 결합 시간은 300밀리초인데 이는 지원되지 않는 값입니다. 예를 들어, 최소 시간(600밀리초)을 충족하기 위해 간격을 100으로 설정하고 재시도 횟수를 6으로 설정할 수 있습니다.

연결 리밸런싱 및 클러스터 **TCP** 복제 지연 구성

연결 리밸런싱을 구성할 수 있습니다. 관리자/백업 플로우 생성을 지연시켜 짧은 수명의 플로우와 관련된 "불필요한 작업"을 제거하는 데 도움을 주기 위해 TCP 연결에 대해 클러스터 복제 지연을 활성화할 수 있습니다. 관리자/백업 플로우가 생성되기 전에 유닛에서 오류가 발생하는 경우, 이러한 플로우는 복구될 수 없습니다. 마찬가지로 플로우가 생성되기 전에 트래픽이 다른 유닛으로 리밸런싱되며 플로우는 복구될 수 없습니다. TCP 임의화를 비활성화하도록 설정한 트래픽에 대해 TCP 복제 지연을 활성화하지 않아야 합니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

단계 **2** (선택 사항) TCP 트래픽을 위해 연결 재밸런싱을 활성화합니다.

conn-rebalance [**frequency** *seconds*]

예제**:**

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

이 명령은 기본적으로 비활성화되어 있습니다. 활성화할 경우 ASA에서는 로드 정보를 주기적으로 교환하며, 로드가 과중한 디바이스에서 적은 디바이스로 새 연결을 오프로드합니다. 빈도는 1에서 360초 사이이며, 로드 정보를 교환하는 빈도를 지정합니다. 기본값은 5일입니다.

사이트 간 토폴로지에 대한 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 대한 연결이 리밸런싱됩니다.

단계 **3** TCP 연결에 대해 클러스터 복제 지연을 활성화합니다.

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

예제**:**

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

1~15 사이의 초를 설정합니다. **http** 지연은 기본적으로 5초 동안 활성화됩니다.

사이트 간 기능 구성

사이트 간 클러스터링의 경우, 구성을 맞춤화하여 이중화 및 안정성을 개선할 수 있습니다.

관리자 현지화 활성화

데이터 센터에 대한 사이트 간 클러스터링을 위해 성능을 개선하고 왕복 시간 레이턴시를 줄이기 위해 관리자 현지화를 활성화할 수 있습니다. 새로운 연결은 일반적으로 로드 밸런싱 상태이며 지정된 사이트 내부의 클러스터 멤버가 소유합니다. 그러나 ASA는 모든 사이트에서 멤버에 관리자 역할을 할당합니다. 관리자 현지화를 사용하면 추가 관리자 역할이 활성화됩니다. 즉, 소유자와 동일한 사이트의 로컬 관리자와 모든 사이트의 전역 관리자 역할이 활성화됩니다. 소유자와 관리자를 동일한 사이트에서 유지하면 성능이 향상됩니다. 또한 원래 소유자가 실패할 경우, 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다. 전역 관리자는 클러스터 멤버가 다른 사이트에서 소유하는 연결에 대한 패킷을 수신하는 경우 사용됩니다.

시작하기 전에

- Firepower 4100/9300 섀시 수퍼바이저에서 섀시의 사이트 ID를 설정합니다.
- NAT 또는 PAT 트래픽, SCTP에서 검사된 트래픽, 단편화 소유자 쿼리 등의 트래픽 유형은 현지화를 지원하지 않습니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

단계 **2** 관리자 현지화를 활성화합니다.

director-localization

사이트 이중화 활성화

사이트 장애로부터 플로우를 보호하기 위해 사이트 이중화를 활성화할 수 있습니다. 연결 백업 소유자가 소유자와 같은 사이트에 있으면 사이트 장애로부터 플로우를 보호하기 위해 다른 사이트에서 추가 백업 소유자가 선택됩니다.

시작하기 전에

- Firepower 4100/9300 섀시 관리자(Supervisor)에서 섀시의 사이트 ID를 설정합니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

단계 **2** 사이트 이중화를 활성화합니다.

site-redundancy

클러스터 플로우 모빌리티 구성

서버가 사이트 간에 이동하는 경우 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

LISP 검사 정보

사이트 간에 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

LISP 정보

VMware VMotion과 같은 데이터 센터 가상 머신 모빌리티를 통해 서버는 클라이언트에 대한 연결을 유지하면서 데이터 센터 간에 데이터를 마이그레이션할 수 있습니다. 그러한 데이터 센터 서버 모빌리티를 지원하려면 라우터는 이동 시 서버에 대한 인그레스 경로를 업데이트할 수 있어야 합니다. Cisco LISP(Locator/ID Separation Protocol) 아키텍처는 디바이스 ID 또는 EDI(endpoint identifier)를 해당 위치 또는 RLOC(routing locator)에서 두 개의 서로 다른 숫자 공간으로 분리하여, 서버 마이그레이션을 클라이언트에 투명하게 만듭니다. 예를 들어 서버가 새 사이트로 이동하고 클라이언트가 서버로 트래픽을 전송하면, 라우터가 트래픽을 새 위치로 리디렉션합니다.

LISP에는 LISP ETR(egress tunnel router), ITR(ingress tunnel router), FHR(first hop router), MR(map resolver), MS(map server) 같은 특정 역할의 라우터 및 서버가 필요합니다. 서버에 대한 FHR(first hop router)은 서버가 다른 라우터에 연결된 것을 감지하면, 클라이언트에 연결된 ITR이 트래픽을 가로채고 캡슐화하여 새로운 서버 위치로 전송할 수 있도록 다른 모든 라우터 및 데이터베이스를 업데이트합니다.

ASA LISP 지원

ASAASAASA는 LISP 자체를 실행하지 않습니다. 그러나 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작동을 위해 이 정보를 사용할 수 있습니다. LISP 통합이 없으면 서버가 새 사이트로 이전할 경우, 원래의 플로우 소유자 대신 새 사이트의 ASA 클러스터 멤버로 트래픽이 전달됩니다. 새 ASA가 트래픽을 이전 사이트의 ASA로 전달하면, 이전 ASA는 서버에 도달하기 위해 트래픽을 다시 새 사이트로 전송합니다. 이 트래픽 플로우는 차선책이며, "tromboning" 또는 hair-pinning"으로 알려져 있습니다.

LISP 통합 시 ASA 클러스터 멤버는 FHR(first hop router)과 ETR 또는 ITR 간에 전달되는 LISP 트래픽을 검사할 수 있으며, 그런 다음 플로우 소유자가 새 사이트에 있도록 변경할 수 있습니다.

LISP 지침

- ASA 클러스터 멤버는 FHR과 사이트의 ITR 또는 ETR 사이에 상주해야 합니다. ASA 클러스터 자체는 확장 세그먼트의 FHR이 될 수 없습니다.
- 완전히 분산된 플로우만 지원됩니다. 중앙 집중식 플로우, 반 분산 플로우 또는 개별 유닛에 속한 플로우는 새 소유자로 이동하지 않습니다. 반 분산 플로우에는, 상위 플로우를 소유하는 동일한 ASA가 모든 하위 플로우도 소유하는 SIP 같은 애플리케이션이 포함됩니다.
- 클러스터는 계층 3 및 4 플로우 상태만 이동하므로, 일부 애플리케이션 데이터가 손실될 수 있습니다.
- 수명이 짧은 플로우 또는 비즈니스 크리티컬 플로우의 경우 소유자를 이동하는 것이 의미가 없을 수 있습니다. 검사 정책을 구성할 때 이 기능으로 지원되는 트래픽의 유형을 제어할 수 있으며, 플로우 모빌리티를 필수 트래픽으로 제한해야 합니다.

ASA LISP 구현

이 기능에는 몇 가지 상호 연결된 구성이 포함됩니다(모두 이 장에서 설명).

1. (선택 사항) Limit inspected EIDs based on the host or server IP address(호스트 또는 서버 IP 주소를 기반으로 검사된 EID 제한) - FHR(first hop router)은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EDI를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개

뿐이지만 LISP가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다.

2. LISP traffic inspection(LISP 트래픽 검사) - ASA는 FHR(first hop router)과 ITR 또는 ETR 간에 EID-notify 메시지를 보낼 수 있도록 UDP 포트 4342에서 LISP 트래픽을 검사합니다. ASA는 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 보수합니다. 예를 들면, FHR(first hop router)의 소스 IP 주소 및 ITR 또는 ETR의 목적지 주소로 LISP 트래픽을 검사해야 합니다. LISP 트래픽에는 관리자가 할당되지 않으며, LISP 트래픽 자체는 클러스터 상태 공유에 참여하지 않습니다.
3. Service Policy to enable flow mobility on specified traffic(지정된 트래픽에서 플로우 모빌리티 활성화를 위한 서비스 정책) - 비즈니스 크리티컬 트래픽에서 플로우 모빌리티를 활성화해야 합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다.
4. Site IDs(사이트 ID) - ASA는 각 클러스터 유닛에 대해 사이트 ID를 사용하여 새로운 소유자를 확인합니다.
5. Cluster-level configuration to enable flow mobility(플로우 모빌리티 활성화를 위한 클러스터 레벨 구성) - 또한 클러스터 레벨에서 플로우 모빌리티를 활성화해야 합니다. 이 켜기/끄기 토글을 사용하면 특정 클래스의 트래픽 또는 애플리케이션에 대한 플로우 모빌리티를 손쉽게 활성화 또는 비활성화할 수 있습니다.

LISP 검사 구성

서버가 사이트 간에 이동하는 경우 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

시작하기 전에

- Firepower 4100/9300 섀시 관리자(Supervisor)에서 섀시의 사이트 ID를 설정합니다.
- LISP 트래픽은 기본 검사 트래픽 클래스에 포함되지 않으므로 이 절차를 수행하는 중에 LISP 트래픽에 대해 별도의 클래스를 구성해야 합니다.

프로시저

단계 **1** (선택 사항) IP 주소를 기반으로 하는 검사된 EID로 제한하고 LISP 사전 공유 키를 구성하려면 다음과 같이 LISP 검사 맵을 구성합니다.

a) 확장된 ACL을 생성합니다. 대상 IP 주소만 EID 임베디드 주소와 일치합니다.

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

IPv4 및 IPv6 ACL이 모두 수락됩니다. 정확한 **access-list extended** 구문에 대한 명령 참조를 참고합니다.

b) LISP 검사 맵을 생성하고 파라미터 모드로 진입합니다.

policy-map type inspect lisp *inspect_map_name*

parameters

c) 생성한 ACL을 식별하여 허용되는 EID를 정의합니다.

allowed-eid access-list *eid_acl_name*

FHR(first hop router) 또는 ITR/ETR은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EID를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개뿐이지만 LISP가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다.

d) 필요한 경우, 사전 공유 키를 입력합니다.

validate-key *key*

예제:

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

단계 **2** 포트 4342에서 FHR(first hop router) 및 ITR 또는 ETR 간에 UDP 트래픽에 대한 LISP 검사를 구성합니다.

a) LISP 트래픽을 식별하기 위해 확장된 ACL을 구성합니다.

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

UDP 포트 4342를 지정해야 합니다. IPv4 및 IPv6 ACL이 모두 수락됩니다. 정확한 **access-list extended** 구문에 대한 명령 참조를 참고합니다.

b) ACL에 대한 클래스 맵을 생성합니다.

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) 정책 맵, 클래스 맵을 지정하고 선택적 LISP 검사 맵을 사용하여 검사를 활성화하고 인터페이스(새 인터페이스인 경우)에 서비스 정책을 적용합니다.

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

기존 서비스 정책이 있으면 기존 정책 맵 이름을 지정합니다. 기본적으로 ASA에는 **global_policy**라고 하는 전역 정책이 포함되어 있으므로 전역 정책에 해당 이름을 지정합니다. 정책을 전역으로 적용하지 않으려는 경우 인터페이스별로 하나의 서비스 정책을 생성할 수도 있습니다. LISP 검사는 트래픽에 양방향으로 적용되므로 소스 및 대상 인터페이스 모두에서 서비스 정책을 적용할 필요가 없습니다. 트래픽이 양쪽 방향의 클래스 맵과 일치할 경우 정책 맵을 적용하는 인터페이스로 들어가거나 나가는 모든 트래픽이 영향을 받습니다.

예제:

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASA는 FHR(first hop router)과 ITR 또는 ETR 간에 EID-notify 메시지를 보낼 수 있도록 LISP 트래픽을 검사합니다. ASA는 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 관리합니다.

단계 **3** 트래픽 클래스에 대한 플로우 모빌리티를 활성화합니다.

a) 서버가 사이트를 변경하는 경우 가장 최적의 사이트에 다시 할당하려는 비즈니스 크리티컬 트래픽을 식별하기 위해 확장된 ACL을 구성합니다.

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

IPv4 및 IPv6 ACL이 모두 수락됩니다. 정확한 **access-list extended** 구문에 대한 명령 참조를 참고합니다. 비즈니스 크리티컬 트래픽에서 플로우 모빌리티를 활성화해야 합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다.

b) ACL에 대한 클래스 맵을 생성합니다.

class-map *flow_map_name*

match access-list *flow_acl_name*

c) LISP 검사가 활성화되어 있는 동일한 정책 맵인 플로우 클래스 맵을 지정하고 플로우 모빌리티를 활성화합니다.

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

예제:

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

단계 **4** 클러스터 그룹 구성 모드로 들어가고 클러스터에 대한 플로우 모빌리티를 활성화합니다.

cluster group *name*

flow-mobility lisp

이 켜기/끄기 토글을 사용하면 플로우 모빌리티를 손쉽게 활성화 또는 비활성화할 수 있습니다.

예

다음 예에서는

- 10.10.10.0/24 네트워크에서의 EID 제한
- 192.168.50.89(내부에서)에서의 LIPS 라우터와 192.168.10.8(다른 ASA 인터페이스에서)에서의 ITR 또는 ETR 라우터 간의 LISP 트래픽(UDP 4342) 검사
- 10.10.10.0/24에서 HTTPS를 사용하여 서버로 이동하는 모든 내부 트래픽에 대한 플로우 모빌리티를 활성화합니다.
- 클러스터에 대한 플로우 모빌리티를 활성화합니다.

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

분산 **Site-to-Site VPN** 구성

기본적으로 ASA 클러스터에서는 중앙 집중식 Site-to-Site VPN 모드를 사용합니다. 클러스터링의 확장성을 활용하기 위해 분산 Site-to-Site VPN 모드를 활성화할 수 있습니다. 이 모드에서 S2S IPsec IKEv2 VPN 연결은 ASA 클러스터의 멤버 전체에서 분산됩니다. 클러스터 멤버 전체에서 VPN 연결을 분산시키면 클러스터의 용량 및 처리량 모두를 완전히 활용하며 특히 중앙 집중식 VPN 기능 이상으로 VPN 지원을 크게 확장합니다.

분산 **Site-to-Site VPN** 정보

분산 **VPN** 연결 역할

분산 VPN 모드에서 실행 중인 경우 다음 역할이 클러스터 멤버에 할당됩니다.

- 액티브 세션 소유자 — 연결을 처음으로 수신하는 유닛 또는 백업 세션을 액티브 세션으로 전환한 유닛입니다. 소유자는 IKE 및 IPsec 터널과 연결된 모든 트래픽을 포함하여 전체 세션에 대한 패킷을 처리하고 상태를 유지 관리합니다.
- 백업 세션 소유자 — 기존 액티브 세션에 대한 백업 세션을 처리하는 유닛입니다. 선택한 백업 전략에 따라 액티브 세션 소유자와 동일한 섀시의 유닛 또는 다른 섀시의 유닛일 수 있습니다. 액티브 세션 소유자에 장애가 발생하는 경우 백업 세션 소유자는 액티브 세션 소유자가 되며 다른 유닛에서 새로운 백업 세션이 설정됩니다.
- 전달자 — VPN 세션에 연결된 트래픽이 VPN 세션을 소유하지 않는 유닛에 전송될 경우, 해당 유닛에서는 CCL(클러스터 제어 링크)을 사용하여 VPN 세션을 소유하는 멤버에 트래픽을 전달합니다.
- 오케스트레이터 — 오케스트레이터(항상 클러스터의 마스터 노드)는 ASR(액티브 세션 재배포)을 실행할 때 어떤 세션이 이동하는지와 어디로 이동하는지를 계산합니다. 오케스트레이터는 소유자 멤버 X에게 N개의 세션을 Y 멤버로 이동하도록 요청합니다. 멤버 X는 작업을 완료하면 이동할 수 있었던 세션 수를 지정하고 오케스트레이터에 다시 응답합니다.

분산 **VPN** 세션 특징

분산 S2S VPN 세션에는 다음과 같은 특징이 있습니다. 그 외의 경우 VPN 연결은 ASA 클러스터에 있지 않으면 일반적인 방식으로 작동합니다.

- VPN 세션은 세션 수준에서 클러스터 전체에 분산됩니다. VPN 연결을 위해 동일한 클러스터 멤버에서 IKE 및 IPsec 터널과 모든 트래픽을 처리하는 것을 의미합니다. VPN 세션 트래픽이 해당 VPN 세션을 소유하지 않는 클러스터 멤버에 전송되는 경우, 트래픽이 VPN 세션을 소유하는 클러스터 멤버로 전달됩니다.
- VPN 세션에는 클러스터 전반에서 고유한 세션 ID가 있습니다. 세션 ID를 사용하여 트래픽이 검증되고 전달 의사 결정이 이루어지며 IKE 협상이 완료됩니다.
- S2S VPN 허브 및 스포크 구성에서 클라이언트가 ASA 클러스터를 통해 연결할 때(헤어피닝이라고 함) 들어오고 나가는 세션 트래픽이 다른 클러스터 멤버에 있을 수 있습니다.
- 백업 세션을 다른 섀시의 보안 모듈에 할당하도록 요청할 수 있습니다. 이렇게 하면 섀시 장애로부터 보호할 수 있습니다. 또는 클러스터의 노드에서 백업 세션을 할당하도록 선택할 수 있습니다. 이렇게 하면 노드 장애에 대해서만 보호됩니다. 클러스터에 두 개의 섀시가 있는 경우, 원격 섀시 백업이 권장됩니다.
- IKEv2 IPsec S2S VPN만 분산 S2S VPN 모드에서 지원되며 IKEv1은 지원되지 않습니다. IKEv1 S2S는 중앙 집중식 VPN 모드에서 지원됩니다.
- 각 보안 모듈은 6개 멤버 전체에서 최댓값인 약 36,000개의 세션에 대해 최대 6,000개의 VPN 세션을 지원합니다. 클러스터 멤버에서 지원되는 세션의 실제 수는 플랫폼 용량, 할당된 라이선스

및 상황별 리소스 할당에 따라 결정됩니다. 사용률이 한도에 가까울 경우 각 클러스터 유닛의 최대 용량에 도달하지 않은 경우에도 세션 생성이 실패할 수 있습니다. 이는 액티브 세션 할당이 외부 스위칭에 의해 결정되며, 백업 세션 할당이 내부 클러스터 알고리즘에 따라 결정되기 때문입니다. 고객은 사용률을 적절하게 조정하고 균일하지 않은 배포를 위한 공간을 확보하는 것이 좋습니다.

클러스터 이벤트의 분산 **VPN** 처리

표 ***16:***

Event(이벤트**)**	분산 **VPN**
멤버 장애	장애가 발생한 이 멤버에 있는 모든 액티브 세션의 경우, 다른 멤버에 있는 백업 세션이 액티브 세션이 되며 백업 세션은 백업 전략에 따라 다른 유닛에서 재할당됩니다.
섀시 장애	원격 섀시 백업 전략을 사용 중인 경우 장애가 발생한 섀시의 모든 액티브 세션에 대해 다른 섀시의 멤버에 있는 백업 세션이 액티브 상태가 됩니다. 유닛이 대체되면 이러한 현재 액티브 세션에 대한 백업 세션이 대체된 섀시에 있는 멤버에 재할당됩니다. 균일 백업 전략을 사용 중인 경우 액티브 세션과 백업 세션이 모두 장애가 발생한 섀시에 있는 경우 연결이 끊어집니다. 다른 섀시의 멤버에 있는 백업 세션을 포함하는 모든 액티브 세션은 이러한 세션으로 대체됩니다. 새 백업 세션이 남아 있는 섀시의 다른 멤버에 할당됩니다.
클러스터 멤버 비활성화	클러스터 멤버에 있는 모든 액티브 세션이 비활성화되면 다른 멤버에 있는 백업 세션이 액티브 세션이 되며 백업 전략에 따라 다른 유닛에서 백업 세션을 재할당합니다.
클러스터 멤버 참가	VPN 클러스터 모드가 분산 모드로 설정되지 않은 경우 마스터 유닛에서 모드 변경을 요청합니다. VPN 모드가 호환 가능하거나 일단 호환 가능한 상태가 되면 정상 작동 플로우에서 클러스터 멤버에 액티브 세션 및 백업 세션이 할당됩니다.

지원되지 않는 검사

다음 유형의 검사는 지원되지 않거나 분산 S2S VPN 모드에서 비활성화됩니다.

- CTIQBE
- DCERPC
- H323, H225, RAS
- IPsec pass-through
- MGCP

- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP(Skinny)
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

IPsec IKEv2 수정 사항

IKEv2는 다음 방식으로 분산 S2S VPN 모드에서 수정됩니다.

- ID는 IP/포트 튜플 대신 사용됩니다. 이렇게 하면 패킷에서 적절한 전달 의사 결정이 가능하며 기타 클러스터 멤버에 나타날 수 있는 이전 연결의 정리가 가능합니다.
- 단일 IKEv2 세션을 식별하는 (SPI) 식별자는 로컬에서 생성되며 클러스터 전체에서 고유한 임의 8바이트 값입니다. SPI에서는 타임스탬프 및 클러스터 멤버 ID를 임베드합니다. IKE 협상 패킷을 수신했는데 타임스탬프 또는 클러스터 멤버 ID 검사에 장애가 발생하면 패킷이 삭제되고 이유를 나타내는 메시지가 기록됩니다.
- 클러스터 멤버 전체에서 분할되어 NAT-T 협상에 장애가 발생하는 것을 방지하기 위해 IKEv2 처리가 수정되었습니다. IKEv2가 인터페이스에서 활성화되면 새 ASP가 도메인을 분류하며 *cluster_isakmp_redirect* 및 규칙이 추가됩니다. **show asp table classify domain cluster_isakmp_redirect** 명령을 사용하여 규칙을 확인합니다.

모델 지원

분산 VPN에 대해 지원되는 유일한 디바이스는 Firepower 9300입니다. 분산 VPN은 최대 2개의 섀시에서 최대 6개의 모듈을 지원합니다. 각 섀시에 설치된 보안 모듈의 수량은 다를 수 있지만 동일한 배포를 사용하는 것이 좋습니다.

사이트 간 클러스터링은 지원되지 않습니다.

방화벽 모드

분산 S2S VPN은 라우팅 모드에서만 지원됩니다.

상황 모드

분산 S2S VPN은 단일 모드와 다중 상황 모드 둘 다에서 작동합니다. 하지만, 다중 상황 모드에서는 액티브 세션 재배포가 상황 수준이 아니라 시스템 수준에서 수행됩니다. 이렇게 하면 상황과 연결된 액티브 세션이 모르는 사이에 지원 불가능한 로드를 생성하면서 다른 상황과 연결된 액티브 세션을 포함하는 클러스터 멤버로 이동하는 것이 방지됩니다.

고가용성

다음 기능은 보안 모듈 또는 섀시의 단일 장애에 대비하여 복원력을 제공합니다.

- 모든 섀시의 클러스터에 있는 다른 보안 모듈에서 백업되어 있는 VPN 세션은 보안 모듈 장애를 견딜 수 있습니다.
- 다른 섀시에서 백업되어 있는 VPN 세션은 섀시 장애를 견딜 수 있습니다.
- 클러스터 마스터는 VPN S2S 세션의 손실 없이 변경될 수 있습니다.

클러스터가 안정화되기 전에 추가 장애가 발생하는 경우, 액티브 세션 및 백업 세션 둘 다 장애가 발생한 유닛에 있으면 연결이 끊어질 수 있습니다.

멤버가 VPN 클러스터 모드 비활성화, 클러스터 멤버 재로드 및 기타 예상된 섀시 변경과 같은 정상적인 방식으로 클러스터를 벗어날 경우 세션 손실을 방지하기 위해 모든 시도가 수행됩니다. 이러한 유형의 작업을 수행하는 동안 클러스터가 작업 간에 세션 백업을 다시 설정할 수 있는 시간을 부여받는 한, 세션은 손실되지 않습니다. 마지막 클러스터 멤버에서 정상 종료가 트리거되는 경우, 기존 세션이 정상적으로 해제됩니다.

동적 **PAT**

분산 VPN 모드에서 사용할 수 없습니다.

CMPv2

CMPv2 ID 인증서 및 키 쌍은 클러스터 멤버 전체에서 동기화됩니다. 그러나, 클러스터의 마스터만 CMPv2 인증서를 자동으로 갱신하고 키를 재생성합니다. 마스터는 갱신 시 이러한 새 ID 인증서와 키를 모든 클러스터 멤버와 동기화합니다. 이 방법으로 클러스터의 모든 멤버가 인증을 위해 CMPv2 인증서를 활용하고 모든 멤버가 마스터로도 인계받을 수 있습니다.

분산 **S2S VPN** 활성화

VPN 세션을 위한 클러스터링의 확장성을 활용하려면 분산 Site-to-Site VPN을 활성화합니다.

참고 VPN 모드를 중앙 집중식과 분산 모드 간에 변경하면 모든 기존 세션이 해제됩니다. 백업 모드의 변경은 동적이며 변경 시 세션이 종료되지 않습니다.

시작하기 전에

- 클러스터의 모든 멤버에서 통신 사업자 라이선스가 구성되어 있어야 합니다.

• S2S VPN 구성을 설정해야 합니다.

프로시저

단계 **1** 클러스터의 마스터 유닛에서 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

단계 **2** 분산 S2S VPN을 활성화합니다.

vpn-mode distributed backup flat

또는

vpn-mode distributed backup remote-chassis

균일 백업 모드에서 스탠바이 세션은 다른 클러스터 멤버에서 설정됩니다. 이 경우 사용자가 블레이드 장애로부터 보호될 수 있지만 섀시 장애가 반드시 방지되는 것은 아닙니다.

원격 섀시 백업 모드에서 스탠바이 세션은 클러스터에서 다른 섀시의 멤버에서 설정됩니다. 이 경우 사용자가 블레이드 장애와 섀시 장애로부터 보호됩니다.

원격 섀시가 단일 섀시 환경에서 구성된 경우(의도적으로 또는 장애로 인해 구성된 경우) 다른 섀시가 조인할 때까지 백업이 생성되지 않습니다.

예제**:**

```
ciscoasa(cfg-cluster)# vpn-mode distributed backup remote-chassis
```

분산 **S2S VPN** 세션 재배포

ASR(액티브 세션 재배포)은 클러스터 멤버 전체에서 액티브 VPN 세션의 로드를 재배포합니다. 세션 시작 및 종료의 동적인 특성으로 인해 ASR은 모든 클러스터 멤버 전체에서 세션의 균형을 유지하는 최선의 작업입니다. 반복된 재배포 작업은 균형을 최적화합니다.

재배포는 언제든지 실행될 수 있으며 클러스터에서 토폴로지를 변경한 이후에 실행되어야 하고 새 멤버가 클러스터에 참가한 이후에 실행하는 것이 좋습니다. 재배포의 목적은 안정적인 VPN 클러스터를 생성하는 것입니다. 안정적인 VPN 클러스터에는 노드 전체에 걸쳐 거의 동일한 수의 액티브 세션 및 백업 세션이 있습니다.

세션을 이동하기 위해 백업 세션이 액티브 세션이 되고 새 백업 세션을 호스트하기 위해 다른 노드가 선택됩니다. 세션의 이동은 액티브 세션의 백업 위치와 해당 특정 백업 노드에 이미 있는 액티브 세션의 수에 따라 달라집니다. 백업 세션 노드가 어떠한 이유로 액티브 세션을 호스트할 수 없는 경우, 원래 노드는 세션의 소유자로 유지됩니다.

다중 상황 모드에서는 액티브 세션 재배포가 개별 상황 수준이 아니라 시스템 수준에서 수행됩니다. 한 상황의 액티브 세션이 다른 상황의 더 많은 액티브 세션을 포함하는 멤버를 이동하여 해당 클러스터 멤버에서 더 많은 로드를 생성할 수 있기 때문에 이 작업은 상황 수준에서 수행되지 않습니다.

시작하기 전에

- 재배포 활동을 모니터링하려는 경우 시스템 로그를 활성화합니다.
- 이 절차는 클러스터의 마스터 노드에서 수행해야 합니다.

프로시저

단계 **1** 클러스터의 마스터 노드에서 **show cluster vpn-sessiondb distribution** 명령을 실행하여 액티브 세션 및 백업 세션이 클러스터 전체에서 분산되는 방식을 확인합니다.

예제**:**

배포 정보는 다음과 같이 표시됩니다.

```
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

각 행에는 멤버 ID, 멤버 이름, 액티브 세션 수 및 백업 세션이 상주하는 멤버가 포함됩니다. 위의 예에서 다음 정보를 확인할 수 있습니다.

- 멤버 0에 209개의 액티브 세션이 있고 111개의 세션이 멤버 1에 백업되어 있으며 98개의 세션이 멤버 2에 백업되어 있습니다.
- 멤버 1에 204개의 액티브 세션이 있고 108개의 세션이 멤버 0에 백업되어 있으며 96개의 세션이 멤버 2에 백업되어 있습니다.
- 멤버 2에는 액티브 세션이 없으므로 클러스터 멤버에서는 이 노드에 대해 세션을 백업하지 않습니다. 이 멤버는 최근에 클러스터에 참가했습니다.

단계 **2** **cluster redistribute vpn-sessiondb** 명령을 실행합니다.

이 명령은 백그라운드에서 실행되는 동안 즉시(메시지 없이) 반환됩니다.

재배포할 세션 수와 클러스터에서의 로드에 따라 이 작업에 시간이 걸릴 수 있습니다. 재배포 활동이 수행될 때 다음 구문(및 기타 시스템 세부 정보는 여기에 표시되지 않음)을 포함하는 Syslog가 제공됩니다.

Syslog 구문	**Notes**(참고)
VPN 세션 재배포가 시작됨	마스터만
*orig-member-name*에서 *dest-member-name*으로 *number* 세션을 이동하기 위한 요청을 전송함	마스터만
*member-name*에 세션 재배포 메시지를 전송하지 못함	마스터만

Syslog 구문	**Notes**(참고)
*orig-member-name*에서 *dest-member-name*으로 *number* 세션을 이동하기 위한 요청을 수신함	슬레이브만
number 세션을 *member-name*으로 이동함	명명된 클러스터로 이동된 활성 세션의 수입니다.
*dest-member-name*에서 세션 이동 응답을 수신하지 못함	마스터만
VPN 세션이 완료됨	마스터만
클러스터 토폴로지 변경이 탐지됨. VPN 세션 재배포가 중단됨.	

단계 **3** **show cluster vpn distribution**의 출력을 사용하여 재배포 활동의 결과를 확인합니다.

ASA: 클러스터 멤버 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 멤버를 관리할 수 있습니다.

멤버 비활성화

클러스터의 멤버를 비활성화하려면, 클러스터링 컨피그레이션은 그대로 유지한 상태로 유닛의 클러스터링을 비활성화합니다.

참고 수동으로 또는 상태 확인 장애를 통해 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 유닛을 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우(예를 들어, 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

- 콘솔 포트를 사용해야 합니다. 원격 CLI 연결에서는 클러스터링을 활성화하거나 비활성화할 수 없습니다.
- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 클러스터 구성 모드로 들어갑니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group pod1
```

단계 **2** 클러스터링을 비활성화합니다.

no enable

이 유닛이 마스터 유닛이었던 경우, 새 마스터가 선택되며 다른 멤버가 마스터 유닛이 됩니다.

클러스터 컨피그레이션은 그대로 유지되므로 클러스터링을 나중에 다시 활성화할 수 있습니다.

마스터 유닛의 멤버

유닛에서 멤버를 비활성화하려면 다음 단계를 수행합니다.

참고 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 유닛을 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우(예를 들어, 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.

프로시저

클러스터에서 유닛을 제거합니다.

cluster remove unit *unit_name*

예제**:**

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
```

```
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

부트스트랩 구성과 마스터 유닛에서 동기화한 마지막 구성도 그대로 유지되므로 나중에 구성을 잃지 않고 다시 유닛을 추가할 수 있습니다. 슬레이브 유닛에 이 명령을 입력하여 마스터 유닛을 제거할 경우 새 마스터 유닛이 선택됩니다.

멤버 이름을 보려면 **cluster remove unit ?**을 입력하거나 **show cluster info** 명령을 입력합니다.

클러스터 다시 참가

유닛이 클러스터에서 제거된 경우, 예를 들어 실패한 인터페이스의 경우 또는 멤버를 수동으로 비활성화한 경우, 클러스터를 수동으로 다시 조인해야 합니다.

시작하기 전에

- 클러스터링을 다시 활성화하려면 콘솔 포트를 사용해야 합니다. 다른 인터페이스는 종료됩니다.
- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.
- 클러스터를 다시 조인하기 전에 장애가 해결되었는지 확인하십시오.

프로시저

단계 **1** 콘솔에서 클러스터 구성 모드를 시작합니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group pod1
```

단계 **2** 클러스터링을 활성화합니다.

enable

마스터 유닛 변경

주의 마스터 유닛을 변경하는 가장 좋은 방법은 마스터 유닛의 클러스터링을 비활성화한 후 새 마스터가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 마스터 유닛이 될 정확한 유닛을 지정해야 할 경우, 이 섹션을 절차를 사용하십시오. 그러나 중앙 집중식 기능의 경우 이 절차를 통해 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

마스터 유닛을 변경하려면 다음 단계를 수행합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우 **changeto system** 명령을 입력합니다.

프로시저

새 유닛을 마스터 유닛으로 설정합니다.

cluster master unit *unit_name*

예제**:**

```
ciscoasa(config)# cluster master unit asa2
```

기본 클러스터 IP 주소에 다시 연결해야 합니다.

멤버 이름을 보려면 **cluster master unit ?**을 입력하거나 (현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.

클러스터 전체에서 명령 실행

클러스터의 모든 멤버 또는 특정 멤버에 명령을 보내려면 다음 단계를 수행합니다. 모든 멤버에 **show** 명령을 보내면 모든 출력이 수집되고 해당 내용이 현재 유닛의 콘솔에 표시됩니다. 또는 클러스터 전체의 통계를 확인하기 위해 마스터 유닛에서 입력할 수 있는 show 명령이 있습니다. **capture** 및 **copy**와 같은 다른 명령의 경우 클러스터 전체 실행을 활용할 수도 있습니다.

프로시저

모든 멤버 또는 유닛 이름을 지정한 경우 특정 멤버에 명령을 전송합니다.

cluster exec [unit *unit_name***]** *command*

예제:

```
ciscoasa# cluster exec show xlate
```

멤버 이름을 확인하려면 **cluster exec unit ?** 또는 **show cluster info** 명령을 입력합니다(현재 유닛을 제외한 모든 이름을 보려는 경우).

예

클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 다음 명령을 마스터 유닛에 입력합니다.

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일의 이름 뒤에는 유닛 이름이 자동으로 연결되며 capture1_asa1.pcap, capture1_asa2.pcap 같은 형식이 됩니다. 이 예에서 asa1 및 asa2는 클러스터 유닛 이름 입니다.

cluster exec show memory 명령에 대한 다음 샘플 출력에는 클러스터의 각 멤버에 대한 메모리 정보가 나와 있습니다.

```
ciscoasa# cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:*******************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA: ASA 클러스터 모니터링 - Firepower 4100/9300 섀시

클러스터의 상태 및 연결을 모니터링하고 문제를 해결할 수 있습니다.

클러스터 상태 모니터링

클러스터 상태 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show cluster info [health], show cluster chassis info**

  키워드가 없는 경우 **show cluster info** 명령을 사용하면 클러스터의 모든 멤버 상태가 표시됩니다.

  show cluster info health 명령을 사용하면 인터페이스, 유닛, 클러스터 전반의 현재 상태가 표시됩니다.

  show cluster info 명령에 대한 다음 출력을 참조하십시오.

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
        CCL MAC   : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

- **show cluster info auto-join**

  시간 지연 이후에 클러스터 유닛이 자동으로 클러스터에 다시 참가하는지 여부 및 오류 상태(예: 라이선스 대기 중, 섀시 상태 검사 오류 등)가 지워졌는지 여부를 표시합니다. 유닛이 영구적으로 비활성화된 경우 또는 유닛이 이미 클러스터에 있는 경우, 이 명령은 출력을 표시하지 않습니다.

show cluster info auto-join 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport** {**asp** | **cp** [**detail**]}

  다음에 대한 전송 관련 통계를 표시합니다.

  - **asp** — 데이터 평면 전송 통계입니다.
  - **cp** — 제어 평면 전송 통계입니다.

    detail 키워드를 입력하는 경우, 클러스터의 신뢰할 수 있는 전송 프로토콜 사용량을 볼 수 있어 버퍼가 제어 평면에서 가득 찬 경우 패킷 삭제 문제를 식별할 수 있습니다. **show cluster info transport cp detail** 명령에 대한 내용은 다음 출력을 참조하십시오.

    ```
    ciscoasa# show cluster info transport cp detail
    Member ID to name mapping:
      0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

    Legend:
      U    - unreliable messages
      UE   - unreliable messages error
      SN   - sequence number
      ESN  - expecting sequence number
      R    - reliable messages
      RE   - reliable messages error
      RDC  - reliable message deliveries confirmed
      RA   - reliable ack packets received
      RFR  - reliable fast retransmits
      RTR  - reliable timer-based retransmits
      RDP  - reliable message dropped
      RDPR - reliable message drops reported
      RI   - reliable message with old sequence number
      RO   - reliable message with out of order sequence number
    ```

```
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-----------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
```

```
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
```

```
Total messages buffered in real-time: 0
```

- **show cluster history**

  클러스터 내역을 표시합니다.

클러스터 전체 패킷 캡처

클러스터의 패킷을 캡처하는 방법에 대한 내용은 다음 명령을 참조하십시오.

cluster exec capture

클러스터 전체의 문제를 해결하기 위해 **cluster exec capture** 명령을 사용하여 마스터 유닛에서 클러스터별 트래픽의 캡처를 활성화할 수 있습니다. 이 경우 클러스터의 모든 슬레이브 유닛에서 캡처가 자동으로 활성화됩니다.

클러스터 리소스 모니터링

클러스터 리소스 모니터링에 대한 내용은 다음 명령을 참조하십시오.

show cluster {cpu | memory | resource} [*options*], **show cluster chassis [cpu | memory | resource usage]**

전체 클러스터에 대한 집계된 데이터를 표시합니다. 사용 가능한 옵션은 데이터 유형에 따라 달라집니다.

클러스터 트래픽 모니터링

클러스터 트래픽 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show conn [detail | count], cluster exec show conn**

  show conn 명령을 사용하면 플로우가 관리자인지, 백업인지 아니면 전달자 플로우인지 표시됩니다. 모든 연결을 확인하려면 유닛에서 **cluster exec show conn** 명령을 사용합니다. 이 명령은 클러스터의 다른 ASA에 단일 플로우에 대한 트래픽이 어떤 방식으로 도착하는지를 표시할 수 있습니다. 클러스터의 처리량은 로드 밸런싱의 효율성과 구성에 따라 달라집니다. 이 명령을 사용하면 연결에 대한 트래픽 흐름이 클러스터를 통해 어떻게 이루어지는지 손쉽게 볼 수 있으며, 로드 밸런서가 이 흐름의 성능에 어떤 영향을 미치는지 파악하는 데 유용합니다.

  다음은 **show conn detail** 명령에 대한 샘플 출력입니다.

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
```

```
        F - outside FIN, f - inside FIN,
        G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
        i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
        k - Skinny media, L - LISP triggered flow owner mobility
        M - SMTP data, m - SIP media, n - GUP
        N - inspected by Snort
        O - outbound data, o - offloaded,
        P - inside back connection,
        Q - Diameter, q - SQL*Net data,
        R - outside acknowledged FIN,
        R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
        s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
        V - VPN orphan, W - WAAS,
        w - secondary domain backup,
        X - inspected by service module,
        x - per session, Y - director stub flow, y - backup stub flow,
        Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

  show cluster info conn-distribution 및 **show cluster info packet-distribution** 명령을 사용하면 모든 클러스터 유닛 전체의 트래픽 배포가 표시됩니다. 이러한 명령은 외부 로드 밸런서를 평가하고 조정하는 데 유용합니다.

  show cluster info loadbalance 명령을 사용하면 연결 리밸런싱 통계가 표시됩니다.

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [*options*], **show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  전체 클러스터에 대한 집계된 데이터를 표시합니다. 사용 가능한 옵션은 데이터 유형에 따라 달라집니다.

  show cluster access-list 명령에 대한 다음 출력을 참조하십시오.

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
```

```
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

모든 디바이스에서 사용 중인 연결의 집계된 수를 표시하려면 다음을 입력합니다.

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):******************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:*************************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  이 명령은 데이터 경로 문제를 해결하는 데 유용합니다.

클러스터 라우팅 모니터링

클러스터 라우팅에 대한 내용은 다음 명령을 참조하십시오.

- **show route cluster**
- **debug route cluster**

  라우팅에 대한 클러스터 정보를 표시합니다.

- **show lisp eid**

  EID 및 사이트 ID를 보여주는 ASA EID 테이블을 표시합니다.

  cluster exec show lisp eid 명령의 다음 출력을 참조하십시오.

```
ciscoasa# cluster exec show lisp eid
```

```
L1(LOCAL):**************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  이 명령은 트러블슈팅에 유용합니다.

분산 **S2S VPN** 모니터링

VPN 세션의 배포 및 상태를 모니터링하려면 다음 명령을 사용합니다.

- 세션의 전반적인 배포는 **show cluster vpn-sessiondb distribution**을 사용하여 제공됩니다. 다중 상황 환경에서 실행 중인 경우, 이 명령은 시스템 상황에서 실행되어야 합니다.

  이 show 명령을 사용하면 각 멤버에서 **show vpn-sessiondb summary**를 실행할 필요 없이 세션에 대한 빠른 보기가 제공됩니다.

- **show cluster vpn-sessiondb summary** 명령을 사용하는 클러스터에서 VPN 연결의 통합된 보기도 사용할 수 있습니다.

- **show vpn-sessiondb** 명령을 사용하는 개별 디바이스 모니터링은 일반적인 VPN 정보 외에도 디바이스에서 액티브 세션 및 백업 세션의 수를 표시합니다.

클러스터링의 로깅 구성

클러스터링의 로깅 구성에 대한 내용은 다음 명령을 참조하십시오.

logging device-id

클러스터의 각 유닛에서는 syslog 메시지를 독립적으로 생성합니다. **logging device-id** 명령을 사용하면 디바이스 ID가 동일하거나 다른 syslog 메시지를 생성하여 클러스터의 동일한 또는 다른 유닛에서 메시지가 표시되도록 할 수 있습니다.

클러스터링 디버깅

클러스터링 디버깅에 대해서는 다음 명령을 참조하십시오.

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  클러스터링에 대한 디버그 메시지가 표시됩니다.

- **debug service-module**

수퍼바이저와 애플리케이션 간의 상태 검사 문제 등 블레이드 수준 문제에 대한 디버그 메시지를 표시합니다.

- **show cluster info trace**

  show cluster info trace 명령을 사용하면 추가적인 문제 해결을 위한 디버깅 정보가 표시됩니다.

  show cluster info trace 명령에 대한 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

분산 **S2S VPN** 트러블슈팅

분산 **VPN** 알림

분산 VPN을 실행하는 클러스터에서 다음 오류 상황이 발생하는 경우, 식별된 구문이 포함된 메시지가 있는 알림을 받게 됩니다.

상태	알림
클러스터에 참가하려고 시도할 때 기존 또는 참가 중인 클러스터 슬레이브가 분산 VPN 모드에 있지 않은 경우 다음을 수행합니다.	새 클러스터 멤버(*member-name*)가 vpn 모드 불일치 때문에 거부되었습니다. 및 마스터(*master-name*)는 vpn 모드 기능이 마스터 구성과 호환되지 않아 유닛(유닛 이름)의 등록 요청을 거부합니다.
라이선싱이 분산 VPN에 대한 클러스터 멤버에서 적절하게 구성되어 있지 않은 경우:	오류: 마스터가 요청한 클러스터 vpn-mode가 분산 모드로 변경되었습니다. 통신 사업자 라이선스의 누락으로 인해 모드를 변경할 수 없습니다.
타임스탬프 또는 멤버 ID가 수신된 IKEv2 패킷의 SPI에서 유효하지 않은 경우:	만료 SPI 수신됨 또는 손상된 SPI 탐지됨
클러스터가 백업 세션을 생성할 수 없는 경우:	IKEv2 세션에 대한 백업을 생성하지 못했습니다.
IKEv2 IC(초기 연락처) 처리 오류:	IKEv2 협상이 오류로 인해 중단됨: 백업에서 오래된 백업 세션이 발견됨

상태	알림
재배포 문제:	*member-name*에 세션 재배포 메시지를 전송하지 못함 *member-name*(마스터만 해당)에서 세션 이동 응답을 수신하지 못했습니다.
세션 재배포를 수행하는 동안 토폴로지가 변경되는 경우:	클러스터 토폴로지 변경이 탐지됨. VPN 세션 재배포가 중단됨.

다음 상황 중 한 가지가 발생했을 수 있습니다.

- N7K 스위치가 **port-channel load-balance src-dst l4port** 명령을 사용하는 로드 밸런싱 알고리즘으로 L4port를 사용하여 구성된 경우 L2L VPN 세션은 클러스터에 있는 섀시 중 하나에만 배포되고 있습니다. . 클러스터 세션 할당의 예는 다음과 같습니다.

```
SSP-Cluster/slave(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

  L2L IKEv2 VPN이 소스 및 대상 포트에 모두 포트 500을 사용하므로 IKE 패킷은 N7K와 섀시 사이에서 연결된 포트 채널의 링크 중 하나에만 전송됩니다.

  port-channel load-balance src-dst ip-l4port를 사용하여 N7K 로드 밸런싱 알고리즘을 IP 및 L4 포트로 변경합니다. 그러면 IKE 패킷이 모든 링크와 두 Firepower 9300 섀시에 전송됩니다.

  더 즉각적인 조정을 위해 ASA 클러스터의 마스터에서는 **cluster redistribute vpn-sessiondb**를 실행하여 액티브 VPN 세션을 다른 섀시의 클러스터 멤버로 재배포합니다.

클러스터링에 대한 참조

이 섹션에는 클러스터링이 작동하는 방식에 대한 자세한 정보가 포함되어 있습니다.

성능 확장 요소

클러스터에 여러 유닛을 결합할 경우 총 클러스터 성능을 대략 다음과 같이 예측할 수 있습니다.

- 통합 TCP 또는 CPS 처리량의 80%
- 통합 UDP 처리량의 90%
- 트래픽 조합에 따라 통합된 EMIX(이더넷 MIX) 처리량의 60%

예를 들어 TCP 처리량의 경우 3개의 모듈이 있는 Firepower 9300은 단독으로 실행하면 실제 방화벽 트래픽 중 약 135Gbps를 처리할 수 있습니다. 2개의 섀시의 경우 최대 통합 처리량은 270Gbps(2개 섀시 x 135Gbps)의 약 80%인 216Gbps입니다.

마스터 유닛 선택

클러스터의 멤버는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 마스터 유닛을 선택합니다.

1. 클러스터를 구축할 때 각 유닛은 3초마다 선택 요청을 브로드캐스트합니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 클러스터를 구축할 때 설정되며 구성 불가능합니다.
3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 마스터 유닛이 됩니다.
4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 마스터 유닛이 되는 것은 아닙니다. 기존 마스터 유닛은 응답이 중지되지 않는 한 항상 마스터 유닛으로 유지되며 응답이 중지될 때에 새 마스터 유닛이 선택됩니다.

참고 유닛을 수동으로 강제 변경하여 마스터 유닛이 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

클러스터 내의 고가용성

클러스터링에서는 섀시, 유닛 및 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

섀시 애플리케이션 모니터링

섀시 애플리케이션 상태 모니터링은 항상 활성화되어 있습니다. Firepower 4100/9300 섀시 수퍼바이저는 ASA 애플리케이션을 주기적으로(1초마다) 검사합니다. ASA가 작동 중인데 Firepower 4100/9300 섀시 수퍼바이저와 3초 동안 통신할 수 없는 경우, ASA에서는 syslog 메시지를 생성하고 클러스터를 떠납니다.

Firepower 4100/9300 섀시 수퍼바이저가 45초 후에 애플리케이션과 통신할 수 없는 경우, ASA를 다시 로드합니다. ASA가 수퍼바이저와 통신할 수 없는 경우, 클러스터에서 자신을 제거합니다.

유닛 상태 모니터링

마스터 유닛에서는 클러스터 제어 링크를 통해 하트비트 메시지를 주기적으로 전송하여 모든 슬레이브 유닛을 모니터링합니다(기간은 구성 가능함). 각 슬레이브 유닛에서는 동일한 메커니즘을 사용하여 마스터 유닛을 모니터링합니다. 유닛 상태 검사에 오류가 발생하는 경우 클러스터에서 유닛이 제거됩니다.

인터페이스 모니터링

각 유닛에서는 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 마스터 유닛에 보고합니다. 섀시 간 클러스터링의 경우 Spanned EtherChannel은 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 섀시에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인하고 인터페이스가 작동 중단 상태인지 ASA 애플리케이션에 정보를 제공합니다. 상태 모니터링을 활성화하면 기본적으로 모든 물리적 인터페이스가 모니터링됩니다(EtherChannel 인터페이스에 대한 기본 EtherChannel 포함). 작동 상태인 명명된 인터페이스만 모니터링 대상이 될 수 있습니다. 예를 들어, EtherChannel의 모든 멤버 포트는 명명된 EtherChannel이 클러스터에서 제거되기 전에 장애가 발생해야 합니다(최소 포트 번들 설정에 따라). 선택적으로 인터페이스별 모니터링을 비활성화할 수 있습니다.

특정 유닛의 모니터링된 인터페이스에 장애가 발생하였으나 다른 유닛에서는 액티브 상태인 경우, 클러스터에서 해당 유닛이 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. ASA에서는 유닛이 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 ASA가 클러스터에서 제거되지 않습니다. 설정된 멤버의 경우, 500밀리초 이후에 유닛이 제거됩니다.

섀시 간 클러스터링의 경우, 클러스터에서 EtherChannel을 추가하거나 삭제하면 인터페이스 상태 모니터링은 각 섀시에서 변경 작업을 수행할 시간을 확보하기 위해 95초 동안 일시 중단됩니다.

데코레이터 애플리케이션 모니터링

인터페이스에서 Radware DefensePro 애플리케이션과 같은 데코레이터 애플리케이션을 설치하는 경우, ASA 및 데코레이터 애플리케이션 둘 다 클러스터에서 계속 작동해야 합니다. 유닛은 두 애플리케이션이 모두 작동할 때까지 클러스터에 참가하지 않습니다. 클러스터에 참가한 이후에 유닛은 3초마다 데코레이터 애플리케이션의 상태를 모니터링합니다. 데코레이터 애플리케이션이 작동하지 않으면 유닛이 클러스터에서 제거됩니다.

실패 이후 상태

클러스터의 유닛에 오류가 발생할 경우, 해당 유닛에서 호스팅하는 연결이 다른 유닛으로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 클러스터 링크를 통해 공유됩니다.

마스터 유닛에 장애가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 마스터 유닛이 됩니다.

ASA는 실패 이벤트에 따라 클러스터에 다시 참가하려고 시도합니다.

참고 ASA가 비활성화되고 클러스터에 자동으로 다시 조인하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우 관리 인터페이스가 비활성화됩니다. 추가 구성을 위해서는 콘솔 포트를 사용해야 합니다.

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 처음 참가 시 클러스터 제어 링크 장애 — 클러스터 제어 링크의 문제를 해결한 후에는 ASA 콘솔 포트에서 **cluster group** *name*을 입력한 다음 **enable**을 입력하여 클러스터링을 다시 활성화함으로써 클러스터에 수동으로 다시 참가해야 합니다.
- 클러스터 참가 후 클러스터 제어 링크 장애 — ASA에서는 자동으로 5분마다 무기한으로 다시 참가하려고 시도합니다. 이 동작은 구성 가능합니다.
- 데이터 인터페이스 장애 — ASA에서는 자동으로 5분, 10분, 마지막으로 20분 후에 다시 참가하도록 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 ASA에서는 클러스터링을 비활성화합니다. 데이터 인터페이스 문제를 해결한 후에는 ASA 콘솔 포트에서 **cluster group** *name*을 입력한 다음 을 입력하여 클러스터링을 수동으로 활성화해야 합니다**enable**.이 동작은 구성 가능합니다.
- 유닛 오류 — 유닛 상태 검사 오류로 인해 클러스터에서 유닛이 제거된 경우, 클러스터에 다시 참가할 수 있을지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한 경우 클러스터 제어 링크가 작동 상태이면 전원을 다시 가동할 때 유닛이 클러스터에 다시 참가할 수 있습니다. 유닛은 5초마다 클러스터에 다시 참가하려고 시도합니다.
- 섀시 애플리케이션 통신 장애 — ASA에서 섀시 애플리케이션 상태가 복구되었는지 탐지할 경우, ASA에서는 클러스터에 자동으로 다시 참가하려고 시도합니다.
- 데코레이터 애플리케이션 장애 — ASA에서는 데코레이터 애플리케이션이 백업되었는지 감지할 경우 클러스터에 다시 참가합니다.
- 내부 오류 — 내부 장애 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등 유닛은 5분, 10분, 20분 간격으로 자동으로 클러스터에 다시 참가하려고 시도합니다. 이 동작은 구성 가능합니다.

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 장애 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다. 백업 소유자는 일반적으로 관리자이기도 합니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 ***17:*** 클러스터 전반에 걸쳐 복제된 기능

트래픽	상태 지원	**Notes**(참고)
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	—

트래픽	상태 지원	**Notes(**참고**)**
MAC 주소 테이블	예	—
사용자 ID	Yes(예)	AAA 규칙(uauth)을 포함하고 방화벽을 식별합니다.
IPv6 네이버 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—
중앙 집중식 VPN(사이트 대 사이트)	아니요	마스터 유닛에 오류가 발생할 경우 VPN 세션의 연결이 끊어집니다.
분산 VPN(사이트 대 사이트)	Yes(예)	백업 세션이 활성 세션이 되며 새 백업 세션이 생성됩니다.

클러스터에서 연결을 관리하는 방법

클러스터의 여러 멤버에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

연결 역할

각 연결에 대해 정의된 다음 역할을 참조하십시오.

- 소유자 - 일반적으로 연결을 가장 처음 수신하는 유닛입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다. 원래 소유자가 실패하고 새 유닛이 연결에서 패킷을 수신하면, 관리자는 해당 유닛으로부터 새 소유자를 선택합니다.
- 백업 소유자 - 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있도록 소유자로부터 수신한 TCP/UDP 상태 정보를 저장하는 유닛입니다. 백업 소유자는 장애 발생 시 연결을 승계할 수 없습니다. 소유자를 사용할 수 없을 경우, 연결에서 패킷을 받을(로드 밸런싱을 기준으로) 첫 번째 유닛이 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

  관리자(아래 설명 참조)는 소유자와 같은 유닛이 아니라면 백업 소유자로도 사용됩니다. 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  Firepower 9300의 섀시 간 클러스터링(섀시 하나에 클러스터 유닛이 3개까지 포함될 수 있음)에서 백업 소유자가 소유자와 같은 섀시에 있으면 섀시 장애로부터 플로우를 보호하기 위해 다른 섀시에서 추가 백업 소유자가 선택됩니다.

  사이트 간 클러스터링에 대한 관리자 지역화를 활성화하는 경우에는 두 가지 백업 소유자 역할, 즉 로컬 백업 및 글로벌 백업이 있습니다. 소유자는 항상 자신과 동일한 사이트의 로컬 백업을

선택합니다(사이트 ID 기반). 글로벌 백업은 어느 사이트에든 있을 수 있으며, 로컬 백업과 동일한 유닛일 수도 있습니다. 소유자는 연결 상태 정보를 두 백업에 모두 전송합니다.

사이트 이중화를 활성화하는 경우 백업 소유자가 소유자와 같은 사이트에 있으면 사이트 장애로부터 플로우를 보호하기 위해 다른 사이트에서 추가 백업 소유자가 선택됩니다. 섀시 백업 및 사이트 백업은 서로 독립적이므로 경우에 따라서는 플로우에 섀시 백업과 사이트 백업이 모두 포함됩니다.

- 관리자 - 전달자의 소유자 조회 요청을 처리하는 유닛입니다. 소유자가 새 연결을 수신할 경우, 소유자 유닛에서는 소스/대상 IP 주소와 포트의 해시를 기준으로 관리자 유닛을 선택하며 관리자 유닛에 메시지를 전송하여 새 연결을 등록합니다. 패킷이 소유자 유닛이 아닌 다른 유닛에 전달될 경우, 해당 유닛에서는 관리자 유닛에 어떤 유닛이 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다. 관리자가 실패하면 소유자는 새 관리자를 선택합니다.

  관리자는 소유자와 같은 유닛이 아니라면 백업 소유자로도 사용됩니다(위의 설명 참조). 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  사이트 간 클러스터링에 대한 관리자 지역화를 활성화하는 경우에는 두 가지 관리자 역할, 즉 로컬 관리자와 전역 관리자가 있습니다. 소유자는 항상 자신과 동일한 사이트의 로컬 관리자를 선택합니다(사이트 ID 기반). 전역 관리자는 어느 사이트에든 있을 수 있으며, 로컬 관리자와 동일한 유닛일 수도 있습니다. 원래 소유자가 실패하면 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다.

- 전달자 — 패킷을 소유자 유닛에 전달하는 유닛입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 흐름을 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 관리자 지역화를 활성화하면, 전달자는 항상 로컬 관리자를 쿼리합니다. 전달자는 로컬 관리자가 소유자를 모르는 경우에만 전역 관리자를 쿼리합니다. 클러스터 멤버가 다른 사이트의 소유인 연결에 대한 패킷을 수신하는 경우를 예로 들 수 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 시퀀스 임의 설정을 비활성화한 경우 SYN 쿠키는 사용되지 않으며, 책임자에게 쿼리해야 합니다.) DNS 및 ICMP 같이 짧은 흐름의 경우 쿼리 대신 전달자가 책임자에게 패킷을 즉시 전송하고 책임자가 소유자에게 전송합니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.

연결에 PAT(Port Address Translation)가 사용되는 경우, PAT 유형(per-session 또는 multi-session)이 클러스터의 어떤 멤버가 새 연결의 소유자가 될지에 영향을 미칩니다.

- Per-session PAT(세션 단위 PAT) - 연결에서 초기 패킷을 수신하는 유닛이 소유자입니다.

  기본적으로 TCP 및 DNS UDP 트래픽은 per-session PAT를 사용합니다.

- Multi-session PAT(다중 세션 PAT) - 항상 마스터 유닛이 소유자입니다. Multi-session PAT 연결이 초기에 슬레이브 유닛에서 수신되면 슬레이브 유닛은 해당 연결을 마스터 유닛으로 전달합니다.

  기본적으로 UDP(DNS UDP 제외) 및 ICMP 트래픽은 multi-session PAT를 사용하므로, 항상 마스터 유닛에서 해당 연결을 소유합니다.

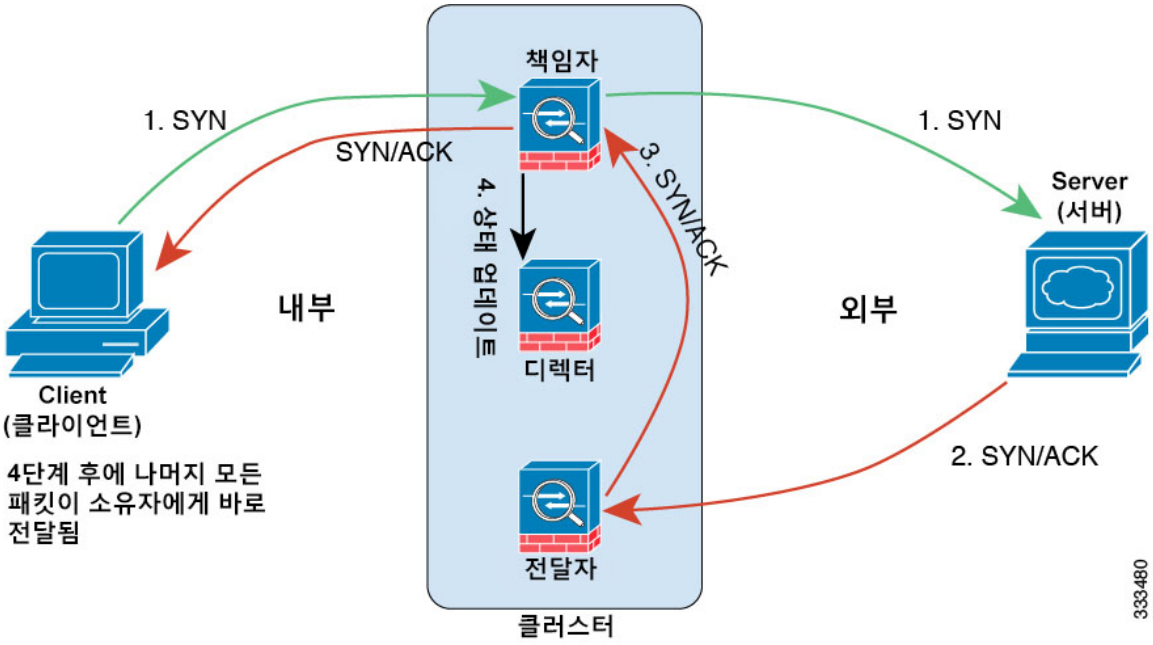
TCP 및 UDP에 대한 per-session PAT 기본값을 변경하여, 이러한 프로토콜에 대한 연결이 구성에 따라 세션 단위 또는 다중 세션으로 처리되도록 할 수 있습니다. ICMP의 경우 기본 multi-session PAT에서 변경할 수 없습니다. 세션당 PAT에 대한 자세한 내용은 방화벽 설정 가이드를 참조하십시오.

새 연결 소유권

로드 밸런싱을 통해 클러스터의 멤버에 새 연결이 전송될 경우, 해당 유닛에서는 연결의 양방향을 모두 소유합니다. 다른 유닛에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 유닛에 전달됩니다. 다른 유닛에 반대 방향의 흐름이 전송될 경우, 이는 원래 유닛으로 다시 리디렉션됩니다.

샘플 데이터 흐름

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.



1. SYN 패킷은 클라이언트에서 시작되고 ASA에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 ASA에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 ASA는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.

5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 흐름을 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 유닛에 전달된 경우, 소유자 유닛에 관리자를 쿼리하고 흐름을 설정합니다.
8. 흐름 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

ASA 클러스터링에 대한 기록 - Firepower 4100/9300 섀시

기능 이름	플랫폼 릴리스	기능 정보
Firepower 9300 섀시당 유닛의 병렬 클러스터 참가	9.10(1)	Firepower 9300에서는 이 기능을 통해 섀시에서 보안 모듈이 클러스터에 동시에 참가하게 되므로 트래픽이 모듈 간에 고르게 분산됩니다. 모듈이 다른 모듈보다 훨씬 먼저 참가하는 경우, 다른 모듈이 로드를 아직 공유할 수 없기 때문에 이 모듈은 원하는 트래픽보다 더 많은 트래픽을 받을 수 있습니다. 신규/수정된 명령: **unit parallel-join**
Firepower 4100/9300에 대한 클러스터 제어 링크의 맞춤화 가능한 IP 주소	9.10(1)	기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 이제 FXOS에서 클러스터를 구축하는 경우 네트워크를 설정할 수 있습니다. 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 따라서 이제 FXOS에서 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외하고 클러스터 제어 링크의 맞춤형 /16 서브넷을 설정할 수 있습니다. 신규/수정된 FXOS 명령: **set cluster-control-link network**

기능 이름	플랫폼 릴리스	기능 정보
이제 클러스터 인터페이스 디바운스 시간이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다.	9.10(1)	인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA에서는 **health-check monitor-interface debounce-time** 명령 또는 ASDM **Configuration(**구성**) > Device Management(**디바이스 관리**) > High Availability and Scalability(**고가용성 및 확장성**) > ASA Cluster(ASA** 클러스터**)** 화면에 지정되어 있는 밀리초 동안 대기합니다. 이제 이 기능이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다. 예를 들어 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다. 명령은 수정하지 않았습니다.
내부 장애 발생 후 클러스터에 자동으로 다시 참가	9.9(2)	이전에는 많은 오류 상태로 인해 클러스터에서 클러스터 유닛이 제거되었으며 문제를 해결한 후에 클러스터에 수동으로 다시 참가해야 했습니다. 이제 유닛은 기본적으로 5분, 10분, 20분 간격으로 자동으로 클러스터에 다시 참가하려고 시도합니다. 이러한 값은 구성할 수 있습니다. 내부 장애로는 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등이 있습니다. 신규 또는 수정된 명령: **health-check system auto-rejoin, show cluster info auto-join**
클러스터의 신뢰할 수 있는 전송 프로토콜 메시지에 대해 전송 관련 통계 표시	9.9(2)	이제 유닛당 클러스터의 신뢰할 수 있는 전송 버퍼 사용량을 볼 수 있어 버퍼가 제어 평면에서 가득 찬 경우 패킷 삭제 문제를 식별할 수 있습니다. 신규 또는 수정된 명령: **show cluster info transport cp detail**

기능 이름	플랫폼 릴리스	기능 정보
Firepower 섀시에 대해 향상된 섀시 상태 검사 장애 탐지	9.9(1)	이제 섀시 상태 검사의 보류 시간을 더 낮게 100밀리초로 구성할 수 있습니다. 이전에는 최소값이 300밀리초였습니다. 최소 결합 시간(간격 x 재시도 횟수)은 600밀리초보다 적을 수 없습니다. 신규 또는 수정된 명령: **app-agent heartbeat interval**
클러스터링를 위한 사이트 간 이중화	9.9(1)	사이트 간 이중화를 통해 트래픽 플로우의 백업 소유자는 항상 소유자의 다른 사이트에 있게 됩니다. 이 기능은 사이트 장애가 발생하지 않도록 보호해줍니다. 신규 또는 수정된 명령: **site-redundancy, show asp cluster counter change, showasp table cluster chash-table, show conn flag**
Firepower 9300에서 클러스터링을 사용하는 분산 Site-to-Site VPN	9.9(1)	Firepower 9300의 ASA 클러스터는 분산 모드에서 Site-to-Site VPN을 지원합니다. 분산 모드에서는 마스터 유닛(예: 중앙 집중식 모드)에서뿐만 아니라 ASA의 멤버 전체에서 여러 Site-to-Site IPsec IKEv2 VPN 연결을 분산시키는 기능을 제공합니다. 이러한 기능은 중앙 집중식 VPN 기능보다 VPN 지원을 훨씬 더 확장하며 고가용성을 제공합니다. 분산 S2S VPN은 최대 2개의 섀시로 구성된 클러스터에서 실행되며, 각 섀시는 최대 3개의 모듈(총 6개의 클러스터 멤버)을 포함하고, 각 모듈은 최대 6,000개의 액티브 세션(총 12,000개)을 지원하며, 최댓값은 약 36,000개의 액티브 세션(총 72,000개)입니다. 신규 또는 수정된 명령: **cluster redistribute vpn-sessiondb**, **show clustervpn-sessiondb**, **vpn mode** , **show cluster resource usage**, **show vpn-sessiondb** , **show connection detail**, **show crypto ikev2**

기능 이름	플랫폼 릴리스	기능 정보
향상된 클러스터 유닛 상태 검사 장애 탐지	9.8(1)	이제 유닛 상태 검사의 보류 시간을 더 낮게 0.3초(최솟값)로 구성할 수 있습니다. 이전에는 최소값이 0.8초였습니다. 이 기능은 유닛 상태 검사 메시징 체계를 제어 평면의 *keepalives*에서 데이터 평면의 하트비트로 변경합니다. 하트비트를 사용하면 제어 평면 CPU 과다 사용 및 예약 지연의 영향을 받지 않으므로 클러스터링의 신뢰성과 응답성이 개선됩니다. 대기 시간을 낮게 구성하면 클러스터 제어 링크 메시징 활동이 증가합니다. 낮은 대기 시간을 구성하기 전에 네트워크를 분석하는 것이 좋습니다. 예를 들어, 한 번의 대기 시간 간격 동안 3개의 하트비트 메시지가 있으므로 클러스터 제어 링크를 통과하는 한 유닛에서 다른 유닛으로의 핑이 *holdtime*/3 이내에 반환되는지 확인하십시오. 대기 시간을 0.3 - 0.7초로 설정한 후에 ASA 소프트웨어를 다운그레이드하는 경우, 새로운 설정이 지원되지 않으므로 이 설정은 3초의 기본값으로 되돌아갑니다. 수정된 명령: **health-check holdtime, show asp drop clustercounter, show cluster info health details**
인터페이스를 실패 상태로 표시하기 위해 구성 가능한 디바운스 시간 - Firepower 4100/9300 섀시	9.8(1)	이제 ASA가 인터페이스를 실패 상태로 간주하고 유닛이 클러스터에서 제거되기 전에 디바운스 시간을 구성할 수 있습니다. 이 기능을 통해 인터페이스 장애 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 지정되어 있는 밀리초 동안 대기합니다. 기본 디바운스 시간은 500밀리초이며 범위는 300밀리초~9초입니다. 신규 또는 수정된 명령: **health-check monitor-interface debounce-time**

기능 이름	플랫폼 릴리스	기능 정보
Firepower 4100/9300 섀시에서 ASA에 대한 사이트 간 클러스터링 개선	9.7(1)	이제 ASA 클러스터를 구축할 때 각 Firepower 4100/9300 섀시에 대한 사이트 ID를 구성할 수 있습니다. 전에는 ASA 애플리케이션 내에서 사이트 ID를 구성해야 했습니다. 이 기능 덕분에 초기 구축이 수월해졌습니다. 더 이상 ASA 구성 내에서 사이트 ID를 설정할 수 없습니다. 또한 사이트 간 클러스터링과의 호환성을 최대한 활용하려면 안정성과 성능이 개선된 ASA 9.7(1) 및 FXOS 2.1.1로 업그레이드하는 것이 좋습니다. 수정된 명령: **site-id**
관리자 현지화: 데이터 센터에 대한 사이트 간 클러스터링 개선 사항	9.7(1)	성능을 개선하고 데이터 센터에 대한 사이트 간 클러스터링을 위해 사이트 내부에서 트래픽을 유지하도록 관리자 현지화를 활성화할 수 있습니다. 새로운 연결은 일반적으로 로드 밸런싱 상태이며 지정된 사이트 내부의 클러스터 멤버가 소유합니다. 그러나 ASA는 모든 사이트에서 멤버에 관리자 역할을 할당합니다. 관리자 현지화를 사용하면 추가 관리자 역할이 활성화됩니다. 즉, 소유자와 동일한 사이트의 로컬 관리자와 모든 사이트의 전역 관리자 역할이 활성화됩니다. 소유자와 관리자를 동일한 사이트에서 유지하면 성능이 향상됩니다. 또한 원래 소유자가 실패할 경우, 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다. 전역 관리자는 클러스터 멤버가 다른 사이트에서 소유하는 연결에 대한 패킷을 수신하는 경우 사용됩니다. 도입 또는 수정된 명령: **director-localization, show asp tablecluster chash, show conn, show conn detail**
16개의 섀시에 대한 지원 - Firepower 4100 Series	9.6(2)	이제 Firepower 4100 Series에 대한 클러스터에 최대 16개의 섀시를 추가할 수 있습니다. 명령은 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
지원 - Firepower 4100 Series	9.6(1)	FXOS 1.1.4를 활용하여 ASA에서는 Firepower 4100 Series에서 최대 6개의 섀시에 대해 섀시 간 클러스터링을 지원합니다. 명령은 수정하지 않았습니다.
라우팅 모드, Spanned EtherChannel 모드에서 사이트별 IP 주소에 대한 지원	9.6(1)	Spanned EtherChannel을 사용하는 라우팅 모드에서 사이트 간 클러스터링을 위해 이제 사이트별 MCA 주소에 추가하여 사이트별 IP 주소를 구성할 수 있습니다. 사이트의 IP 주소를 추가하면 라우팅 문제를 일으킬 수 있는 전역 MAC 주소의 ARP 응답이 DCI(Data Center Interconnect)를 통해 이동하는 것을 방지하기 위해 OTV(Overlay Transport Virtualization) 디바이스에서 ARP 검사를 사용할 수 있습니다. ARP 검사는 VACL을 사용하여 MAC 주소를 필터링할 수 없는 일부 스위치에 필요합니다. 수정된 명령: **mac-address, show interface**
6개 모듈을 위한 섀시 간 클러스터링 및 Firepower 9300 ASA 애플리케이션을 위한 사이트 간 클러스터링	9.5(2.1)	이제 FXOS 1.1.3에서 사이트 간 클러스터링을 확장하여 섀시 간 클러스터링을 활성화할 수 있습니다. 최대 16개의 섀시에 최대 16개의 모듈을 포함할 수 있습니다. 명령은 수정하지 않았습니다.
라우팅 방화벽 모드에서 Spanned EtherChannel에 대한 사이트 간 클러스터링 지원을 위한 사이트별 MAC 주소	9.5(2)	이제 라우팅 모드에서 Spanned EtherChannel에 대한 사이트 간 클러스터링을 사용할 수 있습니다. MAC 주소 플래핑을 방지하려면 각 인터페이스에 대한 사이트별 MAC 주소를 사이트의 유닛 간에 공유할 수 있도록 각 클러스터 멤버에 대한 사이트 ID를 구성합니다. 도입 또는 수정된 명령: **site-id, mac-address site-id, showcluster info, show interface**

기능 이름	플랫폼 릴리스	기능 정보
인터페이스 또는 클러스터 제어 링크 실패 시 자동 다시 참가 동작의 ASA 클러스터 맞춤화	9.5(2)	이제 인터페이스 또는 클러스터 제어 링크 작동이 실패할 경우 자동 다시 참가 동작을 맞춤화할 수 있습니다. 도입된 명령: **health-check auto-rejoin**
ASA 클러스터의 GTPv1 및 GTPv2 지원	9.5(2)	이제 ASA 클러스터는 GTPv1 및 GTPv2 검사를 지원합니다. 명령은 수정하지 않았습니다.
TCP 연결에 대한 클러스터 복제 지연	9.5(2)	이 기능은 관리자/백업 플로우 생성을 지연시켜 짧은 수명의 플로우와 관련된 "불필요한 작업"을 제거하는 데 도움이 됩니다. 도입된 명령: **cluster replication delay**
사이트 간 플로우 모빌리티에 대한 LISP 검사	9.5(2)	Cisco LISP(Locator/ID Separation Protocol) 아키텍처는 디바이스 ID를 해당 위치에서 두 개의 서로 다른 숫자 공간으로 분리하여, 서버 마이그레이션을 클라이언트에 투명하게 만듭니다. ASA는 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작업을 위해 이 정보를 사용할 수 있습니다. ASA 클러스터 멤버는 첫 번째 홉 라우터와 ETR(Egress Tunnel Router) 또는 ITR(Ingress Tunnel Router) 사이를 통과하는 LISP 트래픽을 검사할 수 있으며 플로우 소유자가 새로운 사이트에 있도록 변경할 수 있습니다. 도입 또는 수정된 명령: **allowed-eid, clear cluster info flow-mobility counters, clear lisp eid, cluster flow-mobility lisp, debug cluster flow-mobility, debuglisp eid-notify-intercept, flow-mobility lisp, inspect lisp, policy-map type inspect lisp, site-id, show asp table classify domain inspect-lisp, show cluster info flow-mobility counters, showconn, show lisp eid, show service-policy, validate-key**

기능 이름	플랫폼 릴리스	기능 정보
장애 조치 및 ASA 클러스터링에서의 통신 사업자급 NAT 개선 사항 지원	9.5(2)	통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 이 기능은 이제 장애 조치 및 ASA 클러스터 구축에서 지원됩니다. 수정된 명령: **show local-host**
추적 항목 클러스터링의 구성 가능한 레벨	9.5(2)	기본적으로 클러스터링 이벤트의 모든 레벨이 많은 낮은 레벨의 이벤트를 포함하여 추적 버퍼에 포함되어 있습니다. 더 높은 레벨의 이벤트로 추적을 제한하기 위해 클러스터에 대해 최소한의 추적 레벨을 설정할 수 있습니다. 도입된 명령: **trace-level**
Firepower 9300을 위한 섀시 내 ASA 클러스터링	9.4(1.150)	Firepower 9300 섀시 내부에서 최대 3개의 보안 모듈을 클러스터링할 수 있습니다. 섀시의 모든 모듈은 클러스터에 속해야 합니다. 도입된 명령: **cluster replication delay, debug service-module, management-only individual, show cluster chassis**

III 부

인터페이스

12 장

기본 인터페이스 구성

이 장에서는 이더넷 설정 및 점보 프레임 구성을 비롯한 기본 인터페이스 구성을 다룹니다.

참고 다중 상황 모드의 경우, 시스템 실행 영역에서 모든 작업을 완료합니다. 상황에서 시스템 실행 공간으로 변경하려면 **changeto system** 명령을 입력합니다..

참고 ASA Services Module 인터페이스에 대한 내용은 ASA Services Module 빠른 시작 가이드를 참조하십시오.

Firepower 2100 및 Firepower 4100/9300 섀시에 있는 ASA의 경우, FXOS 운영 체제에서 기본 인터페이스 설정을 구성합니다. 자세한 내용은 섀시에 대한 구성 또는 시작 가이드를 참조하십시오.

기본 인터페이스 구성 정보

이 섹션에서는 인터페이스 기능과 특수 인터페이스에 대해 설명합니다.

Auto-MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

관리 인터페이스

관리 인터페이스는 모델에 따라 다르며 관리 트래픽만을 위한 별도의 인터페이스입니다.

관리 인터페이스 개요

다음에 연결하여 ASA를 관리할 수 있습니다.

- 통과 트래픽 인터페이스
- 전용 관리 슬롯/포트 인터페이스(모델에 제공되는 경우)

#unique_32에 따라 인터페이스에 대한 관리 액세스를 구성해야 할 수도 있습니다.

관리 슬롯/포트 인터페이스

다음 표는 모델별 관리 인터페이스를 보여 줍니다.

표 ***18:*** 모델별 관리 인터페이스

모델	**Management 0/0**	**Management 0/1**	**Management 1/0**	**Management 1/1**	통과 트래픽을 위해 구성 가능	하위 인터페이스 허용
ASA 5506-X	아니요	아니요	아니요	예	아니요	아니요
ASA 5508-X	아니요	아니요	아니요	예	아니요	아니요
ASA 5512-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5515-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5516-X	아니요	아니요	아니요	예	아니요	아니요
ASA 5525-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5545-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5555-X	예	아니요	아니요	아니요	아니요	아니요

모델	**Management 0/0**	**Management 0/1**	**Management 1/0**	**Management 1/1**	통과 트래픽을 위해 구성 가능	하위인터페이스 허용
ASA 5585-X	예	예	예 슬롯 1에 SSP가 설치된 경우 관리 1/0 및 1/1에서는 슬롯 1의 SSP에만 관리 액세스를 제공합니다.	예	예	예
Firepower 2100	아니요	아니요	아니요	예	예	예
ASA - Firepower 4100/9300 섀시	해당 없음 인터페이스 ID는 ASA 논리적 디바이스에 할당한 물리적 관리 유형 인터페이스에 따라 달라집니다.	해당 없음	해당 없음	해당 없음	아니요	예
ISA 3000	아니요	아니요	아니요	예	아니요	아니요
ASASM	아니요	아니요	아니요	아니요	해당 없음	해당 없음
ASAv	예	아니요	아니요	아니요	예	아니요

참고 모듈을 설치한 경우 모듈 관리 인터페이스에서는 해당 모듈에만 관리 액세스를 제공합니다. 소프트웨어 모듈이 있는 모델의 경우, 소프트웨어 모듈에서 ASA와 동일한 물리적 관리 인터페이스를 사용합니다.

관리 전용 트래픽에 모든 인터페이스 사용

어떤 인터페이스든 관리 트래픽용으로 구성함으로써 관리 전용 인터페이스로 사용할 수 있습니다. 여기에는 EtherChannel 인터페이스도 포함됩니다(**management-only** 명령 참조).

투명 모드의 관리 인터페이스

투명 방화벽 모드에서는 최대 허용되는 통과 트래픽 인터페이스 외에도, 관리 인터페이스(물리적 인터페이스 또는 하위 인터페이스(모델에서 지원되는 경우) 또는 여러 개의 관리 인터페이스로 구성된 EtherChannel 인터페이스(관리 인터페이스가 여러 개인 경우))를 별도의 관리 인터페이스로 사용할 수 있습니다. 그 밖의 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다. Firepower 4100/9300

섀시의 경우 관리 인터페이스 ID는 ASA 논리적 디바이스에 할당한 관리 유형 인터페이스에 따라 달라집니다.

다중 상황 모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 상황에서 공유할 수 없습니다. 컨텍스트별 관리를 위해 관리 인터페이스의 하위 인터페이스를 만들고 각 컨텍스트에 관리 하위 인터페이스를 할당할 수 있습니다. ASA 5555-X 이하의 경우 관리 인터페이스에서 하위 인터페이스를 지원하지 않습니다. 따라서 상황별 관리를 위해서는 데이터 인터페이스에 연결해야 합니다.

관리 인터페이스는 일반적인 브리지 그룹에 포함되지 않습니다. 운영상의 목적 때문에 관리 인터페이스는 구성 불가능한 브리지 그룹에 포함됩니다.

참고 투명 방화벽 모드의 경우 관리 인터페이스에서는 MAC 주소 테이블을 데이터 인터페이스와 같은 방식으로 업데이트합니다. 따라서 스위치 포트 중 하나를 라우팅 포트로 구성하지 않는 한 관리 인터페이스와 데이터 인터페이스 둘 다 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않고 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 관리 인터페이스를 사용하여 스위치에 액세스하도록 MAC 주소 테이블을 업데이트합니다. 이 작업으로 인해 일시적인 트래픽 중단이 발생합니다. ASA에서는 보안상의 이유로 인해 스위치에서 데이터 인터페이스로 전달되는 패킷의 MAC 주소 테이블을 최소 30초간 다시 업데이트하지 않습니다.

이중 관리 인터페이스 미지원

이중 인터페이스는 관리 슬롯/포트 인스턴스를 멤버로 지원하지 않습니다. 그러나, 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 있습니다.

ASA 5585-X를 제외한 모든 모델의 관리 인터페이스 특징

관리 인터페이스에는 다음과 같은 특징이 있습니다.

- 통과 트래픽을 지원하지 않음
- 하위 인터페이스를 지원하지 않음
- 우선순위 대기열을 지원하지 않음
- 멀티캐스트 MAC을 지원하지 않음
- 소프트웨어 모듈은 관리 인터페이스를 공유합니다. ASA 및 모듈에서는 별도의 MAC 주소와 IP 주소가 지원됩니다. 모듈 운영 체제 내에서 모듈 IP 주소의 컨피그레이션을 수행해야 합니다. 그러나 물리적 특징(예: 인터페이스 활성화)은 ASA에서 구성됩니다.

기본 인터페이스 구성에 대한 라이센싱

모델	라이센스 요건
ASA 5585-X	SSP-10 및 SSP-20을 위한 인터페이스 속도: • Base 라이센스—파이버 인터페이스용 1기가비트 이더넷 • 10GE I/O 라이센스(Security Plus)—파이버 인터페이스용 10기가비트 이더넷 • (SSP-40 및 SSP-60은 10기가비트 이더넷을 기본적으로 지원)

기본 인터페이스 구성에 대한 지침

투명 방화벽 모드

다중 상황, 투명 모드의 경우 각 상황에서는 다른 인터페이스를 사용해야 하며 상황 간에 인터페이스를 공유할 수 없습니다.

페일오버

장애 조치 또는 상태 인터페이스는 데이터 인터페이스와 공유할 수 없습니다.

추가 지침

일부 관리 관련 서비스는 비 관리 인터페이스가 활성화되고 ASA가 "시스템 준비됨" 상태에 도달할 때까지 사용할 수 없습니다. 이 ASA는 "시스템 준비됨" 상태일 때 다음 syslog 메시지를 생성합니다.

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

기본 인터페이스 구성의 기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형 및 상황 모드에 따라 다릅니다.

다중 상황 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 시스템 실

행 영역에서도 인터페이스가 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.

단일 모드 또는 시스템 실행 영역에서 인터페이스의 기본 상태는 다음과 같습니다.

- 물리적 인터페이스 - 비활성화됨.
- 이중 인터페이스 — 활성화되어 있습니다. 그러나 트래픽이 이중 인터페이스를 통과하려면 물리적 인터페이스 멤버도 활성화되어야 합니다.
- VLAN 하위 인터페이스 - 활성화됨, 그러나 트래픽이 하위 인터페이스를 통과하려면 물리적 인터페이스도 활성화되어야 합니다.
- VXLAN VNI 인터페이스 - 활성화됨
- EtherChannel 포트 채널 인터페이스(ASA 모델) — 활성화되어 있습니다. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 채널 인터페이스(Firepower 모델) — 비활성화되어 있습니다.

참고 Firepower 4100/9300의 경우, 관리를 위해 섀시와 ASA에서 인터페이스를 활성화하고 비활성화할 수 있습니다. 인터페이스는 두 운영 체제에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로 섀시와 ASA 간에 상태가 일치하지 않을 수도 있습니다.

기본 속도와 양방향

- 기본적으로 구리(RJ-45) 인터페이스의 속도와 양방향은 자동 협상이 이루어지도록 설정됩니다.
- 5585-X용 파이버 인터페이스의 경우 자동 링크 협상에 대한 속도가 설정됩니다.

기본 커넥터 유형

일부 모델은 구리 RJ-45와 파이버 SFP의 2가지 커넥터 유형이 있습니다. RJ-45가 기본 유형입니다. 파이버 SFP 커넥터를 사용하도록 ASA를 구성할 수 있습니다.

기본 **MAC** 주소

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

물리적 인터페이스 활성화 및 이더넷 파라미터 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화
- 특정 속도 및 양방향 설정(제공되는 경우)

- 흐름 제어를 위한 일시 중지 프레임 활성화

시작하기 전에

다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 구성할 인터페이스를 지정합니다.

interface *physical_interface*

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID에는 유형, 슬롯, 포트 번호가 유형[슬롯/]포트로 포함되어 있습니다.

물리적 인터페이스 유형은 다음과 같습니다.

- **gigabitethernet**
- **tengigabitethernet**
- **management**

유형 뒤에는 *slot*/*port*를 입력합니다(예: **gigabitethernet0/1**). 유형과 슬롯/포트 사이에 공백을 넣을 수도 있습니다.

단계 **2** (선택사항)모델에 제공되는 경우 미디어 유형을 SFP로 설정합니다.

media-type sfp

기본값 RJ-45를 복원하려면 **media-type rj45** 명령을 입력합니다.

단계 **3** (선택사항) 속도를 설정합니다.

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

예제**:**

```
ciscoasa(config-if)# speed 100
```

RJ-45 인터페이스의 기본 설정은 **auto**입니다.

SFP 인터페이스의 기본 설정은 **no speed nonegotiate**이며, 이 경우 속도가 최대 속도로 설정되고 흐름 제어 매개변수 및 원격 오류 정보에 대한 링크 협상이 활성화됩니다. **nonegotiate** 키워드는 SFP에 사용할 수 있는 유일한 키워드입니다. **speed nonegotiate** 명령을 사용하면 링크 협상이 비활성화됩니다.

단계 **4** (선택사항) RJ-45 인터페이스에 양방향을 설정합니다.

duplex{**auto** | **full** | **half**}

예제:

```
ciscoasa(config-if)# duplex full
```

auto 설정이 기본값입니다. EtherChannel 인터페이스의 양방향 설정은 **full(**전체**)** 또는 **auto(**자동**)**여야 합니다.

단계 **5** (선택사항) GigabitEthernet 및 TenGigabitEthernet 인터페이스에서 흐름 제어를 위한 일시 중지(XOFF) 프레임을 활성화합니다.

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

예제:

```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```

트래픽 버스트가 있을 경우 이러한 버스트가 NIC에서 FIFO 버퍼의 버퍼링 용량을 초과하고 링 버퍼를 수신하면 패킷 손실이 발생할 수 있습니다. 흐름 제어를 위한 일시 중지 프레임을 활성화하면 이러한 문제를 완화할 수 있습니다. 일시 중지(XOFF) 및 XON 프레임은 FIFO 버퍼 사용량을 기준으로 NIC 하드웨어에서 자동으로 생성됩니다. 일시 중지 프레임은 버퍼 사용량이 최고 수위를 넘을 때 전송됩니다. *high_water* 기본값은 128KB(10 GigabitEthernet) 및 24KB(1 GigabitEthernet)이며 0KB ~ 511KB(10 GigabitEthernet) 또는 0KB ~ 47KB(1 GigabitEthernet) 범위에서 설정할 수 있습니다. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. *high_water* 기본값은 64KB(10 GigabitEthernet) 및 16KB(1 GigabitEthernet)이며 0KB ~ 511KB(10 GigabitEthernet) 또는 0KB ~ 47KB(1 GigabitEthernet) 범위에서 설정할 수 있습니다. 연결 파트너는 XON을 수신한 후 또는 XOFF가 만료된 후 일시 중지 프레임의 타이머 값에 따라 트래픽을 다시 시작할 수 있습니다. *pause_time* 기본값은 26624이며 이를 0 ~ 65535에서 설정할 수 있습니다. 버퍼 사용량이 지속적으로 최고 수위를 넘을 경우, 일시 중지 프레임이 반복해서 전송되며 이는 일시 중지 새로 고침 임계값에 의해 제어됩니다.

이 명령을 사용할 경우 다음과 같은 경고가 표시됩니다.

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

메시지 없이 매개변수를 변경하려면 **noconfirm** 키워드를 사용합니다.

참고 802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.

단계 **6** 인터페이스를 활성화합니다.

no shutdown

예제:

```
ciscoasa(config-if)# no shutdown
```

인터페이스를 비활성화하려면 **shutdown** 명령을 입력합니다. **shutdown** 명령을 입력할 경우 모든 하위 인터페이스도 종료됩니다. 시스템 실행 영역에서 인터페이스를 종료할 경우, 이를 공유하는 모든 상황에서 해당 인터페이스가 종료됩니다.

점보 프레임 지원 활성화

점보 프레임은 최대 표준 1518바이트(Layer 2 헤더 및 VLAN 헤더 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. ASA MTU는 페이로드 크기(Layer 2(14바이트) 및 VLAN 헤더(4바이트) 포함 안 함)를 설정하므로 모델에 따라 최대 MTU는 9198이 됩니다.

시작하기 전에

- 다중 상황 모드의 경우 시스템 실행 영역에서 이 옵션을 설정합니다.
- 이 설정을 변경하면 ASA를 다시 로드해야 합니다.
- 점보 프레임을 전송해야 하는 각 인터페이스의 MTU는 기본값 1500보다 높은 값으로 설정해야 합니다. 예를 들어, **mtu** 명령을 사용하여 값을 9198로 설정합니다. 다중 상황 모드의 경우, 각 상황 내에서 MTU를 설정합니다.
- IPsec 이외 트래픽에는 TCP MSS를 비활성화(**sysopt connection tcpmss 0** 명령 사용)하거나 MTU에 맞춰 TCP MSS를 늘리는 방식으로 TCP MSS를 조정해야 합니다.

프로시저

점보 프레임 지원을 활성화합니다.

jumbo-frame reservation

예

다음 예에서는 점보 프레임 예약을 활성화하고 구성을 저장하며 ASA를 다시 로드합니다.

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
```

```
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

모니터링 인터페이스

다음 명령을 참조하십시오.

- **show interface**

  인터페이스 통계를 표시합니다.

- **show interface ip brief**

  인터페이스 IP 주소와 상태를 표시합니다.

기본 인터페이스의 예

다음 구성 예를 참조하십시오.

물리적 인터페이스 파라미터의 예

다음 예에서는 단일 모드에서 물리적 인터페이스의 매개변수를 구성합니다.

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

다중 상황 모드의 예

다음 예에서는 다중 상황 모드에서 시스템 컨피그레이션에 대한 인터페이스 매개변수를 컨피그레이션하고, gigabitethernet 0/1.1 하위 인터페이스를 contextA에 할당합니다.

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

기본 인터페이스 구성 내역

표 ***19:*** 인터페이스 내역

기능 이름	릴리스	기능 정보
ASA 5510의 Base 라이센스 인터페이스 증가	7.2(2)	ASA 5510의 Base 라이센스의 경우, 인터페이스의 최대 수가 3개에서 관리 인터페이스까지 추가하여 무제한 인터페이스로 증가했습니다.
ASA 5510 Security Plus 라이센스의 기가비트 이더넷 지원	7.2(3)	ASA 5510 에서 Security Plus 라이센스와 함께 포트 0 및 1에 GE(기가비트 이더넷)를 지원합니다. Base License를 Security Plus License로 업그레이드할 경우 외부 Ethernet0/0 및 Ethernet0/1 포트의 용량이 원래의 FE(패스트 이더넷)(100Mbps)에서 GE(1000Mbps)로 증가합니다. 인터페이스 이름은 그대로 Ethernet 0/0 및 Ethernet 0/1입니다. **speed** 명령을 사용하여 인터페이스의 속도를 변경하고, **show interface** 명령을 사용하여 각 인터페이스에 현재 구성된 속도를 확인합니다.
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 최대 표준 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. 또한 이 기능은 ASA 5585-X에서도 지원됩니다. 다음 명령을 도입했습니다. **jumbo-frame reservation**

기능 이름	릴리스	기능 정보
ASA 5580 10기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(2)	흐름 제어를 위해 Pause(XOFF) 프레임을 활성화할 수 있습니다. 또한 이 기능은 ASA 5585-X에서도 지원됩니다. 다음 명령을 도입했습니다. **flowcontrol**
기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(5)/8.4(2)	모든 모델에서 기가비트 이더넷 인터페이스에 흐름 제어를 위한 일시 중지(XOFF) 프레임을 사용할 수 있습니다. 다음 명령을 수정했습니다. **flowcontrol**.
ASAv에 대한 Management 0/0 인터페이스에서의 통과 트래픽 지원	9.6(2)	이제 ASAv의 Management 0/0 인터페이스에서 트래픽을 통과하도록 허용할 수 있습니다. 이전에는 Microsoft Azure의 ASAv에서만 통과 트래픽을 지원했지만, 이제 모든 ASAv에서 통과 트래픽을 지원합니다. 이 인터페이스를 관리 전용으로 구성하도록 선택할 수 있지만 기본적으로 관리 전용으로 구성되어 있지 않습니다. 수정된 명령: **management-only**

13 장

EtherChannel 및 이중 인터페이스

이 장에서는 EtherChannel 및 이중 인터페이스를 구성하는 방법을 알려 줍니다.

참고 다중 상황 모드의 경우, 시스템 실행 영역에서 모든 작업을 완료합니다.상황에서 시스템 실행 공간으로 변경하려면 **changeto system** 명령을 입력합니다..

특별한 요구 사항이 있는 ASA 클러스터 인터페이스에 대해서는 ASA 클러스터, 351 페이지의 내용을 참조하십시오.

참고 Firepower 2100 및 Firepower 4100/9300 섀시에 있는 ASA의 경우, FXOS 운영 체제에서 EtherChannel 인터페이스가 구성됩니다. 이중 인터페이스는 지원되지 않습니다. 자세한 내용은 섀시에 대한 구성 또는 시작 가이드를 참조하십시오.

EtherChannel 및 이중 인터페이스 정보

이 섹션에서는 EtherChannel 및 이중 인터페이스를 설명합니다.

이중 인터페이스

논리적 이중 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중 인터페이스와 함께 디바이스 수준 장애 조치를 구성할 수 있습니다.

최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.

이중 인터페이스 MAC 주소

이중 인터페이스는 추가한 첫 번째 물리적 인터페이스의 MAC 주소를 사용합니다. 구성에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 변경됩니다. 또는 멤버 인터페이스 MAC 주소에 관계없이 사용되는 이중 인터페이스에 수동 MAC 주소를 할당할 수 있습니다. 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 때 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

관련 항목

MTU 및 TCP MSS 구성, 657 페이지
다중 상황 구성, 231 페이지

EtherChannel

802.3ad EtherChannel은 개별 이더넷 링크(채널 그룹)의 번들로 구성된 논리적 인터페이스(일명 포트 채널 인터페이스)이므로, 단일 네트워크의 대역폭을 늘리게 됩니다. 포트 채널 인터페이스는 인터페이스 관련 기능을 구성할 경우 물리적 인터페이스와 동일한 방식으로 사용됩니다.

최대 48개의 EtherChannel을 구성할 수 있습니다.

채널 그룹 인터페이스

각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다. 16개의 액티브 인터페이스를 사용하려는 경우 스위치에서 해당 기능을 지원하는지 확인하십시오(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000).

채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다. RJ-45 또는 SFP 커넥터를 사용하도록 구성할 수 있는 인터페이스의 경우 RJ-45 및 SFP 인터페이스를 동일한 EtherChannel에 모두 포함할 수 있습니다.

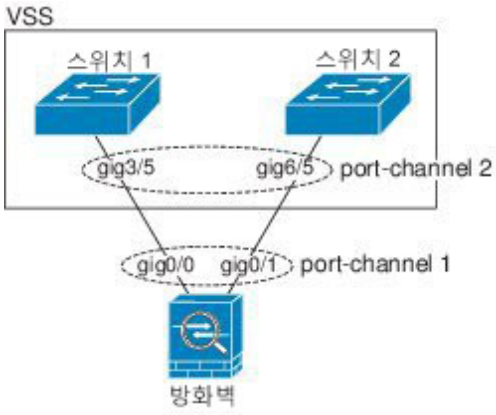
EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

다른 디바이스에서 **EtherChannel**에 연결

ASA EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어 Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.

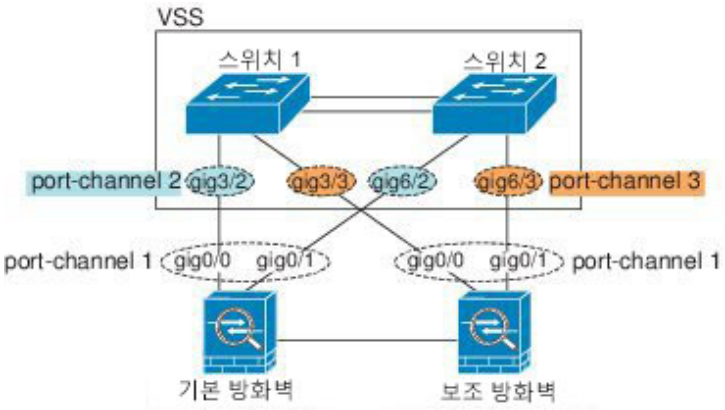
스위치가 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel)의 일부인 경우, 동일한 EtherChannel 내에서 ASA 인터페이스를 연결하여 VSS/vPC에서 스위치를 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다.

그림 ***55: VSS/vPC***에 연결



활성/대기 장애 조치 구축 시 ASA를 사용할 경우 VSS/vPC의 스위치에 각 ASA에 별도의 EtherChannel을 생성해야 합니다. 각 ASA에서 하나의 EtherChannel이 두 스위치 모두에 연결됩니다. 모든 스위치 인터페이스를 ASA에 연결된 단일 EtherChannel으로 그룹화하는 것은 가능하지만(이 경우 별도의 ASA 시스템 ID로 인해 EtherChannel이 설정되지 않음), 스탠바이 ASA로 트래픽이 전송되는 것은 바람직하지 않으므로 단일 EtherChannel은 권장되지 않습니다.

그림 ***56:*** 액티브/스탠바이 장애 조치 및 ***VSS/vPC***



LACP(Link Aggregation Control Protocol)

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 인터페이스를 다음과 같이 구성할 수 있습니다.

- 액티브 — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- 패시브 — LACP 업데이트를 받습니다. 패시브 EtherChannel은 오로지 액티브 EtherChannel과 연결을 설정할 수 있습니다.
- 켜짐 — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

부하 균형

ASA에서는 패킷의 소스 및 대상 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(이 조건은 구성 가능함). 결과의 나머지 부분에 따라 흐름을 보유하는 인터페이스가 결정되는 모듈로 작업의 액티브 링크 수를 기준으로 결과 해시가 분할됩니다. *hash_value* **mod** *active_links*의 결과가 0인 모든 패킷은 EtherChannel의 첫 번째 인터페이스로 이동하고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스로 이동하는 방식이 이어집니다. 예를 들어 액티브 링크가 15개 있는 경우 모듈로 작업에서는 0에서 14까지의 값을 제공합니다. 액티브 링크가 6개인 경우 해당 값은 0 ~ 5가 되며, 이런 식으로 계속 적용할 수 있습니다.

클러스터링의 Spanned EtherChannel에서는 ASA 단위로 로드 밸런싱이 이루어집니다. 예를 들어 8개의 ASA 전체에서 Spanned EtherChannel에 32개의 액티브 인터페이스가 있는 경우 EtherChannel의 ASA당 인터페이스는 4개이며 ASA의 4개 인터페이스에만 로드 밸런싱이 실행됩니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 Layer 2의 스패닝 트리와 Layer 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

관련 항목

EtherChannel 사용자 지정, 578 페이지

EtherChannel MAC 주소

채널 그룹의 일부인 모든 인터페이스에서는 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다.

포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다.다중 상황 모드에서는 EtherChannel 포트 인터페이스를 비롯한 공유 인터페이스에 고유한 MAC 주소를 자동으로 할당할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 공유 인터페이스에 대한 다중 상황 모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널

MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

EtherChannel 및 이중 인터페이스에 대한 지침

브리지 그룹

라우팅 모드에서 EtherChannel은 브리지 그룹 멤버로 지원되지 않습니다.

장애 조치

- 이중 또는 EtherChannel 인터페이스를 장애 조치 링크로 사용할 경우, 장애 조치 쌍의 두 유닛에 모두 이를 사전 구성해야 합니다. 장애 조치복제를 위해서는 링크 자체가 필요하므로 이러한 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 이중 또는 EtherChannel 인터페이스를 사용할 경우, 특별한 구성이 필요하지 않으며 구성을 기본 유닛에서 정상적으로 복제할 수 있습니다.
- **monitor-interface** 명령을 사용하여 장애 조치를 위한 이중 또는 EtherChannel 인터페이스를 모니터링할 수 있습니다. 이때 논리적 이중 인터페이스 이름을 참조해야 합니다. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준의 장애 조치가 모니터링되고 있으면 이 작업을 수행해도 이중 또는 EtherChannel 인터페이스에 장애가 발생하는 것으로 나타나지 않습니다. 모든 물리적 인터페이스에 장애가 발생한 경우에만 이중 또는 EtherChannel 인터페이스에 장애가 발생하는 것으로 나타납니다(EtherChannel 인터페이스의 경우 장애 발생이 허용되는 인터페이스 수를 구성할 수 있음).
- 장애 조치 또는 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 패킷의 장애를 방지하기 위해 EtherChannel에서 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 구성을 변경할 수 없습니다. 구성을 변경하려면 변경하는 동안에는 EtherChannel을 종료하거나 장애 조치를 일시적으로 비활성화해야 합니다. 이렇게 하면 해당 기간에는 장애 조치가 발생하지 않습니다.

모델 지원

- EtherChannel은 ASA 어플라이언스에서만 지원되며 ASAv 또는 ASASM에서는 지원되지 않습니다.
- Firepower 2100 및 Firepower 4100/9300 섀시의 경우, ASA OS가 아니라 FXOS에 EtherChannel을 구성합니다.
- 이중 인터페이스는 Firepower 2100, Firepower 4100/9300 섀시 및 ASASM에서 지원되지 않습니다.

클러스터링

- 이중 또는 EtherChannel 인터페이스를 클러스터 제어 링크로 사용할 경우, 클러스터의 모든 유닛에 이를 사전 구성해야 합니다. 복제를 위해서는 클러스터 제어 링크 자체가 필요하므로 이러한 인터페이스를 기본 유닛에 구성한 다음 이를 멤버 유닛에 복제할 수 없습니다.
- 스팬 EtherChannel 또는 개별 클러스터 인터페이스를 구성하려면 클러스터링 장을 참조하십시오.

이중 인터페이스

- 최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 이중 인터페이스를 참조합니다.
- 이중 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중 인터페이스 일부로 사용할 수 없습니다. 이중 인터페이스 및 EtherChannel 인터페이스에서 동일한 물리적 인터페이스를 사용할 수 없습니다. 그러나 이러한 인터페이스에서 동일한 물리적 인터페이스를 사용하지 않을 경우 ASA에서 두 가지 유형을 구성할 수 있습니다.
- 액티브 인터페이스를 종료할 경우 스탠바이 인터페이스가 액티브 상태로 됩니다.
- 이중 인터페이스는 관리 슬롯/포트 인스턴스를 멤버로 지원하지 않습니다. 그러나, 비관리 인터페이스로 구성된 이중 인터페이스를 관리 전용으로 설정할 수 있습니다.

EtherChannel

- EtherChannel은 ASA 어플라이언스에서만 지원되며 ASAv 또는 ASASM에서는 지원되지 않습니다.
- 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다.
- 채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다. RJ-45 또는 SFP 커넥터를 사용하도록 구성할 수 있는 인터페이스의 경우, 동일한 네트워크 모듈에 있는 RJ-45 및 SFP 인터페이스를 모두 동일한 EtherChannel에 포함할 수 있습니다.
- ASA EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. Catalyst 6500 스위치 또는 Cisco Nexus 7000 스위치에 연결할 수 있는 경우를 예로 들 수 있습니다.
- ASA에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS **vlan dot1Q tag native** 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, ASA에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니

다. 다중 상황 모드의 경우 이러한 메시지가 패킷 캡처에 포함되지 않으므로 문제를 쉽게 진단할 수 없습니다.

- 15.1(1)S2 이전 Cisco IOS 소프트웨어 버전에서는 ASA가 EtherChannel과 스위치 스택 간의 연결을 지원하지 않았습니다. 기본 스위치 설정으로 ASA EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.
- 모든 ASA 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.
- 이중 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중 인터페이스 일부로 사용할 수 없습니다. 이중 인터페이스 및 EtherChannel 인터페이스에서 동일한 물리적 인터페이스를 사용할 수 없습니다. 그러나 이러한 인터페이스에서 동일한 물리적 인터페이스를 사용하지 않을 경우 ASA에서 두 가지 유형을 구성할 수 있습니다.

EtherChannel 및 이중 인터페이스에 대한 기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형 및 상황 모드에 따라 다릅니다.

다중 상황 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 시스템 실행 영역에서도 인터페이스가 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.

단일 모드 또는 시스템 실행 영역에서 인터페이스의 기본 상태는 다음과 같습니다.

- 물리적 인터페이스 - 비활성화됨.
- 이중 인터페이스 — 활성화되어 있습니다. 그러나 이중 인터페이스를 통해 트래픽을 전달하려면 멤버 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 채널 인터페이스—활성화됨. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.

이중 인터페이스 구성

논리적 이중 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니

다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중 인터페이스와 함께 장애 조치를 구성할 수 있습니다.

이 섹션에서는 이중 인터페이스를 구성하는 방법에 대해 설명합니다.

이중 인터페이스 구성

이 섹션에서는 이중 인터페이스를 생성하는 방법에 대해 설명합니다. 기본적으로 이중 인터페이스는 활성화되어 있습니다.

시작하기 전에

- 최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.
- 이중 인터페이스 지연 값은 구성 가능하나, 기본적으로 ASA에서는 멤버 인터페이스의 물리적 유형을 기준으로 기본 지연 값을 상속합니다.
- 두 멤버 인터페이스 모두 물리적 유형이 같아야 합니다. 이를테면 모두 GigabitEthernet이어야 합니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중 인터페이스에 추가할 수 없습니다. 우선 **no nameif** 명령을 사용하여 이름을 제거해야 합니다.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다.상황에서 시스템 실행 공간으로 변경하려면 **changeto system** 명령을 입력합니다..

⚠

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

프로시저

단계 **1** 논리적 이중 인터페이스를 추가합니다.

interface redundant *number*

예제**:**

```
ciscoasa(config)# interface redundant 1
```

number 인수는 1~8 사이의 정수입니다.

논리적 매개변수(예: 이름)를 구성하기 전에 하나 이상의 멤버 인터페이스를 이중 인터페이스에 추가해야 합니다.

단계 **2** 첫 번째 멤버 인터페이스를 이중 인터페이스에 추가합니다.

member-interface *physical_interface*

예제:

```
ciscoasa(config-if)# member-interface gigabitethernet 0/0
```

이중 인터페이스는 관리 슬롯/포트 인스턴스를 멤버로 지원하지 않습니다.

인터페이스를 추가하면 해당 인터페이스의 모든 컨피그레이션(예: IP 주소)이 제거됩니다.

단계 **3** 두 번째 멤버 인터페이스를 이중 인터페이스에 추가합니다.

member-interface *physical_interface*

예제:

```
ciscoasa(config-if)# member-interface gigabitethernet 0/1
```

두 번째 인터페이스는 첫 번째 인터페이스와 물리적 유형이 동일해야 합니다.

멤버 인터페이스를 제거하려면 **no member-interface** *physical_interface* 명령을 입력합니다. 이중 인터페이스에서 두 멤버 인터페이스를 모두 제거할 수 없습니다. 이중 인터페이스에는 최소 하나의 멤버 인터페이스가 필요합니다.

예

다음 예에서는 2개의 이중 인터페이스를 생성합니다.

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

활성 인터페이스 변경

기본적으로 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 인터페이스입니다.

프로시저

단계 **1** 어떤 인터페이스가 액티브 상태인지 보려면 에 다음 명령을 입력합니다.

show interface redundant *number* **detail | grep Member**

예제:

```
ciscoasa# show interface redundant1 detail | grep Member
```

```
Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

단계 **2** 활성 인터페이스를 변경합니다.

redundant-interface redundant *number* **active-member** *physical_interface*

redundant*number* 인수는 이중 인터페이스 ID(예: **redundant1**)입니다.

*physical_interface*는 액티브로 변경하려는 멤버 인터페이스 ID입니다.

EtherChannel 구성

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하며, EtherChannel을 맞춤화하는 방법에 대해 알아봅니다.

EtherChannel에 인터페이스 추가

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고 EtherChannel에 인터페이스를 할당하는 방법에 대해 알아봅니다. 기본적으로 포트 채널 인터페이스는 활성화되어 있습니다.

시작하기 전에

- 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다.
- 클러스터링에 스팬 EtherChannel을 구성하려면 이 절차 대신 클러스터링 장을 참조하십시오.
- 채널 그룹의 모든 인터페이스는 유형, 속도, 양방향이 동일해야 합니다. 반이중은 지원되지 않습니다. 참고로, RJ-45 또는 SFP 커넥터를 사용하도록 구성할 수 있는 인터페이스의 경우 RJ-45 및 SFP 인터페이스를 동일한 EtherChannel에 모두 포함할 수 있습니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 채널 그룹에 추가할 수 없습니다. 우선 **no nameif** 명령을 사용하여 이름을 제거해야 합니다.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다.상황에서 시스템 실행 공간으로 변경하려면 **changeto system** 명령을 입력합니다..

⚠

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

프로시저

단계 **1** 채널 그룹에 추가할 인터페이스를 지정합니다.

interface *physical_interface*

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID에는 유형, 슬롯, 포트 번호가 유형[슬롯/] 포트로 포함되어 있습니다. 채널 그룹의 첫 번째 인터페이스는 그룹에 있는 모든 기타 인터페이스의 유형과 속도를 결정합니다.

투명 모드에서 여러 개의 관리 인터페이스가 있는 채널 그룹을 생성할 경우, 이 EtherChannel을 관리 전용 인터페이스로 사용할 수 있습니다.

단계 **2** 이 물리적 인터페이스를 EtherChannel에 할당합니다.

channel-group *channel_id* **mode** {**active** | **passive** | **on**}

예제**:**

```
ciscoasa(config-if)# channel-group 1 mode active
```

*channel_id*는 1~48 사이의 정수입니다. 이러한 채널 ID의 채널 포트 인터페이스가 컨피그레이션에 아직 없을 경우, 다음이 추가됩니다.

interface port-channel *channel_id*

active 모드를 사용하는 것이 좋습니다.

단계 **3** (선택사항) 채널 그룹의 물리적 인터페이스에 대한 우선순위를 설정합니다.

lacp port-priority *number*

예제**:**

```
ciscoasa(config-if)# lacp port-priority 12345
```

우선순위 *number*는 1~65535 사이의 정수입니다. 기본값은 32768입니다. 숫자가 높을수록 우선 순위는 낮아집니다. 사용할 수 있는 인터페이스보다 더 많은 인터페이스가 할당된 경우, ASA에서는 이 설정을 사용하여 어떤 인터페이스가 액티브이고 스탠바이인지 확인합니다. 포트 우선 순위 설정이 모든 인터페이스에 대해 동일한 경우, 인터페이스 ID(슬롯/포트)로 우선 순위가 결정됩니다. 가장 낮은 인터페이스 ID의 우선 순위가 가장 높습니다. 예를 들어 GigabitEthernet 0/0은 GigabitEthernet 0/1보다 우선 순위가 더 높습니다.

인터페이스 ID가 더 큰 인터페이스에 우선 순위를 부여하여 액티브 상태로 만들려면 이 명령을 더 낮은 값으로 설정합니다. 예를 들어 GigabitEthernet 1/3을 GigabitEthernet 0/7보다 우선 순위가 높은 액티브 상태로 만들려면 0/7 인터페이스의 기본값인 32768과 달리 1/3 인터페이스의 **lacp port-priority** 값을 12345로 설정합니다.

EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선 순위가 충돌할 경우, 시스템 우선 순위를 통해 어느 포트 우선 순위를 사용해야 할지 결정됩니다. **lacp system-priority** 명령을 참조하십시오.

단계 **4** 채널 그룹에 추가할 각 인터페이스에 1단계 ~ 3단계를 반복합니다.

채널 그룹의 각 인터페이스는 유형과 속도가 같아야 합니다. 반이중은 지원되지 않습니다. 일치하지 않는 인터페이스를 추가할 경우 보류 상태가 됩니다.

관련 항목

LACP(Link Aggregation Control Protocol), 569 페이지
EtherChannel 사용자 지정, 578 페이지

EtherChannel 사용자 지정

이 섹션에서는 EtherChannel의 인터페이스 최대 개수, 활성 상태가 되어야 할 EtherChannel의 최소 운영 인터페이스 개수, 로드 밸런싱 알고리즘, 기타 선택적 매개변수를 설정하는 방법에 대해 설명합니다.

프로시저

단계 **1** 포트 채널 인터페이스를 지정합니다.

interface port-channel *channel_id*

예제:

```
ciscoasa(config)# interface port-channel 1
```

채널 그룹에 어떤 인터페이스를 추가했을 때 이 인터페이스가 자동으로 생성되었습니다. 인터페이스를 아직 추가하지 않은 경우 이 명령을 사용하면 포트 채널 인터페이스가 생성됩니다.

논리적 매개변수(예: 이름)를 구성하기 전에 하나 이상의 멤버 인터페이스를 포트 채널 인터페이스에 추가해야 합니다.

단계 **2** 채널 그룹에서 허용되는 활성 인터페이스의 최대 개수를 지정합니다.

lacp max-bundle *number*

예제:

```
ciscoasa(config-if)# lacp max-bundle 6
```

*number*는 1에서 16 사이입니다. 기본값은 16입니다. 스위치에서 16개의 액티브 인터페이스를 지원하지 않을 경우, 이 명령을 8 이하로 설정합니다.

단계 **3** 포트 채널 인터페이스를 활성 상태로 설정하는 데 필요한 활성 인터페이스의 최소 개수를 지정합니다.

port-channel min-bundle *number*

예제:

```
ciscoasa(config-if)# port-channel min-bundle 2
```

*number*는 1에서 16 사이입니다. 기본값은 1입니다. 채널 그룹의 액티브 인터페이스가 이 값의 범위에 속할 경우, 포트 채널 인터페이스가 종료되며 디바이스 수준 장애 조치가 일어납니다.

단계 **4** 로드 밸런싱 알고리즘을 구성합니다.

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

예제:

```
ciscoasa(config-if)# port-channel load-balance src-dst-mac
```

기본적으로 ASA에서는 패킷의 소스 및 대상 IP 주소(**src-dst-ip**)에 따라 인터페이스에서 패킷 로드 밸런싱을 수행합니다. 패킷이 분류되는 속성을 변경하려면 이 명령을 사용합니다. 예를 들어 동일한 소스와 목적지 IP 주소에 트래픽이 심하게 편중된 경우 EtherChannel의 인터페이스에 트래픽 할당이 불균형해질 수 있습니다. 다른 알고리즘으로 변경할 경우 트래픽이 보다 고르게 분산될 수 있습니다.

단계 **5** LACP 시스템 우선순위를 설정합니다.

lacp system-priority *number*

예제:

```
ciscoasa(config)# lacp system-priority 12345
```

*number*는 1에서 65535 사이입니다. 기본값은 32768입니다. 숫자가 높을수록 우선 순위는 낮아집니다. 이 명령은 ASA에서 전역으로 적용됩니다.

EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선 순위가 충돌할 경우, 시스템 우선 순위를 통해 어느 포트 우선 순위를 사용해야 할지 결정됩니다. EtherChannel 내의 인터페이스 우선 순위에 대한 자세한 내용은 **lacp port-priority** 명령을 참조하십시오.

단계 **6** (선택사항) 포트 채널 인터페이스에 대한 이더넷 속성을 설정하여 개별 인터페이스의 속성 설정을 재정의할 수 있습니다.

이더넷 명령에 대해서는 물리적 인터페이스 활성화 및 이더넷 파라미터 구성, 560 페이지를 참조하십시오. 이러한 매개변수는 채널 그룹의 모든 인터페이스와 일치해야 하므로, 이 방법을 사용하면 이러한 매개변수를 빠르게 설정할 수 있습니다.

관련 항목

부하 균형, 570 페이지
EtherChannel에 인터페이스 추가, 576 페이지

EtherChannel 및 이중 인터페이스 모니터링

다음 명령을 참조하십시오.

- **show interface**

  인터페이스 통계를 표시합니다.

- **show interface ip brief**

  인터페이스 IP 주소와 상태를 표시합니다.

- **show lacp**{[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

  EtherChannel의 경우 트래픽 통계, 시스템 식별자, 인접 세부 정보 같은 LACP 정보가 표시됩니다.

- **show port-channel** [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

  EtherChannel의 경우 EtherChannel 정보가 자세한 형식 및 한 줄짜리 요약 형식으로 표시됩니다. 이 명령은 포트 및 포트-채널 정보도 표시합니다.

- **show port-channel** *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]

  EtherChannel의 경우 정해진 매개변수에 선택된 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보가 표시됩니다.

EtherChannel 및 이중 인터페이스 예

다음 예에서는 세 가지 인터페이스를 EtherChannel의 일부로 구성합니다. 또한 시스템 우선 순위를 더 높은 우선 순위로 설정하고, EtherChannel에 8개 이상의 인터페이스가 할당된 경우 GigabitEthernet 0/2의 우선 순위를 다른 인터페이스보다 높게 설정합니다.

```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

EtherChannel 및 이중 인터페이스 내역

표 ***20: EtherChannel*** 및 이중 인터페이스 내역

기능 이름	릴리스	기능 정보
이중 인터페이스	8.0(2)	논리적 이중 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중 인터페이스와 함께 장애 조치를 구성할 수 있습니다. 최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.
EtherChannel 지원	8.4(1)	8개의 액티브 인터페이스마다 최대 48개의 802.3ad EtherChannel을 구성할 수 있습니다. 다음 명령을 도입했습니다. **channel-group**, **lacp port-priority**, **interface port-channel**, **lacp max-bundle**, **port-channel min-bundle**, **port-channel load-balance**, **lacp system-priority**, **clear lacp counters**, **show lacp**, **show port-channel** 참고 EtherChannel은 ASA 5505에서 지원되지 않습니다.

기능 이름	릴리스	기능 정보
EtherChannel에 16개의 액티브 링크 지원	9.2(1)	이제 EtherChannel에서 최대 16개의 액티브 링크를 구성할 수 있습니다. 이전에는 액티브 링크 8개와 스탠바이 링크 8개를 구성할 수 있었습니다. 스위치에서 16개의 액티브 링크를 지원하는지 확인하십시오(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000). 참고 이전 ASA 버전에서 업그레이드할 경우 호환성을 위해 액티브 인터페이스의 최대 수는 8개로 설정됩니다(**lacp max-bundle** 명령). 다음 명령을 수정했습니다. **lacp max-bundle** 및 **port-channel min-bundle**

14 장

VLAN 인터페이스

이 장에서는 VLAN 하위 인터페이스를 구성하는 방법에 대해 설명합니다.

참고 다중 상황 모드의 경우, 시스템 실행 영역에서 모든 작업을 완료합니다.상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

VLAN 인터페이스 정보

VLAN 하위 인터페이스를 사용하면 물리적, 이중 또는 EtherChannel 인터페이스를 다른 VLAN ID가 태그 처리된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 실제 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 실제 인터페이스 또는 ASA를 더 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다. 이 기능은 다중 상황 모드에서 특히 유용하며 각 상황에 고유한 인터페이스를 할당할 수 있습니다.

기본 VLAN뿐만 아니라 하나 이상의 보조 VLAN을 구성할 수 있습니다. ASA는 보조 VLAN에서 트래픽을 수신할 경우 트래픽을 기본 VLAN에 매핑합니다.

VLAN 인터페이스에 대한 라이센싱

모델	라이센스 요건
ASA 5506-X ASA 5506W-X ASA 5506H-X	Base 라이센스: 5 Security Plus 라이센스: 30
ASA 5508-X	Base 라이센스: 50
ASA 5512-X	Base 라이센스: 50 Security Plus 라이센스: 100
ASA 5515-X	Base 라이센스: 100
ASA 5516-X	Base 라이센스: 50
ASA 5525-X	Base 라이센스: 200
ASA 5545-X	Base 라이센스: 300
ASA 5555-X	Base 라이센스: 500
ASA 5585-X	Base 및 Security Plus 라이센스: 1024
Firepower 2100	Standard 라이선스: 1024
Firepower 4100의 ASA	Standard 라이선스: 1024
Firepower 9300의 ASA	Standard 라이선스: 1024
ISA 3000	Base 라이센스: 5 Security Plus License: 25
ASAv5 ASAv10	Standard 라이선스: 50
ASAv30	Standard 라이선스: 200
ASAv50	Standard 라이선스: 1024
ASASM	지원 안 함

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예:

```
interface gigabitethernet 0/0.100
  vlan 100
```

VLAN 인터페이스에 대한 지침 및 제한 사항

모델 지원

- ASASM — VLAN 하위 인터페이스는 ASASM에서 지원되지 않습니다. ASASM 인터페이스는 이미 스위치에서 할당된 VLAN 인터페이스입니다.

추가 지침

- 물리적 인터페이스의 태그 지정되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 지정되지 않은 패킷을 전달하기 때문입니다. 이러한 속성은 이중 인터페이스 쌍의 물리적 인터페이스 및 EtherChannel 링크에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적, 이중화 또는 EtherChannel 인터페이스를 활성화해야 하므로, **nameif** 명령을 제외하여 물리적, 이중화 또는 EtherChannel 인터페이스에서 트래픽을 전달하지 않도록 합니다. 물리적, 이중화 또는 EtherChannel 인터페이스에서 태깅되지 않은 패킷을 전달하는 것을 허용하려면 평소와 같이 **nameif** 명령을 구성합니다.
- (ASA 5585-X를 제외한 모든 모델) 관리 인터페이스에서 하위 인터페이스를 구성할 수 없습니다.
- 동일한 상위 인터페이스에 있는 모든 하위 인터페이스는 브리지 그룹 멤버 또는 라우팅 인터페이스 중 하나여야 하며 이를 혼합하고 일치시킬 수 없습니다.
- ASA에서는 DTP(Dynamic Trunking Protocol)를 지원하지 않으므로 조건 없이 트렁킹을 수행할 연결된 스위치 포트를 구성해야 합니다.
- ASA에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있어 ASA의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

VLAN 인터페이스의 기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형 및 상황 모드에 따라 다릅니다.

다중 상황 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 시스템 실행 영역에서도 인터페이스가 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.

단일 모드 또는 시스템 실행 영역에서 인터페이스의 기본 상태는 다음과 같습니다.

- 물리적 인터페이스 - 비활성화됨.
- VLAN 하위 인터페이스 - 활성화되어 있습니다. 그러나 트래픽이 하위 인터페이스를 통과하려면 물리적 인터페이스도 활성화되어야 합니다.

VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

물리적, 이중 또는 EtherChannel 인터페이스에 VLAN 하위 인터페이스를 추가합니다.

시작하기 전에

다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다.상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 새 하위 인터페이스를 지정합니다.

interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}.*subinterface*

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

redundant *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다.

port-channel *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다.

subinterface ID는 1 ~ 4294967293의 정수입니다.

단계 **2** 하위 인터페이스에 대한 VLAN을 지정합니다.

vlan *vlan_id* [**secondary** *vlan_range*]

예제**:**

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

*vlan_id*는 1 ~ 4094의 정수입니다. 일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로 스위치 설명서에서 자세한 내용을 확인하십시오.

보조 VLAN은 공백, 쉼표 및 대시(연속된 범위)로 구분할 수 있습니다. ASA가 보조 VLAN에서 트래픽을 수신할 경우 트래픽을 기본 VLAN에 매핑합니다.

동일한 VLAN은 여러 하위 인터페이스에 할당할 수 없습니다. 물리적 인터페이스에는 VLAN을 지정할 수 없습니다. 각 하위 인터페이스는 VLAN ID가 있어야 트래픽을 전달할 수 있습니다. VLAN ID를 변경하려는 경우 **no** 옵션을 사용하여 이전 VLAN ID를 제거할 필요가 없습니다. 다른 VLAN ID와 함께 **vlan** 명령을 입력하면 ASA에서 이전 ID를 변경합니다. 목록에서 보조 VLAN 중 일부를 제거하려면 **no** 명령을 사용하여 제거할 VLAN만 나열하면 됩니다. 나열된 VLAN만 선택적으로 제거할 수 있습니다. 예를 들어, 단일 VLAN을 범위에서 제거할 수는 없습니다.

예

다음 예에서는 보조 VLAN 집합을 VLAN 200에 매핑합니다.

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

다음 예에서는 보조 VLAN 503을 목록에서 제거합니다.

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
 no nameif
 no security-level
 no ip address
```

관련 항목

VLAN 인터페이스에 대한 라이센싱, 584 페이지

VLAN 인터페이스 모니터링

다음 명령을 참조하십시오.

- **show interface**

  인터페이스 통계를 표시합니다.

- **show interface ip brief**

  인터페이스 IP 주소와 상태를 표시합니다.

- **show vlan mapping**

인터페이스, 보조 VLAN 및 보존 VLAN이 매핑되는 기본 VLAN을 표시합니다.

VLAN 인터페이스의 예

다음 예에서는 단일 모드에서 하위 인터페이스의 매개변수를 구성합니다.

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

다음 예에는 VLAN 매핑이 Catalyst 6500에서 작동하는 방식이 나와 있습니다. PVLAN에 노드를 연결하는 방법에 대한 내용은 Catalyst 6500 구성 가이드를 참조하십시오.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
```

```
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

VLAN 인터페이스 내역

표 ***21: VLAN*** 인터페이스 내역

기능 이름	릴리스	기능 정보
VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base 라이센스의 VLAN을 0개에서 10개로 • ASA5510 Security Plus 라이센스의 VLAN을 10개에서 25개로 • ASA5520 VLAN을 25개에서 100개로 • ASA5540 VLAN을 100개에서 200개로
VLAN 증가	7.2(2)	ASA 5510(Base 라이센스는 10에서 50으로, Security Plus 라이센스는 25에서 100으로), ASA 5520(100에서 150으로), ASA 5550(200에서 250으로)의 VLAN 제한이 증가했습니다.
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
기본 VLAN에 대한 보조 VLAN 매핑 지원	9.5(2)	이제 하위 인터페이스에 하나 이상의 보조 VLAN을 구성할 수 있습니다. ASA가 보조 VLAN에서 트래픽을 수신할 경우 ASA는 트래픽을 기본 VLAN에 매핑합니다. 도입 또는 수정된 명령: **vlan secondary, show vlan mapping**

15 장

VXLAN 인터페이스

이 장에서는 VXLAN(확장 가능 가상 LAN) 인터페이스를 구성하는 방법을 알려 줍니다. VXLAN은 Layer 2 네트워크를 확장하기 위해 Layer 3 물리적 네트워크에서 Layer 2 가상 네트워크 역할을 합니다.

VXLAN 인터페이스 정보

VXLAN은 VLAN과 동일한 이더넷 Layer 2 네트워크 서비스를 제공하지만 확장성과 유연성이 우수합니다. VLAN에 비해 VXLAN은 다음과 같은 이점을 제공합니다.

- 데이터 센터 전체에서 다중 테넌시 세그먼트를 유연하게 배치합니다.
- 더 많은 Layer 2 세그먼트를 해결하기 위한 우수한 확장성: 최대 1600만 개의 VXLAN 세그먼트.

이 섹션에서는 VXLAN의 작동 방식을 설명합니다. 자세한 정보는 RFC 7348을 참조하십시오.

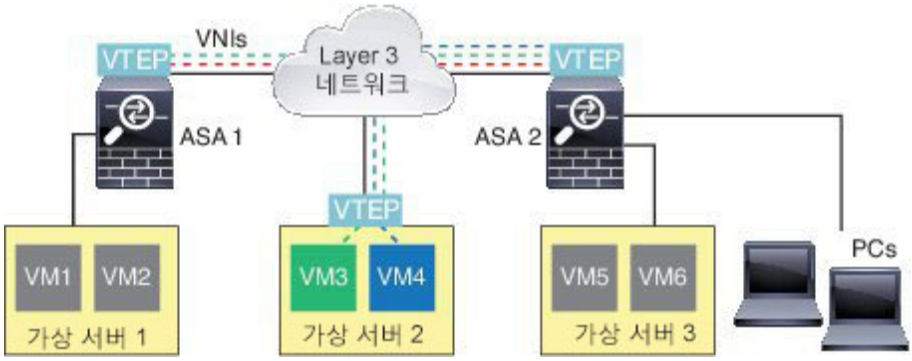
VXLAN 캡슐화

VXLAN은 Layer 3 네트워크에서의 Layer 2 오버레이 구성입니다. 또한 MAC-in-UDP(사용자 데이터그램 프로토콜의 MAC 주소) 캡슐화를 사용합니다. 원래의 Layer 2 프레임에는 VXLAN 헤더가 추가됩니다. 그런 다음 UDP-IP 패킷에 배치됩니다.

VXLAN 터널 엔드포인트

VXLAN 터널 엔드포인트(VTEP) 디바이스는 VXLAN 캡슐화 및 역캡슐화를 수행합니다. 각 VTEP에는 2개의 인터페이스 유형이 있습니다. VNI(VXLAN 네트워크 식별자) 인터페이스라고 하는 하나 이상의 가상 인터페이스에는 보안 정책이 적용되며 VTEP 소스 인터페이스라고 하는 일반 인터페이스는 VTEP 사이에서 VNI 인터페이스를 터널링합니다. VTEP 소스 인터페이스는 VTEP대 VTEP 통신을 위해 전송 IP 네트워크에 연결됩니다.

다음 그림에는 여러 사이트 사이에서 VNI 1, 2, 3 네트워크를 확장하여 Layer 3 네트워크 전체에서 VTEP 역할을 수행하는 2개의 ASA 및 가상 서버 2가 나와 있습니다. ASA에서는 VXLAN 및 VXLAN 이외 네트워크 간의 브리지 또는 게이트웨이 역할을 수행합니다.



VTEP 간의 기반 IP 네트워크는 VXLAN 오버레이와 상관이 없습니다. 캡슐화된 패킷은 소스 IP 주소로 시작 VTEP 및 대상 IP 주소로 종료 VTEP가 있는 외부 IP 주소 헤더에 기반하여 라우팅됩니다. 대상 IP 주소는 원격 VTEP가 알려지지 않은 경우 멀티캐스트 그룹일 수 있습니다. 대상 포트는 기본적으로 UDP 포트 4789입니다(사용자가 구성 가능).

VTEP 소스 인터페이스

VTEP 소스 인터페이스는 모든 VNI 인터페이스를 연결할 일반 ASA 인터페이스(물리적, 이중, EtherChannel 또는 VLAN)입니다. ASA/보안 상황별로 1개의 VTEP 소스 인터페이스를 구성할 수 있습니다.

VTEP 소스 인터페이스는 VXLAN 트래픽에 사용하도록 제한되지 않는 경우에도 VXLAN 트래픽에 모두 사용될 수 있습니다. 필요 시, 일반 트래픽에 이 인터페이스를 사용하고 해당 트래픽에 대한 인터페이스에 보안 정책을 적용할 수 있습니다. 단, VXLAN 트래픽의 경우 모든 보안 정책을 VNI 인터페이스에 적용해야 합니다. VTEP 인터페이스는 물리적 포트로만 사용됩니다.

투명한 방화벽 모드에서, VTEP 소스 인터페이스는 BVI의 일부가 아니며 관리 인터페이스가 처리되는 방식과 유사하게 이 인터페이스에 대해 IP 주소를 구성합니다.

VNI 인터페이스

VNI 인터페이스는 VLAN 인터페이스와 유사합니다. 이 인터페이스는 네트워크 트래픽을 태그 지정을 사용하여 지정된 물리적 인터페이스에서 분리되게 유지하는 가상 인터페이스입니다. 각 VNI 인터페이스에 보안 정책을 직접 적용하십시오.

모든 VNI 인터페이스는 동일한 VTEP 인터페이스와 연결되어 있습니다.

VXLAN 패킷 처리

VTEP 소스 인터페이스를 드나드는 트래픽은 VXLAN 처리, 특히 캡슐화 또는 역캡슐화 과정을 거칩니다.

캡슐화 처리에는 다음 작업이 포함됩니다.

- VTEP 소스 인터페이스는 VXLAN 헤더가 있는 내부 MAC 프레임을 캡슐화합니다.
- UDP 체크섬 필드가 0으로 설정됩니다.
- 외부 프레임 소스 IP가 VTEP 인터페이스 IP로 설정됩니다.
- 외부 프레임 대상 IP는 원격 VTEP IP 조회에 따라 결정됩니다.

역캡슐화: ASA에서는 다음과 같은 경우 VXLAN 패킷에 역캡슐화만 수행합니다.

- 대상 포트가 4789로 설정된 UDP 패킷인 경우(이 값은 사용자가 구성 가능함).
- 인그레스 인터페이스가 VTEP 소스 인터페이스입니다.
- 인그레스 인터페이스 IP 주소가 대상 IP 주소와 동일합니다.
- VXLAN 패킷 형식은 표준을 준수합니다.

피어 VTEP

ASA에서 피어 VTEP 뒤에 있는 디바이스에 패킷을 전송하는 경우 ASA에는 다음의 2가지 중요한 정보가 필요합니다.

- 원격 디바이스의 대상 MAC 주소
- 피어 VTEP의 대상 IP 주소

ASA에서는 다음의 2가지 방법으로 이 정보를 찾을 수 있습니다.

- 단일 피어 VTEP IP 주소를 ASA에서 정적으로 구성할 수 있습니다.

  수동으로 여러 피어를 정의할 수 없습니다.

  그런 다음 ASA에서는 엔드 노드 MAC 주소를 확인하기 위해 VTEP에 VXLAN 캡슐화 ARP 브로드캐스트를 전송합니다.

- 멀티캐스트 그룹은 각각의 VNI 인터페이스에서 구성될 수 있습니다(또는 VTEP에서 전체로 구성 가능).

  ASA에서는 VTEP 소스 인터페이스를 통해 IP 멀티캐스트 패킷 내에서 VXLAN 캡슐화 ARP 브로드캐스트 패킷을 전송합니다. 이 ARP 요청에 대한 응답을 통해 ASA에서는 원격 엔드 노드의 대상 MAC 주소와 함께 원격 VTEP IP 주소를 확인할 수 있습니다.

ASA는 VNI 인터페이스에 대한 원격 VTEP IP 주소로의 대상 MAC 주소 매핑을 유지합니다.

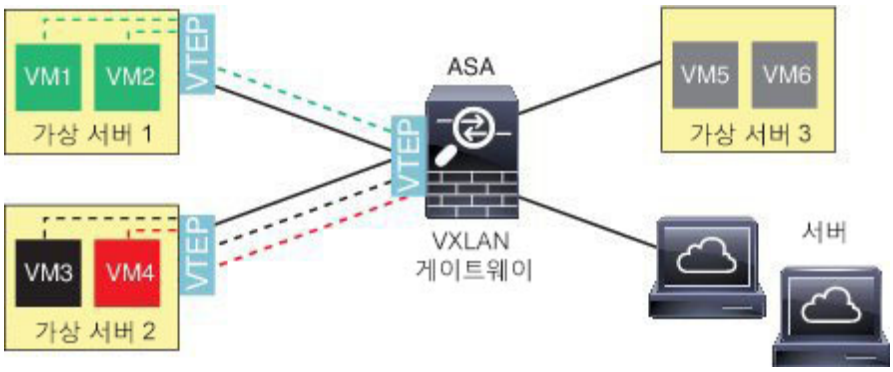
VXLAN 사용 사례

이 섹션에서는 ASA에서의 VXLAN 구현에 대한 사용 사례를 설명합니다.

VXLAN 브리지 또는 게이트웨이 개요

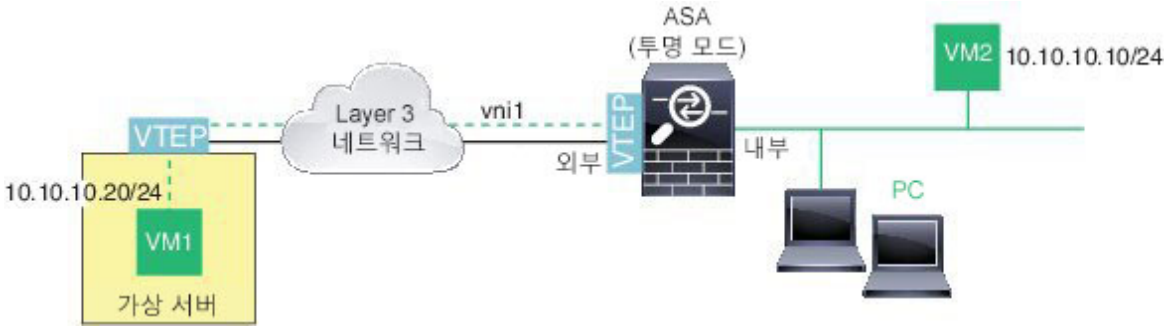
각 ASA VTEP는 VM, 서버, PC 및 VXLAN 오버레이 네트워크 등의 엔드 노드 사이에서 브리지 또는 게이트웨이 역할을 합니다. VTEP 소스 인터페이스에서 VXLAN 캡슐화를 통해 받은 수신 프레임의 경우 ASA에서는 VXLAN 헤더를 제거하여 이 헤더를 내부 이더넷 프레임의 대상 MAC 주소에 기반하는 VXLAN 이외 네트워크에 연결되어 있는 물리적 인터페이스에 전달합니다.

ASA에서는 항상 VXLAN 패킷을 처리하며 2개의 다른 VTEP 사이에서 원래 상태로 있는 VXLAN 패킷은 전달하지 않습니다.



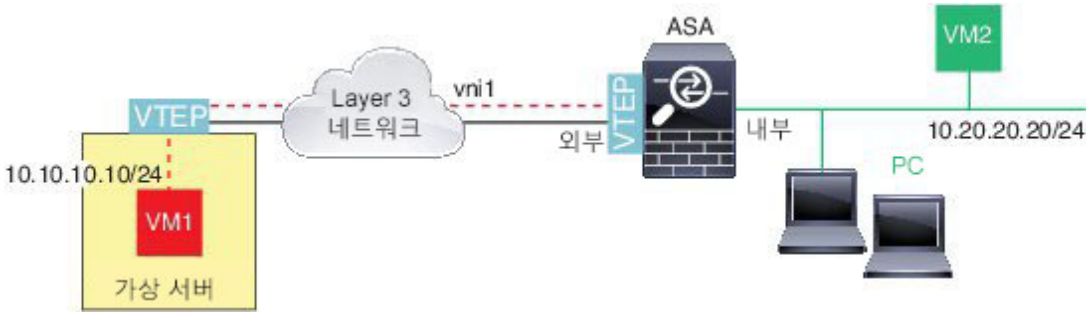
VXLAN 브리지

투명한 방화벽 모드 또는 라우팅 모드(선택 사항)에서 브리지 그룹을 사용할 경우, ASA에서는 동일한 네트워크에 있는 원격 VXLAN 세그먼트와 로컬 세그먼트 사이에서 VXLAN 브리지 역할을 수행할 수 있습니다. 이 경우, 브리지 그룹의 한 멤버는 일반 인터페이스이며 이때 다른 멤버는 VNI 인터페이스입니다.



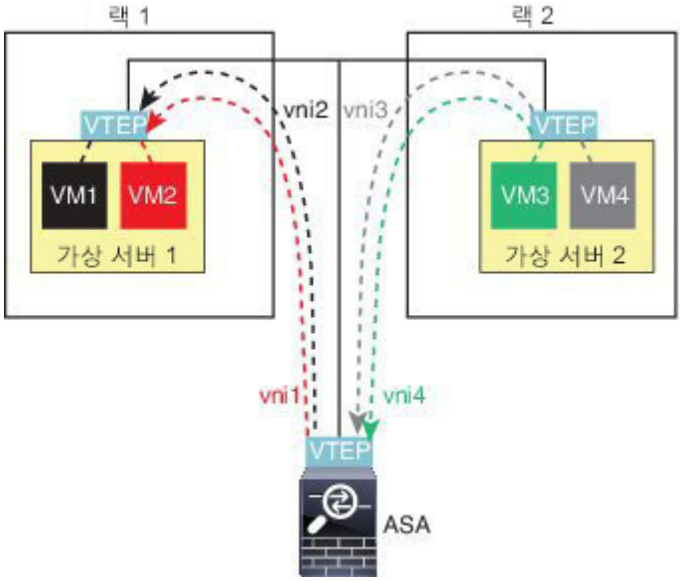
VXLAN 게이트웨이(라우팅 모드)

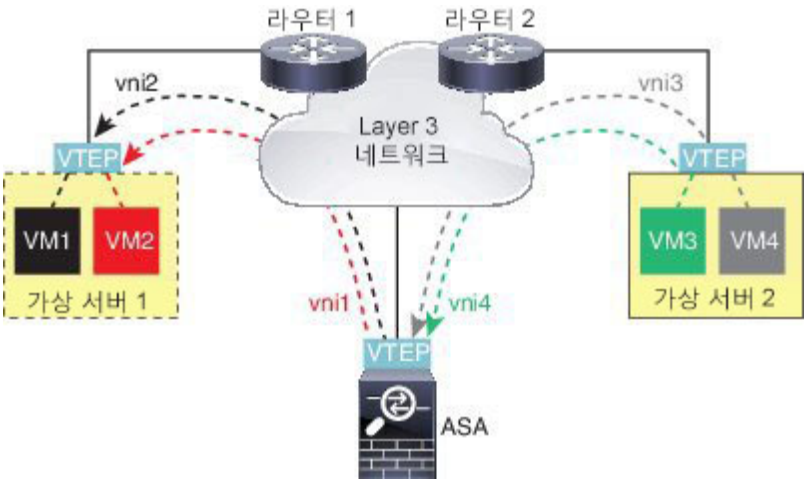
ASA에서는 다른 네트워크에 있는 디바이스를 연결하여 VXLAN과 VXLAN 이외 도메인 사이에서 라우터 역할을 수행할 수 있습니다.



VXLAN 도메인 사이의 라우터

VXLAN 확장 Layer 2 도메인에서 VM은 ASA가 동일한 랙에 있지 않은 경우 또는 ASA가 Layer 3 네트워크 상에서 멀리 있는 경우에도 게이트웨이로 ASA를 가리킬 수 있습니다.





이 시나리오에 대한 다음 주의사항을 참조하십시오.

1. VM3~VM1 패킷의 경우, ASA가 기본 게이트웨이이므로 대상 MAC 주소는 ASA MAC 주소입니다.
2. 가상 서버 2의 VTEP 소스 인터페이스에서 VM3로부터 패킷을 수신하고 VNI 3의 VXLAN 태그로 패킷을 캡슐화한 다음 ASA에 전송합니다.
3. ASA가 이 패킷을 수신하면 내부 프레임을 얻기 위해 패킷을 역캡슐화합니다.
4. ASA에서는 경로 조회를 위해 내부 프레임을 사용한 다음 해당 대상이 VNI 2에 있는지 확인합니다. VM1에 대한 매핑이 없는 경우, ASA에서는 VNI 2에서 멀티캐스트 그룹 IP에 대해 캡슐화 ARP 브로드캐스트를 전송합니다.

참고 이 시나리오에서 ASA에서는 여러 VTEP 피어를 지니므로 동적 VTEP 피어 검색을 사용해야 합니다.

5. ASA에서는 VNI 2에 대한 VXLAN 태그를 사용하여 패킷을 다시 캡슐화한 다음 이 패킷을 가상 서버 1에 전송합니다. 캡슐화하기 전에 ASA에서는 내부 프레임 대상 MAC 주소를 VM1의 MAC로 변경합니다(ASA에서 VM1 MAC 주소를 파악하는 데 멀티캐스트 캡슐화 ARP가 필요할 수 있음).
6. 가상 서버 1에서 VXLAN 패킷을 수신하는 경우 패킷을 역캡슐화하고 내부 프레임을 VM1에 제공합니다.

VXLAN 인터페이스에 대한 지침

IPv6

- VNI 인터페이스는 IPv6 트래픽을 지원하지만 VTEP 소스 인터페이스 IP 주소는 IPv4만 지원합니다.

- IPv6 OSPF 인터페이스 설정은 지원되지 않습니다.

클러스터링

ASA 클러스터링은 개별 인터페이스 모드에서 VXLAN을 지원하지 않습니다. 스팬 EtherChannel 모드만 VXLAN을 지원합니다.

라우팅

- 고정 라우팅 또는 정책 기반 라우팅만 VNI 인터페이스에서 지원되며 동적 라우팅 프로토콜은 지원되지 않습니다.

MTU

소스 인터페이스 MTU가 1554바이트보다 작은 경우, ASA에서는 자동으로 MTU를 1554바이트로 늘립니다. 이 경우 전체 이더넷 데이터그램이 캡슐화되고 있으므로 새 패킷이 더 크며, 더 큰 MTU가 필요합니다. 다른 디바이스에서 사용된 MTU가 더 큰 경우, 소스 인터페이스 MTU를 네트워크 MTU + 54바이트로 설정해야 합니다. 이 MTU에서는 점보 프레임 예약을 활성화해야 합니다. 점보 프레임 지원 활성화, 563 페이지의 내용을 참조하십시오.

VXLAN 인터페이스의 기본 설정

VNI 인터페이스는 기본적으로 활성화되어 있습니다.

VXLAN 인터페이스 구성

VXLAN을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** VTEP 소스 인터페이스 구성, 597 페이지.
단계 **2** VNI 인터페이스 구성, 599 페이지
단계 **3** (선택사항) VXLAN UDP 포트 변경, 601 페이지.

VTEP 소스 인터페이스 구성

ASA 또는 보안 상황별로 1개의 VTEP 소스 인터페이스를 구성할 수 있습니다. VTEP는 NVE(네트워크 가상화 엔드포인트)로 정의되며 VXLAN VTEP는 현재 지원되는 유일한 NVE입니다.

시작하기 전에

다중 상황 모드에서는 상황 실행 영역에서 이 섹션의 작업을 수행합니다. 구성할 상황으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

프로시저

단계 **1** (투명 모드) 소스 인터페이스가 NVE 전용임을 지정합니다.

interface *id*

nve-only

예제:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

이 설정을 사용하여 인터페이스의 IP 주소를 구성할 수 있습니다. 이 명령은 라우팅 모드에서 선택사항이며 이때 이 설정에서 트래픽을 이 인터페이스의 VXLAN과 일반 관리 트래픽으로 제한합니다.

단계 **2** 소스 인터페이스 이름 및 IPv4 주소를 구성합니다.

예제:

(라우팅 모드)

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

예제:

(투명 모드)

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

단계 **3** NVE 인스턴스를 지정합니다.

nve 1

ID 1을 사용하여 하나의 NVE 인스턴스만 지정할 수 있습니다.

참고 **encapsulation vxlan** 명령은 NVE 인스턴스에 대해 기본값으로 추가되므로 명시적으로 추가할 필요가 없습니다.

단계 **4** 사용자가 2단계에서 구성한 소스 인터페이스 이름을 지정합니다.

source-interface *interface-name*

예제:

```
ciscoasa(cfg-nve)# source-interface outside
```

참고 소스 인터페이스 MTU가 1554바이트보다 작은 경우, ASA에서는 자동으로 MTU를 1554바이트로 늘립니다.

단계 **5** (다중 상황 모드, 단일 모드의 경우 선택사항) 피어 VTEP IP 주소를 직접 지정합니다.

peer ip *ip_address*

예제**:**

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

피어 IP 주소를 지정한 경우, 멀티캐스트 그룹 검색을 사용할 수 없습니다. 멀티캐스트가 다중 상황 모드에서 지원되지 않으므로 수동 구성이 고유한 옵션입니다. VTEP에 대해 하나의 피어만 지정할 수 있습니다.

단계 **6** (선택사항, 단일 모드 전용) 모든 연결된 VNI에 대해 기본 멀티캐스트 그룹을 지정합니다.

default-mcast-group *mcast_ip*

예제**:**

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

VNI 인터페이스별로 멀티캐스트 그룹을 구성하지 않은 경우, 이 그룹이 사용됩니다. VNI 인터페이스 수준에서 그룹을 구성하는 경우 이 그룹은 다음 설정을 재정의합니다.

VNI 인터페이스 구성

VNI 인터페이스를 추가하고 VTEP 소스 인터페이스에 연결하며 기본 인터페이스 파라미터를 구성합니다.

프로시저

단계 **1** VNI 인터페이스를 만듭니다.

interface vni *vni_num*

예제**:**

```
ciscoasa(config)# interface vni 1
```

1에서 10000 사이에서 ID를 설정합니다. 이 ID는 유일한 내부 인터페이스 식별자입니다.

단계 **2** VXLAN 세그먼트 ID를 지정합니다.

segment-id *id*

예제:

```
ciscoasa(config-if)# segment-id 1000
```

1에서 16777215 사이에서 ID를 설정합니다. 세그먼트 ID는 VXLAN 태그 지정에 사용됩니다.

단계 **3** (투명 모드의 경우 필수) 이 인터페이스에 연결할 브리지 그룹을 지정합니다.

bridge-group *number*

예제:

```
ciscoasa(config-if)# bridge-group 1
```

BVI 인터페이스를 구성하고 이 브리지 그룹에 일반 인터페이스를 연결하려면 브리지 그룹 인터페이스 구성, 618 페이지를 참조하십시오.

단계 **4** VTEP 소스 인터페이스와 이 인터페이스를 연결합니다.

vtep-nve 1

단계 **5** 인터페이스 이름을 지정합니다.

nameif *vni_interface_name*

예제:

```
ciscoasa(config-if)# nameif vxlan1000
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다. **no** 형식은 입력하지 마십시오. 그러면 해당 이름을 참조하는 모든 명령이 삭제됩니다.

단계 **6** (라우팅 모드) IPv4 및/또는 IPv6 주소를 할당합니다.

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address*]}

예제:

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

단계 **7** 보안 레벨을 설정합니다.

security-level 레벨

예제:

```
ciscoasa(config-if)# security-level 50
```

*number*는 0(최저) ~ 100(최고) 범위의 정수입니다.

단계 **8** (단일 모드) 멀티캐스트 그룹 주소를 설정합니다.

mcast-group *multicast_ip*

예제:

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

VNI 인터페이스에 대해 멀티캐스트 그룹을 설정하지 않은 경우, VTEP 소스 인터페이스 구성의 기본 그룹이 사용됩니다(사용 가능한 경우). VTEP 소스 인터페이스에 대해 VTEP 피어 IP를 직접 설정하는 경우, VNI 인터페이스에 대해 멀티캐스트 그룹을 지정할 수 없습니다. 멀티캐스트는 다중 상황 모드에서 지원되지 않습니다.

(선택사항) VXLAN UDP 포트 변경

기본적으로, VTEP 소스 인터페이스는 UDP 포트 4789에 대해 VXLAN 트래픽을 승인합니다. 네트워크에서 비표준 포트를 사용하는 경우 변경할 수 있습니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 공간에서 이 작업을 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

VXLAN UDP 포트를 설정합니다.

vxlan 포트 번호

예제:

```
ciscoasa(config)# vxlan port 5678
```

VXLAN 인터페이스 모니터링

VTEP 및 VNI 인터페이스를 모니터링하려면 다음 명령을 참조하십시오.

- **show nve** [*id*] [**summary**]

  이 명령은 NVE 인터페이스의 파라미터, 상태 및 통계, 캐리어 인터페이스(소스 인터페이스)의 상태, 캐리어 인터페이스의 IP 주소를 보여 줍니다. 이 NVE를 VXLAN VTEP 및 이 NVE 인터페이스와 연결된 피어 VTEP IP 주소로 사용하는 VNI입니다. **summary** 옵션을 사용할 경우 이 명

령은 NVE 인터페이스의 상태, NVE 인터페이스 뒤에 있는 VNI 개수 및 발견된 VTEP 개수만 보여 줍니다.

show nve 1 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

show nve 1 summary 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

- **show interface vni** *id* [**summary**]

  이 명령은 VNI 인터페이스의 파라미터, 상태 및 통계, 브리지 인터페이스 상태(구성된 경우) 및 연결된 NVE 인터페이스의 상태를 보여 줍니다. **summary** 옵션은 VNI 인터페이스 파라미터만 표시합니다.

  show interface vni 1 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
```

```
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

show interface vni 1 summary 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

- **show vni vlan-mapping**

  이 명령은 VNI 세그먼트 ID 간의 매핑 및 VLAN 인터페이스 또는 물리적 인터페이스를 보여 줍니다. 이 명령은 라우팅 모드에서, 투명한 방화벽 모드에서만 사용 가능합니다. VXLAN 및 VLAN 간의 매핑에는 너무 많은 값이 포함되어 있어 표시할 수 없습니다.

  show vni vlan-mapping 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
 'g112', vlan 4
```

- **show arp vtep-mapping**

  이 명령은 원격 세그먼트 도메인 및 원격 VTEP IP 주소에 있는 IP 주소에 대한 VNI 인터페이스에서 캐시된 MAC 주소를 표시합니다.

  show arp vtep-mapping 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

- **show mac-address-table vtep-mapping**

  이 명령을 사용하면 원격 VTEP IP 주소의 VNI 인터페이스에 있는 Layer 2 전달 테이블(MAC 주소 테이블)이 표시됩니다.

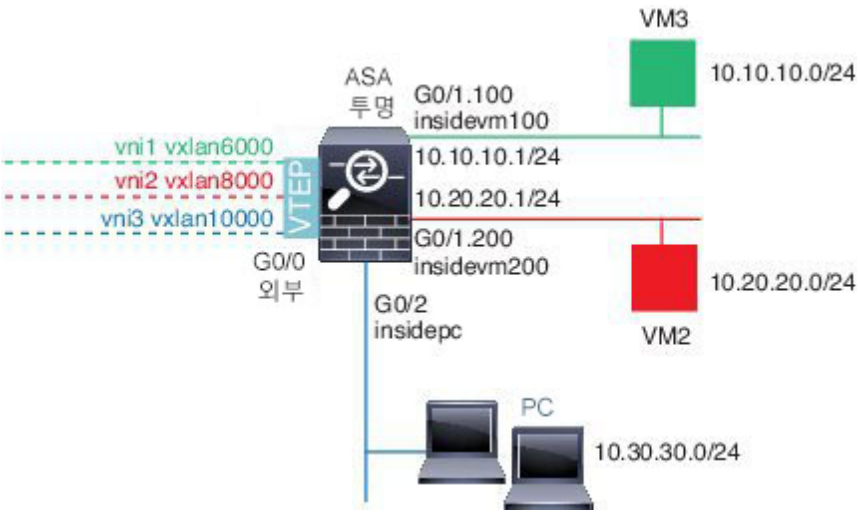
  show mac-address-table vtep-mapping 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type     Age(min)   bridge-group    VTEP
-------------------------------------------------------------------------------------------
vni-outside               00ff.9200.0000      dynamic      5         1        10.9.1.3
vni-inside                 0041.9f00.0000      dynamic      5         1      10.9.1.3
```

VXLAN 인터페이스 예

VXLAN에 대한 다음의 구성 예를 참조하십시오.

투명 VXLAN 게이트웨이 예



이 예의 다음 설명을 참조하십시오.

- GigabitEthernet 0/0의 외부 인터페이스는 VTEP 소스 인터페이스로 사용되며, Layer 3 네트워크에 연결됩니다.
- GigabitEthernet 0/1.100의 insidevm100 VLAN 하위 인터페이스는 VM3가 있는 10.10.10.0/24 네트워크에 연결됩니다. VM3가 VM1과 통신하는 경우(표시되지 않고 모두 10.10.10.0/24 IP 주소를 지님), ASA에서는 VXLAN 태그 6000을 사용합니다.
- GigabitEthernet 0/1.200의 insidevm200 VLAN 하위 인터페이스는 VM2가 있는 10.20.20.0/24 네트워크에 연결됩니다. VM2가 VM4와 통신하는 경우(표시되지 않고 모두 10.20.20.0/24 IP 주소를 지님), ASA에서는 VXLAN 태그 8000을 사용합니다.
- GigabitEthernet 0/2의 insidepc 인터페이스는 몇 대의 PC가 있는 10.30.30.0/24 네트워크에 연결됩니다. 이러한 PC가 동일한 네트워크에 속하는(모두 10.30.30.0/24 IP 주소를 지님) 원격 VTEP 뒤에서 VM/PC(표시되지 않음)와 통신하는 경우 ASA에서는 VXLAN 태그 10000을 사용합니다.

ASA 컨피그레이션

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
```

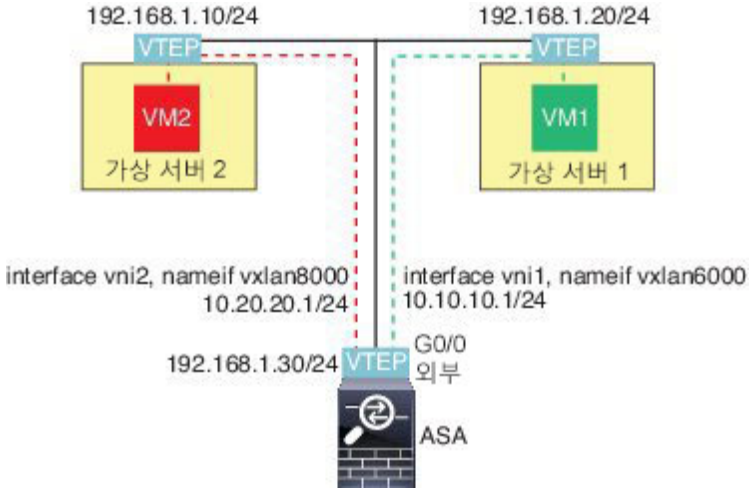
```
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

참고

- VNI 인터페이스 vni1 및 vni2의 경우, 내부 VLAN 태그가 캡슐화 동안 제거됩니다.
- VNI 인터페이스 vni2 및 vni3는 멀티캐스트를 통해 캡슐화된 ARP에 대해 동일한 멀티캐스트 IP 주소를 공유합니다. 이러한 공유는 허용됩니다.

- ASA에서는 상위 BVI 및 브리지 그룹 구성에 기반하여 VXLAN 이외 지원 인터페이스에 VXLAN 트래픽을 브리징합니다. 확장된 Layer 2 네트워크 세그먼트 각각(10.10.10.0/24, 10.20.20.0/24 및 10.30.30.0/24)에 대해 ASA에서는 브리지 역할을 합니다.
- 또한 브리지 그룹에서 하나 이상의 VNI 또는 하나 이상의 일반 인터페이스(VLAN 또는 물리적 인터페이스)가 허용됩니다. VLAN ID(또는 물리적 인터페이스)에 대한 VXLAN 세그먼트 ID 간의 전달 또는 연결은 대상 MAC 주소와 어떠한 인터페이스가 대상에 연결되는지에 따라 결정됩니다.
- VTEP 소스 인터페이스는 인터페이스 구성에서 **nve-only**로 표시된 투명 방화벽 모드에서 Layer 3 인터페이스입니다. VTEP 소스 인터페이스는 BVI 인터페이스 또는 관리 인터페이스가 아니지만 IP 주소를 가지고 있으며 라우팅 테이블을 사용합니다.

VXLAN 라우팅 예



이 예의 다음 설명을 참조하십시오.

- VM1(10.10.10.10)은 가상 서버 1에서 호스팅되고 VM2(10.20.20.20)는 가상 서버 2에서 호스팅됩니다.
- VM1의 기본 게이트웨이는 ASA이며, 이는 가상 서버 1과 동일한 포드에 있지 않지만 VM1에서는 이를 인식하지 않습니다. VM1은 기본 게이트웨이 IP 주소가 10.10.10.1이라는 사실만 알고 있습니다. VM2는 기본 게이트웨이 IP 주소가 10.20.20.1이라는 사실만 알고 있습니다.
- 가상 서버 1 및 2의 VTEP 지원 하이퍼바이저는 동일한 서브넷 또는 Layer 3 네트워크(표시되지 않음, 이 경우 ASA 및 가상 서버의 업링크는 다른 네트워크 주소를 지님)를 통해 ASA와 통신할 수 있습니다.
- VM1 패킷은 하이퍼바이저의 VTEP로 캡슐화되고 VXLAN 터널링을 통해 기본 게이트웨이로 전송됩니다.

- VM1이 VM2에 패킷을 전송할 때, 패킷은 이 관점에서 기본 게이트웨이 10.10.10.1을 통해 전송됩니다. 가상 서버1은 10.10.10.1이 로컬이 아닌 점을 알고 있으므로 VTEP에서는 VXLAN을 통해 패킷을 캡슐화하고 ASA의 VTEP에 전송합니다.
- ASA에서 이 패킷은 역캡슐화됩니다. VXLAN 세그먼트 ID는 역캡슐화 동안 확인됩니다. 그런 다음, ASA에서는 VXLAN 세그먼트 ID에 기반하여 해당 VNI 해당 인터페이스(vni1)에 내부 프레임을 다시 삽입합니다. ASA에서는 이후에 경로 조회를 수행하고 다른 VNI 인터페이스인 vni2를 통해 내부 패킷을 전송합니다. vni2를 통해 모든 이그레스 패킷이 VXLAN 세그먼트 8000으로 캡슐화되고 VTEP를 통해 외부로 전송됩니다.
- 최종적으로 이 캡슐화된 패킷은 패킷을 역캡슐화하고 VM2에 전달하는 가상 서버 2의 VTEP가 수신합니다.

ASA 구성

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN 인터페이스 내역

표 ***22: VXLAN*** 인터페이스 내역

기능 이름	릴리스	기능 정보
VXLAN 지원	9.4(1)	VTEP(VXLAN 터널 엔드포인트) 지원을 비롯해 VXLAN 지원이 추가되었습니다. ASA 또는 보안 상황별로 1개의 VTEP 소스 인터페이스를 정의할 수 있습니다. 도입된 명령: **debug vxlan**, **default-mcast-group**, **encapsulation vxlan**, **inspect vxlan**, **interface vni**, **mcast-group**, **nve**, **nve-only**, **peer ip**, **segment-id**, **show arp vtep-mapping**, **show interface vni**, **show mac-address-table vtep-mapping**, **show nve**, **show vni vlan-mapping**, **source-interface**, **vtep-nve**, **vxlan port**

16 장

라우팅 및 투명 모드 인터페이스

이 장에는 라우팅 또는 투명 방화벽 모드에서 모든 모델의 인터페이스 구성을 완료하는 작업이 포함되어 있습니다.

참고 다중 상황 모드에서는 상황 실행 영역에서 이 섹션의 작업을 수행합니다. 구성할 상황으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

라우팅 및 투명 모드 인터페이스 정보

ASA에서는 라우팅과 브리지라는 두 가지 유형의 인터페이스를 지원합니다.

각 Layer 3 라우팅 인터페이스에는 고유한 서브넷의 IP 주소가 필요합니다.

브리지 인터페이스는 브리지 그룹에 속하며 모든 인터페이스는 동일한 네트워크에 있습니다. 브리지 그룹은 브리지 네트워크에 IP 주소가 있는 BVI(브리지 가상 인터페이스)로 표시됩니다. 라우팅 모드에서는 라우팅 인터페이스와 브리지 인터페이스를 둘 다 지원하며 라우팅 인터페이스와 BVI 간에 라우팅을 수행할 수 있습니다. 투명 방화벽 모드에서는 브리지 그룹과 BVI 인터페이스만 지원합니다.

보안 수준

각 인터페이스에는 브리지 그룹 멤버 인터페이스를 포함하여 0(가장 낮음)~100(가장 높음) 범위의 보안 수준이 있어야 합니다. 예를 들어 내부 호스트 네트워크와 같이 가장 안전한 네트워크는 레벨 100으로 지정해야 합니다. 반면에 인터넷에 연결된 외부 네트워크는 레벨 0이 될 수 있습니다. DMZ와 같은 다른 네트워크는 그 사이의 값이 될 수 있습니다. 인터페이스를 동일한 보안 레벨에 지정할 수 있습니다.

보안 수준을 BVI에 할당하는지 여부는 방화벽 모드에 따라 달라집니다. 투명 모드에서 BVI 인터페이스는 인터페이스 간의 라우팅에 참여하지 않기 때문에 이 인터페이스에는 보안 수준이 없습니다. 라우팅 모드에서 BVI와 다른 인터페이스 간에 라우팅하도록 선택하는 경우 BVI 인터페이스에는 보안 수준이 있습니다. 라우팅 모드에서 브리지 그룹 멤버 인터페이스의 보안 수준은 브리지 그룹 내의 통신에만 적용됩니다. 마찬가지로, BVI 보안 수준은 BVI/Layer 3 인터페이스 간의 통신에만 적용됩니다.

레벨은 다음 동작을 제어합니다.

- 네트워크 액세스 - 기본적으로 상위 보안 인터페이스에서 하위 보안 인터페이스(아웃바운드)로의 액세스는 암시적으로 허용됩니다. 상위 보안 인터페이스의 호스트에서 하위 보안 인터페이스의 모든 호스트에 액세스할 수 있습니다. 인터페이스에 ACL을 적용하여 액세스를 제한할 수 있습니다.

  동일한 보안 인터페이스에 대한 통신을 활성화할 경우, 해당 인터페이스에서 보안 수준이 같거나 더 낮은 다른 인터페이스에 액세스하는 것이 암시적으로 허용됩니다.

- 검사 엔진—일부 애플리케이션 검사 엔진은 보안 레벨에 좌우됩니다. 동일한 보안 인터페이스의 경우 한쪽 방향의 트래픽에 검사 엔진이 적용됩니다.
  - NetBIOS 검사 엔진 - 아웃바운드 연결에만 적용됩니다.
  - SQL*Net 검사 엔진 — 어떤 호스트 쌍 간에 SQL*Net(이전의 OraServ) 포트에 대한 제어 연결이 있을 경우 인바운드 데이터 연결만 ASA를 통해 허용됩니다.

이중 **IP** 스택**(IPv4** 및 **IPv6)**

ASA에서는 인터페이스에서 IPv6 및 IPv4 주소를 모두 지원합니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다.

31비트 서브넷 마스크

라우팅 인터페이스의 경우, 지점 간 연결을 위해 31비트 서브넷에서 IP 주소를 구성할 수 있습니다. 31비트 서브넷 주소는 주소를 2개만 포함합니다. 일반적으로 서브넷의 첫 번째 주소 및 마지막 주소는 네트워크 및 브로드캐스트용으로 예약되어 있으므로 2개의 주소 서브넷은 사용할 수 없습니다. 그러나 지점 간 연결이 있으며 네트워크 또는 브로드캐스트 주소가 필요하지 않은 경우, 31비트 서브넷은 IPv4에서 주소를 보존하는 유용한 방법입니다. 예를 들어, 2개의 ASA 간의 장애 조치 링크에는 주소가 2개만 필요합니다. 링크의 한 쪽 끝에서 전송되는 모든 패킷은 항상 다른 쪽에서 수신되며 브

로드캐스팅이 필요하지 않습니다. SNMP 또는 Syslog를 실행하는 직접 연결된 관리 스테이션을 사용할 수도 있습니다.

31비트 서브넷 및 클러스터링

관리 인터페이스 및 클러스터 제어 링크를 제외하고 Spanned 클러스터링 모드에서 31비트 서브넷 마스크를 사용할 수 있습니다.

모든 인터페이스의 개별 클러스터링 모드에서 31비트 서브넷 마스크를 사용할 수는 없습니다.

31비트 서브넷 및 장애 조치

장애 조치를 위해 ASA 인터페이스 IP 주소에 대해 31비트 서브넷을 사용하는 경우, 주소가 충분하지 않으므로 인터페이스에 대해 스탠바이 IP 주소를 구성할 수 없습니다. 일반적으로, 스탠바이 인터페이스 상태를 확인하기 위해 액티브 유닛에서 인터페이스 테스트를 수행할 수 있도록 장애 조치를 위한 인터페이스에는 스탠바이 IP 주소가 있어야 합니다. 스탠바이 IP 주소가 없으면 ASA에서는 모든 네트워크 테스트를 수행할 수 없으며 링크 상태만 추적할 수 있습니다.

포인트 투 포인트 연결인 장애 조치 및 별도의 상태 링크(선택 사항)에서 31비트 서브넷도 사용할 수 있습니다.

31비트 서브넷 및 관리

직접 연결된 관리 스테이션을 사용하는 경우 ASA의 SSH 또는 HTTP에 대해 또는 관리 스테이션의 SNMP 또는 Syslog에 대해 포인트 투 포인트 연결을 사용할 수 있습니다.

31비트 서브넷의 지원되지 않는 기능

다음 기능은 31비트 서브넷을 지원하지 않습니다.

- 브리지 그룹에 대한 BVI 인터페이스 — 브리지 그룹에는 최소 3개의 호스트 주소가 필요합니다. 즉, 두 개의 브리지 그룹 멤버 인터페이스에 연결된 BVI 및 2개의 호스트가 필요합니다. /29 서브넷 또는 더 작은 서브넷을 사용해야 합니다.
- 멀티캐스트 라우팅

라우팅 및 투명 모드 인터페이스에 대한 지침 및 요구 사항

상황 모드

- 다중 상황 모드에서는 시스템 컨피그레이션에서 다중 상황 구성, 231 페이지에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 컨피그레이션할 수 있습니다.
- PPPoE는 다중 상황 모드에서 지원되지 않습니다.
- 다중 상황, 투명 모드의 경우 각 상황에서는 다른 인터페이스를 사용해야 하며 상황 간에 인터페이스를 공유할 수 없습니다.

- 다중 상황, 투명 모드의 경우 일반적으로 상황마다 다른 서브넷을 사용합니다. 겹치는 서브넷을 사용할 수도 있으나, 네트워크 토폴로지상 라우터 및 NAT 컨피그레이션에서 라우팅과 관련하여 이를 허용해야 합니다.
- DHCPv6 및 접두사 위임 옵션은 다중 상황 모드에서 지원되지 않습니다.
- 라우팅 방화벽 모드에서 브리지 그룹 인터페이스는 다중 상황 모드에서 지원되지 않습니다.

장애 조치

- 이 장의 절차를 사용하여 장애 조치 링크를 구성해서는 안 됩니다. 자세한 내용은 장애 조치 장을 참조하십시오.
- 장애 조치를 사용하는 경우 데이터 인터페이스에 대해 IP 주소 및 스탠바이 주소를 수동으로 설정해야 하며, DHCP 및 PPPoE는 지원되지 않습니다.

IPv6

- 모든 인터페이스에서 IPv6가 지원됩니다.
- 투명 모드에서 IPv6 주소만 수동으로 구성할 수 있습니다.
- ASA는 IPv6 애니캐스트 주소를 지원하지 않습니다.
- DHCPv6 및 접두사 위임 옵션은 다중 상황 모드, 투명 모드 또는 클러스터링에서 지원되지 않습니다.

모델 지원

- PPPoE 및 DHCP는 ASASM에서 지원되지 않습니다.
- ASAv50의 경우, 브리지 그룹이 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.

ASASM에 대한 VLAN ID

어떤 VLAN ID도 구성에 추가할 수 있으나, 스위치에 의해 ASA에 할당된 VLAN만 트래픽을 전달할 수 있습니다. ASA에 할당된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다.

아직 스위치에 의해 ASA에 할당되지 않은 VLAN을 위해 인터페이스를 추가할 경우 해당 인터페이스는 중지 상태가 됩니다. VLAN을 ASA에 할당하면 인터페이스는 작동 상태로 바뀝니다. 인터페이스 상태에 대한 자세한 내용은 **show interface** 명령을 참조하십시오.

투명 모드 및 브리지 그룹 지침

- 브리지 그룹당 64개의 인터페이스가 있는 최대 250개의 브리지 그룹을 생성할 수 있습니다.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.

- ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.
- IPv4에서는 관리 트래픽과 ASA를 거칠 트래픽 모두 브리지 그룹마다 BVI용 IP 주소가 필요합니다. IPv6 주소는 지원되지만 BVI에는 필요하지 않습니다.
- IPv6 주소만 수동으로 구성할 수 있습니다.
- BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다.
- 관리 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 투명 모드에서는 1개 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 투명 모드에서는 BVI IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 ASA의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 투명 모드에서는 관리 트래픽의 반환 경로를 제공하는 데 필요한 기본 경로가 하나의 브리지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브리지 그룹의 인터페이스 및 브리지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브리지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 일반 고정 경로를 지정해야 합니다.
- 투명 모드에서 PPPoE는 관리 인터페이스에 대해 지원되지 않습니다.
- 라우팅 모드에서 브리지 그룹 및 기타 라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다.
- 라우팅 모드에서 EtherChannel 및 VNI 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 브리지 그룹 멤버를 사용할 때 ASA를 통과하는 것이 허용되지 않습니다. BFD를 실행하는 ASA의 양쪽 측면에 두 개의 네이버가 있는 경우, ASA는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

기본 보안 레벨

기본 보안 레벨은 0입니다. 인터페이스의 이름을 “inside”로 지정한 다음, 보안 수준을 명시적으로 설정하지 않으면 ASA에서 보안 수준을 100으로 설정합니다.

참고 인터페이스의 보안 레벨을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

라우팅 모드 인터페이스 구성

라우팅 모드 인터페이스를 구성하려면 다음 단계를 수행하십시오.

일반 라우팅 모드 인터페이스 파라미터 구성

이 절차에서는 이름, 보안 수준, IPv4 주소 및 기타 옵션을 설정하는 방법에 대해 설명합니다.

시작하기 전에

다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context***name* 명령을 입력합니다.

프로시저

단계 **1** 인터페이스 컨피그레이션 모드를 시작합니다.

interface *id*

예제**:**

```
ciscoasa(config)# interface gigabithethernet 0/0
```

인터페이스 ID는 다음 값이 가능합니다.

- **redundant**
- 포트 채널
- *physical*—예: **ethernet**, **gigabitethernet**, **tengigabitethernet**, **management**. 인터페이스 이름에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.
- *physical***.***subinterface*— 예: **gigabitethernet0/0.100**.
- **vni**
- **vlan**
- *mapped_name* — 다중 상황 모드의 경우

단계 **2** 인터페이스 이름을 지정합니다.

nameif *name*

예제**:**

```
ciscoasa(config-if)# nameif inside
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다. **no** 형식은 입력하지 마십시오. 그러면 해당 이름을 참조하는 모든 명령이 삭제됩니다.

단계 **3** 다음 방법 중 하나를 사용하여 IP 주소를 설정합니다.

- IP 주소를 직접 설정합니다.

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  예:

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  참고 장애 조치를 사용하는 경우 IP 주소 및 대기 주소를 수동으로 설정해야 하며, DHCP 및 PPPoE는 지원되지 않습니다.

  스탠바이 *ip_address* 인수는 장애 조치에 사용됩니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  ip_address 및 *mask* 인수는 인터페이스 IP 주소와 서브넷 마스크를 설정합니다. 포인트 투 포인트 연결을 위해 31비트 서브넷 마스크(255.255.255.254)를 지정할 수 있습니다. 이 경우 IP 주소가 네트워크 또는 브로드캐스트 주소에 대해 예약되어 있습니다. 이 경우 스탠바이 IP 주소를 설정할 수 없습니다.

  예:

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- DHCP 서버에서 IP 주소를 얻습니다.

  ip address dhcp [**setroute**]

  예:

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute 키워드를 사용하면 ASA에서 DHCP 서버가 제공한 기본 경로를 사용할 수 있습니다.

  DHCP 리스를 재설정하고 새 리스를 요청하려면 이 명령을 다시 입력합니다.

  참고 **ip address dhcp** 명령을 입력하기 전에 **no shutdown** 명령을 사용하여 인터페이스를 활성화하지 않은 경우 일부 DHCP 요청이 전송되지 않을 수 있습니다.

- PPPoE 서버에서 IP 주소를 얻습니다.

  ip address pppoe [**setroute**]

  예:

```
ciscoasa(config-if)# ip address pppoe setroute
```

IP 주소를 직접 입력하여 PPPoE를 대신 활성화할 수 있습니다.

ip address *ip_address mask* **pppoe**

예:

```
ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
```

setroute 옵션은 PPPoE 클라이언트가 아직 연결을 설정하지 않은 경우에 기본 경로를 설정합니다. **setroute** 옵션을 사용 중인 경우 구성에서 정적으로 정의된 경로를 사용할 수 없습니다.

참고 PPPoE가 두 개의 인터페이스(예: 기본 및 백업 인터페이스)에서 활성화되어 있고 이중 ISP 지원을 구성하지 않은 경우, ASA에서는 첫 번째 인터페이스를 통해서만 트래픽을 전송하여 IP 주소를 얻을 수 있습니다.

단계 **4** 보안 레벨을 설정합니다.

security-level *number*

예제**:**

```
ciscoasa(config-if)# security-level 50
```

*number*는 0(가장 낮음)~100(가장 높음) 범위의 정수입니다.

단계 **5** (선택사항) 인터페이스를 관리 전용 모드로 설정하여 통과 트래픽을 전달하지 않도록 합니다.

management-only

기본적으로 관리 인터페이스는 관리 전용으로 구성됩니다. ASA 5585-X를 제외하고 관리 인터페이스에서 **management-only(**관리 전용**)**를 비활성화할 수 없습니다.

예

다음 예에서는 VLAN 101에 대한 매개변수를 구성합니다.

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

다음 예에서는 다중 상황 모드에서 컨텍스트 컨피그레이션을 위한 매개변수를 컨피그레이션합니다. 인터페이스 ID는 매핑된 이름입니다.

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
```

```
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

관련 항목

IPv6 주소 지정 구성, 624 페이지
물리적 인터페이스 활성화 및 이더넷 파라미터 구성, 560 페이지
PPPoE 구성, 617 페이지

PPPoE 구성

인터페이스가 DSL, 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하며 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, 다음 파라미터를 구성합니다.

프로시저

단계 **1** 선택한 VPDN(Virtual Private Dialup Network) 그룹의 이름을 정의하여 이 연결을 나타냅니다.

vpdn group *group_name* **request dialout pppoe**

예제:

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

단계 **2** ISP에서 인증을 요청하는 경우, 인증 프로토콜을 선택합니다.

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

예제:

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

ISP에서 사용하는 인증 유형에 대해 적절한 키워드를 입력합니다.

CHAP 또는 MS-CHAP를 사용 중인 경우 사용자 이름은 원격 시스템 이름이라고 하고 비밀번호는 CHAP 암호라고도 합니다.

단계 **3** ISP에서 할당한 사용자 이름을 VPDN 그룹에 연결합니다.

vpdn group *group_name* **localname** *username*

예제:

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

단계 **4** PPPoE 연결을 위한 사용자 이름 및 비밀번호 쌍을 만듭니다.

vpdn username *username* **password** *password* [**store-local**]

예제:

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local 옵션은 ASA에서 NVRAM의 특정 위치에 사용자 이름 및 비밀번호를 저장합니다. 자동 업데이트 서버에서 ASA에 **clear config** 명령을 전송하여 연결이 중단되면 ASA에서는 NVRAM에서 사용자 이름 및 비밀번호를 읽고 액세스 집중장치에 대해 재인증할 수 있습니다.

브리지 그룹 인터페이스 구성

브리지 그룹은 ASA에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 그룹은 투명 방화벽 모드와 라우팅 방화벽 모드 둘 다에서 지원됩니다. 브리지 그룹에 대한 자세한 내용은 브리지 그룹 정보, 189 페이지를 참조하십시오.

브리지 그룹 및 연결된 인터페이스를 구성하려면, 다음 단계를 수행하십시오.

BVI(Bridge Virtual Interface) 구성

각 브리지 그룹에는 IP 주소를 구성하는 BVI가 필요합니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. IPv4 트래픽의 경우 트래픽을 전달하려면 BVI IP 주소가 필요합니다. IPv6 트래픽에서는 적어도 트래픽을 전달하기 위해서는 링크-로컬 주소를 구성해야 합니다. 그러나 원격 관리, 기타 관리 작업을 포함한 전체 기능에 하나의 전역 관리 주소를 사용하는 것이 좋습니다.

라우팅 모드에서 BVI의 이름을 제공하는 경우 BVI는 라우팅에 참여합니다. 이름이 없는 경우 브리지 그룹은 투명 방화벽 모드에서와 같이 격리된 상태로 남아 있습니다.

일부 모델에서는 기본 구성에 브리지 그룹 및 BVI가 포함되어 있습니다. 추가 브리지 그룹 및 BVI를 생성하고 그룹 간에 멤버 인터페이스를 다시 할당할 수 있습니다.

참고 투명 모드에서 별도의 관리 인터페이스(지원되는 모델)의 경우, 구성 불가한 브리지 그룹(ID 301)이 자동으로 구성에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

프로시저

단계 **1** BVI를 생성합니다.

interface bvi *bridge_group_number*

예제:

```
ciscoasa(config)# interface bvi 2
```

*bridge_group_number*는 1(가장 낮음)에서 250(가장 높음)까지의 정수입니다. 나중에 물리적 인터페이스를 이 브리지 그룹 번호에 할당합니다.

단계 **2** (투명 모드) BVI에 대한 IP 주소를 지정합니다.

ip address *ip_address* [*mask*] [**standby** *ip_address*]

예제**:**

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

BVI에 호스트 주소(/32 또는 255.255.255.255)를 할당하지 마십시오. 또한 /30 서브넷(255.255.255.252)과 같이 3개 미만의 호스트 주소(업스트림 라우터, 다운스트림 라우터, BVI 각각 하나씩)를 포함한 다른 서브넷은 사용하지 마십시오. ASA에서는 서브넷의 첫 주소 및 마지막 주소와의 모든 ARP 패킷을 삭제합니다. 따라서 /30 서브넷을 사용하고 그 서브넷에서 업스트림 라우터에 예약된 주소를 지정할 경우 ASA에서는 다운스트림 라우터에서 업스트림 라우터로 ARP 요청을 삭제합니다.

standby 키워드와 주소는 장애 조치에 사용됩니다.

단계 **3** (라우팅 모드) 다음 방법 중 하나를 사용하여 IP 주소를 설정합니다.

- IP 주소를 직접 설정합니다.

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  예:

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  스탠바이 *ip_address* 인수는 장애 조치에 사용됩니다.

  ip_address 및 *mask* 인수는 인터페이스 IP 주소와 서브넷 마스크를 설정합니다.

- DHCP 서버에서 IP 주소를 얻습니다.

  ip address dhcp [**setroute**]

  예:

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute 키워드는 ASA에서 DHCP 서버가 제공한 기본 경로를 사용할 수 있게 합니다.

  DHCP 리스를 재설정하고 새 리스를 요청하려면 이 명령을 다시 입력합니다.

  ip address dhcp 명령을 입력하기 전에 no shutdown 명령을 사용하여 인터페이스를 활성화하지 않은 경우, 일부 DHCP 요청이 전송되지 않을 수 있습니다.

단계 **4** (라우팅 모드) 인터페이스의 이름을 지정합니다.

nameif *name*

예제**:**

```
ciscoasa(config-if)# nameif inside
```

브리지 그룹 외부 멤버에게 트래픽을 라우팅하려는 경우 BVI의 이름을 지정해야 합니다. 예를 들어, 외부 인터페이스 또는 기타 브리지 그룹의 멤버에게 트래픽을 라우팅하는 경우입니다. *name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다. **no** 형식은 입력하지 마십시오. 그러면 해당 이름을 참조하는 모든 명령이 삭제됩니다.

단계 **5** (라우팅 모드) 보안 수준을 설정합니다.

security-level *number*

예제**:**

```
ciscoasa(config-if)# security-level 50
```

*number*는 0(가장 낮음)~100(가장 높음) 범위의 정수입니다.

예

다음 예에서는 BVI 2주소와 스탠바이 주소를 설정합니다.

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

일반 브리지 그룹 멤버 인터페이스 파라미터 구성

이 절차에서는 각 브리지 그룹 멤버 인터페이스의 이름, 보안 수준, 브리지 그룹을 설정하는 방법을 설명합니다.

시작하기 전에

- 동일한 브리지 그룹은 다양한 유형의 인터페이스를 포함할 수 있습니다. 예를 들어, 물리적 인터페이스, VLAN 하위 인터페이스, VNI 인터페이스, EtherChannel 및 이중 인터페이스가 있습니다. 관리 인터페이스는 지원되지 않습니다. 라우팅 모드에서 EtherChannel 및 VNI는 지원되지 않습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context***name* 명령을 입력합니다.
- 투명 모드에서 관리 인터페이스에는 이 절차를 사용하지 마십시오. 관리 인터페이스 구성에 대한 내용은 투명 모드의 관리 인터페이스 구성, 622 페이지을 참조하십시오.

프로시저

단계 **1** 인터페이스 컨피그레이션 모드를 시작합니다.

interface *id*

예제**:**

```
ciscoasa(config)# interface gigabithethernet 0/0
```

인터페이스 ID는 다음 값이 가능합니다.

- **redundant**
- 포트 채널
- *physical* — **ethernet**, **gigabitethernet**, **tengigabitethernet**을 예로 들 수 있습니다. 관리 인터페이스는 지원되지 않습니다. 인터페이스 이름에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.
- *physical***.***subinterface*— 예: **gigabitethernet0/0.100**.
- **vni**
- **vlan**
- *mapped_name* — 다중 상황 모드의 경우.

참고 라우팅 모드에서 **port-channel**, **redundant** 및 **vni** 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.

단계 **2** 브리지 그룹에 인터페이스를 할당합니다.

bridge-group *number*

예제**:**

```
ciscoasa(config-if)# bridge-group 1
```

*number*는 1~250 범위의 정수이며 BVI 인터페이스 번호와 일치해야 합니다. 최대 64개의 인터페이스를 하나의 브리지 그룹에 할당할 수 있습니다. 동일한 인터페이스를 둘 이상의 브리지 그룹에 지정할 수 없습니다.

단계 **3** 인터페이스 이름을 지정합니다.

nameif *name*

예제**:**

```
ciscoasa(config-if)# nameif inside1
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다. **no** 형식은 입력하지 마십시오. 그러면 해당 이름을 참조하는 모든 명령이 삭제됩니다.

단계 **4** 보안 레벨을 설정합니다.

security-level *number*

예제**:**

```
ciscoasa(config-if)# security-level 50
```

*number*는 0(가장 낮음)에서 100(가장 높음)까지의 정수입니다.

관련 항목

MTU 및 TCP MSS 구성, 657 페이지

투명 모드의 관리 인터페이스 구성

투명 방화벽 모드에서는 모든 인터페이스가 브리지 그룹에 속해야 합니다. 한 가지 예외는 별도의 관리 인터페이스로 구성할 수 있는 관리 인터페이스(물리적 인터페이스, 하위 인터페이스(모델에서 지원되는 경우) 또는 관리 인터페이스로 구성된 EtherChannel 인터페이스(관리 인터페이스가 여러 개인 경우))입니다. Firepower 4100/9300 섀시의 경우, 관리 인터페이스 ID는 ASA 논리적 디바이스에 할당한 관리 유형 인터페이스에 따라 달라집니다. 그 밖의 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다. 단일 모드에서 또는 상황별로 한 개의 관리 인터페이스를 구성할 수 있습니다. 자세한 내용은 투명 모드의 관리 인터페이스, 557 페이지를 참조하십시오.

시작하기 전에

- 이 인터페이스는 브리지 그룹에 할당하지 마십시오. 구성 불가한 브리지 그룹(ID 301)이 자동으로 구성에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.
- 사용하는 모델에 관리 인터페이스가 없을 경우 데이터 인터페이스에서 투명 방화벽 모드를 관리해야 합니다. 이 절차를 예를 들어 ASASM에서는 건너뜁니다. Firepower 4100/9300 섀시의 경우 관리 인터페이스 ID는 ASA 논리적 디바이스에 할당한 관리 유형 인터페이스에 따라 달라집니다.
- 다중 컨텍스트 모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 컨텍스트에서 공유할 수 없습니다. 데이터 인터페이스에 연결해야 합니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

프로시저

단계 **1** 인터페이스 컨피그레이션 모드를 시작합니다.

interface {{ **port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

예제**:**

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. EtherChannel 인터페이스는 관리 멤버 인터페이스만 있어야 합니다.

이중 인터페이스는 관리 슬롯/포트 인스턴스를 멤버로 지원하지 않습니다. 그러나, 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 있습니다.

다중 상황 모드에서는 **allocate-interface** 명령을 사용하여 할당된 인터페이스가 있으면 *mapped_name*을 입력합니다.

Firepower 4100/9300 섀시의 경우, ASA 논리적 디바이스에 할당된 관리 유형 인터페이스(개별 또는 EtherChannel)에 대한 인터페이스 ID를 지정합니다.

단계 **2** 인터페이스 이름을 지정합니다.

nameif *name*

예제**:**

```
ciscoasa(config-if)# nameif management
```

*name*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다. **no** 형식은 입력하지 마십시오. 그러면 해당 이름을 참조하는 모든 명령이 삭제됩니다.

단계 **3** 다음 방법 중 하나를 사용하여 IP 주소를 설정합니다.

- IP 주소를 직접 설정합니다.

  장애 조치에서 사용할 경우 IP 주소와 스탠바이 주소를 직접 설정해야 합니다. DHCP가 지원되지 않습니다.

  ip_address 및 *mask* 인수는 인터페이스 IP 주소와 서브넷 마스크를 설정합니다.

  스탠바이 *ip_address* 인수는 장애 조치에 사용됩니다.

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  예:

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- DHCP 서버에서 IP 주소를 얻습니다.

  ip address dhcp [**setroute**]

  예:

```
ciscoasa(config-if)# ip address dhcp
```

setroute 키워드는 ASA에서 DHCP 서버가 제공한 기본 경로를 사용할 수 있게 합니다.

DHCP 리스를 재설정하고 새 리스를 요청하려면 이 명령을 다시 입력합니다.

ip address dhcp 명령을 입력하기 전에 no shutdown 명령을 사용하여 인터페이스를 활성화하지 않은 경우, 일부 DHCP 요청이 전송되지 않을 수 있습니다.

단계 **4** 보안 레벨을 설정합니다.

security-level *number*

예제**:**

```
ciscoasa(config-if)# security-level 100
```

*number*는 0(가장 낮음)에서 100(가장 높음)까지의 정수입니다.

IPv6 주소 지정 구성

이 섹션에서는 IPv6 주소 지정의 구성 방법을 설명합니다.

IPv6 정보

이 섹션에서는 IPv6에 대한 정보를 다룹니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- 전역—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 브리지 그룹의 경우 이 주소는 멤버 인터페이스가 아닌 BVI에 대해 구성되어야 합니다. 투명 모드에서는 관리 인터페이스에 대해 전역 IPv6 주소를 구성할 수도 있습니다.
- 링크-로컬—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 주소 구성에 또는 주소 확인과 같은 네이버 검색 기능에 사용할 수 있습니다. 브리지 그룹에서 멤버 인터페이스에만 링크 로컬 주소가 있습니다. BVI에는 링크 로컬 주소가 없습니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 브리지 그룹 멤버 인터페이스에서 BVI에 전역 주소를 구성하는 경우, ASA에서는 멤버 인터페이스에 대한 링크 로컬 주소를 자동으로 생성합니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

참고 링크 로컬 주소만 구성하려면 **ipv6 enable**(자동 구성) 또는 **ipv6 address link-local**(수동 구성) 명령을 참조하십시오.

수정된 **EUI-64** 인터페이스 **ID**

RFC 3513: IPv6(Internet Protocol Version 6) Addressing Architecture에 따르면, 모든 유니캐스트 IPv6 주소(이진 값 000으로 시작하는 것 제외)의 인터페이스 식별자 부분은 길이가 64비트이고 Modified EUI-64 형식이어야 합니다. ASA는 로컬 링크에 연결된 호스트에 이 요구 사항을 적용할 수 있습니다.

이 기능이 인터페이스에서 활성화된 경우, 그 인터페이스에서 수신한 IPv6 패킷의 소스 주소를 소스 MAC 주소와 비교하여 검증함으로써 인터페이스 식별자가 Modified EUI-64 형식을 사용하는지 확인합니다. IPv6 패킷에서 인터페이스 식별자에 Modified EUI-64 형식을 사용하지 않을 경우 패킷은 폐기되고 다음 시스템 로그 메시지가 생성됩니다.

```
325003: EUI-64 source address check failed.
```

주소 형식 검증은 흐름이 생성되는 경우에만 수행됩니다. 기존 흐름의 패킷은 검사하지 않습니다. 또한 이 주소 검증은 로컬 링크의 호스트에 대해서만 수행할 수 있습니다.

IPv6 접두사 위임 클라이언트 구성

ASA에서는 클라이언트 인터페이스(예: 케이블 모뎀에 연결된 외부 인터페이스)가 하나 이상의 IPv6 접두사를 수신할 수 있도록 DHPCv6 접두사 위임 클라이언트 역할을 수행할 수 있습니다. 그런 다음 ASA에서는 내부 인터페이스에 서브넷을 지정하고 할당할 수 있습니다.

IPv6 접두사 위임 정보

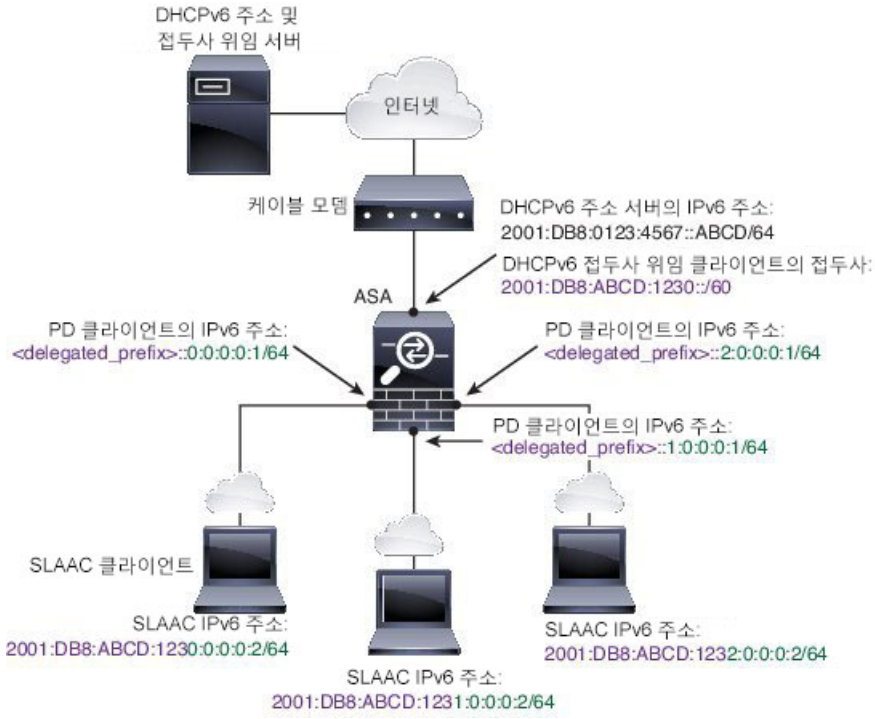
ASA는 클라이언트 인터페이스(예: 케이블 모뎀에 연결된 외부 인터페이스)가 하나 이상의 IPv6 접두사를 수신할 수 있도록 DHPCv6 접두사 위임 클라이언트 역할을 수행할 수 있습니다. 그런 다음 ASA는 내부 인터페이스에 서브넷을 지정하고 할당할 수 있습니다. 그러면 내부 인터페이스에 연결된 호스트는 SLAAC(StateLess Address Auto Configuration)를 사용하여 전역 IPv6 주소를 획득할 수 있습니다. 내부 ASA 인터페이스는 결과적으로 접두사 위임 서버 역할을 수행하지 않습니다. ASA에서는 SLAAC 클라이언트에 전역 IP 주소만 제공할 수 있습니다. 예를 들어, 라우터가 ASA에 연결된 경우, 라우터는 IP 주소를 획득하기 위해 SLAAC 클라이언트 역할을 수행할 수 있습니다. 그러나, 라우터 뒤에 있는 네트워크에 대해 위임된 접두사의 서브넷을 사용하려는 경우, 라우터의 내부 인터페이스에서 이러한 주소를 수동으로 구성해야 합니다.

ASA에는 경량 DHCPv6 서버가 포함되어 있으므로 ASA에서는 SLAAC 클라이언트가 ASA에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 DNS 서버 및 도메인 이름 등의 정보를 제공할 수 있습니다. ASA는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다.

IPv6 접두사 위임 **/64** 서브넷의 예

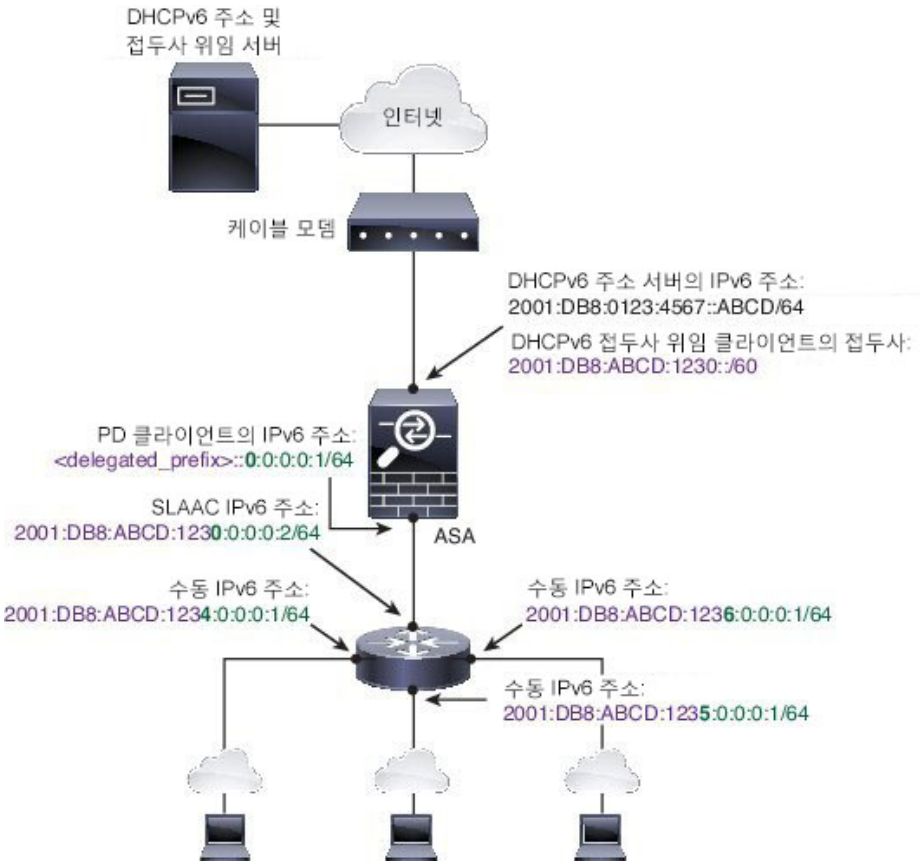
다음 예에는 DHCPv6 주소 클라이언트를 사용하여 외부 인터페이스의 IP 주소를 수신하는 ASA가 나와 있습니다. 또한 DHCPv6 접두사 위임 클라이언트를 사용하여 위임된 접두사를 가져옵니다. ASA

에서는 위임된 접두사를 /64 네트워크에 대해 서브넷을 지정하고 전역 IPv6 주소를 위임된 접두사를 사용하여 내부 인터페이스에 동적으로 할당하고 인터페이스별로 구성된 서브넷(::0, ::1 또는 ::2)과 IPv6 주소(0:0:0:1)를 수동으로 구성합니다. 이러한 내부 인터페이스에 연결된 SLAAC 클라이언트는 각 /64 서브넷에서 IPv6 주소를 획득합니다.



IPv6 접두사 위임 /62 서브넷의 예

다음 예에는 접두사를 4 /62 서브넷으로 서브넷 지정하는 ASA가 나와 있습니다. 2001:DB8:ABCD:123**0**::/62, 2001:DB8:ABCD:123**4**::/62, 2001:DB8:ABCD:123**8**::/62, and 2001:DB8:ABCD:123**C**::/62. ASA에서는 내부 네트워크(::0)에 대해 2001:DB8:ABCD:1230::/62에서 4개의 사용 가능한 /64 서브넷 중 하나를 사용합니다. 그런 다음 다운스트림 라우터에 대해 추가 /62 서브넷을 수동으로 사용할 수 있습니다. 표시된 라우터는 내부 인터페이스(::4, ::5 및 ::6)에 대해 2001:DB8:ABCD:1234::/62에서 4개의 사용 가능한 /64 서브넷 중 3개를 사용합니다. 이 경우, 내부 라우터 인터페이스는 위임된 접두사를 동적으로 획득할 수 없으므로 ASA에서 위임된 접두사를 확인한 다음 해당 접두사를 라우터 구성에 사용해야 합니다. 일반적으로 리스가 만료되면 ISP에서는 지정된 클라이언트에 동일한 접두사를 위임하지만 ASA에서 새 접두사를 수신하는 경우, 새 접두사를 사용하도록 라우터 구성을 수정해야 합니다.



IPv6 접두사 위임 클라이언트 활성화

하나 이상의 인터페이스에서 DHCPv6 접두사 위임 클라이언트를 활성화합니다. ASA에서는 서브넷을 지정하고 내부 네트워크에 할당할 수 있는 하나 이상의 IPv6 접두사를 획득합니다. 일반적으로 접두사 위임 클라이언트를 활성화하는 인터페이스는 DHCPv6 주소 클라이언트를 사용하여 IP 주소를 획득합니다. 다른 ASA 인터페이스만 위임된 접두사에서 파생된 주소를 사용합니다.

시작하기 전에

- 이 기능은 라우팅 방화벽 모드에서만 지원됩니다.
- 이 기능은 다중 컨텍스트 모드에서 지원되지 않습니다.
- 이 기능은 클러스터링에서 지원되지 않습니다.
- 관리 전용 인터페이스에서는 이 기능을 구성할 수 없습니다.
- 접두사 위임을 사용하는 경우, IPv6 트래픽 중단을 방지하기 위해 DHCPv6 서버에서 할당한 접두사에 기본적으로 설정된 수명보다 훨씬 낮게 ASA IPv6 네이버 검색 라우터 알림 간격을 설정해야 합니다. 예를 들어, DHCPv6 서버에서 기본 설정 접두사 위임 수명을 300초로 설정하는 경우, ASA RA 간격을 150초로 설정해야 합니다. 기본 설정 수명을 설정하려면 **show ipv6 general-prefix** 명령을 사용합니다. ASA RA 간격을 설정하려면 IPv6 네이버 검색 구성, 632 페이지의 내용을 참조하십시오. 기본값은 200초입니다.

프로시저

단계 **1** DHCPv6 서버 네트워크에 연결된 인터페이스의 인터페이스 구성 모드로 들어갑니다.

interface *id*

예제:

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

단계 **2** DHCPv6 접두사 위임 클라이언트를 활성화하고 이 인터페이스에서 획득한 접두사의 이름을 지정합니다.

ipv6 dhcp client pd *name*

예제:

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

*name*은 최대 200자입니다.

단계 **3** 수신하려는 위임된 접두사에 대해 하나 이상의 힌트를 제공합니다.

ipv6 dhcp client pd hint *ipv6-prefix/prefix-length*

예제:

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

일반적으로 ::/60과 같은 특정한 접두사 길이를 요청하거나 이전에 특정한 접두사를 받은 적이 있으며 리스가 만료될 때 이 접두사를 다시 획득하고 싶은 경우, 전체 접두사를 힌트로 입력할 수 있습니다. 여러 힌트(다양한 접두사 또는 길이)를 입력하는 경우, 어떤 힌트를 준수할 것인지 또는 힌트를 모두 준수할 것인지 여부는 DHCP 서버에 달려 있습니다.

단계 **4** 접두사의 서브넷을 ASA 인터페이스의 전역 IP 주소로 할당하려면 전역 IPv6 주소 구성, 629 페이지의 내용을 참조하십시오.

단계 **5** (선택 사항) 도메인 이름 및 서버 파라미터를 SLAAC 클라이언트에 제공하려면 DHCPv6 스테이트리스 서버 구성, 711 페이지의 내용을 참조하십시오.

단계 **6** (선택 사항) BGP를 통해 접두사를 알리려면 IPv6 네트워크 설정 구성, 886 페이지의 내용을 참조하십시오.

예

다음 예에서는 GigabitEthernet 0/0에서 DHCPv6 주소 클라이언트와 접두사 위임 클라이언트를 구성한 다음 GigabitEthernet 0/1 및 0/2에서 접두사를 사용하여 주소를 할당합니다.

```
interface gigabitethernet 0/0
```

```
  ipv6 address dhcp default
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

전역 IPv6 주소 구성

모든 라우팅 모드 인터페이스와 투명 또는 라우팅 모드 BVI에 전역 IPv6 주소를 구성하려면, 다음 단계를 수행하십시오.

DHCPv6 및 접두사 위임 옵션은 다중 상황 모드에서 지원되지 않습니다.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다. 브리지 그룹에서 BVI에 전역 주소를 구성하면 모든 멤버 인터페이스에서 링크 로컬 주소가 자동으로 구성됩니다.

하위 인터페이스는 상위 인터페이스의 동일한 번인된(burned-in) MAC 주소를 사용하기 때문에 MAC 주소도 수동으로 설정하는 것이 좋습니다. IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 ASA의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다. MAC 주소 수동 구성, 655 페이지를 참조하십시오.

시작하기 전에

- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

프로시저

단계 **1** 인터페이스 컨피그레이션 모드를 시작합니다.

interface *id*

예제:

```
ciscoasa(config)# interface gigabithethernet 0/0
```

투명 모드에서 또는 라우팅 모드의 브리지 그룹에 대해 BVI를 지정합니다.

예제:

```
ciscoasa(config)# interface bvi 1
```

BVI 외에 투명 모드에서 관리 인터페이스를 지정할 수도 있습니다.

예제**:**

```
ciscoasa(config)# interface management 1/1
```

단계 **2** (라우팅 인터페이스) 다음 방법 중 하나를 사용하여 IP 주소를 설정합니다.

- 인터페이스에서 스테이트리스 자동 구성을 활성화합니다.

  ipv6 address autoconfig [**default trust** {**dhcp** | **ignore**}]

  인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화하면, 라우터 광고 메시지에서 수신된 접두사를 기반으로 IPv6 주소가 구성됩니다. 스테이트리스 자동 컨피그레이션이 활성화될 경우, Modified EUI-64 인터페이스 ID를 기반으로 하는 Link-Local 주소가 인터페이스에 대해 자동으로 생성됩니다.

  참고 RFC 4862에서는 스테이트리스 자동 구성이 구성된 호스트에서 라우터 알림 메시지를 보내지 않도록 지정하지만, 이 경우에는 ASA에서 라우터 알림 메시지를 전송합니다. 메시지를 보내지 않게 하려면 **ipv6 nd suppress-ra** 명령을 참조하십시오.

  기본 경로를 설치하려는 경우 **default trust dhcp** 또는 **ignore**를 지정합니다. **dhcp**는 ASA가 신뢰할 수 있는 소스(즉, IPv6 주소를 제공한 동일한 서버에서 가져옴)에서 가져오는 라우터 알림의 기본 경로만 사용하도록 지정합니다. **ignore**는 라우터 알림을 다른 네트워크에서 가져올 수 있도록 지정하며 이는 더 위험한 방법에 해당합니다.

- DHCPv6를 사용하여 주소를 획득합니다.

  ipv6 address dhcp [**default**]

  예:

  ```
  ciscoasa(config-if)# ipv6 address dhcp default
  ```

  default 키워드를 사용하면 라우터 알림에서 기본 경로를 획득하게 됩니다.

- 인터페이스에 전역 주소를 직접 할당합니다.

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  예:

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

  전역 주소를 지정하면 인터페이스에 대한 링크-로컬 주소가 자동으로 생성됩니다.

  standby는 장애 조치 쌍에서 보조 유닛 또는 장애 조치 그룹에서 사용하는 인터페이스 주소를 지정합니다.

- 지정된 접두사를 Modified EUI-64 형식을 사용하여 인터페이스 MAC 주소에서 생성한 인터페이스 ID와 결합하여 인터페이스에 전역 주소를 할당합니다.

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

예:

```
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

전역 주소를 지정하면 인터페이스에 대한 링크-로컬 주소가 자동으로 생성됩니다.

스탠바이 주소를 지정하지 않아도 되며, 인터페이스 ID가 자동으로 생성됩니다.

- 위임된 접두사를 사용합니다.

  ipv6 address *prefix_name ipv6_address*/*prefix_length*

  예:

  ```
  ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ```

  이 기능을 사용하려면 DHCPv6 접두사 위임 클라이언트가 활성화되어 있는 ASA 인터페이스가 필요합니다. IPv6 접두사 위임 클라이언트 활성화, 627 페이지을 참조하십시오. 일반적으로 위임된 접두사는 /60보다 작으므로 여러 개의 /64 네트워크에 서브넷을 지정할 수 있습니다. 연결된 클라이언트에 대해 SLAAC를 지원하려는 경우 /64는 지원되는 서브넷 길이입니다. /60 서브넷을 완성하는 주소를 지정해야 합니다. 예를 들면 ::1:0:0:0:1과 같습니다. 접두사가 /60보다 작은 경우, 주소 앞에 ::를 입력합니다. 예를 들어, 위임된 접두사가 2001:DB8:1234:5670::/60인 경우, 이 인터페이스에 할당된 전역 IP 주소는 2001:DB8:1234:5671::1/64입니다. 라우터 알림에서 알려진 접두사는 2001:DB8:1234:5671::/64입니다. 이 예에서는 접두사가 /60보다 작은 경우, 접두사의 나머지 비트는 앞에 ::를 사용하여 표시한 것처럼 0이 됩니다. 예를 들어, 접두사가 2001:DB8:1234::/48이면 IPv6 주소는 2001:DB8:1234::1:0:0:0:1/64가 됩니다.

단계 **3** (BVI 인터페이스) BVI에 전역 주소를 직접 할당합니다. 투명 모드의 관리 인터페이스의 경우에도 이 방법을 사용합니다.

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

예:

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

전역 주소를 지정하면 인터페이스에 대한 링크-로컬 주소가 자동으로 생성됩니다.

standby는 장애 조치 쌍에서 보조 유닛 또는 장애 조치 그룹에서 사용하는 인터페이스 주소를 지정합니다.

단계 **4** (선택사항) 로컬 링크의 IPv6 주소에서 반드시 수정된 EUI-64 형식 인터페이스 식별자를 사용하게 합니다.

ipv6 enforce-eui64 *if_name*

예제:

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 인수는 **nameif** 명령으로 지정된, 주소 형식 강제 적용을 활성화하고 있는 인터페이스의 이름입니다.

IPv6 네이버 검색 구성

IPv6 네이버 검색 프로세스는 ICMPv6 메시지와 solicited-node 멀티캐스트 주소를 사용하여 동일 네트워크(로컬 링크)에 있는 네이버의 링크 계층 주소를 확인하고 네이버의 가독성을 확인하며 주변 라우터를 추적합니다.

노드(호스트)는 네이버 검색을 사용하여 연결된 링크에 상주하는 것으로 알려진 네이버에 대한 링크 계층 주소를 확인하고 무효화되는 충돌 값을 빠르게 삭제합니다. 호스트는 또한 네이버 검색을 사용하여 대신 패킷을 전달할 의사가 있는 주변 라우터를 찾기도 합니다. 또한 노드는 프로토콜을 이용하여 네이버의 연결 가능 여부를 능동적으로 추적하고 변경된 링크 계층 주소를 감지합니다. 라우터 또는 라우터 경로가 실패할 경우 호스트가 정상 작동하는 대안을 능동적으로 검색합니다.

-

프로시저

단계 **1** 구성할 IPv6 인터페이스를 지정합니다.

interface *name*

예제:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

단계 **2** DAD(Duplicate Address Detection) 시도 횟수를 지정합니다.

ipv6 nd dad attempts *value*

value 인수에 유효한 값의 범위는 0 ~ 600입니다. 값을 0으로 하면 지정된 인터페이스에서 DAD 처리가 비활성화됩니다. 기본값은 메시지 1개입니다.

DAD는 새로운 유니캐스트 IPv6 주소가 할당되기에 앞서 이 주소가 고유하도록 지정하고 네트워크에서 링크 기준으로 중복 IPv6 주소 탐지를 수행하게 합니다. ASA에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다.

중복 주소가 확인되면 주소 상태가 DUPLICATE로 설정되고 주소가 사용되지 않으며 다음 오류 메시지가 생성됩니다.

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다.

예제:

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

단계 **3** IPv6 네이버 요청 재전송 간격을 설정합니다.

ipv6 nd ns-interval *value*

value 인수의 값 범위는 1000~3600000밀리초입니다.

네이버 요청 메시지(ICMPv6 Type 135)는 로컬 링크에 있는 다른 노드의 링크 계층 주소를 발견하려는 노드가 로컬 링크에서 전송합니다. 네이버 요청 메시지를 수신한 후 목적지 노드는 로컬 링크에서 네이버 광고 메시지(ICPMv6 Type 136)를 전송함으로써 응답합니다.

소스 노드가 네이버 광고를 수신한 후 소스 노드와 목적지 노드가 통신할 수 있습니다. 네이버 요청 메시지는 네이버의 링크 계층 주소를 식별한 후 네이버의 연결 가능성을 확인하는 데 사용됩니다. 노드가 네이버의 연결 가능성을 확인하고자 하는 경우 네이버 요청 메시지의 목적지 주소는 네이버의 유니캐스트 주소입니다.

네이버 광고 메시지는 로컬 링크에 있는 노드의 링크 계층 주소가 변경될 경우에도 전송됩니다.

예제**:**

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

단계 **4** 원격 IPv6 노드 연결 가능 시간을 설정합니다.

ipv6 nd reachable-time *value*

value 인수의 값 범위는 0~3600000밀리초입니다. 값이 0이면 연결 가능 시간은 undetermined로 전송됩니다. 연결 가능 시간의 값을 설정하고 추적하는 일은 수신 디바이스에서 담당합니다.

네이버 연결 가능 시간으로 사용 불가 네이버를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 네이버를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

예제**:**

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

단계 **5** IPv6 라우터 알림 전송의 간격을 설정합니다.

ipv6 nd ra-interval [**msec**] *value*

msec 키워드는 값이 밀리초 단위임을 의미합니다. 이 키워드가 없으면 초 단위입니다. *value* 인수에 유효한 값의 범위는 3초 ~ 1800초, **msec** 키워드가 있는 경우 500밀리초 ~ 1800000밀리초입니다. 기본값은 200초입니다.

간격의 값은 이 인터페이스에서 전송되는 모든 IPv6 라우터 광고에 포함됩니다.

ASA가 기본 라우터로 구성된 경우 전송 간격은 IPv6 라우터 알림 수명보다 짧거나 같아야 합니다. 다른 IPv6 노드와 동기화하지 않게 하려면 실제 사용하는 값을 원하는 값의 20% 범위로 조정합니다.

예제**:**

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

단계 **6** 로컬 링크의 노드가 ASA를 해당 링크의 기본 라우터로 간주해야 하는 기간을 지정합니다.

ipv6 nd ra-lifetime [**msec**] *value*

선택 사항인 **msec** 키워드는 값이 밀리초 단위임을 의미합니다. 그 외의 경우 값은 초 단위입니다. *value* 인수의 값 범위는 0~9000초입니다. 0을 입력하면 선택한 인터페이스에서 ASA를 기본 라우터로 간주할 수 없음을 의미합니다.

라우터 수명 값은 인터페이스에서 발송된 모든 IPv6 라우터 광고에 포함됩니다. 이 값은 이 인터페이스의 기본 라우터인 ASA의 효용성을 나타냅니다.

예제**:**

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

단계 **7** 라우터 알림을 억제합니다.

ipv6 nd suppress-ra

라우터 알림 메시지(ICMPv6 Type 134)는 라우터 요청 메시지(ICMPv6 Type 133)에 대한 응답으로 자동 전송됩니다. 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

ASA가 IPv6 접두사를 전송하길 원치 않는 인터페이스에서 이 메시지를 비활성화할 수 있습니다(예: 인터페이스 외부).

이 명령을 입력하면 ASA는 링크에서 IPv6 라우터가 아닌 일반 IPv6 네이버로 나타나게 됩니다.

단계 **8** IPv6 라우터 알림에 플래그를 추가하여 IPv6 자동 구성 클라이언트에게 DHCPv6를 사용하여 IPv6 주소와 파생된 스테이트리스 자동 구성 주소를 획득하라고 알립니다.

ipv6 nd managed-config-flag

이 옵션은 IPv6 라우터 알림 패킷에서 Managed Address Config 플래그를 설정합니다.

단계 **9** IPv6 라우터 알림에 플래그를 추가하여 IPv6 자동 구성 클라이언트에게 DHCPv6를 사용하여 DNS 서버 주소 또는 기타 정보를 획득하라고 알립니다.

ipv6 nd other-config-flag

이 옵션은 IPv6 라우터 알림 패킷에서 Other Address Config 플래그를 설정합니다.

단계 **10** IPv6 라우터 광고에 포함할 IPv6 접두사를 구성합니다.

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* | **default**} [*valid_lifetime preferred_lifetime* |**at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

네이버가 접두사 광고를 사용하여 인터페이스 주소를 자동으로 구성할 수 있습니다. 스테이트리스 자동 컨피그레이션은 라우터 광고 메시지에서 제공된 IPv6 접두사를 사용하여 링크-로컬 주소에서 전역 유니캐스트 주소를 생성합니다.

기본적으로 **ipv6 address** 명령을 사용하여 인터페이스에서 주소로 구성된 접두사는 라우터 광고에서 광고됩니다. **ipv6 nd prefix** 명령을 사용하여 접두사를 구성할 경우 해당 접두사만 광고됩니다.

스테이트리스 자동 컨피그레이션이 바르게 작동하려면 라우터 광고 메시지의 광고된 접두사 길이가 항상 64비트여야 합니다.

- **default**— 기본 접두사가 사용됨을 나타냅니다.
- *valid_lifetime preferred_lifetime* — 지정된 IPv6 접두사가 유효 및 기본 설정 수명으로 알려지는 기간을 지정합니다. 주소에는 기본 설정 수명 동안에 제한 사항이 없습니다. 기본 설정 수명이 만료된 후에 주소는 사용 중단된 상태가 되는 반면, 주소가 사용 중단 상태일 동안에는 기본 설정 수명의 사용이 권장되지 않지만 엄격하게 금지되지는 않습니다. 유효 수명이 만료되면 주소가 무효화되어 사용할 수 없습니다. 유효 수명은 기본 설정 수명보다 더 크거나 같아야 합니다. 값은 0~4294967295초입니다. 최댓값은 무한대를 의미하며, **infinite** 키워드를 사용하여 지정할 수도 있습니다. 유효 수명의 기본값은 2592000(30일)입니다. 기본 설정 수명의 기본값은 604800(7일)입니다.
- **at** *valid_date preferred_date* — 접두사가 만료되는 특정 날짜와 시간을 나타냅니다. 날짜를 *month_name day hh*:*mm*으로 지정합니다. 예를 들어, **dec 1 13:00**을 입력합니다.
- **no-advertise**— 접두사 알림을 비활성화합니다.
- **no-autoconfig**— IPv6 자동 구성에 접두사를 사용할 수 없도록 지정합니다.
- **off-link**— 지정된 접두사를 off-link로 구성합니다. 접두사는 L-bit 지우기를 사용하여 알려집니다. 접두사는 연결된 접두사로서 라우팅 테이블에 삽입되지 않습니다.

  onlink가 켜진 경우(기본값) 지정된 접두사가 링크에 할당됩니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 목적지를 링크에서 로컬 연결이 가능한 것으로 간주합니다.

예제:

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

단계 **11** IPv6 네이버 검색 캐시에서 고정 항목을 구성합니다.

ipv6 neighbor *ipv6_address if_name mac_address*

고정 IPv6 라우터 구성에는 다음 지침과 제한 사항이 적용됩니다.

- **ipv6 neighbor** 명령은 **arp** 명령과 유사합니다. 지정된 IPv6 주소의 항목이 네이버 검색 캐시에 이미 있을 경우(IPv6 네이버 검색 프로세스를 통해 학습) 이 항목은 고정 항목으로 자동 변환됩니다. 컨피그레이션 저장을 위해 copy 명령이 사용될 때 이 항목은 컨피그레이션에 저장됩니다.
- IPv6 네이버 검색 캐시의 고정 항목을 보려면 **show ipv6 neighbor** 명령을 사용합니다.
- **clear ipv6 neighbor** 명령은 IPv6 네이버 검색 캐시에서 고정 항목을 제외한 모든 항목을 삭제합니다. **no ipv6 neighbor** 명령은 네이버 검색 캐시에서 특정 고정 항목을 삭제합니다. 동적 항목(IPv6 네이버 검색 검색 프로세스에서 학습한 항목)은 캐시에서 삭제하지 않습니다. **no ipv6 enable** 명령을 사용하여 인터페이스에서 IPv6를 비활성화하면 고정 항목을 제외하고 해당 인터페이스에 대해 구성된 모든 IPv6 네이버 검색 캐시 항목이 삭제됩니다(항목의 상태가 INCMP [Incomplete]로 변경됨).

- IPv6 네이버 검색 캐시의 고정 항목은 네이버 검색 프로세스에 의해 변경되지 않습니다.
- **clear ipv6 neighbor** 명령은 IPv6 네이버 검색 캐시에서 고정 항목을 삭제하지 않습니다. 동적 항목만 삭제합니다.
- IPv6 네이버 항목의 정기적인 새로고침에 의해 ICMP syslog가 생성됩니다. IPv6 네이버 항목에 대한 ASA 기본 타이머는 30초입니다. 즉 ASA는 30초마다 ICMPv6 네이버 검색 및 응답 패킷을 생성합니다. ASA에서 장애 조치 LAN 및 상태 인터페이스 모두 IPv6 주소로 구성된 경우 ASA는 구성된 IPv6 주소 및 링크-로컬 IPv6 주소 모두에 대해 30초마다 ICMPv6 네이버 검색 및 응답 패킷을 생성합니다. 또한 각 패킷이 여러 syslog(ICMP 연결 및 로컬-호스트 생성 또는 해체)를 생성하므로 연속적인 ICMP syslog가 생성되는 것으로 보일 수 있습니다. IPV6 네이버 항목의 새로고침 시간은 일반 데이터 인터페이스에서 구성 가능하지만 장애 조치 인터페이스에서는 구성할 수 없습니다. 그러나 이 ICMP 네이버 검색 트래픽은 CPU에 별 영향을 미치지 않습니다.

예제:

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

라우팅 및 투명 모드 인터페이스 모니터링

인터페이스 통계, 상태, PPPoE을 모니터링할 수 있습니다.

인터페이스 통계 및 정보

- **show interface**

  인터페이스 통계를 표시합니다.

- **show interface ip brief**

  인터페이스 IP 주소와 상태를 표시합니다.

- **show bridge-group**

  할당된 인터페이스, MAC 주소 및 IP 주소와 같은 브리지 그룹 정보를 표시합니다.

DHCP 정보

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface 명령을 사용하면 모든 인터페이스에 대한 DHCPv6 정보가 표시됩니다. 인터페이스가 DHCPv6 스테이트리스 서버 구성(DHCPv6 스테이트리스 서버 구성, 711 페이지 참조)에 대해 구성된 경우, 이 명령을 사용하면 서버에서 사용 중인 DHCPv6 풀이 나열됩니다. 인터페이스에 DHCPv6 주소 클라이언트 또는 접두사 위임 클라이언트 구성이 있는 경우, 이 명령을 사용하면 각 클라이언트의 상태와 서버에서 수신한 값이 표시됩니다. 특정 인터페이스의 경

우 DHCP 서버 또는 클라이언트에 대한 메시지 통계를 표시할 수 있습니다. 다음 예는 이 명령이 제공하는 정보를 보여 줍니다.

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
```

```
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client [pd] statistics**

  show ipv6 dhcp client statistics 명령을 사용하면 DHCPv6 클라이언트 통계와 전송 및 수신된 메시지 수의 출력이 표시됩니다. **show ipv6 dhcp client pd statistics** 명령을 사용하면 접두사 위임 클라이언트 통계가 표시됩니다. 다음 예는 이 명령이 제공하는 정보를 보여 줍니다.

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
```

```
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics 명령을 사용하면 유닛 간에 DUID 정보가 동기화된 횟수를 비롯하여 장애 조치 유닛 간의 트랜잭션 통계가 표시됩니다. 다음 예에서 이 명령이 제공하는 정보를 확인할 수 있습니다.

  액티브 유닛의 경우:

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             1
  DUID sync messages received:         0

DHCPv6 HA error statistics:
  Send errors:                         0
```

  스탠바이 유닛의 경우:

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             0
  DUID sync messages received:         1

DHCPv6 HA error statistics:
  Send errors:                         0
```

- **show ipv6 general-prefix**

  show ipv6 general-prefix 명령을 사용하면 DHCPv6 접두사 위임 클라이언트와 다른 프로세스("소비자 목록")에 대한 해당 접두사의 ASA 배포에서 얻은 모든 접두사가 표시됩니다. 다음 예에서 이 명령이 제공하는 정보를 확인할 수 있습니다.

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List               Usage count
    BGP network command        1
    inside (Address command)   1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  현재 PPPoE 클라이언트 구성 정보를 표시합니다.

- **debug pppoe** {**event** | **error** | **packet**}

  PPPoE 클라이언트에 대한 디버깅을 활성화합니다.

- **show vpdn session** [**l2tp** | **pppoe**] [**id** *sess_id* | **packets** | **state** | **window**]

  PPPoE 세션 상태를 확인합니다.

  다음 예는 이 명령이 제공하는 정보를 보여 줍니다.

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

IPv6 네이버 검색

IPv6 네이버 검색 매개변수를 모니터링하려면 다음 명령을 입력합니다.

- **show ipv6 interface**

  이 명령을 사용하면 "outside"와 같은 인터페이스 이름을 비롯하여 IPv6에 대해 구성된 인터페이스의 사용성 상태가 표시되고 지정된 인터페이스의 설정이 표시됩니다. 그러나, 명령의 이름은 제외하고 IPv6가 활성화된 모든 인터페이스에 대한 설정이 표시됩니다. 명령의 출력에서 다음 내용을 표시합니다.

- 인터페이스의 이름과 상태
- 링크-로컬 및 전역 유니캐스트 주소
- 인터페이스가 속한 멀티캐스트 그룹
- ICMP 리디렉션 및 오류 메시지 설정
- 네이버 검색 설정
- 명령이 0으로 설정된 시점의 실제 시간
- 사용 중인 네이버 검색 연결 가능 시간

라우팅 및 투명 모드 인터페이스의 예

2개의 브리지 그룹이 있는 투명 모드의 예

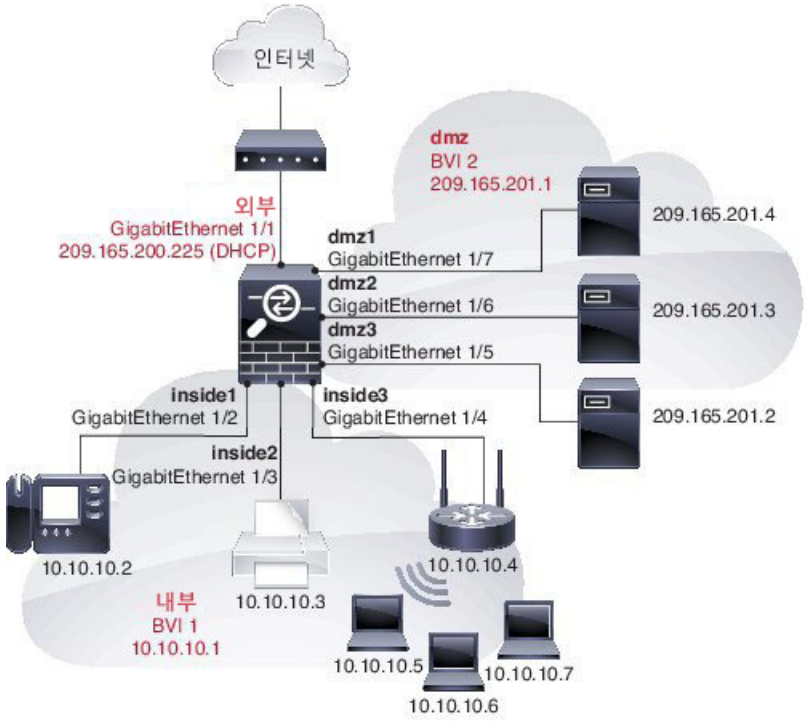
투명 모드에 대한 다음 예에서는 각각 3개의 인터페이스로 구성된 2개의 브리지 그룹과 관리 전용 인터페이스가 있습니다.

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
```

```
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

2개의 브리지 그룹이 있는 전환된 LAN 세그먼트의 예

다음 예에서는 각각 3개의 인터페이스가 있는 2개의 브리지 그룹과 외부용으로 1개의 일반 라우팅 인터페이스를 구성합니다. 브리지 그룹 1은 내부 그룹이며 브리지 그룹 2는 공용 웹 서버가 있는 dmz입니다. 브리지 그룹 멤버 인터페이스는 각 멤버가 동일한 보안 수준에 있으며 동일한 보안 통신을 활성화했기 때문에 브리지 그룹 내부에서 자유롭게 통신할 수 있습니다. 내부 멤버 보안 수준이 100이며 dmz 멤버 보안 수준 또한 100인 경우에도 이러한 보안 수준은 BVI 간 통신에 적용되지 않으며 BVI 보안 수준만 BVI 간 트래픽에 영향을 미칩니다. BVI의 보안 수준 및 외부(100, 50 및 0)는 내부에서 dmz로의 트래픽, 내부에서 외부로의 트래픽, dmz에서 외부로의 트래픽을 암시적으로 허용합니다. 액세스 규칙은 dmz에서 서버에 대한 트래픽을 허용하도록 외부에 적용됩니다.




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
```

```
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
```

```
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

라우팅 및 투명 모드 인터페이스 내역

기능 이름	플랫폼 릴리스	기능 정보
IPv6 네이버 검색	7.0(1)	이 기능을 도입했습니다. 다음 명령을 도입했습니다. **ipv6 nd ns-interval**, **ipv6 nd ra-lifetime**, **ipv6 nd suppress-ra**, **ipv6 neighbor**, **ipv6 nd prefix**, **ipv6 nd dad-attempts**, **ipv6 nd reachable-time**, **ipv6 address**, **ipv6 enforce-eui64**.
투명 모드의 IPv6 지원	8.2(1)	투명 방화벽 모드를 위한 IPv6 지원을 도입했습니다.
투명 모드의 브리지 그룹	8.4(1)	보안 컨텍스트의 오버헤드를 원치 않을 경우 또는 보안 컨텍스트 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 단일 모드에서 또는 각 상황에서 각각 4개의 인터페이스를 포함하는 브리지 그룹을 8개까지 구성할 수 있습니다. 도입된 명령: **interface bvi**, **show bridge-group**
IPv6 DHCP 릴레이에 대한 주소 구성 플래그	9.0(1)	다음 명령을 도입했습니다. **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**.
투명 모드 브리지 그룹 최대 개수 250개로 증가	9.3(1)	브리지 그룹의 최대 개수가 8개에서 250개로 늘어났습니다. 단일 모드에서 또는 다중 모드의 각 컨텍스트에서 최대 250개의 브리지 그룹을 구성할 수 있으며, 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 수정된 명령: **interface bvi**, **bridge-group**

기능 이름	플랫폼 릴리스	기능 정보
브리지 그룹당 투명 모드 최대 인터페이스 개수 64개로 증가	9.6(2)	브리지 그룹당 최대 인터페이스 개수가 4개에서 64개로 증가되었습니다. 명령은 수정하지 않았습니다.
IPv6 DHCP	9.6(2)	이제 ASA는 IPv6 주소 지정에 대해 다음 기능을 지원합니다. • DHCPv6 주소 클라이언트 — ASA는 DHCPv6 서버에서 IPv6 전역 주소 및 선택 사항인 기본 경로를 가져옵니다. • DHCPv6 접두사 위임 클라이언트 — ASA는 DHCPv6 서버에서 위임된 접두사를 가져옵니다. 그런 다음 ASA는 이러한 접두사를 사용하여 SLAAC(Stateless Address Auto Configuration) 클라이언트가 동일한 네트워크에서 IPv6 주소를 자동으로 구성할 수 있도록 다른 ASA 인터페이스 주소를 구성할 수 있습니다. • 위임된 접두사에 대한 BGP 라우터 알림 • DHCPv6 스테이트리스 서버 — ASA는 SLAAC 클라이언트가 ASA에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 도메인 이름 등의 기타 정보를 제공합니다. ASA는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 추가 또는 수정된 명령: **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address autoconfig, ipv6 address dhcp, ipv6 dhcp client pd, ipv6 dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix, sip address, sip domain-name, sntp address**

기능 이름	플랫폼 릴리스	기능 정보
통합 라우팅 및 브리징	9.7(1)	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 ASA에서 경로 대신 브리징하는 인터페이스 그룹입니다. ASA는 실제 브리지가 아닙니다. ASA는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이전에는 브리지 그룹 간에 라우팅할 수 없는 투명 방화벽 모드에서만 브리지 그룹을 구성할 수 있었습니다. 이 기능을 사용하면 라우팅 방화벽 모드에서 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 ASA에 있는 경우에는 외부 Layer 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. 라우팅 모드에서 BVI는 명명된 인터페이스가 될 수 있으며 액세스 규칙 및 DHCP 서버와 같은 일부 기능에서 멤버 인터페이스와 별도로 참여할 수 있습니다. 투명 모드에서 지원되는 다중 상황 모드, ASA 클러스터링 기능은 라우팅 모드에서는 지원되지 않습니다. 동적 라우팅 및 멀티캐스트 라우팅 기능은 BVI에서도 지원되지 않습니다. 수정된 명령: **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**

기능 이름	플랫폼 릴리스	기능 정보
31비트 서브넷 마스크	9.7(1)	라우팅 인터페이스의 경우, 지점 간 연결을 위해 31비트 서브넷에서 IP 주소를 구성할 수 있습니다. 31비트 서브넷 주소는 주소를 2개만 포함합니다. 일반적으로 서브넷의 첫 번째 주소 및 마지막 주소는 네트워크 및 브로드캐스트용으로 예약되어 있으므로 2개의 주소 서브넷은 사용할 수 없습니다. 그러나 지점 간 연결이 있으며 네트워크 또는 브로드캐스트 주소가 필요하지 않은 경우, 31비트 서브넷은 IPv4에서 주소를 보존하는 유용한 방법입니다. 예를 들어, 2개의 ASA 간의 장애 조치 링크에는 주소가 2개만 필요합니다. 링크의 한 쪽 끝에서 전송되는 모든 패킷은 항상 다른 쪽에서 수신되며 브로드캐스팅이 필요하지 않습니다. SNMP 또는 Syslog를 실행하는 직접 연결된 관리 스테이션을 사용할 수도 있습니다. 이 기능은 브리지 그룹 또는 멀티캐스트 라우팅을 위한 BVI에서는 지원되지 않습니다. 수정된 명령: **ip address, http, logging host, snmp-server, ssh**

17 장

고급 인터페이스 구성

이 장에서는 인터페이스에 대한 MAC 주소를 구성하는 방법, MTU(최대 전송 단위) 및 TCP MSS(TCP 최대 세그먼트 크기)를 설정하는 방법 및 동일한 보안 수준의 통신을 허용하는 방법을 설명합니다. 올바른 MTU 및 최대 TCP 세그먼트 크기 설정은 최상의 네트워크 성능에 필수적입니다.

고급 인터페이스 구성 정보

이 섹션에서는 고급 인터페이스 설정을 설명합니다.

MAC 주소 정보

MAC 주소를 수동으로 할당하여 기본값을 재정의할 수 있습니다. 다중 컨텍스트 모드의 경우 특정컨텍스트에 할당된 모든 인터페이스에 대해 고유한 MAC 주소를 자동으로 생성할 수 있습니다.

참고 ASA에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있어 ASA의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

기본 MAC 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- 이중 인터페이스 - 이중 인터페이스에서는 추가하는 첫 물리적 인터페이스의 MAC 주소를 사용합니다. 구성에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 이중 인터페이스에 MAC 주소를 할당하면 멤버 인터페이스 MAC 주소와 상관없이 이 주소가 사용됩니다.
- EtherChannel(Firepower 모델) - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.
- EtherChannel(ASA 모델) - 포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 구성할 수도 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.
- 하위 인터페이스 - 물리적 인터페이스의 모든 하위 인터페이스에서도 동일한 번인된(burned-in) MAC 주소를 사용합니다. 하위 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있어 ASA의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.
- ASASM VLAN - ASASM에서는 모든 VLAN이 백플레인에서 제공한 동일한 MAC 주소를 사용합니다.

자동 **MAC** 주소

다중 컨텍스트 모드에서는 자동 생성 기능이 특정 컨텍스트에 할당된 모든 인터페이스에 고유한 MAC 주소를 할당합니다.

직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우 직접 지정한 수동 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 제거하면 자동 생성 주소가 사용됩니다(활성화된 경우).

드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 해당 인터페이스의 MAC 주소를 직접 설정할 수 있습니다.

자동 생성 주소는 (접두사 사용 시) A2로 시작하므로, 자동 생성도 사용하려는 경우 수동 MAC 주소가 A2로 시작해서는 안 됩니다.

ASA에서는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx.yyzz.zzzz*

여기서 *xx.yy*는 사용자가 정의한 접두사이거나 인터페이스 MAC 주소의 마지막 2바이트에 근거하여 자동 생성된 접두사이며, *zz.zzzz*는 ASA에서 생성한 내부 카운터입니다. 스탠바이 MAC 주소는 동일하지만, 내부 카운터가 1만큼 증가합니다.

접두사 사용 방식의 예를 들자면, 접두사를 77로 설정한 경우 ASA에서는 77을 16진수 값인 004D(*yyxx*)로 변환합니다. 접두사를 MAC 주소에서 사용하는 경우 다음과 같이 ASA 기본 형식에 부합하도록 역전됩니다(*xxyy*).

A24**D.00***zz.zzzz*

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2**F1.03***zz.zzzz*

참고 접두사가 없는 MAC 주소 형식은 레거시 버전입니다. 레거시 형식에 대한 자세한 내용은 명령 참조에서 **mac-address auto** 명령을 참조하십시오.

MTU 정보

MTU에서는 ASA이(가) 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 없는 프레임 크기입니다. 예를 들어, MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더 포함 시 1518바이트이고 VLAN 사용 시에는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오.

VXLAN의 경우 전체 이더넷 데이터그램이 캡슐화되므로 새 IP 패킷이 더 크기 때문에 더 큰 MTU가 필요합니다. 따라서 ASA VTEP 소스 인터페이스 MTU를 네트워크 MTU + 54바이트로 설정해야 합니다.

경로 MTU 검색

ASA에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

기본 MTU

ASA의 기본 MTU는 1500바이트입니다. 이 값에는 18~22바이트의 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 포함되지 않습니다.

VTEP 소스 인터페이스에서 VXLAN을 활성화하는 경우, MTU가 1554바이트보다 작으면 ASA에서 자동으로 MTU를 1554바이트로 늘립니다. 이 경우 전체 이더넷 데이터그램이 캡슐화되고 있으므로 새 패킷이 더 크고 더 대량의 MTU가 필요합니다. 일반적으로, ASA 소스 인터페이스 MTU를 네트워크 MTU + 54바이트로 설정해야 합니다.

MTU 및 단편화

IPv4의 경우 지정된 MTU보다 큰 발신 IP 패킷은 2개 이상의 프레임으로 단편화됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. IPv6의 경우에는 일반적으로 패킷의 단편화가 전혀 허용되지 않습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

TCP 패킷의 경우 엔드포인트는 일반적으로 해당 MTU를 사용해 TCP 최대 세그먼트 크기(예: MTU - 40)를 결정합니다. 중간에 사이트 대 사이트 VPN 터널 등에 사용하기 위해 TCP 헤더가 더 추가된 경우에는 터널링 엔티티를 통해 TCP MSS를 하향 조정해야 할 수 있습니다. TCP MSS 정보, 652 페이지를 참조하십시오.

UDP 또는 ICMP의 경우 애플리케이션은 단편화 방지를 위해 MTU를 고려해야 합니다.

참고 ASA에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다.

MTU와 점보 프레임

큰 MTU를 사용하는 경우 더 큰 패킷을 전송할 수 있습니다. 큰 패킷은 네트워크에서 더욱 효율적으로 사용할 수 있습니다. 다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 — 모든 ASA 인터페이스 및 기타 디바이스 인터페이스의 MTU를 트래픽 경로와 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용 - 점보 프레임을 활성화할 때 MTU를 최대 9198바이트로 설정할 수 있습니다. 최대값은 ASAv의 경우 9000이고 Firepower 4100/9300 섀시에 있는 ASA의 경우에는 9184입니다.

참고 ASA 5585-X에서는 VLAN 태깅을 사용하는 경우 최대 MTU가 4바이트 더작습니다. 즉, 이 경우에는 8996입니다.

TCP MSS 정보

TCP MSS(최대 세그먼트 크기)는 TCP 및 IP 헤더가 추가되기 전의 TCP 페이로드 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

ASA에서 통과 트래픽에 대해 참조). 기본적으로 최대 TCP MSS는 1380바이트로 설정됩니다. 이 설정은 ASA에서 IPsec VPN 캡슐화를 할 때 패킷 크기를 추가해야 하는 경우 유용합니다. 그러나 IPsec 이외의 엔드포인트에 대해서는 ASA에서 최대 TCP MSS를 비활성화해야 합니다.

최대 TCP MSS를 설정하는 경우, 연결의 엔드포인트에서 ASA에 설정된 값보다 큰 TCP MSS를 요청하면 ASA에서는 요청 패킷의 TCP MSS를 ASA 최대값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우, ASA에서는 RFC 793 기본값을 536바이트(IPv4) 또는 1220바이트(IPv6)로 가정하며 패킷을 수정하지 않습니다. 기본 MTU를 1500바이트로 유지하는 경우를 예로 들어보겠습니다. 이 경우 호스트는 1500바이트에서 TCP 및 IP 헤더 길이를 뺀 MSS를 요청하므로 MSS는 1460으로 설정됩니다. ASA 최대 TCP MSS가 1380(기본값)이면 ASA에서는 TCP 요청 패킷의 MSS 값을 1380으로 변경합니다. 그러면 서버에서는 1380바이트 페이로드가 포함된 패킷을 전송합니다. 이 경우 ASA이(가) 최대 120바이트의 헤더를 패킷에 추가해도 MTU 크기인 1500을 맞출 수 있습니다.

또한 최소 TCP MSS를 구성할 수 있습니다. 호스트 또는 서버에서 요청한 TCP MSS가 매우 작을 경우, ASA에서는 값을 조정하여 올릴 수 있습니다. 기본적으로 최소 TCP MSS는 활성화되어 있지 않습니다.

SSL VPN 연결 트래픽을 포함한 to-the-box 트래픽에는 이 설정이 적용되지 않습니다. 이 경우 ASA에서는 MTU를 사용하여 TCP MSS: MTU - 40(IPv4) 또는 MTU - 60(IPv6)을 파생합니다.

기본 **TCP MSS**

기본적으로 ASA의 최대 TCP MSS는 1380바이트입니다. 이 기본값을 사용하면 헤더가 120바이트와 동일한 값까지 가능한 경우 IPv4 IPsec VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

최대 **TCP MSS** 설정 제안

기본 TCP MSS는 ASA가 IPv4 IPsec VPN 엔드포인트 역할을 수행하고 1500바이트의 MTU를 갖는다고 가정합니다. ASA가 IPv4 IPsec VPN 엔드포인트 역할을 수행하는 경우, TCP 및 IP 헤더용으로 최대 120바이트까지 수용해야 합니다.

MTU 값을 변경하고 IPv6를 사용하거나 ASA를 IPsec VPN 엔드포인트로 사용하지 않는 경우, FlexConfig에서 Sysopt_Basic 개체를 사용하여 TCP MSS 설정의 내용을 참조하십시오. 다음 지침을 참조하십시오.

- 정상 트래픽 — TCP MSS 제한을 비활성화하고 연결 엔드포인트 간에 설정한 값을 허용합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 IPsec 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- IPv4 IPsec 엔드포인트 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 9000으로 설정할 경우 새로운 MTU를 활용하기 위해 TCP MSS를 8880으로 설정해야 합니다.
- IPv6 IPsec 엔드포인트 트래픽 — MTU에 대한 최대 TCP MSS를 140으로 설정합니다.

인터페이스 간 통신

동일한 보안 레벨에서 각 인터페이스끼리 서로 통신을 수행할 수 있도록 허용할 경우 다음과 같은 이점이 제공됩니다.

- 101개가 넘는 통신 인터페이스를 구성할 수 있습니다.

  인터페이스마다 다른 레벨을 사용하고 인터페이스에 동일한 보안 레벨을 할당하지 않을 경우, 레벨(0~100)별로 한 개의 인터페이스만 구성할 수 있습니다.
- 모든 동일한 보안 인터페이스 간에 ACL 없이도 트래픽 흐름이 자유롭게 이루어지도록 하고자 할 수 있습니다.

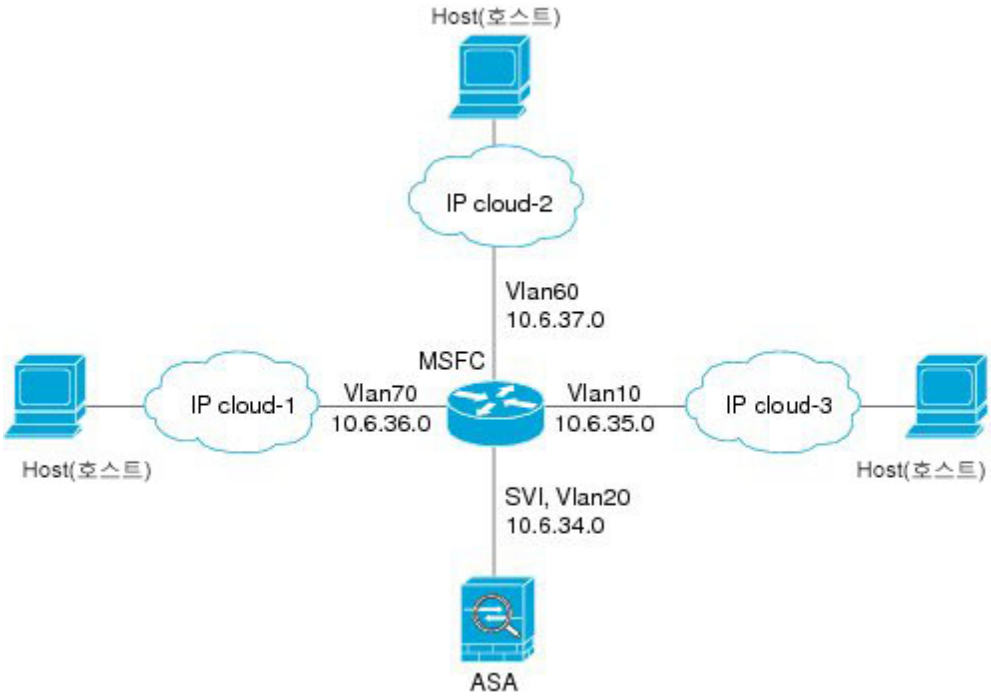
동일한 보안 인터페이스 통신을 활성화하더라도 기존처럼 여러 보안 레벨에서 인터페이스를 구성할 수 있습니다.

인터페이스 내 통신(라우팅된 방화벽 모드)

인터페이스 내 통신은 인터페이스에 들어오지만 동일한 인터페이스 밖으로 라우팅되는 VPN 트래픽에 유용할 수 있습니다. 이 경우 VPN 트래픽은 암호화되지 않거나 다른 VPN 연결을 위해 다시 암호화될 수 있습니다. 예를 들어 허브 및 스포크 VPN 네트워크가 있는 경우(여기서 ASA는 허브이고 원격 VPN 네트워크는 스포크) 스포크 간에 통신하려면 트래픽이 ASA로 들어간 다음 다른 스포크로 다시 나가야 합니다.

참고 이 기능을 통해 허용되는 모든 트래픽은 여전히 방화벽 규칙의 적용을 받습니다. 따라서 ASA를 트래버스하지 않기 위해 트래픽을 반환할 수 있는 비대칭 라우팅 상황을 만들지 마십시오.

ASASM의 경우 이 기능을 활성화하기 전에, MSFC를 먼저 올바르게 구성하여 패킷이 스위치를 직접 통해 대상 호스트에서 전송되는 대신 ASA MAC 주소로 전송되도록 해야 합니다. 다음 그림에는 동일한 인터페이스의 호스트 간에 통신을 수행해야 하는 네트워크가 나와 있습니다.



다음 샘플 구성에는 Cisco IOS **route-map** 명령을 사용하여 다음 그림에 표시된 네트워크에서 정책 라우팅을 활성화하는 방법이 나와 있습니다.

```
route-map intra-inter3 permit 0
  match ip address 103
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
  match ip address 102
  set interface Vlan20
  set ip next-hop 10.6.34.7
```

```
!
route-map intra-inter1 permit 10
  match ip address 101
  set interface Vlan20
  set ip next-hop 10.6.34.7
```

MAC 주소 수동 구성

수동으로 MAC 주소를 할당해야 하는 경우, 다음 절차대로 수행할 수 있습니다.

ASA에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있어 ASA의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

시작하기 전에

다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

프로시저

단계 **1** 인터페이스 컨피그레이션 모드를 시작합니다.

interface *id*

예제**:**

```
ciscoasa(config)# interface gigabithethernet 0/0
```

단계 **2** 이 인터페이스에 사설 MAC 주소를 할당합니다.

mac-address *mac_address* [**standby** *mac_address*]

예제**:**

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

*mac_address*는 H.H.H 형식이며, 여기서 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다. 즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없습니다.

자동 생성된 MAC 주소도 사용하려는 경우 수동 MAC 주소의 처음 2바이트는 A2가 될 수 없습니다.

장애 조치와 함께 사용하려면 **standby** MAC 주소를 설정합니다. 액티브 유닛이 장애 조치되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

다중 상황 모드에서 **MAC** 주소 자동 할당

이 섹션에서는 MAC 주소의 자동 생성을 구성하는 방법을 설명합니다. 다중 상황 모드에서는 이 기능이 특정 상황에 할당된 모든 인터페이스 유형에 고유한 MAC 주소를 할당합니다.

시작하기 전에

- 인터페이스에 대해 **nameif** 명령을 구성하면 새 MAC 주소가 즉시 생성됩니다. 인터페이스를 구성한 다음 이 기능을 활성화한 경우, 활성화한 직후에 모든 인터페이스에 대해 MAC 주소가 생성됩니다. 이 기능을 비활성화한 경우 각 인터페이스의 MAC 주소가 기본 MAC 주소로 돌아갑니다. 예를 들어, GigabitEthernet 0/1의 하위 인터페이스는 다시 GigabitEthernet 0/1의 MAC 주소를 사용하게 됩니다.
- 드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 해당 인터페이스의 MAC 주소를 직접 설정할 수 있습니다.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

각 인터페이스에 사설 MAC 주소를 자동으로 할당합니다.

mac-address auto [**prefix** *prefix*]

접두사를 입력하지 않으면 ASA에서 인터페이스 MAC 주소의 마지막 2바이트를 기반으로 접두사를 자동으로 생성합니다.

직접 접두사를 입력할 경우 *prefix*는 0 ~ 65535 범위의 십진수입니다. 이 접두사가 4자리 16진수로 변환되어 MAC 주소의 일부로 사용됩니다.

예제**:**

```
ciscoasa(config)# mac-address auto prefix 19
```

MTU 및 TCP MSS 구성

시작하기 전에

- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context***name* 명령을 입력합니다.
- MTU를 1500 이상으로 높이려면 점보 프레임 지원 활성화, 563 페이지에 따라 점보 프레임을 활성화합니다. ASASM에서는 기본적으로 점보 프레임을 지원하므로 활성화할 필요가 없습니다.

프로시저

단계 **1** MTU를 300~9198바이트(ASAv의 경우 9000바이트, Firepower 4100/9300 섀시의 경우 9184) 범위에서 설정합니다.

mtu *interface_name bytes*

예제**:**

```
ciscoasa(config)# mtu inside 9000
```

기본값은 1500바이트입니다.

참고 이중 또는 포트 채널 인터페이스를 위해 MTU를 설정하면 ASA에서는 모든 멤버 인터페이스에 이 설정을 적용합니다.

점보 프레임을 지원하는 많은 모델에서 어떤 인터페이스에 1500보다 큰 값을 입력한 경우 점보 프레임 지원을 활성화해야 합니다. 점보 프레임 지원 활성화, 563 페이지을 참조하십시오.

참고 VLAN 태깅을 사용하는 경우, ASA 5585-X에서는 최댓값이 4바이트 더 작습니다. 즉 ASA 5585-X의 경우에는 9194의 경우에는 입니다. ASA를 사용하여 MTU를 9195~9198 범위의 값으로 설정하는 경우에도 실제 페이로드 크기는 9194입니다.

단계 **2** 최대 TCP 세그먼트 크기(바이트)를 48에서 임의의 최대값 범위에서 설정합니다.

sysopt connection tcpmss [**minimum**] *bytes*

예제**:**

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

기본값은 1380바이트입니다. bytes를 **0**으로 설정하여 이 기능을 비활성화할 수 있습니다.

minimum 키워드는 최대 세그먼트 크기를 48 ~ 65535 범위에서 *bytes*보다 작지 않은 값으로 설정합니다. 최소값 기능은 기본적으로 비활성화되어 있습니다(0으로 설정).

단계 **3** **ASA Cluster(ASA** 클러스터**)** 설정에 대한 내용은 마스터 유닛의 인터페이스 구성, 392 페이지을 참조하십시오.

예

다음 예에서는 점보 프레임을 활성화하고, 모든 인터페이스의 MTU를 높이며, TCP MSS를 0으로 설정하여 비 VPN 트래픽의 TCP MSS를 비활성화합니다(이 경우 제한이 없어짐).

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

다음 예에서는 점보 프레임을 활성화하고, 모든 인터페이스의 MTU를 높이며, VPN 트래픽의 TCP MSS를 9078로 변경합니다(MTU 빼기 120).

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

동일한 보안 수준 통신 허용

기본적으로 동일한 보안 레벨의 인터페이스는 서로 통신할 수 없고 패킷이 동일한 인터페이스에 들어오고 나갈 수 없습니다. 이 섹션에서는 동일한 보안 레벨에 있는 인터페이스 간의 통신을 활성화하는 방법 및 인터페이스 내 통신을 활성화하는 방법을 설명합니다.

프로시저

단계 **1** 동일한 보안 수준에서 인터페이스를 활성화하여 서로 통신할 수 있게 합니다.

same-security-traffic permit inter-interface

단계 **2** 동일한 인터페이스에 연결된 호스트 간의 통신을 활성화합니다.

same-security-traffic permit intra-interface

고급 인터페이스 구성에 대한 기록

표 ***23:*** 고급 인터페이스 구성에 대한 기록

기능 이름	릴리스	기능 정보
최대 MTU: 현재는 9198바이트	9.1(6), 9.2(1)	ASA에서 사용할 수 있는 최대 MTU는 9198바이트(CLI 도움말에서 모델의 정확한 제한 확인)입니다. 이 값은 Layer 2 헤더를 포함하지 않습니다. 이전에는 ASA에서 최대 MTU를 65535바이트로 지정할 수 있었으며 이는 부정확해서 문제를 유발하기도 했습니다. MTU가 9198보다 더 높은 값으로 설정된 경우 MTU는 업그레이드할 때 자동으로 낮아집니다. 경우에 따라 이 MTU를 변경하면 MTU가 불일치할 수 있으므로 연결 중인 장비에서 새 MTU 값을 사용하도록 설정해야 합니다. 수정된 명령: **mtu**
ASA용 MTU 크기 증가됨 Firepower 4100/9300 섀시	9.6(2)	Firepower 4100 및 9300에서 최대 MTU를 9184바이트로 설정할 수 있습니다. 이전에는 최댓값이 9000바이트였습니다. 이 MTU는 FXOS 2.0.1.68 이상 버전에서 지원됩니다. 수정된 명령: **mtu**

18 장

트래픽 영역

기존 플로우의 트래픽이 영역 내 모든 인터페이스에서 ASA로 들어가거나 ASA에서 나올 수 있도록 트래픽 영역에 여러 인터페이스를 할당할 수 있습니다. 이 기능을 사용하면 ASA에서 ECMP(Equal-Cost Multi-Path) 라우팅이 가능해질 뿐만 아니라, 여러 인터페이스에 걸쳐 ASA에 대한 트래픽의 외부 로드 밸런싱도 가능해집니다.

트래픽 영역 소개

이 섹션에서는 네트워크에서 트래픽 영역을 사용하는 방법을 설명합니다.

영역 비지정 동작

Adaptive Security Algorithm에서는 트래픽을 허용할지 아니면 거부할지 결정할 때 패킷의 상태를 고려합니다. 흐름에 대해 강제 적용한 파라미터 중 하나는 동일한 인터페이스로 드나드는 트래픽입니다. 다른 인터페이스에 들어오는 기존 플로우에 대한 트래픽은 모두 ASA에서 삭제합니다.

트래픽 영역을 사용하여 여러 인터페이스를 그룹화함으로써 해당 영역에 속한 임의의 인터페이스를 드나드는 트래픽에 대해 Adaptive Security Algorithm 보안 검사가 이루어질 수 있습니다.

관련 항목

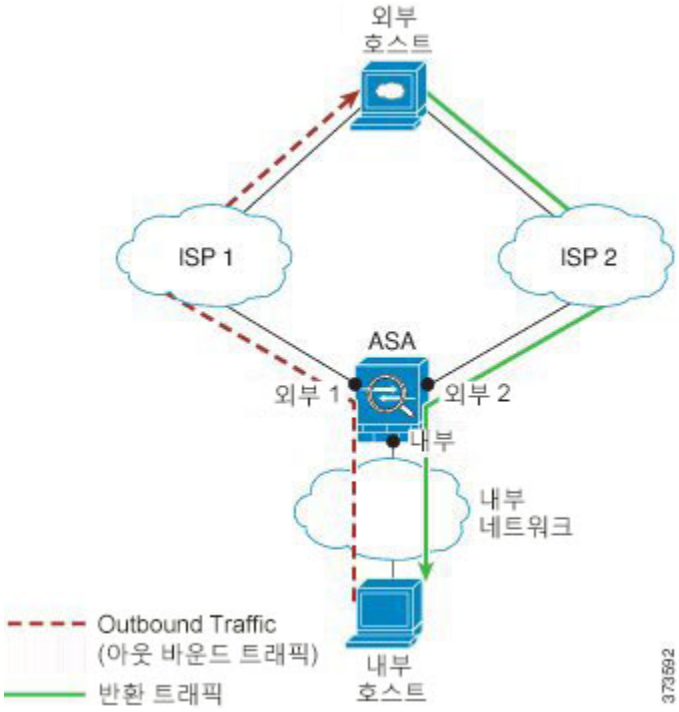
상태 저장 감시 개요, 8 페이지

영역을 사용하는 이유

여러 라우팅 시나리오에서 영역을 사용할 수 있습니다.

비대칭 라우팅

다음 시나리오에서는 Outside1 인터페이스의 ISP 1을 통해 내부 호스트와 외부 호스트 간의 연결이 설정되었습니다. 목적지 네트워크의 비대칭 라우팅 때문에 Outside2 인터페이스의 ISP 2에서 온 트래픽을 반환합니다.

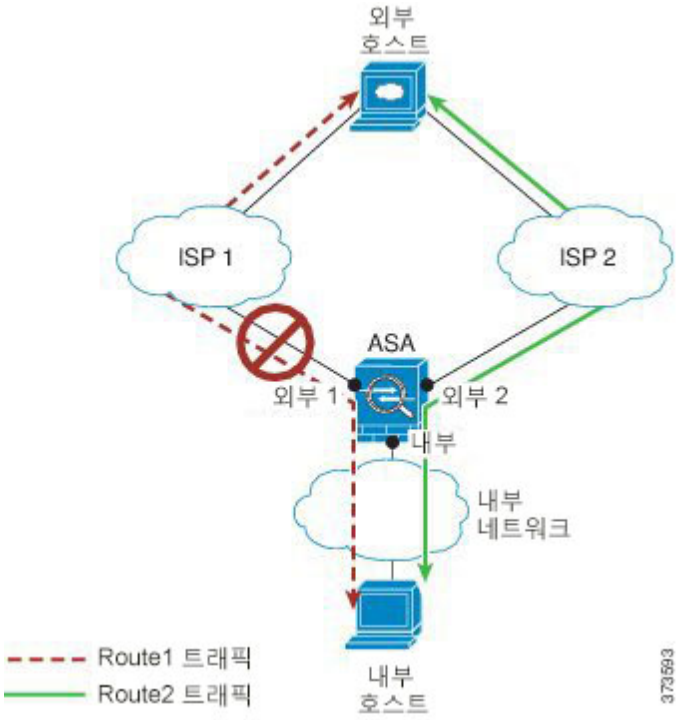


영역 비지정 문제: ASA에서 인터페이스별로 연결 테이블을 유지 관리합니다. 반환 트래픽이 Outside2에 도착하면 연결 테이블과 매치하지 않아 폐기됩니다. ASA 클러스터의 경우 클러스터가 동일한 라우터에 대해 여러 개의 인접성을 갖는 경우, 비대칭 라우팅은 허용되지 않는 트래픽 손실로 이어질 수 있습니다.

영역 지정 해결책: ASA에서 영역별로 연결 테이블을 유지 관리합니다. Outside1과 Outside2를 하나의 영역으로 그룹화할 경우 반환 트래픽이 Outside2에 도착하면 영역별 연결 테이블과 매치하고 연결이 허용됩니다.

손실 경로

다음 시나리오에서는 Outside1 인터페이스의 ISP 1을 통해 내부 호스트와 외부 호스트 간의 연결이 설정되었습니다. Outside1과 ISP 1 간의 경로가 손실되었거나 이동했기 때문에 트래픽은 ISP 2를 지나는 다른 경로를 택해야 합니다.

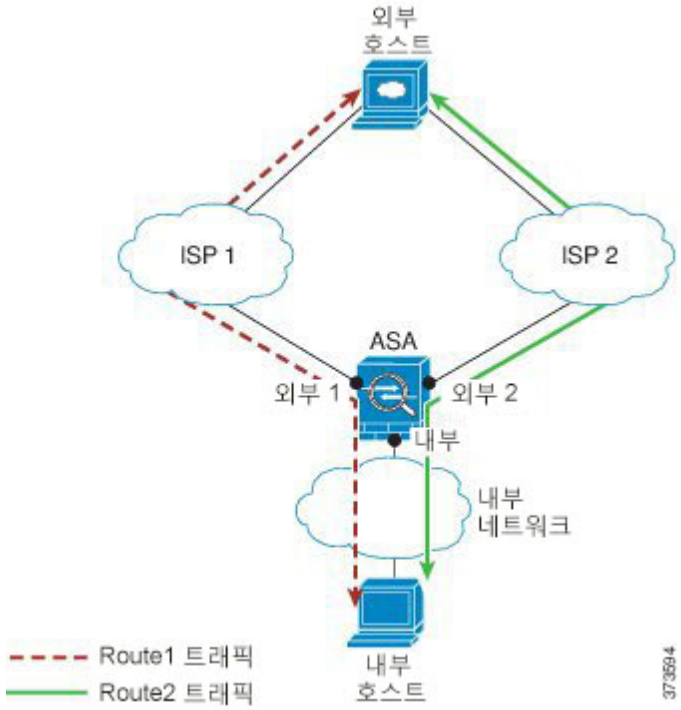


영역 비지정 문제: 내부 호스트와 외부 호스트 간의 연결이 삭제됩니다. 새로운 차선책 경로를 사용하여 새 연결을 설정해야 합니다. UDP의 경우 단일 패킷이 폐기된 후 새 경로가 사용됩니다. 그러나 TCP에서는 새 연결을 재설정해야 합니다.

영역 지정 해결책: ASA에서 손실 경로를 탐지하고 ISP 2를 지나는 새 경로로 플로우를 전환합니다. 어떤 패킷도 폐기되지 않고 원활하게 트래픽이 전달됩니다.

부하 균형

다음 시나리오에서는 Outside1 인터페이스의 ISP 1을 통해 내부 호스트와 외부 호스트 간의 연결이 설정되었습니다. Outside2의 ISP 2를 지나는 동일 비용 경로를 통해 제2의 연결이 설정되었습니다.



영역 비지정 문제: 여러 인터페이스를 포괄하는 로드 밸런싱은 불가합니다. 단일 인터페이스의 동일 비용 경로에서만 로드 밸런싱이 가능합니다.

영역 지정 해결책: ASA에서는 영역의 모든 인터페이스에서 최대 8개의 동일 비용 경로를 대상으로 연결을 로드 밸런싱합니다.

영역별 연결 및 라우팅 테이블

ASA에서 영역별 연결 테이블을 유지 관리하므로 트래픽이 영역 인터페이스 중 어디라도 도착할 수 있습니다. 또한 ASA에서는 ECMP 지원을 위해 영역별 라우팅 테이블을 유지 관리합니다.

ECMP 라우팅

ASA에서는 ECMP(Equal-Cost Multi-Path) 라우팅을 지원합니다.

영역 비지정 ECMP 지원

영역이 없을 경우 인터페이스당 최대 8개의 동일 비용 고정 또는 동적 경로가 가능합니다. 예를 들어 외부 인터페이스에서 서로 다른 게이트웨이를 지정하는 3개의 기본 경로를 구성할 수 있습니다.

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

여기서는 외부 인터페이스에서 0.1.1.2, 10.1.1.3, 10.1.1.4끼리 트래픽 로드 밸런싱을 수행합니다. 트래픽은 소스와 목적지 IP 주소를 해싱하는 알고리즘에 따라 지정된 게이트웨이 사이에서 분배됩니다.

ECMP는 다중 인터페이스에서 지원되지 않으므로 동일한 목적지의 경로를 다른 인터페이스에서 정의할 수 없습니다. 다음 경로는 위의 경로 중 어느 것이든 구성될 경우 거부됩니다.

```
route outside2 0 0 10.2.1.1
```

영역 지정 ECMP 지원

영역을 사용할 경우 하나의 영역 내에서 최대 8개의 동일 비용 고정 또는 동적 경로가 가능합니다. 예를 들어 영역의 3개 인터페이스 전 범위에서 3개의 기본 경로를 구성할 수 있습니다.

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

또한 동적 라우팅 프로토콜은 동일 비용 경로를 자동으로 구성할 수 있습니다. ASA에서는 더 강력한 로드 밸런싱 메커니즘을 통해 인터페이스 간의 트래픽을 로드 밸런싱합니다.

어떤 경로가 사라지면 ASA에서는 원활하게 다른 경로로 플로우를 이동합니다.

연결이 로드 밸런싱되는 방법

ASA에서는 패킷 6-tuple(소스 및 대상 IP 주소, 소스 및 대상 포트, 프로토콜, 인그레스 인터페이스)에서 생성된 해시를 사용하여 동일 비용 경로 전반에서 연결을 로드 밸런싱합니다. 경로가 손실되지 않는 한 연결은 선택된 인터페이스에서 끊길 때까지 지속됩니다.

어떤 연결 내의 패킷은 여러 경로 전반에서 로드 밸런싱되지 않습니다. 경로가 손실되지 않는 한 연결에서는 단일 경로를 사용합니다.

ASA에서는 로드 밸런싱할 때 인터페이스 대역폭 또는 기타 파라미터를 고려하지 않습니다. 동일한 영역에 속한 모든 인터페이스는 MTU, 대역폭 등의 특성이 동일해야 합니다.

로드 밸런싱 알고리즘은 사용자가 구성할 수 없습니다.

다른 영역의 경로에 장애 조치

어떤 인터페이스에서 경로가 손실된 경우 그 영역 내에 사용 가능한 다른 경로가 없다면 ASA에서는 다른 인터페이스/영역의 경로를 사용합니다. 이 백업 경로를 사용할 경우 영역 비지정 라우팅 지원으로 패킷 폐기가 일어날 수 있습니다.

인터페이스 기반 보안 정책

영역은 해당 영역 내 인터페이스에서 트래픽이 들어오고 나갈 수 있도록 하지만 보안 정책 자체(액세스 규칙, NAT 등)는 영역별이 아니라 여전히 인터페이스별로 적용됩니다. 영역 내의 모든 인터페이스에 대해 동일한 보안 정책을 구성한 경우 해당 트래픽에 대한 ECMP 및 로드 밸런싱을 성공적으로 구현할 수 있습니다. 필요한 병렬 인터페이스 컨피그레이션에 대한 자세한 내용은 트래픽 영역에 대한 사전 요건, 667 페이지를 참조하십시오.

트래픽 영역에 대해 지원되는 서비스

영역과 관련하여 다음 서비스가 지원됩니다.

- 액세스 규칙
- NAT
- QoS 트래픽 정책을 제외한 서비스 규칙
- 라우팅

to-the-box 및 from-the-box 트래픽, 667 페이지 목록의 to-the-box 및 from-the-box 서비스도 구성할 수 있습니다. 단, 전체 영역 지정 지원은 사용할 수 없습니다.

트래픽 영역의 인터페이스에 대해 다른 서비스(VPN 또는 봇네트 트래픽 필터)를 구성하지 마십시오. 이 서비스는 예상대로 작동하거나 확장되지 않을 수 있습니다.

참고 보안 정책을 구성하는 방법에 대한 자세한 내용은 트래픽 영역에 대한 사전 요건, 667 페이지를 참조하십시오.

보안 수준

영역에 추가한 첫 번째 인터페이스는 영역의 보안 레벨을 결정합니다. 모든 추가 인터페이스는 보안 레벨이 동일해야 합니다. 영역에서 인터페이스의 보안 레벨을 변경하려면 하나의 인터페이스를 제외하고 모든 인터페이스를 제거한 다음 보안 레벨을 변경하고 인터페이스를 다시 추가해야 합니다.

흐름을 위한 기본 및 현재 인터페이스

각 연결 흐름은 첫 번째 인그레스 및 이그레스 인터페이스에 기반하여 구축됩니다. 이러한 인터페이스가 기본 인터페이스입니다.

경로 변경 또는 비대칭 라우팅 때문에 새 인그레스 인터페이스가 사용되는 경우 새로운 인터페이스가 현재 인터페이스입니다.

영역에 가입 또는 나가기

영역에 인터페이스를 할당하면 해당 인터페이스의 모든 연결이 삭제됩니다. 연결을 다시 설정해야 합니다.

영역에서 인터페이스를 제거하면 해당 인터페이스를 기본 인터페이스로 사용하는 모든 연결이 삭제됩니다. 연결을 다시 설정해야 합니다. 인터페이스가 현재 인터페이스인 경우 ASA에서는 연결을 기본 인터페이스로 다시 이동합니다. 또한 영역 경로 테이블이 새로 고쳐집니다.

내부 영역 트래픽

트래픽이 하나의 인터페이스에 들어오고 동일한 영역에 있는 다른 인터페이스에서 나가도록 허용하려면 **same-security permit intra-interface** 명령을 활성화합니다. 이렇게 하면 트래픽이 동일한 인터페이스에 들어오고 나갈 수 있으며 **same-security permit inter-interface** 명령에서 동일한 보안 인터페이스 간에 트래픽을 허용할 수 있습니다. 그렇지 않으면, 흐름은 동일한 영역에 있는 2개의 인터페이스 간에 라우팅될 수 없습니다.

to-the-box 및 **from-the-box** 트래픽

- 영역에 관리 전용 또는 관리 액세스 인터페이스를 추가할 수 없습니다.
- 영역에 있는 일반 인터페이스의 관리 트래픽인 경우, 기존 흐름에서만 비대칭 라우팅이 지원되며 ECMP 지원은 없습니다.
- 1개의 영역 인터페이스에서만 관리 서비스를 구성할 수 있지만, 비대칭 라우팅 지원을 활용하려면 모든 인터페이스에서 이 기능을 구성해야 합니다. 구성이 모든 인터페이스에서 병렬인 경우에도 ECMP는 지원되지 않습니다.
- ASA는 영역에서 다음 to-the-box 및 from-the-box 서비스를 지원합니다.
  - 텔넷
  - SSH
  - HTTPS
  - SNMP
  - Syslog

영역에서 중복된 **IP** 주소

영역 비지정 인터페이스의 경우 NAT를 올바르게 구성한 경우에 한해 ASA는 인터페이스에서 중복 IP 주소 네트워크를 지원합니다. 그러나, 중복 네트워크는 동일한 영역에 있는 인터페이스에서 지원되지 않습니다.

트래픽 영역에 대한 사전 요건

- 이름, IP 주소, 보안 레벨 등 모든 인터페이스 매개변수를 구성합니다. 보안 수준이 영역에 있는 모든 인터페이스와 일치해야 합니다. 대역폭과 기타 Layer 2 속성의 기준에서 인터페이스와 마찬가지로 그룹화 계획을 세워야 합니다.
- 모든 영역 인터페이스에서 일치하도록 다음 서비스를 구성하십시오.
  - 액세스 규칙 — 모든 영역 멤버 인터페이스에 동일한 액세스 규칙을 적용하거나 전역 액세스 규칙을 사용합니다.

예를 들면 다음과 같습니다.

```
access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
access-group ZONE1 in interface outside1
access-group ZONE1 in interface outside2
access-group ZONE1 in interface outside3
```

- NAT — 영역의 모든 멤버 인터페이스에서 동일한 NAT 정책을 구성하거나 전역 NAT 규칙을 사용합니다(즉 NAT 규칙에서 영역 인터페이스를 나타내는 “any”를 사용합니다).

  인터페이스 PAT는 지원되지 않습니다.

  예를 들면 다음과 같습니다.

```
object network WEBSERVER1
  host 10.9.9.9 255.255.255.255
  nat (inside,any) static 209.165.201.9
```

  참고 인터페이스 특정 NAT 및 PAT 풀을 사용하는 경우 ASA에서는 원래 인터페이스 장애 시 연결을 전환할 수 없습니다.

  인터페이스 특정 PAT 풀을 사용하는 경우, 동일한 호스트의 여러 연결에서 다른 인터페이스에 로드 밸런싱을 조정하고 다른 매핑된 IP 주소를 사용합니다. 여러 동시 연결을 사용하는 인터넷 서비스는 이 경우 올바르게 작동하지 않을 수 있습니다.

- 서비스 규칙 — 전역 서비스 정책을 사용하거나 영역에 있는 각 인터페이스에 동일한 정책을 할당합니다.

  QoS 트래픽 폴리싱은 지원되지 않습니다.

  예를 들면 다음과 같습니다.

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

참고 VoIP 검사 시 영역 로드 밸런싱은 오류가 있는 패킷이 증가하는 원인이 될 수 있습니다. 이 상황은 최근 패킷이 다른 경로를 사용하는 초기 패킷보다 먼저 ASA에 도달하여 발생할 수 있습니다. 오류가 있는 패킷 증상은 다음과 같습니다.

- 중간 노드(방화벽 및 IDS)에서 높은 메모리 사용률 및 큐잉 사용 시 엔드 노드 수신
- 불량한 비디오 또는 음성 품질

이러한 영향을 줄이려면 VoIP 트래픽에 대한 로드 분산용으로만 IP 주소를 사용하는 것이 좋습니다.

- ECMP 영역 기능과 함께 라우팅을 구성해야 합니다.

트래픽 영역에 대한 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드 또는 라우팅 모드의 브리지 그룹 인터페이스를 지원하지 않습니다.

페일오버

- 영역에 장애 조치 또는 상태 링크를 추가할 수 없습니다.
- 활성/활성 장애 조치 모드에서, ASR(비대칭 라우팅) 그룹에 각 상황의 인터페이스를 할당할 수 있습니다. 이 서비스를 활용하면 원래 유닛으로 복원할 피어 유닛의 동일한 인터페이스에서 트래픽을 반환할 수 있습니다. 한 컨텍스트 내에서 ASR 그룹과 트래픽 영역을 모두 구성할 수 없습니다. 어떤 컨텍스트에서 영역을 구성할 경우 어떤 컨텍스트 인터페이스도 ASR 그룹의 일부가 될 수 없습니다. ASR 그룹에 대한 자세한 내용은 비대칭 라우팅 패킷을 위한 지원 구성(활성/활성 모드), 313 페이지를 참조하십시오.
- 각 연결에 대한 기본 인터페이스만 대기 유닛에 복제되며 현재 인터페이스는 복제되지 않습니다. 대기 유닛이 활성 상태가 되는 경우, 필요 시 새로운 현재 인터페이스를 할당합니다.

클러스터링

- 영역에 클러스터 제어 링크를 추가할 수 없습니다.

추가 지침

- 최대 256개의 영역을 만들 수 있습니다.

- 영역에 다음 유형의 인터페이스를 추가할 수 있습니다.
  - 물리적
  - VLAN
  - EtherChannel
  - 이중화
- 다음 유형의 인터페이스는 추가할 수 없습니다.
  - 관리 전용
  - 관리 액세스
  - 장애 조치 또는 상태 링크
  - 클러스터 제어 링크
  - EtherChannel 또는 이중 인터페이스의 멤버 인터페이스
  - VNI 또한 일반 데이터 인터페이스가 nve 전용으로 표시된 경우 영역의 멤버가 될 수 없습니다.
  - BVI 또는 브리지 그룹 멤버 인터페이스입니다.
- 인터페이스는 하나의 영역에만 속할 수 있습니다.
- 영역당 최대 8개의 인터페이스를 포함할 수 있습니다.
- ECMP의 경우 모든 영역 인터페이스 전체에서 영역당 최대 8개의 동일 비용 경로를 추가할 수 있습니다. 또한 8개의 경로 제한의 일부로 단일 인터페이스에 여러 경로를 구성할 수 있습니다.
- 영역에 인터페이스를 추가하는 경우 해당 인터페이스에 대한 고정 경로가 모두 제거됩니다.
- 영역의 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.

트래픽 영역 구성

명명된 영역을 구성하고 영역에 인터페이스를 지정합니다.

프로시저

단계 **1** 영역을 추가합니다.

zone *name*

예제**:**

```
zone outside
```

영역 이름은 길이가 최대 48자까지 가능합니다.

단계 **2** 영역에 인터페이스를 추가합니다.

interface *id* **zone-member** *zone_name*

예제**:**

```
interface gigabitethernet0/0
  zone-member outside
```

단계 **3** 영역에 다른 인터페이스를 추가합니다. 처음에 추가한 인터페이스와 동일한 보안 레벨이어야 합니다.

예제**:**

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

예

다음 예에서는 4개의 멤버 인터페이스가 있는 외부 영역을 구성합니다.

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

트래픽 영역 모니터링

이 섹션에서는 트래픽 영역을 모니터링하는 방법을 설명합니다.

영역 정보

- **show zone** [*name*]

영역 ID, 컨텍스트, 보안 레벨, 멤버를 표시합니다.

show zone 명령에 대해서는 다음 출력을 참조하십시오.

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  인터페이스 이름 및 영역 이름을 표시합니다.

  show nameif zone 명령에 대해서는 다음 출력을 참조하십시오.

```
ciscoasa# show nameif zone
Interface                Name                   zone-name      Security
GigabitEthernet0/0       inside-1               inside-zone     100
GigabitEthernet0/1.21    inside                 inside-zone     100
GigabitEthernet0/1.31    4                                        0
GigabitEthernet0/2       outside                outside-zone   0
Management0/0            lan                                      0
```

영역 연결

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  show conn zone 명령은 영역에 대한 연결을 표시합니다. **long** 및 **detail** 키워드는 연결이 설정된 기본 인터페이스 및 트래픽을 전달하는 데 사용되는 현재 인터페이스를 보여 줍니다.

  show conn long zone 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  디버깅을 위해 가속화된 보안 경로 테이블을 표시합니다.

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  영역 내 로컬 호스트의 네트워크 상태를 표시합니다.

  show local-host zone 명령에 대한 다음 출력을 참고하십시오. 기본 인터페이스가 먼저 나열되고 현재 인터페이스는 괄호로 표시됩니다.

```
ciscoasa# show local-host zone outside-zone
```

```
Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

영역 라우팅

- **show route zone**

  영역 인터페이스에 대한 경로를 표시합니다.

  show route zone 명령에 대해서는 다음 출력을 참조하십시오.

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

  디버깅을 위해 가속화된 보안 경로 테이블을 표시하며 각 경로와 연계된 영역을 표시합니다.

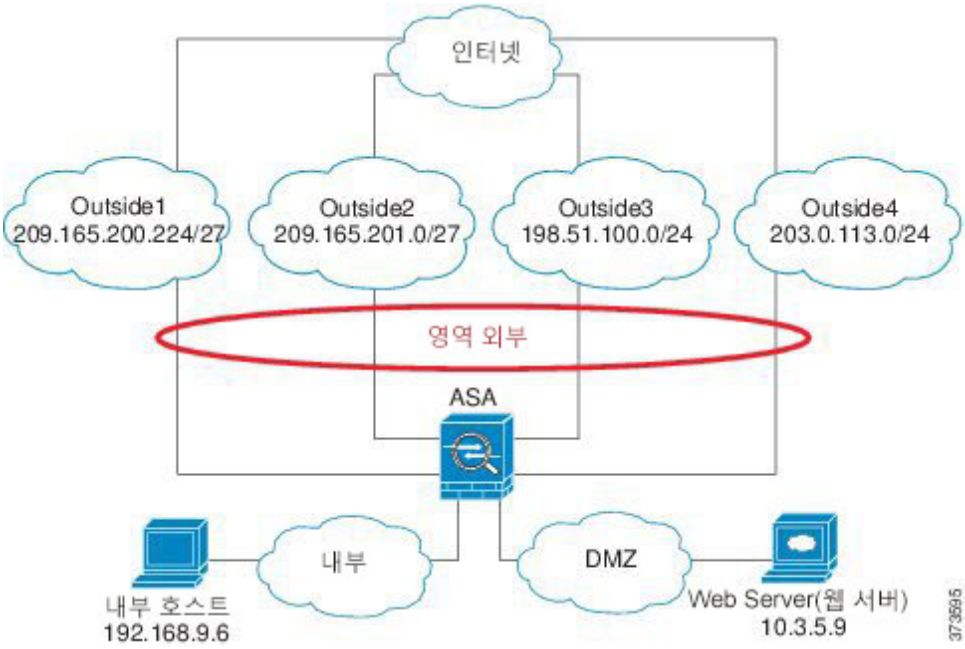
  show asp table routing 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
```

```
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

트래픽 영역 예

다음의 예에서는 외부 영역에 4개의 VLAN 인터페이스를 할당하고 4개의 동일 비용 기본 경로를 구성합니다. PAT는 내부 인터페이스용으로 구성되며 웹 서버는 정적 NAT를 사용하는 DMZ 인터페이스에서 사용할 수 있습니다.




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
```

```
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99
```

```
# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

트래픽 영역 내역

기능 이름	플랫폼 릴리스	설명
트래픽 영역	9.3(2)	인터페이스를 트래픽 영역으로 그룹화하여 여러 인터페이스를 대상으로 트래픽 로드 밸런싱(ECMP(Equal Cost Multi-Path) 라우팅 사용), 경로 이중화, 비대칭 라우팅을 구현할 수 있습니다. 참고 명명된 영역에는 보안 정책을 적용할 수 없으며, 보안 정책은 인터페이스를 기준으로 합니다. 영역의 인터페이스가 동일한 액세스 규칙, NAT, 서비스 정책으로 구성된 경우 로드 밸런싱 및 비대칭 라우팅이 올바르게 작동합니다. 도입 또는 수정된 명령: **zone**, **zone-member**, **show running-config zone**, **clear configure zone**, **show zone**, **showasp table zone**, **show nameif zone**, **show conn long**, **show local-host zone**, **show route zone**, **show asp table routing**, **clear conn zone**, **clear local-host zone**

IV 부

기본 설정

19 장

기본 설정

이 장에서는 일반적으로 구성의 원활한 작동에 필요한 ASA의 기본 설정을 구성하는 방법을 설명합니다.

호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정

호스트 이름, 도메인 이름, enable 및 텔넷 비밀번호를 설정하려면 다음 단계를 수행합니다.

시작하기 전에

호스트 이름, 도메인 이름, enable 및 텔넷 비밀번호를 설정하기 전에 먼저 다음 요구사항을 확인합니다.

- 다중 컨텍스트 모드에서는 시스템 및 컨텍스트 실행 영역 모두에서 호스트 이름과 도메인 이름을 구성할 수 있습니다.
- enable 비밀번호와 텔넷 비밀번호는 각 컨텍스트에서 설정합니다. 시스템에서는 사용할 수 없습니다. 다중 상황 모드에서 스위치로부터 ASASM으로 세션을 연결할 때 ASASM에서는 관리 상황에서 설정한 로그인 비밀번호를 사용합니다.
- 시스템에서 컨텍스트 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

프로시저

단계 **1** ASA 또는 어떤 상황을 위한 호스트 이름을 지정합니다. 기본 호스트 이름은 “asa”입니다.

hostname *name*

예제**:**

```
ciscoasa(config)# hostname myhostnamexample12345
```

이 이름은 최대 63자입니다. 호스트 이름은 문자 또는 숫자로 시작하고 끝나야 하며 문자, 숫자 또는 하이픈만 사용할 수 있습니다.

ASA를 위한 호스트 이름을 설정하면 해당 이름이 명령줄 프롬프트에 나타납니다. 여러 디바이스와의 세션을 설정한 경우 호스트 이름은 명령을 입력할 위치를 추적하는 데 도움이 됩니다.

다중 컨텍스트 모드에서는 시스템 실행 영역에서 설정한 호스트 이름이 모든 컨텍스트의 명령줄 프롬프트에 나타납니다. 어떤 컨텍스트 내에서 선택적으로 설정한 호스트 이름은 명령줄에 나타나지 않지만, **banner** 명령 **$(hostname)** 토큰을 통해 사용할 수 있습니다.

단계 **2** ASA의 도메인 이름을 지정합니다. 기본 도메인 이름은 default.domain.invalid입니다.

domain-name *name*

예제**:**

```
ciscoasa(config)# domain-name example.com
```

ASA에서는 도메인 이름을 정규화되지 않은 이름에 접미사로 추가합니다. 예를 들어, 도메인 이름을 “example.com”으로 설정하고 “jupiter”라는 정규화되지 않은 이름으로 syslog 서버를 지정하는 경우 ASA에서는 해당 이름을 “jupiter.example.com”으로 정규화합니다.

단계 **3** enable 비밀번호를 변경합니다. 기본적으로 enable 비밀번호는 비어을 처음 입력하면 비밀번호를 변경하라는 프롬프트가 표시됩니다.

enable password *password*

예제**:**

```
ciscoasa(config)# enable password Pa$$w0rd
```

enable 인증을 구성하지 않은 경우 enable 비밀번호를 사용하여 특별 권한 EXEC 모드를 시작할 수 있습니다. 또한 enable 비밀번호는 HTTP 인증을 구성하지 않은 경우에 빈 사용자 이름으로 ASDM에 로그인할 수 있게 합니다.

password 인수는 최대~127자 길이의 대/소문자를 구분하는 비밀번호로, 공백 및 물음표를 제외하고 ASCII 인쇄 가능 문자(문자 코드 32~126)의 조합을 사용할 수 있습니다.

이 명령은 최고 권한 레벨(15)의 비밀번호를 변경합니다. 로컬 명령 권한 부여를 구성한 경우 다음 구문을 사용하여 0부터 15까지의 각 권한 레벨에 enable 비밀번호를 설정할 수 있습니다.

enable password *password* **level** *number*

encrypted 키워드(9.6 이하 버전에서 32자 이하의 비밀번호용) 또는 **pbkdf2** 키워드(9.6 이상 버전에서 32자 보다 긴 비밀번호 및 9.7 이상 버전에서 모든 길이의 비밀번호용)는 비밀번호가 암호화되어 있음을 나타냅니다(MD5 기반 해시 또는 PBKDF2(비밀번호 기반 키 파생 함수 2) 해시 사용). 새 비밀번호를 입력하지 않는 한, 기존 비밀번호에서는 MD5 기반 해시를 계속해서 사용합니다. **enable password** 명령에서 비밀번호를 정의하는 경우 ASA에서는 비밀번호를 구성에 저장할 때 암호화하여 보안을 강화합니다. **show running-config** 명령을 입력하면 **enable password** 명령에서는 실제 비밀번호를 표시하지 않습니다. 암호화된 비밀번호 뒤에 **encrypted** 또는 **pbkdf2** 키워드가 표시됩니다. 예를 들어 "test"라는 비밀번호를 입력할 경우 다음과 비슷한 내용의 **show running-config** 명령 출력이 표시됩니다.

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

CLI에서 **encrypted** 또는 **pbkdf2** 키워드를 실제로 입력하는 유일한 경우는 다른 ASA에서 사용할 구성 파일을 잘라서 붙여넣은 다음, 동일한 비밀번호를 사용하는 경우입니다.

비밀번호를 기본값으로 설정하려면, 즉 비워 두려면 어떤 비밀번호도 없이 **enable password** 명령을 입력합니다.

단계 **4** 텔넷 액세스를 위한 로그인 비밀번호를 설정합니다. 비밀번호는 기본값이 없습니다.

로그인 비밀번호는 텔넷 인증을 구성하지 않은 경우 텔넷 액세스에 사용됩니다. **session** 명령을 사용하여 스위치에서 ASASM에 액세스할 때도 이 비밀번호를 사용합니다.

{**passwd** | **password**} *password* [**encrypted**]

예제**:**

```
ciscoasa(config)# password cisco12345
```

passwd 또는 **password**를 입력할 수 있습니다. *password*는 대/소문자를 구분하는 비밀번호이며 영숫자와 특수 문자를 사용하여 최대 16자까지 가능합니다. 물음표와 공백을 제외한 어떤 문자도 비밀번호에 사용할 수 있습니다.

비밀번호는 암호화된 형태로 컨피그레이션에 저장되므로 비밀번호를 입력하더라도 원래의 비밀번호를 볼 수 없습니다. 어떤 이유로든 다른 ASA에 비밀번호를 복사해야 하는데 원래의 비밀번호를 모르는 경우 **passwd** 명령을 암호화된 비밀번호 및 **encrypted** 키워드와 함께 입력할 수 있습니다. 일반적으로 **show running-config passwd** 명령을 입력해야 이 키워드를 볼 수 있습니다.

날짜 및 시간 설정

참고 ASASM 또는 Firepower 9300 ASA 보안 모듈에 날짜 및 시간을 설정하지 마십시오. 호스트 디바이스에서 이러한 설정을 수신합니다.

시간대 및 일광 절약 날짜 설정

표준 시간대 및 날짜 범위를 설정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 표준 시간대를 설정합니다. 기본적으로, 시간대는 UTC이며 일광 절약 시간 날짜 범위는 4월의 첫 일요일 오전 2:00시에서 10월의 마지막 일요일 오전 2:00시까지입니다.

clock timezone *zone* [-]*hours* [*minutes*]

예제**:**

```
ciscoasa(config)# clock timezone PST -8
```

zone 인수는 표준 시간대를 문자열로 지정합니다(예: PST는 태평양 표준시).

[-]*hours* 값은 UTC에서 차감할 시간을 설정합니다. 예를 들어, PST는 -8시간입니다.

minutes 값은 UTC에서 차감할 분을 설정합니다.

단계 **2** 일광 절약 시간의 날짜 범위를 기본값에서 변경하려면 다음 명령 중 하나를 입력합니다. 기본 반복 날짜 범위는 3월의 두 번째 일요일 오전 2:00시부터 11월의 첫 번째 일요일 오전 2:00시까지 입니다.

- 일광 절약 시간의 시작일과 종료일을 특정 연도의 특정 날짜로 설정합니다. 이 명령을 사용하는 경우 매년 날짜를 재설정해야 합니다.

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

  예:

  ```
  ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
  ```

  zone 값은 표준 시간대를 문자열로 지정합니다(예: PDT는 태평양 일광 절약 시간).

  day 값은 1~31 범위의 일을 설정합니다. 표준 날짜 형식에 따라 일과 월을 **A**pril 1 또는 1 April과 같이 입력할 수 있습니다.

  month 값은 월을 문자열로 설정합니다. 표준 날짜 형식에 따라 일과 월을 April 1 또는 1 April과 같이 입력할 수 있습니다.

  year 값은 4자리 숫자를 사용하여 연도를 설정합니다(예: 2004). 연도 범위는 1993~2035입니다.

  hh:mm 값은 시간과 분을 24시간 표시로 설정합니다.

  offset 값은 일광 절약 시간을 위해 변경할 시간(분)을 설정합니다. 기본값은 60분입니다.

- 일광 절약 시간의 시작일과 종료일을 어떤 연도의 특정 날짜가 아닌 해당 월의 요일 및 시각 형식으로 지정합니다. 이 명령으로 매년 변경할 필요 없는 반복 날짜 범위를 설정할 수 있습니다.

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

예:

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

zone 값은 표준 시간대를 문자열로 지정합니다(예: PDT는 태평양 일광 절약 시간).

week 값은 해당 월의 주를 1~4의 정수 혹은 first 또는 last로 지정합니다. 예를 들어, 어떤 날이 부분적 5번째 주에 속할 경우 last라고 지정합니다.

weekday 값은 요일을 지정합니다(예: Monday, Tuesday, Wednesday 등).

month 값은 월을 문자열로 설정합니다.

hh:mm 값은 시간과 분을 24시간 표시로 설정합니다.

offset 값은 일광 절약 시간을 위해 변경할 시간(분)을 설정합니다. 기본값은 60분입니다.

NTP 서버를 사용하여 날짜 및 시간 설정

NTP는 네트워크 시스템 간에 정확하게 동기화된 시간을 제공하는 계층적 서버 시스템을 구현하는 데 사용합니다. 정밀한 타임 스탬프가 포함된 CRL 검증과 같이 시간에 민감한 작업에는 이러한 정확성이 필요합니다. 여러 NTP 서버를 구성할 수 있습니다. ASA는 데이터의 신뢰도 지표인 stratum이 가장 낮은 서버를 선택합니다.

NTP 서버에서 가져온 시간은 직접 설정한 어떤 시간도 재정의합니다.

시작하기 전에

다중 상황 모드에서는 시스템 컨피그레이션에서만 시간을 설정할 수 있습니다.

프로시저

단계 **1** NTP 서버를 통한 인증을 활성화합니다.

ntp authenticate

예제**:**

```
ciscoasa(config)# ntp authenticate
```

NTP 인증을 활성화할 경우, **ntp trusted-key** 명령에서 키 ID도 지정하고 이 키를 **ntp server key** 명령을 사용하여 서버에 연결해야 합니다. **ntp authentication-key** 명령을 사용하여 ID의 실제 키를 구성합니다. 여러 서버를 사용하는 경우 각 서버의 개별 ID를 구성합니다.

단계 **2** 신뢰 키가 될 인증 키 ID를 지정합니다. 이는 NTP 서버와의 인증에 필요합니다.

ntp trusted-key *key_id*

예제**:**

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

key_id 인수는 1~4294967295 범위의 값입니다. 여러 서버에서 사용할 수 있도록 여러 신뢰 키를 입력할 수 있습니다.

단계 **3** NTP 서버와 인증하기 위한 키를 설정합니다.

ntp authentication-key *key_id* **md5** *key*

예제**:**

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

key_id 인수는 **ntp trusted-key** 명령으로 설정한 ID이고 *key* 인수는 최대 길이가 32자인 문자열입니다.

단계 **4** NTP 서버를 지정합니다.

ntp server*ipv4_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

예제**:**

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
```

NTP 인증(**ntp authenticate**)을 활성화한 경우, **ntp trusted-key** 명령을 사용하여 설정한 ID를 사용하여 **key** *key_id* 인수를 지정해야 합니다.

source *interface_name* 키워드-인수 쌍은 라우팅 테이블의 기본 인터페이스를 사용하지 않을 경우 NTP 패킷의 발신 인터페이스를 식별합니다. 다중 컨텍스트 모드에서는 어떤 인터페이스도 포함하지 않으므로 관리 컨텍스트에 정의된 인터페이스 이름을 지정합니다.

prefer 키워드를 사용하면 여러 서버의 정확도가 비슷할 경우 이 NTP 서버가 기본 서버로 설정됩니다. NTP는 알고리즘을 사용하여 어떤 서버가 가장 정확한지 알아내고 그 서버와 동기화합니다. 서버의 정확도가 비슷할 경우 **prefer** 키워드로 이러한 서버 중에서 사용할 서버를 지정합니다. 그러나 어떤 서버가 기본 서버보다 훨씬 더 정확할 경우 ASA는 더 정확한 쪽을 사용합니다. 예를 들어, ASA는 기본 서버인 stratum 3 서버 대신 stratum 2 서버를 사용합니다.

여러 서버를 지정할 수 있습니다. ASA는 가장 정확한 서버를 사용합니다.

날짜 및 시간 직접 설정

날짜와 시간을 직접 설정하려면 다음 단계를 수행합니다.

시작하기 전에

다중 컨텍스트 모드에서는 시스템 컨피그레이션에서만 시간을 설정할 수 있습니다.

프로시저

날짜 및 시간을 직접 설정합니다.

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

예제:

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:*mm*:*ss* 인수는 시간, 분, 초를 24시간 형식으로 설정합니다. 예를 들어, 오후 8:54는 20:54:00으로 입력합니다.

day 값은 1~31 범위의 일을 설정합니다. 표준 날짜 형식에 따라 일과 월을 april 1 또는 1 april과 같이 입력할 수 있습니다.

month 값은 월을 설정합니다. 표준 날짜 형식에 따라 일과 월을 april 1 또는 1 april과 같이 입력할 수 있습니다.

year 값은 4자리 숫자를 사용하여 연도를 설정합니다(예: 2004). 연도 범위는 1993~2035입니다.

기본 표준 시간대는 UTC입니다. **clock set** 명령을 입력한 후 **clock timezone** 명령을 사용하여 표준 시간대를 변경하면 자동으로 새 표준 시간대에 맞게 시간이 조정됩니다.

이 명령은 하드웨어 칩의 시간을 설정하며, 컨피그레이션 파일에 시간을 저장하지 않습니다. 이 시간은 재부팅해도 유지됩니다. 다른 **clock** 명령과 달리 이 명령은 특별 권한 EXEC 명령입니다. 시계를 재설정하려면 clock set 명령으로 새 시간을 설정해야 합니다.

PTP를 사용하여 날짜 및 시간 동기화(ISA 3000)

PTP(Precision Time Protocol)는 패킷 기반 네트워크에서 다양한 디바이스의 클록을 동기화하기 위해 개발된 시간 동기화 프로토콜이며 이러한 디바이스 클록은 일반적으로 정확성과 안정성이 다양합니다. 이 프로토콜은 산업, 네트워크에 연결된 측정 및 제어 시스템을 위해 특별히 설계되었으며 최소한의 대역폭 및 적은 처리 오버헤드를 필요로 하기 때문에 분산 시스템에서 사용하기에 가장 적합합니다.

PTP 시스템은 PTP 및 비 PTP 디바이스의 조합으로 구성된 분산형, 네트워크에 연결된 시스템입니다. PTP 디바이스에는 일반 클록, 경계 클록 및 투명 클록이 있습니다. 비 PTP 디바이스에는 네트워크 스위치, 라우터 및 기타 인프라 디바이스가 있습니다.

참고 검사를 위해 PTP 트래픽이 ASA FirePOWER 모듈에 전송되지 않았는지 확인하기 위해 다음 명령을 ASA 기본 구성에 추가했습니다. 기존 구축의 경우 다음 명령을 수동으로 추가해야 합니다.

```
object-group service bypass_sfr_inspect
service-object udp destination range 319 320
access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any
```

시작하기 전에

- 이 기능은 Cisco ISA 3000 어플라이언스에서만 사용할 수 있습니다.
- PTP 사용은 단일 상황 모드에서만 지원됩니다.
- Cisco PTP는 멀티캐스트 PTP 메시지만 지원합니다.
- PTP는 투명 모드의 모든 ISA 3000 인터페이스에서 기본적으로 활성화되어 있습니다. 라우팅 모드에서 PTP 패킷이 디바이스를 통해 이동할 수 있도록 필수 구성을 추가해야 합니다.
- PTP는 IPv4 네트워크용으로만 사용할 수 있으며 IPv6 네트워크용으로는 사용할 수 없습니다.
- PTP 구성은 모든 물리적 이더넷 인터페이스에서 지원됩니다. 다음에서는 지원되지 않습니다.
  - 관리 인터페이스
  - 하위 인터페이스, 채널 그룹, BVI 또는 기타 가상 인터페이스
- VLAN 하위 인터페이스에서 이동하는 PTP가 지원되며 이때 적절한 PTP 구성이 현재 상위 인터페이스에 있다고 가정합니다.
- PTP 패킷이 디바이스를 통해 이동할 수 있는지 확인해야 합니다. 투명 방화벽 모드에서 PTP 트래픽을 허용하기 위한 액세스 목록 구성이 기본적으로 구성됩니다. PTP 트래픽은 UDP 포트 319 및 320과 대상 IP 주소 224.0.1.129로 식별되므로 라우팅 방화벽 모드에서는 이 트래픽을 허용하는 ACL이 허용되어야 합니다.

  라우팅 방화벽 모드에서는 PTP 멀티캐스트 그룹에 대해 멀티캐스트 라우팅도 활성화해야 합니다.
  - 전역 구성 모드의 **multicast-routing** 명령을 입력합니다.
  - PTP가 활성화되어 있는 각 인터페이스에서 PTP 멀티캐스트 그룹 멤버십을 정적으로 활성화하려면 인터페이스 구성 명령인 **igmp join-group 224.0.1.129**를 입력합니다.

PTP 시간 동기화를 활성화하려면 다음 단계를 따르십시오.

프로시저

단계 **1** 디바이스의 모든 포트의 도메인 수를 지정합니다.

ptp domain *domain_num*

예제:

```
ciscoasa(config)# ptp domain 54
```

domain_num 인수는 디바이스에 있는 모든 포트의 도메인 수입니다. 다른 도메인에서 수신한 패킷은 일반 멀티캐스트 패킷으로 처리되며 PTP 처리를 거치지 않습니다. 이 값의 범위는 0~255이며 기본값은 0입니다.

단계 **2** (선택 사항) 디바이스에서 PTP 클록 모드를 구성합니다.

ptp mode e2etransparent

예제:

```
ciscoasa(config)# ptp mode e2etransparent
```

이 명령을 사용하면 모든 PTP 활성화 인터페이스에서 엔드 투 엔드 투명 모드가 활성화됩니다.

단계 **3** 인터페이스에서 PTP를 활성화합니다.

ptp enable

예제:

```
ciscoasa(config)# interface gigabitethernet1/2
ciscoasa(config-if)# ptp enable
```

마스터 패스프레이즈 구성

마스터 패스프레이즈를 사용하면 일반 텍스트 비밀번호를 암호화된 형식으로 안전하게 저장할 수 있습니다. 또한 제공되는 키를 사용하여 기능 변경 없이 모든 비밀번호를 종합적으로 암호화하거나 마스킹할 수 있습니다. 다음과 같은 기능에서 마스터 패스프레이즈를 사용합니다.

- OSPF
- EIGRP
- VPN 로드 밸런싱
- VPN(원격 액세스 및 사이트 대 사이트)
- 장애 조치
- AAA 서버
- 로깅
- SHARED 라이센스

마스터 패스프레이즈 추가 또는 변경

마스터 패스프레이즈를 추가하거나 변경하려면 다음 단계를 수행합니다.

시작하기 전에

- 이 절차는 보안 세션(예: 콘솔, SSH, HTTPS를 통한 ASDM)에서만 가능합니다.
- 장애 조치가 활성화되었지만 장애 조치 공유 키가 설정되지 않은 경우, 마스터 패스프레이즈를 변경하면 오류 메시지가 나타나 마스터 패스프레이즈 변경 사항이 일반 텍스트로 전송되지 않게 하려면 장애 조치 공유 키를 입력해야 함을 알립니다.
- 액티브/스탠바이 장애 조치에서 비밀번호 암호화를 활성화하거나 변경하여 **write standby**가 발생할 수 있으며 이로 인해 액티브 구성이 스탠바이 유닛에 복제됩니다. 복제를 수행하지 않으면 스탠바이 유닛에서 암호화된 비밀번호가 동일한 패스프레이즈를 사용하는 경우에도 달라지는 반면, 구성 복제를 수행하면 동일한 구성이 보장됩니다. 액티브/액티브 장애 조치를 위해 **write standby**를 직접 입력해야 합니다. 새 구성이 동기화되기 전에 보조 유닛에서 구성이 지워지므로 **write standby**로 인해 액티브/액티브 모드에서 트래픽이 중단될 수 있습니다. **failover active group 1** 및 **failover active group 2** 명령을 사용하여 기본 ASA에서 모든 상황을 액티브 상태로 설정한 다음 **write standby**를 입력하고 **no failover active group 2** 명령을 사용하여 보조 유닛으로 그룹 2 상황을 복원해야 합니다.

프로시저

단계 **1** 암호화 키를 생성하는 데 사용한 패스프레이즈를 설정합니다. 암호는 6자에서 128자 사이여야 합니다. 백스페이스와 큰따옴표를 제외한 모든 문자를 패스프레이즈에 사용할 수 있습니다. 명령에 새 패스프레이즈를 입력하지 않으면 입력하라는 메시지가 나타납니다. 패스프레이즈를 변경하려면 이전 패스프레이즈를 입력해야 합니다.

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

예제**:**

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

참고 비밀번호가 명령 기록 버퍼에 로깅되지 않도록 대화형 프롬프트에서 비밀번호를 입력합니다.

no key config-key password-encrypt 명령을 사용할 때는 주의해야 합니다. 암호화된 비밀번호가 일반 텍스트 비밀번호로 바뀌기 때문입니다. 비밀번호 암호화를 지원하지 않는 소프트웨어 버전으로 다운그레이드할 때는 이 명령의 **no** 형식을 사용할 수 있습니다.

단계 **2** 비밀번호 암호화를 활성화합니다.

password encryption aes

예제**:**

```
ciscoasa(config)# password encryption aes
```

비밀번호 암호화가 활성화되고 마스터 패스프레이즈가 사용 가능해지는 즉시 모든 사용자 비밀번호가 암호화됩니다. 실행 중인 컨피그레이션에서는 암호화된 형식으로 비밀번호를 표시합니다.

비밀번호 암호화가 활성화된 시점에 패스프레이즈가 구성되지 않은 경우, 나중에 패스프레이즈가 만들어질 것으로 예상하면서 이 명령은 성공합니다.

나중에 **no password encryption aes** 명령을 사용하여 비밀번호 암호화를 비활성화하면, 기존의 모든 암호화된 비밀번호는 바뀌지 않습니다. 그리고 마스터 패스프레이즈가 있는 한, 암호화된 비밀번호는 애플리케이션의 요구 사항에 따라 해독됩니다.

단계 **3** 마스터 패스프레이즈의 런타임 값 및 그 결과 컨피그레이션을 저장합니다.

write memory

예제**:**

```
ciscoasa(config)# write memory
```

이 명령을 입력하지 않으면, 시작 컨피그레이션의 비밀번호가 이전에 암호화되어 저장되지 않았다면 이 비밀번호가 계속 표시될 수 있습니다. 또한 다중 컨텍스트 모드에서는 시스템 컨텍스트 컨피그레이션에서 마스터 패스프레이즈가 변경됩니다. 따라서 모든 컨텍스트의 패스프레이즈가 영향을 받습니다. write memory 명령이 시스템 컨텍스트 모드에서 입력되었지만 모든 사용자 컨피그레이션에서 입력되지는 않았다면, 사용자 컨피그레이션의 암호화된 비밀번호는 부실화될 수 있습니다. 또는 시스템 컨텍스트에서 write memory all 명령을 사용하여 모든 컨피그레이션을 저장합니다.

예

다음 예는 어떤 키도 없었음을 보여줍니다.

```
ciscoasa(config)# key config-key password-encryption 12345678
```

다음 예는 키가 이미 있음을 보여줍니다.

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

다음 예에서는 매개 변수 없이 명령을 입력하기 때문에 키를 묻는 프롬프트가 표시됩니다. 키가 이미 있으므로 그에 대한 메시지가 나타납니다.

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

다음 예에서는 기존 키가 없으므로 이를 묻는 메시지가 나타나지 않습니다.

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
```

```
Confirm key: 12345678
```

마스터 패스프레이즈 비활성화

마스터 패스프레이즈를 비활성화하면 암호화된 비밀번호가 일반 텍스트 비밀번호로 돌아갑니다. 암호화된 비밀번호를 지원하지 않는 이전 소프트웨어 버전으로 다운그레이드하는 경우 패스프레이즈 삭제 기능이 유용할 수 있습니다.

시작하기 전에

- 마스터 패스프레이즈를 비활성화하려면 현재 마스터 패스프레이즈를 알아야 합니다. 패스프레이즈를 모르는 경우 마스터 패스프레이즈 삭제, 693 페이지의 내용을 참조하십시오.
- 이 절차는 텔넷, SSH, HTTPS를 통한 ASDM과 같은 보안 세션에서만 가능합니다.

  마스터 패스프레이즈를 비활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 마스터 패스프레이즈를 삭제합니다. 명령에 패스프레이즈를 입력하지 않으면 입력하라는 메시지가 나타납니다.

no key config-key password-encryption [*old_passphrase*]]

예제:

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

단계 **2** 마스터 패스프레이즈의 런타임 값 및 그 결과 컨피그레이션을 저장합니다.

write memory

예제:

```
ciscoasa(config)# write memory
```

패스프레이즈가 들어 있는 비휘발성 메모리가 지워지고 0xFF 패턴으로 덮어쓰기됩니다.

또한 다중 컨텍스트 모드에서는 시스템 컨텍스트 컨피그레이션에서 마스터 패스프레이즈가 변경됩니다. 따라서 모든 컨텍스트의 패스프레이즈가 영향을 받습니다. write memory 명령이 시스템 컨텍스트 모드에서 입력되었지만 모든 사용자 컨피그레이션에서 입력되지는 않았다면, 사용자 컨텍스트의

암호화된 비밀번호는 부실화될 수 있습니다. 또는 시스템 컨텍스트에서 write memory all 명령을 사용하여 모든 컨피그레이션을 저장합니다.

마스터 패스프레이즈 삭제

마스터 패스프레이즈를 복구할 수 없습니다. 마스터 패스프레이즈를 잊었거나 알 수 없는 경우 이를 삭제할 수 있습니다.

마스터 패스프레이즈를 제거하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 마스터 키 및 암호화된 비밀번호가 들어 있는 컨피그레이션을 삭제합니다.

write erase

예제**:**

```
ciscoasa(config)# write erase
```

단계 **2** 마스터 키 또는 암호화된 비밀번호가 없는 시작 구성으로 ASA를 다시 로드합니다.

reload

예제**:**

```
ciscoasa(config)# reload
```

DNS 서버 구성

ASA에서 호스트 이름의 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다. 또한 액세스 규칙에서 FQDN(Fully Qualified Domain Name) 네트워크 객체를 사용하려면 DNS 서버를 구성해야 합니다.

일부 ASA 기능에서는 도메인 이름으로 외부 서버에 액세스하려면 DNS 서버를 사용해야 합니다. 예를 들어, 봇넷 트래픽 필터 기능은 동적 데이터베이스 서버에 액세스하고 정적 데이터베이스의 항목을 확인하는 데 DNS 서버가 필요합니다. **ping** 또는 **traceroute** 명령과 같은 기타 기능에서는 ping하거나 트레이스라우트(traceroute)하려는 이름을 입력할 수 있는데, ASA에서는 DNS 서버와 통신하면서 해당 이름을 확인합니다. 여러 SSL VPN 및 인증 명령도 이름을 지원합니다.

참고 ASA는 기능에 따라 DNS 서버 사용을 제한적으로 지원합니다.예를 들어, 대부분의 명령에서는 IP 주소를 입력해야 하며, 이름과 IP 주소를 연결하기 위해 **name** 명령을 직접 구성하는 경우 이름만 사용할 수 있고 names 명령을 사용하여 names의 사용을 활성화할 수 있습니다.

시작하기 전에

DNS 서버에 연결할 수 있도록 DNS 도메인 조회를 활성화하는 모든 인터페이스에 적합한 라우팅 및 액세스 규칙을 구성해야 합니다.

프로시저

단계 **1** ASA에서 지원되는 명령에서 이름 조회가 가능하도록 DNS 서버에 DNS 요청을 보낼 수 있게 합니다.

dns domain-lookup *interface_name*

예제**:**

```
ciscoasa(config)# dns domain-lookup inside
```

인터페이스에서 DNS 조회를 활성화하지 않는 경우 DNS 서버 소스 인터페이스 또는 라우팅 테이블을 사용하여 찾은 인터페이스를 사용할 수 없습니다.

단계 **2** ASA에서 발신 요청에 사용하는 DNS 서버 그룹을 지정합니다.

dns server-group DefaultDNS

예제**:**

```
ciscoasa(config)# dns server-group DefaultDNS
```

VPN 터널 그룹을 위해 다른 DNS 서버 그룹을 구성할 수 있습니다. 자세한 내용은 명령 참조에서 **tunnel-group** 명령을 참고하십시오.

단계 **3** 하나 이상의 DNS 서버를 지정합니다. 6개의 IP 주소 모두 동일한 명령에 입력하고 공백으로 구분하거나 각 명령을 따로 입력할 수 있습니다. ASA는 응답을 받을 때까지 각 DNS 서버를 순서대로 시도합니다.

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] *[interface_name]*

예제**:**

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6 dmz
```

(선택 사항) ASA가 서버와 통신하는 데 사용되는 *interface_name*을 지정합니다. 인터페이스를 지정하지 않은 경우 ASA는 데이터 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 관리 전용 라우팅 테이블을 확인합니다.

단계 **4** 도메인 이름이 정규화되지 않은 경우 호스트 이름에 추가할 도메인 이름을 구성합니다.

domain-name *name*

예제**:**

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

단계 **5** (선택 사항). DNS 서버 그룹의 추가 속성을 구성합니다.

기본 설정이 네트워크에 적합하지 않은 경우, 다음 명령을 사용하여 그룹 특성을 변경합니다.

- **timeout** *seconds* — 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. ASA가 서버 목록을 재시도할 때마다 이 시간제한이 두 배가 됩니다.
- **retries** *number* — ASA가 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수(0~10회)입니다.
- **expire-entry-timer minutes** *number* — DNS 항목 만료(TTL이 경과함) 이후의 시간(분)으로, DNS 조회 테이블에서 항목이 제거됩니다. 항목 제거 시 테이블을 다시 컴파일해야 하므로 자주 제거하면 디바이스의 처리 부하가 증가할 수 있습니다. 일부 DNS 항목은 매우 짧은 TTL(3초 정도)을 가질 수 있으므로 이 설정을 사용하여 TTL을 가상으로 늘릴 수 있습니다. 기본값은 1분입니다(즉, TTL이 경과한지 1분 이후에 항목이 제거됨). 범위는 1~65535분입니다. 이 옵션은 FQDN 네트워크 객체를 해석할 때만 사용됩니다.
- **poll-timer minutes** *number* — FQDN 네트워크/호스트 개체의 IP 주소를 확인하는 데 사용되는 폴링 주기의 시간(분)입니다. FQDN 객체는 방화벽 정책에서 사용되는 경우에만 확인됩니다. 타이머는 최대 확인 주기를 결정합니다. DNS 항목의 TTL(Time to Live) 값은 또한 IP 주소 확인으로 업데이트해야 할 시기를 결정하는 데 사용되므로 개별 FQDN은 폴링 주기보다 더 자주 확인될 수 있습니다. 기본값은 240분(4시간)입니다. 범위는 1~65535분입니다.

하드웨어 우회 및 듀얼 전력 공급 장치 구성(Cisco ISA 3000)

정전 상태에서도 인터페이스 쌍 간에 트래픽 플로우가 계속되도록 하드웨어 우회를 활성화할 수 있습니다. 지원되는 인터페이스 쌍은 구리 GigabitEthernet 1/1 및 1/2, GigabitEthernet 1/3 및 1/4입니다. 하드웨어 우회가 액티브 상태인 경우, 방화벽 기능은 없으므로 트래픽의 통과를 허용하는 경우의 위험을 파악해야 합니다. 다음 하드웨어 우회 지침을 참조하십시오.

- 이 기능은 Cisco ISA 3000 어플라이언스에서만 사용할 수 있습니다.
- 파이버 이더넷 모델을 사용하는 경우에는 구리 이더넷 쌍(GigabitEthernet 1/1 및 1/2)만 하드웨어 우회를 지원합니다.
- ISA 3000이 정전되고 하드웨어 우회 모드로 전환되는 경우, 지원되는 인터페이스 쌍을 통해서만 통신할 수 있습니다. 기본 구성을 사용 중인 경우, inside1 <---> inside2 및 outside1 <---> outside2는 더 이상 통신할 수 없습니다. 이러한 인터페이스 간에 모든 기존 연결이 손실됩니다.

- 이 절차에서 설명하는 대로 TCP 시퀀스 임의 설정을 비활성화하는 것이 좋습니다. 임의 설정이 활성화된 경우(기본값) 하드웨어 우회가 활성화된 상태이면 TCP 세션을 다시 설정해야 합니다. 기본적으로 ISA 3000을 통과하는 TCP 연결의 ISN(초기 시퀀스 번호)는 임의의 숫자로 재작성됩니다. 하드웨어 우회가 활성화된 경우 ISA 3000은 더 이상 데이터 경로에 없으며 시퀀스 번호를 변환하지 않습니다. 수신 클라이언트는 예기치 않은 시퀀스 번호를 수신하며 연결을 끊습니다. TCP 시퀀스 임의 설정을 비활성화하더라도 전환 중에 일시적으로 중단되는 링크 때문에 일부 TCP 연결은 다시 설정해야 합니다.
- 하드웨어 우회가 활성화된 경우 하드웨어 우회 인터페이스에서 Cisco TrustSec 연결이 끊어집니다. ISA 3000의 전원이 켜져 있고 하드웨어 우회가 비활성화된 경우, 연결이 재협상됩니다.
- 하드웨어 우회가 비활성화된 경우 트래픽은 ISA 3000 데이터 경로를 통과하는 작업을 재개하며, 전환 중에 일시적으로 중단되는 링크 때문에 일부 기존 TCP 세션은 재설정되어야 합니다.
- 하드웨어 우회가 활성화된 경우, 이더넷 PHY의 연결이 끊어지므로 ASA에서 인터페이스 상태를 확인할 수 없습니다. 인터페이스는 작동 중단 상태로 표시될 수 있습니다.

ISA 3000의 듀얼 전원 공급 장치의 경우 ASA OS의 예상 구성대로 듀얼 전원 공급 장치를 설정할 수 있습니다. 1개의 전원 공급 장치에 장애가 발생하면 ASA는 알람을 발행합니다. 기본적으로 ASA는 단일 전원 공급 장치를 예상하며 하나의 작업 중인 전원 공급 장치를 포함하는 한 알람을 발행하지 않습니다.

시작하기 전에

- 스위치의 액세스 포트에 하드웨어 우회 인터페이스를 연결해야 합니다. 트렁크 포트에는 인터페이스를 연결하지 마십시오.

프로시저

단계 **1** 정전 중에 활성화하려면 하드웨어 우회를 구성합니다.

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

예제**:**

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

sticky 키워드를 사용하면 전력이 복구되고 어플라이언스가 부팅된 후 어플라이언스가 하드웨어 우회 모드로 유지됩니다. 이 경우 준비가 되면 하드웨어 우회를 수동으로 해제해야 하며 이 옵션을 사용하여 트래픽에 잠시 중단이 발생하는 경우 이를 제어할 수 있습니다.

단계 **2** 하드웨어 우회를 수동으로 활성화 또는 비활성화합니다.

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** | **1/3-1/4**}

예제**:**

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

단계 **3** (선택 사항) ASA FirePOWER 모듈이 부팅된 후까지 액티브 상태를 유지하려면 하드웨어 우회를 구성합니다.

hardware-bypass boot-delay module-up sfr

부팅 지연을 작동하려면 스티키 옵션을 사용하지 않고 하드웨어 우회를 활성화해야 합니다. **hardware-bypass boot-delay** 명령을 사용하지 않으면 ASA FirePOWER 모듈이 부팅을 마치기 전에 하드웨어 우회가 액티브가 아닌 상태가 되기 쉽습니다. 이 시나리오로 인해 예를 들어 fail-close로 모듈을 구성한 경우 트래픽이 삭제될 수 있습니다.

단계 **4** TCP 시퀀스 임의 설정을 비활성화합니다. 이 예에는 기본 구성에 설정을 추가하여 모든 트래픽에 대해 임의 설정을 비활성화하는 방법이 나와 있습니다.

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

나중에 다시 활성화하려는 경우 "disable"을 **enable**로 바꿉니다.

단계 **5** 듀얼 전원 공급 장치를 예상 구성대로 설정합니다.

power-supply dual

ASP(가속화된 보안 경로) 성능 및 동작 모니터링

ASP는 정책과 컨피그레이션을 실행에 옮기는 구현 레이어입니다. Cisco Technical Assistance Center와 문제를 해결할 때가 아니면 직접적인 연관성은 없습니다. 그러나 몇 가지 성능 및 안정성 관련 동작은 조정할 수 있습니다.

규칙 엔진 트랜잭션 커밋 모델 선택

기본적으로 규칙 기반 정책(예: 액세스 규칙)을 바꾸면 그 변경 사항이 즉시 적용됩니다. 하지만 이와 같은 신속성이 다소 성능에 영향을 미칩니다. 이 성능 문제는 초당 연결 수가 많은 환경에서 매우 큰 규칙 목록을 사용할 때 더욱 두드러집니다. 예를 들면, ASA에서 초당 18,000건의 연결을 처리하는 동안 25,000개의 규칙이 포함된 정책을 변경하는 경우입니다.

규칙 엔진이 규칙 조회 속도를 높이고자 규칙을 컴파일하면서 성능에 영향을 줍니다. 기본적으로 이 시스템은 연결 시도를 평가할 때 새로운 규칙을 적용할 수 있도록 컴파일되지 않은 규칙도 검색합니다. 규칙이 컴파일되지 않았으므로 검색 시간이 늘어납니다.

규칙 엔진에서 규칙 변경을 구현할 때 트랜잭션 모델을 사용함으로써 새 규칙이 컴파일되어 사용 가능해질 때까지 기존 규칙을 계속 사용하도록 위 동작을 변경할 수 있습니다. 트랜잭션 모델을 사용하면 규칙 컴파일 과정에서 성능이 저하되지 않습니다. 다음 표에서 동작의 차이점을 확인할 수 있습니다.

모델	컴파일 전	컴파일 과정	컴파일 후
기본	기존 규칙에 매칭합니다.	새 규칙에 매칭합니다. (초당 연결 수 감소)	새 규칙에 매칭합니다.
트랜잭션	기존 규칙에 매칭합니다.	기존 규칙에 매칭합니다. (초당 연결 수 변동 없음)	새 규칙에 매칭합니다.

트랜잭션 모델의 또 다른 이점은 인터페이스에서 ACL을 대체할 때 기존 ACL을 삭제하는 시점과 새 ACL을 적용하는 시점 사이에 공백이 없다는 것입니다. 이 기능 덕분에 작업 과정에서 적합한 연결이 폐기될 가능성이 줄어듭니다.

팁 규칙 유형에 대해 트랜잭션 모델을 활성화하면 컴파일의 시작과 끝을 알리는 syslog가 생성됩니다. 이 syslog의 번호는 780001~ 780004입니다.

규칙 엔진을 위해 트랜잭션 커밋 모델을 활성화하려면 다음 절차를 사용합니다.

프로시저

규칙 엔진을 위해 트랜잭션 커밋 모델을 활성화합니다.

asp rule-engine transactional-commit *option*

옵션:

- **access-group**—전역에 또는 인터페이스에 적용되는 액세스 규칙
- **nat**—네트워크 주소 변환 규칙

예제**:**

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

ASP 로드 밸런싱 활성화

ASP 로드 밸런싱 메커니즘으로 다음 문제를 예방할 수 있습니다.

- 흐름에서 산발적인 트래픽 급증으로 인한 오버런
- 특정 인터페이스 수신 링에 초과 유입되는 대량 플로우에 의한 오버런
- 비교적 과부하 상태인 인터페이스 수신 링으로 인한 오버런. 단일 코어에서 로드를 수용할 수 없음

ASP 로드 밸런싱을 통해 여러 코어가 단일 인터페이스 수신 링에서 받은 패킷에서 동시에 작업을 수행할 수 있습니다. 시스템에서 패킷을 삭제하고 **show cpu** 명령 출력이 100%보다 훨씬 적은 경우, 패킷이 관련 없는 다수의 연결에 속한 것이라면 이 기능으로 처리량을 늘릴 수 있습니다.

참고 ASP 로드 밸런싱은 ASAv에서 비활성화되어 있습니다. ASAv는 ASAv의 ASP(가속화된 보안 경로)에 DPDK(Dataplane Development Kit)를 통합하여 이 기능이 비활성화된 상태에서 더 우수한 성능을 보여줍니다.

프로시저

단계 **1** ASP 로드 밸런싱의 자동 전환 켜기/끄기를 활성화합니다.

asp load-balance per-packet auto

단계 **2** ASP 로드 밸런싱을 수동으로 활성화합니다.

asp load-balance per-packet

auto 명령을 활성화했더라도 ASP 로드 밸런싱은 수동으로 비활성화할 때까지 활성화되어 있습니다.

단계 **3** ASP 로드 밸런싱을 수동으로 비활성화합니다.

no asp load-balance per-packet

이 명령은 ASP 로드 밸런싱을 수동으로 활성화한 경우에만 적용됩니다. **auto** 명령을 활성화한 경우에도 시스템은 ASP 로드 밸런싱을 자동으로 활성화하거나 비활성화하는 상태로 되돌아갑니다.

DNS 캐시 모니터링

ASA에서는 특정 클라이언트리스 SSL VPN 및 인증서 명령에 대해 전송된 외부 DNS 쿼리로부터 DNS 정보의 로컬 캐시를 제공합니다. DNS 변환 요청이 있을 때마다 먼저 로컬 캐시를 검색합니다. 로컬 캐시에 해당 정보가 있으면 그 결과 IP 주소를 반환합니다. 로컬 캐시에서 요청을 해결하지 못하면 구성된 다양한 DNS 서버에 DNS 쿼리를 보냅니다. 외부 DNS 서버에서 요청을 해결한 경우 그 결과 IP 주소는 해당 호스트 이름과 함께 로컬 캐시에 저장됩니다.

DNS 캐시를 모니터링하려면 다음 명령을 참조하십시오.

- **show dns-hosts**

  이 명령은 DNS 캐시를 보여줍니다. 여기에는 DNS 서버로부터 동적으로 입수한 항목뿐 아니라 name 명령을 사용하여 직접 입력한 이름과 IP 주소가 들어 있습니다.

기본 설정 기록

기능 이름	플랫폼 릴리스	설명
마스터 패스프레이즈	8.3(1)	이 기능을 도입했습니다. 마스터 패스프레이즈를 사용하면 일반 텍스트 비밀번호를 암호화된 형식으로 안전하게 저장할 수 있습니다. 또한 제공되는 키를 사용하여 기능 변경 없이 모든 비밀번호를 종합적으로 암호화하거나 마스킹할 수 있습니다. 도입된 명령: **key config-key password-encryption**, **password encryption aes**, **clear configure password encryption aes**,**show running-config password encryption aes, show password encryption**
비밀번호 암호화 가시성	8.4(1)	**show password encryption** 명령을 수정했습니다.
기본 텔넷 비밀번호 삭제	9.0(2), 9.1(2)	ASA에 대한 관리 액세스의 보안을 강화하기 위해 텔넷의 기본 로그인 비밀번호가 제거되었습니다. 텔넷을 사용하여 로그인하려면 먼저 비밀번호를 수동으로 설정해야 합니다. 참고 로그인 비밀번호는 텔넷 사용자 인증(**aaa authentication telnet console** 명령)을 구성하지 않은 경우에 텔넷에서만 사용됩니다. 이전에는 비밀번호를 지운 경우 ASA에서 기본값인 "cisco"를 복원했습니다. 현재 비밀번호를 지우면 해당 비밀번호가 제거됩니다. 로그인 비밀번호는 스위치에서 ASASM으로 연결하는 텔넷 세션에도 사용됩니다(**session** 명령 참조). 최초로 ASASM에 액세스할 경우 로그인 비밀번호를 설정할 때까지 **service-module session** 명령을 사용해야 합니다. 수정된 명령: **password**

기능 이름	플랫폼 릴리스	설명
자동 ASP 로드 밸런싱	9.3(2)	이제 ASP 로드 밸런싱 기능의 자동 전환 켜기/끄기를 활성화할 수 있습니다. 참고 자동 기능은 ASAv에서 지원되지 않습니다. 수동 활성화 및 비활성화만 지원됩니다. 도입된 명령: **asp load-balance per-packet auto**
ISA 3000 하드웨어 우회	9.4(1.225)	ISA 3000에서는 전력 손실이 발생할 경우 어플라이언스를 통해 트래픽이 계속 이동하게 해주는 하드웨어 우회 기능을 지원합니다. 도입된 명령: **hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay, show hardware-bypass** 이 기능은 버전 *9.5(1)*에서 사용할 수 없습니다.
ISA 3000에 대한 듀얼 전원 공급 장치 지원	9.6(1)	ISA 3000의 듀얼 전원 공급 장치의 경우 ASA OS의 예상 구성대로 듀얼 전원 공급 장치를 설정할 수 있습니다. 1개의 전원 공급 장치에 장애가 발생하면 ASA는 알람을 발행합니다. 기본적으로 ASA는 단일 전원 공급 장치를 예상하며 하나의 작업 중인 전원 공급 장치를 포함하는 한 알람을 발행하지 않습니다. 도입된 명령: **power-supply dual**
로컬 **username** 및 **enable** 비밀번호에 대한 더 긴 비밀번호 지원(최대 127자)	9.6(1)	이제 로컬 **username** 및 **enable** 비밀번호를 최대 127자까지(이전 제한은 32자였음) 생성할 수 있습니다. 32자 보다 긴 비밀번호를 생성하는 경우, 비밀번호는 PBKDF2(비밀번호 기반 키 파생 함수 2) 해시를 사용하여 구성에 저장됩니다. 더 짧은 비밀번호는 계속해서 MD5 기반 해싱 방법을 사용합니다. 수정된 명령: **enable, username**

기능 이름	플랫폼 릴리스	설명
모든 로컬 **username** 및 **enable** 비밀번호에 대한 PBKDF2 해싱	9.7(1)	모든 길이의 로컬 **username** 및 **enable** 비밀번호는 PBKDF2(비밀번호 기반 키 파생 함수 2) 해시를 사용하여 구성에 저장됩니다. 이전에는 32자 이하의 비밀번호에서 MD5 기반 해싱 방법을 사용했습니다. 이미 있는 기존 비밀번호는 새 비밀번호를 입력하지 않으면 MD5 기반 해시를 계속해서 사용합니다. 다운그레이드 지침을 확인하려면 일반적인 작업 구성 가이드의 "소프트웨어 및 구성" 장을 참조하십시오. 수정된 명령: **enable, username**
ASAv에 대한 자동 ASP 로드 밸런싱 지원	9.8(1)	이전에는 ASP 로드 밸런싱을 수동으로만 활성화 및 비활성화할 수 있었습니다. 수정된 명령: **asp load-balance per-packet auto**
ASP 로드 밸런싱이 ASAv에서 비활성화되어 있음	9.10(1)	ASAv는 ASAv의 ASP(가속화된 보안 경로)에 DPDK(Dataplane Development Kit)를 최근에 통합하여 이 기능이 비활성화된 상태에서 더 우수한 성능을 보여줍니다.

20 장

DHCP 및 DDNS 서비스

이 장에서는 DHCP 서버나 DHCP 릴레이 및 DDNS(동적 DNS) 업데이트 방법을 어떻게 구성하는지에 대해 설명합니다.

DHCP 및 DDNS 서비스 정보

다음 주제에서는 DHCP 서버, DHCP 릴레이 에이전트 및 DDNS 업데이트를 설명합니다.

DHCPv4 서버 정보

DHCP는 IP 주소와 같은 네트워크 컨피그레이션 매개변수를 DHCP 클라이언트에 제공합니다. ASA에서는 ASA 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버를 제공할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 직접 네트워크 컨피그레이션 매개변수를 제공합니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다.

DHCP 옵션

DHCP는 TCP/IP 네트워크에서 호스트할 구성 정보를 전달하기 위한 프레임워크를 제공합니다. 구성 파라미터는 DHCP 메시지의 Options(옵션) 필드에 저장된 태깅 항목으로 전달되며, 데이터는 옵션이라고도 합니다. 벤더 정보는 Options(옵션)에도 저장되어 있으며 모든 벤더 정보는 확장하여 DHCP 옵션으로 사용될 수 있습니다.

예를 들어, Cisco IP Phones는 TFTP 서버에서 구성을 다운로드합니다. Cisco IP Phone이 시작할 때 IP 주소 및 TFTP 서버 IP 주소 모두 사전에 구성되지 않았다면 이 정보를 얻고자 DHCP 서버에 옵션 150 또는 66으로 요청을 보냅니다.

- DHCP 옵션 150은 일련의 TFTP 서버의 IP 주소를 제공합니다.
- DHCP 옵션 66은 단일 TFTP 서버의 IP 주소 또는 호스트 이름을 제공합니다.
- DHCP 옵션 3은 기본 경로를 설정합니다.

하나의 요청에서 옵션 150과 66을 모두 포함할 수 있습니다. 이 경우, 두 옵션의 값이 이미 ASA에 구성되어 있다면 ASA DHCP 서버에서는 두 옵션을 모두 포함하여 응답합니다.

DHCP 클라이언트에 DNS, WINS 및 도메인 이름 파라미터를 제공하기 위해 고급 DHCP 옵션을 사용할 수 있습니다. DHCP 옵션 15는 DNS 도메인 접미사에 사용됩니다. 이러한 값을 얻거나 수동으로 정의하기 위해 DHCP 자동 구성 설정을 사용할 수도 있습니다. 이 정보를 정의하는 데 둘 이상의 방법을 사용할 경우 다음 순서로 DHCP 클라이언트에 전달됩니다.

1. 직접 구성한 설정
2. 고급 DHCP 옵션 설정
3. DHCP 자동 컨피그레이션 설정

이를테면 DHCP 클라이언트에서 수신할 도메인 이름을 직접 정의한 다음 DHCP 자동 컨피그레이션을 활성화할 수 있습니다. DHCP 자동 컨피그레이션에서 DNS 및 WINS 서버와 함께 도메인을 검색하더라도, 수동으로 정의된 도메인 이름이 검색된 DNS 및 WINS 서버 이름과 함께 DHCP 클라이언트에 전달됩니다. DHCP 자동 컨피그레이션 프로세스에 의해 검색된 도메인 이름보다 수동 정의된 도메인 이름이 우선하기 때문입니다.

DHCPv6 스테이트리스 서버 정보

접두사 위임 기능(IPv6 접두사 위임 클라이언트 활성화, 627 페이지)과 함께 SLAAC(StateLess Address Auto Configuration)를 사용하는 클라이언트의 경우, IR(정보 요청) 패킷을 ASA에 보낼 때 DNS 서버 또는 도메인 이름과 같은 정보를 제공하도록 ASA를 구성할 수 있습니다. ASA는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다.

DHCP 릴레이 에이전트 소개

인터페이스에서 수신한 DHCP 요청을 하나 이상의 DHCP 서버에 전달하도록 DHCP 릴레이 에이전트를 구성할 수 있습니다. DHCP 클라이언트는 최초 DHCPDISCOVER 메시지를 보내는 데 UDP 브로드캐스트를 사용합니다. 연결된 네트워크에 대한 정보가 없기 때문입니다. 클라이언트가 연결된 세그먼트에 서버가 없을 경우, ASA는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다. DHCP 릴레이 에이전트를 통해 브로드캐스트를 수신하는 ASA의 인터페이스를 구성하여 DHCP 요청을 다른 인터페이스의 DHCP 서버에 전달할 수 있습니다.

DDNS 소개

DDNS 업데이트는 DNS와 DHCP를 통합합니다. 두 프로토콜은 상호 보완적입니다. DHCP는 IP 주소 할당을 중앙화하고 자동화합니다. DDNS 업데이트는 미리 정의된 간격에 따라 지정된 주소와 호스트 이름의 연결을 자동으로 기록합니다. DDNS는 주소-호스트 이름 연결의 잦은 변경 사항을 자주 업데이트하는 것을 허용합니다. 따라서 이를테면 모바일 호스트가 사용자 또는 관리자의 개입 없이 자유롭게 네트워크에서 이동할 수 있습니다. DDNS는 DNS 서버에서 필요한 이름-주소 매핑 및 주소-이름 매핑의 동적 업데이트와 동기화를 제공합니다.

DDNS 이름 및 주소 매핑은 DHCP 서버에서 2개의 RR(리소스 레코드)에 저장됩니다. A RR은 이름-IP 주소 매핑을 포함하는 반면 PTR RR은 이름에 주소를 매핑합니다. ASA는 DDNS 업데이트를 수행하는 2가지 메서드(RFC 2136에 의해 정의된 IETF 표준 및 일반 HTTP 메서드) 중에서 IETF 메서드를 지원합니다.

참고 DDNS는 브리지 그룹 멤버 인터페이스 또는 BVI에서 지원되지 않습니다.

DDNS 업데이트 구성

가장 일반적인 DDNS 업데이트 컨피그레이션 2가지는 다음과 같습니다.

- DHCP 클라이언트가 A RR을 업데이트하고, DHCP 서버가 PTR RR을 업데이트합니다.
- DHCP 서버가 A RR과 PTR RR을 모두 업데이트합니다.

일반적으로 DHCP 서버가 클라이언트를 대신하여 DNS PTR RR을 유지 관리합니다. 클라이언트가 필요한 모든 DNS 업데이트를 수행하도록 구성할 수 있습니다. 서버가 이 업데이트를 인정하거나 인정하지 않도록 구성할 수 있습니다. DHCP 서버가 PTR RR을 업데이트하려면 클라이언트의 FQDN(fully qualified domain name)을 알고 있어야 합니다. 클라이언트는 Client FQDN이라는 DHCP 옵션을 사용하여 서버에 FQDN을 제공합니다.

UDP 패킷 크기

DDNS는 DNS 요청자가 UDP 패킷의 크기를 알리는 것을 허용하며, 512옥텟보다 큰 패킷의 전송을 지원합니다. DNS 서버는 UDP를 통해 요청을 받으면, OPT RR로부터 UDP 패킷의 크기를 확인한 다음 요청자가 지정한 최대 UDP 패킷 크기의 허용 범위에서 최대한 많은 RR을 포함할 수 있도록 응답을 확장합니다. DNS 패킷의 최대 크기는 4096바이트(BIND) 또는 1280바이트(Windows 2003 DNS Server)입니다.

몇몇 추가 **message-length maximum** 명령을 사용할 수 있습니다.

- 기존 전역 한도: **message-length maximum 512**
- 클라이언트 또는 서버별 한도: **message-length maximum client 4096** 및 message-length maximum server 4096
- OPT RR 필드에 지정된 동적 값: **message-length maximum client auto**

3개의 명령이 동시에 있을 경우, ASA는 구성된 클라이언트 또는 서버의 최대 한도에서 자동 구성 길이를 허용합니다. 그 밖의 DNS 트래픽에서는 message-length maximum이 사용됩니다.

DHCP 및 DDNS 서비스에 대한 지침

이 섹션에는 DHCP 및 DDNS 서비스를 구성하기 전에 확인해야 하는 제한사항 및 지침이 포함되어 있습니다.

상황 모드

- DHCPv6 스테이트리스 서버는 다중 상황 모드에서 지원되지 않습니다.

방화벽 모드

- DHCP 릴레이는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.
- DHCP 서버는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드에서 지원됩니다. 라우팅 모드에서 DHCP 서버는 브리지 그룹 멤버 인터페이스가 아닌 BVI 인터페이스에서 지원됩니다. DHCP 서버가 작동하려면 BVI에 이름이 있어야 합니다.
- DDNS는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.
- DHCPv6 스테이트리스 서버는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.

클러스터링

- DHCPv6 스테이트리스 서버는 클러스터링에서 지원되지 않습니다.

IPv6

DHCP 스테이트리스 서버 및 DHCP 릴레이에 대한 IPv6를 지원합니다.

DHCPv4 서버

- 최대 가용 DHCP 풀은 주소 256개입니다.
- DHCP 서버는 각 인터페이스에서 1개씩만 구성할 수 있습니다. 각 인터페이스는 자체 주소 풀을 두고 사용할 수 있습니다. 그러나 DNS 서버, 도메인 이름, 옵션, ping 시간 초과, WINS 서버와 같은 나머지 DHCP 설정은 전역으로 구성되며 모든 인터페이스에서 DHCP 서버에 의해 사용됩니다.
- 서버가 활성화된 인터페이스에서 DHCP 클라이언트 또는 DHCP 릴레이 서비스를 구성할 수 없습니다. 또한 DHCP 클라이언트는 서버가 활성화된 인터페이스에 직접 연결되어야 합니다.
- ASA - QIP DHCP 서버를 DHCP 프록시 서비스와 함께 사용하는 것은 지원되지 않습니다.

- DHCP 서버가 활성화되지 않으면 릴레이 에이전트도 활성화될 수 없습니다.
- DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

DHCPv6 서버

DHCPv6 스테이트리스 서버는 DHCPv6 주소, 접두사 위임 클라이언트 또는 DHCPv6 릴레이가 구성되어 있는 인터페이스에서 구성할 수 없습니다.

DHCP 릴레이

- 단일 모드 및 각 상황에서 전역 서버와 인터페이스 특정 서버를 포함하여 최대 10개의 DHCPv4 릴레이 서버를 구성할 수 있으며, 각 인터페이스에는 최대 4개의 서버가 가능합니다.
- 단일 모드 및 각 상황에서 최대 10개의 DHCPv6 릴레이 서버를 구성할 수 있습니다. IPv6 인터페이스 특정 서버는 지원되지 않습니다.
- DHCP 서버 기능이 활성화되지 않으면 릴레이 에이전트도 활성화될 수 없습니다.
- DHCP 릴레이 서비스는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 사용할 수 없습니다. 그러나 액세스 규칙을 사용하는 방법으로 DHCP 트래픽을 허용할 수 있습니다. DHCP 요청과 응답이 ASA를 지날 수 있게 하려면 2개의 액세스 규칙을 구성해야 합니다. 하나는 내부 인터페이스에서 외부(UDP 대상 포트 67)로 보내는 DHCP 요청을 허용하는 것이고 다른 하나는 반대 방향(UDP 대상 포트 68)으로 서버의 응답을 허용하는 것입니다.
- IPv4에서는 클라이언트가 ASA에 직접 연결되어야 하며, 다른 릴레이 에이전트 또는 라우터를 통해 요청을 보낼 수 없습니다.IPv6에서는 ASA가 다른 릴레이 서버에서 보낸 패킷을 지원합니다.
- DHCP 클라이언트는 ASA에서 요청을 릴레이하는 DHCP 서버와 다른 인터페이스에 있어야 합니다.
- 트래픽 영역의 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.

DHCP 서버 구성

이 섹션에서는 ASA에서 제공하는 DHCP 서버의 구성 방법을 설명합니다.

프로시저

단계 **1** DHCPv4 서버 활성화, 708 페이지.
단계 **2** 고급 DHCPv4 옵션 구성, 710 페이지.
단계 **3** DHCPv6 스테이트리스 서버 구성, 711 페이지.

DHCPv4 서버 활성화

ASA 인터페이스에서 DHCP 서버를 활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 인터페이스의 DHCP 주소 풀을 생성합니다. ASA에서는 이 풀의 주소 중에서 지정된 기간 동안 사용할 주소 하나를 클라이언트에 할당합니다. 이 주소는 직접 연결 네트워크를 위한 변환되지 않은 로컬 주소입니다.

dhcpd address *ip_address_start-ip_address_end if_name*

예제:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

주소 풀이 ASA 인터페이스와 동일한 서브넷에 있어야 합니다. 투명 모드에서 브리지 그룹 멤버 인터페이스를 지정합니다. 라우팅 모드에서 라우팅 인터페이스 또는 BVI를 지정합니다. 브리지 그룹 멤버 인터페이스는 지정하지 마십시오.

단계 **2** (선택 사항) (라우팅 모드) DHCP 또는 PPPoE 클라이언트를 실행 중인 인터페이스 또는 VPN 서버에서 획득한 도메인 이름 값, DNS, WINS를 자동으로 구성합니다.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

예제:

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

다음 명령을 사용하여 DNS, WINS 또는 도메인 이름 파라미터를 지정할 경우, 자동 구성을 통해 획득한 파라미터를 덮어씁니다.

단계 **3** (선택 사항) DNS 서버의 IP 주소를 지정합니다.

dhcpd dns *dns1* [*dns2*]

예제:

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

단계 **4** (선택 사항) WINS 서버의 IP 주소를 지정합니다. 최대 2개의 WINS 서버를 지정할 수 있습니다.

dhcpd wins *wins1* [*wins2*]

예제:

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

단계 **5** (선택 사항) 클라이언트에 적용할 리스 기간을 변경합니다. 리스 기간은 클라이언트가 할당받은 IP 주소를 리스 만료 전까지 사용할 수 있는 기간(초)과 같습니다. 0 ~ 1,048,575의 값을 입력합니다. 기본값은 3600초입니다.

dhcpd lease *lease_length*

예제**:**

```
ciscoasa(config)# dhcpd lease 3000
```

단계 **6** (선택 사항) 도메인 이름을 구성합니다.

dhcpd domain *domain_name*

예제**:**

```
ciscoasa(config)# dhcpd domain example.com
```

단계 **7** (선택 사항) ICMP 패킷을 위한 DHCP ping 시간 초과 값을 구성합니다. 주소 충돌을 방지하고자 ASA에서는 DHCP 클라이언트에 주소를 할당하기 전에 주소에 2개의 ICMP ping 패킷을 보냅니다. 기본값은 50밀리초입니다.

dhcpd ping timeout *milliseconds*

예제**:**

```
ciscoasa(config)# dhcpd ping timeout 20
```

단계 **8** DHCP 클라이언트에 보내는 기본 게이트웨이를 정의합니다. 라우팅 모드의 경우 **dhcpd option 3 ip** 명령을 사용하지 않으면 ASA에서 DHCP 서버 활성화 인터페이스 IP 주소를 기본 게이트웨이로 전송합니다. 투명 모드에서는 기본 게이트웨이를 설정하려는 경우, **dhcpd option 3 ip**를 설정해야 합니다. ASA는 그 자체로 기본 게이트웨이 역할을 수행할 수 없습니다.

dhcpd option 3 ip *gateway_ip*

예제**:**

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

단계 **9** 활성화된 인터페이스에서 DHCP 클라이언트 요청을 수신하도록 ASA 내 DHCP 데몬을 활성화합니다.

dhcpd enable *interface_name*

예제**:**

```
ciscoasa(config)# dhcpd enable inside
```

dhcpd address 범위와 동일한 인터페이스를 지정합니다.

고급 DHCPv4 옵션 구성

ASA에서는 정보 전송을 위해 RFC 2132, RFC 2562, RFC 5510에 규정된 DHCP 옵션을 지원합니다. 1, 12, 50–54, 58–59, 61, 67, 82를 제외하고 모든 DHCP 옵션(1 ~ 255)이 지원됩니다.

프로시저

단계 **1** IP 주소 1개 또는 2개를 반환하는 DHCP 옵션을 구성합니다.

dhcpd option *code* **ip** *addr_1* [*addr_2*]

예제:

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

Cisco IP Phones에서 사용하기 위해 옵션 150은 TFTP 서버 1개 또는 2개의 IP 주소 또는 이름을 제공합니다. 옵션 3은 Cisco IP phones의 기본 경로를 설정합니다.

단계 **2** 문자열을 반환하는 DHCP 옵션을 구성합니다.

dhcpd option *code* **ascii** *text*

예제:

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

Cisco IP Phones에서 사용하기 위해 옵션 66은 TFTP 서버의 IP 주소 또는 이름을 제공합니다.

단계 **3** 16진수 값을 반환하는 DHCP 옵션을 구성합니다.

dhcpd option code hex 값

예제:

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

참고 ASA에서는 사용자가 제공하는 옵션의 유형 및 값이 RFC 2132에 정의된 옵션 코드의 예상 유형 및 값과 일치하는지 확인하지 않습니다. 예를 들어, **dhcpd option 46 ascii hello** 명령을 입력할 수 있습니다. RFC 2132에 따르면 옵션 46이 1자리의 16진수 값을 가져야 하지만 ASA에서는 이 구성을 허용합니다. 옵션 코드와 그 유형 및 예상 값에 대한 자세한 내용은 RFC 2132를 참조하십시오.

다음 표에는 **dhcpd option** 명령에서 지원하지 않는 DHCP 옵션이 나와 있습니다.

표 ***24:*** 지원되지 않는 ***DHCP*** 옵션

옵션 코드	설명
0	DHCPOPT_PAD

옵션 코드	설명
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

DHCPv6 스테이트리스 서버 구성

접두사 위임 기능(IPv6 접두사 위임 클라이언트 활성화, 627 페이지)과 함께 SLAAC(StateLess Address Auto Configuration)를 사용하는 클라이언트의 경우, IR(정보 요청) 패킷을 ASA에 보낼 때 DNS 서버 또는 도메인 이름 같은 정보를 제공하도록 ASA를 구성할 수 있습니다. ASA는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다.

시작하기 전에

이 기능은 단일 라우팅 모드에서만 지원됩니다. 이 기능은 클러스터링에서 지원되지 않습니다.

프로시저

단계 **1** DHCPv6 서버가 제공할 정보가 포함된 IPv6 DHCP 풀을 구성합니다.

ipv6 dhcp pool *pool_name*

예제:

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

원하는 경우 각 인터페이스에 개별 풀을 구성하거나 여러 인터페이스에서 동일한 풀을 사용할 수 있습니다.

단계 **2** IR 메시지에 대한 응답으로 클라이언트에 제공하기 위해 다음 파라미터 중 한 개 이상을 구성합니다.

dns-server *dns_ipv6_address*

domain-name *domain-name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

import {[**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**]}

예제**:**

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

import 명령의 경우 ASA가 접두사 위임 클라이언트 인터페이스의 DHCPv6 서버에서 획득한 파라미터를 하나 이상 사용합니다. 수동으로 구성한 파라미터를 가져온 파라미터와 혼합하고 일치시킬 수 있습니다. 그러나 동일한 파라미터를 수동으로 **import** 명령에서 구성할 수는 없습니다.

단계 **3** ASA가 IR 메시지를 수신할 인터페이스에 대한 인터페이스 구성 모드로 들어갑니다.

interface *id*

예제**:**

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

단계 **4** DHCPv6 서버를 활성화합니다.

ipv6 dhcp server *pool_name*

예제**:**

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

단계 **5** DHCPv6 서버에 대한 정보를 SLAAC 클라이언트에 알려주기 위해 라우터 알림을 구성합니다.

ipv6 nd other-config-flag

이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.

예

다음 예에서는 두 개의 인터페이스에서 2개의 IPv6 DHCP 풀을 생성하고 DHCPv6 서버를 활성화합니다.

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

DHCP 릴레이 에이전트 구성

DHCP 요청이 인터페이스에 들어올 때 ASA에서 해당 요청을 릴레이할 DHCP 서버는 구성에 따라 달라집니다. 다음 유형의 서버를 구성할 수 있습니다.

- 인터페이스 특정 DHCP 서버 — DHCP 요청이 특정 인터페이스에 들어올 때 ASA는 해당 인터페이스 특정 서버에만 요청을 릴레이합니다.
- 전역 DHCP 서버 — DHCP 요청이 인터페이스 특정 서버가 구성되지 않은 인터페이스에 들어오면 ASA는 모든 전역 서버에 요청을 릴레이합니다. 인터페이스에 인터페이스 특정 서버가 있는 경우 전역 서버는 사용되지 않습니다.

DHCPv4 릴레이 에이전트 구성

DHCP 요청이 인터페이스에 들어올 때 ASA에서는 해당 요청을 DHCP 서버에 릴레이합니다.

프로시저

단계 **1** 다음 중 하나를 또는 둘 다 수행합니다.

- 전역 DHCP 서버 IP 주소 및 이 서버와의 연결에 사용할 인터페이스를 지정합니다.

  dhcprelay server *ip_address if_name*

  예:

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- DHCP 클라이언트 네트워크에 연결된 인터페이스 ID 및 이 인터페이스에 들어오는 DHCP 요청에 사용할 DHCP 서버 IP 주소를 지정합니다.

```
interface interface_id
  dhcprelay server ip_address
```

  예:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

  전역 **dhcprelay server** 명령에서처럼 요청에 대해 이그레스 인터페이스를 지정하지 않습니다. 그 대신 ASA에서는 라우팅 테이블을 사용하여 이그레스 인터페이스를 확인합니다.

단계 **2** DHCP 클라이언트에 연결된 인터페이스에서 DHCP 릴레이 서비스를 활성화합니다. 여러 인터페이스에서 DHCP 릴레이를 활성화할 수 있습니다.

dhcprelay enable *interface*

예제**:**

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

단계 **3** (선택 사항) DHCP 릴레이 주소를 처리할 수 있는 시간(초)을 설정합니다.

dhcprelay timeout *seconds*

예제**:**

```
ciscoasa(config)# dhcprelay timeout 25
```

단계 **4** (선택 사항) DHCP 서버에서 ASA 인터페이스의 주소로 보낸 패킷의 첫 번째 기본 라우터 주소를 변경합니다.

dhcprelay setroute *interface_name*

예제:

```
ciscoasa(config)# dhcprelay setroute inside
```

이 작업을 수행하면 클라이언트는 DHCP 서버가 다른 라우터를 지정하더라도 ASA를 가리키는 기본 경로를 설정할 수 있습니다.

패킷에 기본 라우터 옵션이 없는 경우 ASA는 인터페이스 주소를 포함하는 옵션을 추가합니다.

단계 **5** (선택 사항) 인터페이스를 신뢰할 수 있는 인터페이스로 구성합니다. 다음 중 하나를 수행합니다.

- 신뢰할 DHCP 클라이언트 인터페이스를 지정합니다.

  interface *interface_id*
  dhcprelay information trusted

  예:

  ```
  ciscoasa(config)# interface gigabitethernet 0/0
  ciscoasa(config-if)# dhcprelay information trusted
  ```

  DHCP Option 82를 보존하기 위해 인터페이스를 신뢰받는 인터페이스로 구성할 수 있습니다. DHCP Option 82는 다운스트림 스위치 및 라우터에서 DHCP 스누핑과 IP 소스 가드에 사용합니다. 일반적으로 ASA DHCP 릴레이 에이전트에서 옵션 82가 이미 설정된 DHCP 패킷을 수신하지만 giaddr 필드(서버에 패킷을 전달하기 전에 릴레이 에이전트에 의해 설정되는 DHCP 릴레이 에이전트 주소 지정)가 0으로 설정된 경우 ASA는 기본적으로 해당 패킷을 폐기합니다. 이제는 어떤 인터페이스를 신뢰받는 인터페이스로 지정함으로써 Option 82를 보존하고 패킷을 전달할 수 있습니다.

- 모든 클라이언트 인터페이스를 신뢰받는 인터페이스로 구성합니다.

  dhcprelay information trust-all

  예:

  ```
  ciscoasa(config)# dhcprelay information trust-all
  ```

DHCPv6 릴레이 에이전트 구성

DHCPv6 요청이 인터페이스에 들어오면 ASA에서는 모든 DHCPv6 전역 서버에 해당 요청을 릴레이합니다.

프로시저

단계 **1** 클라이언트 메시지가 전달되는 IPv6 DHCP 서버 목적지 주소를 지정합니다.

ipv6 dhcprelay server *ipv6_address* [*interface*]

예제:

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 인수는 링크 범위 유니캐스트, 멀티캐스트, 사이트 범위 유니캐스트 또는 전역 IPv6 주소일 수 있습니다. 미지정, 루프백, 노드-로컬 멀티캐스트 주소는 릴레이 목적지로 허용되지 않습니다. 선택 사항인 *interface* 인수는 목적지를 위한 이그레스 인터페이스를 지정합니다. 클라이언트 메시지는 이그레스 인터페이스가 연결된 링크를 통해 목적지 주소에 전달됩니다. 지정된 주소가 링크 범위 주소일 경우 인터페이스를 지정해야 합니다.

단계 **2** 인터페이스에서 DHCPv6 릴레이 서비스를 활성화합니다.

ipv6 dhcprelay enable *interface*

예제:

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

단계 **3** (선택 사항) DHCPv6 서버에서 릴레이 주소 처리를 위해 릴레이 바인딩을 거쳐 DHCPv6 클라이언트에 전달하는 응답에 허용된 시간(초)을 지정합니다.

ipv6 dhcprelay timeout *seconds*

예제:

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 인수에 유효한 값의 범위는 1~3600입니다. 기본값은 60초입니다.

DDNS 구성

이 섹션에서는 DDNS 구성 방법을 설명합니다.

정적 IP 주소의 A RR 및 PTR RR 모두 업데이트

클라이언트가 고정 IP 주소에 대해 A RR과 PTR RR 둘 다 업데이트할 것임을 요청하도록 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예제:

```
ciscoasa(config)# ddns update method ddns-2
```

단계 **2** 클라이언트가 DNS A RR과 PTR RR 모두 업데이트하도록 지정합니다.

ddns both

예제:

```
ciscoasa(DDNS-update-method)# ddns both
```

단계 **3** 인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.

interface *mapped_name*

예제:

```
ciscoasa(DDNS-update-method)# interface eth1
```

단계 **4** DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예제:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

단계 **5** 인터페이스에 대해 고정 IP 주소를 구성합니다.

ip address *ip_address* [*mask*] [*standby ip_address*]

예제:

```
ciscoasa(config-if)# ip address 10.0.0.40 255.255.255.0
```

A RR 및 PTR RR 모두 업데이트

DHCP 클라이언트가 A RR 및 PTR RR 모두 업데이트하고 DHCP 서버에서 이를 적용할 것을 요청하도록 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** DHCP 클라이언트가 DHCP 서버에서 어떤 업데이트도 하지 않게끔 요청하도록 구성합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예제:

```
ciscoasa(config)# dhcp-client update dns server none
```

단계 **2** 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예제:

```
ciscoasa(config)# ddns update method ddns-2
```

단계 **3** 클라이언트가 DNS A RR과 PTR RR 모두 업데이트하도록 지정합니다.

ddns both

예제:

예:

```
ciscoasa(DDNS-update-method)# ddns both
```

단계 **4** 인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.

interface *mapped_name*

예제:

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

단계 **5** DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예제:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

단계 **6** DHCP를 사용하여 인터페이스의 IP 주소를 얻습니다.

ip address dhcp

예제:

```
ciscoasa(if-config)# ip address dhcp
```

단계 **7** DHCP 서버에서 DDNS 업데이트를 수행하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예제:

```
ciscoasa(if-config)# dhcpd update dns
```

모든 RR의 업데이트 무시

DHCP 서버에 A 또는 PTR 업데이트 모두 적용하지 않도록 지시하는 FQDN 옵션을 포함하게끔 DHCP 클라이언트를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예제:

```
ciscoasa(config)# ddns update method ddns-2
```

단계 **2** 클라이언트가 DNS A RR과 PTR RR 모두 업데이트하도록 지정합니다.

ddns both

예제:

```
ciscoasa(DDNS-update-method)# ddns both
```

단계 **3** 인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.

interface *mapped_name*

예제:

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

단계 **4** DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예제:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

단계 **5** DHCP 클라이언트가 DHCP 서버에서 어떤 업데이트도 하지 않게끔 요청하도록 구성합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예제:

```
ciscoasa(config)# dhcp-client update dns server none
```

단계 **6** DHCP를 사용하여 인터페이스의 IP 주소를 얻습니다.

ip address dhcp

예제:

```
ciscoasa(if-config)# ip address dhcp
```

단계 **7** DHCP 서버가 클라이언트 업데이트 요청을 재정의하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예제:

```
ciscoasa(if-config)# dhcpd update dns both override
```

PTR RR만 업데이트

서버에서 기본적으로 PTR RR 업데이트만 하도록 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 인터페이스를 구성합니다.

interface *mapped_name*

예제:

```
ciscoasa(config)# interface Ethernet0
```

단계 **2** DHCP 서버가 DNS A 및 PTR RR 모두 업데이트하도록 요청합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예제:

```
ciscoasa(config-if)# dhcp-client update dns both
```

단계 **3** 구성된 인터페이스에서 DHCP 클라이언트를 구성합니다.

ddns update [*method-name* | **hostname** *hostname*]

예제:

```
ciscoasa(config-if)# ddns update hostname asa
```

단계 **4** DHCP 서버에서 DDNS 업데이트를 수행하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예제:

```
ciscoasa(config-if)# dhcpd update dns
```

단계 **5** DHCP 클라이언트의 DNS 도메인 이름을 정의합니다.

dhcpd domain *domain_name* [**interface** *if_name*]

예제:

```
ciscoasa(config-if)# dhcpd domain example.com
```

클라이언트로 **RR** 업데이트 및 서버로 **PTR RR** 업데이트

클라이언트에서 A RR을 업데이트하고 서버에서 PTR 레코드를 업데이트하도록 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예제:

```
ciscoasa(config)# ddns update method ddns-2
```

단계 **2** DDNS 업데이트 메서드를 지정합니다.

ddns both

예제:

```
ciscoasa(DDNS-update-method)# ddns both
```

단계 **3** 인터페이스를 구성합니다.

interface *mapped_name*

예제:

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

단계 **4** DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개변수를 구성합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예제:

```
ciscoasa(config-if)# dhcp-client update dns
```

단계 **5** DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예제:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa
```

단계 **6** DHCP 서버에서 DDNS 업데이트를 수행하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예제:

```
ciscoasa(if-config)# dhcpd update dns
```

단계 **7** DHCP 클라이언트의 DNS 도메인 이름을 정의합니다.

dhcpd domain *domain_name* [**interface** *if_name*]

예제:

```
ciscoasa(config-if)# dhcpd domain example.com
```

DHCP 및 DDNS 서비스 모니터링

이 섹션에는 DHCP 및 DDNS 서비스를 모니터링하기 위한 절차가 포함되어 있습니다.

DHCP 서비스 모니터링

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  이 명령을 사용하면 현재 DHCP 서버 클라이언트 바인딩, 상태 및 통계가 표시됩니다.

- **show dhcprelay** {**state** | **statistics**}

  이 명령을 사용하면 DHCP 릴레이 상태 및 통계가 표시됩니다.

- **show ipv6 dhcprelay binding**

  이 명령은 릴레이 에이전트에서 생성한 릴레이 바인딩 항목을 보여줍니다.

- **show ipv6 dhcprelay statistics**

  이 명령은 IPv6의 DHCP 릴레이 에이전트 통계를 보여줍니다.

- **show ipv6 dhcp server statistics**

  이 명령을 사용하면 DHCPv6 스테이트리스 서버 통계가 표시됩니다. 다음 예는 이 명령이 제공하는 정보를 보여줍니다.

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                  10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface 명령은 모든 인터페이스에 대한 DHCPv6 정보를 표시합니다. 인터페이스가 DHCPv6 스테이트리스 서버 구성(DHCPv6 스테이트리스 서버 구성, 711 페이지 참조)에 대해 구성된 경우, 이 명령은 서버에서 사용 중인 DHCPv6 풀을 나열합니다. 인터페이스에 DHCPv6 주소 클라이언트 또는 접두사 위임 클라이언트 구성이 있는 경우, 이 명령은 각 클라이언트의 상태와 서버에서 수신한 값을 보여줍니다. 특정 인터페이스의 경우 DHCP 서버 또는 클라이언트에 대한 메시지 통계를 표시할 수 있습니다. 다음 예는 이 명령이 제공하는 정보를 보여 줍니다.

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
```

```
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:
```

```
 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics 명령은 유닛 간에 DUID 정보가 동기화된 횟수를 포함하여 장애 조치 유닛 간의 트랜잭션 통계를 보여줍니다. 다음 예는 이 명령이 제공하는 정보를 보여줍니다.

  액티브 유닛에서 다음과 같습니다.

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  스탠바이 유닛에서 다음과 같습니다.

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

DDNS 상태 모니터링

DDNS 상태를 모니터링하려면 다음 명령을 참조하십시오.

- **show running-config ddns**

  이 명령은 현재 DDNS 컨피그레이션을 보여줍니다.

- **show running-config dns server-group**

  이 명령은 현재 DNS 서버 그룹 상태를 보여줍니다.

DHCP 및 DDNS 서비스 내역

기능 이름	플랫폼 릴리스	설명
DHCP	7.0(1)	ASA에서는 ASA 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버 또는 DHCP 릴레이 서비스를 제공할 수 있습니다. 도입된 명령: **dhcp client update dns**, **dhcpd address**, **dhcpd domain**, **dhcpd enable**, **dhcpd lease**, **dhcpd option**, **dhcpd ping timeout**, **dhcpd update dns**, **dhcpd wins**, **dhcp-network-scope**, **dhcprelay enable**, **dhcprelay server**, **dhcprelay setroute**, **dhcp-server**. **show running-config dhcpd**, **show running-config dhcprelay**
DDNS	7.0(1)	이 기능을 도입했습니다. 다음 명령을 도입했습니다. **ddns**, **ddns update**, **dhcp client update dns**, **dhcpd update dns**, **show running-config ddns**, **show running-config dns server-group**
IPv6용 DHCP 릴레이(DHCPv6)	9.0(1)	IPv6용 DHCP 릴레이에 대한 지원이 추가되었습니다. 다음 명령을 도입했습니다. **ipv6 dhcprelay server**, **ipv6 dhcprelay enable**, **ipv6 dhcprelay timeout**, **clear config ipv6 dhcprelay**, **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**, **debug ipv6 dhcp**, **debug ipv6 dhcprelay**, **show ipv6 dhcprelay binding**, **clear ipv6 dhcprelay binding**, **show ipv6 dhcprelay statistics**, **clear ipv6 dhcprelay statistics**

기능 이름	플랫폼 릴리스	설명
인터페이스별 DHCP 릴레이 서버(IPv4만 해당)	9.1(2)	인터페이스별로 DHCP 릴레이 서버를 구성할 수 있습니다. 그러면 해당 인터페이스에 들어오는 요청은 그 인터페이스에 지정된 서버에만 릴레이합니다. IPv6에서는 인터페이스별 DHCP 릴레이를 지원하지 않습니다. 다음 명령을 도입했거나 수정했습니다. **dhcprelay server** (interface config mode), **clear configure dhcprelay**, **show running-config dhcprelay**.
DHCP 신뢰받는 인터페이스	9.1(2)	DHCP Option 82를 보존하기 위해 인터페이스를 신뢰받는 인터페이스로 구성할 수 있습니다. DHCP Option 82는 다운스트림 스위치 및 라우터에서 DHCP 스누핑과 IP 소스 가드에 사용합니다. 일반적으로 ASA DHCP 릴레이 에이전트에서 옵션 82가 이미 설정된 DHCP 패킷을 수신하지만 giaddr 필드(서버에 패킷을 전달하기 전에 릴레이 에이전트에 의해 설정되는 DHCP 릴레이 에이전트 주소 지정)가 0으로 설정된 경우 ASA는 기본적으로 해당 패킷을 폐기합니다. 이제는 어떤 인터페이스를 신뢰받는 인터페이스로 지정함으로써 Option 82를 보존하고 패킷을 전달할 수 있습니다. 다음 명령을 도입했거나 수정했습니다. **dhcprelay information trusted**, **dhcprelay information trust-all**, **show running-config dhcprelay**.
DHCP 리바인드 기능	9.1(4)	DHCP 리바인드 단계에서 클라이언트가 터널 그룹 목록에 있는 다른 DHCP 서버와의 리바인드를 시도합니다. 이 릴리스 전에는 DHCP 리스 갱신에 실패했을 때 클라이언트가 대체 서버에 리바인드하지 않았습니다. 어떤 명령도 도입하거나 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	설명
응답에 대한 DHCP 릴레이 서버의 DHCP 서버 식별자 검증	9.2(4)/9.3(3)	ASA DHCP 릴레이 서버가 잘못된 DHCP 서버에서 응답을 수신할 경우, 이제 응답에 대해 작업을 수행하기 전에 응답이 올바른 서버에서 오는지 확인합니다. 어떤 명령도 도입하거나 수정하지 않았습니다. ASDM 화면은 수정하지 않았습니다. 어떤 명령도 도입하거나 수정하지 않았습니다.
DHCPv6 모니터링	9.4(1)	이제 IPv6에 대한 DHCP 통계 및 IPv6에 대한 DHCP 바인딩을 모니터링할 수 있습니다.

기능 이름	플랫폼 릴리스	설명
IPv6 DHCP	9.6(2)	이제 ASA에서 IPv6 주소 지정에 대해 다음 기능을 지원합니다. • DHCPv6 주소 클라이언트 — ASA는 DHCPv6 서버에서 IPv6 전역 주소 및 선택 사항인 기본 경로를 가져옵니다. • DHCPv6 접두사 위임 클라이언트 — ASA는 DHCPv6 서버에서 위임된 접두사를 가져옵니다. 그런 다음 ASA는 이러한 접두사를 사용하여 SLAAC(Stateless Address Auto Configuration) 클라이언트가 동일한 네트워크에서 IPv6 주소를 자동으로 구성할 수 있도록 다른 ASA 인터페이스 주소를 구성할 수 있습니다. • 위임된 접두사에 대한 BGP 라우터 알림 • DHCPv6 스테이트리스 서버 — ASA는 SLAAC 클라이언트가 ASA에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 도메인 이름 등의 기타 정보를 제공합니다. ASA는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 추가 또는 수정된 명령: **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address, ipv6 address dhcp, ipv6 dhcp client pd, ipv6dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, showipv6 general-prefix, sip address, sip domain-name, sntp address**

21 장

디지털 인증서

이 장에서는 디지털 인증서를 구성하는 방법에 대해 설명합니다.

디지털 인증서 소개

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 상황에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다.

디지털 인증서를 사용하여 인증할 경우, 하나 이상의 ID 인증서와 이를 발급한 CA 인증서가 ASA에 있어야 합니다. 이 컨피그레이션에서는 복수의 ID, 루트, 인증서 계층 구조가 가능합니다. ASA는 ID 인증서부터 시작하여 부속 CA 체인을 따라 올라가면서 CRL(Certificate Revocation List)과 대조하는 방식으로 서드파티 인증서를 평가합니다.

다음은 사용 가능한 각기 다른 디지털 인증서의 유형에 대한 설명입니다.

- CA 인증서는 다른 인증서에 서명하는 데 사용되며 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.
- CA는 ID 인증서도 발급하는데, 이는 특정 시스템이나 호스트를 위한 인증서입니다.
- 코드 서명자 인증서는 특수한 인증서로서 코드 서명을 위한 디지털 서명을 만드는 데 사용합니다. 서명된 코드 자체에서 인증서의 출처를 나타냅니다.

로컬 CA는 독립적인 CA 기능을 ASA에 통합하고, 인증서를 배포하고, 발급된 인증서에 대해 안전한 폐기 검사를 실시합니다. 로컬 CA는 웹사이트 로그인 페이지를 통한 사용자 등록 기능과 함께 안전하고 구성 가능한 내부 인증서 인증 권한을 제공합니다.

참고 CA 인증서와 ID 인증서는 사이트 대 사이트(site-to-site) VPN 연결과 원격 액세스 VPN 연결 모두에 적용됩니다. 이 문서의 절차는 ASDM GUI에서 원격 액세스 VPN을 사용하는 것을 대상으로 합니다.

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 상황에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다.

디지털 인증서를 사용하여 인증할 경우, 적어도 하나의 ID 인증서와 이를 발급한 CA 인증서가 ASA에 있어야 합니다. 이 컨피그레이션에서는 복수의 ID, 루트, 인증서 계층 구조가 가능합니다. 다음은 사용 가능한 각기 다른 디지털 인증서의 유형에 대한 설명입니다.

- CA 인증서는 다른 인증서에 서명하는 데 사용되며 자체 서명되며 루트 인증서라고도 합니다.
- 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. CA는 VeriSign과 같이 신뢰받는 서드파티이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다.

팁 인증서 구성 및 로드 밸런싱이 포함된 시나리오의 예는 URL https://supportforums.cisco.com/docs/DOC-5964에서 확인하십시오.

공개 키 암호화

공개 키 암호 방식에 의한 디지털 서명은 디바이스와 사용자를 인증할 방법을 제공합니다. RSA 암호화 시스템과 같은 공개 키 암호 방식에서는 각 사용자가 공개 키와 개인 키로 구성된 키 쌍을 갖습니다. 키는 상호 보완적 역할을 하는데, 둘 중 하나의 키로 암호화된 것은 다른 하나의 키를 사용하여 해독할 수 있습니다.

간단하게 설명하자면, 개인 키를 사용하여 데이터를 암호화할 때 서명이 생성됩니다. 이 서명이 데이터에 첨부되어 수신자에게 전송됩니다. 수신자는 발신자의 공개 키를 데이터에 적용합니다. 데이터와 함께 보내진 서명이 공개 키를 데이터에 적용한 결과와 일치하면 메시지가 유효한 것으로 확인됩니다.

이 프로세스에서는 수신자가 발신자의 공개 키 사본을 가지고 있어야 하며 이 키가 발신자를 가장하는 누군가가 아닌 발신자 본인의 것이어야 합니다.

발신자의 공개 키를 취득하는 것은 대개 외부에서 이루어지거나 설치 시 수행되는 어떤 작업을 통해 이루어집니다. 예를 들어, 대부분의 웹 브라우저는 기본적으로 여러 CA의 루트 인증서가 구성되어 있습니다. VPN의 경우 IPsec의 구성 요소인 IKE 프로토콜에서 보안 연결을 설정하기에 앞서 피어(peer) 디바이스를 인증하는 데 디지털 서명을 사용할 수 있습니다.

인증서 확장성

디지털 인증서가 없으면 각 IPsec 피어에서 통신 대상인 피어를 하나씩 구성해야 합니다. 따라서 네트워크에 새 피어를 추가할 때마다 이 피어가 안전하게 통신하려는 개별 피어의 컨피그레이션을 변경해야 합니다.

디지털 인증서를 사용하면 각 피어가 CA에 등록됩니다. 두 피어가 통신을 시도할 때 서로 인증서를 교환하고 데이터에 디지털 서명을 하여 상대방을 인증합니다. 새로운 피어가 네트워크에 추가되면 그 피어를 CA에 등록하며, 나머지 피어 중 어느 것도 수정할 필요 없습니다. 새 피어가 IPsec 연결을 시도할 때 인증서가 자동으로 교환되고 이 피어는 인증될 수 있습니다.

CA를 이용할 경우, 피어가 원격 피어로 인증서를 보내고 공개 키 암호 작업을 수행하는 방법으로 원격 피어에 자신을 인증합니다. 각 피어가 CA에서 발급한 자신의 고유한 인증서를 보냅니다. 이러한 프로세스는 각 인증서가 해당 피어의 공개 키를 캡슐화하고 각 인증서가 CA에 의해 인증되며 모든 참여 피어가 CA를 인증 기관으로 인정하기 때문에 효과적입니다. 이를 RSA 서명을 사용하는 IKE라고 합니다.

피어는 인증서가 만료될 때까지 계속해서 여러 IPsec 세션을 위해, 여러 IPsec 피어로 인증서를 보낼 수 있습니다. 인증서가 만료되면 피어 관리자가 CA로부터 새로운 인증서를 받아야 합니다.

CA는 더 이상 IPsec에 참여하지 않는 피어의 인증서를 폐기할 수도 있습니다. 폐기된 인증서는 다른 피어에서 유효한 것으로 인정하지 않습니다. 해지된 인증서는 CRL에 나열되는데, 각 피어는 다른 피어가 보낸 인증서를 받아들이기 전에 이 목록을 점검할 수 있습니다.

어떤 CA는 그 구현에 RA가 포함되어 있습니다. RA란 CA를 위해 프록시 역할을 하는 서버로서 CA가 사용 불가능한 상태이더라도 CA 기능이 계속될 수 있게 합니다.

키 쌍

키 쌍은 다음과 같은 특성을 갖는 RSA 키 또는 ECDSA(Elliptic Curve Signature Algorithm) 키입니다.

- RSA 키는 SSH 또는 SSL에 사용할 수 있습니다.
- SCEP 등록에서는 RSA 키의 인증을 지원합니다.
- 최대 RSA 키 크기는 4096이고 기본값은 2048입니다.
- 최대 ECDSA 키 길이는 521이고 기본값은 384입니다.
- 서명 및 암호화에 모두 사용되는 범용 RSA 키 쌍을 생성하거나, 용도별로 각각 RSA 키 쌍을 생성할 수 있습니다. 서명용 키와 암호화용 키를 달리하면 키의 노출을 줄일 수 있습니다. SSL에서는 서명이 아닌 암호화 용도로 키를 사용하기 때문입니다. 그러나 IKE는 암호화가 아닌 서명을 위해 키를 사용합니다. 각각에 별도의 키를 사용하면 키 노출이 최소화됩니다.

신뢰 지점

신뢰 지점을 사용하여 CA와 인증서를 관리하고 추적할 수 있습니다. 신뢰 지점은 CA 또는 ID 쌍을 나타낸 것입니다. 신뢰 지점에는 CA의 ID, CA별 구성 파라미터, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

신뢰 지점을 정의했으면 CA를 지정해야 하는 명령에서 그 이름을 참조할 수 있습니다. 여러 신뢰 지점을 구성할 수 있습니다.

참고 Cisco ASA에서 여러 신뢰 지점이 동일한 CA를 공유하는 경우, 그중 하나만 사용자 인증서의 유효성 검사에 사용할 수 있습니다. 동일한 CA를 공유하는 신뢰 지점 중 어느 것을 해당 CA가 발급한 사용자 인증서의 유효성 검사에 사용할 것인가는 **support-user-cert-validation** 명령을 사용하여 제어합니다.

자동 등록의 경우, 등록 URL과 함께 신뢰 지점을 구성해야 하고 그 신뢰 지점이 가리키는 CA가 네트워크에서 사용 가능하고 SCEP를 지원해야 합니다.

신뢰 지점과 연결된 키 쌍 및 발급된 인증서를 PKCS12 형식으로 내보내고 가져올 수 있습니다. 이 형식은 신뢰 지점 구성을 다른 ASA에서 수동으로 복제하는 데 유용합니다.

인증서 등록

ASA에서는 신뢰 지점별로 1개의 CA 인증서가 필요하며, 신뢰 지점에서 사용하는 키의 구성에 따라 ASA 자체를 위한 인증서가 1개 또는 2개 필요합니다. 신뢰 지점에서 서명과 암호화에 각기 다른 RSA 키를 사용할 경우 ASA에서는 용도별로 하나씩, 2개의 인증서가 필요합니다. 다른 키 컨피그레이션에서는 인증서 1개만 있으면 됩니다.

ASA에서는 SCEP 자동 등록과 수동 등록을 지원합니다. 즉 터미널에 곧바로 base64 인코딩 인증서를 붙여넣을 수 있습니다. Site-to-Site VPN에서는 각 ASA를 등록해야 합니다. 원격 액세스 VPN에서는 각 ASA와 각 원격 액세스 VPN 클라이언트를 등록해야 합니다.

SCEP 요청을 위한 프록시

ASA에서는 AnyConnect와 서드파티 CA 사이에서 SCEP 요청을 프록시할 수 있습니다. CA는 프록시의 역할을 하는 경우에만 ASA에 대한 액세스가 필요합니다. ASA에서 이 서비스를 제공하려면 ASA에서 등록 요청을 보내기 전에 사용자가 AAA에서 지원되는 방법 중 하나를 사용하여 인증해야 합니다. 호스트 스캔 및 동적 액세스 정책을 사용하여 등록 자격 요건 규칙을 적용할 수도 있습니다.

ASA에서는 AnyConnect SSL 또는 IKEv2 VPN 세션에만 이 기능을 지원합니다. Cisco IOS CS, Windows Server 2003 CA, Windows Server 2008 CA 등 SCEP 규격을 준수하는 모든 CA를 지원합니다.

클라이언트리스(브라우저 기반) 액세스에서는 SCEP 프록시를 지원하지 않습니다. 단, WebLaunch(클라이언트 없이 시작된 AnyConnect)는 이를 지원합니다.

ASA에서는 인증서 폴링을 지원하지 않습니다.

ASA에서는 이 기능을 위한 로드 밸런싱을 지원합니다.

해지 검사

발급된 인증서는 일정한 기간 동안 유효합니다. CA가 유효 기한 만료 전에, 이를테면 보안상의 이유로 또는 이름이나 연결의 변경 때문에 인증서를 폐기하는 경우도 있습니다. CA는 정기적으로 폐기 인증서 목록에 서명하여 이를 배포합니다. 폐기 검사를 활성화할 경우, ASA에서는 인증 목적으로 인증서를 사용할 때마다 CA가 인증서를 폐기하지 않았음을 확인해야 합니다.

폐기 검사를 활성화하면 ASA에서는 PKI 인증서 유효성 검사 과정에서 인증서 폐기 상태를 확인합니다. 이를 위해 CRL 검사, OCSP 또는 둘 다 사용할 수 있습니다. OCSP는 CRL 검사 방법에서 오류가 생긴 경우(예: 서버를 사용할 수 없다는 메시지 표시)에만 사용합니다.

CRL 검사에서 ASA는 CRL에 대한 검색, 구문 분석, 캐싱을 수행합니다. CRL은 폐기된 인증서 및 폐기되지 않은 인증서와 해당 인증서 일련 번호의 전체 목록입니다. ASA에서는 ID 인증서부터 시작하여 부속 CA 체인을 따라 올라가면서 권한 폐기 목록이라고도 하는 CRL을 토대로 인증서를 평가합니다.

OCSP는 보다 확장 가능한 방식으로 폐기 상태를 검사합니다. 즉 특정 인증서의 상태를 쿼리하는 VA(validation authority)를 통해 인증서 상태를 로컬화합니다.

지원되는 **CA** 서버

ASA에서는 다음과 같은 CA 서버를 지원합니다.

Cisco IOS CS, ASA 로컬 CA 및 타사 X.509 규격 준수 CA 벤더(다음을 포함하되 이에 국한되지 않음):

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL은 ASA에서 유효 기한이 지나지 않은 인증서가 해당 발급 CA에 의해 폐기되었는지를 확인할 수 있는 방법 중 하나입니다. CRL 컨피그레이션은 신뢰 지점 컨피그레이션에 포함되어 있습니다.

ASA에서 인증서를 인증할 때마다 반드시 CRL 검사를 수행하도록 **revocation-check crl** 명령을 사용하여 구성할 수 있습니다. 또한 **revocation-check crl none** 명령을 사용하여 CRL 검사를 선택 사항으

로 설정할 수도 있습니다. 그러면 CA에서 업데이트된 CRL 데이터를 제공할 수 없는 경우에도 인증서 인증에 성공할 수 있습니다.

ASA에서는 HTTP, SCEP 또는 LDAP을 사용하여 CA에서 CRL을 검색할 수 있습니다. 각 신뢰 지점에 대해 검색된 CRL은 신뢰 지점별로 구성 가능한 기간만큼 캐시에 저장할 수 있습니다.

ASA에서는 CRL을 캐시하기 위해 구성된 시간보다 더 오래 CRL을 캐시한 경우 CRL을 너무 오래되어 신뢰할 수 없거나 "시간이 경과된" 상태로 간주합니다. ASA에서는 다음 번에 인증서 인증에서 시간이 경과된 CRL에 대한 검사를 필요로 할 때 CRL의 새로운 버전을 검색하려고 시도합니다.

CRL 항목 제한을 초과하면 사용자 연결/인증서에 대해 폐기 검사 장애가 발생할 수 있습니다. Syslog는 CRL당 항목의 최대 수가 65534를 초과하는 경우 처리해야 할 항목이 너무 많다는 메시지를 반환합니다.

ASA에서 CRL을 캐시하는 시간은 다음과 같은 2가지 변수에 따라 결정됩니다.

- **cache-time** 명령에서 지정한 시간(분). 기본값은 60분입니다.
- 검색된 CRL의 NextUpdate 필드. 이 필드가 CRL에 없을 수도 있습니다. ASA에서 NextUpdate 필드를 필수 항목으로 하고 사용할 것인가는 **enforcenextupdate** 명령으로 제어합니다.

ASA에서는 이 2가지 변수를 다음과 같이 사용합니다.

- NextUpdate 필드가 필수 항목이 아닐 경우, ASA에서는 **cache-time** 명령으로 지정된 기간이 지나면 CRL을 오래된 것으로 표시합니다.
- NextUpdate 필드가 필수 항목일 경우, ASA에서는 **cache-time** 명령으로 지정된 값과 NextUpdate 필드의 값 중 더 빠른 시점에 CRL을 오래된 것으로 표시합니다. 예를 들어, **cache-time** 명령에서 100분으로 설정되었고 NextUpdate 필드에서 다음 업데이트가 70분 후라고 지정되었다면 ASA에서는 70분이 지나면 CRL을 오래된 것으로 표시합니다.

ASA에서 어떤 신뢰 지점에 대해 캐시된 모든 CRL을 저장하기에 메모리가 부족할 경우, 가장 오래전에 사용한 CRL을 삭제하여 새로 검색된 CRL을 위한 공간을 마련합니다.

OCSP

OCSP는 ASA에서 유효 기한이 지나지 않은 인증서가 해당 발급 CA에 의해 폐기되었는지를 확인할 수 있는 방법 중 하나입니다. OCSP 컨피그레이션은 신뢰 지점 컨피그레이션에 포함되어 있습니다.

OCSP는 VA(OCSP 서버, *responder*라고도 함)에서 인증서 상태를 로컬화합니다. ASA에서는 VA에 특정 인증서의 상태를 쿼리합니다. 이는 CRL 검사보다 확장 가능한 방법이고 더 최신 버전의 폐기 상태 정보를 제공합니다. 또한 PKI 설치 규모가 큰 조직에서 보안 네트워크를 구축하고 확장하는 데 유용합니다.

참고 ASA에서는 OCSP 응답에서 5초의 시간차를 허용합니다.

ASA에서 인증서를 인증할 때마다 반드시 OCSP 검사를 수행하도록 **revocation-check ocsp** 명령을 사용하여 구성할 수 있습니다. 또한 **revocation-check ocsp none** 명령을 사용하여 OCSP 검사를 선택 사

항으로 설정할 수도 있습니다. 그러면 VA에서 업데이트된 OCSP 데이터를 제공할 수 없는 경우에도 인증서 인증에 성공할 수 있습니다.

OCSP에서는 3가지 방법으로 OCSP 서버 URL을 정의할 수 있습니다. ASA에서는 다음 순서대로 이 서버를 사용합니다.

1. **match certificate** 명령을 사용하여 일치 인증서 재정의(override) 규칙에 정의한 OCSP URL
2. **ocsp url** 명령을 사용하여 구성한 OCSP URL
3. 클라이언트 인증서의 AIA 필드

참고 자체 서명된 OCSP responder 인증서의 유효성 검사를 위한 신뢰 지점을 구성하려면, 자체 서명된 responder 인증서를 신뢰할 수 있는 CA 인증서로 간주하면서 해당 신뢰 지점으로 가져옵니다. 그런 다음 클라이언트 인증서의 유효성을 검사하는 신뢰 지점에서 **match certificate** 명령을 구성하여 responder 인증서의 유효성 검사에 자체 서명된 OCSP responder 인증서가 포함된 신뢰 지점을 사용합니다. 클라이언트 인증서의 유효성 검사 경로에 속하지 않은 responder 인증서의 유효성 검사를 구성하는 데에도 동일한 절차를 사용합니다.

일반적으로 OCSP 서버(responder) 인증서가 OCSP 응답에 서명합니다. ASA에서는 응답을 받은 후 responder 인증서의 확인을 시도합니다. 일반적으로 CA는 OCSP responder 인증서의 수명을 상대적으로 짧게 설정하여 문제가 발생할 가능성을 최소화합니다. 일반적으로 CA는 responder 인증서에 ocsp-no-check 확장도 포함하는데, 이는 해당 인증서에 대해 폐기 상태 검사가 필요하지 않음을 나타냅니다. 그러나 이 확장이 없을 경우 ASA에서는 신뢰 지점에 지정된 방식을 사용하여 폐기 상태 검사를 시도합니다. responder 인증서가 확인 불가할 경우 폐기 검사는 실패합니다. 이러한 상황을 방지하기 위해 **revocation-check none** 명령을 사용하여 responder 인증서의 유효성을 검사하는 신뢰 지점을 구성하고 r**evocation-check ocsp** 명령을 사용하여 클라이언트 인증서를 구성합니다.

로컬 CA

로컬 CA는 다음 작업을 수행합니다.

- ASA에서의 기본 CA 작업 통합
- 인증서 배포
- 발급된 인증서에 대해 안전한 폐기 검사 실시
- ASA에서 브라우저 기반 및 클라이언트 기반 SSL VPN 연결에 사용할 CA 제공
- 외부 인증서 권한 부여를 이용할 필요 없이 사용자에게 신뢰할 수 있는 디지털 인증서 제공
- 안전한 내부 인증서 인증 권한 제공, 웹사이트 로그인을 통한 간편한 사용자 등록 기능 제공

로컬 **CA** 파일의 저장소

ASA에서는 사용자 정보, 발급된 인증서, 폐기 목록의 액세스 및 구현에 로컬 CA 데이터베이스를 사용합니다. 이 데이터베이스는 기본적으로 로컬 플래시 메모리에 상주하지만, ASA에 마운트되고 액세스 가능한 외부 파일 시스템에 상주하도록 구성할 수도 있습니다.

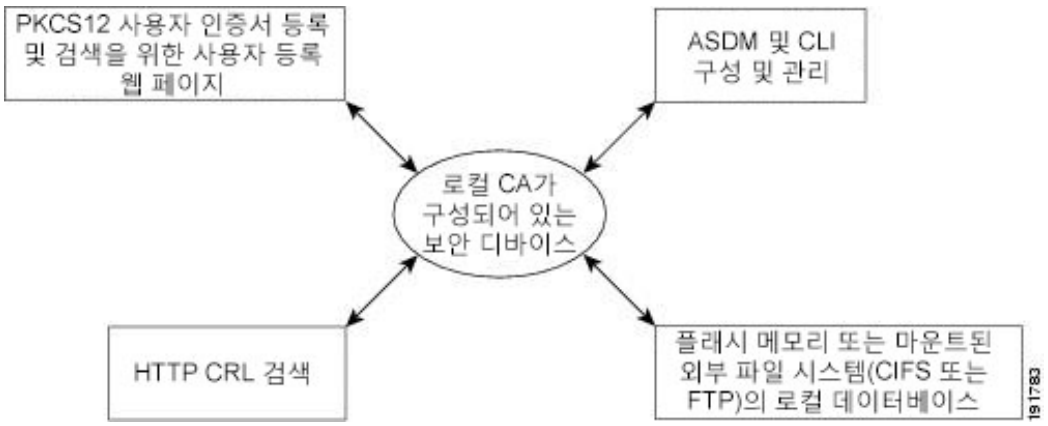
로컬 CA 사용자 데이터베이스에 저장할 수 있는 사용자 수에는 제한이 없습니다. 그러나 플래시 메모리 저장소 문제가 생길 경우, syslog가 생성되어 관리자에게 조치를 취하도록 알리며 저장소 문제가 해결될 때까지 로컬 CA를 사용하지 못할 수도 있습니다. 플래시 메모리는 사용자 수가 3,500명 이하인 데이터베이스를 저장할 수 있습니다. 사용자 수가 3,500명이 넘는 데이터베이스는 외부 저장소가 필요합니다.

로컬 **CA** 서버

ASA에서 로컬 CA 서버를 구성한 다음에는 사용자가 웹 사이트에 로그인하고 사용자 이름과 로컬 CA 관리자가 제공한 일회용 비밀번호를 입력하여 등록 자격을 검증하는 방법으로 인증서에 등록할 수 있습니다.

다음 그림에서는 로컬 CA 서버가 ASA에 상주하고 있으며 웹 사이트 사용자의 등록 요청, 다른 인증서 유효성 검사 디바이스 및 ASA의 CRL 문의를 처리함을 확인할 수 있습니다. 로컬 CA 데이터베이스와 구성 파일은 ASA 플래시 메모리(기본 저장소) 또는 별도의 스토리지 디바이스에서 유지 관리됩니다.

그림 ***57:*** 로컬 ***CA***



인증서 및 사용자 로그인 자격 증명

다음 섹션에서는 인증 및 권한 부여에 인증서와 사용자 로그인 자격 증명(사용자 이름과 비밀번호)을 사용하는 여러 가지 방법에 대해 설명합니다. 이 방법은 IPsec, AnyConnect, 클라이언트리스 SSL VPN에 적용됩니다.

어떤 경우에도 LDAP 권한 부여에서는 비밀번호를 자격 증명으로 사용하지 않습니다. RADIUS 권한 부여에서는 모든 사용자의 공통 비밀번호 또는 사용자 이름을 비밀번호로 사용합니다.

사용자 로그인 자격 증명

기본적인 인증 및 권한 부여 방법에서는 사용자 로그인 자격 증명을 사용합니다.

- 인증
  - ASDM 연결 프로필이라고도 하는 터널 그룹의 인증 서버 그룹 설정을 통해 활성화
  - 사용자 이름과 비밀번호를 자격 증명으로 사용
- 권한 부여
  - ASDM 연결 프로필이라고도 하는 터널 그룹의 권한 부여 서버 그룹 설정을 통해 활성화
  - 사용자 이름을 자격 증명으로 사용

인증서

사용자 디지털 인증서가 구성된 경우 ASA에서는 먼저 인증서의 유효성을 검사합니다. 그러나 인증서의 어떤 DN도 인증용 사용자 이름으로 사용하지 않습니다.

인증과 권한 부여 모두 활성화된 경우 ASA에서는 사용자 로그인 크리덴셜을 사용자 인증 및 권한 부여 둘 다에 사용합니다.

- 인증
  - 인증 서버 그룹 설정에 의해 활성화됨
  - 사용자 이름과 비밀번호를 자격 증명으로 사용
- 권한 부여
  - 권한 부여 서버 그룹 설정에 의해 활성화됨
  - 사용자 이름을 자격 증명으로 사용

인증이 비활성화되고 권한 부여가 활성화된 경우 ASA에서는 기본 DN 필드를 권한 부여에 사용합니다.

- 인증
  - 인증 서버 그룹 설정에 의해 비활성화됨(None으로 설정됨)
  - 자격 증명 사용 안 함
- 권한 부여
  - 권한 부여 서버 그룹 설정에 의해 활성화됨
  - 인증서 기본 DN 필드의 사용자 이름 값을 자격 증명으로 사용

참고 기본 DN 필드가 인증서에 없을 경우 ASA에서는 보조 DN 필드 값을 권한 부여 요청의 사용자 이름으로 사용합니다.

예를 들어, 다음 주체 DN(Subject DN) 필드와 값을 갖는 사용자 인증서가 있다고 가정합니다.

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

기본 DN = EA(E-mail Address)이고 보조 DN = CN(Common Name)이라면 권한 부여 요청에서 쓰일 사용자 이름은 anyuser@example.com입니다.

디지털 인증서 지침

이 섹션에서는 디지털 인증서를 구성하기 전에 확인해야 하는 지침 및 제한사항에 대해 설명합니다.

상황 모드 지침

- 서드파티 CA의 경우 단일 상황 모드에서만 지원됩니다.

장애 조치 지침

- 스테이트풀 장애 조치에서는 세션 복제를 지원하지 않습니다.
- 로컬 CA에 대해서는 장애 조치를 지원하지 않습니다.

IPv6 지침

IPv6를 지원하지 않습니다.

로컬 **CA** 인증서

- ASA가 인증서를 지원하도록 올바르게 구성되어야 합니다. ASA가 잘못 구성되면 등록이 실패하거나 부정확한 정보가 들어 있는 인증서를 요청할 수 있습니다.
- ASA의 호스트 이름과 도메인 이름이 올바르게 구성되어야 합니다. 현재 구성된 호스트 이름 및 도메인 이름을 보려면 **show running-config** 명령을 입력합니다.
- CA 구성에 앞서 ASA 시계가 정확하게 설정되어야 합니다. 인증서는 유효 기간이 시작하고 종료하는 날짜와 시간이 있습니다. ASA에서는 CA에 등록하여 인증서를 받을 때 현재 시간이 인증서의 유효 기간 안에 포함되는지 확인합니다. 그 범위를 벗어나면 등록이 실패합니다.
- 로컬 CA 인증서가 만료되기 30일 전에 롤오버 대체 인증서가 생성되고 syslog 메시지를 통해 관리자에게 로컬 CA 롤오버 시점임을 알립니다. 현재 인증서가 만료되기 전에 새 로컬 CA 인증서를 필요한 모든 디바이스에 가져와야 합니다. 관리자가 응답하여 롤오버 인증서를 새로운 로컬 CA 인증서로 설치하지 않을 경우, 유효성 검사가 실패할 수 있습니다.

- 인증서가 만료되면 로컬 CA 인증서는 동일한 키 쌍을 사용하여 자동으로 롤오버합니다. 롤오버 인증서는 base64 형식으로 내보낼 수 있습니다.

  다음 예는 base64 인코딩 로컬 CA 인증서를 보여줍니다.

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP 프록시 지원

- ASA 및 Cisco ISE 정책 서비스 노드가 동일한 NTP 서버를 사용하여 동기화되는지 확인합니다.
- 엔드포인트에서 AnyConnect Secure Mobility Client 3.0 이상이 실행되고 있어야 합니다.
- 그룹 정책의 연결 프로필에 구성된 인증 방법이 AAA와 인증서 인증을 모두 사용하도록 설정되어야 합니다.
- IKEv2 VPN 연결을 위한 SSL 포트가 열려 있어야 합니다.
- CA가 자동 허용(auto-grant) 모드여야 합니다.

로컬 **CA** 인증서 데이터베이스

로컬 CA 인증서 데이터베이스를 유지 관리하려면, 데이터베이스의 변경 사항이 발생할 때마다 **write memory** 명령을 사용하여 인증서 데이터베이스 파일인 LOCAL-CA-SERVER.cdb를 저장해야 합니다. 로컬 CA 인증서 데이터베이스에는 다음 파일이 있습니다.

- LOCAL-CA-SERVER.p12 파일은 로컬 CA 인증서 및 키 쌍의 아카이브로서 로컬 CA 서버가 처음으로 활성화될 때 생성됩니다.
- LOCAL-CA-SERVER.crl 파일은 실제 CRL입니다.
- LOCAL-CA-SERVER.ser 파일은 발급된 인증서의 일련 번호를 지속적으로 추적합니다.

추가 지침

- CA 서버 또는 클라이언트로 구성된 ASA의 경우, 인증서 유효 기한을 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빠르게 설정합니다. 이 지침은 서드파티 벤더로부터 가져온 인증서에도 해당됩니다.
- 장애 조치가 활성화된 상태에서는 로컬 CA를 구성할 수 없습니다. 장애 조치 없는 독립형 ASA에 대해서만 로컬 CA 서버를 구성할 수 있습니다. 자세한 내용은 CSCty43366을 참조하십시오.
- 인증서 등록이 완료되면 ASA는 사용자의 키 쌍과 인증서 체인이 들어 있는 PKCS12 파일을 저장합니다. 이를 위해 각 등록에서 약 2KB의 플래시 메모리 또는 디스크 공간이 필요합니다. 실제

디스크 공간 용량은 구성된 RSA 키 크기 및 인증서 필드에 따라 달라집니다. 사용 가능한 플래시 메모리의 양이 제한된 ASA에서 보류 중인 인증서 등록을 다수 추가할 때 이 점을 염두에 두십시오. 이 PKCS12 파일은 구성된 등록 검색 타임아웃에 도달할 때까지 플래시 메모리에 저장되기 때문입니다. 크기가 2048 이상인 키를 사용하는 것이 좋습니다.

- **lifetime ca-certificate** 명령은 로컬 CA 서버 인증서가 처음 생성될 때(즉, 처음에 로컬 CA 서버를 구성하고 **no shutdown** 명령을 실행할 때) 효력을 발휘합니다. CA 인증서가 만료되면, 구성된 수명 값을 사용하여 새 CA 인증서를 생성합니다. 기존 CA 인증서의 수명 값은 변경할 수 없습니다.
- ASA에서 관리 인터페이스에 대한 ASDM 트래픽 및 HTTPS 트래픽을 보호하는 데 ID 인증서를 사용하도록 구성해야 합니다. SCEP로 자동 생성된 ID 인증서는 재부팅할 때마다 다시 생성되므로, 각자의 ID 인증서를 수동으로 설치해야 합니다. SSL에만 적용되는 이 절차의 예는 다음 URL에서 확인할 수 있습니다. http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- ASA와 AnyConnect 클라이언트는 X520Serialnumber 필드(Subject Name의 일련 번호)가 PrintableString 형식인 인증서에 대해서만 유효성 검사를 수행할 수 있습니다. 일련 번호 형식에서 UTF8과 같은 인코딩을 사용할 경우 인증서 권한 부여가 실패합니다.
- ASA에 인증서 매개변수를 가져올 때 유효한 문자와 값만 사용합니다.
- 와일드카드(*) 기호를 사용하려면 문자열 값에서 이 문자가 허용되는 인코딩을 CA 서버에서 사용해야 합니다. RFC 5280에서 UTF8String 또는 PrintableString 중 하나를 사용하도록 권장하지만, UTF8String을 사용해야 합니다. PrintableString은 와일드카드를 유효한 문자로 인식하지 않기 때문입니다. ASA에서는 가져오기 과정에서 유효하지 않은 문자 또는 값이 발견되면 가져온 인증서를 거부합니다. 예를 들면 다음과 같습니다.

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

디지털 인증서 구성

다음 주제에서는 디지털 인증서를 구성하는 방법에 대해 설명합니다.

키 쌍 구성

키 쌍을 생성하거나 제거하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 기본 범용 RSA 키 쌍 1개를 생성합니다.

crypto key generate rsa modulus 2048

예제:

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

기본 키 모듈러스는 2048이지만 필요한 크기를 얻으려면 모듈러스를 명시적으로 지정해야 합니다. 키의 이름은 Default-RSA-Key로 지정됩니다.

ECDSA(Elliptic Curve Signature Algorithm) 키도 필요한 경우, Default-ECDSA-Key를 생성할 수 있습니다. 기본 길이는 384이지만 256 또는 521을 사용할 수도 있습니다.

crypto key generate ecdsa elliptic-curve 384

단계 **2** (선택 사항) 고유한 이름의 추가 키를 생성합니다.

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

예제:

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

이 레이블은 해당 키 쌍을 사용하는 신뢰 지점에서 참조합니다.

RSA 키의 경우, 모듈러스는 512, 768, 1024, 2048, 4096 중 하나(비트 단위)일 수 있습니다.

ECDSA 키의 경우, EC(Elliptic Curve)는 256, 384, 521 중 하나(비트 단위)일 수 있습니다.

단계 **3** 생성한 키 쌍을 확인합니다.

show crypto key mypubkey {**rsa** | **ecdsa**}

예제:

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

단계 **4** 생성한 키 쌍을 저장합니다.

write memory

예제:

```
ciscoasa(config)# write memory
```

단계 **5** 필요한 경우 키 쌍을 새로 생성할 수 있도록 기존 키 쌍을 제거합니다.

crypto key zeroize {**rsa** | **ecdsa**}

예제:

```
ciscoasa(config)# crypto key zeroize rsa
```

단계 **6** (선택 사항) 로컬 CA 서버 인증서 및 키 쌍을 보관합니다.

copy

예제**:**

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

이 명령을 사용하면 ASA의 로컬 CA 서버 인증서와 키 쌍 및 모든 파일이 FTP 또는 TFTP를 사용하여 복사됩니다.

참고 가급적 자주 모든 로컬 CA 파일을 백업해야 합니다.

예

다음 예에서는 키 쌍을 제거하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

신뢰 지점 구성

신뢰 지점을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** ASA에서 인증서를 받아야 하는 CA의 신뢰 지점을 생성합니다.

crypto ca trustpoint *trustpoint_name*

예제**:**

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

crypto ca trustpoint 구성 모드를 시작하십시오. 여기서는 CA 관련 신뢰 지점 파라미터를 제어하는데, 3단계부터 이 파라미터를 구성할 수 있습니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 지정된 신뢰 지점으로 SCEP를 사용한 자동 등록을 요청하고 등록 URL을 구성합니다.

  enrollment protocol scep *url*

예:

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- 지정된 신뢰 지점으로 CMP를 사용한 자동 등록을 요청하고 등록 URL을 구성합니다.

  enrollment protocol cmp*url*

  예

```
ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- CA에서 가져온 인증서를 터미널에 붙여넣어 지정된 신뢰 지점으로 수동 등록을 요청합니다.

  enrollment terminal

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
```

- 자체 서명 인증서를 요청합니다.

  enrollment self

단계 **3** 위의 단계에서 CMP를 사용하도록 신뢰 지점이 구성된 경우, 필요에 따라 자동으로 인증서를 요청하는 기능을 활성화할 수 있습니다. 이 자동화는 CMPv2 자동 업데이트 사용 여부, 트리거되는 시간 및 새 키 쌍이 생성되는지 여부를 제어하는 구성 가능한 트리거를 기반으로 합니다. 추후 자동 등록이 필요한 인증서의 절대 수명 백분율을 입력하고 인증서를 갱신할 때 새 키를 생성할지를 지정합니다.

```
[no] auto-enroll [<percent>] [regenerate]
```

단계 **4** 사용 가능한 CRL 구성 옵션을 지정합니다.

revocation-check crl none

예제**:**

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl none
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

참고 필수 또는 선택 사항인 CRL 검사를 활성화하려면 인증서 취득 후 CRL 관리를 위해 신뢰 지점을 구성해야 합니다.

단계 **5** 기본 제약 조건 확장 및 CA 플래그를 활성화하거나 비활성화합니다.

[**no**] **ca-check**

기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있으면 인증서의 공용 키를 사용하여 인증서 서명을 검증할 수 있는 것입니다.

ca-check 명령은 기본적으로 활성화되어 있으므로 기본 제약 조건 및 CA 플래그를 비활성화하려는 경우에만 이 명령을 입력해야 합니다.

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

단계 **6** 등록 과정에서 CA에게 지정된 이메일 주소를 인증서의 SAN(Subject Alternative Name) 확장에 포함하도록 요청합니다.

email *address*

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

단계 **7** (선택사항) 재시도 기간(분)을 지정하며, SCEP 등록에만 적용됩니다.

enrollment retry period

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

단계 **8** (선택사항) 허용된 재시도 최대 횟수를 지정하며, SCEP 등록에만 적용됩니다.

enrollment retry count

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

단계 **9** 등록 과정에서 CA에게 특정 FQDN(Fully Qualified Domain Name)을 인증서의 SAN(Subject Alternative Name) 확장에 포함하도록 요청합니다.

fqdn *fqdn*

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

단계 **10** 등록 시 ASA의 IP 주소를 인증서에 포함해 달라고 CA에 요청합니다.

ip-address *ip-address*

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

단계 **11** 공개 키를 인증할 키 쌍을 지정합니다.

keypair *name*

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

단계 **12** CMP에 대해 구성된 신뢰 지점이 있는 경우에만 CMP 수동 및 자동 등록을 위해 EDCSA 키 또는 RSA 키를 생성할지 여부를 결정합니다.

```
no keypair name | [rsa modulus 1024|2048|4096|512|768] | [edcsa elliptic-curve 256|384|521]
```

단계 **13** OCSP responder 인증서의 유효성 검사에 사용할 OCSP URL 재정의 및 신뢰 지점을 구성합니다.

match certificate map-name override ocsp

예제**:**

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

단계 **14** OCSP 요청에서 nonce 확장을 비활성화합니다. nonce 확장은 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지합니다.

ocsp disable-nonce

예제**:**

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

단계 **15** ASA에서 신뢰 지점과 연결된 모든 인증서를 검사하는 데 클라이언트 인증서의 AIA 확장에 지정된 서버 대신 사용할 OCSP 서버를 구성합니다.

ocsp url

예제**:**

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

단계 **16** 등록 과정에서 CA에 등록되는 챌린지 구문을 지정합니다. 일반적으로 CA는 후속 폐기(revocation) 요청을 인증하는 데 이 구문을 사용합니다.

password *tring*

예제**:**

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

단계 **17** 해지 검사 방법(CRL, OCSP, 없음)을 하나 이상 설정합니다.

revocation check

예제**:**

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

단계 **18** 등록 과정에서 CA에게 지정된 주체 DN을 인증서에 포함하도록 요청합니다. DN 문자열에 쉼표가 있을 경우 큰따옴표로 값 문자열을 묶습니다(예: O="Company, Inc.").

subject-name *X.500 name*

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

단계 **19** 등록 시 ASA 일련 번호를 인증서에 포함해 달라고 CA에 요청합니다.

serial-number

예제:

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

단계 **20** 실행 중인 구성을 저장합니다.

write memory

예제:

```
ciscoasa/contexta(config)# write memory
```

신뢰 지점의 **CRL** 구성

인증서 인증 과정에서 필수 또는 선택 사항인 CRL 검사를 사용하려면 신뢰 지점별로 CRL을 구성해야 합니다. 신뢰 지점의 CRL을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** CRL 구성을 수정할 신뢰 지점에 대해 crypto ca trustpoint 구성 모드를 시작합니다.

crypto ca trustpoint *trustpoint_name*

예제:

```
ciscoasa (config)# crypto ca trustpoint Main
```

참고 이 명령을 입력하기 전에 CRL을 활성화해야 합니다. 또한 CRL이 인증에 사용 가능한 상태여야 성공할 수 있습니다.

단계 **2** 현재 신뢰 지점에 대한 crl 구성 모드를 시작합니다.

crl configure

예제:

```
ciscoasa(config-ca-trustpoint)# crl configure
```

팁 모든 CRL 컨피그레이션 매개변수를 기본값으로 설정하려면 **default** 명령을 사용합니다. CRL 컨피그레이션 중에 언제라도 이 명령을 재입력하여 절차를 재시작할 수 있습니다.

단계 **3** 검색 정책을 구성하려면 다음 중 하나를 선택합니다.

- CRL은 인증된 인증서에 지정된 CRL 배포 지점에서만 검색됩니다.

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  참고 SCEP 검색은 인증서에 지정된 배포 지점에서 지원하지 않습니다.

- CRL은 사용자가 구성하는 URL에서만 검색됩니다.

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- CRL은 인증된 인증서에 지정된 CRL 배포 지점 및 사용자가 구성하는 URL에서 검색됩니다.

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

단계 **4** CRL 정책 구성 시 **static** 또는 **both** 키워드를 사용한 경우 CRL 검색용 URL을 구성해야 합니다. 1순위부터 5순위까지 최대 5개의 URL을 입력할 수 있습니다. 인수 *n*은 URL에 할당된 순위입니다.

url *n url*

예제**:**

```
ciscoasa (config-ca-crl)# url 2 http://www.example.com
```

URL을 제거하려면 **no url** *n* 명령을 사용합니다.

단계 **5** HTTP, LDAP 또는 SCEP를 CRL 검색 방법으로 지정합니다.

protocol http | **ldap** | **scep**

예제**:**

```
ciscoasa(config-ca-crl)# protocol http
```

단계 **6** ASA에서 현재 신뢰 지점의 CRL을 캐시하는 시간을 구성합니다. *refresh-time* 인수는 ASA에서 CRL을 오래된 것으로 간주할 때까지의 경과 시간(분)입니다.

cache-time *refresh-time*

예제**:**

```
ciscoasa(config-ca-crl)# cache-time 420
```

단계 **7** 다음 중 하나를 선택합니다.

- CRL에 NextUpdate 필드가 있어야 합니다. 'Cisco'가 기본 설정입니다.

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- CRL에서 NextUpdate 필드가 없는 경우를 허용합니다.

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

단계 **8** LDAP이 검색 프로토콜로 지정된 경우 ASA에 대해 LDAP 서버를 식별합니다. DNS 호스트 이름 또는 IP 주소로 서버를 지정할 수 있습니다. 서버가 기본 포트인 389가 아닌 포트에서 LDAP 쿼리를 수신할 경우 포트 번호도 지정할 수 있습니다.

ldap-defaults *server*

예제**:**

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

참고 IP 주소 대신 호스트 이름을 사용하여 LDAP 서버를 지정할 경우, DNS를 사용하도록 ASA를 구성했는지 확인합니다.

단계 **9** LDAP 서버에서 자격 증명이 필요할 경우 CRL 검색을 허용합니다.

ldap-dn *admin-DN password*

예제**:**

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ
```

단계 **10** 지정된 신뢰 지점의 CA로부터 현재 CRL을 검색하고, 현재 신뢰 지점에 대해 CRL 구성을 테스트합니다.

crypto ca crl request *trustpoint*

예제**:**

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

단계 **11** 실행 중인 구성을 저장합니다.

write memory

예제:

```
ciscoasa (config)# write memory
```

신뢰 지점 구성 내보내기 또는 가져오기

신뢰 지점 구성을 내보내고 가져오려면 다음 단계를 수행합니다.

프로시저

단계 **1** 모든 연결된 키와 인증서를 포함한 신뢰 지점 구성을 PKCS12 형식으로 내보냅니다.

crypto ca export 신뢰 지점

예제:

```
ciscoasa(config)# crypto ca export Main
```

ASA에서는 터미널에 PKCS12 데이터를 표시합니다. 데이터를 복사할 수 있습니다. 신뢰 지점 데이터는 비밀번호로 보호됩니다. 그러나 신뢰 지점 데이터를 파일에 저장할 경우 파일이 안전한 위치에 있는지 확인합니다.

단계 **2** 신뢰 지점 구성과 연결된 키 쌍 및 발급된 인증서를 가져옵니다.

crypto ca import 신뢰 지점 **pkcs12**

예제:

```
ciscoasa(config)# crypto ca import Main pkcs12
```

ASA에서는 터미널에 base64 형식으로 텍스트를 붙여넣으라는 메시지를 표시합니다. 신뢰 지점과 함께 가져온 키 쌍에는 생성한 신뢰 지점의 이름과 일치하는 레이블이 지정됩니다.

참고 ASA에 동일한 CA를 공유하는 신뢰 지점이 있을 경우, CA를 공유하는 신뢰 지점 중 하나만 사용자 인증서의 유효성 검사에 사용할 수 있습니다. CA를 공유하는 신뢰 지점 중 어느 것을 해당 CA가 발급한 사용자 인증서의 유효성 검사에 사용할 것인가는 **support-user-cert-validation** 키워드를 사용하여 제어합니다.

예

다음 예에서는 신뢰 지점 Main의 PKCS12 데이터를 비밀번호 Wh0zits를 사용하여 내보냅니다.

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

다음 예에서는 신뢰 지점 Main에 PKCS12 데이터를 비밀번호 Wh0zits를 사용하여 수동으로 가져옵니다.

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

다음 예에서는 신뢰 지점 Main의 인증서를 수동으로 가져옵니다.

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

CA 인증서 맵 규칙 구성

인증서의 Issuer 및 Subject 필드를 기반으로 규칙을 구성할 수 있습니다. 생성한 규칙을 사용하면 **tunnel-group-map** 명령으로 IPsec 피어 인증서를 터널 그룹에 매핑할 수 있습니다.

CA 인증서 맵 규칙을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 구성하려는 규칙에 대한 CA 인증서 맵 구성 모드를 시작하고 규칙 시퀀스 번호를 지정합니다.

crypto ca certificate map [*map_name*]*sequence-number*

예제:

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

맵 이름을 지정하지 않으면 규칙이 기본 맵(DefaultCertificateMap)에 추가됩니다. 각 규칙 번호에 대해 일치시킬 필드를 하나 이상 지정할 수 있습니다.

단계 **2** 발급자 이름 또는 주체 이름을 지정합니다.

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

예제:

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

전체 값과 일치시키거나 일치시킬 속성을 지정할 수 있습니다. 유효한 속성은 다음과 같습니다.

- c — 국가
- cn — 공통 이름
- dc — 도메인 구성 요소
- dnq — DN 한정자
- ea — 이메일 주소
- genq — 세대 한정자
- gn — 이름
- i — 이니셜
- ip — IP 주소
- l — 구/군/시
- n — 이름
- o — 조직 이름
- ou — 조직 단위
- ser — 일련 번호
- sn — 성
- sp — 시/도
- t — 직함
- uid — 사용자 ID
- uname — 구조화되지 않은 이름

다음은 유효한 연산자입니다.

- eq—필드 또는 특성이 주어진 값과 같아야 합니다.
- ne—필드 또는 특성이 주어진 값과 같아서는 안 됩니다.
- co—필드 또는 특성의 일부 또는 전체가 주어진 값과 일치해야 합니다.
- nc—필드 또는 특성의 어떤 부분도 주어진 값과 일치해서는 안 됩니다.

단계 **3** 대체 주체 이름을 지정합니다.

alt-subject-name *operator string*

예제**:**

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

다음은 유효한 연산자입니다.

- eq — 필드가 주어진 값과 같아야 합니다.
- ne — 필드가 주어진 값과 같아서는 안 됩니다.
- co — 필드의 일부 또는 전체가 주어진 값과 일치해야 합니다.
- nc — 필드의 어떤 부분도 주어진 값과 일치해서는 안 됩니다.

단계 **4** 확장 키 사용을 지정합니다.

extended-key-usage *operator OID_string*

예제**:**

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

다음은 유효한 연산자입니다.

- co — 필드의 일부 또는 전체가 주어진 값과 일치해야 합니다.
- nc — 필드의 어떤 부분도 주어진 값과 일치해서는 안 됩니다.

유효한 OID 문자열은 다음과 같습니다.

- *string* — 사용자 정의 문자열입니다.
- clientauth — 클라이언트 인증(1.3.6.1.5.5.7.3.2)
- codesigning — 코드 서명(1.3.6.1.5.5.7.3.3)
- emailprotection — 보안 이메일 보호(1.3.6.1.5.5.7.3.4)
- ocspsigning — OCSP 서명(1.3.6.1.5.5.7.3.9)
- serverauth — 서버 인증(1.3.6.1.5.5.7.3.1)
- timestamping — 타임스탬프(1.3.6.1.5.5.7.3.8)

참조 ID 구성

ASA에서는 TLS 클라이언트 역할을 수행 중인 경우 RFC 6125에 정의된 대로 애플리케이션 서버의 ID 확인을 위한 규칙을 지원합니다. 이 RFC는 참조 ID(ASA에 구성됨)를 나타내고 제공된 ID(애플리

케이션 서버에서 전송됨)에 대해 확인을 수행하는 절차를 지정합니다. 표시되는 ID가 구성된 참조 ID에 대해 일치될 수 없는 경우 연결이 설정되지 않으며 오류가 기록됩니다.

서버는 연결을 설정하는 동안 ASA에 제공된 서버 인증서에서 하나 이상의 식별자를 포함하여 해당 ID를 제공합니다. 참조 ID는 연결을 설정하는 동안 서버 인증서에 제공된 ID와 비교할 수 있도록 ASA에 구성됩니다. 이러한 식별자는 RFC 6125에 지정된 4개의 식별자 유형의 특정 인스턴스입니다. 4개의 식별자 유형은 다음과 같습니다.

- CN_ID: 값이 도메인 이름의 전체 양식과 일치하는 CN(공통 이름) 유형의 속성 유형 및 값 쌍을 하나만 포함하는 인증서 주체 필드의 RDN(상대 고유 이름)입니다. CN 값은 일반 텍스트가 될 수 없습니다. CN-ID 참조 식별자는 애플리케이션 서비스를 식별하지 않습니다.
- DNS-ID: dNSName 유형의 subjectAltName 항목입니다. 이는 DNS 도메인 이름입니다. DNS-ID 참조 식별자는 애플리케이션 서비스를 식별하지 않습니다.
- SRV-ID: RFC 4985에 정의된 대로 이름 양식이 SRVName인 otherName 유형의 subjectAltName 항목입니다. 도메인 이름 및 애플리케이션 서비스 유형 둘 다 SRV-ID 식별자를 포함할 수 있습니다. 예를 들어, “_imaps.example.net”의 SRV-ID는 "example.net"이라는 DNS 도메인 이름 부분과 “imaps.”라는 애플리케이션 서비스 유형 부분으로 나눠집니다.
- URI-ID: uniformResourceIdentifier 유형의 subjectAltName 항목으로, 이 유형의 값은 RFC 3986에 지정된 “reg-name” 규칙과 일치하는 (i) “scheme” 및 (ii) “host” 구성 요소(또는 이에 해당하는 요소)를 둘 다 포함합니다. URI-ID 식별자는 IP 주소가 아닌 DNS 도메인 이름을 포함해야 하며 호스트 이름만 포함할 수 없습니다. 예를 들어, “sip:voice.example.edu”의 URI-ID는 “voice.example.edu”라는 DNS 도메인 이름 부분과 “sip”라는 애플리케이션 서비스 유형 부분으로 나눠집니다.

참조 ID는 이전에 사용되지 않은 이름으로 구성할 때 생성됩니다. 참조 ID가 생성되면 4개의 식별자 유형 및 연관된 값이 추가되거나 참조 ID에서 삭제될 수 있습니다. 참조 식별자는 애플리케이션 서비스를 식별하는 정보를 포함할 수 있으며 DNS 도메인 이름을 식별하는 정보를 포함해야 합니다.

시작하기 전에

- 참조 ID는 Syslog 서버 및 Smart Licensing 서버에 연결할 때만 사용됩니다. 다른 ASA SSL 클라이언트 모드 연결은 현재 구성 또는 참조 ID의 사용을 지원하지 않습니다.
- ASA에서는 RFC 6125에 설명된 식별자를 일치시키기 위해 모든 규칙을 구현합니다. 이때 인터랙티브 클라이언트에 대해 고정된 인증서와 대체는 제외합니다.
- 인증서를 고정하는 기능은 구현되지 않습니다. 따라서 `No Match Found, Pinned Certificate` 메시지가 발생하지 않습니다. 또한 구현이 인터랙티브 클라이언트가 아니기 때문에 일치하는 항목을 찾을 수 없는 경우 사용자에게 인증서를 고정할 수 있는 기회가 제공되지 않습니다.

프로시저

단계 **1** ASA를 ca-reference-identity 모드에 배치하려면 전역 구성 모드에서 **[no] crypto ca reference-identity** 명령을 입력합니다.

[no] crypto ca reference-identity *reference-identity-name*

이 *reference-identity-name*을 사용하는 참조 ID를 찾을 수 없는 경우, 새 참조 ID가 생성됩니다. 명령의 **no** 형식이 아직 사용 중인 참조 ID에 대해 발행된 경우, 경고가 표시되고 참조 ID는 삭제되지 않습니다.

단계 **2** ca-reference-identity 모드에 있을 때 참조 ID를 입력합니다. 모든 유형의 여러 참조 ID를 참조 ID에 추가할 수 있습니다.

- **[no] cn-id** 값
- **[no] dns-id** 값
- **[no] srv-id** 값
- **[no] uri-id** 값

참조 ID를 제거하려면 이 명령의 no 형식을 사용합니다.

예

Syslog 서버에 대한 RFC 6125 서버 인증서 검증을 위해 참조 ID를 구성합니다.

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

다음에 수행할 작업

Syslog 및 Smart Call Home 서버 연결을 구성할 때 참조 ID를 사용합니다.

수동으로 인증서 취득

수동으로 인증서를 취득하려면 다음 단계를 수행합니다.

시작하기 전에

신뢰 지점이 나타내는 CA로부터 base64 인코딩 CA 인증서를 이미 취득한 상태임을 전제로 합니다.

프로시저

단계 **1** 구성된 신뢰 지점에 대한 CA 인증서를 가져옵니다.

crypto ca authenticate 신뢰 지점

예제**:**

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
```

```
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

신뢰 지점에서 인증서의 수동 취득을 요구할지는 신뢰 지점 구성 시 **enrollment terminal** 명령을 사용하여 결정합니다.

단계 **2** ASA를 신뢰 지점에 등록합니다.

crypto ca enroll 신뢰 지점

예제**:**

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n
```

이 명령은 데이터 서명을 위해 그리고 구성한 키 유형에 따라 데이터 암호화를 위해 인증서를 생성합니다. 서명과 암호화에 각기 다른 RSA 키를 사용할 경우 **crypto ca enroll** 명령을 사용하면 각 키에 하나씩, 2개의 인증서 요청이 표시됩니다. 범용 RSA 키를 서명과 암호화 모두에 사용할 경우 **crypto ca enroll** 명령은 하나의 인증서 요청을 표시합니다.

등록을 완료하려면 해당 신뢰 지점이 나타내는 CA로부터 **crypto ca enroll** 명령에 의해 생성된 모든 인증서 요청을 위한 인증서를 취득합니다. 인증서는 base64 형식이어야 합니다.

단계 **3** 신뢰 지점을 CMP에 대해 구성한 경우, 요청(cr)을 서명할 인증서를 포함하는 신뢰 지점의 이름 또는 공유 비밀 값(ir) 중 하나가 지정될 수 있지만 둘 다 지정되지는 않습니다. CA가 ASA와 교환한 메시지의 무결성 및 신뢰성을 확인하는 데 사용하는 OOB(Out of Band) 값을 제공하거나 이전에 발행되어 CMP 등록 요청을 서명하는 데 사용된 디바이스 인증서로 신뢰 지점의 이름을 제공합니다. 공유 비밀 또는 서명 인증서 키워드는 신뢰 지점 등록 프로토콜이 CMP로 설정된 경우에만 사용할 수 있습니다.

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

단계 **4** 등록 요청을 구축하기 전에 새 키 쌍을 생성해야 하는지 여부를 결정합니다.

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

단계 **5** 사용자가 CA에서 수신한 각 인증서를 가져오고 base-64 형식의 터미널에 인증서를 붙여넣어야 합니다.

crypto ca import 신뢰 지점 **certificate**

예제**:**

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

단계 **6** ASA에 대해 발급된 인증서 세부 사항 및 신뢰 지점을 위한 CA 인증서를 표시하여 등록 프로세스가 성공했음을 확인합니다.

show crypto ca server certificate

예제**:**

```
ciscoasa(config)# show crypto ca server certificate Main
```

단계 **7** 실행 중인 구성을 저장합니다.

write memory

예제**:**

```
ciscoasa(config)# write memory
```

단계 **8** 수동 등록을 위해 구성하는 각 신뢰 지점에 대해 이 단계를 반복합니다.

SCEP로 인증서 자동 취득

이 섹션에서는 SCEP를 사용하여 인증서를 자동으로 취득하는 방법을 설명합니다.

시작하기 전에

신뢰 지점이 나타내는 CA로부터 base64 인코딩 CA 인증서를 이미 취득한 상태임을 전제로 합니다.

프로시저

단계 **1** 구성된 신뢰 지점에 대한 CA 인증서를 취득합니다.

crypto ca authenticate 신뢰 지점

예제:

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

신뢰 지점을 구성할 때 **enrollment url** 명령을 사용하여 SCEP를 통해 자동으로 인증서를 취득해야 하는지를 결정합니다.

단계 **2** ASA를 신뢰 지점에 등록합니다. 이 명령은 데이터 서명을 위해 그리고 구성한 키 유형에 따라 데이터 암호화를 위해 인증서를 검색합니다. 이 명령을 입력하기 전에 CA 관리자에게 문의합니다. CA에서 인증서를 부여하기 전에 CA 관리자가 수동으로 등록 요청을 인증해야 하는 경우도 있습니다.

crypto ca enroll 신뢰 지점

예제:

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

ASA에서는 인증서 요청을 보내고 1분(기본값) 이내에 CA로부터 인증서를 받지 못할 경우 인증서 요청을 재전송합니다. ASA에서는 인증서를 수신할 때까지 계속 1분마다 인증서 요청을 보냅니다.

신뢰 지점에 대해 구성된 FQDN(Fully Qualified Domain Name)이 ASA의 FQDN과 같지 않을 경우(대소문자 구분) 경고가 나타납니다. 이 문제를 해결하려면 등록 프로세스를 종료하고 필요한 수정을 한 다음 **crypto ca enroll** 명령을 재입력합니다.

참고 ASA 재부팅이 **crypto ca enroll** 명령을 실행한 후에 그러나 아직 인증서를 받지 못한 시점에 이루어질 경우, **crypto ca enroll** 명령을 재입력하고 CA 관리자에게 알립니다.

단계 **3** ASA에 대해 발급된 인증서 세부사항 및 신뢰 지점을 위한 CA 인증서를 표시하여 등록 프로세스가 성공했음을 확인합니다.

show crypto ca server certificate

예제:

```
ciscoasa/contexta(config)# show crypto ca server certificate Main
```

단계 **4** 실행 중인 구성을 저장합니다.

write memory

예제:

```
ciscoasa/contexta(config)# write memory
```

SCEP 요청을 위한 프록시 지원 구성

ASA에서 서드파티 CA를 사용하여 원격 액세스 엔드포인트를 인증하도록 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** tunnel-group ipsec-attributes 구성 모드를 시작합니다.

tunnel-group *name* **ipsec-attributes**

예제:

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

단계 **2** 클라이언트 서비스를 활성화합니다.

crypto ikev2 enable outside client-services port *portnumber*

예제:

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

기본 포트 번호는 443입니다.

참고 이 명령은 IKEv2를 지원하는 경우에만 필요합니다.

단계 **3** tunnel-group general-attributes 구성 모드를 시작합니다.

tunnel-group *name* **general-attributes**

예제:

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

단계 **4** 터널 그룹에 대해 SCEP 등록을 활성화합니다.

scep-enrollment enable

예제:

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.
```

단계 **5** 그룹 정책 특성 구성 모드를 시작합니다.

group-policy *name* **attributes**

예제:

```
ciscoasa(config)# group-policy FirstGroup attributes
```

단계 **6** 그룹 정책에 대해 SCEP CA를 등록합니다. 서드파티 디지털 인증서를 지원하려면 그룹 정책마다 한 번씩 이 명령을 입력합니다.

scep-forwarding-url value *URL*

예제:

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

*URL*은 CA의 SCEP URL입니다.

단계 **7** SCEP 프록시의 WebLaunch 지원을 위해 인증서를 사용할 수 없는 경우 일반적인 보조 비밀번호를 제공합니다.

secondary-pre-fill-username clientless hide use-common-password *password*

예제:

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

SCEP 프록시를 지원하려면 **hide** 키워드를 사용해야 합니다.

이를테면 어떤 엔드포인트에서 인증서가 없어 하나를 요청합니다. 이 엔드포인트가 인증서를 취득하면 AnyConnect는 연결을 끊었다가 다시 ASA에 연결하여 내부 네트워크 리소스에 대한 액세스를 제공하는 DAP 정책에 부합하는지 확인합니다.

단계 **8** AnyConnect VPN 세션에서 미리 채워진 보조 사용자 이름을 숨깁니다.

secondary-pre-fill-username ssl-client hide use-common-password *password*

예제:

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password secret
```

이전 릴리스의 **ssl-client** 키워드도 계속 사용 가능하지만, IKEv2 또는 SSL을 사용하는 AnyConnect 세션을 지원하려면 이 명령을 사용합니다.

SCEP 프록시를 지원하려면 **hide** 키워드를 사용해야 합니다.

단계 **9** 인증서를 사용할 수 없는 경우 사용자 이름을 제공합니다.

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

예제:

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback
 cisco-secure-desktop machine-unique-id
```

CA 인증서 수명 구성

로컬 CA 서버 인증서의 수명을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 인증서에 포함할 만료 날짜를 결정합니다. 로컬 CA 인증서의 기본 수명은 3년입니다.

lifetime ca-certificate 시간

예제**:**

```
ciscoasa(config-ca-server)# lifetime ca-certificate 365
```

인증서의 유효 기한이 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빨라야 합니다.

단계 **3** (선택 사항) 로컬 CA 인증서 수명을 기본값인 3년으로 재설정합니다.

no lifetime ca-certificate

예제**:**

```
ciscoasa(config-ca-server)# no lifetime ca-certificate
```

로컬 CA 서버는 만료 30일 전에 대체 CA 인증서를 자동으로 생성합니다. 이 대체 인증서를 다른 디바이스에 내보내고 가져오는 방법으로 기존 로컬 CA 인증서 만료 시 로컬 CA 인증서에서 발급한 사용자 인증서의 유효성 검사를 수행할 수 있습니다. 다음과 같은 만료 전 syslog 메시지가 생성됩니다.

```
%ASA-1-717049: Local CA Server certificate is due to expire in days and a replacement
 certificate is available for export.
```

참고 관리자는 이 자동 롤오버에 대한 알림을 받으면 기존 인증서가 만료되기 전에 필요한 모든 디바이스에서 새 로컬 CA 인증서의 가져오기가 이루어졌는지 확인해야 합니다.

사용자 인증서 수명 구성

사용자 인증서 수명을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제:

```
ciscoasa(config)# crypto ca server
```

단계 **2** 원하는 사용자 인증서 유효 기간을 설정합니다.

lifetime certificate 시간

예제:

```
ciscoasa(config-ca-server)# lifetime certificate 60
```

참고 사용자 인증서가 만료되기 전에 로컬 CA 서버는 인증서 갱신 처리를 자동으로 시작합니다. 즉 인증서가 만료되기 며칠 전에 사용자에게 등록 권한을 부여하고, 갱신 알림을 설정하고, 인증서 갱신을 위한 등록 사용자 이름과 OTP를 포함한 이메일 메시지를 전달합니다. 인증서의 유효 기한이 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빨라야 합니다.

CRL 수명 구성

CRL 수명을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제:

```
ciscoasa(config)# crypto ca server
```

단계 **2** 원하는 CRL 유효 기간을 설정합니다.

lifetime crl 시간

예제:

```
ciscoasa(config-ca-server)# lifetime crl 10
```

사용자 인증서가 폐기되거나 폐기 해제될 때마다 로컬 CA가 CRL을 업데이트하고 재배포하지만, 폐기 변경이 없을 경우에는 각 CRL 수명 기간에 한 번씩 자동으로 CRL이 재배포됩니다. CRL 수명을 지정하지 않을 경우 기본 기간은 6시간입니다.

단계 **3** 언제라도 강제적으로 CRL을 배포합니다. 그러면 즉시 업데이트하여 최신 CRL을 재생성하여 기존 CRL을 덮어씁니다.

crypto ca server crl issue

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server crl issue

A new CRL has been issued.
```

참고 CRL 파일이 실수로 제거되었거나 손상되어 재생성해야 하는 경우에만 이 명령을 사용합니다.

서버 키 크기 구성

서버 키 크기를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 사용자 인증서 등록 시 생성되는 공개 및 개인 키의 크기를 지정합니다.

keysize server

예제**:**

```
ciscoasa(config-ca-server)# keysize server 2048
```

키 쌍 크기 옵션은 512비트, 768비트, 1024비트, 2048비트, 4096비트이며 기본값은 1024비트입니다.

참고 로컬 CA를 활성화한 다음에는 로컬 CA 키 크기를 변경할 수 없습니다. 발급된 모든 인증서가 무효화되기 때문입니다. 로컬 CA 키 크기를 변경하려면 현재 로컬 CA를 삭제하고 새로 재구성해야 합니다.

예

다음은데이터베이스의 사용자 인증서 2개를 표시하는 샘플 출력 입니다.

```
Username: user1
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:45:52 UTC Fri Jan 4 2017
Certificates Issued:
serial:   0x71
issued:   12:45:52 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
Username: user2
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:27:59 UTC Fri Jan 4 2008
Certificates Issued:
serial:   0x2
issued:   12:27:59 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
<--- More --->
```

특정 인증서 유형을 설정하는 방법

신뢰할 수 있는 인증서를 설정한 후에 ID 인증서 설정과 같은 다른 기본적인 작업 또는 로컬 CA나 코드 서명 인증서 설정과 같은 고급 구성을 시작할 수 있습니다.

시작하기 전에

디지털 인증서 정보를 읽고 신뢰할 수 있는 인증서를 설정합니다. 개인 키가 없는 CA 인증서는 모든 VPN 프로토콜 및 webvpn에서 사용되며 수신 클라이언트 인증서를 검증하기 위해 신뢰 지점에서 구성됩니다. 마찬가지로, 신뢰 풀은 https 서버에 대한 프록시 연결을 검증하고 스마트 콜 홈 인증서를 검증하기 위해 webvpn 기능에서 사용되는 신뢰할 수 있는 인증서의 목록입니다.

프로시저

로컬 CA를 통해 VPN 클라이언트가 ASA에서 직접 인증서를 등록할 수 있습니다. 이 고급 구성은 ASA를 CA로 변환합니다. CA를 구성하려면 CA 인증서, 765 페이지의 내용을 참조하십시오.

다음에 수행할 작업

인증서 만료 경고를 설정하거나 디지털 인증서 및 인증서 관리 기록을 모니터링합니다.

CA 인증서

이 페이지에서 CA 인증서를 관리합니다. 다음 주제에서는 수행할 수 있는 작업을 설명합니다.

로컬 CA 서버 구성

로컬 CA 서버를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 1 local ca server 구성 모드를 시작합니다.

crypto ca server

예제:

```
ciscoasa(config)# crypto ca server
```

단계 2 SMTP from-address를 지정합니다. 이는 로컬 CA에서 사용자에게 등록 초대를 위한 OTP(일회용 비밀번호)를 전달하는 이메일 메시지를 보낼 때 발신 주소로 사용하는 유효한 이메일 주소입니다.

smtp from-address *e-mail_address*

예제:

```
ciscoasa(config-ca-server) # smtp from-address SecurityAdmin@example.com
```

단계 3 (선택사항) 발급된 인증서에서 각 사용자 이름에 추가되는 주체-이름 DN을 지정합니다.

subject-name-default *dn*

예제:

```
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc systems, c="US"
```

로컬 CA 서버에서 발급하는 모든 사용자 인증서에서 주체-이름 DN과 사용자 이름의 조합으로 DN을 구성합니다. 주체-이름 DN을 지정하지 않을 경우, 사용자 데이터베이스에 사용자를 추가할 때마다 사용자 인증서에 포함할 주체 이름 DN을 정확하게 지정해야 합니다.

참고 구성된 로컬 CA를 활성화하기 전에 모든 선택적 매개변수를 면밀하게 검토해야 합니다. 처음으로 로컬 CA를 활성화한 다음에는 발급자-이름 및 키 크기 서버 값을 변경할 수 없기 때문입니다.

단계 4 자체 서명 인증서를 생성하고 이를 ASA의 로컬 CA와 연결합니다.

no shutdown

예제:

```
ciscoasa(config-ca-server)# no shutdown
```

자체 서명 인증서 키 사용 확장에는 키 암호화, 키 서명, CRL 서명, 인증서 서명 기능이 있습니다.

참고 자체 서명 로컬 CA 인증서가 생성된 후에는 어떤 특성이든 변경하기 위해서는 기존 로컬 CA 서버를 삭제하고 완전히 다시 생성해야 합니다.

로컬 CA 서버가 지속적으로 사용자 인증서를 추적하므로, 관리자가 필요에 따라 권한을 취소하거나 복원할 수 있습니다.

예

다음 예는 모든 필수 파라미터에 사전 정의된 기본값을 사용하면서 로컬 CA 서버를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
ciscoasa(config-ca-server)# no shutdown
```

CA 서버 관리

로컬 CA 서버 삭제

(활성화되었거나 비활성화된) 기존 로컬 CA 서버를 삭제하려면 다음 단계를 수행합니다.

프로시저

(활성화되었거나 비활성화된) 기존 로컬 CA 서버를 제거하려면 다음 명령 중 하나를 입력합니다.

- **no crypto ca server**

  예

  ```
  ciscoasa(config)# no crypto ca server
  ```

- **clear configure crypto ca server**

  예

  ```
  ciscoasa(config)# clear config crypto ca server
  ```

참고 로컬 CA 서버를 삭제하면 ASA에서 구성이 제거됩니다. 삭제된 컨피그레이션은 복구 불가합니다.

해당 로컬 CA 서버 데이터베이스와 컨피그레이션 파일(즉 와일드카드 이름 LOCAL-CA-SERVER.*을 가진 모든 파일)도 삭제해야 합니다.

사용자 인증서 관리

인증서 상태를 변경하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Manage User Certificates(**사용자 인증서 관리**)** 창에서 사용자 이름 또는 인증서 일련 번호에 따라 특정한 인증서를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 사용자 인증서 수명 기간이 초과된 경우 **Revoke(**폐기**)**를 클릭하여 사용자 액세스를 제거합니다. 또한 로컬 CA가 인증서 데이터베이스에서 해당 인증서를 폐기됨으로 표시하고 자동으로 정보를 업데이트하며 CRL을 재배포합니다.
- 액세스를 복원하려면 해지된 인증서를 선택하고 **Unrevoke(**해지 취소**)**를 클릭합니다. 또한 로컬 CA가 인증서 데이터베이스에서 해당 인증서를 폐기 해제됨으로 표시하고 자동으로 정보를 업데이트하며 업데이트된 CRL을 재발급합니다.

단계 **3** 완료했으면 **Apply(**적용**)**를 클릭하여 변경 사항을 저장합니다.

로컬 **CA** 서버 활성화

로컬 CA 서버를 활성화하려면 다음 단계를 수행합니다.

시작하기 전에

로컬 CA 서버를 활성화하기 전에 먼저 7자 이상의 패스프레이즈를 생성해야 합니다. 이는 생성할 로컬 CA 인증서 및 키 쌍이 포함된 PKCS12 파일을 인코딩하고 보관하는 데 필요합니다. CA 인증서 또는 키 쌍을 분실할 경우 이 패스프레이즈로 PKCS12 아카이브의 잠금을 해제합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 로컬 CA 서버를 활성화합니다.

no shutdown

예제**:**

```
ciscoasa(config-ca-server)# no shutdown
```

이 명령은 로컬 CA 서버 인증서, 키 쌍 및 필요한 데이터베이스 파일을 생성하고 로컬 CA 서버 인증서 및 키 쌍을 PKCS12 파일 형식으로 보관합니다. 8~65자의 영숫자 비밀번호를 입력하십시오. 최초 시작 후 비밀번호 입력 화면 없이 로컬 CA를 비활성화할 수 있습니다.

단계 **3** 구성을 저장하여 재부팅하더라도 로컬 CA 인증서와 키 쌍이 손실되지 않게 합니다.

write memory

예제**:**

```
ciscoasa(config)# write memory
```

예

다음 예에서는 로컬 CA 서버를 휠성화합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...
```

다음은 로컬 CA 서버 컨피그레이션과 상태를 보여주는 샘플 출력입니다.

```
Certificate Server LOCAL-CA-SERVER:
    Status: enabled
    State: enabled
    Server's configuration is locked (enter “shutdown” to unlock it)
    Issuer name: CN=wz5520-1-16
    CA certificate fingerprint/thumbprint: (MD5)
        76dd1439 ac94fdbc 74a0a89f cb815acc
    CA certificate fingerprint/thumbprint: (SHA1)
        58754ffd 9f19f9fd b13b4b02 15b3e4be b70b5a83
    Last certificate issued serial number: 0x6
    CA certificate expiration timer: 14:25:11 UTC Jan 16 2008
    CRL NextUpdate timer: 16:09:55 UTC Jan 24 2007
    Current primary storage dir: flash:
```

신뢰 풀 인증서의 자동 가져오기 구성

스마트 라이선싱은 Smart Call Home 인프라를 사용합니다. ASA가 Smart Call Home 백그라운드에서 익명 보고를 구성하면 ASA에서 자동으로 Call Home 서버 인증서를 발급한 CA 인증서를 포함하는 트러스트 포인트를 생성합니다. ASA는 이제 인증서 계층 구조 변경 사항을 조정하기 위해 고객이 참여할 필요 없이 서버 인증서 변경 사항의 계층 구조를 발급하는 경우, 인증서 유효성 검사를 지원합

니다. CA 서버의 자체 서명된 인증서가 변경되는 경우 해당 Smart Call Home이 활성 상태로 남아 있을 수 있도록 신뢰 풀 번들의 업데이트를 주기적으로 자동화할 수 있습니다. 다중 상황 구축에서는 이 기능이 지원되지 않습니다.

신뢰 풀 인증서 번들의 자동 가져오기를 수행하려면 ASA에서 번들을 다운로드하고 가져오기 위해 사용하는 URL을 지정해야 합니다. 기본 Cisco URL을 사용하며 기본 시간이 22시간인 기본 간격으로 매일 가져오기를 수행하려면 다음 명령을 사용하십시오.

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

다음 명령을 사용하여 맞춤형 URL로 자동 가져오기를 활성화할 수도 있습니다.

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

피크 시간 또는 다른 편리한 시간 동안 다운로드하도록 설정하는 유연한 기능을 활용하려면 맞춤형 시간에 가져오기를 활성화하는 다음 명령을 입력하십시오.

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

맞춤형 URL 및 맞춤형 시간에 자동 가져오기를 설정하려면 다음 명령이 필요합니다.

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

신뢰 풀 정책의 상태 표시

신뢰 풀 정책의 현재 상태를 확인하려면 다음 명령을 사용하십시오.

```
show crypto ca trustpool policy
```

이 명령은 다음과 같은 정보를 반환합니다.

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

CA 신뢰 풀 지우기

신뢰 풀 정책을 기본 상태로 재설정하려면 다음 명령을 사용하십시오.

```
clear configure crypto ca trustpool
```

트러스트 포인트 인증서 자동 가져오기가 기본적으로 해제되어 있으므로 이 명령을 사용하면 이 기능이 비활성화됩니다.

로컬 **CA** 서버 사용자 지정

사용자 지정 로컬 CA 서버를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 기본값이 없는 파라미터를 지정합니다.

issuer-name *DN-string*

예제**:**

```
ciscoasa(config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC
Systems
```

단계 **3** 로컬 CA 서버에서 생성하는 모든 이메일 메시지의 From: 필드에 사용할 이메일 주소를 지정합니다.

smtp from-address *e-mail_address*

예제**:**

```
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
```

단계 **4** 로컬 CA 서버에서 보내는 모든 이메일 메시지의 주체 필드에 나타나는 텍스트를 사용자 지정합니다.

smtp subject *subject-line*

예제**:**

```
ciscoasa(config-ca-server)# smtp subject Priority E-Mail: Enclosed Confidential Information
 is Required for Enrollment
```

단계 **5** 발급된 인증서의 사용자 이름에 추가될 선택적 주체-이름 DN을 지정합니다.

subject-name-default *dn*

예제**:**

```
ciscoasa(config-ca-server)# subject-name default cn=engineer, o=ASC Systems, c=US
```

로컬 CA 서버에서 발급하는 모든 사용자 인증서에서 기본 주체-이름 DN이 사용자 이름의 일부가 됩니다.

허용된 DN 특성 키워드는 다음과 같습니다.

- C = 국가
- CN = 공용 이름(Common Name)
- EA = 이메일 주소(E-mail Address)
- L = 소재지(Locality)
- O = 조직 이름(Organization Name)
- OU = 조직 단위(Organization Unit)
- ST = 시/도(State/Province)
- SN = 성
- ST = 주/도(State/Province)

참고 표준 주체-이름 기본값으로 사용할 subject-name-default를 지정하지 않을 경우, 사용자를 추가할 때마다 DN을 지정해야 합니다.

로컬 **CA** 서버 비활성화

로컬 CA 서버를 비활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 로컬 CA 서버를 비활성화합니다.

shutdown

예제**:**

```
ciscoasa(config-ca-server)# shutdown
INFO: Local CA Server has been shutdown.
```

이 명령은 웹 사이트 등록을 비활성화하고 로컬 CA 서버 구성을 수정할 수 있게 해 주며 현재 구성 및 연관된 파일을 저장합니다. 최초 시작 후 비밀번호 입력 화면 없이 로컬 CA를 다시 활성화할 수 있습니다.

외부 로컬 **CA** 파일 저장소 설정

외부 로컬 CA 파일 저장소를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 특정 파일 시스템 유형의 구성 모드에 액세스합니다.

mount *name* **type**

예제**:**

```
ciscoasa(config)# mount mydata type cifs
```

단계 **2** CIFS 파일 시스템을 마운트합니다.

mount *name* **type cifs**

예제**:**

```
ciscoasa(config-mount-cifs)# mount mydata type cifs
server 10.1.1.10 share myshare
domain example.com
username user6
password ********
status enable
```

참고 파일 시스템을 마운트한 사용자만 **no mount** 명령을 사용하여 마운트 해제할 수 있습니다.

단계 **3** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **4** *mydata*, 즉 로컬 CA 서버 데이터베이스에 사용할 미리 마운트된 CIFS 파일 시스템의 위치를 지정합니다.

database path *mount-name directory-path*

예제**:**

```
ciscoasa(config-ca-server)# database path mydata:newuser
```

이 명령은 서버에 대한 경로를 설정한 다음 저장 및 검색에 사용할 로컬 CA 파일 또는 폴더 이름을 지정합니다. 로컬 CA 파일 저장소를 ASA 플래시 메모리에 반환하려면 **no database path** 명령을 사용합니다.

참고 외부 서버에 저장된 로컬 CA 파일을 보호하려면 미리 마운트된 파일 시스템이 필요합니다. 이는 CIFS 또는 FTP 파일 유형이고 사용자 이름으로 보호되고 비밀번호로 보호되어야 합니다.

단계 **5** 실행 중인 구성을 저장합니다.

write memory

예제**:**

```
ciscoasa(config)# write memory
```

외부 로컬 CA 파일 저장소의 경우, ASA 구성을 저장할 때마다 ASA의 사용자 정보가 미리 마운트된 파일 시스템 및 파일 위치, *mydata:newuser*에 저장됩니다.

플래시 메모리 저장소에서는 시작(start-up) 컨피그레이션의 기본 위치에 자동으로 사용자 정보가 저장됩니다.

예

다음 예는 플래시 메모리 또는 외부 저장소에 나타나는 로컬 CA 파일의 목록을 보여줍니다.

```
ciscoasa(config-ca-server)# dir LOCAL* //
Directory of disk0:/LOCAL*

75     -rwx  32          13:07:49 Jan 20 2007  LOCAL-CA-SERVER.ser
77     -rwx  229         13:07:49 Jan 20 2007  LOCAL-CA-SERVER.cdb
69     -rwx  0           01:09:28 Jan 20 2007  LOCAL-CA-SERVER.udb
81     -rwx  232         19:09:10 Jan 20 2007  LOCAL-CA-SERVER.crl
72     -rwx  1603        01:09:28 Jan 20 2007  LOCAL-CA-SERVER.p12

127119360 bytes total (79693824 bytes free)
```

CRL 다운로드 및 저장

CRL을 다운로드하고 저장하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 인터페이스에서 CRL에 액세스할 수 있도록 설정하려면 이 인터페이스에서 포트를 엽니다. 지정된 인터페이스 및 포트는 CRL에 대한 수신 요청을 대기하는 데 사용됩니다.

publish-crl interface *interface* **port** *portnumber*

예제:

```
ciscoasa(config-ca-server)# publish-crl outside 70
```

인터페이스와 선택 사항인 포트 옵션은 다음과 같습니다.

- 내부—인터페이스 이름/GigabitEthernet0/1
- 관리—인터페이스 이름/ Management0/0
- 외부—인터페이스 이름/GigabitEthernet0/0
- 가능한 포트 번호의 범위는 1 ~ 65535입니다. TCP 포트 80은 HTTP 기본 포트 번호입니다.

참고 이 명령을 지정하지 않을 경우 CDP 위치에서 CRL에 액세스할 수 없습니다. CRL 파일을 다운로드하기 위해 인터페이스를 여는 데 이 명령이 필요하기 때문입니다.

CDP URL은 인터페이스의 IP 주소와 CDP URL의 경로를 사용하도록 구성할 수 있습니다. 그리고 파일 이름도 구성 가능합니다(예: http://10.10.10.100/user8/my_crl_file).

이러한 경우 IP 주소가 구성된 인터페이스만 CRL 요청을 수신합니다. 그리고 요청이 수신되면 ASA에서는 해당 경로, /user8/my_crl_file이 구성된 CDP URL과 일치하는지 확인합니다. 경로가 일치하면 ASA에서는 저장된 CRL 파일을 반환합니다.

참고 프로토콜은 HTTP여야 합니다. 즉 표시되는 접두사는 http://입니다.

단계 **3** 모든 발급된 인증서에 포함할 CDP를 지정합니다. CDP에 대해 구체적인 위치를 구성하지 않을 경우 기본 URL 위치는 http://*hostname.domain*/+CSCOCA+/asa_ca.crl입니다.

cdp-url *url*

예제:

```
ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl
```

사용자 인증서가 폐기되거나 폐기 해제될 때마다 로컬 CA가 CRL을 업데이트하고 재배포합니다. 어떤 폐기 변경도 없을 경우, 각 CRL 수명 기간에 한 번씩 CRL이 재배포됩니다.

이 명령이 로컬 CA ASA에서 곧바로 CRL을 서비스하도록 설정된 경우, 해당 인터페이스에서 CRL에 액세스할 수 있도록 인터페이스의 포트를 여는 방법에 대한 지침은 CRL 다운로드 및 저장페이지를 참조하십시오.

다른 디바이스에서 로컬 CA에 의해 발급된 인증서의 폐기를 검증할 수 있도록 CRL이 제공됩니다. 또한 로컬 CA는 자신의 인증서 데이터베이스에 있는 발급된 모든 인증서와 상태를 추적합니다. 폐기

검사는 유효성 검사 당사자가 외부 서버(인증서를 발급한 CA 또는 CA에서 지정한 서버일 수 있음)로부터 폐기 상태를 검색하여 사용자 인증서의 유효성을 검사해야 하는 경우에 수행됩니다.

등록 및 사용자 관리

등록 파라미터 설정

등록 파라미터를 설정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 로컬 CA 등록 페이지를 위해 발급된 OTP의 유효 기간(시간)을 지정합니다. 기본 유효 기간은 72시간입니다.

otp expiration *timeout*

예제**:**

```
ciscoasa(config-ca-server)# otp expiration 24
```

참고 등록 웹 사이트에서 인증서를 등록하는 데 필요한 사용자 OTP는 해당 사용자에 대해 발급된 인증서와 키 쌍이 포함된 PKCS12 파일을 잠금 해제할 때 비밀번호로도 사용됩니다.

단계 **3** 등록된 사용자가 PKCS12 등록 파일을 검색할 수 있는 시간을 지정합니다.

enrollment-retrieval *timeout*

예제**:**

```
ciscoasa(config-ca-server)# enrollment-retrieval 120
```

이 기간은 사용자가 성공적으로 등록할 때 시작됩니다. 기본 검색 기간은 24시간입니다. 검색 기간에 유효한 값의 범위는 1시간 ~ 720시간입니다. 등록 검색 기간은 OTP 만료 기간과 상관없습니다.

등록 검색 기간이 끝나면 사용자 인증서와 키 쌍은 더 이상 사용할 수 없습니다. 사용자가 인증서를 수신할 수 있는 유일한 방법은 관리자가 인증서 등록을 다시 초기화하고 사용자가 다시 로그인할 수 있게 하는 것입니다.

사용자 추가 및 등록

로컬 CA 데이터베이스에 등록 가능한 사용자를 추가하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 로컬 CA 데이터베이스에 새 사용자를 추가합니다.

crypto ca server user-db add *username* [**dn** *dn*] [**email** *emailaddress*]

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server user-db add user1 dn user1@example.com, Engineer,
 Example Company, US, email user1@example.com
```

username 인수는 4자~64자의 문자열이며, 추가되는 사용자의 간단한 사용자 이름입니다. 사용자 이름으로 이메일 주소도 가능합니다. 그러면 등록 초대를 위해 필요할 때 사용자에게 연락하는 데 사용됩니다.

dn 인수는 고유 이름, 즉 OSI Directory(X.500) 항목의 전역 정식 이름입니다(예: cn=user1@example.com, cn=Engineer, o=Example Company, c=US).

e-mail-address 인수는 OTP 및 알림이 전송될 새 사용자의 이메일 주소입니다.

단계 **2** 새로 추가된 사용자에게 사용자 권한을 부여합니다.

crypto ca server user-db allow *user*

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user
```

단계 **3** 로컬 CA 데이터베이스의 사용자에게 사용자 인증서를 등록하고 다운로드하도록 알립니다. 자동으로 사용자에게 이메일을 통해 OTP를 보냅니다.

crypto ca server user-db email-otp *username(사용자 이름)*

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp exampleuser1
```

참고 관리자가 사용자에게 이메일을 통해 알림을 보내기 위해서는 그 사용자를 추가할 때 사용자 이름 필드 또는 이메일 필드에 이메일 주소를 지정해야 합니다.

단계 **4** 발급된 OTP를 표시합니다.

crypto ca server user-db show-otp

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp
```

단계 **5** 등록 기한(시간)을 설정합니다. 기본 유효 기간은 72시간입니다.

otp expiration *timeout*

예제**:**

```
ciscoasa(config-ca-server)# otp expiration 24
```

이 명령은 사용자 등록 시 OTP의 유효 기간을 정의합니다. 이 기간은 사용자가 등록 가능해질 때 시작합니다.

사용자가 기한 내에 올바른 OTP를 사용하여 성공적으로 등록되면, 로컬 CA 서버는 PKCS12 파일을 생성합니다. 여기에는 해당 사용자의 키 쌍과 사용자 인증서가 들어 있습니다. 이 사용자 인증서는 키 쌍의 공개 키와 사용자 추가 시 지정된 주체-이름 DN을 기반으로 합니다. PKCS12 파일의 내용은 패스프레이즈, 즉 OTP에 의해 보호됩니다. OTP는 수동으로 처리하거나, 로컬 CA에서 사용자에게 이메일로 이 파일을 보내 관리자가 등록을 허용하면 다운로드하게 할 수 있습니다.

PKCS12 파일은 *username.p12*라는 이름과 함께 임시 저장소에 저장됩니다. PKCS12 파일이 저장소에 있는 상태에서 사용자는 등록 검색 기간 내에 돌아와 PKCS12 파일을 필요한 만큼 자주 다운로드할 수 있습니다. 기간이 만료되면 PKCS12 파일이 자동으로 저장소에서 삭제되며 더 이상 다운로드할 수 없게 됩니다.

참고 사용자가 사용자 인증서가 포함된 PKCS12 파일을 검색하기 전에 등록 기간이 끝날 경우, 등록 불가합니다.

사용자 갱신

갱신 알림 시간을 지정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 로컬 CA 인증서가 만료되기 며칠(1~90) 전에 최초의 재등록 알림을 인증서 소유자에게 보낼 것인지 지정합니다.

renewal-reminder 시간

예제**:**

```
ciscoasa(config-ca-server)# renewal-reminder 7
```

인증서가 만료되면 무효화됩니다. 갱신 알림 및 사용자에게 이메일로 발송되는 횟수는 가변적입니다. 그리고 관리자가 로컬 CA 서버 컨피그레이션 과정에서 이를 구성할 수 있습니다.

알림이 3번 발송됩니다. 3번의 알림 각각 인증서 소유자에게 이메일로 자동 발송됩니다. 단, 이메일 주소가 사용자 데이터베이스에 지정되어야 합니다. 해당 사용자의 이메일 주소가 없을 경우 syslog 메시지를 통해 갱신 요구 사항을 알립니다.

ASA에서는 곧 만료되는 유효한 인증서를 보유한 모든 사용자에게 인증서 갱신 권한을 자동으로 부여합니다. 단, 사용자가 사용자 데이터베이스에 있어야 합니다. 따라서 관리자가 특정 사용자의 자동 갱신을 원치 않을 경우 갱신 기한 전에 데이터베이스에서 사용자를 삭제해야 합니다.

사용자 복원

사용자를 복원하고 로컬 CA 서버에서 발급했으나 폐기되었던 인증서를 복원하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 사용자를 복원하고 로컬 CA에서 발급했으나 해지되었던 인증서를 해지 취소합니다.

crypto ca server unrevoke *cert-serial-no*

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
```

로컬 CA는 폐기된 모든 사용자 인증서의 일련 번호를 포함한 최신 CRL을 갖고 있습니다. 이 목록은 외부 디바이스에 제공할 수 있으며, 로컬 CA에서 곧바로 검색할 수도 있습니다. 단, 그러한 작업이 가능하도록 **cdp-url** 명령과 **publish-crl** 명령을 사용하여 구성해야 합니다. 인증서 일련 번호를 사용하여 현재 인증서를 폐기(또는 폐기 해제)하면 CRL은 자동으로 이 변경 사항을 반영합니다.

사용자 제거

사용자 이름을 사용하여 사용자 데이터베이스에서 사용자를 삭제하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 사용자 데이터베이스에서 사용자를 삭제하고, 그 사용자에게 발급되었던 모든 유효한 인증서를 해지할 수 있게 합니다.

crypto ca server user-db remove *username(*사용자 이름*)*

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1
```

인증서 해지

사용자 인증서를 폐기하려면 다음 단계를 수행합니다.

프로시저

단계 **1** local ca server 구성 모드를 시작합니다.

crypto ca server

예제**:**

```
ciscoasa(config)# crypto ca server
```

단계 **2** 인증서 일련 번호를 16진수 형식으로 입력합니다.

crypto ca server revoke *cert-serial-no*

예제**:**

```
ciscoasa(config-ca-server)# crypto ca server revoke 782ea09f
```

이 명령은 로컬 CA 서버의 인증서 데이터베이스 및 CRL에서 해당 인증서를 해지된 것으로 표시합니다. CRL은 자동으로 재배포됩니다.

참고 ASA의 인증서를 폐기해야 하는 경우 비밀번호도 필요합니다. 따라서 비밀번호를 기록하여 안전한 곳에 보관해야 합니다.

인증서 만료 알림 설정(ID 또는 CA 인증서용)

ASA는 24시간에 한 번, 만료에 대해 신뢰 지점에서 모든 CA 및 ID 인증서를 검사합니다. 인증서의 만료일이 가까워지는 경우, syslog가 알림으로 발행됩니다.

CLI는 알림과 반복 간격을 구성하기 위해 제공됩니다. 기본적으로, 알림은 만료 60일 전에 시작되며 7일 마다 반복됩니다. 다음 명령을 사용하여 알림이 전송되는 간격과 첫 번째 알림이 전송된 만료일 이전의 일수를 구성할 수 있습니다.

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

알림 구성에 관계없이, 만료 마지막 주 동안 알림이 매일 전송됩니다. 다음 **show** 및 **clear** 명령도 추가되었습니다.

```
clear conf crypto ca alerts
show run crypto ca alerts
```

갱신 알림 외에도, 이미 만료된 인증서가 구성에 있는 경우, 인증서를 갱신하거나 만료된 인증서를 제거하여 구성을 수정하도록 syslog가 매일 생성됩니다.

예를 들어 만료 알림이 60일에 시작되고 이후에 6일마다 반복되는 것으로 가정해 보겠습니다. ASA가 40일에 재부팅되는 경우 알림이 해당 날짜에 전송되고, 다음 알림은 36번째 날짜에 전송됩니다.

참고 만료 검사는 신뢰 풀 인증서에서 수행되지 않습니다. 로컬 CA 신뢰 지점은 만료 검사에 대한 일반적인 신뢰 지점으로도 처리됩니다.

디지털 인증서 모니터링

디지털 인증서 상태 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show crypto ca server**

  이 명령은 로컬 CA 구성 및 상태를 표시합니다.

- **show crypto ca server cert-db**

  이 명령은 로컬 CA에서 발급한 사용자 인증서를 표시합니다.

- **show crypto ca server certificate**

이 명령은 로컬 CA 인증서를 base64 형식으로 콘솔에 표시하고, 롤오버 인증서가 있으면 이 역시 표시합니다. 여기에는 다른 디바이스로 새 인증서를 가져오는 과정에서 인증서를 확인하기 위한 롤오버 인증서 지문이 포함됩니다.

- **show crypto ca server crl**

  이 명령은 CRL을 표시합니다.

- **show crypto ca server user-db**

  이 명령은 사용자와 사용자의 상태를 표시합니다. 표시되는 레코드 수를 줄이기 위해 다음 한정자를 사용할 수 있습니다.

  - allowed. 현재 등록이 허용된 사용자만 표시합니다.
  - enrolled. 등록되었고 유효한 인증서를 가진 사용자만 표시합니다.
  - expired. 만료된 인증서를 가진 사용자만 표시합니다.
  - on-hold. 인증서가 없고 현재 등록이 허용되지 않은 사용자만 표시합니다.

- **show crypto ca server user-db allowed**

  이 명령은 등록할 자격이 있는 사용자를 표시합니다.

- **show crypto ca server user-db enrolled**

  이 명령은 등록된 사용자를 유효한 인증서와 함께 표시합니다.

- **show crypto ca server user-db expired**

  이 명령은 사용자를 만료된 인증서와 함께 표시합니다.

- **show crypto ca server user-db on-hold**

  이 명령은 인증서가 없고 등록이 허용되지 않은 사용자를 표시합니다.

- **show crypto key** *name of key*

  이 명령은 생성한 키 쌍을 표시합니다.

- **show running-config**

  이 명령은 로컬 CA 인증서 맵 규칙을 표시합니다.

예

다음 예는 RSA 범용 키를 보여줍니다.

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:
```

```
  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

다음 예는 로컬 CA CRL을 보여줍니다.

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

다음 예는 보류 중인 사용자 1명을 보여줍니다.

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

다음 예에는 로컬 CA 인증서 맵 규칙이 나타나 있는 **show running-config** 명령의 출력이 나와 있습니다.

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

인증서 관리 내역

표 ***25:*** 인증서 관리 내역

기능 이름	플랫폼 릴리스	설명
인증서 관리	7.0(1)	디지털 인증서(CA 인증서, ID 인증서, 코드 서명 인증서 포함)가 인증을 위한 디지털 식별을 수행합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 상황에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다.
인증서 관리	7.2(1)	다음 명령을 도입했습니다. **issuer-name** *DN-string*, **revocation-check crl none**, **revocation-check crl**, **revocation-check none** 사용이 중단된 명령: **crl** {**required** | **optional** | **nocheck**}

기능 이름	플랫폼 릴리스	설명
인증서 관리	8.0(2)	다음 명령을 도입했습니다. **cdp-url**, **crypto ca server**, **crypto ca server crl issue**, **crypto ca serverrevoke** *cert-serial-no*, **crypto ca server unrevoke** *cert-serial-no*, **crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*], **crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**], **crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}, **crypto ca server user-db remove** *username*, **crypto ca server user-db show-otp** {*username*| **all-certholders** | **all-unenrolled**}, **crypto ca server user-db write**, [**no**] **database path** *mount-name directory-path*, **debugcrypto ca server** [*level*], **lifetime** {**ca-certificate** | **certificate** | **crl**} *time*, **no shutdown**, **otp expiration** *timeout*, **renewal-reminder** *time*, **show crypto ca server**, **show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial***certificate-serial-number*], **show crypto ca server certificate**, **showcrypto ca server crl**, **show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**], **show crypto key** *nameof key*, **show running-config**, **shutdown**
SCEP 프록시	8.4(1)	서드파티 CA의 디바이스 인증서를 안전하게 배포하는 이 기능을 도입했습니다. 다음 명령을 도입했습니다. **crypto ikev2 enable outside client-services port** *portnumber*, **scep-enrollment enable**, **scep-forwarding-url value** *URL*, **secondary-pre-fill-username clientless hide use-common-password** *password*, **secondary-pre-fill-username ssl-client hide use-common-password** *password*, **secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**].

기능 이름	플랫폼 릴리스	설명
참조 ID	9.6(2)	이제 TLS 클라이언트 처리 시 RFC 6125, 섹션 6에 정의되어 있는 서버 ID를 확인하기 위해 규칙을 지원합니다. ID 확인은 Syslog 서버 및 스마트 라이선싱 서버에 대한 TLS 연결을 대상으로 PKI 검증을 하는 동안에만 수행됩니다. 표시되는 ID가 구성된 참조 ID에 대해 일치될 수 없는 경우 연결이 설정되지 않습니다. 추가 또는 수정된 명령: **crypto ca reference-identity**, **logging host**, **call home profile destination address**

22 장

ARP 검사 및 MAC 주소 테이블

이 장에서는 MAC 주소 테이블을 맞춤화하고 브리지 그룹에 대해 ARP 검사를 구성하는 방법을 설명합니다.

ARP 검사 및 MAC 주소 테이블 정보

브리지 그룹의 인터페이스에 대한 ARP 검사는 "중간자" 공격을 방지합니다. 또한 다른 ARP 설정을 맞춤화할 수 있습니다. MAC 스푸핑을 방지하기 위한 고정 ARP 항목의 추가를 포함하여 브리지 그룹에 대해 MAC 주소 테이블을 맞춤화할 수 있습니다.

브리지 그룹 트래픽에 대한 ARP 검사

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

ARP 감시 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP 응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 감시 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

ARP 감시를 활성화할 경우 ASA에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.
- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 ASA에서는 패킷을 누락시킵니다.
- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 ASA를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 관리 인터페이스는 이 파라미터가 플러딩을 실행하도록 설정된 경우에도 패킷을 플러딩하지 않습니다.

브리지 그룹에 대한 **MAC** 주소 테이블

ASA에서는 일반적인 브리지 또는 스위치와 유사한 방식으로 MAC 주소 테이블을 학습하고 구축합니다. 디바이스에서 브리지 그룹을 통해 패킷을 전송하면 ASA에서는 MAC 주소를 해당 테이블에 추가합니다. 테이블에서는 MAC 주소와 소스 인터페이스를 연결하므로 ASA에서는 디바이스에 대해 주소가 지정된 모든 패킷을 올바른 인터페이스로 전송할 수 있다는 사실을 파악합니다.

ASA는 방화벽이므로 패킷의 목적지 MAC 주소가 테이블에 없을 경우, 일반적인 브리지에서는 원래 패킷을 모든 인터페이스에 플러딩하지만 ASA의 경우에는 이러한 작업을 수행하지 않습니다. 그 대신 ASA에서는 직접 연결된 디바이스 또는 원격 디바이스에 다음 패킷을 생성합니다.

- 직접 연결된 디바이스에 대한 패킷 — ASA에서 대상 IP 주소에 대한 ARP 요청을 생성하므로 어떤 인터페이스에서 ARP 응답을 수신하는지 알 수 있습니다.
- 원격 디바이스에 대한 패킷 — ASA에서 대상 IP 주소에 대한 Ping을 생성하므로 어떤 인터페이스에서 Ping 응답을 수신하는지 알 수 있습니다.

원래 패킷은 손실됩니다.

기본 설정

- ARP 감시를 활성화할 경우 기본 설정은 불일치 패킷을 플러딩하는 것입니다.
- 동적 MAC 주소 테이블 항목의 기본 시간 초과 값은 5분입니다.
- 기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다.

ARP 검사 및 MAC 주소 테이블에 대한 지침

- ARP 검사는 브리지 그룹에만 지원됩니다.
- MAC 주소 테이블 구성은 브리지 그룹에만 지원됩니다.

ARP 검사 및 기타 ARP 파라미터 구성

브리지 그룹에 대해 ARP 검사를 활성화할 수 있습니다. 라우팅 모드 인터페이스와 브리지 그룹 모두에 대해 다른 ARP 파라미터를 구성할 수도 있습니다.

프로시저

단계 **1** 고정 ARP 항목 추가 및 다른 ARP 파라미터 맞춤화, 789 페이지에 따라 고정 ARP 항목을 추가합니다. ARP 감시 기능은 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교하므로, 이 기능에는 고정 ARP 항목이 필요합니다. 다른 ARP 파라미터를 구성할 수도 있습니다.

단계 **2** ARP 감시 활성화, 791 페이지의 내용에 따라 ARP 검사를 활성화합니다.

고정 ARP 항목 추가 및 다른 ARP 파라미터 맞춤화

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 인터페이스 간에 허용됩니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다. ARP 검사에서는 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교합니다.

라우팅 인터페이스의 경우 고정 ARP 항목을 입력할 수 있지만 일반적으로 동적 항목이면 충분합니다. 라우팅 인터페이스의 경우 패킷을 직접 연결된 호스트에 전달하는 데 ARP 테이블이 사용됩니다. 발신자가 IP 주소로 패킷 대상을 식별하긴 하지만, 이더넷에서 패킷이 실제 전달되는 것은 이더넷 MAC 주소에 달려 있습니다. 라우터 또는 호스트에서 패킷을 직접 연결된 디바이스에 전달하려는 경우, IP 주소와 연관된 MAC 주소를 묻는 ARP 요청이 전송되며 그 후 ARP 응답에 따라 패킷이 MAC 주소로 전달됩니다. 호스트 또는 라우터에서는 ARP 테이블을 보관하므로, 모든 패킷을 전달할 때마다 ARP 요청을 보내지 않아도 됩니다. ARP 테이블은 ARP 응답이 네트워크로 전송될 때마다 동적으로 업데이트되며, 일정 기간 동안 사용되지 않는 항목이 있으면 해당 항목은 시간 초과로 만료됩니다. 항목이 잘못된 경우(예: 제공된 IP 주소의 MAC 주소가 변경된 경우), 해당 항목은 새 정보로 업데이트되기 전에 시간 제한에 도달해야 합니다.

투명 모드의 경우 ASA에서는 ASA로 들어오고 나가는 트래픽(예: 관리 트래픽)에 ARP 테이블의 동적 ARP 항목만 사용합니다.

ARP 시간 제한 및 기타 ARP 동작을 설정할 수도 있습니다.

프로시저

단계 **1** 정적 ARP 항목을 추가합니다.

arp *interface_name ip_address mac_address* [**alias**]

예제**:**

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

이 예에서는 외부 인터페이스에서 MAC 주소가 0009.7cbe.2100인 10.1.1.1의 라우터로부터의 ARP 응답을 허용합니다.

이 매핑에 대해 프록시 ARP를 활성화하려면 라우팅 모드에서 **alias**를 지정합니다. ASA에서는 지정된 IP 주소의 ARP 요청을 수신하면 ASA MAC 주소에 응답합니다. 이 키워드는 이를테면 ARP를 수행하지 않는 디바이스가 있을 경우 유용합니다. 투명 방화벽 모드에서는 이 키워드가 무시됩니다. ASA에서 프록시 ARP를 수행하지 않습니다.

단계 **2** 동적 ARP 항목에 대해 ARP 시간 제한을 설정합니다.

arp timeout *seconds*

예제**:**

```
ciscoasa(config)# arp timeout 5000
```

이 필드에서는 ASA에서 ARP 테이블을 재구성하기 전까지 걸리는 시간을 60~4294967초 범위에서 설정합니다. 기본값은 14400초입니다. ARP 테이블을 재구성하면 새 호스트 정보가 자동으로 업데이트되고 기존 호스트 정보가 제거됩니다. 호스트 정보는 자주 변경되므로 시간 초과 값을 낮출 수 있습니다.

단계 **3** 연결되지 않은 서브넷을 허용합니다.

arp permit-nonconnected

ASA ARP 캐시에는 기본적으로 직접 연결된 서브넷의 항목만 포함됩니다. ARP 캐시에 직접 연결되지 않은 서브넷도 포함되도록 설정할 수 있습니다. 그러나 보안 위험을 잘 숙지하고 있지 않다면 이 기능은 사용하지 않는 것이 좋습니다. 이 기능은 ASA에 대한 DoS(서비스 거부 시도) 공격을 촉진할 수 있습니다. 즉, 임의의 인터페이스에서 사용자가 다량의 ARP 응답을 전송하고 ASA ARP 테이블에 false 항목이 오버로드되도록 할 수 있습니다.

다음을 사용하는 경우 이 기능을 사용할 수 있습니다.

- 보조 서브넷
- 트래픽 전달을 지원하는 인접 경로의 프록시 ARP

단계 **4** 초당 ARP 패킷의 수를 제어하려면 ARP 속도 제한을 설정합니다.

arp rate-limit *seconds*

예제**:**

```
ciscoasa(config)# arp rate-limit 1000
```

10~32768 범위의 값을 입력합니다. 기본값은 ASA 모델에 따라 달라집니다. ARP 스톰 공격을 방지하기 위해 이 값을 맞춤화할 수 있습니다.

ARP 감시 활성화

이 섹션에서는 브리지 그룹에 대해 ARP 검사를 활성화하는 방법을 설명합니다.

프로시저

ARP 감시를 활성화합니다.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

예제:

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

flood 키워드를 사용하면 불일치 ARP 패킷이 모든 인터페이스에 전달되며, **no-flood** 키워드를 사용하면 불일치 패킷이 삭제됩니다.

기본 설정은 불일치 패킷을 플러딩하는 것입니다. ASA를 통과하는 ARP를 고정 항목으로만 제한하려면 이 명령을 **no-flood**로 설정합니다.

브리지 그룹에 대해 MAC 주소 테이블 맞춤화

이 섹션에서는 브리지 그룹에 대해 MAC 주소 테이블을 맞춤화하는 방법을 설명합니다.

브리지 그룹에 대해 고정 MAC 주소 추가

일반적으로 MAC 주소는 특정 MAC 주소의 트래픽이 인터페이스에 들어올 때 MAC 주소 테이블에 동적으로 추가됩니다. 고정 MAC 주소를 MAC 주소 테이블에 추가할 수 있습니다. 고정 항목을 추가함으로써 얻을 수 있는 한 가지 혜택은 MAC 스푸핑을 차단할 수 있다는 점입니다. 동일한 MAC 주소를 고정 항목으로 보유한 클라이언트에서 고정 항목이 일치하지 않는 인터페이스에 트래픽을 전송하려고 시도할 경우, ASA에서는 해당 트래픽을 삭제하며 시스템 메시지가 생성됩니다. 고정 ARP 항목을 추가할 경우(고정 ARP 항목 추가 및 다른 ARP 파라미터 맞춤화, 789 페이지 참조), 고정 MAC 주소가 MAC 주소 테이블에 자동으로 추가됩니다.

MAC 주소 테이블에 고정 MAC 주소를 추가하려면 다음 단계를 수행하십시오.

프로시저

고정 MAC 주소 항목을 추가합니다.

mac-address-table static *interface_name mac_address*

예제:

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

*interface_name*은 소스 인터페이스입니다.

MAC 주소 시간 제한 설정

동적 MAC 주소 테이블의 기본 시간 초과 값은 5분이지만, 시간 초과 값을 변경할 수 있습니다. 시간 제한을 변경하려면 다음 단계를 수행합니다.

프로시저

MAC 주소 항목 시간 제한을 설정합니다.

mac-address-table aging-time *timeout_value*

예제:

```
ciscoasa(config)# mac-address-table aging-time 10
```

timeout_value(분 단위)의 범위는 5분 ~ 720분(12시간)입니다. 5분이 기본값입니다.

MAC 주소 학습 비활성화

기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다. 원하는 경우 MAC 주소 학습을 비활성화할 수 있으나, 테이블에 MAC 주소를 고정으로 추가하지 않으면 트래픽이 ASA를 통과하여 전달될 수 없습니다.

MAC 주소 학습을 비활성화하려면 다음 단계를 수행합니다.

프로시저

MAC 주소 학습을 비활성화합니다.

mac-learn *interface_name* **disable**

예제:

```
ciscoasa(config)# mac-learn inside disable
```

이 명령을 **no** 형식으로 사용하면 MAC 주소 학습을 다시 활성화할 수 있습니다.

clear configure mac-learn 명령을 사용하면 모든 인터페이스에서 MAC 주소 학습을 다시 활성화할 수 있습니다.

ARP 검사 및 MAC 주소 테이블 모니터링

- **show arp-inspection**

  ARP 감시를 모니터링합니다. 모든 인터페이스에서 ARP 감시에 대한 현재 설정을 표시합니다.

- **show mac-address-table [*interface_name*]**

  MAC 주소 테이블을 모니터링합니다. 전체 MAC 주소 테이블(두 인터페이스의 고정 및 동적 항목 포함)을 보거나, 인터페이스의 MAC 주소 테이블을 볼 수 있습니다.

  다음은 전체 테이블을 표시하는 **show mac-address-table** 명령의 샘플 출력입니다.

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

  다음은 내부 인터페이스의 테이블을 표시하는 **show mac-address-table** 명령의 샘플 출력입니다.

```
ciscoasa# show mac-address-table inside
interface        mac address       type         Time Left
------------------------------------------------------------------------
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

ARP 검사 및 MAC 주소 테이블에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
ARP 감시	7.0(1)	ARP 감시 기능은 모든 ARP 패킷의 MAC 주소, IP 주소, 소스 인터페이스를 ARP 테이블의 고정 항목과 비교합니다. 이 기능은 투명 방화벽 모드에서 사용할 수 있으며 9.7(1)에서 시작되는 투명 모드 및 라우팅 모드 둘 다의 브리지 그룹 인터페이스에서 사용할 수 있습니다. 다음 명령을 도입했습니다. **arp**, **arp-inspection**, **show arp-inspection**
MAC 주소 테이블	7.0(1)	투명 모드와 9.7(1)에서 시작되는 투명 모드 및 라우팅 모드 둘 다의 브리지 그룹 인터페이스에 대해 MAC 주소 테이블을 맞춤화할 수 있습니다. 다음 명령을 도입했습니다. **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable**, **show mac-address-table**
연결되지 않은 서브넷에 대한 ARP 캐시 추가	8.4(5), 9.1(2)	ASA ARP 캐시에는 기본적으로 직접 연결된 서브넷의 항목만 포함됩니다. ARP 캐시에 직접 연결되지 않은 서브넷도 포함되도록 설정할 수 있습니다. 그러나 보안 위험을 잘 숙지하고 있지 않다면 이 기능은 사용하지 않는 것이 좋습니다. 이 기능은 ASA에 대한 DoS(서비스 거부 시도) 공격을 촉진할 수 있습니다. 즉, 임의의 인터페이스에서 사용자가 다량의 ARP 응답을 전송하고 ASA ARP 테이블에 false 항목이 오버로드되도록 할 수 있습니다. 다음을 사용하는 경우 이 기능을 사용할 수 있습니다. • 보조 서브넷 • 트래픽 전달을 지원하는 인접 경로의 프록시 ARP 다음 명령을 도입했습니다. **arp permit-nonconnected**

기능 이름	플랫폼 릴리스	기능 정보
맞춤화 가능한 ARP 속도 제한	9.6(2)	초당 허용되는 ARP 패킷의 최대 수를 설정할 수 있습니다. 기본값은 ASA 모델에 따라 달라집니다. ARP 스톰 공격을 방지하기 위해 이 값을 맞춤화할 수 있습니다. 추가된 명령: **arp rate-limit, show arp rate-limit**

기능 이름	플랫폼 릴리스	기능 정보
통합 라우팅 및 브리징	9.7(1)	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 ASA에서 경로 대신 브리징하는 인터페이스 그룹입니다. ASA는 실제 브리지가 아닙니다. ASA는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이전에는 브리지 그룹 간에 라우팅할 수 없는 투명 방화벽 모드에서만 브리지 그룹을 구성할 수 있었습니다. 이 기능을 사용하면 라우팅 방화벽 모드에서 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 ASA에 있는 경우에는 외부 Layer 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. 라우팅 모드에서 BVI는 명명된 인터페이스가 될 수 있으며 액세스 규칙 및 DHCP 서버와 같은 일부 기능에서 멤버 인터페이스와 별도로 참여할 수 있습니다. 투명 모드에서 지원되는 다중 상황 모드, ASA 클러스터링 기능은 라우팅 모드에서는 지원되지 않습니다. 동적 라우팅 및 멀티캐스트 라우팅 기능은 BVI에서도 지원되지 않습니다. 수정된 명령: **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**

V 부

IP 라우팅

23 장

라우팅 개요

이 장에서는 ASA 내에서의 라우팅 동작 방식을 설명합니다.

경로 결정

라우팅 프로토콜은 메트릭을 사용하여 패킷이 이동할 최적의 경로를 평가합니다. 메트릭은 경로 대역폭과 같은 측정 기준이며, 목적지에 대한 최적 경로를 결정하는 라우팅 알고리즘에 사용됩니다. 라우팅 알고리즘은 경로 결정을 돕기 위해 경로 정보를 포함하는 라우팅 테이블을 초기화하고 유지합니다. 경로 정보는 사용된 경로 알고리즘에 따라 달라집니다.

라우팅 알고리즘은 다양한 정보로 라우팅 테이블을 채웁니다. 목적지 또는 다음 홉 연결은 최종 목적지로 향하는 과정에서 다음 홉에 해당하는 라우터에 패킷을 전달하는 것이 목적지에 도달하는 최적의 방식임을 라우터에 알립니다. 라우터가 수신 패킷을 수신하면 목적지 주소를 확인하고 이 주소를 다음 홉과 연결하려고 시도합니다.

라우팅 테이블은 또한 경로의 선호도와 같은 다른 정보도 포함합니다. 라우터는 메트릭을 비교하여 최적의 경로를 결정하고 이러한 메트릭은 사용된 라우팅 알고리즘의 설계에 따라 달라집니다.

라우터는 서로 통신하며 다양한 메시지의 전송을 통해 라우팅 테이블을 유지합니다. 라우팅 업데이트 메시지는 일반적으로 라우팅 테이블 전체 또는 일부로 구성되는 메시지입니다. 라우터는 다른 모든 라우터의 라우팅 업데이트를 분석함으로써 네트워크 토폴로지에 대한 자세한 그림을 그릴 수 있습니다. 라우터 간에 전송되는 메시지의 또 다른 예인 링크-상태 알림은 다른 라우터에 발신자 링크의 상태를 알려줍니다. 연결 정보는 라우터가 네트워크 목적지로의 최적의 경로를 결정할 수 있도록 네트워크 토폴로지의 완전한 그림을 그리는 데에도 사용됩니다.

참고 비대칭 라우팅은 다중 컨텍스트 모드의 액티브/액티브 장애 조치에 대해서만 지원됩니다.

지원되는 경로 유형

라우터는 몇 가지 경로 유형을 사용할 수 있습니다. ASA는 다음 경로 유형을 사용합니다.

- 고정 대 동적
- 단일 경로 대 다중 경로
- 평면 대 계층형
- 연결 상태 대 거리 벡터

고정 대 동적

고정 라우팅 알고리즘은 실제로 네트워크 관리자가 설정한 테이블 매핑입니다. 이러한 매핑은 네트워크 관리자가 변경하지 않는 한 변경되지 않습니다. 고정 경로를 사용하는 알고리즘은 설계하기가 쉽고 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다.

고정 라우팅 시스템은 네트워크 변화에 대응할 수 없기 때문에 꾸준히 변화하는 대규모 네트워크에는 일반적으로 적합하지 않습니다. 대부분의 주요 라우팅 알고리즘은 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 대응하는 동적 라우팅 알고리즘입니다. 메시지가 네트워크 변경 사실을 알리면 라우팅 소프트웨어가 경로를 다시 계산하고 새로운 라우팅 업데이트 메시지를 보냅니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

동적 라우팅 알고리즘은 고정 경로로 적절히 보완할 수 있습니다. 예를 들어 최후의 수단으로 사용하는 라우터(모든 라우팅 불가 패킷이 전송되는 라우터의 기본 경로)는 모든 라우팅 불가 패킷에 대한 저장소 역할을 하도록 지정되어 모든 메시지가 어떻게든 처리되도록 할 수 있습니다.

단일 경로 대 다중 경로

일부 고급 라우팅 프로토콜은 동일 목적지에 대한 다중 경로를 지원합니다. 단일 경로 알고리즘과 달리 이러한 다중 경로 알고리즘은 여러 회선에 걸친 트래픽 멀티플렉싱을 허용합니다. 다중 경로 알고리즘의 이점은 보통 로드 공유라고 부르는 훨씬 뛰어난 처리량과 신뢰성입니다.

평면 대 계층형

일부 라우팅 알고리즘은 평면 공간에서 작동하고 또 다른 일부는 라우팅 계층을 사용합니다. 평면 라우팅 시스템에서 라우터는 다른 모든 라우터의 피어입니다. 계층형 라우팅 시스템에서는 일부 라우터가 모여 라우팅 백본을 형성합니다. 비 백본 라우터의 패킷은 백본 라우터로 이동하고, 여기서 백

본을 통해 대상의 일반 영역에 전달됩니다. 이 지점에 이르면 마지막 백본 라우터에서 하나 이상의 비 백본 라우터를 거쳐 최종 대상으로 이동합니다.

대개 라우팅 시스템은 도메인, 자율 시스템 또는 영역이라고 하는 논리적인 노드 그룹을 지정합니다. 계층형 시스템에서는 다른 도메인의 라우터와 통신할 수 있는 라우터도 있고 같은 도메인의 라우터하고만 통신할 수 있는 라우터도 있습니다. 대규모 네트워크에서는 추가적인 계층 수준이 있을 수 있고 가장 높은 계층 수준의 라우터가 라우팅 백본을 형성합니다.

계층형 라우팅의 가장 큰 장점은 기업 대부분의 조직 구조와 비슷하기 때문에 조직의 트래픽 패턴도 잘 지원한다는 점입니다. 대부분의 네트워크 통신은 소규모 기업 그룹(도메인) 내에서 발생합니다. 인트라도메인 라우터는 도메인 내의 다른 라우터에 대해서만 알면 되므로 라우팅 알고리즘을 간소화할 수 있고 사용되는 라우팅 알고리즘에 따라 라우팅 업데이트 트래픽을 줄일 수 있습니다.

연결 상태 대 거리 벡터

링크 상태 알고리즘 (최단 경로 우선 알고리즘)은 인터네트워크의 모든 노드로 라우팅 정보를 전달합니다. 하지만 각 라우터는 자신의 링크 상태를 설명하는 라우팅 테이블의 일부만 전송합니다. 링크 상태 알고리즘에서는 각 라우터가 라우팅 테이블에서 전체 네트워크의 상태를 그립니다. 거리 벡터 알고리즘(Bellman-Ford 알고리즘이라고도 함)은 각 라우터를 호출하여 라우팅 테이블의 전체 또는 일부를 네이버에 한해 전송하도록 합니다. 기본적으로 링크 상태 알고리즘은 모든 곳으로 소규모 업데이트를 전송하는 반면 거리 벡터 알고리즘은 대규모 업데이트를 인접 디바이스로만 보냅니다. 거리 벡터 알고리즘은 네이버에 대해서만 알고 있습니다. 일반적으로 링크 상태 알고리즘은 OSPF 라우팅 프로토콜과 함께 사용됩니다.

라우팅을 위한 지원되는 인터넷 프로토콜

ASA는 라우팅을 위해 몇 가지 인터넷 프로토콜을 지원합니다. 이 섹션에서는 각 프로토콜에 대해 간단하게 설명합니다.

- EIGRP(Enhanced Interior Gateway Routing Protocol)

  EIGRP는 IGRP 라우터와의 호환성 및 원활한 상호 작용을 제공하는 Cisco 고유의 프로토콜입니다. 자동 재배포 메커니즘이 IGRP 경로를 Enhanced IGRP로 또한 그 반대로 가져올 수 있게 합니다. 따라서 Enhanced IGRP를 기존 IGRP 네트워크에 점진적으로 추가할 수 있습니다.

- OSPF(Open Shortest Path First)

  OSPF는 IETF(Internet Engineering Task Force)의 IGP(interior gateway protocol) 작업 그룹에서 IP(Internet Protocol) 네트워크를 위해 개발한 라우팅 프로토콜입니다. OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터는 동일한 링크 상태 데이터베이스를 갖고 있는데, 이는 각 라우터에서 사용 가능한 인터페이스 및 연결 가능한 네이버의 목록입니다.

- RIP(Routing Information Protocol)

  RIP는 홉 카운트를 메트릭으로 사용하는 거리 벡터 프로토콜입니다. RIP는 글로벌 인터넷에서 라우팅 트래픽을 위해 널리 사용되며 내부 게이트웨이 프로토콜(IGP)이기 때문에 단일 자율 시스템 내에서 라우팅을 수행합니다.

- BGP(Border Gateway Protocol)

  BGP는 자율 시스템 간 라우팅 프로토콜입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. AS(autonomous system) 사이에서 BGP가 사용될 때 이 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때의 프로토콜은 IBGP(Interior BGP)라고 합니다.

- IS-IS(Intermediate System to Intermediate System)

  IS-IS는 링크 상태 IGP(Interior Gateway Protocol)입니다. 링크 상태 프로토콜은 각 참여 라우터에서 전체 네트워크 연결 맵을 작성하는 데 필요한 정보를 전파하는 것이 특징입니다. 그런 다음 해당 맵은 대상에 대한 최단 경로를 계산하는 데 사용됩니다.

라우팅 테이블

이 섹션에서는 라우팅 테이블을 설명합니다.

라우팅 테이블을 채우는 방법

ASA 라우팅 테이블은 정적으로 정의된 경로, 직접 연결된 경로, 그리고 동적 라우팅 프로토콜에서 검색한 경로로 채울 수 있습니다. ASA는 라우팅 테이블에 고정 경로와 연결 경로를 가지는 것 외에도 여러 라우팅 프로토콜을 실행할 수 있기 때문에 같은 경로가 하나 이상의 방법으로 다시 발견되거나 입력될 수 있습니다. 같은 목적지로의 두 경로를 라우팅 테이블에 넣으면 라우팅 테이블에 유지되는 항목은 다음과 같이 결정됩니다.

- 두 경로의 네트워크 접두사 길이(네트워크 마스크)가 다르면 두 경로 모두 고유한 것으로 간주되어 라우팅 테이블에 입력됩니다. 그런 다음 패킷 전달 로직에서 둘 중 어느 것을 사용할지 결정합니다.

  예를 들어 RIP 및 OSPF 프로세스에서 다음 경로를 검색한 경우

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  비록 OSPF 경로의 관리 영역이 더 낮지만, 접두사 길이(서브넷 마스크)가 다르기 때문에 두 경로 모두 라우팅 테이블에 설치됩니다. 이들은 다른 목적지로 간주되며 패킷 전달 로직에서 사용할 경로를 결정합니다.

- ASA가 RIP와 같이 단일 라우팅 프로토콜에서 같은 대상으로의 여러 경로를 학습하는 경우 메트릭이 더 나은 경로(라우팅 프로토콜이 결정)가 라우팅 테이블에 입력됩니다.

  메트릭은 특정 경로와 연결되는 값이며, 선호도가 가장 높은 것부터 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 목적지의 다중 경로가 메트릭 값이 같을 경우 이 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

- ASA가 두 개 이상이 라우팅 프로토콜로부터 대상에 대해 학습하는 경우 경로의 관리 거리를 비교하고 관리 거리가 짧은 경로가 라우팅 테이블에 입력됩니다.

경로의 관리 거리

라우팅 프로토콜에서 검색 또는 재배포되는 경로에 대한 관리 영역을 변경할 수 있습니다. 서로 다른 두 라우팅 프로토콜의 두 경로가 관리 영역이 같을 경우 기본 관리 영역이 낮은 경로가 라우팅 테이블에 입력됩니다. EIGRP 및 OSPF 경로의 경우 EIGRP 경로와 OSPF 경로가 관리 영역이 같으면 기본적으로 EIGRP 경로가 선택됩니다.

관리 영역은 서로 다른 두 라우팅 프로토콜로부터 동일한 목적지의 서로 다른 경로가 2개 이상 나올 경우 최적의 경로를 선택하기 위해 ASA에서 사용하는 경로 매개변수입니다. 라우팅 프로토콜은 다른 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 서로 다른 라우팅 프로토콜에서 생성된 동일 목적지의 경로 2개 중에서 최적의 경로를 결정하는 것이 가능하지 않을 수도 있습니다.

각 라우팅 프로토콜은 관리 영역 값을 사용하여 우선순위가 지정됩니다. 다음 표에는 ASA에서 지원하는 라우팅 프로토콜의 기본 관리 거리 값이 정리되어 있습니다.

표 ***26:*** 지원되는 라우팅 프로토콜의 기본 관리 영역

경로 소스	기본 관리 영역
연결된 인터페이스	0
고정 경로	1
EIGRP 요약 경로	5
외부 BGP	20
내부 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 외부 경로	170
내부 및 로컬 BGP	200
Unknown	255

관리 영역의 값이 작을수록 프로토콜 우선순위가 높습니다. 예를 들어, ASA가 OSPF 라우팅 프로세스(기본 관리 거리 - 110)와 RIP 라우팅 프로세스(기본 관리 거리 - 120)로부터 모두 특정 네트워크로의 경로를 수신할 경우 ASA는 우선순위가 더 높은 OSPF 경로를 선택합니다. 이러한 경우 라우터가 라우팅 테이블에 경로의 OSPF 버전을 추가합니다.

이 예에서, OSPF 파생 경로의 소스가 손실된 경우(예: 전원 꺼짐) ASA는 OSPF 파생 경로가 다시 나타날 때까지 RIP 파생 경로를 사용합니다.

관리 영역은 로컬 설정입니다. 예를 들어 OSPF를 통해 얻은 경로의 관리 영역을 변경하면 이 변경 사항은 이 명령을 입력한 ASA의 라우팅 테이블에만 영향을 미칩니다. 관리 영역은 라우팅 업데이트에서 광고되지 않습니다.

관리 영역은 라우팅 프로세스에 영향을 주지 않습니다. 라우팅 프로세스에서는 라우팅 프로세스를 통해 검색되었거나 라우팅 프로세스로 재배포된 경로만 알립니다. 예를 들어 RIP 라우팅 프로세스는 OSPF 라우팅 프로세스를 통해 발견된 경로가 라우팅 테이블에 사용되더라도 RIP 경로를 광고합니다.

동적 및 부동 정적 경로 백업

다른 경로가 설치되었기 때문에 라우팅 테이블에 경로를 설치하려는 첫 번째 시도가 실패하면 백업 경로가 등록됩니다. 라우팅 테이블에 설치된 경로가 실패할 경우 라우팅 테이블 유지 관리 프로세스는 백업 경로를 등록한 각 라우팅 프로토콜 프로세스를 호출하고 해당 경로를 라우팅 테이블에 다시 설치하도록 요청합니다. 실패한 경로에 대해 백업이 등록된 프로토콜이 여럿인 경우 관리 영역을 기준으로 우선 경로가 선택됩니다.

이 프로세스 때문에 동적 라우팅 프로토콜을 통해 발견된 경로가 실패할 때 라우팅 테이블에 설치된 유동 고정 경로를 생성할 수 있습니다. 유동 고정 경로는 단순히 ASA에서 실행되는 동적 라우팅 프로토콜보다 큰 관리 영역으로 설정된 고정 경로입니다. 동적 라우팅 프로세스에서 발견한 경로가 실패하면 라우팅 테이블에 고정 경로가 설치됩니다.

포워딩 결정 방법

포워딩 결정은 다음과 같이 이루어집니다.

- 목적지가 라우팅 테이블 내의 항목과 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 포워딩됩니다. 기본 경로가 구성되지 않은 경우 패킷이 폐기됩니다.
- 목적지가 라우팅 테이블의 단일 항목과 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 포워딩됩니다.
- 목적지가 라우팅 테이블에 있는 두 개 이상의 항목과 일치하면 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷은 라우팅 테이블의 다음 경로를 통해 인터페이스에 도착합니다.

- 192.168.32.0/24 게이트웨이 10.1.1.2
- 192.168.32.0/19 게이트웨이 10.1.1.3

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 이 주소는 라우팅 테이블 내 다른 경로에도 포함되지만, 라우팅 테이블의 다른 경로 접두사는 19비트인 데 비해 192.168.32.0/24의 접두사는 24비트이므로 이 경로의 접두사가 가장 깁니다. 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

참고 새로운 유사한 연결이 경로 변경으로 인해 다른 동작을 유발하는 경우에도 기존의 연결은 계속해서 설정된 인터페이스를 사용합니다.

동적 라우팅 및 장애 조치

라우팅 테이블이 액티브 유닛에서 변경될 때 동적 경로는 스탠바이 유닛에서 동기화됩니다. 즉, 액티브 유닛의 모든 추가, 삭제 또는 변경 작업은 즉시 스탠바이 유닛에 전파됩니다. 스탠바이 유닛이 액티브/스탠바이 준비 장애 조치 쌍에서 액티브 상태가 되면 경로가 장애 조치 대량 동기화 및 연속 복제 프로세스의 일부로 동기화되므로 해당 유닛은 이전 액티브 유닛과 동일한 라우팅 테이블을 이미 갖게 됩니다.

동적 라우팅 및 클러스터링

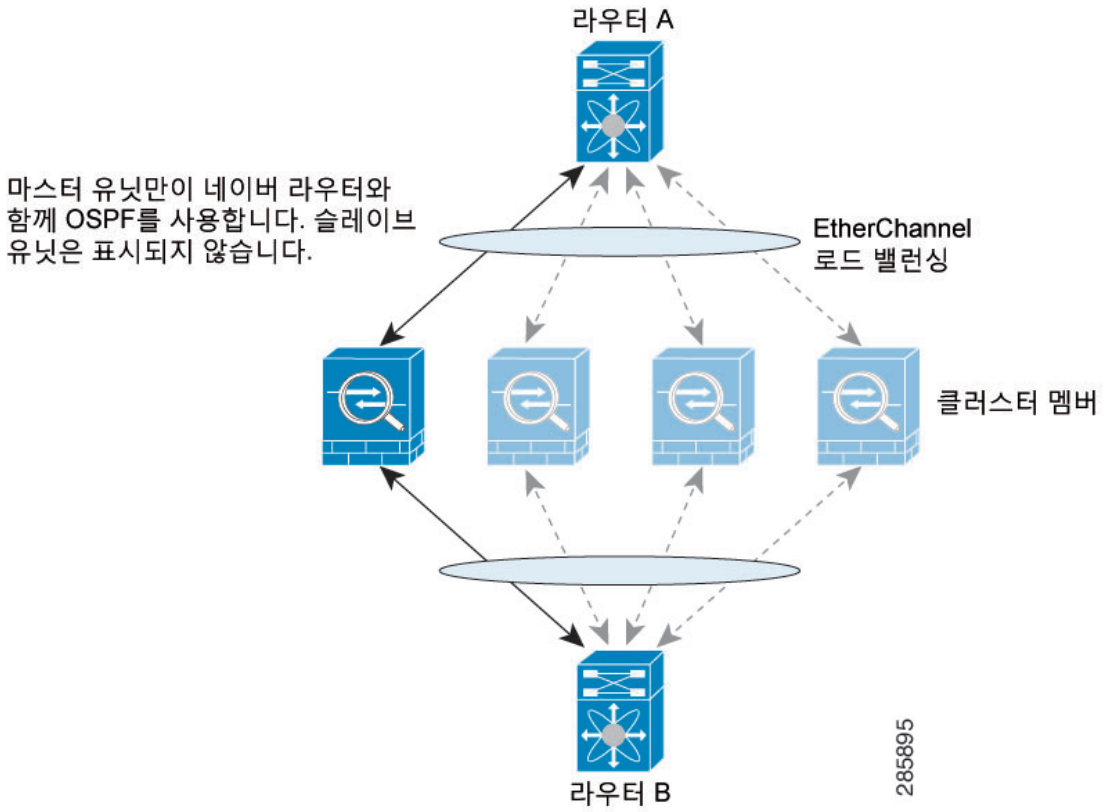
이 섹션에서는 클러스터링을 통해 동적 라우팅을 사용하는 방법에 대해 설명합니다.

Spanned EtherChannel 모드의 동적 라우팅

참고 IS-IS는 Spanned EtherChannel 모드에서 지원되지 않습니다.

스팬 EtherChannel 모드의 경우 라우팅 프로세스는 마스터 유닛에서만 실행되며, 마스터 유닛을 통해 경로가 파악되고 슬레이브에 복제됩니다. 라우팅 패킷이 슬레이브에 전송되면 해당 패킷은 마스터 유닛에 리디렉션됩니다.

그림 ***58: Spanned EtherChannel*** 모드의 동적 라우팅



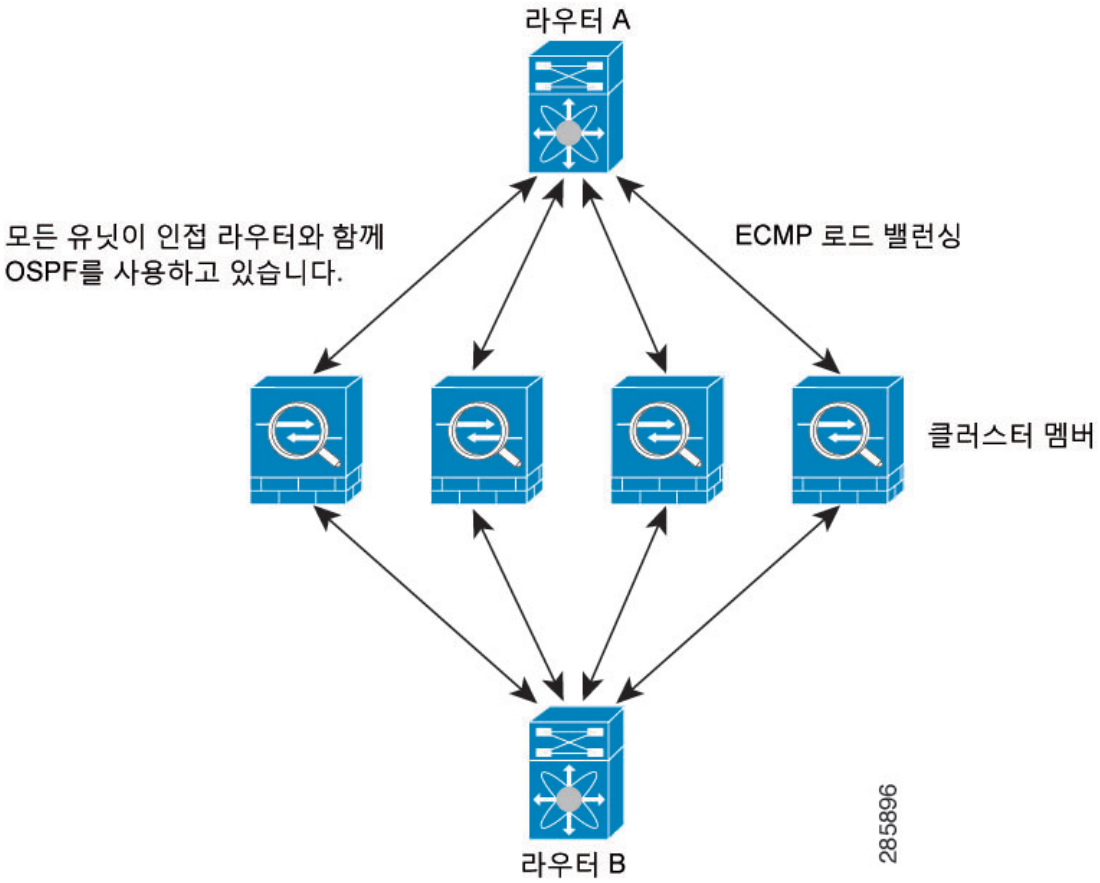
슬레이브 멤버가 마스터 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 마스터 유닛에서 슬레이브 유닛으로 동기화되지 않습니다. 마스터 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

개별 인터페이스 모드의 동적 라우팅

개별 인터페이스 모드의 경우 각 유닛에서는 라우팅 프로토콜을 독립형 라우터로 실행하며, 경로에 대한 정보 파악은 각 유닛에서 개별적으로 수행합니다.

그림 **59:** 개별 인터페이스 모드의 동적 라우팅



위 다이어그램에서 라우터 A는 라우터 B에 각각 ASA를 통한 4개의 Equal-Cost 경로가 있다는 정보를 파악합니다. ECMP는 4개 경로 간의 트래픽을 로드 밸런싱하는 데 사용됩니다. 각각의 ASA는 외부 라우터와 통신할 경우 다른 라우터 ID를 선택합니다.

라우터 ID에 대한 클러스터 풀을 구성하여 유닛마다 개별 라우터 ID를 보유하도록 해야 합니다.

EIGRP는 개별 인터페이스 모드에서 클러스터 피어와 네이버 관계를 형성하지 않습니다.

참고 클러스터가 이중화를 위해 동일한 라우터의 여러 위치에 인접하는 경우 비대칭 라우팅으로 인해 트래픽이 너무 많이 손실될 수 있습니다. 비대칭 라우팅을 피하려면 모든 ASA 인터페이스를 동일한 트래픽 영역으로 그룹화하십시오. 트래픽 영역 구성, 670 페이지을 참조하십시오.

다중 상황 모드의 동적 라우팅

다중 컨텍스트 모드에서 각 컨텍스트는 별도의 라우팅 테이블과 라우팅 프로토콜 데이터베이스를 유지합니다. 따라서 각 컨텍스트에서 OSPFv2 및 EIGRP를 독립적으로 구성할 수 있습니다. 일부 컨텍스트에서 EIGRP를 구성하고 동일 컨텍스트 또는 다른 컨텍스트에서 OSPFv2를 구성할 수 있습니

다. 혼합 컨텍스트 모드에서 라우팅 모드의 컨텍스트에서 어떤 동적 라우팅 프로토콜이라도 활성화할 수 있습니다. RIP 및 OSPFv3는 다중 컨텍스트 모드에서 지원되지 않습니다.

다음 표에서는 EIGRP 특성, OSPFv2, OSPFv2 및 EIGRP 프로세스로 경로를 배포하는 데 사용되는 경로 맵, 다중 컨텍스트 모드로 사용할 때 영역을 드나드는 라우팅 업데이트를 필터링하기 위해 OSPFv2에서 사용하는 접두사 목록을 나열합니다.

EIGRP	**OSPFv2**	경로 맵 및 접두사 목록
컨텍스트당 하나의 인스턴스가 지원됩니다.	컨텍스트당2개의 인스턴스가 지원됩니다.	해당 없음
시스템 컨텍스트에서 비활성화됩니다.		해당 없음
두 컨텍스트가 사용하는 자율 시스템 번호가 같을 수도 있고 다를 수도 있습니다.	두 컨텍스트가 사용하는 지역 ID가 같을 수도 있고 다를 수도 있습니다.	해당 없음
두 컨텍스트가 공유하는 인터페이스는 여러 EIGRP 인스턴스를 실행할 수도 있습니다.	두 컨텍스트가 공유하는 인터페이스는 여러 OSPF 인스턴스를 실행할 수도 있습니다.	해당 없음
공유 인터페이스 간 EIGRP 인스턴스의 상호 작용이 지원됩니다.	공유 인터페이스 간 OSPFv2 인스턴스의 상호 작용이 지원됩니다.	해당 없음
단일 모드에서 사용 가능한 모든 CLI는 다중 컨텍스트 모드에서도 사용 가능합니다.		
각 CLI는 사용되는 컨텍스트에만 영향을 미칠 수 있습니다.		

경로 리소스 관리

경로라고 하는 리소스 클래스는 상황에 존재할 수 있는 라우팅 테이블 항목의 최대 개수를 지정합니다. 이는 하나의 컨텍스트가 다른 컨텍스트의 가용 라우팅 테이블에 영향을 주는 문제를 해결하고 컨텍스트당 최대 경로 엔트리 수를 더욱 효과적으로 제어할 수 있게 합니다.

시스템 제한이 따로 정해지지 않았기 때문에 이 리소스 제한에 대한 절대값만 지정할 수 있습니다. 백분율 제한은 사용할 수 없습니다. 또한 컨텍스트당 최소 및 최대 제한이 없으므로 기본 클래스는 변경되지 않습니다. 컨텍스트에서 고정 또는 동적 라우팅 프로토콜(연결, 고정, OSPF, EIGRP 및 RIP)을 위한 새로운 경로를 추가할 경우 해당 컨텍스트의 리소스 제한에 도달했다면 경로 추가가 실패하고 syslog 메시지가 생성됩니다.

관리 트래픽용 라우팅 테이블

표준 보안 관행으로 데이터 트래픽에서 관리 트래픽을 분리 및 격리할 필요가 있는 경우가 많습니다. 이 격리를 달성하기 위해 ASA에서는 데이터 트래픽과 관리 전용 트래픽에 대해 각각 별도의 라우팅 테이블을 사용합니다.

관리 라우팅 테이블에서는 데이터 인터페이스 라우팅 테이블과 별도로 동적 라우팅을 지원합니다. 지정된 동적 라우팅 프로세스는 관리 전용 인터페이스 또는 데이터 인터페이스에서 실행해야 합니다. 두 유형을 혼용할 수는 없습니다. 별도의 관리 라우팅 테이블 없이 이전 릴리스에서 업그레이드할 경우, 동일한 동적 라우팅 프로세스를 사용하여 데이터 및 관리 인터페이스를 혼용하면 관리 인터페이스는 삭제됩니다.

HTTP, SCP, TFTP 등을 사용해 원격 파일을 여는 모든 기능의 경우, 인터페이스를 지정하지 않으면 ASA에서는 관리 전용 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 데이터 라우팅 테이블을 확인합니다. **copy** 명령, Smart Call Home, **trustpoint**, **trustpool** 등을 예로 들 수 있습니다.

기타 기능의 경우, 인터페이스를 지정하지 않으면 ASA에서는 데이터 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 관리 전용 라우팅 테이블을 확인합니다. ping, DNS, DHCP 등을 예로 들 수 있습니다.

관리 전용 인터페이스에는 관리 x/x 인터페이스뿐 아니라 관리 전용으로 컨피그레이션한 모든 인터페이스도 포함됩니다.

참고 VPN을 사용할 때 ASA를 입력한 인터페이스가 아닌 다른 인터페이스에 대해 관리 액세스를 허용하는 관리 액세스 기능을 컨피그레이션하는 경우, 별도 관리 및 데이터 라우팅 테이블 관련 라우팅 고려 사항으로 인해 VPN 종료 인터페이스 및 관리 액세스 인터페이스는 동일한 유형이어야 합니다. 즉 모두 관리 전용 인터페이스이거나 모두 일반 데이터 인터페이스이어야 합니다.

관리 인터페이스 식별

관리 전용으로 구성된 인터페이스는 관리 인터페이스로 간주됩니다.

다음 구성에서 GigabitEthernet0/0 및 Management0/0 인터페이스 둘 다 관리 인터페이스로 간주됩니다.

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

ECMP(Equal-Cost Multi-Path) 라우팅

ASA에서는 ECMP(Equal-Cost Multi-Path) 라우팅을 지원합니다.

인터페이스당 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 외부 인터페이스에서 서로 다른 게이트웨이를 지정하는 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

여기서는 외부 인터페이스에서 0.1.1.2, 10.1.1.3, 10.1.1.4끼리 트래픽 로드 밸런싱을 수행합니다. 트래픽은 소스와 대상 IP 주소, 수신 인터페이스, 프로토콜, 소스 및 대상 포트를 해싱하는 알고리즘에 따라 지정된 게이트웨이 사이에서 분배됩니다.

ECMP는 다중 인터페이스에서 지원되지 않으므로 동일한 목적지의 경로를 다른 인터페이스에서 정의할 수 없습니다. 다음 경로는 위의 경로 중 어느 것이든 구성될 경우 거부됩니다.

```
route outside2 0 0 10.2.1.1
```

영역을 사용할 경우, 하나의 영역 내에서 최대 8개의 인터페이스에 걸쳐 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 다음과 같이 영역 내 인터페이스 3개의 전 범위에 걸쳐 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

또한 동적 라우팅 프로토콜은 동일 비용 경로를 자동으로 구성할 수 있습니다. ASA에서는 더 강력한 로드 밸런싱 메커니즘을 통해 인터페이스 간의 트래픽을 로드 밸런싱합니다.

어떤 경로가 사라지면 디바이스에서는 다른 경로로 원활하게 플로우를 이동합니다.

프록시 ARP 요청 비활성화

호스트가 같은 이더넷 네트워크의 다른 디바이스로 IP 트래픽을 전송하는 경우 호스트가 디바이스의 MAC 주소를 알아야 합니다. ARP는 IP 주소를 MAC 주소로 확인하는 레이어 2 프로토콜입니다. 호스트는 "이 IP 주소는 누구입니까?"를 묻는 ARP 요청을 보냅니다. IP 주소를 소유한 디바이스에서 "저는 해당 IP 주소를 보유하고 있으며 내 MAC 주소입니다."라고 응답합니다.

프록시 ARP는 디바이스가 해당 IP 주소를 소유하지 않더라도 자신의 MAC 주소로 ARP 요청에 응답할 때 사용됩니다. ASA에서는 NAT를 구성할 때 프록시 ARP를 사용하고 ASA 인터페이스와 같은 네트워크에 있는 매핑된 주소를 지정합니다. 트래픽이 호스트에 도달할 수 있는 유일한 방법은 ASA에서 프록시 ARP를 사용하여 MAC 주소가 대상이 매핑된 주소에 할당되어 있음을 주장하는 것입니다.

아주 드문 경우 NAT 주소에 대한 프록시 ARP를 비활성화할 수 있습니다.

기존 네트워크와 겹치는 VPN 클라이언트 주소 풀이 있는 경우 ASA에서는 기본적으로 모든 인터페이스에서 프록시 ARP 요청을 전송합니다. 동일한 레이어 2 도메인에 다른 인터페이스가 있는 경우 이 인터페이스가 ARP 요청을 보고 인터페이스의 MAC 주소로 응답할 것입니다. 따라서 내부 호스트로 반환되는 VPN 클라이언트의 트래픽이 잘못된 인터페이스로 이동하여 삭제됩니다. 이 경우 원치 않는 인터페이스에 대한 프록시 ARP 요청을 비활성화해야 합니다.

프로시저

프록시 ARP 요청을 비활성화합니다.

sysopt noproxyarp *interface*

예제**:**

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

라우팅 테이블 표시

라우팅 테이블의 항목을 보려면 **show route** 명령을 사용합니다.

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

경로 개요에 대한 기록

표 ***27:*** 경로 개요에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
관리 인터페이스용 라우팅 테이블	9.5(1)	데이터 트래픽에서 관리 트래픽을 구분하고 분리하기 위해 관리 트래픽용으로 별도의 라우팅 테이블이 추가되었습니다. 각각 관리 및 데이터에 사용되는 별도의 라우팅 테이블이 ASA의 각 상황에 대한 IPv4와 IPv6용으로 생성됩니다. 또한, ASA의 각 상황에 대한 2개의 추가 라우팅 테이블이 RIB 및 FIB에서 추가되었습니다. 도입된 명령: show route management-only, show ipv6 routemanagement-only, show asp table route-management- only, clear route management-only, clear ipv6 route management-only, copy interface <interface> tftp/ftp

24 장

고정 경로 및 기본 경로

이 장에서는 Cisco ASA에서 고정 경로와 기본 경로를 구성하는 방법을 설명합니다.

고정 경로 및 기본 경로 소개

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다. 일반적으로 최소한 하나의 고정 경로를 구성해야 합니다. 다른 방법으로는 기본 네트워크 게이트웨이(대개는 다음 홉 라우터)에 라우팅되지 않는 모든 트래픽을 위한 기본 경로입니다.

기본 라우터

가장 간단한 옵션은 트래픽을 라우팅해주는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 정적 경로를 컨피그레이션하는 것입니다. 기본 고정 경로는 ASA가 학습 경로나 고정 경로를 가지고 있지 않은 모든 IP 패킷을 보낼 게이트웨이 IP 주소를 식별합니다. 기본 정적 경로는 대상 IP 주소가 0.0.0.0/0(IPv4) 또는 ::/0(IPv6)인 정적 경로일 뿐입니다.

항상 기본 경로를 정의해야 합니다.

정적 경로

다음과 같은 경우, 정적 경로를 사용할 수 있습니다.

- 네트워크에서 지원하지 않는 라우터 검색 프로토콜을 사용합니다.
- 네트워크 규모가 작고 고정 경로를 쉽게 관리할 수 있습니다.

- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.
- 기본 경로만으로 충분하지 않을 때도 있습니다. 기본 게이트웨이가 목적지 네트워크에 도달할 수 없는 경우가 있기 때문에 보다 구체적인 고정 경로도 구성해야 합니다. 예를 들어 기본 게이트웨이가 밖에 있는 경우 기본 경로는 ASA에 직접 연결되지 않은 내부 네트워크로 트래픽을 안내할 수 없습니다.
- 동적 라우팅 프로토콜을 지원하지 않는 기능을 사용 중입니다.

원치 않는 트래픽을 “완전히 사라지게 하기”위한 null0 인터페이스에 대한 경로

액세스 규칙을 통해 패킷 헤더의 정보에 따라 패킷을 필터링할 수 있습니다. null0 인터페이스에 대한 고정 경로는 액세스 규칙을 보완합니다. null0 경로를 사용하여 원치 않는 트래픽을 "블랙홀"로 전달함으로써 트래픽을 폐기할 수 있습니다.

고정 null0 경로는 성능을 향상시킵니다. 또한 라우팅 루프를 방지하는 데 고정 null0 경로를 사용할 수 있습니다. BGP는 Remotely Triggered Black Hole 라우팅을 위해 고정 null0 경로를 활용할 수 있습니다.

경로 우선 순위

- 특정 대상을 식별하는 경로가 기본 경로보다 우선합니다.
- 동일한 목적지에 대한 여러 경로(고정 또는 동적)가 있을 경우 경로의 관리 영역에 따라 우선 순위가 결정됩니다. 고정 경로는 1로 설정되므로 대개 우선 순위가 높은 경로입니다.
- 동일한 관리 거리에서 동일한 대상에 대해 여러 고정 경로가 있는 경우, ECMP(Equal-Cost Multi-Path) 라우팅, 809 페이지를 참조하십시오.
- 터널링 옵션을 사용하여 터널로부터 생성된 트래픽의 경우 이 경로는 구성되었거나 학습된 다른 기본 경로를 무시합니다.

투명 방화벽 모드 및 브리지 그룹 경로

ASA에서 발생하고 브리지 그룹 멤버 인터페이스를 거쳐 직접 연결되지 않은 네트워크로 가는 트래픽의 경우, 기본 경로 또는 고정 경로를 구성하여 ASA에서 어떤 브리지 그룹 멤버 인터페이스로 트래픽을 보낼지 알 수 있게 해야 합니다. ASA에서 발생하는 트래픽은 syslog 서버 또는 SNMP 서버로의 통신을 포함할 수 있습니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다. 투명 모드에서는 BVI를 게이트웨이 인터페이스로 지정할 수 없습니다. 멤버 인터페이스만 사용할 수 있습니다. 라우팅 모드의 브리지 그룹에 대해서는 고정 경로에서 BVI를 지정해야 합니다. 멤버 인터페이스는 지정할 수 없습니다. 자세한 내용은 MAC 주소 대 경로 조회 비교, 192 페이지를 참조하십시오.

고정 경로 추적

고정 경로의 문제 중 하나는 경로가 정상인지 다운되었는지 확인할 수 있는 내재적인 메커니즘이 없다는 것입니다. 다음 홉 게이트웨이가 사용할 수 없게 되어도 라우팅 테이블에 남습니다. 고정 경로는 ASA의 연결된 인터페이스가 다운되는 경우에만 라우팅 테이블에서 제거됩니다.

고정 경로 추적 기능은 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 보조 경로를 설치하는 수단을 제공합니다. 예를 들어 기본 ISP를 사용할 수 없는 경우에 대비하여 ISP 게이트웨이로의 기본 경로와 보조 ISP로의 보조 기본 경로를 정의할 수 있습니다.

ASA에서는 ASA에서 ICMP 에코 요청을 통해 모니터링하는 목적지 네트워크의 모니터링 대상 호스트와 고정 경로를 연결하는 방법으로 고정 경로 추적을 구현합니다. 에코 응답이 지정된 시간 동안 수신되지 않으면 호스트는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다. 메트릭이 높은 비추적 백업 경로를 제거된 경로 대신 사용합니다.

모니터링 대상을 선택할 때, ICMP 에코 요청에 응답할 수 있는지 확인해야 합니다. 대상은 사용자가 선택하는 아무 네트워크 객체나 될 수 있지만 다음을 사용할 것을 고려해야 합니다.

- ISP 게이트웨이(이중 ISP 지원) 주소
- 다음 홉 게이트웨이 주소(게이트웨이의 가용성이 우려되는 경우)
- syslog 서버와 같이 ASA가 통신해야 하는 대상 네트워크에 있는 서버
- 목적지 네트워크에 있는 지속적인 네트워크 객체

참고 야간에 꺼질 수 있는 PC는 좋은 선택이 아닙니다.

DHCP 나 PPPoE를 통해 얻은 고정으로 정의된 경로나 기본 경로를 위해 고정 경로 추적을 구성할 수 있습니다. 경로 추적이 구성된 여러 인터페이스에서만 PPPoE 클라이언트를 활성화할 수 있습니다.

고정 경로 및 기본 경로를 위한 지침

방화벽 모드 및 브리지 그룹

- 투명 모드의 경우, 정적 경로에서는 브리지 그룹 멤버 인터페이스를 게이트웨이로 사용해야 하며 BVI는 지정할 수 없습니다.
- 라우티드 모드에서는 BVI를 게이트웨이로 지정해야 하며 멤버 인터페이스는 지정할 수 없습니다.
- 브리지 그룹 멤버 인터페이스 또는 BVI에 대해서는 고정 경로 추적이 지원되지 않습니다.

IPv6

- 고정 경로 추적은 IPv6에서 지원되지 않습니다.

클러스터링

클러스터링에서는 정적 경로 모니터링을 기본 유닛에서만 지원합니다.

기본 및 고정 경로 구성

최소한 기본 경로 하나를 구성해야 합니다. 고정 경로 구성도 필요할 수 있습니다. 이 섹션에서는 기본 경로 구성, 고정 경로 구성 및 고정 경로 추적을 수행합니다.

기본 경로 구성

기본 경로는 단순히 목적지 IP 주소가 0.0.0.0/0인 고정 경로입니다. 이 절차를 사용하여 수동으로 구성하거나 DHCP 서버 또는 기타 라우팅 프로토콜에서 파생된 기본 경로가 항상 있어야 합니다.

시작하기 전에

터널링 옵션에 대해서는 다음 지침을 참조하십시오.

- 터널링 경로의 이그레스 인터페이스에서 유니캐스트 RPF(**ip verify reverse-path** 명령)를 활성화하지 마십시오. 이 설정 때문에 세션이 실패할 수 있습니다.
- 터널링 경로의 이그레스 인터페이스에서 TCP 인터셉트를 활성화하지 마십시오. 이 설정 때문에 세션이 실패할 수 있습니다.
- VoIP 검사 엔진(CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), DNS 검사 엔진 또는 DCE RPC 검사 엔진을 터널링 경로에 사용하지 마십시오. 이러한 검사 엔진은 터널링 경로를 무시하기 때문입니다.
- tunneled 옵션으로 둘 이상의 기본 경로를 정의할 수 없습니다.
- 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

프로시저

기본 경로를 추가합니다.

IPv4:

route *if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6:

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

예제**:**

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

*if_name*은 특정 트래픽을 전송할 때 통과할 인터페이스입니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스 이름을 지정합니다. 브리지 그룹이 있는 라우팅 모드에서 BVI 이름을 지정합니다.

distance 인수는 경로에 대한 관리 거리로, 1~254 범위의 값입니다. 값을 지정하지 않으면 기본값은 **1**입니다. 관리 영역은 서로 다른 라우팅 프로토콜의 경로를 비교하는 데 사용되는 매개변수입니다. 고정 경로에서 기본 관리 영역은 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다. OSPF가 발견한 경로에 대한 기본 관리 영역은 110입니다. 고정 경로의 관리 영역이 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

참고 메트릭이 서로 다른 인터페이스에서 2개의 기본 경로를 구성한 경우 더 높은 메트릭 인터페이스에서 ASA로의 연결은 실패하지만 낮은 메트릭에서 ASA로의 연결은 예상대로 성공합니다.

tunneled 키워드를 사용하여 VPN 트래픽이 비 VPN 트래픽과 다른 기본 경로를 사용하도록 하기 위해, VPN 트래픽에 대해 별도의 기본 경로를 정의할 수 있습니다. 예를 들어, VPN 연결에서 들어오는 트래픽은 내부 네트워크를 향하도록 쉽게 방향을 정할 수 있는 반면, 내부 네트워크의 트래픽은 외부를 향하도록 방향을 정할 수 있습니다. 터널링 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 ASA에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다.

팁 다음 예에서와 같이 대상 네트워크 주소와 마스크로 **0 0**을 **0.0.0.0 0.0.0.0** 대신 입력할 수 있습니다. 예: **route outside 0 0 192.168.2.4**

고정 경로 구성

고정 경로는 특정 목적지 네트워크로 향하는 트래픽을 어디로 보낼지 정의합니다.

프로시저

고정 경로를 추가합니다.

IPv4:

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6:

ipv6 route *if_name dest_ipv6_prefix*/*prefix_length gateway_ip* [**distance**]

예제**:**

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

*if_name*은 특정 트래픽을 전송할 때 통과할 인터페이스입니다. 원치 않는 트래픽을 "완전히 사라지게 하려면" **null0** 인터페이스를 입력합니다. 투명 모드에서, 브리지 그룹 멤버 인터페이스 이름을 지정합니다. 브리지 그룹이 있는 라우팅 모드에서 BVI 이름을 지정합니다.

dest_ip 및 *mask* 또는 *dest_ipv6_prefix*/*prefix_length* 인수는 대상 네트워크의 IP 주소를 나타내고 *gateway_ip* 인수는 next-hop 라우터의 주소입니다. 사용자가 고정 경로에 대해 지정하는 주소는 ASA를 입력하고 NAT를 수행하기 전에 패킷에 존재하는 주소입니다.

distance 인수는 경로에 대한 관리 거리입니다. 값을 지정하지 않으면 기본값은 **1**입니다. 관리 영역은 서로 다른 라우팅 프로토콜의 경로를 비교하는 데 사용되는 매개변수입니다. 고정 경로에서 기본 관리 영역은 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다. OSPF가 발견한 경로에 대한 기본 관리 영역은 110입니다. 고정 경로의 관리 영역이 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

예

다음 예에서는 동일한 게이트웨이로 향하는 3개 네트워크 및 다른 게이트웨이로 향하는 또 다른 네트워크에 대한 고정 경로를 보여줍니다.

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

고정 경로 추적 구성

고정 경로 추적을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 모니터링 프로세스를 정의합니다.

sla monitor sla_id

예제**:**

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

단계 **2** 모니터링 프로토콜, 추적되는 네트워크의 대상 호스트, 네트워크에 연결할 때 거칠 인터페이스를 지정합니다.

type echo protocol ipicmpecho target_ip **interface** if_name

예제**:**

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134
ciscoasa(config-sla-monitor-echo)#
```

target_ip 인수는 추적 프로세스가 가용성을 모니터링하는 네트워크 객체의 IP 주소입니다. 이 객체를 사용할 수 있을 때 추적 프로세스 경로가 라우팅 테이블에 설치됩니다. 이 객체를 사용할 수 없게 되면 추적 프로세스가 경로를 삭제하고 그 자리에 백업 경로가 대신 사용됩니다.

단계 **3** (선택 사항) 모니터링 옵션을 구성합니다. **frequency, num-packets, request-data-size, threshold, timeout, tos** 명령에 대해서는 명령 참조를 참고하십시오.

단계 **4** 모니터링 프로세스 예약:

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time**{hh:mm [:ss] [month day | day month] | **pending** | **now** | **after**hh:mm:ss}] [**ageout** seconds] [**recurring**]

예제**:**

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

일반적으로 모니터링 예약을 위해 **sla monitor schedule** *sla_id* **life forever start-time now** 명령을 사용하고 모니터링 구성이 테스트 실행 빈도를 결정하도록 허용합니다.

하지만 모니터링 프로세스를 나중에 지정된 시간에만 실행되도록 예약할 수 있습니다.

단계 **5** 추적 고정 경로를 SLA 모니터링 프로세스와 연결:

track track_id **rtr** sla_id **reachability**

예제**:**

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 인수는 이 명령으로 할당하는 추적 번호입니다. *sla_id* 인수는 SLA 프로세스의 ID 번호입니다.

단계 **6** 다음 경로 유형 중 하나를 추적합니다.

- 고정 경로:

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  예:

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  tunneled 옵션은 사용할 수 없습니다.

- DHCP를 통해 얻은 기본 경로:

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- PPPoE를 통해 얻은 기본 경로:

  ```
  interface interface_id
  ```

```
pppoe client route track track_id
ip address pppoe setroute
```

단계 **7** 비추적 백업 경로를 생성합니다.

백업 경로는 추적 경로와 대상은 같지만 다른 인터페이스 또는 게이트웨이를 통하는 경로입니다. 이 경로에는 추적 경로보다 높은 관리 영역(메트릭)을 할당해야 합니다.

고정 또는 기본 경로 모니터링

- **show route**

  라우팅 테이블을 표시합니다.

고정 또는 기본 경로의 예

다음 예는 라우터 10.1.2.45에 10.1.1.0/24가 목적지인 모든 트래픽을 보내는 고정 경로 생성 방법을 보여줍니다. 이 라우터는 내부 인터페이스에 연결되어 있고 트래픽을 DMZ 인터페이스의 3가지 게이트웨이로 안내하는 동일 비용 고정 경로 3개를 정의하며 터널링 트래픽을 위한 기본 경로와 일반 트래픽을 위한 경로 하나를 추가합니다.

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

고정 경로 및 기본 경로 기록

표 ***28:*** 고정 경로 및 기본 경로 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
고정 경로 추적	7.2(1)	고정 경로 추적 기능은 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 보조 경로를 설치하는 수단을 제공합니다. 다음 명령을 도입했습니다. **clear configure sla, frequency, num-packets, request-data-size, show sla monitor, show running-config sla, sla monitor, sla monitor schedule, threshold, timeout, tos, track rtr**
트래픽을 "완전히 사라지게 하기 위한" 고정 null0 경로	9.2(1)	Null0 인터페이스로 트래픽을 보내면 지정된 네트워크로 향하는 패킷이 드롭될 수 있습니다. 이 기능은 BGP를 위한 RTBH(Remotely Triggered Black Hole)를 구성할 때 유용합니다. 다음 명령을 수정했습니다. **route**.

25 장

정책 기반 라우팅

이 장에서는 PBR(정책 기반 라우팅)을 지원하도록 Cisco ASA를 구성하는 방법을 설명합니다. 다음 섹션에서는 PBR에 대한 정책 기반 라우팅, 지침, 및 PBR의 구성을 설명합니다.

정책 기반 라우팅 정보

기존 라우팅은 대상 기반이며 이는 대상 IP 주소를 기반으로 패킷이 라우팅됨을 의미합니다. 그러나 대상 기반 라우팅 시스템에서 특정 트래픽의 라우팅을 변경하기는 어렵습니다. PBR(Policy Based Routing)을 사용하여 대상 네트워크 이외의 기준을 기반으로 라우팅을 정의할 수 있습니다. PBR을 통해 소스 주소, 소스 포트, 대상 주소, 대상 포트, 프로토콜 또는 이들 조합을 기반으로 트래픽을 라우팅할 수 있습니다.

정책 기반 라우팅:

- 구분된 트래픽에 QoS(Quality of Service)를 제공할 수 있습니다.
- 낮은 대역폭, 저비용 영구 경로 및 높은 대역폭, 고비용 전환 경로 전체에서 인터랙티브 및 배치 트래픽을 배포할 수 있습니다.
- 인터넷 서비스 제공자 및 다른 조직에서 제대로 정의된 인터넷 연결을 통해 다양한 유형의 사용자 집합에서 시작되는 트래픽을 라우팅할 수 있습니다.

정책 기반 라우팅은 네트워크 에지에서 트래픽을 분류하고 표시한 다음, 특정 경로를 따라 표시된 트래픽의 경로를 지정하기 위해 네트워크 전체에서 PBR을 사용하여 QoS를 구현할 수 있습니다. 이렇게 하면 대상이 동일한 경우에도 다른 소스에서 시작하는 패킷을 다른 네트워크로 라우팅할 수 있으며 여러 개의 사설 네트워크를 상호 연결할 때 유용할 수 있습니다.

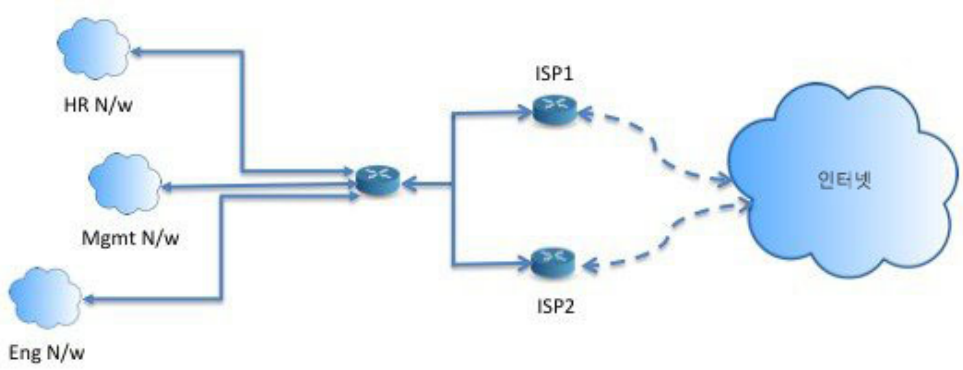
정책 기반 라우팅을 사용하는 이유

지점 간에 두 개의 링크가 있는 회사를 생각해 보십시오. 하나는 대역폭이 높고 지연 비용이 낮은 링크이고 또 다른 하나는 대역폭이 낮고 지연 시간이 길지만 비용이 낮은 링크입니다. 기존의 라우팅 프로토콜을 사용하는 동안에는 링크의 대역폭 및/또는 지연(EIGRP 또는 OSPF 사용) 특성에서 얻은 메트릭 절약을 기반으로 하여 높은 대역폭 링크가 전송 트래픽의 전부는 아니더라도 대부분을 맡습니다. PBR을 활용하면 높은 대역폭/낮은 지연 링크를 통해 우선순위가 높은 트래픽을 라우팅하고 낮은 대역폭/높은 지연 링크를 통해 모든 기타 트래픽을 전송할 수 있습니다.

정책 기반 라우팅의 일부 애플리케이션은 다음과 같습니다.

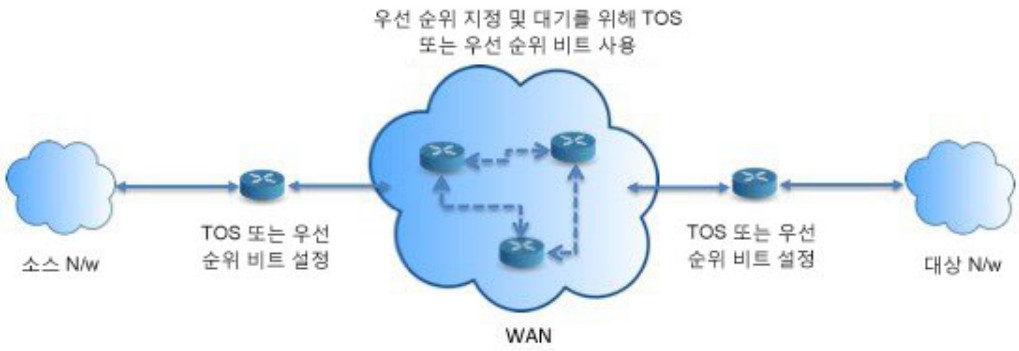
동일 액세스 및 소스를 구분하는 라우팅

이 토폴로지에서 HR 네트워크 및 관리 네트워크의 트래픽은 ISP1을 통해 구성될 수 있으며, Eng 네트워크의 트래픽은 ISP2를 통해 구성될 수 있습니다. 따라서 정책 기반 라우팅은 네트워크 관리자가 여기의 내용과 같이 동일 액세스 및 소스를 구분하는 라우팅을 제공하도록 지원합니다.



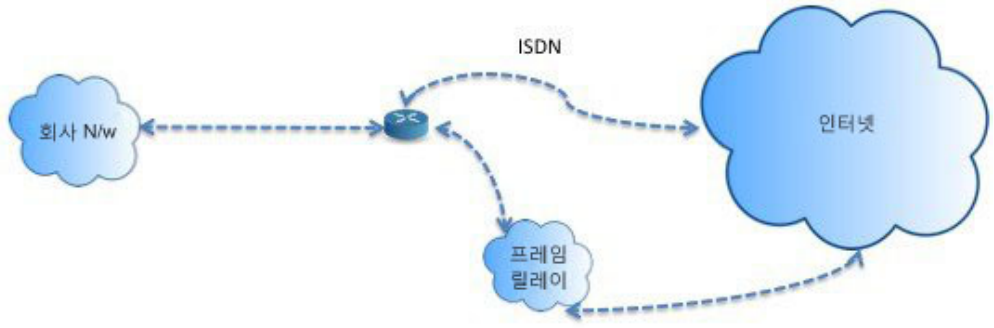
Quality of Service

패킷에 정책 기반 라우팅으로 태그를 지정할 경우, 네트워크 관리자는 다양한 서비스 등급의 네트워크 경계별로 네트워크 트래픽을 분류한 후 우선 순위, 맞춤형 또는 Weighted Fair Queuing을 사용하여 네트워크 코어에 이러한 서비스 등급을 구현할 수 있습니다(아래 그림에 표시된 내용 참조). 이러한 설정은 코어 또는 백본 네트워크의 각 WAN 인터페이스에서 트래픽을 명시적으로 분류할 필요가 없으므로 네트워크 성능을 향상시킵니다.



비용 절감

조직에서는 특정 활동과 관련된 대량 트래픽에서 높은 대역폭의 비용이 많이 드는 링크를 잠시 사용하도록 지시하고 다음과 같이 토폴로지를 정의하여 양방향 트래픽을 위해 낮은 대역폭의 비용이 적게 드는 링크를 통해 기본 연결을 계속 유지합니다.



로드 공유

ECMP 로드 밸런싱에서 제공하는 동적인 로드 공유 기능 외에, 네트워크 관리자는 이제 트래픽 특성에 따라 여러 경로에서 트래픽을 분산시키기 위해 정책을 구현할 수 있습니다.

예를 들어, 동일 액세스 소스 구분 라우팅 시나리오에 설명되어 있는 토폴로지에서 관리자는 ISP1을 통한 HR 네트워크의 트래픽과 ISP2를 통한 Eng 네트워크 트래픽의 로드를 공유하기 위해 정책 기반 라우팅을 구성할 수 있습니다.

PBR구현

ASA는 ACL을 사용하여 트래픽을 일치시킨 다음 이 트래픽에서 라우팅 작업을 수행합니다. 특히, 일치에 대해 ACL을 지정하는 경로 맵을 구성한 다음 해당 트래픽에 대해 하나 이상의 작업을 지정합니다. 마지막으로, 모든 수신 트래픽에 PBR을 적용할 인터페이스에 경로 맵을 연결합니다.

정책 기반 라우팅에 대한 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

플로우당 라우팅

ASA에서 플로우를 기준으로 라우팅을 수행하므로 정책 라우팅은 첫 번째 패킷에서 적용되고 결과 라우팅 의사 결정은 패킷용으로 생성된 플로우에 저장됩니다. 동일한 연결에 속하는 모든 후속 패킷은 간단하게 이 플로우와 일치하고 적절하게 라우팅됩니다.

출력 경로 조회에 적용되지 않는 **PBR** 정책

정책 기반 라우팅은 인그레스 전용 기능입니다. 즉, 새로 수신되는 연결의 첫 번째 패킷에만 적용되며 이때 연결의 전달 레그에 대한 이그레스 인터페이스가 선택됩니다. 수신 패킷이 기존 연결에 속하는 경우 또는 NAT가 적용된 경우, PBR은 트리거되지 않습니다.

클러스터링

- 클러스터링이 지원됩니다.
- 클러스터 시나리오에서 고정 또는 동적 경로 없이 ip-verify-reverse 경로가 활성화된 경우 비대칭 트래픽이 삭제될 수 있습니다. 따라서 ip-verify-reverse 경로를 비활성화하는 것이 좋습니다.

IPv6 지원

IPv6가 지원됩니다.

추가 지침

구성 제한사항 및 한계와 관련된 모든 기존의 경로 맵이 이후에 수행됩니다.

정책 기반 라우팅 구성

경로 맵은 하나 이상의 route-map 구문으로 구성됩니다. 각 문에는 시퀀스 번호와 허용 또는 거부 절이 있습니다. 각 route-map 문에는 match 및 set 명령이 포함됩니다. match 명령은 패킷에서 적용될 일치 기준을 표시합니다. set 명령은 패킷에서 수행될 작업을 표시합니다.

- 경로 맵이 IPv4 및 IPv6 match/set 절로 구성된 경우 또는 통합 ACL 일치 IPv4 및 IPv6 트래픽이 사용되는 경우, set 작업은 대상 IP 버전에 기반하여 적용됩니다.
- 여러 next-hop 또는 인터페이스가 set 작업으로 구성된 경우, 모든 옵션은 사용 가능한 유효한 옵션을 찾을 때까지 하나씩 평가됩니다. 구성된 여러 옵션 중에서 로드 밸런싱은 수행되지 않습니다.
- verify-availability 옵션은 다중 상황 모드에서 지원되지 않습니다.

프로시저

단계 **1** 표준 또는 확장 액세스 목록을 정의합니다.

access-list *name* **standard** {**permit** | **deny**} {**any4** | **host** *ip_address* | *ip_address mask*}

access-list *name* **extended** {**permit** | **deny**} *protocol source_and_destination_arguments*

예제**:**

```
ciscoasa(config)# access-list testacl extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

표준 ACL을 사용하는 경우 대상 주소에서만 일치 작업이 수행됩니다. 확장된 ACL을 사용하는 경우 소스, 대상 또는 둘 다에서 일치 작업을 수행할 수 있습니다.

확장된 ACL의 경우 IPv4, IPv6, ID 방화벽 또는 Cisco TrustSec 파라미터를 지정할 수 있습니다. 전체 구문에 대한 내용은 ASA 명령 참조를 참고하십시오.

단계 **2** 경로 맵 항목을 생성합니다.

route-map *name* {**permit** | **deny**} [*sequence_number*]

예제**:**

```
ciscoasa(config)# route-map testmap permit 12
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 인수를 사용하여 순서를 파악합니다. 그렇게 하지 않으면 ASA에서는 경로 맵 항목을 추가하는 순서를 사용합니다.

또한 ACL은 자체 permit 및 deny 명령문을 포함합니다. 경로 맵과 ACL 간에 Permit/Permit이 일치하는 경우, 정책 기반 라우팅 처리가 계속됩니다. Permit/Deny가 일치하는 경우, 이 경로 맵과 다른 경로 맵에 대한 처리 종료가 선택됩니다. 결과가 여전히 Permit/Deny인 경우, 일반 라우팅 테이블이 사용됩니다. Deny/Deny가 일치하는 경우, 정책 기반 라우팅 처리가 계속됩니다.

참고 경로 맵이 허용 또는 거부 작업을 사용하지 않고 시퀀스 번호 없이 구성된 경우, 기본적으로 이 작업은 허용이며 시퀀스 번호를 10으로 간주합니다.

단계 **3** 적용할 일치 기준을 access-list를 사용하여 정의합니다.

match ip address *access-list_name* [*access-list_name...*]

예제**:**

```
ciscoasa(config-route-map)# match ip address testacl
```

단계 **4** 하나 이상의 set 작업을 구성합니다.

- next hop 주소를 설정합니다.

  set {ip | ipv6} next-hop *ipv4_or_ipv6_address*

  유효한 라우팅 가능한 next-hop IP 주소를 찾을 때까지 지정된 순서대로 평가되는 여러 개의 next-hop IP 주소를 구성할 수 있습니다. 구성된 next-hop에는 직접 연결되어야 합니다. 그렇지 않은 경우 set 작업은 적용되지 않습니다.

- 기본 next hop 주소를 설정합니다.

  set {ip | ipv6} default next-hop *ipv4_or_ipv6_address*

  일반 경로 조회가 트래픽 일치에 대해 실패하는 경우, ASA에서는 지정된 이 next-hop IP 주소를 사용하여 트래픽을 전달합니다.

- 재귀적인 next hop IPv4 주소를 설정합니다.

  set ip next-hop recursive *ip_address*

set ip next-hop 및 **set ip default next-hop** 둘 다 직접 연결된 서브넷에서 next-hop을 찾아야 합니다. **set ip next-hop recursive**를 사용할 경우 next-hop 주소에 직접 연결할 필요가 없습니다. 대신 재귀 조회가 next-hop 주소에서 수행되며 일치하는 트래픽이 라우터에서 사용 중인 라우팅 경로에 따라 경로 항목에서 사용하는 next-hop에 전달됩니다.

- 경로 맵의 next IPv4 hop을 사용할 수 있는지 확인합니다.

  set ip next-hop verify-availability *next-hop-addresssequence number* **track** *object*

  next-hop의 연결성을 확인하기 위해 SLA 모니터 추적 개체를 구성할 수 있습니다. 여러 개의 next-hop의 가용성을 확인하기 위해 여러 **set ip next-hop verify-availability** 명령을 다른 시퀀스 번호 및 다른 추적 개체와 함께 구성할 수 있습니다.

- 패킷의 출력 인터페이스를 설정합니다.

  set interface *interface_name*

  또는

  set interface null0

  이 명령을 사용하면 일치하는 트래픽이 전달되면서 통과하는 인터페이스가 구성됩니다. 유효한 인터페이스를 찾을 때까지 지정된 순서대로 평가되는 여러 개의 인터페이스를 구성할 수 있습니다. **null0**을 지정할 때 경로-맵과 일치하는 모든 트래픽이 삭제됩니다. 지정된 인터페이스(고정 또는 동적)를 통해 라우팅될 수 있는 대상에 대한 경로가 있어야 합니다.

- 기본 인터페이스를 null0으로 설정합니다.

  set default interface null0

  일반 경로 조회가 실패하는 경우 ASA에서는 트래픽 null0을 전달하며, 트래픽은 삭제됩니다.

- IP 헤더에서 DF(Don't Fragment) 비트 값을 설정합니다.

  set ip df {0|1}

- 패킷에서 DSCP(차등 서비스 코드 포인트) 또는 IP 우선순위 값을 설정하여 IP 트래픽을 분류합니다.

  set {ip | ipv6} dscp *new_dscp*

참고 여러 set 작업이 구성된 경우, ASA에서는 작업을 다음 순서대로 평가합니다. **set ip next-hop verify-availability**, **set ip next-hop**, **set ip next-hop recursive**, **set interface**, **set ip default next-hop**, **set default interface.**

단계 **5** 인터페이스를 구성하고 인터페이스 구성 모드를 시작합니다.

interface *interface_id*

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
```

단계 **6** through-the-box 트래픽에 대해 정책 기반 라우팅을 구성합니다.

policy-route route-map *route-map_name*

예제:

```
ciscoasa(config-if)# policy-route route-map testmap
```

기존 정책 기반 라우팅 맵을 제거하려면 이 명령의 **no** 형식을 입력하기만 하면 됩니다.

예제:

```
ciscoasa(config-if)# no policy-route route-map testmap
```

정책 기반 라우팅 예

다음 섹션에는 경로 맵 구성, 정책 기반 라우팅의 예, 작업 중인 PBR의 특정 예가 나와 있습니다.

경로 맵 구성 예

다음 예에서는 작업 및 순서가 지정되어 있지 않으므로 허용에 내포된 작업 및 시퀀스 번호 10을 가정해 보겠습니다.

```
ciscoasa(config)# route-map testmap
```

다음 예에서는 일치 기준이 지정되어 있지 않으므로 내포된 일치 'any'를 가정해 보겠습니다.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

이 예에서는 모든 트래픽 일치 <acl>은 정책이 라우팅되고 외부 인터페이스를 통해 전달됩니다.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
ciscoasa(config-route-map)# set interface outside
```

이 예에서는 인터페이스 또는 next-hop 작업이 구성되지 않았으므로 모든 트래픽 일치 <acl>은 구성에 따라 수정된 df 비트 및 dscp 필드를 지니며 일반 라우팅을 사용하여 전달됩니다.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

다음 예에서 모든 트래픽 일치 <acl_1>은 next hop 1.1.1.10을 사용하여 전달되며, 모든 트래픽 일치 <acl_2>도 next hop 2.1.1.10을 사용하여 전달되며 나머지 트래픽은 드롭됩니다. 어떤 "일치" 기준도 내포된 일치 "any"를 의미하지 않습니다.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

다음 예에서 경로 맵 평가는 (i) route-map 작업 permit 및 acl 작업 permit이 설정 작업에 적용됩니다. (ii) route-map 작업 deny 및 acl 작업 permit이 일반적인 경로 조회로 건너뜁니다. (Iii) permit/deny route-map 작업 및 acl 작업 deny가 다음 경로 맵 항목에 계속해서 작업을 수행합니다. 다음 경로 맵 항목을 사용할 수 없는 경우, 일반 경로 조회를 대신 수행합니다.

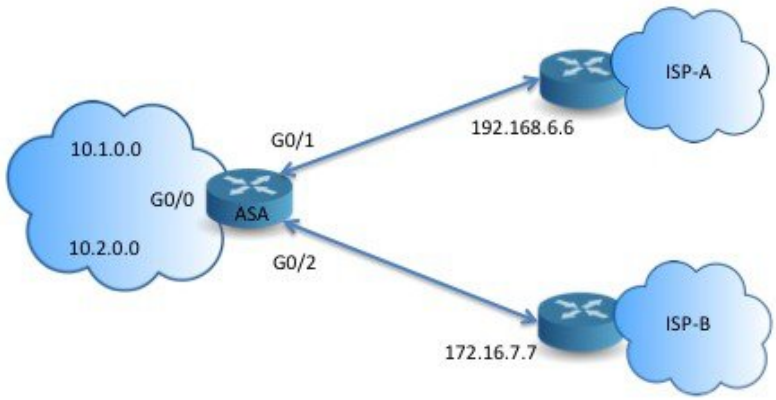
```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
ciscoasa(config-route-map)# set interface outside
```

다음 예에서 여러 설정 작업이 구성된 경우 위에서 언급한 순서대로 평가됩니다. 설정 작업의 모든 옵션이 평가되고 이를 적용할 수 없는 경우에만 다음 설정 작업이 고려됩니다. 이 순서에서는 가장 사용하기 쉽고 가장 가까운 next hop이 처음에 시도된 다음 다음으로 사용하기 쉽고 덜 먼 next hop이 시도되며 이러한 순서로 계속 진행됩니다.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

PBR 구성의 예

이 섹션에서는 다음 시나리오에 대해 PBR을 구성하는 데 필요한 완벽한 구성에 대해 설명합니다.



먼저, 인터페이스를 구성해야 합니다.

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-1
ciscoasa(config-if)# ip address 192.168.6.5 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-2
ciscoasa(config-if)# ip address 172.16.7.6 255.255.255.0
```

그런 다음 트래픽 일치를 위해 access-list를 구성해야 합니다.

```
ciscoasa(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
ciscoasa(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

일치 기준이 필수 설정 작업과 함께 수행되므로 위의 access-list를 지정하여 경로 맵을 구성해야 합니다.

```
ciscoasa(config)# route-map equal-access permit 10
ciscoasa(config-route-map)# match ip address acl-1
ciscoasa(config-route-map)# set ip next-hop 192.168.6.6

ciscoasa(config)# route-map equal-access permit 20
ciscoasa(config-route-map)# match ip address acl-2
ciscoasa(config-route-map)# set ip next-hop 172.16.7.7

ciscoasa(config)# route-map equal-access permit 30
ciscoasa(config-route-map)# set ip interface Null0
```

이제, 이 경로 맵은 인터페이스에 연결되어야 합니다.

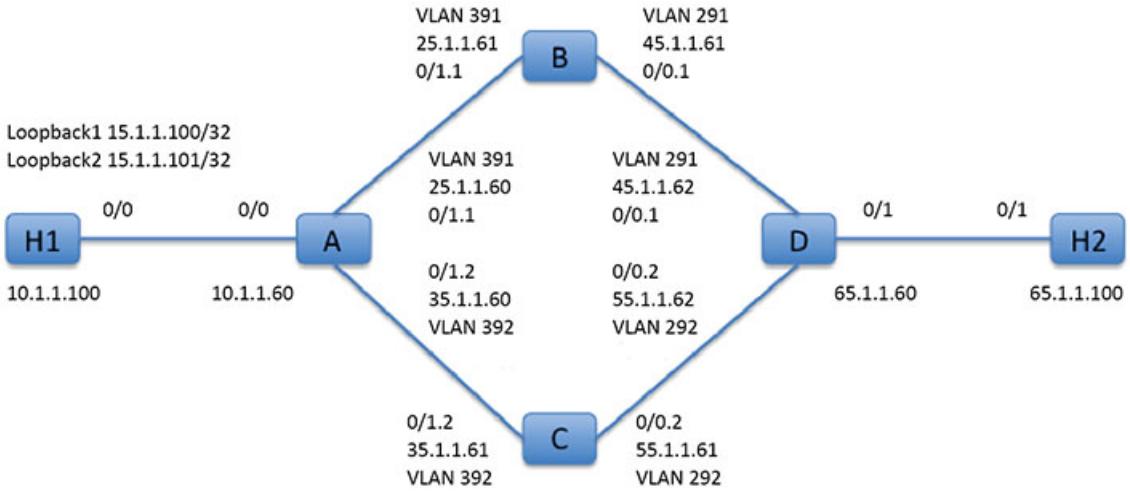
```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map equal-access
```

정책 라우팅 구성을 표시합니다.

```
ciscoasa(config)# show policy-route
Interface                  Route map
GigabitEthernet0/0   equal-access
```

정책 기반 라우팅 작업

이 테스트 설정을 사용하여 다양한 일치 기준 및 set 작업을 지닌 정책 기반 라우팅을 구성해 이러한 라우팅이 평가 및 적용되는 방식을 확인해보겠습니다.



먼저, 설정과 관련된 모든 디바이스에 대한 기본 구성부터 시작해보겠습니다. 여기서 A, B, C 및 D는 ASA 디바이스를 나타내고 H1 및 H2는 IOS 라우터를 나타냅니다.

ASA-A:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
```

```
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
```

```
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1:

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255

ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.60
```

H2:

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

H1에서 오는 트래픽을 라우팅하기 위해 ASA-A에 PBR을 구성하십시오.

ASA-A:

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap

ciscoasa(config-if)# debug policy-route
```

H1: ping 65.1.1.100 repeat 1 source loopback1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1 sub_proto
 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

패킷은 경로 맵의 next hop 주소를 사용하여 예상대로 전달됩니다.

next hop을 구성할 때, 즉 입력 라우트 테이블에서 조회를 수행하여 구성된 next hop에 연결된 경로를 식별하고 해당하는 인터페이스를 사용합니다. 이 예의 입력 경로 테이블은 다음과 같습니다(일치 경로 항목이 강조 표시되어 있음).

```
in   255.255.255.255 255.255.255.255 identity
in   10.1.1.60       255.255.255.255 identity
in   25.1.1.60       255.255.255.255 identity
in   35.1.1.60       255.255.255.255 identity
in   10.127.46.17    255.255.255.255 identity
```

```
in   10.1.1.0        255.255.255.0   inside
in   25.1.1.0        255.255.255.0   outside
in   35.1.1.0        255.255.255.0   dmz
```

다음으로, ASA-A dmz 인터페이스 외부로 H1 loopback2의 패킷을 라우팅하기 위해 ASA-A를 구성해 보겠습니다.

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl_2
  set ip next-hop 35.1.1.61
!
```

H1: ping 65.1.1.100 repeat 1 source loopback2

디버그는 다음과 같습니다.

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6 sub_proto
 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

입력 경로 테이블에서 선택한 경로 항목은 다음과 같습니다.

```
in   255.255.255.255 255.255.255.255 identity
 in   10.1.1.60       255.255.255.255 identity
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   10.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

정책 기반 라우팅 내역

표 ***29:*** 경로 맵 내역

기능 이름	플랫폼 릴리스	기능 정보
정책 기반 라우팅	9.4(1)	PBR(정책 기반 라우팅)은 ACL을 사용하여 지정된 QoS가 있는 특정 경로를 통해 라우팅되는 메커니즘입니다. ACL은 트래픽을 패킷의 Layer 3 및 Layer 4 헤더의 콘텐츠를 기준으로 분류합니다. 이 솔루션을 사용하면 관리자가 차별화된 트래픽에 QoS를 제공하고 낮은 대역폭, 낮은 비용의 영구 경로 및 높은 대역폭, 높은 비용의 전환된 경로 사이에서 상호 작용 및 배치 트래픽을 분배할 수 있으며 인터넷 서비스 공급자와 다른 조직이 제대로 정의된 인터넷 연결을 통해 다양한 사용자 집합에서 시작되는 트래픽을 라우팅할 수 있습니다. 도입된 명령: **set ip next-hop verify-availability**, **set ip next-hop**, **set ip next-hop recursive**, **set interface**, **set ip default next-hop, set default interface**, **set ip df**, **set ip dscp**, **policy-route route-map**, **show policy-route**, **debug policy-route**
정책 기반 라우팅에 대한 IPv6 지원	9.5(1)	이제 IPv6 주소가 정책 기반 라우팅에 대해 지원됩니다. 도입된 명령: **set ipv6 next-hop**,**set default ipv6-next hop**, **set ipv6 dscp**
정책 기반 라우팅에 대한 VXLAN 지원	9.5(1)	이제 VNI 인터페이스에서 정책 기반 라우팅을 활성화할 수 있습니다. 명령은 수정하지 않았습니다.
Identity Firewall 및 Cisco Trustsec에 대한 정책 기반 라우팅 지원	9.5(1)	Identity Firewall 및 Cisco TrustSec을 구성한 다음 정책 기반 라우팅 경로 맵에서 Identity Firewall 및 Cisco TrustSec ACL을 사용할 수 있습니다. 명령은 수정하지 않았습니다.

26 장

경로 맵

이 장에서는 Cisco ASA에서 경로 맵을 구성 및 사용자 지정하는 방법을 설명합니다.

경로 맵 정보

경로 맵은 경로를 OSPF, RIP, EIGRP 또는 BGP 라우팅 프로세스로 재배포할 때 사용됩니다. 또한 OSPF 라우팅 프로세스로 기본 경로를 생성할 때도 사용됩니다. 경로 맵은 지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 정의합니다.

경로 맵은 널리 알려진 ACL과 여러 기능을 공유합니다. 다음은 두 가지에서 모두 일반적인 특성입니다.

- 이들은 순서가 정해진 개별 구문이며 각각 허용 또는 거부라는 결과를 갖습니다. ACL 또는 경로 맵의 평가는 사전 정의된 순서에 따른 목록 스캔과 그에 일치하는 각 구문의 기준에 대한 평가로 구성됩니다. 목록 스캔은 첫 번째 구문 일치가 발견되고 해당 구문 일치와 연결된 작업이 수행되면 중단됩니다.
- 이들은 일반 메커니즘입니다. 기준 일치와 일치 해석은 적용되는 방식과 이를 사용하는 기능에 따라 정해집니다. 같은 경로 맵이라도 다른 기능에 적용되면 다르게 해석될 수 있습니다.

다음은 경로 맵과 ACL의 차이점입니다.

- 경로 맵은 ACL보다 유연하며 ACL이 확인할 수 없는 기준으로 경로를 확인할 수 있습니다. 예를 들어 경로 맵은 경로 유형이 내부인지 확인할 수 있습니다.
- 각 ACL은 설계 관행에 따라 암시적 거부 문구로 종료됩니다. 일치 시도 중에 경로 맵의 끝에 도달하는 경우 결과는 경로 맵의 애플리케이션이 무엇인지에 따라 달라집니다. 재배포에 적용되

는 경로 맵은 ACL과 동일하게 작동합니다. 경로가 경로 맵의 조항과 일치하지 않으면 마치 경로 맵이 끝에 거부 구문을 포함한 것처럼 경로 재배포가 거부됩니다.

허용 및 거부 절

경로 맵은 허용 및 거부 절을 가질 수 있습니다. 거부 절은 재배포에서 경로 일치를 거부합니다. 경로 맵의 일치 기준으로 ACL을 사용할 수 있습니다. ACL에도 허용 및 거부 절이 있으므로 패킷이 ACL과 일치하는 경우 다음 규칙이 적용됩니다.

- ACL 허용 + 경로 맵 허용: 경로가 재배포됩니다.
- ACL 허용 + 경로 맵 거부: 경로가 재배포되지 않습니다.
- ACL 거부 + 경로 맵 허용 또는 거부: 경로 맵 절이 일치하지 않으며 다음 경로 맵 절이 평가됩니다.

절의 일치 및 설정 값

각 경로 맵 절은 두 가지 값을 갖습니다.

- 일치 값은 이 절을 적용할 경로를 선택합니다.
- 설정 값은 대상 프로토콜로 재배포될 정보를 수정합니다.

재배포되는 각 경로에 대해 라우터는 먼저 경로 맵에 있는 절의 일치 기준을 평가합니다. 일치 기준이 성공하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부되고 set 명령에서 설정된 값으로 일부 속성이 수정될 수 있습니다. 일치 기준이 실패하면 이 절은 경로에 적용되지 않고 소프트웨어가 경로 맵의 다음 절에 대해 경로를 평가합니다. 절이 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 스캔이 계속됩니다.

다음 조건 중 하나가 존재할 경우 각 절의 일치 또는 설정 값은 누락되거나 여러 번 반복될 수 있습니다.

- 절에 여러 match 항목이 존재하는 경우 주어진 경로에 대해 모두 성공해야 경로가 절에 일치할 수 있습니다(논리 AND 알고리즘이 여러 일치 명령에 적용됨).
- match 항목이 하나의 항목에서 여러 개체를 참조하는 경우 둘 중 하나가 일치해야 합니다(논리 OR 알고리즘 적용).
- match 항목이 존재하지 않으면 모든 경로가 절과 일치합니다.
- set 항목이 경로 맵 허용 절에 없는 경우 현재 속성의 수정 없이 경로가 재배포됩니다.

참고 경로 맵의 set 항목이 절을 거부하도록 구성하지 마십시오. 거부 절은 경로 재배포를 금지하므로 수정할 정보가 없기 때문입니다.

match 또는 set 항목이 없는 경로 맵 절이 작업을 수행합니다. 빈 허용 절은 수정 없이 남은 경로의 재배포를 허용합니다. 빈 거부 절은 다른 경로의 재배포를 허용하지 않습니다(경로 맵을 완전히 스캔했으나 정확한 match 항목을 찾지 못한 경우 이것이 기본 작업).

경로 맵에 대한 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

추가 지침

경로 맵은 사용자, 사용자 그룹 또는 정규화된 도메인 이름 객체를 포함하는 ACL을 지원하지 않습니다.

경로 맵 정의

지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 지정할 때 경로 맵을 정의해야 합니다.

프로시저

경로 맵 엔트리 생성:

route-map *name* {**permit** | **deny**} [*sequence_number*]

예제**:**

```
ciscoasa(config)# route-map name {permit} [12]
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 인수를 사용하여 순서를 파악합니다. 그러지 않으면 ASA에서는 경로 맵 항목을 추가하는 순서를 사용합니다.

경로 맵 사용자 지정

이 섹션은 경로 맵을 사용자 정의하는 방법을 설명합니다.

특정 대상 주소와 일치하도록 경로 정의

프로시저

단계 **1** 경로 맵 엔트리 생성:

route-map *name* {**permit** | **deny**} [*sequence_number*]

예제**:**

```
ciscoasa(config)# route-map name {permit} [12]
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 옵션을 사용하여 순서를 파악합니다. 그렇게 하지 않으면 ASA에서 경로 맵 항목을 추가하는 순서를 사용합니다.

단계 **2** 표준 ACL 또는 접두사 목록과 일치하는 목적지 네트워크를 가진 모든 경로와 일치:

match ip address *acl_id* [*acl_id*] [...] [prefix-list]

예제**:**

```
ciscoasa(config-route-map)# match ip address acl1
```

ACL을 하나 이상 지정한 경우 경로가 모든 ACL과 일치할 수 있습니다.

단계 **3** 지정된 메트릭을 가진 경로와 일치:

match metric *metric_value*

예제**:**

```
ciscoasa(config-route-map)# match metric 200
```

*metric_value*의 범위는 0 ~ 4294967295입니다.

단계 **4** 표준 ACL과 일치하는 다음 홉 라우터 주소를 가진 경로와 일치:

match ip next-hop *acl_id* [*acl_id*] [...]

예제**:**

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

ACL을 하나 이상 지정한 경우 경로가 모든 ACL과 일치할 수 있습니다.

단계 **5** 지정된 다음 홉 인터페이스를 가진 모든 경로와 일치:

match interface *if_name*

예제**:**

```
ciscoasa(config-route-map)# match interface if_name
```

하나 이상의 인터페이스를 지정하는 경우 경로가 아무 인터페이스나 일치할 수 있습니다.

단계 **6** 표준 ACL과 일치하는 라우터가 알린 경로와 일치:

match ip route-source *acl_id* [*acl_id*] [...]

예제**:**

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

ACL을 하나 이상 지정한 경우 경로가 모든 ACL과 일치할 수 있습니다.

단계 **7** 경로 유형과 일치:

match route-type {**internal** | **external** [**type-1** | **type-2**]}

경로 작업에 대한 메트릭 값 구성

경로가 **match** 명령과 일치하는 경우 다음 **set** 명령이 재배포 전에 경로에서 수행할 작업을 결정합니다.

경로 작업에 대한 메트릭 값을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 경로 맵 엔트리 생성:

route-map *name* {**permit** | **deny**} [*sequence_number*]

예제**:**

```
ciscoasa(config)# route-map name {permit} [12]
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 인수를 사용하여 순서를 파악합니다. 그러지 않으면 ASA에서는 경로 맵 항목을 추가하는 순서를 사용합니다.

단계 **2** 경로 맵에 대한 메트릭 값 설정:

set metric *metric_value*

예제**:**

```
ciscoasa(config-route-map)# set metric 200
```

metric_value 인수의 범위는 0 ~ 294967295입니다.

단계 **3** 경로 맵에 대한 메트릭 유형 설정:

set metric-type {**type-1** | **type-2**}

예제**:**

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 인수는 type-1 또는 type-2가 될 수 있습니다.

경로 맵의 예

다음 예는 홉 개수가 1과 같은 경로를 OSPF로 재배포하는 방법을 보여줍니다.

ASA에서는 이러한 경로를 메트릭이 5이고 메트릭 유형이 Type 1인 외부 LSA로서 재배포합니다.

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

다음 예는 10.1.1.0 고정 경로를 다음의 구성된 메트릭 값의 eigrp 프로세스 1로 재배포하는 방법을 설명합니다.

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

경로 맵 내역

표 ***30:*** 경로 맵의 기록

기능 이름	플랫폼 릴리스	기능 정보
경로 맵	7.0(1)	이 기능을 도입했습니다. 다음 명령을 도입했습니다. **route-map**.
고정 및 동적 경로 맵에 대한 지원 개선	8.0(2)	동적 및 고정 경로 맵에 대한 향상된 지원이 추가되었습니다.

기능 이름	플랫폼 릴리스	기능 정보
동적 라우팅 프로토콜(EIGRP, OSPF 및 RIP)에 대한 스테이트풀 장애 조치 지원, 일반 라우팅 관련 작업 디버깅	8.4(1)	다음 명령을 도입했습니다. **debug route**, **show debug route**. 다음 명령을 수정했습니다. **show route**.
다중 상황 모드의 동적 라우팅	9.0(1)	경로 맵은 다중 상황 모드에서 지원됩니다.
BGP 지원	9.2(1)	이 기능을 도입했습니다. 다음 명령을 도입했습니다. **router bgp**
접두사 규칙에 대한 IPv6 지원	9.3(2)	이 기능을 도입했습니다.

27 장

Bidirectional Forwarding Detection 라우팅

이 장에서는 BFD(Bidirectional Forwarding Detection) 라우팅 프로토콜을 사용하여 ASA를 구성하는 방법을 설명합니다.

BFD 라우팅 정보

BFD는 모든 미디어 유형, 캡슐화, 토폴로지, 라우팅 프로토콜 등을 위해 신속한 전달 경로 장애 탐지 시간을 제공하기 위해 만들어진 탐지 프로토콜입니다. BFD는 두 시스템 간에 전달되는 모든 데이터 프로토콜 상의 유니캐스트, 포인트 투 포인트 모드에서 작동합니다. 미디어 및 네트워크에 적절한 캡슐화 프로토콜의 페이로드로 패킷이 전달됩니다.

BFD는 빠른 전달 경로 장애 탐지 이외에도 네트워크 관리자를 위한 일관성 있는 장애 탐지 방법을 제공합니다. 네트워크 관리자는 BFD를 사용하여 전달 경로 장애를 다른 라우팅 프로토콜 Hello 메커니즘에 대한 가변 속도가 아닌 균일한 속도로 탐지할 수 있기 때문에 네트워크 프로파일링 및 계획이 더 쉽고 재통합 시간이 일관되며 예측 가능합니다.

BFD 비동기 모드 및 에코 기능

BFD는 에코 기능의 활성화 여부와 관계없이 비동기 모드에서 작동될 수 있습니다.

비동기 모드

비동기 모드에서 시스템은 BFD 제어 패킷을 다른 패킷에 주기적으로 전송하며, 계속해서 해당 패킷의 수가 다른 시스템에서 수신되지 않으면 세션이 작동 중단된 것으로 선언됩니다. 순수 비동기 모드(에코 기능 사용 안 함)는 에코 기능에 필요한 특정 탐지 시간을 달성하는 데 패킷의 절반을 필요로 하기 때문에 유용합니다.

BFD 에코 기능

BFD 에코 기능은 전달 엔진에서 직접 연결된 단일 홉 BFD 네이버로 에코 패킷을 전송합니다. 에코 패킷은 전달 엔진에 의해 전송되고 탐지를 수행하기 위해 동일한 경로를 따라 다시 전달됩니다. 다른 쪽 끝에 있는 BFD 세션은 에코 패킷의 실제 전달에는 참여하지 않습니다. 에코 기능 및 전달 엔진이 탐지 프로세스를 담당하므로 BFD 네이버 간에 전송되는 BFD 제어 패킷의 수는 줄어듭니다. 또한 전달 엔진이 원격 네이터 시스템에서 원격 시스템과 관계없이 전달 경로를 테스트하므로 패킷 간 지연 분산이 개선됩니다. 이로 인해 장애 탐지가 더 신속하게 수행됩니다.

에코 기능을 활성화하면 BFD가 비동기 세션의 속도를 느리게 하고 BFD 네이버 간에 전송되는 BFD 제어 패킷의 수를 줄이기 위해 느린 타이머를 사용할 수 있어 더 빠른 장애 탐지를 제공하면서 동시에 처리 오버헤드를 줄여줍니다.

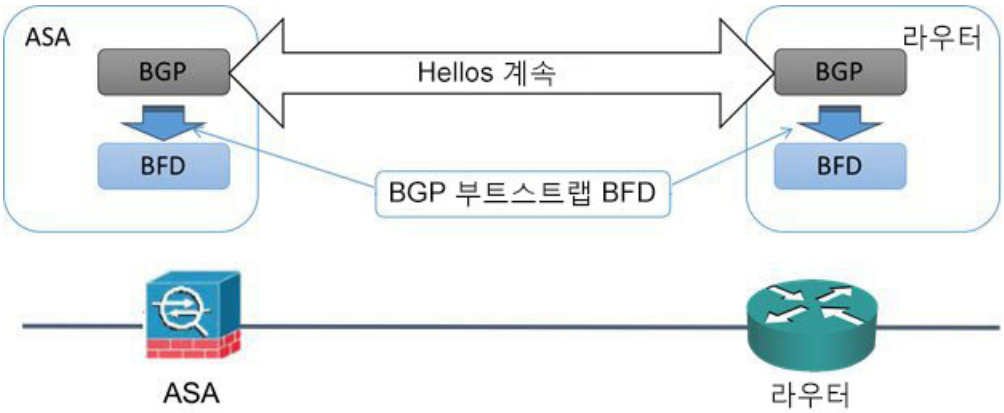
참고 에코 기능은 IPv4 멀티 홉 또는 IPv6 단일 홉 BFD 네이버에 대해서는 지원되지 않습니다.

인터페이스 및 라우팅 프로토콜 수준에서 BFD를 활성화할 수 있습니다. 두 시스템(BFD 피어)에서 BFD를 구성해야 합니다. 인터페이스와 적절한 라우팅 프로토콜에 대한 라우터 수준에서 BFD를 활성화하면, BFD 세션이 생성되고 BFD 타이머가 협상 대상이 되고 BFD 피어가 협상된 수준에서 서로 BFD 제어 패킷 전송을 시작합니다.

BFD 세션 설정

다음 예에는 BGP(Border Gateway Protocol)를 실행하는 네이버 라우터와 ASA가 나와 있습니다. 두 디바이스가 작동 중일 때는 두 디바이스 간에 BFD 세션이 설정되지 않습니다.

그림 *60:* 설정된 ***BFD*** 세션



BGP가 BGP 네이버를 식별한 후에는 네이버의 IP 주소를 사용하여 BFD 프로세스에서 부트스트랩을 수행합니다. BFD는 피어를 동적으로 검색하지 않습니다. BFD는 어떤 IP 주소를 사용하고 어떤 피어 관계를 구성할지 알려주기 위해 구성된 라우팅 프로토콜을 활용합니다.

라우터의 BFD 및 ASA의 BFD는 BFD 제어 패킷을 형성하고 BFD 세션이 설정될 때까지 1초 간격으로 서로에게 패킷을 전송하기 시작합니다. 두 시스템의 초기 제어 패킷은 매우 유사합니다. 예를 들어, Vers, Diag, H, D, P, 및 F비트는 모두 0으로 설정되고 상태는 Down(작동 중단)으로 설정됩니다. My

Discriminator(내 판별자) 필드는 전송 중인 디바이스에서 고유한 값으로 설정됩니다. BFD 세션이 아직 설정되지 않았으므로 Your Discriminator(사용자의 판별자) 필드는 0으로 설정됩니다. TX 및 RX 타이머는 디바이스의 구성에서 발견한 값으로 설정됩니다.

원격 BFD 디바이스는 세션 시작 단계에서 BFD 제어 패킷을 수신한 후 My Discriminator(내 판별자) 필드의 값을 Your Discriminator(사용자의 판별자) 필드에 복사하고 Down(작동 중단) 상태를 초기 상태로 전환하여 최종적으로 Up(작동) 상태가 발생합니다. 두 시스템이 서로의 제어 패킷에서 고유한 판별자를 확인하면 세션이 공식적으로 설정됩니다.

다음 그림에는 설정된 BFD 연결이 나와 있습니다.

그림 ***61: BFD*** 세션이 설정되지 않은 ***BGP***

BFD 타이머 협상

BFD 디바이스는 BFD 제어 패킷의 전송 속도를 동기화하고 제어하기 위해 BFD 타이머와 협상해야 합니다. 디바이스는 BFD 타이머와 협상하기 위해 다음 사항을 먼저 확인해야 합니다.

- 해당 피어 디바이스에서 로컬 디바이스의 제안된 타이머를 포함하는 패킷을 확인했는지 여부
- 피어가 BFD 제어 패킷을 수신하도록 구성된 속도보다 더 빠르게 BFD 제어 패킷을 전송하지 않는지 여부
- 피어가 로컬 시스템이 BFD 제어 패킷을 수신하도록 구성된 속도보다 더 빠르게 BFD 제어 패킷을 전송하지 않는지 여부

Your Discriminator(사용자의 판별자) 필드 설정과 H비트를 설정하면 원격 디바이스가 초기 타이머 교환 중에 패킷을 확인했는지 로컬 디바이스에서 충분히 허용됩니다. BFD 제어 패킷을 수신한 후에 각 시스템은 필요한 최소 RX 간격을 취하여 이를 고유한 필요 최소 TX 간격과 비교한 다음 두 값 중에서 더 큰(느림) 값을 취하고 BFD 패킷에 대한 전송 속도로 사용합니다. 두 시스템 중에서 더 느린 시스템이 전송 속도를 결정합니다.

이러한 타이머가 협상된 경우, 타이머는 세션 재설정을 야기하지 않고도 세션 중에 언제든지 재협상될 수 있습니다. 타이머를 변경하는 디바이스는 원격 시스템에서 F비트가 설정된 BFD 제어 패킷을 수신할 때까지 모든 후속 BFD 제어 패킷에서 P비트를 설정합니다. 이 비트 교환은 전송 중에 손실될 수 있는 패킷을 보호합니다.

참고 원격 시스템에서 F비트를 설정한다고 해서 새로 제안된 타이머를 허용하는 것은 아닙니다. 이는 원격 시스템에서 타이머가 변경된 패킷을 확인했음을 나타냅니다.

BFD 실패 탐지

BFD 세션 및 타이머가 협상된 경우, BFD 피어는 협상된 간격으로 서로에게 BFD 제어 패킷을 전송합니다. 이러한 제어 패킷은 속도가 더 가속화된 것을 제외하고 IGP Hello 프로토콜과 매우 유사한 하트비트 역할을 합니다.

각 BFD 피어가 구성된 탐지 간격(필요한 최소 RX 간격) 내에서 BFD 제어 패킷을 수신하는 경우에 한해 BFD 세션은 가동 상태를 유지하고 BFD와 연결된 모든 라우팅 프로토콜은 인접성을 유지합니다. BFD 피어가 이 간격 내에서 제어 패킷을 수신하지 않는 경우, BFD 세션에 참여 중인 모든 클라이언트에 장애에 대해 알립니다. 라우팅 프로토콜은 정보에 대한 적절한 응답을 결정합니다. 일반적인 응답은 라우팅 프로토콜 피어링 세션을 종료하고 재통합하여 실패한 피어를 우회하기 위한 것입니다.

BFD 피어가 BFD 세션에서 BFD 제어 패킷을 성공적으로 수신할 때마다 해당 세션에 대한 탐지 타이머가 0으로 재설정됩니다. 따라서 장애 탐지는 수신자가 마지막으로 패킷을 전송했을 때가 아니라 수신된 패킷에 따라 달라집니다.

BFD 구축 시나리오

다음은 BFD가 이러한 특정 시나리오에서 작동하는 방법을 설명합니다.

페일오버

장애 조치 시나리오에서 BFD 세션은 액티브 유닛과 네이버 유닛 사이에서 설정되고 유지 관리됩니다. 스탠바이 유닛은 네이버와 함께 BFD 세션을 유지 관리하지 않습니다. 세션 정보가 액티브 유닛과 스탠바이 유닛 사이에서 동기화되지 않기 때문에 장애 조치가 발생하면 새 액티브 유닛은 네이버와 함께 세션 설정을 시작해야 합니다.

정상적인 재시작/NSF 시나리오의 경우, 클라이언트(BGP IPv4/IPv6)는 이벤트에 대해 네이버에게 알릴 책임이 있습니다. 네이버가 정보를 수신하는 경우, 장애 조치가 완료될 때까지 RIB 테이블을 유지합니다. 장애 조치 동안 BFD 및 BGP 세션은 디바이스에서 중단됩니다. 장애 조치가 완료되면 BGP 세션이 시작될 때 네이버 간에 새 BFD 세션이 설정됩니다.

Spanned EtherChannel 및 **L2** 클러스터

Spanned EtherChannel 클러스터 시나리오에서 BFD 세션은 기본 유닛과 해당 네이버 사이에서 설정되고 유지 관리됩니다. 종속 유닛은 네이버와 함께 BFD 세션을 유지 관리하지 않습니다. 스위치에서의 로드 밸런싱 때문에 BFD 패킷이 종속 유닛에 라우팅된 경우, 종속 유닛은 클러스터 링크를 통해 이 패킷을 기본 유닛에 전달해야 합니다. 클러스터 전환이 발생할 경우, 세션 정보가 기본 유닛과 종속 유닛 사이에서 동기화되지 않기 때문에 새 기본 유닛은 네이버와 함께 세션 설정을 시작해야 합니다.

개별 인터페이스 모드 및 **L3** 클러스터

개별 인터페이스 모드 클러스터 시나리오에서는 개별 유닛이 네이버와 함께 해당 BFD 세션을 유지 관리합니다.

BFD 라우팅에 대한 지침

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원됩니다.

방화벽 모드 지침

라우팅 방화벽 모드에서 지원되며 독립형, 장애 조치 및 클러스터 모드에 대해 지원합니다. BFD는 장애 조치 및 클러스터 인터페이스에서 지원되지 않습니다. 클러스터링에서 이 기능은 기본 유닛에서만 지원됩니다. 투명 모드에서는 BFD가 지원되지 않습니다.

IPv6 지침

에코 모드는 IPv6에 대해 지원되지 않습니다.

추가 지침

BGP IPv4 및 BGP IPv6 프로토콜이 지원됩니다.

OSPFv2, OSPFv3, IS-IS 및 EiGRP 프로토콜은 지원되지 않습니다.

고정 경로에 대한 BFD는 지원되지 않습니다.

전송 및 터널에서의 BFD는 지원되지 않습니다.

BFD 구성

이 섹션에서는 시스템에서 BFD 라우팅 프로세스를 활성화하고 구성하는 방법을 설명합니다.

프로시저

단계 **1** BFD 템플릿 생성, 850 페이지.
단계 **2** BFD 인터페이스 구성, 851 페이지.
단계 **3** BFD 맵 구성, 853 페이지.

BFD 템플릿 생성

이 섹션에서는 BFD 템플릿을 생성하고 BFD 구성 모드로 들어가는 데 필요한 단계를 설명합니다.

BFD 템플릿은 BFD 간격 값의 집합을 지정합니다. BFD 템플릿에 구성된 BFD 간격 값은 단일 인터페이스에 한정되지 않습니다. 단일 홉 및 멀티 홉 세션에 대한 인증을 구성할 수도 있습니다. 단일 홉에서만 에코를 활성화할 수 있습니다.

프로시저

단계 **1** 단일 홉 또는 멀티 홉 중 하나로 BFD 템플릿을 생성하여 ASA에서 라우팅 프로토콜로 BFD를 활성화합니다.

bfd-template [single-hop | multi-hop] *template_name*

예제**:**

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)#
```

- **single-hop**— 단일 홉 BFD 템플릿을 지정합니다.
- **multi-hop**— 멀티 홉 BFD 템플릿을 지정합니다.
- *template-name* — 템플릿 이름을 지정합니다. 템플릿 이름에는 공백을 포함할 수 없습니다.

bfd-template 명령을 사용하면 BFD 템플릿을 생성하고 BFD 구성 모드로 들어갈 수 있습니다.

단계 **2** (선택 사항) 단일 홉 BFD 템플릿에서 에코를 구성합니다.

bfd-template single-hop *template_name*

예제**:**

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa (config-bfd)# echo
```

단일 홉 템플릿에서만 에코 모드를 활성화할 수 있습니다. BFD 에코는 IPv6 BFD 세션에서는 지원되지 않습니다.

단계 **3** BFD 템플릿에서 간격을 구성합니다.

interval [**both** *milliseconds* | **microseconds {both | min-tx}** *microseconds* | **min-tx** *milliseconds*

예제**:**

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# interval both 50
```

- **both**— 최소 전송 및 수신 간격 기능입니다.
- *milliseconds* — 밀리초 단위의 간격입니다. 범위는 50~999입니다.

- **microseconds** — **both** 및 **min-tx**에 대한 밀리초 단위의 BFD 간격을 지정합니다.
- *microseconds* — 범위는 50,000~999,000입니다.
- **min-tx**— 최소 전송 간격 기능입니다.

BFD 템플릿의 일부로 지정된 BFD 간격 값은 단일 인터페이스에 한정되지 않습니다. 인터페이스별로 개별 BFD 템플릿을 적용할 수 있습니다. BFD 인터페이스 구성, 851 페이지을 참조하십시오.

단계 **4** BFD 템플릿에서 인증을 구성합니다.

authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1} [0|8] *word* **key-id** *id*

예제**:**

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

- **authentication**— 인증 유형을 지정합니다.
- **md5**— MD5(Message Digest 5) 인증입니다.
- **meticulous-md5**— 정확한 키 입력 MD5 인증입니다.
- **meticulous-sha-1**— 정확한 키 입력 SHA-1 인증입니다.
- **sha-1**— 키 입력 SHA-1 인증입니다.
- **0|8**— 0은 암호화되지 않은 비밀번호가 뒤따르도록 지정합니다. — 8은 암호화된 비밀번호가 뒤따르도록 지정합니다.
- *word* — BFD 비밀번호(키)는 최대 29자의 한 자릿수 비밀번호/키입니다. 숫자로 시작되고 뒤에 공백이 오는 비밀번호는 지원되지 않습니다. 예를 들어, '0 pass' 및 '1'은 유효하지 않습니다.
- **key-id**— 인증 키 ID입니다.
- *id* — 키 문자열과 일치하는 공유 키 ID입니다. 범위는 0~255자입니다.

단일 홉 및 멀티 홉 템플릿에서 인증을 구성할 수 있습니다. 보안을 강화하기 위해 인증을 구성하는 것이 좋습니다. 각 BFD 소스-대상 쌍에서 인증을 구성해야 하며 인증 파라미터는 두 디바이스에서 일치해야 합니다.

BFD 인터페이스 구성

BFD 템플릿을 인터페이스에 바인딩하고 인터페이스별로 베이스라인 BFD 세션 파라미터를 구성하며 인터페이스별로 에코 모드를 활성화할 수 있습니다.

프로시저

단계 **1** 인터페이스 구성 모드로 들어갑니다.

interface *interface_id*

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#
```

단계 **2** BFD 템플릿을 인터페이스에 적용합니다.

bfd template *template-name*

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# bfd template TEMPLATE1
```

bfd-template 명령을 사용하여 템플릿을 생성하지 않은 경우에도 인터페이스 아래에서 템플릿의 이름을 구성할 수 있지만, 템플릿을 정의할 때까지는 템플릿이 유효하지 않은 것으로 간주됩니다. 템플릿 이름을 다시 구성할 필요는 없습니다. 자동으로 유효한 상태가 됩니다.

단계 **3** BFD 세션 파라미터를 구성합니다.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-router)# bfd interval 200 min_rx 200 multiplier 3
```

- **interval** *milliseconds* — BFD 제어 패킷이 BFD 피어로 전송되는 속도를 지정합니다. 범위는 50~999밀리초입니다.
- **min_rx** *milliseconds* — BFD 제어 패킷이 BFD 피어에서 수신될 것으로 예상되는 속도를 지정합니다. 범위는 50~ 999밀리초입니다.
- **multiplier** *multiplier-value* — BFD가 피어를 사용할 수 없는 것으로 선언하고 Layer 3 BFD 피어에 장애를 알리기 전에 BFD 피어에서 누락되어야 하는 연속 BFD 제어 패킷의 수를 지정합니다. 범위는 3개~50개입니다.

단계 **4** 인터페이스에서 BFD 에코 모드를 활성화합니다.

bfd echo

예제**:**

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(if)# bfd echo
```

에코 모드는 기본적으로 활성화되어 있지만 BFD IPv6 세션에서 지원되지 않습니다. 에코 모드가 활성화된 경우, 최소 에코 전송 수준 및 필요한 최소 전송 간격 값은 **bfd interval** *milliseconds* **min_rx** *milliseconds* 구성에서 가져옵니다.

참고 BFD 에코 모드를 사용하기 전에 **no ip redirects** 명령을 사용하여 ICMP 리디렉션 메시지를 비활성화해야 합니다. 이렇게 하면 CPU를 많이 사용하는 것을 방지합니다.

BFD 맵 구성

멀티 홉 템플릿과 연결할 수 있는 대상을 포함하는 BFD 맵을 생성할 수 있습니다. 멀티 홉 BFD 템플릿을 이미 구성해 두었어야 합니다.

프로시저

단계 **1** 멀티 홉 BFD 템플릿을 생성합니다. 절차는 BFD 템플릿 생성, 850 페이지를 참조하십시오.

단계 **2** BFD 멀티 홉 템플릿을 대상의 맵에 연결합니다.

bfd map {ipv4 | ipv6} *destination/cdir source/cdire template-name*

예제:

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
ciscoasa(config-bfd)#
```

- **ipv4** — IPv4 주소를 구성합니다.
- **ipv6** — IPv6 주소를 구성합니다.
- *destination/cdir* — 대상 접두사/길이를 지정합니다. 형식은 A.B.C.D/<0-32>입니다.
- *source/cdir* — 대상 접두사/길이를 지정합니다. 형식은 X:X:X;X::X/<0-128>입니다.
- *template-name* — 이 BFD 맵과 연결된 멀티 홉 템플릿의 이름을 지정합니다.

단계 **3** (선택 사항) BFD 느린 타이머 값을 구성합니다.

bfd slow-timers [*milliseconds*]

예제:

```
ciscoasa(config)# bfd slow-timers 14000
ciscoasa(config-bfd)#
```

milliseconds — (선택 사항) BFD 느린 타이머 값입니다. 범위는 1000~30000입니다. 기본값은 1000입니다.

BFD에 대한 모니터링

다음 명령을 사용하여 BFD 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조를 참고하십시오.

다양한 BFD 라우팅 통계를 모니터링하거나 비활성화하려면 다음 명령 중 하나를 입력합니다.

- **show bfd neighbors**

  기존 BFD 인접성의 줄 단위 목록을 표시합니다.

- **show bfd summary**

  BFD, BFD 클라이언트 또는 BFD 세션에 대한 요약 정보를 표시합니다.

- **show bfd drops**

  BFD에서 삭제된 패킷 수를 표시합니다.

- **show bfd map**

  구성된 BFD 맵을 표시합니다.

- **show running-config bfd**

  모든 BFD 관련 전역 구성을 표시합니다.

BFD 라우팅에 대한 기록

표 ***31: BFD*** 라우팅에 대한 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
BFD 라우팅 지원	9.6(2)	이제 ASA에서 BFD 라우팅 프로토콜을 지원합니다. BFD 템플릿, 인터페이스 및 맵 구성에 대한 지원이 추가되었습니다. 또한 BFD를 사용하기 위한 BGP 라우팅 프로토콜 지원도 추가되었습니다. 추가된 명령: **bfd echo, bfd interval, bfd map, bfd slow-timers, bfd-template, clear bfd counters, clear conf bfd, neighbor fall-over bfd, show bfd drops, showbfd map, show bfd neighbors, show bfd summary, show running-config bfd**

28 장

BGP

이 장에서는 BGP(Border Gateway Protocol)를 이용하여 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 Cisco ASA를 구성하는 방법을 설명합니다.

BGP 소개

BGP는 자율 시스템 간 라우팅 프로토콜과 자율 시스템 내부 라우팅 프로토콜입니다. 자율 시스템은 공통 관리와 공통 라우팅 정책에 따르는 네트워크 또는 네트워크 그룹입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다.

BGP를 사용해야 하는 시기

대학 및 기업과 같은 고객 네트워크는 일반적으로 네트워크 내 라우팅 정보 교환을 위해 OSPF와 같은 IGP(Interior Gateway Protocol)를 활용합니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. AS(autonomous system) 사이에서 BGP가 사용될 때 이 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때의 프로토콜은 IBGP(Interior BGP)라고 합니다.

BGP를 IPv6 네트워크를 통해 IPv6 접두사를 위한 라우팅 정보를 전달하는 데도 사용할 수 있습니다.

참고 BGPv6 디바이스가 클러스터에 참가하면 로깅 수준 7이 활성화될 때 소프트 추적이 생성됩니다.

라우팅 테이블 변경 사항

네이버 간 TCP 연결이 처음 설정되면 BGP 네이버가 전체 라우팅 정보를 교환합니다. 라우팅 테이블 변경 사항이 감지되면 BGP 라우터가 변경된 경로만 네이버로 전송합니다. BGP 라우터는 주기적인 라우팅 업데이트를 전송하지 않고 BGP 라우팅 업데이트는 목적지 네트워크로의 최적의 경로만 알립니다.

BGP를 통해 학습된 경로에는 특정 목적지로 향하는 경로가 여럿일 때 최적의 경로를 결정하는 데 사용되는 속성이 포함되어 있습니다. 이러한 속성을 BGP 속성이라고 하며 경로 선택 과정에서 사용됩니다.

- Weight — 이는 Cisco가 정의한 라우터에 대한 로컬 속성입니다. 가중치 속성은 주변의 라우터에 알려지지 않습니다. 라우터가 동일한 목적지에 대하여 하나 이상의 경로를 학습한 경우 가중치가 가장 높은 경로가 우선합니다.
- Local preference — 로컬 기본 설정 속성은 로컬 AS로부터 출구 지점을 선택하는 데 사용됩니다. 가중치 속성과 달리 로컬 우선 속성은 로컬 AS 전체에 걸쳐 전파됩니다. AS에서 출구 지점이 여럿인 경우 로컬 우선 속성이 가장 높은 출구 지점이 특정 경로에 대한 출구 지점으로 사용됩니다.
- Multi-exit discriminator — MED(multi-exit discriminator) 또는 메트릭 속성은 메트릭에 알려지는 AS로의 우선 경로에 관한 외부 AS에 대한 제안으로 사용됩니다. MED를 수신하는 외부 AS가 경로 선택을 위해 다른 BGP 속성을 사용할 수도 있기 때문에 제안이라고 하는 것입니다. MED 메트릭이 낮은 경로가 우선합니다.
- Origin — 발신지 속성은 BGP가 특정 경로에 관해 어떻게 확인하는지 나타냅니다. 발신지 속성은 3가지 값을 가질 수 있으며 경로 선택에 사용됩니다.
  - IGP — 경로가 발신 AS 내부에 있습니다. 이 값은 경로를 BGP로 삽입하기 위해 네트워크 라우터 컨피그레이션 명령을 사용할 때 설정됩니다.
  - EGP — 경로는 EBGP(Exterior Border Gateway Protocol)를 통해 확인됩니다.
  - Incomplete — 경로의 발신지가 알 수 없거나 확인되지 않았습니다. 경로가 BGP로 재배포되면 불완전한 발신지가 됩니다.
- AS_path — 경로 알림이 자율 시스템을 통과할 때 경로가 전달된 AS 번호의 주문 목록에 AS 번호가 추가됩니다. 가장 짧은 AS_path 목록을 가진 경로만 IP 라우팅 테이블에 설치됩니다.
- Next hop — EBGP next-hop 속성은 전달되는 라우터에 도달하기 위해 사용되는 IP 주소입니다. EBGP 피어의 경우 next-hop 주소는 피어 간 연결의 IP 주소입니다. IBGP의 경우 EBGP next-hop 주소가 로컬 AS로 전달됩니다.
- Community — 커뮤니티 속성은 라우팅 결정(허용, 우선, 재배포)을 적용할 수 있는 커뮤니티라는 대상 그룹화 방법을 제공합니다. 경로 맵은 커뮤니티 속성을 설정하는 데 사용됩니다. 미리 정의된 커뮤니티 속성은 다음과 같습니다.
  - no-export — 이 경로를 EBGP 피어에게 알리지 않습니다.
  - no-advertise — 이 경로를 어느 피어에게도 알리지 않습니다.

- internet — 이 경로를 인터넷 커뮤니티에 알립니다. 네트워크의 모든 라우터가 여기 포함됩니다.

BGP 경로 선택

BGP는 같은 경로에 대해 서로 다른 소스로부터 여러 공지를 수신할 수 있습니다. BGP는 최적의 경로로 하나의 경로만 선택합니다. 이 경로가 선택된 경우 BGP는 선택된 경로를 IP 라우팅 테이블에 놓고 네이버에 전파합니다. BGP는 제시된 순서대로 다음 기준에 따라 목적지에 대한 경로를 선택합니다.

- 경로가 접근할 수 없는 next hop을 지정하면 업데이트를 삭제합니다.
- 가중치가 가장 높은 경로가 우선합니다.
- 가중치가 동일한 경우 로컬 우선이 가장 높은 경로가 우선합니다.
- 로컬 우선이 동일한 경우 이 라우터에서 실행 중인 BGP에서 발생한 경로가 우선합니다.
- 경로가 시작되지 않은 경우 AS_path가 가장 짧은 경로가 우선합니다.
- 모든 경로의 AS_path 길이가 같은 경우 발신지 유형이 가장 낮은 경로(IGP가 EGP보다 낮고 EGP가 incomplete보다 낮은 경로)가 우선합니다.
- 발신지 코드가 동일한 경우 MED 속성이 가장 낮은 경로가 우선합니다.
- MED가 같은 경로의 경우 내부 경로보다 외부 경로가 우선합니다.
- 그래도 경로가 동일한 경우 가장 가까운 IGP 네이버를 통한 경로가 우선합니다.
- 여러 경로에 BGP 다중 경로, 857 페이지에 대한 라우팅 테이블에서의 설치 작업이 필요한지 결정합니다.
- 두 경로 모두 외부인 경우 먼저 수신된 경로가 우선합니다(오래된 경로).
- BGP 라우터 ID가 지정한 대로 IP 주소가 가장 낮은 경로가 우선합니다.
- 여러 경로의 발신자 또는 라우터 ID가 동일할 경우 클러스터 목록 길이가 가장 짧은 경로가 우선합니다.
- 가장 낮은 네이버 주소에서 시작하는 경로가 우선합니다.

BGP 다중 경로

BGP 다중 경로를 사용하면 동일한 대상 접두사에 대해 비용이 동일한 여러 BGP 경로의 IP 라우팅 테이블에 설치할 수 있습니다. 그러면 대상 접두사에 대한 트래픽이 모든 설치된 경로에서 공유됩니다.

이러한 경로는 로드 공유에 최적의 경로와 함께 테이블에 설치됩니다. BGP 다중 경로는 최적의 경로를 선택할 때는 영향을 주지 않습니다. 예를 들어, 라우터는 알고리즘에 따라 경로 중 하나를 계속해서 최적의 경로로 지정하고 BGP 피어에 이 최적의 경로를 알립니다.

다중 경로의 후보가 되려면 동일한 대상에 대한 경로에 최적의 경로 특성과 동일한 다음 특성이 있어야 합니다.

- 무게
- 로컬 기본 설정
- AS-PATH 길이
- 출처 코드
- MED(Multi Exit Discriminator)
- 다음 중 하나입니다.
  - 네이버 AS 또는 하위-AS(BGP 다중 경로 추가 전)
  - AS-PATH(BGP 다중 경로 추가 후)

일부 BGP 다중 경로 기능은 다중 경로 후보에게 다음과 같은 추가 요구 사항을 제시합니다.

- 경로는 외부 또는 연합-외부 네이버(eBGP)에서 확인되어야 합니다.
- BGP next hop에 대한 IGP 메트릭은 최적의 경로 IGP 메트릭과 동일해야 합니다.

다음은 내부 BGP(iBGP) 다중 경로 후보에 대한 추가 요구 사항입니다.

- 경로는 내부 네이버(iBGP)에서 확인되어야 합니다.
- 라우터가 동일하지 않은 비용의 iBGP 다중 경로에 대해 구성되지 않은 경우 BGP next hop에 대한 IGP 메트릭은 최적의 경로 IGP 메트릭과 동일해야 합니다.

BGP는 다중 경로 후보에서 가장 최근에 수신한 경로를 최대 *n*개까지 IP 라우팅 테이블에 삽입합니다. 이때 *n*은 라우팅 테이블에 설치할 경로의 수이며 BGP 다중 경로를 구성할 때 지정된 수입니다. 다중 경로가 비활성화된 경우 기본값은 1입니다.

비용이 동일하지 않은 로드 밸런싱에 BGP 링크 대역폭을 사용할 수도 있습니다.

참고 동일한 next-hop-self는 내부 피어에 전달되기 전에 eBGP 다중 경로 중에서 선택된 최적의 경로에서 수행됩니다.

BGP를 위한 지침

상황 모드 지침

단일 및 다중 상황 모드에서 지원합니다.

방화벽 모드 지침

투명한 방화벽 모드를 지원하지 않습니다. BGP는 라우터 모드에서만 지원됩니다.

IPv6 지침

IPv6를 지원합니다. IPv6 주소군에 대해서는 graceful restart가 지원되지 않습니다.

BGP 구성

이 섹션에서는 시스템에서 BGP 프로세스를 활성화하고 구성하는 방법을 설명합니다.

프로시저

단계 **1** BGP 활성화, 859 페이지.
단계 **2** BGP 라우팅 프로세스를 위한 최적의 경로 정의, 861 페이지.
단계 **3** 정책 목록 구성, 862 페이지.
단계 **4** AS 경로 필터 구성, 863 페이지.
단계 **5** 커뮤니티 규칙 구성, 863 페이지.
단계 **6** IPv4 주소군 설정 구성, 864 페이지.
단계 **7** IPv6 주소군 설정 구성, 878 페이지.

BGP 활성화

이 섹션에서는 BGP 라우팅 활성화, BGP 라우팅 프로세스 설정 및 일반 BGP 매개변수 구성에 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제:

```
ciscoasa(config)# router bgp 2
```

autonomous-num에 대한 유효한 값은 1 ~ 4294967295와 1.0 ~ XX.YY입니다.

단계 **2** 지정된 값을 초과하는 as-path 세그먼트를 포함한 경로는 버립니다.

bgp maxas-limit number

예제:

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 인수는 허용된 최대 자율 시스템 세그먼트 개수를 지정합니다. 유효한 값은 1 ~ 254입니다.

단계 **3** 로그 BGP 네이버 재설정:

bgp log-neighbor-changes

단계 **4** BGP가 자동으로 각 BGP 세션에 대한 최적의 TCP 경로 MTU를 발견하도록 합니다.

bgp transport path-mtu-discovery

단계 **5** BGP가 피어에 도달하기 위해 사용되는 링크가 다운될 경우 홀드다운 타이머를 기다릴 필요 없이 바로 근처의 피어에 대한 외부 BGP 세션을 종료할 수 있게 합니다.

bgp fast-external-fallover

단계 **6** BGP 라우팅 프로세스가 외부 BGP(eBGP) 피어에서 수신한 업데이트 중 자율 시스템(AS) 번호를 수신 경로의 AS_PATH 속성에 있는 첫 번째 AS 세그먼트와 같이 나열하지 않는 것을 버리도록 허용합니다.

bgp enforce-first-as

단계 **7** BGP 4바이트 자율 시스템 번호의 기본 표시 및 정규식 일치 형식을 asplain(10진수)에서 dot notation으로 바꿉니다.

bgp asnotation dot

단계 **8** BGP 네트워크 타이머 조정:

timers bgp keepalive holdtime [min-holdtime]

예제**:**

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive — ASA가 피어로 keepalive 메시지를 보내는 빈도(초)입니다. 기본값은 60초입니다.
- holdtime — ASA가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)입니다. 기본값은 180초입니다.
- (선택 사항) min-holdtime — ASA가 데드 네이버를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)입니다.

단계 **9** BGP 정상 재시작 기능을 활성화합니다.

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

예제**:**

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time — graceful-restart-capable 네이버가 이벤트 발생 후 정상 작업으로 복귀하기까지 ASA가 대기할 최대 시간(초)입니다. 기본값은 120초입니다. 유효한 값은 1초 ~ 3600초입니다.

- stalepath-time — ASA가 재시작 피어를 위해 오래된 경로를 유지할 최대 시간(초)입니다. 모든 오래된 경로가 이 시간 이후 삭제됩니다. 기본값은 360초입니다. 유효한 값은 1초 ~ 3600초입니다.

BGP 라우팅 프로세스를 위한 최적의 경로 정의

이 섹션에서는 BGP 최적의 경로 구성에 필요한 단계를 설명합니다. 최적의 경로에 대한 자세한 정보는 BGP 경로 선택, 857 페이지에서 참조하십시오.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제:

```
ciscoasa(config)# router bgp 2
```

단계 **2** 기본 로컬 우선 값을 변경:

bgp default local-preference number

예제:

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 인수는 0과 4294967295 사이의 모든 값이 될 수 있습니다. 값이 높을수록 우선순위가 높습니다.

기본값은 100입니다.

단계 **3** 다른 자율 시스템의 네이버에서 학습된 경로 간 MED(Multi Exit Discriminator) 비교 활성화:

bgp always-compare-med

단계 **4** 최적의 경로 선정 과정 중 eBGP(external BGP) 피어에서 수신된 비슷한 경로를 비교하고 라우터 ID가 가장 낮은 최적의 경로로 전환:

bgp bestpath compare-routerid

단계 **5** 주변의 AS에서 전달된 최적의 MED 경로를 선택:

bgp deterministic-med

단계 **6** MED 속성이 누락된 경로를 우선순위가 가장 낮은 경로로 설정:

bgp bestpath med missing-as-worst

정책 목록 구성

경로 맵 내에서 정책 목록이 참조되는 경우 정책 목록의 모든 일치 문장이 평가 및 처리됩니다. 경로 맵 내에 둘 이상의 정책 목록을 구성할 수 있습니다. 정책 목록은 같은 경로 맵 내에 있으나 정책 목록 밖에서 구성된 기존 일치 항목 및 설정 명령문과도 공존할 수 있습니다. 이 섹션은 정책 목록 구성에 필요한 단계를 설명합니다.

프로시저

단계 **1** 정책-맵 컨피그레이션 모드를 활성화하고 BGP 정책 목록 생성을 허용:

policy-list policy_list_name {permit | deny}

예제**:**

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

permit 키워드는 일치 조건에 대해 액세스를 허용합니다.

deny 키워드는 일치 조건에 대해 액세스를 거부합니다.

단계 **2** next hop이 지정된 인터페이스 중 하나를 벗어난 경로를 배포합니다.

match interface [...interface_name]

예제**:**

```
ciscoasa(config-policy-list)# match interface outside
```

단계 **3** 목적지 주소, next hop 라우터 주소 및 라우터/액세스 서버 소스 중 하나 또는 모두를 일치시켜 경로를 재배포:

match ip {address | next-hop | route-source}

단계 **4** BGP 자율 시스템 경로 일치:

match as-path

단계 **5** BGP 커뮤니티 일치:

match community {community-list_name | exact-match}

예제**:**

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

- community-list_name — 하나 이상의 커뮤니티 목록.
- exact-match — 정확한 일치가 요구됨을 나타냅니다. 모든 커뮤니티와 지정된 커뮤니티가 모두 있어야 합니다.

단계 **6** 지정된 메트릭을 포함한 경로 재배포:

match metric

단계 **7** 지정된 태그와 일치하는 라우팅 테이블에서 경로 재배포:

match tag

AS 경로 필터 구성

AS 경로 필터는 액세스 목록을 사용하고 업데이트 메시지 내에 개별 접두사를 살펴봄으로써 라우팅 업데이트 메시지를 필터링할 수 있습니다. 업데이트 메시지 내 접두사가 필터 기준과 일치하면 필터 엔트리에서 수행하도록 구성된 작업에 따라 해당 개별 접두사가 필터링되거나 승인됩니다. 이 섹션에서는 AS 경로 필터 구성에 필요한 단계를 설명합니다.

참고 as-path access-lists는 일반 방화벽 ACL과 다릅니다.

프로시저

글로벌 컨피그레이션 모드의 정규식을 사용하여 자율 시스템 경로 필터를 구성:

as-path access-list acl-number {permit|deny} regexp

예제**:**

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number* — AS-path 액세스 목록 번호. 유효한 값은 1 ~ 500입니다.
- regexp — AS-path 필터를 정의하는 정규식. 자율 시스템 번호는 1 ~ 65535 범위로 표현됩니다.

커뮤니티 규칙 구성

커뮤니티는 공통 속성을 공유하는 목적지 그룹입니다. 커뮤니티 목록을 사용하여 경로 맵의 일치 조항에서 사용할 커뮤니티 그룹을 만들 수 있습니다. 액세스 목록과 마찬가지로 일련의 커뮤니티 목록을 생성할 수 있습니다. 일치 항목을 찾을 때까지 구문을 확인합니다. 1개 구문이 만족되면 테스트가 종료됩니다. 이 섹션은 커뮤니티 규칙 구성에 필요한 단계를 설명합니다.

프로시저

BGP 커뮤니티 목록 및 액세스 제어를 생성 또는 구성:

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

예제:

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise no-export
```

- standard — 1부터 99까지의 숫자를 사용하여 표준 커뮤니티 목록을 만들어서 하나 이상의 허용 또는 거부 커뮤니티 그룹을 식별합니다.
- (선택 사항) community-number — 1부터 4294967200 사이의 32비트 숫자로 표현된 커뮤니티. 단일 커뮤니티를 입력하거나 공백으로 구분된 여러 커뮤니티를 입력할 수 있습니다.
- AA:NN — 4바이트의 새로운 커뮤니티 형식으로 입력되는 자율 시스템 번호 및 네트워크 번호. 이 값은 콜론으로 구분된 2개의 2바이트 숫자로 구성됩니다. 각 2바이트 숫자에 대해 1부터 65535 사이의 숫자를 입력할 수 있습니다. 단일 커뮤니티를 입력하거나 공백으로 구분된 여러 커뮤니티를 입력할 수 있습니다.
- (선택 사항) internet — 인터넷 커뮤니티를 지정합니다. 이 커뮤니티 경로는 모든 피어(내부 및 외부)에게 알려집니다.
- (선택 사항) no-advertise — no-advertise 커뮤니티를 지정합니다. 이 커뮤니티 경로는 모든 피어(내부 또는 외부)에게 알려지지 않습니다.
- (선택 사항) no-export — no-export 커뮤니티를 지정합니다. 이 커뮤니티 경로는 같은 자율 시스템 안에 있는 피어 또는 연합 내에 다른 하위 자율 시스템으로만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.
- (선택 사항) expanded— 100 ~ 500의 확장된 커뮤니티 목록 번호를 구성하여 하나 이상의 허용 또는 거부 커뮤니티 그룹을 식별합니다.
- regexp — AS-path 필터를 정의하는 정규식. 자율 시스템 번호는 1 ~ 65535 범위로 표현됩니다.

  참고 정규 표현식은 확장 커뮤니티 목록에서만 사용할 수 있습니다.

IPv4 주소군 설정 구성

BGP에 대한 IPv4 설정은 BGP 컨피그레이션 설정 내 IPv4 주소군 옵션에서 설정 가능합니다. IPv4 주소군 섹션에는 일반 설정, 종합 주소 설정, 필터링 설정 및 네이버 설정에 대한 하위 섹션이 포함됩니다. 이 하위 섹션을 통해 IPv4 주소군에 대한 매개변수를 사용자 정의할 수 있습니다.

IPv4 주소군 일반 설정 구성

이 섹션에서는 일반 IPv4 설정에 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 라우터를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제:

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 **3** (선택 사항) 로컬 BGP 라우팅 프로세스에 대한 고정 라우터 ID를 구성:

bgp router-id A.B.C.D

예제:

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

인수 A.B.C.D는 IP 주소 형식으로 라우터 ID를 지정합니다. 라우터 ID를 지정하지 않으면 자동으로 할당됩니다.

단계 **4** (선택 사항) 개별 인터페이스(L3) 모드에서 IP 주소의 클러스터 풀을 구성:

bgp router-id cluster-pool

예제:

```
ciscoasa(config-router-af)# bgp router-id cp
```

참고 L3 클러스터에서 BGP 네이버를 클러스터 풀 IP 주소 중 하나로 정의할 수 없습니다.

단계 **5** BGP 경로에 대한 관리 거리를 구성:

distance bgp external-distance internal-distance local-distance

예제:

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance — 외부 BGP 경로를 위한 관리 거리. 외부 자동 시스템에서 학습한 경로는 외부 경로입니다. 이 인수 값 범위는 1 ~ 255입니다.

- internal-distance — 내부 BGP 경로를 위한 관리 거리. 로컬 자동 시스템의 피어에서 학습한 경로는 내부 경로입니다. 이 인수 값 범위는 1 ~ 255입니다.
- local-distance — 로컬 BGP 경로에 대한 관리 거리. 로컬 경로는 다른 프로세스에서 재배포되는 라우터나 네트워크에 대한 네트워크 라우터 컨피그레이션 명령을 통해 종종 백도어로 나열된 네트워크입니다. 이 인수 값 범위는 1 ~ 255입니다.

단계 **6** BGP 학습 경로를 통해 IP 라우팅 테이블이 업데이트될 때 메트릭 및 태그 값 수정:

table-map {WORD|route-map_name}

예제:

```
ciscoasa(config-router-af)# table-map example1
```

route-map_name 인수는 route-map 명령의 경로 맵을 지정합니다.

단계 **7** 기본 경로를 배포하도록 BGP 라우팅 프로세스를 구성(네트워크 0.0.0.0):

default-information originate

단계 **8** 네트워크 수준 경로로 서브넷 경로 자동 요약을 구성:

auto-summary

단계 **9** RIB(routing information base)에 설치되지 않은 경로 알림을 억제:

bgp suppress-inactive

단계 **10** BGP와 IGP(Interior Gateway Protocol) 시스템 간 동기화:

synchronization

단계 **11** OSPF와 같은 IGP로의 iBGP 재배포 구성:

bgp redistribute-internal

단계 **12** next hop 확인을 위한 BGP 라우터 스캔 간격을 구성:

bgp scan-time scanner-interval

예제:

```
ciscoasa(config-router-af)# bgp scan-time 15
```

scanner-interval 인수는 BGP 라우팅 정보의 스캔 간격을 지정합니다. 유효한 값은 5초 ~ 75초입니다. 기본값은 60초입니다.

단계 **13** BGP next-hop 주소 추적 구성:

bgp nexthop trigger {delay seconds|enable}

예제:

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger — BGP next-hop 주소 추적 사용을 지정합니다. 이 키워드를 delay 키워드와 함께 사용하여 next-hop 추적 지연을 변경합니다. 이 키워드를 enable 키워드와 함께 사용하여 next-hop 주소 추적을 활성화합니다.
- delay — 라우팅 테이블에 설치된 업데이트된 next-hop 경로 간 지연 간격을 변경합니다.
- seconds — 지연을 초로 지정합니다. 범위는 0 ~ 100입니다. 기본값은 5입니다.
- enable — BGP next-hop 주소 추적을 즉시 활성화합니다.

단계 **14** 라우팅 테이블에 설치할 수 있는 병렬 iBGP 경로의 최대 수를 제어:

maximum-paths {number_of_paths|ibgp number_of_paths}

예제**:**

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

참고 ibgp 키워드를 사용하지 않으면 number_of_paths 인수가 병렬 EBGP 경로의 최대 개수를 제어합니다.

number_of_paths argument는 라우팅 테이블에 설치할 경로의 수를 지정합니다. 유효한 값은 1 ~ 8입니다.

IPv4 주소군 종합 주소 설정 구성

이 섹션에서는 하나의 경로로의 특정 경로 종합을 정의하는 데 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 **3** BGP 데이터베이스에 종합 엔트리를 생성:

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

예제:

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address — 종합 주소.
- mask — 종합 마스크.
- map-name — 경로 맵.
- (선택 사항) as-set — 자율 시스템 설정 경로 정보를 생성합니다.
- (선택 사항) summary-only — 업데이트에서 모든 more-specific 경로를 필터링합니다.
- (선택 사항) Suppress-map map-name — 억제할 경로 선택에 사용할 경로 지도의 이름을 지정합니다.
- (선택 사항) Advertise-map map-name — AS_SET 오리진 커뮤니티 생성을 위한 경로 선택에 사용할 경로 지도 이름을 지정합니다.
- (선택 사항) attribute-map map-name — 종합 경로 속성 설정에 사용할 경로 지도 이름을 지정합니다.

IPv4 주소군 필터링 설정 구성

이 섹션에서는 수신 BGP 업데이트에서 수신된 경로나 네트워크 필터링에 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 라우터 구성 모드로 들어갑니다.

router bgp *autonomous-num*

예제:

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [**unicast**]

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 **3** 발신 BGP 업데이트에서 수신된 경로나 네트워크를 필터링:

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

acl-number 인수는 IP 액세스 목록 번호를 지정합니다. 액세스 목록은 라우팅 업데이트에서 어떤 네트워크를 수신하고 어떤 네트워크를 억제할지 정의합니다.

in 키워드를 사용하면 필터가 수신 BGP 업데이트에 적용되며 **out** 키워드를 사용하면 필터가 발신 BGP 업데이트에 적용됩니다.

아웃바운드 필터의 경우 선택적으로 배포 목록에 적용할 프로세스 번호(RIP용 제외)로 프로토콜(**bgp**, **eigrp**, **ospf** 또는 **rip**)을 지정할 수 있습니다. 피어와 네트워크를 **connected** 또는 **static** 경로를 통해 확인했는지 여부를 필터링할 수도 있습니다.

예제:

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

IPv4 주소군 BGP 네이버 설정 구성

이 섹션은 BGP 네이버 및 네이버 설정 정의에 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 라우터를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제:

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 **3** BGP 네이버 테이블에 엔트리 추가:

neighbor ip-address remote-as autonomous-number

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

단계 **4** (선택 사항) 네이버 또는 피어 그룹 비활성화:

neighbor ip-address shutdown

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

단계 **5** BGP 네이버와 정보 교환:

neighbor ip-address activate

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

단계 **6** BGP 네이버에 대한 BGP(Border Gateway Protocol) graceful restart 기능 활성화 또는 비활성화:

neighbor ip-address ha-mode graceful-restart [disable]

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

(선택 사항) disable 키워드는 네이버에 대한 BGP graceful restart 기능을 비활성화합니다.

단계 **7** BGP 네이버 정보를 액세스 목록에 지정된 대로 배포:

neighbor {ip-address} distribute-list {access-list-name}{in|out}

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number — 표준 또는 확장 액세스 목록의 개수. 표준 액세스 목록 개수 범위는 1 ~ 99입니다. 확장 액세스 목록 개수 범위는 100 ~ 199입니다.
- expanded-list-number — 확장 액세스 목록 번호의 개수입니다. 확장 액세스 목록 범위는 1300 ~ 2699입니다.
- access-list-name — 표준 또는 확장 액세스 목록의 이름.
- prefix-list-name — BGP 접두사 목록의 이름.
- in — 액세스 목록이 해당 네이버의 수신 알림에 적용됩니다.
- out — 액세스 목록이 해당 네이버의 발신 알림에 적용됩니다.

단계 **8** 수신 또는 발신 경로에 경로 맵 적용:

neighbor {ip-address} route-map map-name {in|out}

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

in 키워드는 수신 경로에 대한 경로 맵에 적용됩니다.

out 키워드는 발신 경로에 대한 경로 맵에 적용됩니다.

단계 **9** BGP 네이버 정보를 접두사 목록에 지정된 대로 배포:

neighbor {ip-address} prefix-list prefix-list-name {in|out}

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

in 키워드는 접두사 목록이 해당 네이버의 수신 알림에 적용됨을 의미합니다.

out 키워드는 접두사 목록이 해당 네이버의 발신 알림에 적용됨을 의미합니다.

단계 **10** 필터 목록 설정:

neighbor {ip-address} filter-list access-list-number {in|out}

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name — 자율 시스템 경로 액세스 목록의 개수를 지정합니다. ip as-path access-list 명령으로 이 액세스 목록을 정의합니다.
- in — 액세스 목록이 해당 네이버의 수신 알림에 적용됩니다.
- out — 액세스 목록이 해당 네이버의 발신 알림에 적용됩니다.

단계 **11** 네이버에서 수신할 수 있는 접두사 개수를 제어:

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum — 이 네이버에서 최대 개수의 접두사가 허용됩니다.
- (선택 사항) threshold — 라우터가 경고 메시지 생성을 시작할 최대 비율을 나타내는 정수입니다. 범위는 1 ~ 100입니다. 기본값은 75(백분율)입니다.
- (선택 사항) restart interval — BGP 네이버가 재시작되는 시간 간격을 지정하는 정수 값(분)입니다.
- (선택 사항) warning-only — 접두사 최대 개수를 초과하면 피어링을 종료하는 대신 라우터가 로그 메시지를 생성하도록 허용합니다.

단계 **12** BGP 스피커(로컬 라우터)가 기본 경로 0.0.0.0을 네이버로 전송하도록 허용:

neighbor {ip-address} default-originate [route-map map-name]

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

인수 map-name은 route-map의 이름입니다. 이 경로 맵은 경로 0.0.0.0을 조건부로 삽입하도록 허용합니다.

단계 **13** BGP 라우팅 업데이트 전송 최소 간격을 설정:

neighbor {ip-address} advertisement-interval seconds

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

seconds 인수는 시간(초)입니다. 유효한 값은 0 ~ 600입니다.

단계 **14** 구성된 route-map과 일치하는 BGP 테이블의 경로를 알림:

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

예제:

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name — exist 맵 또는 non-exist 맵의 조건이 충족될 경우 알릴 경로 맵의 이름입니다.
- exist-map map name — exist-map의 이름을 BGP 테이블의 경로와 비교하여 advertise-map 경로의 알림 여부를 결정합니다.
- non-exist-map map name — non-exist-map의 이름을 BGP 테이블의 경로와 비교하여 advertise-map 경로의 알림 여부를 결정합니다.
- (선택 사항) check all paths — BGP 테이블의 접두사를 통해 모든 경로를 exist-map으로 확인할 수 있도록 허용합니다.

단계 **15** 아웃바운드 라우팅 업데이트에서 비공개 자율 시스템 번호를 제거:

neighbor {ip-address} remove-private-as

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

단계 **16** 특정 BGP 피어 또는 피어 그룹에 대한 타이머를 설정합니다.

neighbor {ip-address} timers keepalive holdtime min holdtime

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive — ASA가 keepalive 메시지를 피어로 전송하는 빈도(초)입니다. 기본값은 60초입니다. 유효한 값은 0 ~ 65535입니다.

- holdtime — ASA가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)입니다. 기본값은 180초입니다.
- min holdtime — ASA가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 최소 간격(초)입니다.

단계 **17** 두 BGP 피어 간 TCP 연결에 대한 MD5(Message Digest 5) 인증 활성화:

neighbor {ip-address} password string

예제**:**

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

string 인수는 service password-encryption 명령이 활성화되어 있을 때 최대 25자, service password-encryption 명령이 활성화되지 않은 경우 최대 81자의 대/소문자를 구분하는 비밀번호입니다. 문자열은 공백을 포함하여 모든 영숫자 문자를 포함할 수 있습니다.

참고 첫 번째 문자는 숫자가 될 수 없습니다. number-space-anything 형식의 비밀번호는 지정할 수 없습니다. 숫자 뒤에 공백이 오면 인증이 실패할 수 있습니다.

단계 **18** 커뮤니티 속성을 BGP 네이버로 전송하도록 지정:

neighbor {ip-address} send-community[both|standard|extended]

예제**:**

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

- (선택 사항) both 키워드 — 표준 및 확장 커뮤니티를 모두 전송합니다.
- (선택 사항) standard 키워드 — 표준 커뮤니티만 전송됩니다.
- (선택 사항) extended 키워드 — 확장된 커뮤니티만 전송됩니다.

단계 **19** 라우터를 BGP 네이버 또는 피어 그룹에 대한 next hop으로 구성:

neighbor {ip-address}next-hop-self

예제**:**

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

단계 **20** 직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도:

neighbor {ip-address} ebgp-multihop [ttl]

예제**:**

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

ttl 인수는 1 ~ 255홉 범위의 time-to-live를 지정합니다.

단계 **21** 연결 확인을 비활성화하여 루프백 인터페이스를 사용하는 단일 홉 피어를 통한 eBGP 피어링 세션을 설정:

neighbor {ip-address} disable-connected-check

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

단계 **22** BGP 피어링 세션을 보안하고 두 외부 BGP(eBGP) 피어를 분리하는 최대 홉 개수를 구성:

neighbor {ip-address} ttl-security hops hop-count

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

hop-count 인수는 eBGP 피어를 분리하는 홉의 개수입니다. TTL 값은 구성된 hop-count 인수로부터 라우터에 의해 계산됩니다. 유효한 값은 1 ~ 254입니다.

단계 **23** 네이버 연결에 가중치 할당:

neighbor {ip-address} weight number

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

number 인수는 네이버 연결에 할당하는 가중치입니다. 유효한 값은 0 ~ 65535입니다.

단계 **24** ASA가 특정 BGP 버전만 승인하도록 구성:

neighbor {ip-address} version number

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

number 인수는 BGP 버전 번호를 지정합니다. 버전을 2로 설정하여 소프트웨어가 지정된 네이버에서 버전 2만 사용하도록 강제할 수 있습니다. 기본값은 버전 4를 사용하고 요청 시 동적으로 버전 2까지 사용할 수 있도록 하는 것입니다.

단계 **25** BGP 세션에 대한 TCP 전송 세션 옵션 활성화:

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode — 연결 유형(active 또는 passive).
- path-mtu-discovery — TCP 전송 경로 최대 전송 단위(MTU) 검색을 활성화합니다. TCP 경로 MTU 검색은 기본적으로 활성화되어 있습니다.

- (선택 사항) disable — TCP 경로 MTU 검색을 비활성화합니다.

단계 **26** eBGP(Border Gateway Protocol) 네이버에서 수신된 AS_PATH 속성을 사용자 정의:

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

예제**:**

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (선택 사항) autonomous-system-number — AS_PATH 속성에 접두사로 붙일 최대 자율 시스템 개수입니다. 이 인수의 갑 범위는 1 ~ 4294967295 또는 1.0 ~ XX.YY의 유효한 자율 시스템 번호입니다.
- (선택 사항) no-prepend — 로컬 자율 시스템 번호를 eBGP 네이버에서 수신한 경로에 붙이지 않습니다.

IPv4 네트워크 설정 구성

이 섹션은 BGP 라우팅 프로세스가 알릴 네트워크를 정의합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 **3** BGP 라우팅 프로세스가 알릴 네트워크를 지정:

network {network-number [mask network-mask]}[route-map map-tag]

예제**:**

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

- network-number — BGP가 알릴 네트워크.
- (선택 사항) network-mask — 마스크 주소를 포함한 네트워크 또는 서브 네트워크 마스크.

- (선택 사항) map-tag — 구성된 경로 맵의 식별자. 알릴 네트워크를 필터링하려면 경로 맵을 검사해야 합니다. 지정하지 않으면 모든 네트워크를 광고합니다.

IPv4 재배포 설정 구성

이 섹션은 다른 라우팅 도메인의 경로로부터 BGP로 재배포하는 조건을 정의하기 위한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

예제**:**

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 **3** 다른 라우팅 도메인의 경로를 BGP 자율 시스템으로 재배포:

redistribute protocol [process-id] [metric] [route-map [map-tag]]

예제**:**

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol — 경로를 재배포하는 소스 프로토콜. Connected, EIGRP, OSPF, RIP 또는 Static 중 하나가 될 수 있습니다.
- (선택 사항) process-id — 특정 라우팅 프로세스의 이름.
- (선택 사항) metric — 재배포된 경로의 메트릭.
- (선택 사항) map-tag — 구성된 경로 맵의 식별자.

참고 재배포할 네트워크를 필터링하려면 경로 맵을 검사해야 합니다. 지정하지 않으면 모든 네트워크를 재배포합니다.

IPv4 경로 삽입 설정 구성

이 섹션에서는 BGP 라우팅 테이블에 조건부로 삽입할 경로를 정의하기 위한 단계를 설명합니다.

프로시저

단계 1 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제:

```
ciscoasa(config)# router bgp 2
```

단계 2 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

예제:

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

unicast 키워드는 IPv4 유니캐스트 주소 접두사를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

단계 3 조건부 경로 삽입을 구성하여 BGP 라우팅 테이블로 더 많은 특정 경로를 삽입:

bgp inject-map inject-map exist-map exist-map [copy-attributes]

예제:

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map — 로컬 BGP 라우팅 테이블로 삽입할 접두사를 지정하는 경로 맵 이름.
- exist-map — BGP 스피커가 추적하는 접두사를 포함하는 경로 맵의 이름.
- (선택 사항) copy-attributes — 삽입된 경로가 종합 경로의 속성을 상속받도록 구성합니다.

IPv6 주소군 설정 구성

BGP에 대한 IPv6 설정은 BGP 컨피그레이션 설정 내 IPv6 패밀리 옵션에서 설정 가능합니다. IPv6 주소군 섹션에는 일반 설정, 종합 주소 설정 및 네이버 설정에 대한 하위 섹션이 포함됩니다. 이 하위 섹션을 통해 IPv6 주소군에 대한 매개변수를 사용자 정의할 수 있습니다.

이 섹션에서는 BGP IPv6 주소군 설정 사용자 정의 방법을 설명합니다.

IPv6 주소군 일반 설정 구성

이 섹션에서는 일반 IPv6 설정에 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 라우터를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv6 [unicast]

단계 **3** BGP 경로에 대한 관리 거리를 구성:

distance bgp external-distance internal-distance local-distance

예제**:**

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance — 외부 BGP 경로를 위한 관리 거리. 외부 자동 시스템에서 학습한 경로는 외부 경로입니다. 이 인수 값 범위는 1 ~ 255입니다.
- internal-distance — 내부 BGP 경로를 위한 관리 거리. 로컬 자동 시스템의 피어에서 학습한 경로는 내부 경로입니다. 이 인수 값 범위는 1 ~ 255입니다.
- local-distance — 로컬 BGP 경로에 대한 관리 거리. 로컬 경로는 다른 프로세스에서 재배포되는 라우터나 네트워크에 대한 네트워크 라우터 컨피그레이션 명령을 통해 종종 백도어로 나열된 네트워크입니다. 이 인수 값 범위는 1 ~ 255입니다.

단계 **4** (선택 사항) 기본 경로를 배포하도록 BGP 라우팅 프로세스를 구성(네트워크 0.0.0.0):

default-information originate

단계 **5** (선택 사항) RIB(routing information base)에 설치되지 않은 경로 알림을 억제:

bgp suppress-inactive

단계 **6** BGP와 IGP(Interior Gateway Protocol) 시스템 간 동기화:

synchronization

단계 **7** OSPF와 같은 IGP로의 iBGP 재배포 구성:

bgp redistribute-internal

단계 **8** next hop 확인을 위한 BGP 라우터 스캔 간격을 구성:

bgp scan-time scanner-interval

예제**:**

```
ciscoasa(config-router-af)# bgp scan-time 15
```

scanner-interval 인수에 대한 유효한 값은 5 ~ 60초입니다. 기본값은 60초입니다.

단계 **9** 라우팅 테이블에 설치할 수 있는 병렬 iBGP 경로의 최대 수를 제어:

maximum-paths {number_of_paths|ibgp number_of_paths}

예제**:**

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

number_of_paths 인수의 유효한 값은 1 ~ 8입니다.

ibgp 키워드를 사용하지 않으면 number_of_paths 인수가 병렬 EBGP 경로의 최대 개수를 제어합니다.

IPv6 주소군 종합 주소 설정 구성

이 섹션에서는 하나의 경로로의 특정 경로 종합을 정의하는 데 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv6 unicast

단계 **3** BGP 데이터베이스에 종합 엔트리를 생성:

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

예제**:**

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address — 종합 IPv6 주소.
- (선택 사항) as-set — 자율 시스템 설정 경로 정보를 생성합니다.
- (선택 사항) summary-only — 업데이트에서 모든 more-specific 경로를 필터링합니다.
- (선택 사항) Suppress-map map-name — 억제할 경로 선택에 사용할 경로 지도의 이름을 지정합니다.
- (선택 사항) Advertise-map map-name — AS_SET 오리진 커뮤니티 생성을 위한 경로 선택에 사용할 경로 지도 이름을 지정합니다.
- (선택 사항) attribute-map map-name — 종합 경로 속성 설정에 사용할 경로 지도 이름을 지정합니다.

단계 **4** BGP 경로가 종합되는 간격을 설정:

bgp aggregate-timer seconds

예제**:**

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

IPv6 주소군 BGP 인접 디바이스 설정 구성

이 섹션은 BGP 네이버 및 네이버 설정 정의에 필요한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 라우터를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv6 [unicast]

단계 **3** BGP 네이버 테이블에 엔트리 추가:

neighbor ipv6-address remote-as autonomous-number

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

ipv6-address 인수는 지정된 네트워크 도달에 사용할 수 있는 next hop의 IPv6 주소를 지정합니다. next hop의 IPv6 주소는 직접 연결될 필요가 없습니다. 직접 연결된 next hop의 IPv6 주소를 찾기 위해 재귀가 수행됩니다. 인터페이스 유형과 인터페이스 숫자가 지정된 경우 선택 사항으로 패킷이 출력되는 next hop의 IPv6 주소를 지정할 수 있습니다. link-local 주소를 next hop으로 사용할 때는 인터페이스 유형과 인터페이스 숫자를 반드시 지정해야 합니다(link-local next hop이 네이버이기도 해야 함).

참고 이 인수는 RFC 2373에 나와 있는 형식이어야 합니다. 즉, 콜론 사이의 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.

단계 **4** (선택 사항) 네이버 또는 피어 그룹 비활성화:

neighbor ipv6-address shutdown

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

단계 **5** BGP 네이버와 정보 교환:

neighbor ipv6-address activate

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

단계 **6** 수신 또는 발신 경로에 경로 맵 적용:

neighbor {ipv6-address} route-map map-name {in|out}

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

in 키워드는 수신 경로에 대한 경로 맵에 적용됩니다.

out 키워드는 발신 경로에 대한 경로 맵에 적용됩니다.

단계 **7** BGP 네이버 정보를 접두사 목록에 지정된 대로 배포:

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

in 키워드는 접두사 목록이 해당 네이버의 수신 알림에 적용됨을 의미합니다.

out 키워드는 접두사 목록이 해당 네이버의 발신 알림에 적용됨을 의미합니다.

단계 **8** 필터 목록 설정:

neighbor {ipv6-address} filter-list access-list-name {in|out}

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name — 자율 시스템 경로 액세스 목록의 개수를 지정합니다. ip as-path access-list 명령으로 이 액세스 목록을 정의합니다.
- in — 액세스 목록이 해당 네이버의 수신 알림에 적용됩니다.
- out — 액세스 목록이 해당 네이버의 발신 알림에 적용됩니다.

단계 **9** 네이버에서 수신할 수 있는 접두사 개수를 제어:

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum — 이 네이버에서 최대 개수의 접두사가 허용됩니다.
- (선택 사항) threshold — 라우터가 경고 메시지 생성을 시작할 최대 비율을 나타내는 정수입니다. 범위는 1 ~ 100입니다. 기본값은 75(백분율)입니다.
- (선택 사항) restart interval — BGP 네이버가 재시작되는 시간 간격을 지정하는 정수 값(분)입니다.
- (선택 사항) warning-only — 접두사 최대 개수를 초과하면 피어링을 종료하는 대신 라우터가 로그 메시지를 생성하도록 허용합니다.

단계 **10** BGP 스피커(로컬 라우터)가 기본 경로 0.0.0.0을 네이버로 전송하도록 허용:

neighbor {ipv6-address} default-originate [route-map map-name]

예제**:**

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

인수 map-name은 route-map의 이름입니다. 이 경로 맵은 경로 0.0.0.0을 조건부로 삽입하도록 허용합니다.

단계 **11** BGP 라우팅 업데이트 전송 최소 간격을 설정:

neighbor {ipv6-address} advertisement-interval seconds

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

seconds 인수는 시간(초)입니다. 유효한 값은 0 ~ 600입니다.

단계 **12** 아웃바운드 라우팅 업데이트에서 비공개 자율 시스템 번호를 제거:

neighbor {ipv6-address} remove-private-as

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

단계 **13** 구성된 route-map과 일치하는 BGP 테이블의 경로를 알림:

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name — exist 맵 또는 non-exist 맵의 조건이 충족될 경우 알릴 경로 맵의 이름입니다.
- exist-map map name — exist-map의 이름을 BGP 테이블의 경로와 비교하여 advertise-map 경로의 알림 여부를 결정합니다.
- non-exist-map map name — non-exist-map의 이름을 BGP 테이블의 경로와 비교하여 advertise-map 경로의 알림 여부를 결정합니다.
- (선택 사항) check all paths — BGP 테이블의 접두사를 통해 모든 경로를 exist-map으로 확인할 수 있도록 허용합니다.

단계 **14** 특정 BGP 피어 또는 피어 그룹에 대한 타이머를 설정합니다.

neighbor {ipv6-address} timers keepalive holdtime min holdtime

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive — ASA가 keepalive 메시지를 피어로 전송하는 빈도(초)입니다. 기본값은 60초입니다. 유효한 값은 0 ~ 65535입니다.
- holdtime — ASA가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)입니다. 기본값은 180초입니다.
- min holdtime — ASA가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 최소 간격(초)입니다.

단계 **15** 두 BGP 피어 간 TCP 연결에 대한 MD5(Message Digest 5) 인증 활성화:

neighbor {ipv6-address} password string

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

string 인수는 service password-encryption 명령이 활성화되어 있을 때 최대 25자, service password-encryption 명령이 활성화되지 않은 경우 최대 81자의 대/소문자를 구분하는 비밀번호입니다. 문자열은 공백을 포함하여 모든 영숫자 문자를 포함할 수 있습니다.

참고 첫 번째 문자는 숫자가 될 수 없습니다. number-space-anything 형식의 비밀번호는 지정할 수 없습니다. 숫자 뒤에 공백이 오면 인증이 실패할 수 있습니다.

단계 **16** 커뮤니티 속성을 BGP 네이버로 전송하도록 지정:

neighbor {ipv6-address} send-community [standard]

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

(선택 사항) standard 키워드 — 표준 커뮤니티만 전송됩니다.

단계 **17** 라우터를 BGP 네이버 또는 피어 그룹에 대한 next hop으로 구성:

neighbor {ipv6-address}next-hop-self

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

단계 **18** 직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도:

neighbor {ipv6-address} ebgp-multihop [ttl]

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

ttl 인수는 1 ~ 255홉 범위의 time-to-live를 지정합니다.

단계 **19** 연결 확인을 비활성화하여 루프백 인터페이스를 사용하는 단일 홉 피어를 통한 eBGP 피어링 세션을 설정:

neighbor {ipv6-address} disable-connected-check

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

단계 **20** BGP 피어링 세션을 보안하고 두 외부 BGP(eBGP) 피어를 분리하는 최대 홉 개수를 구성:

neighbor {ipv6-address} ttl-security hops hop-count

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

hop-count 인수는 eBGP 피어를 분리하는 홉의 개수입니다. TTL 값은 구성된 hop-count 인수로부터 라우터에 의해 계산됩니다. 유효한 값은 1 ~ 254입니다.

단계 **21** 네이버 연결에 가중치 할당:

neighbor {ipv6-address} weight number

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

number 인수는 네이버 연결에 할당하는 가중치입니다. 유효한 값은 0 ~ 65535입니다.

단계 **22** ASA가 특정 BGP 버전만 승인하도록 구성:

neighbor {ipv6-address} version number

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

number 인수는 BGP 버전 번호를 지정합니다. 기본값은 버전 4입니다. 현재 BGP 버전 4만 지원됩니다.

단계 **23** BGP 세션에 대한 TCP 전송 세션 옵션 활성화:

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

예제:

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode — 연결 유형(active 또는 passive).
- path-mtu-discovery — TCP 전송 경로 최대 전송 단위(MTU) 검색을 활성화합니다. TCP 경로 MTU 검색은 기본적으로 활성화되어 있습니다.
- (선택 사항) disable — TCP 경로 MTU 검색을 비활성화합니다.

단계 **24** eBGP(Border Gateway Protocol) 네이버에서 수신된 AS_PATH 속성을 사용자 정의:

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

예제:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (선택 사항) autonomous-system-number — AS_PATH 속성에 접두사로 붙일 최대 자율 시스템 개수입니다. 이 인수의 값 범위는 1~4294967295 또는 1.0~XX.YY의 유효한 자율 시스템 번호입니다.
- (선택 사항) no-prepend — 로컬 자율 시스템 번호를 eBGP 네이버에서 수신한 경로에 붙이지 않습니다.

주의 BGP는 네트워크 도달 정보를 유지하고 라우팅 루프를 예방하기 위해 경로가 이동하는 각 BGP 네트워크에서 자동 시스템을 접두사로 추가합니다. 이 명령은 자율 시스템 마이그레이션에 대해 구성해야 하고 이전이 완료된 후에 제거해야 합니다. 이 절차는 숙련된 네트워크 운영자만 시도해야 합니다. 라우팅 루프가 부적절한 컨피그레이션을 통해 생성될 수 있습니다.

IPv6 네트워크 설정 구성

이 섹션은 BGP 라우팅 프로세스가 알릴 네트워크를 정의합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv6 [unicast]

단계 **3** BGP 라우팅 프로세스가 알릴 네트워크를 지정:

network {*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] | *ipv6_prefix*/*prefix_length*} [**route-map** *route_map_name*]

예제**:**

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
ciscoasa(config-router-af)# network outside-prefix 1::/64
ciscoasa(config-router-af)# network outside-prefix 2::/64
```

- *prefix_delegation_name* — DHCPv6 접두사 위임 클라이언트(**ipv6 dhcp client pd**)를 활성화하는 경우, 접두사를 알릴 수 있습니다. 접두사를 서브넷으로 지정하려면 *subnet_prefix*/*prefix_length*를 지정합니다.
- *ipv6 network*/*prefix_length* — BGP가 알리는 네트워크입니다.

- (선택 사항) **route-map** *name* — 구성된 경로 맵의 식별자입니다. 알릴 네트워크를 필터링하려면 경로 맵을 검사해야 합니다. 지정하지 않으면 모든 네트워크를 광고합니다.

IPv6 재배포 설정 구성

이 섹션은 다른 라우팅 도메인의 경로로부터 BGP로 재배포하는 조건을 정의하기 위한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제**:**

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv6 [unicast]

예제**:**

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

단계 **3** 다른 라우팅 도메인의 경로를 BGP 자율 시스템으로 재배포:

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

예제**:**

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol — 경로를 재배포하는 소스 프로토콜. Connected, EIGRP, OSPF, RIP 또는 Static 중 하나가 될 수 있습니다.
- (선택 사항) process-id — ospf 프로토콜의 경우 이것은 경로가 재배포되는 적절한 OSPF 프로세스 ID입니다. 이것은 라우팅 프로세스를 식별합니다. 이 값은 0이 아닌 10진수 형태를 취합니다.

  참고 이 값은 다른 프로토콜에 대해 자동으로 채워집니다.

- (선택 사항) metric metric value — 특정 OSPF 프로세스에서 같은 라우터의 다른 OSPF 프로세스로 재배포할 때 메트릭 값을 지정하지 않은 경우 매트릭이 그대로 전달됩니다. OSPF 프로세스에

다른 프로세스를 재배포할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다. 기본값은 0입니다.

- (선택 사항) match internal | external1 | external2 | NSSA external 1 | NSSA external 2 — OSPF 경로가 다른 라우팅 도메인으로 재배포되는 기준. 다음 중 하나일 수 있습니다.
  - internal — 특정 자율 시스템의 내부 경로.
  - external 1 — 자율 시스템의 외부 경로이지만 OSPF 타입 1 외부 경로로서 BGP로 가져오는 경로.
  - external 2 — 자율 시스템의 외부 경로이지만 OSPF 타입 2 외부 경로로서 BGP로 가져오는 경로.
  - NSSA external 1 — 자율 시스템의 외부 경로이지만 OSPF NSSA 타입 1 외부 경로로서 BGP로 가져오는 경로.
  - NSSA external 2 — 자율 시스템의 외부 경로이지만 OSPF NSSA 타입 2 외부 경로로서 BGP로 가져오는 경로.
- (선택 사항) map-tag — 구성된 경로 맵의 식별자.

참고 재배포할 네트워크를 필터링하려면 경로 맵을 검사해야 합니다. 지정하지 않으면 모든 네트워크를 재배포합니다.

IPv6 경로 삽입 설정 구성

이 섹션에서는 BGP 라우팅 테이블에 조건부로 삽입할 경로를 정의하기 위한 단계를 설명합니다.

프로시저

단계 **1** BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp autonomous-num

예제:

```
ciscoasa(config)# router bgp 2
```

단계 **2** 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

address-family ipv6 [unicast]

예제:

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

단계 **3** 조건부 경로 삽입을 구성하여 BGP 라우팅 테이블로 더 많은 특정 경로를 삽입:

bgp inject-map inject-map exist-map exist-map [copy-attributes]

예제**:**

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map — 로컬 BGP 라우팅 테이블로 삽입할 접두사를 지정하는 경로 맵 이름.
- exist-map — BGP 스피커가 추적하는 접두사를 포함하는 경로 맵의 이름.
- (선택 사항) copy-attributes — 삽입된 경로가 종합 경로의 속성을 상속받도록 구성합니다.

BGP 모니터링

다음 명령을 사용하여 BGP 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조를 참고하십시오. 또한 네이버 변경 메시지 및 네이버 경고 메시지의 로깅을 비활성화할 수 있습니다.

다양한 BGP 라우팅 통계를 모니터링하려면 다음 명령 중 하나를 입력합니다.

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

  BGP 라우팅 테이블의 엔트리를 표시합니다.

- **show bgp** cidr-only

  비자연 네트워크 마스크가 있는 경로(CIDR, 즉 Classless Interdomain Routing)를 표시합니다.

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  지정된 BGP 커뮤니티에 속하는 경로를 표시합니다.

- **show bgp community-list community-list-name [exact-match]**

  BGP 커뮤니티 목록에서 허용하는 경로를 표시합니다.

- **show bgp filter-list** *access-list-number*

  지정된 필터 목록에 순응하는 경로를 표시합니다.

- **show bgp injected-paths**

  BGP 라우팅 테이블의 모든 삽입된 경로를 표시합니다.

- **show bgp ipv4 unicast**

  유니캐스트 세션에 대한 IPv4(IP version 4) BGP 라우팅 테이블의 엔트리를 표시합니다.

- show bgp ipv6 unicast

  IPv6 BGP(Border Gateway Protocol) 라우팅 테이블의 엔트리를 표시합니다.

- show bgp ipv6 community

  지정된 IPv6 BGP(Border Gateway Protocol) 커뮤니티에 속하는 경로를 표시합니다.

- show bgp ipv6 community-list

  IPv6 BGP(Border Gateway Protocol) 커뮤니티 목록에서 허용된 경로를 표시합니다.

- show bgp ipv6 filter-list

  지정된 IPv6 필터 목록에 순응하는 경로를 표시합니다.

- show bgp ipv6 inconsistent-as

  발신 자율 시스템이 일치하지 않는 IPv6 BGP(Border Gateway Protocol) 경로를 표시합니다.

- show bgp ipv6 neighbors

  네이버에 대한 IPv6 BGP(Border Gateway Protocol) 연결에 관한 정보를 표시합니다.

- show bgp ipv6 paths

  데이터베이스의 모든 IPv6 BGP(Border Gateway Protocol) 경로를 표시합니다.

- show bgp ipv6 prefix-list

  접두사 목록과 일치하는 경로를 표시합니다.

- show bgp ipv6 quote-regexp

  인용된 문자열로서 자율 시스템 정규식과 일치하는 IPv6 BGP(Border Gateway Protocol) 경로를 표시합니다.

- show bgp ipv6 regexp

  자율 시스템 경로 정규식과 일치하는 IPv6 BGP(Border Gateway Protocol) 경로를 표시합니다.

- show bgp ipv6 route-map

  라우팅 테이블에서 설치에 실패한 IPv6 BGP(Border Gateway Protocol) 경로를 표시합니다.

- show bgp ipv6 summary

  모든 IPv6 BGP(Border Gateway Protocol) 연결 상태를 표시합니다.

- show bgp neighbors ip_address

  네이버에 대한 BGP 및 TCP 연결에 관한 정보를 표시합니다.

- show bgp paths [LINE]

  데이터베이스의 모든 BGP 경로를 표시합니다.

- show bgp pending-prefixes

  삭제 대기 중인 접두사를 표시합니다.

- show bgp prefix-list prefix_list_name [WORD]

  지정된 접두사 목록과 일치하는 경로를 표시합니다.

- show bgp regexp regexp

  자율 시스템 경로 정규식과 일치하는 경로를 표시합니다.

- show bgp replication [index-group | ip-address]

  BGP 업데이트 그룹에 대한 업데이트 복제 통계를 표시합니다.

- show bgp rib-failure

  RIB(Routing Information Base) 테이블에서 설치에 실패한 BGP 경로를 표시합니다.

- show bgp route-map map-name

  지정된 경로 맵을 기반으로 BGP 라우팅 테이블에 엔트리를 입력합니다.

- show bgp summary

  모든 BGP 연결의 상태를 표시합니다.

- show bgp system-config

  다중 컨텍스트 모드에서 시스템 컨텍스트별 BGP 컨피그레이션을 표시합니다.

  이 명령은 다중 컨텍스트 모드의 모든 사용자 컨텍스트에서 이용 가능합니다.

- show bgp update-group

  BGP 업데이트 그룹에 대한 정보를 표시합니다.

참고 BGP 로그 메시지를 비활성화하려면 **no bgp log-neighbor-changes** 명령을 라우터 구성 모드에 입력합니다. 이는 네이버 변경 메시지 로깅을 비활성화합니다. 이 명령을 BGP 라우팅 프로세스에 대한 라우터 구성 모드에 입력합니다. 기본적으로 네이버 변경 사항은 기록됩니다.

BGP의 예

이 예는 다양한 프로세스 옵션으로 BGPv4를 활성화하고 구성하는 방법을 보여줍니다.

1. 하나의 라우팅 프로토콜에서 다른 프로토콜로 경로를 재배포하거나 정책 라우팅을 활성화하는 조건을 정의:

   ```
   ciscoasa(config)# route-map mymap2 permit 10
   ```

2. 경로 주소가 있거나 지정된 액세스 목록 중 하나로 통과한 패킷과 일치하는 경로를 재배포:

   ```
   ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
   ```

3. 정책 라우팅을 위해 경로 맵의 match 절을 통과하는 트래픽을 출력할 위치를 나타냅니다.

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4. 글로벌 컨피그레이션 모드에서 BGP 라우팅 프로세스를 활성화:

```
ciscoasa(config)# router bgp 2
```

5. 주소 제품군 컨피그레이션 모드에서 로컬 BGP(Border Gateway Protocol) 라우팅 프로세스에 대한 고정 라우터 ID를 컨피그레이션:

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. BGP 네이버 테이블에 엔트리 추가:

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7. 수신 또는 발신 경로에 경로 맵 적용:

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

이 예는 다양한 프로세스 옵션으로 BGPv6를 활성화하고 구성하는 방법을 보여줍니다.

1. 하나의 라우팅 프로토콜에서 다른 프로토콜로 경로를 재배포하거나 정책 라우팅을 활성화하는 조건을 정의:

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. 경로 주소가 있거나 지정된 액세스 목록 중 하나로 통과한 패킷과 일치하는 경로를 재배포:

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. 정책 라우팅을 위해 경로 맵의 match 절을 통과하는 트래픽을 출력할 위치를 나타냅니다.

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. 글로벌 컨피그레이션 모드에서 BGP 라우팅 프로세스를 활성화:

```
ciscoasa(config)# router bgp 2
```

5. 주소 제품군 컨피그레이션 모드에서 로컬 BGP(Border Gateway Protocol) 라우팅 프로세스에 대한 고정 라우터 ID를 컨피그레이션:

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 6(IPv6) 주소 접두사를 사용한 라우팅 세션 컨피그레이션:

```
address-family ipv6 [unicast]
```

7. BGP 네이버 테이블에 엔트리 추가:

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. 수신 또는 발신 경로에 경로 맵 적용:

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

BGP 기록

표 *32: BGP* 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
BGP 지원	9.2(1)	데이터 라우팅, 인증 수행, Border Gateway Protocol을 사용한 라우팅 정보 재배포 및 모니터링에 대한 지원이 추가되었습니다. 도입된 명령: **router bgp, bgp maxas-limit, bgp log-neighbor-changes, bgp transport path-mtu-discovery, bgp fast-external-fallover, bgp enforce-first-as, bgp asnotation dot, timers bgp, bgp default local-preference, bgp always-compare-med, bgp bestpath compare-routerid, bgp deterministic-med, bgp bestpath med missing-as-worst, policy-list, match as-path, match community, match metric, match tag, as-path access-list, community-list, address-family ipv4, bgp router-id, distance bgp, table-map, bgp suppress-inactive, bgp redistribute-internal, bgp scan-time, bgp nexthop, aggregate-address, neighbor, bgp inject-map, show bgp, show bgp cidr-only, show bgp all community, show bgp all neighbors, show bgp community, show bgp community-list, show bgp filter-list, show bgp injected-paths, show bgp ipv4 unicast, show bgp neighbors, show bgp paths, show bgp pending-prefixes, show bgp prefix-list, show bgp regexp, show bgp replication, show bgp rib-failure, show bgp route-map, show bgp summary, show bgp system-config, show bgp update-group, clear route network, maximum-path, network** 다음 명령을 수정했습니다. **show route**, **show route summary**, **show running-config router**, **clear config router**, **clear route all**, **timers lsa arrival**, **timers pacing**, **timers throttle**, **redistribute bgp**.

기능 이름	플랫폼 릴리스	기능 정보
ASA 클러스터링을 위한 BGP 지원	9.3(1)	L2 및 L3 클러스터링에 대한 지원을 추가했습니다. 다음 명령을 도입했습니다. bgp router-id clusterpool
NSF를 위한 BGP 지원	9.3(1)	무중단 전달을 위한 지원을 추가했습니다. 다음 명령을 도입했습니다. bgp graceful-restart, neighbor ha-mode graceful-restart
광고 맵을 위한 BGP 지원	9.3(1)	BGPv4 광고 맵 지원을 추가했습니다. 다음 명령을 도입했습니다. neighbor advertise-map
IPv6에 BGP 지원	9.3(2)	IPv6에 대한 지원을 추가했습니다. 다음 명령을 도입했습니다. address-family ipv6, ipv6 prefix-list, ipv6 prefix-list description, ipv6 prefix-list sequence-number, match ipv6 next-hop, match ipv6 route-source, match ipv6-address prefix-list, set ipv6-address prefix -list, set ipv6 next-hop, set ipv6 next-hop peer-address 다음 명령을 수정했습니다. bgp router-id
위임된 접두사에 대한 IPv6 네트워크 알림	9.6(2)	이제 ASA에서 DHCPv6 접두사 위임 클라이언트를 지원합니다. ASA가 DHCPv6 서버에서 위임된 접두사를 가져옵니다. 그런 다음 ASA는 이러한 접두사를 사용하여 SLAAC(Stateless Address Auto Configuration) 클라이언트가 동일한 네트워크에서 IPv6 주소를 자동으로 구성할 수 있도록 다른 ASA 인터페이스 주소를 구성할 수 있습니다. 이러한 접두사를 알리기 위해 BGP 라우터를 구성할 수 있습니다. 수정된 명령: **network**

29 장

OSPF

이 장에서는 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 데이터를 라우팅하고, 인증을 수행하고, 라우팅 정보를 재분배할 수 있도록 Cisco ASA를 구성하는 방법에 대해 설명합니다.

OSPF 정보

OSPF는 경로 선택 시 거리 벡터 대신 링크 상태를 사용하는 내부 게이트웨이 라우팅 프로토콜입니다. OSPF는 라우팅 테이블 업데이트가 아닌 링크 상태 광고를 전파합니다. 전체 라우팅 테이블 대신 LSA만 교환되므로, OSPF 네트워크는 RIP 네트워크보다 더 빠르게 통합될 수 있습니다.

OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터에는 동일한 링크 상태 데이터베이스가 포함되며, 여기에는 각 라우터의 사용 가능한 인터페이스 및 연결 가능한 네이버 목록이 있습니다.

RIP를 능가하는 OSPF의 장점은 다음과 같습니다.

- OSPF 링크 상태 데이터베이스 업데이트는 RIP 업데이트보다 전송되는 빈도가 낮으며, 링크 상태 데이터베이스는 천천히 업데이트되지 않고 오래된 정보의 기간이 만료되는 즉시 업데이트됩니다.

- 라우팅 결정은 비용을 기준으로 하며, 이는 특정 인터페이스 전체에 패킷을 전송하는 데 필요한 오버헤드를 나타낸 것입니다. ASA에서는 목적지까지의 홉 개수가 아닌 링크 대역폭을 기준으로 인터페이스의 비용을 계산합니다. 비용을 구성하여 선호하는 경로를 지정할 수 있습니다.

최단 경로 우선 알고리즘의 단점은 CPU 주기 및 메모리가 많이 필요하다는 점입니다.

ASA에서는 OSPF 프로토콜의 프로세스 2개를 다른 인터페이스 집합에서 동시에 실행합니다. 동일한 IP 주소를 사용하는 인터페이스가 있을 경우 2개의 프로세스를 실행하고자 할 수 있습니다(NAT 사용 시 이러한 인터페이스가 공존할 수 있으나, OSPF에서는 중복 주소를 허용하지 않음). 또는 내부에서 한 프로세스를 실행하고 외부에서 다른 프로세스를 실행한 다음, 두 프로세스 간의 경로 하위 집합을 재분배하고자 할 수 있습니다. 이 경우에도 마찬가지로, 사설 주소를 공용 주소에서 분리해야 할 수 있습니다.

경로를 다른 OSPF 라우팅 프로세스, RIP 라우팅 프로세스 또는 OSPF 지원 인터페이스에서 구성된 고정 및 연결된 경로의 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

ASA에서는 다음과 같은 OSPF 기능을 지원합니다.

- 영역 내, 영역 간 및 외부(유형 I 및 유형 II) 경로
- 가상 링크
- LSA 플러딩
- OSPF 패킷에 대한 인증(비밀번호 및 MD5 인증)
- ASA를 전용 라우터 또는 전용 백업 라우터로 구성. ASA는 ABR로 설정할 수도 있습니다.
- 스텁 영역 및 not-so-stubby 영역
- 영역 경계 라우터 유형 3 LSA 필터링

OSPF에서는 MD5 및 일반 텍스트 인접 디바이스 인증을 지원합니다. OSPF와 다른 프로토콜(예: RIP) 간의 경로 재분배 시 공격자가 라우팅 정보를 교란시키기 위해 이를 이용할 우려가 있으므로, 가능한 경우 모든 라우팅 프로토콜에 인증을 사용해야 합니다.

NAT를 사용하면 OSPF가 공용 및 사설 영역에서 가동되며, 주소 필터링이 필요한 경우 2개의 OSPF 프로세스를 실행해야 합니다. 하나는 공용 영역에 사용되는 프로세스이고 다른 하나는 사설 영역에서 사용되는 프로세스입니다.

여러 영역에 인터페이스가 있는 라우터는 ABR(영역 경계선 라우터)라고 합니다. OSPF를 사용하는 라우터와 다른 라우팅 프로토콜을 사용하는 라우터 간에 트래픽을 재분배하는 게이트웨이 역할을 수행하는 라우터를 ASBR(자동 시스템 경계 라우터)이라고 합니다.

ABR에서는 LSA를 사용하여 사용 가능한 경로에 대한 정보를 다른 OSPF 라우터로 전송합니다. ABR 유형 3 LSA 필터링을 사용할 경우, ABR 역할을 수행하는 ASA를 통해 별도의 사설 및 공용 영역을 확보할 수 있습니다. 유형 3 LSA(영역 간 경로)는 한 영역에서 다른 영역으로 필터링할 수 있으며, 이렇게 하면 사설 네트워크를 알리지 않고도 NAT와 OSPF를 함께 사용할 수 있습니다.

참고 유형 3 LSA만 필터링할 수 있습니다. 사설 네트워크에서 ASA를 ASBR로 구성하면 사설 네트워크를 설명하는 유형 5 LSA가 전송되며, 이 경우 공용 영역을 비롯한 전체 AS에 플러딩이 발생합니다.

NAT가 적용되었으나 공용 영역에서 OSPF만 실행 중인 경우, 공용 네트워크에 대한 경로가 사설 네트워크 내부에 기본 또는 유형 5 AS 외부 LSA로서 재배포될 수 있습니다. 그러나 ASA에서 보호하는 사설 네트워크에 대한 고정 경로를 구성해야 합니다. 또는 동일한 ASA 인터페이스에서 공용 네트워크와 사설 네트워크를 혼합할 수 없습니다.

ASA에서 하나는 RIP 라우팅 프로세스, 다른 하나는 EIGRP 라우팅 프로세스로 된 2개의 OSPF 라우팅 프로세스를 동시에 실행할 수 있습니다.

Fast Hello 패킷에 대한 OSPF 지원

OSPF의 Fast Hello 패킷 지원 기능에서는 hello 패킷을 1초 미만의 간격으로 전송하도록 구성하는 방법을 제공합니다. 이러한 컨피그레이션을 통해 OSPF(Open Shortest Path First) 네트워크에서 통합 속도를 단축할 수 있습니다.

OSPF의 Fast Hello 패킷 지원 사전 요구 사항

OSPF는 네트워크에서 기존에 구성해야 하거나 OSPF의 Fast Hello 패킷 지원 기능과 동시에 구성해야 합니다.

Fast Hello 패킷에 대한 OSPF 지원 정보

Fast Hello 패킷에 대한 OSPF 지원과 관련된 핵심 개념과 OSPF Fast Hello 패킷의 이점이 아래에 설명되어 있습니다.

OSPF Hello 간격 및 Dead 간격

OSPF Hello 패킷은 OSPF 프로세스에서 OSPF 네이버와의 연결을 유지하기 위해 이러한 네이버에 전송하는 패킷입니다. Hello 패킷은 구성 가능한 간격(초 단위)으로 전송됩니다. 기본값은 이더넷 링크의 경우 10초이고, 비 브로드캐스트 링크의 경우 30초입니다. Hello 패킷에는 Dead 간격 내에 수신된 Hello 패킷에 대한 모든 네이버 목록이 포함됩니다. Dead 간격도 구성 가능한 간격(초 단위)이며, 기본값은 Hello 간격 값의 4배로 설정됩니다. 모든 Hello 간격의 값은 네트워크 내에서 동일해야 합니다. 마찬가지로, 모든 Dead 간격의 값도 네트워크 내에서 동일해야 합니다.

이러한 두 간격의 상호 작용을 통해 링크가 작동 중임을 나타내어 연결을 유지할 수 있습니다. 라우터가 Dead 간격 내에 네이버에서 Hello 패킷을 수신하지 못할 경우, 해당 네이버는 중단된 것으로 선언됩니다.

OSPF Fast Hello 패킷

OSPF Fast Hello 패킷은 1초 미만의 간격으로 전송되는 Hello 패킷을 참조합니다. Fast Hello 패킷에 대한 내용을 이해하려면 OSPF Fast Hello 패킷과 Dead 간격 간의 관계에 대해서도 숙지해야 합니다. OSPF Hello 간격 및 Dead 간격, 899 페이지를 참조하십시오.

OSPF Fast Hello 패킷 기능은 ospf dead-interval 명령을 사용하여 구현할 수 있습니다. Dead 간격은 1초로 설정되고, hello 승수 값은 1초 동안 전송하려는 Hello 패킷의 수로 설정되므로 1초 미만의 또는 "빠른" Hello 패킷이 제공됩니다.

Fast Hello 패킷이 인터페이스에서 구성되면, 이 인터페이스로 전송되는 Hello 패킷에서 광고되는 Hello 간격은 0으로 설정됩니다. 이 인터페이스를 통해 수신되는 Hello 패킷의 Hello 간격은 무시됩니다.

1초로 설정하든(Fast Hello 패킷의 경우) 다른 값으로 설정하든 Dead 간격은 세그먼트에서 일정해야 합니다. Hello 승수의 경우에는 Dead 간격 내에 최소 하나 이상의 Hello 패킷이 전송된다면 전체 세그먼트에서 동일하지 않아도 됩니다.

OSPF Fast Hello 패킷 기능의 이점

OSPF Fast Hello 패킷 기능의 이점은 OSPF 네트워크에서 Fast Hello 패킷을 사용하지 않는 경우와 비교했을 때 더 빠른 통합이 가능하다는 점입니다. 이 기능을 사용하면 1초 내에 손실된 네이버를 감지할 수 있습니다. 이 기능은 특히 OSI(Open System Interconnection) 물리적 레이어 및 데이터 링크 레이어로 감지할 수 없는 네이버가 손실된 LAN 세그먼트에 유용합니다.

OSPFv2와 OSPFv3의 구현 차이점

OSPFv3는 이전 버전인 OSPFv2와 호환되지 않습니다. OSPF를 사용하여 IPv4와 IPv6 트래픽을 모두 라우팅하려면 OSPFv2와 OSPFv3를 동시에 실행해야 합니다. 이들은 서로 공존하지만 상호 작용을 수행하지는 않습니다.

OSPFv3에서 제공하는 추가 기능은 다음과 같습니다.

- 링크당 프로토콜 처리
- 주소 지정 시맨틱 제거
- 플러딩 범위 추가
- 링크당 다중 인스턴스 지원
- IPv6 링크-로컬 주소를 사용하여 네이버 검색 및 기타 기능 지원
- LSA를 접두사와 접두사 길이로 표시
- LSA 유형 2개 추가
- 알 수 없는 LSA 유형 처리
- RFC-4552에 지정된 대로, OSPFv3 라우팅 프로토콜 트래픽에 IPsec ESP 표준을 사용한 인증 지원

OSPF에 대한 지침

상황 모드 지침

OSPFv2에서는 단일 또는 다중 상황 모드를 지원합니다.

- OSPFv2 인스턴스는 기본적으로 멀티캐스트 트래픽의 상황 간 교환이 공유 인터페이스에서 지원되지 않기 때문에 공유 인터페이스에서 서로 인접 관계를 형성할 수 없습니다. 그러나 공유 인터페이스에서 OSPFv2 네이버 관계를 가져오기 위해 OSPFv2 프로세스의 OSPFv2 프로세서 구성에서 고정 네이버 구성을 사용할 수 있습니다.
- 별도 인터페이스에서의 상황 간 OSPFv2가 지원됩니다.

OSPFv3에서는 단일 모드만 지원합니다.

방화벽 모드 지침

OSPF에서는 라우팅 방화벽 모드만 지원합니다. OSPF에서는 투명 방화벽 모드를 지원하지 않습니다.

장애 조치 지침

OSPFv2 및 OSPFv3는 스테이트풀 장애 조치를 지원합니다.

IPv6 지침

- OSPFv2에서는 IPv6을 지원하지 않습니다.
- OSPFv3에서는 IPv6을 지원합니다.
- OSPFv3에서는 인증에 IPv6을 사용합니다.
- ASA에서는 OSPFv3 경로가 최상의 경로인 경우, 이를 IPv6 RIB에 설치합니다.
- OSPFv3 패킷은 **capture** 명령에서 IPv6 ACL을 사용하여 필터링할 수 있습니다.

클러스터링 지침

- OSPFv3 암호화는 지원되지 않습니다. 클러스터링 환경에서 OSPFv3 암호화를 구성하려고 할 경우 오류 메시지가 표시됩니다.
- Spanned 인터페이스 모드의 경우, 동적 라우팅은 관리 전용 인터페이스에서 지원되지 않습니다.
- 개별 인터페이스 모드의 경우, 마스터 및 슬레이브 유닛을 OSPFv2 또는 OSPFv3 네이버로 설정해야 합니다.
- 개별 인터페이스 모드의 경우, OSPFv2 인접성은 마스터 유닛의 공유 인터페이스에 있는 두 상황 간에만 설정할 수 있습니다. 고정 네이버 구성은 포인트-투-포인트 링크에서만 지원되므로, 하나의 인터페이스에서는 하나의 네이버 명령문만 허용됩니다.
- 클러스터에서 마스터 역할이 변경될 경우, 다음 동작이 발생합니다.

- Spanned 인터페이스 모드의 경우, 라우터 프로세스는 마스터 유닛에서만 액티브 상태이며 슬레이브 유닛에서는 일시 중단 상태입니다. 마스터 유닛에서 컨피그레이션이 동기화되었으므로 각 클러스터 유닛에서는 동일한 라우터 ID를 보유하게 됩니다. 결과적으로, 인접한 라우터에서는 역할이 변경되는 동안 클러스터의 라우터 ID 변경을 알 수 없습니다.
- 개별 인터페이스 모드의 경우 라우터 프로세스는 모든 개별 클러스터 유닛에서 액티브 상태입니다. 각 클러스터 유닛에서는 구성된 클러스터 풀에서 고유한 개별 라우터 ID를 선택합니다. 클러스터에서 마스터 권한 역할이 변경되어도 라우팅 토폴로지는 변경되지 않습니다.

MPLS(Multiprotocol Label Switching) 및 OSPF 지침

MPLS 구성 라우터가 MPLS 헤더를 포함하는 불투명 Type-10 링크 상태 알림(LSA)이 포함된 링크 상태(LS) 업데이트 패킷을 전송하는 경우, 인증이 실패하고 어플라이언스가 이를 승인하지 않고 자동으로 업데이트 패킷을 삭제합니다. 결국 피어 라우터가 승인을 받지 않았기 때문에 피어 라우터는 네이버 관계를 종료합니다.

네이버 관계를 안정적으로 유지하려면 ASA에서 불투명 기능을 비활성화합니다.

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

추가 지침

- OSPFv2 및 OSPFv3에서는 하나의 인터페이스에 여러 인스턴스를 지원합니다.
- OSPFv3에서는 클러스터링되지 않은 환경에서 ESP 헤더를 통해 암호화를 지원합니다.
- OSPFv3에서는 Non-Payload Encryption을 지원합니다.
- OSPFv2에서는 RFCs 4811, 4812 및 3623에서 각각 정의된 대로 Cisco NSF Graceful Restart 및 IETF NSF Graceful Restart 메커니즘을 지원합니다.
- OSPFv3에서는 RFC 5187에 정의된 대로 Graceful Restart 메커니즘을 지원합니다.
- 배포될 수 있는 내부 영역(유형 1) 경로의 수에는 제한이 있습니다. 이러한 경로의 경우, 단일 유형-1 LSA는 모든 접두사를 포함합니다. 시스템에서 패킷 크기에 35KB의 제한이 있으므로 3000개의 경로로 인해 패킷이 제한을 초과합니다. 2900개의 유형 1 경로를 지원되는 최대 수로 간주하십시오.

OSPFv2 구성

이 섹션에서는 ASA에서 OSPFv2 프로세스를 활성화하는 방법을 설명합니다.

OSPFv2를 활성화한 후에는 경로 맵을 정의해야 합니다. 자세한 내용은 경로 맵 정의, 839 페이지를 참조하십시오. 그런 다음 기본 경로를 생성합니다. 자세한 내용은 고정 경로 구성, 817 페이지를 참조하십시오.

OSPFv2 프로세스의 경로 맵을 정의한 후에는 특정한 요구 사항에 맞게 이를 맞춤화할 수 있습니다. ASA에서 OSPFv2 프로세스를 맞춤화하는 방법을 알아보려면 OSPFv2 사용자 지정, 905 페이지의 내용을 참조하십시오.

OSPFv2를 활성화하려면 OSPFv2 라우팅 프로세스를 생성한 후 라우팅 프로세스와 관련된 IP 주소 범위를 지정한 다음, 해당 IP 주소 범위와 관련된 영역 ID를 할당해야 합니다.

최대 2개의 OSPFv2 프로세스 인스턴스를 활성화할 수 있습니다. 각 OSPFv2 프로세스에는 고유한 관련 영역 및 네트워크가 있습니다.

OSPFv2를 활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제**:**

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

ASA에서 OSPF 프로세스가 하나만 활성화된 경우, 해당 프로세스가 기본적으로 선택됩니다. 기존 영역을 편집할 경우 OSPF 프로세스 ID를 변경할 수 없습니다.

단계 **2** OSPF가 실행되는 IP 주소 및 해당 인터페이스의 영역 ID를 정의합니다.

network *ip_address mask* **area** *area_id*

예제**:**

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

새 영역을 추가할 경우 영역 ID를 입력합니다. 영역 ID는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다. 기존 영역을 편집할 경우 영역 ID를 변경할 수 없습니다.

OSPFv2 라우터 ID 구성

OSPF 라우터 ID는 OSPF 데이터베이스 내에서 특정 디바이스를 식별하는 데 사용됩니다. OSPF 시스템에서는 두 개의 라우터가 동일한 라우터 id를 가질 수 없습니다.

OSPF 라우팅 프로세스에서 라우터 id가 수동으로 구성되지 않은 경우, 라우터는 논리적 인터페이스(루프백 인터페이스)의 가장 높은 IP 주소 또는 액티브 인터페이스의 가장 높은 IP 주소에서 확인된 라우터 id를 자동으로 구성합니다. 라우터 id를 구성할 때 라우터가 실패했거나 OSPF 프로세스가 지워지고 네이버 관계가 다시 설정될 때까지 네이버는 자동으로 업데이트되지 않습니다.

OSPF 라우터 ID 수동 구성

이 섹션에서는 ASA의 OSPFv2 프로세스에서 라우터 id를 수동으로 구성하는 방법을 설명합니다.

프로시저

단계 **1** 고정된 라우터 ID를 사용하려면 **router-id** 명령을 사용합니다.

router-id *ip-address*

예제:

```
ciscoasa(config-router)# router-id 193.168.3.3
```

단계 **2** 이전 OSPF 라우터 ID 동작으로 되돌리려면 **no router-id** 명령을 사용합니다.

no router-id *ip-address*

예제:

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

마이그레이션 시 라우터 ID 동작

하나의 ASA에서 OSPF 구성을 마이그레이션하는 동안 ASA 1을 다른 ASA라고 언급하고 ASA 2를 언급하면 다음 라우터 id 선택 동작이 관찰됩니다.

1. ASA 2는 모든 인터페이스가 종료 모드일 때 OSPF 라우터 id에 대한 임의의 IP 주소를 사용하지 않습니다. 모든 인터페이스가 "admin down(관리자 중단)" 상태이거나 종료 모드일 때 라우터 id를 구성할 가능성은 다음과 같습니다.
   - ASA 2에 이전에 구성된 라우터 id가 없는 경우, 이 메시지를 볼 수 있습니다.

     ```
     %OSPF: 라우터 프로세스 1이 실행 중이 아닙니다. 라우터 id를 구성하십시오.
     ```

     첫 번째 인터페이스를 불러온 후에 ASA 2는 이 인터페이스의 IP 주소를 라우터 id로 사용합니다.
   - 이전에 ASA 2에 라우터 id가 구성되어 있었고 "no router-id" 명령이 발행되었을 때 모든 인터페이스가 "admin down(관리자 중단)" 상태였던 경우, ASA 2는 이전 라우터 id를 사용합니다. ASA 2는 불러온 인터페이스의 IP 주소가 변경된 경우에도 "clear ospf process" 명령이 발행될 때까지 이전 라우터 id를 사용합니다.

2. 이전에 ASA 2에 라우터 id가 구성되어 있었고 "no router-id" 명령이 발행되었을 때 인터페이스 중 1개 이상이 "admin down(관리자 중단)" 상태 또는 종료 모드에 있지 않았던 경우 ASA 2는 새 라우터 id를 사용합니다. ASA 2는 인터페이스가 "down/down(중단/중단)" 상태인 경우에도 인터페이스의 IP 주소의 새 라우터 id를 사용합니다.

OSPF Fast Hello 패킷 구성

이 섹션에서는 OSPF Fast Hello 패킷 기능을 구성하는 방법에 대해 설명합니다.

프로시저

단계 **1** 인터페이스를 구성합니다.

interface *port-channel number*

예제**:**

```
ciscoasa(config)# interface port-channel 10
```

number 인수는 포트 채널 인터페이스 수를 나타냅니다.

단계 **2** 최소 하나 이상의 hello 패킷이 수신되어 간격을 설정합니다. 아니면 수신되지 않을 경우 해당 네이버는 중단된 것으로 간주됩니다.

ospf dead-interval minimal hello-multiplier *no.of times*

예제**:**

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
ciscoasa
```

no. of times 인수는 1초마다 전송되는 Hello 패킷의 수를 나타냅니다. 유효한 값은 3 ~ 20입니다.

이 예에서는 최소 키워드 및 hello 승수 키워드와 값을 지정하여 OSPF Support for Fast Hello Packets가 활성화되어 있습니다. 승수가 5로 설정되어 있으므로 5개의 Hello 패킷이 1초마다 전송됩니다.

OSPFv2 사용자 지정

이 섹션에서는 OSPFv2 프로세스를 사용자 정의하는 방법에 대해 설명합니다.

OSPFv2에 경로 재배포

ASA에서는 OSPFv2 라우팅 프로세스 간의 경로 재배포를 제어할 수 있습니다.

참고 지정된 라우팅 프로토콜에서 어떤 경로를 대상 라우팅 프로세스로 재분배할 수 있는지 정의하여 경로를 재분배하려면, 우선 기본 경로를 생성해야 합니다. 고정 경로 구성, 817 페이지를 참조한 다음 경로 맵 정의, 839 페이지에 따라 경로 맵을 정의합니다.

고정 경로, 연결된 경로, RIP 또는 OSPFv2 경로를 OSPFv2 프로세스에 재분배하려면 다음 단계를 수행합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 연결된 경로를 OSPF 라우팅 프로세스에 재분배합니다.

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예제:

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

단계 **3** 고정 경로를 OSPF 라우팅 프로세스에 재분배합니다.

redistribute static [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*

예제:

```
ciscoasa(config)# redistribute static 5 type-1 route-map-practice
```

단계 **4** OSPF 라우팅 프로세스의 경로를 다른 OSPF 라우팅 프로세스에 재분배합니다.

redistribute ospf pid [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예제:

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
```

```
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

이 명령에서 **match** 옵션을 사용하여 경로 속성을 일치시키고 설정하거나, 경로 맵을 사용할 수 있습니다. **subnets** 옵션에는 **route-map** 명령과 동일한 항목이 없습니다. **redistribute** 명령에서 경로 맵과 **match** 옵션을 모두 사용할 경우 두 가지가 일치해야 합니다.

이 예에는 경로의 메트릭을 1로 일치시켜 OSPF 프로세스 1에서 OSPF 프로세스 2로 경로 재분배를 수행하는 경우가 나와 있습니다. ASA에서는 이러한 경로를 메트릭이 5이고 메트릭 유형이 Type 1인 외부 LSA로서 재배포합니다.

단계 **5** RIP 라우팅 프로세스의 경로를 OSPF 라우팅 프로세스에 재분배합니다.

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예제**:**

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

단계 **6** EIGRP 라우팅 프로세스의 경로를 OSPF 라우팅 프로세스에 재분배합니다.

redistribute eigrp as-num [**metric** *metric-value*] [**metric-type**{**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예제**:**

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

경로를 OSPFv2로 재배포 시 경로 요약 구성

다른 프로토콜의 경로가 OSPF에 재분배될 경우, 각 경로는 외부 LSA에 개별적으로 광고됩니다. 그러나 ASA를 구성하여 지정된 네트워크 주소 및 마스크에 포함되는 모든 재배포된 경로에 대한 단일 경로를 알릴 수 있습니다. 이렇게 구성하면 OSPF 링크 상태 데이터베이스의 크기가 줄어듭니다.

지정된 IP 주소 마스크 쌍과 일치하는 경로는 억제할 수 있습니다. 태그 값을 일치 값으로 사용하여 경로 맵을 통한 재분배를 제어할 수 있습니다.

경로 요약 주소 추가

네트워크 주소 및 마스크에 포함되는 모든 재분배 경로의 단일한 요약 경로에 대한 소프트웨어 광고를 구성하려면, 다음 단계를 수행합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제**:**

```
ciscoasa(config)# router ospf 1
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 요약 주소를 설정합니다.

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

예제**:**

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

이 예에서 요약 주소 10.1.0.0에는 10.1.1.0, 10.1.2.0, 10.1.3.0 등의 주소가 포함됩니다. 10.1.0.0 주소만 외부 링크 상태 광고에서 광고됩니다.

OSPFv2 영역 간의 경로 요약 구성

경로 요약은 광고된 주소를 통합하는 작업입니다. 이 기능을 사용하면 영역 경계 라우터에 의해 하나의 요약 경로를 다른 영역으로 광고됩니다. OSPF의 경우, 영역 경계 라우터에서는 하나의 영역에 있는 네트워크를 다른 영역으로 광고합니다. 영역에 네트워크 번호가 어느 정도 할당되어 있고 번호가 연속적일 경우, ABR을 구성하여 지정된 범위에 속하는 영역 내의 모든 개별 네트워크가 포함된 요약 경로를 광고할 수 있습니다.

경로 요약을 위한 주소 범위를 정의하려면 다음 단계를 수행합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성하고 이 OSPF 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 1
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자입니다. 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 주소 범위를 설정합니다.

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

예제:

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

이 예에서 주소 범위는 OSPF 영역 사이의 범위로 설정됩니다.

OSPFv2 인터페이스 파라미터 구성

필요한 경우 일부 인터페이스별 OSPFv2 매개변수를 변경할 수 있습니다. 이러한 파라미터는 변경할 필요가 없지만 **ospf hello-interval**, **ospf dead-interval**, **ospf authentication-key** 같은 인터페이스 파라미터는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 컨피그레이션할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

OSPFv2 인터페이스 매개변수를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPF가 실행되는 IP 주소 및 해당 인터페이스의 영역 ID를 정의합니다.

network *ip_address mask* **area** *area_id*

예제:

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

단계 **3** 인터페이스 컨피그레이션 모드를 시작합니다.

interface *interface_name*

예제**:**

```
ciscoasa(config)# interface my_interface
```

단계 **4** 인터페이스의 인증 유형을 지정합니다.

ospf authentication [**message-digest** | **null**]

예제**:**

```
ciscoasa(config-interface)# ospf authentication message-digest
```

단계 **5** OSPF 단순 비밀번호 인증을 사용하는 네트워크 세그먼트의 인접한 OSPF 라우터에서 사용할 비밀번호를 할당합니다.

ospf authentication-key *key*

예제**:**

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

key 인수는 최대 8바이트 길이의 연속된 문자열을 사용할 수 있습니다.

이 명령으로 생성된 비밀번호는 ASA 소프트웨어에서 라우팅 프로토콜 패킷을 시작할 때 OSPF 헤더에 직접 삽입되는 키로 사용됩니다. 인터페이스 하나당 각 네트워크에 별도의 비밀번호를 할당할 수 있습니다. 동일한 네트워크의 모든 인접한 라우터에는 OSPF 정보를 교환할 수 있는 동일한 비밀번호가 있어야 합니다.

단계 **6** OSPF 인터페이스에서 패킷을 전송하는 비용을 명시적으로 지정합니다.

ospf cost *cost*

예제**:**

```
ciscoasa(config-interface)# ospf cost 20
```

*cost*는 1 ~ 65535의 정수입니다.

이 예에서 비용은 20으로 설정되었습니다.

단계 **7** Hello 패킷이 수신되지 않는 네이버 OSPF 라우터를 중단된 라우터로 선언하기 전까지 디바이스가 대기해야 하는 시간을 초 단위로 설정합니다.

ospf dead-interval *seconds*

예제**:**

```
ciscoasa(config-interface)# ospf dead-interval 40
```

이 값은 네트워크의 모든 노드에서 동일해야 합니다.

단계 **8** OSPF 인터페이스의 ASA에서 전송하는 Hello 패킷 간의 시간을 지정합니다.

ospf hello-interval *seconds*

예제**:**

```
ciscoasa(config-interface)# ospf hello-interval 10
```

이 값은 네트워크의 모든 노드에서 동일해야 합니다.

단계 **9** OSPF MD5 인증을 활성화합니다.

ospf message-digest-key *key_id* md5 *key*

예제**:**

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

다음 인수 값을 설정할 수 있습니다.

key_id — 1 ~ 255 범위의 식별자입니다.

key — 최대 16바이트로 된 영숫자 비밀번호입니다.

일반적으로 인터페이스당 키 1개를 사용하여 패킷 전송 시 인증 정보를 생성하고 수신 패킷을 인증합니다. 네이버 라우터의 동일한 키 식별자에는 동일한 키 값이 있어야 합니다.

인터페이스당 여러 개의 키를 유지하는 것이 좋습니다. 새 키를 추가할 때마다 기존 키를 제거하여 로컬 시스템이 기존 키를 알고 있는 악성 시스템과 계속 통신을 수행하지 않도록 방지해야 합니다. 기존 키를 제거하면 롤오버 동안의 오버헤드도 감소합니다.

단계 **10** 네트워크에 대한 OSPF 전용 라우터를 결정하는 데 도움이 되는 우선 순위를 설정합니다.

ospf priority *number_value*

예제**:**

```
ciscoasa(config-interface)# ospf priority 20
```

number_value 인수의 범위는 0~255입니다.

단계 **11** OSPF 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다.

ospf retransmit-interval *seconds*

예제**:**

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds 값은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 범위는 1초 ~ 8192초입니다. 기본값은 5초입니다.

단계 **12** OSPF 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 설정합니다.

ospf transmit-delay *seconds*

예제:

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds 값의 범위는 1초 ~ 8192초입니다. 기본값은 1초입니다.

단계 **13** 1초 동안 전송되는 Hello 패킷의 수를 설정합니다.

ospf dead-interval minimal hello-interval multiplier

예제:

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

유효한 값은 3 ~ 20의 정수입니다.

단계 **14** 인터페이스를 포인트-투-포인트 비 브로드캐스트 네트워크로 지정합니다.

ospf network point-to-point non-broadcast

예제:

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

인터페이스를 포인트-투-포인트 및 비 브로드캐스트로 지정할 경우, OSPF 네이버를 수동으로 정의해야 합니다. 동적 네이버 검색은 지원되지 않습니다. 자세한 내용은 고정 OSPFv2 인접 디바이스 정의, 916 페이지를 참조하십시오. 또한 해당 인터페이스에서는 하나의 OSPF 네이버만 정의할 수 있습니다.

OSPFv2 영역 파라미터 구성

일부 OSPF 영역 매개변수를 구성할 수 있습니다. 이러한 영역 매개변수(다음 작업 목록에 나와 있음)에는 인증 설정, 스텁 영역 정의, 기본 요약 경로에 특정 비용 할당이 포함됩니다. 인증에서는 영역에 무단 액세스를 차단하는 비밀번호 기반의 보호 기능을 제공합니다.

스텁 영역은 외부 경로에 대한 정보가 전송되지 않는 영역입니다. 그 대신, 스텁 영역에는 ABR에서 생성된 기본 외부 경로가 있으며 이는 자동 시스템 외부의 목적지를 위한 경로입니다. OSPF 스텁 영역 지원을 사용하려면 스텁 영역에서 기본 라우팅을 사용해야 합니다. 스텁 영역에 전송되는 LSA의 수를 더 줄이려면, ABR에서 **area stub** 명령의 **no-summary** 키워드를 사용하여 요약 링크 광고(LSA Type 3)가 스텁 영역에 전송되지 않도록 할 수 있습니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPF 영역에 인증 활성화

area *area-id* authentication

예제:

```
ciscoasa(config-rtr)# area 0 authentication
```

단계 **3** OSPF 영역에 MD5 인증 활성화

area *area-id* authentication message-digest

예제:

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

OSPFv2 필터 규칙 구성

OSPF 업데이트에서 수신 또는 전송된 경로 또는 네트워크를 필터링하려면 다음 절차를 수행합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 활성화하여 라우터 구성 모드로 들어갑니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

단계 **2** 수신 OSPF 업데이트에서 수신되었거나 발신 OSPF 업데이트에서 알려진 경로나 네트워크를 필터링합니다.

distribute-list *acl-number* **in** [**interface** *ifname*]

distribute-list *acl-number* **out** [*protocol process-number* | **connected** | **static**]

acl-number 인수는 IP 액세스 목록 번호를 지정합니다. 액세스 목록은 라우팅 업데이트에서 어떤 네트워크를 수신하고 어떤 네트워크를 억제할지 정의합니다.

수신 업데이트에 필터를 적용하려면 **in**을 지정합니다. 해당 인터페이스에서 수신되는 업데이트로 필터를 제한하도록 인터페이스를 선택적으로 지정할 수 있습니다.

아웃바운드 업데이트에 필터를 적용하려면 **out**을 지정합니다. 배포 목록에 적용할 프로세스 번호(RIP용 제외)로 선택적으로 프로토콜(**bgp**, **eigrp**, **ospf** 또는 **rip**)을 지정할 수 있습니다. 피어와 네트워크를 **connected** 또는 **static** 경로를 통해 확인했는지 여부를 필터링할 수도 있습니다.

예제:

```
ciscoasa(config-rtr)# distribute-list ExampleAcl in interface inside
```

OSPFv2 NSSA 구성

NSSA의 OSPFv2 구현은 OSPFv2 스텁 영역과 비슷합니다. NSSA의 경우 코어의 Type 5 외부 LSA를 영역으로 플러딩하지 않으나, 제한된 방식을 통해 자동 시스템 외부 경로를 영역 내로 가져올 수 있습니다.

NSSA는 재분배를 통해 Type 7 자동 시스템 외부 경로를 NSSA 영역 내로 가져옵니다. 이러한 Type 7 LSA는 NSSA ABR에 의해 Type 5 LSA로 변환되며, 이는 전체 라우팅 도메인에 걸쳐 플러딩됩니다. 변환이 이루어지는 동안 요약 및 필터링이 지원됩니다.

OSPFv2를 사용하는 중앙 사이트를 다른 라우팅 프로토콜을 사용하는 원격 사이트에 연결해야 하는 ISP 또는 네트워크 관리자의 경우 NSSA를 통해 관리 작업을 간소화할 수 있습니다.

NSSA를 구현하기 전에는, 원격 사이트의 경로를 스텁 영역으로 재분배할 수 없었고 2개의 라우팅 프로토콜을 유지해야 했기 때문에 기업 사이트 경계선 라우터와 원격 라우터 간의 연결을 OSPFv2 스텁 영역으로 실행할 수 없었습니다. 일반적으로 RIP 같은 단순 프로토콜을 실행하여 재분배를 처리했습니다. NSSA를 활용할 경우, 기업 라우터와 원격 라우터 간의 영역을 NSSA로 정의함으로써 OSPFv2를 확장하여 원격 연결을 지원할 수 있습니다.

이 기능을 사용하기 전에 다음 지침을 고려하십시오.

- 외부 목적지에 도착하는 데 사용할 Type 7 기본 경로를 설정할 수 있습니다. 구성된 경우, 라우터에서는 Type 7 기본값을 NSSA 또는 NSSA 영역 경계 라우터에 생성합니다.
- 동일한 영역 내의 모든 라우터는 해당 영역을 NSSA로 인식해야 합니다. 그렇지 않을 경우 라우터 간에 서로 통신을 수행할 수 없습니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자입니다. 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** NSSA 영역을 정의합니다.

area *area-id* nssa [**no-redistribution**] [**default-information-originate**]

예제:

```
ciscoasa(config-rtr)# area 0 nssa
```

단계 **3** 요약 주소를 설정하고 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

예제:

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

OSPF에 요약 경로를 사용하면 OSPF ASBR에서는 단일한 외부 경로를 해당 주소에서 다루는 모든 재분배 경로의 취합본으로 광고하게 됩니다.

이 예에서 요약 주소 10.1.0.0에는 10.1.1.0, 10.1.2.0, 10.1.3.0 등의 주소가 포함됩니다. 10.1.0.0 주소만 외부 링크 상태 광고에서 광고됩니다.

참고 OSPF에서는 요약 주소 0.0.0.0 0.0.0.0을 지원하지 않습니다.

클러스터링(OSPFv2 및 OSPFv3)에 대한 IP 주소 풀 구성

개별 인터페이스 클러스터링을 사용할 경우 라우터 ID 클러스터 풀에 대한 IPv4 주소의 범위를 할당할 수 있습니다.

OSPFv2 및 OSPFv3를 지원하는 개별 인터페이스 클러스터링에서 라우터 ID 클러스터 풀에 대한 IPv4 주소의 범위를 할당하려면 다음 명령을 입력합니다.

프로시저

개별 인터페이스 클러스터링에 대한 라우터 ID 클러스터 풀을 지정합니다.

router-id cluster-pool hostname | A.B.C.D ip_pool

예제:

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

cluster-pool 키워드를 사용하면 개별 인터페이스 클러스터링이 컨피그레이션될 때 IP 주소 풀을 컨피그레이션할 수 있습니다. **hostname** | **A.B.C.D.** 키워드는 이 OSPF 프로세스에 대한 OSPF 라우터 ID를 지정합니다. *ip_pool* 인수는 IP 주소 풀의 이름을 지정합니다.

참고 클러스터링을 사용할 경우, 라우터 ID에 대한 IP 주소를 지정할 필요가 없습니다. IP 주소 풀을 구성하지 않으면 ASA에서는 자동으로 생성된 라우터 ID를 사용합니다.

고정 OSPFv2 인접 디바이스 정의

고정 OSPFv2 네이버를 정의하여 포인트-투-포인트 비 브로드캐스트 네트워크를 통해 OSPFv2 경로를 광고할 수 있습니다. 이 기능을 사용하면 GRE 터널에 광고를 캡슐화하지 않고도 기존 VPN 연결 전체에 OSPFv2 광고를 브로드캐스트할 수 있습니다.

시작하기 전에, OSPFv2 네이버에 대한 고정 경로를 생성해야 합니다. 고정 경로 생성에 대한 자세한 내용은 고정 경로 구성, 817 페이지을 참조하십시오.

프로시저

단계 **1** OSPFv2 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPFv2 네이버 정의

neighbor *addr* [**interface** if_name]

예제:

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

addr 인수는 OSPFv2 네이버의 IP 주소입니다. *if_name* 인수는 네이버와 통신을 수행하는 데 사용되는 인터페이스입니다. OSPFv2 네이버가 직접 연결된 인터페이스와 동일한 네트워크에 있지 않을 경우, 인터페이스를 지정해야 합니다.

경로 계산 타이머 구성

OSPFv2에서 토폴로지 변경을 수신하는 시간과 SPF 계산을 시작하는 시간 사이의 지연 시간을 구성할 수 있습니다. 두 번 연속으로 SPF를 계산하는 작업 사이의 대기 시간을 구성할 수도 있습니다.

프로시저

단계 **1** OSPFv2 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제**:**

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 경로 계산 시간을 구성합니다.

timers throttle spf *spf-start spf-hold spf-maximum*

예제**:**

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

spf-start 인수는 OSPF에서 토폴로지 변경을 수신하는 시간과 SPF 계산을 시작하는 시간 사이의 지연 시간(밀리초 단위)입니다. 입력 가능한 값은 0 ~ 600000의 정수입니다.

spf-hold 인수는 두 번 연속으로 SPF를 계산하는 작업 사이의 최소 시간(밀리초 단위)입니다. 입력 가능한 값은 0 ~ 600000의 정수입니다.

spf-maximum 인수는 두 번 연속으로 SPF를 계산하는 작업 사이의 최소 시간(밀리초 단위)입니다. 입력 가능한 값은 0 ~ 600000의 정수입니다.

인접 디바이스 작동 또는 중단 로그

OSPFv2 네이버가 작동 또는 중단될 경우 기본적으로 syslog 메시지가 생성됩니다.

debug ospf adjacency 명령을 켜지 않고 OSPFv2 네이버의 작동 또는 중단에 대한 정보를 보려면 **log-adj-changes** 명령을 구성합니다. **log-adj-changes** 명령을 사용하면 적은 출력 결과로도 피어 관계에 대한 심층적인 뷰가 제공됩니다. 각 상태 변경에 대한 메시지를 보려면 **log-adj-changes detail** 명령을 구성합니다.

프로시저

단계 **1** OSPFv2 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예제:

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 인접 디바이스의 작동 또는 중단을 기록하도록 구성합니다.

log-adj-changes [**detail**]

OSPFv3 구성

이 섹션에서는 OSPFv3 라우팅 프로세스 구성과 관련된 작업을 설명합니다.

OSPFv3 활성화

OSPFv3를 활성화하려면 OSPFv3 라우팅 프로세스를 생성하고, OSPFv3에 대한 영역을 생성하고, OSPFv3에 대한 인터페이스를 활성화하고, 경로를 대상 OSPFv3 라우팅 프로세스에 재분배해야 합니다.

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 생성합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config)# ipv6 router ospf 10
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 태그이며 어떠한 양수이든 사용 가능합니다. 이 태그는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 인터페이스를 활성화합니다.

interface *interface_name*

예제**:**

```
ciscoasa(config)# interface Gigabitethernet0/0
```

단계 **3** 지정된 프로세스 ID로 OSPFv3 라우팅 프로세스를 생성하고, 지정된 영역 ID로 OSPFv3에 대한 영역을 생성합니다.

ipv6 ospf *process-id* **area** *area_id*

예제**:**

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

OSPFv3 인터페이스 파라미터 구성

필요한 경우 특정 인터페이스별 OSPFv3 매개변수를 변경할 수 있습니다. 이러한 파라미터는 변경할 필요가 없지만, hello 간격 및 dead 간격과 같은 인터페이스 파라미터는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 컨피그레이션할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제**:**

```
ciscoasa(config-if)# ipv6 router ospf 10
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 태그이며 어떠한 양수이든 사용 가능합니다. 이 태그는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPFv3 영역을 생성합니다.

ipv6 ospf **area** [*area-num*] [**instance**]

예제**:**

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

area-num 인수는 인증을 활성화하는 영역이며 십진수 값 또는 IP 주소가 될 수 있습니다. **instance** 키워드는 인터페이스에 할당할 영역 인스턴스 ID를 지정합니다. 하나의 인터페이스에는 하나의 OSPFv3 영역만 포함할 수 있습니다. 여러 인터페이스에서 동일한 영역을 사용할 수 있으며, 각 인터페이스에서는 다른 영역 인스턴스 ID를 사용할 수 있습니다.

단계 **3** 인터페이스에서 패킷을 전송하는 비용을 지정합니다.

ipv6 ospf cost *interface-cost*

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

interface-cost 인수는 링크 상태 메트릭으로 표시되는 무부호 정수 값을 지정하며, 입력 가능한 값의 범위는 1 ~ 65535입니다. 기본 비용은 대역폭을 기준으로 합니다.

단계 **4** OSPFv3 인터페이스에 대한 발송 LSA를 필터링합니다.

ipv6 ospf database-filter all out

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf database-filter all out
```

기본적으로 모든 발신 LSA는 인터페이스에 플러딩됩니다.

단계 **5** 인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간을 초 단위로 설정합니다.

ipv6 ospf dead-interval *seconds*

예제**:**

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf dead-interval 60
```

이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 **ipv6 ospf hello-interval** 명령으로 설정된 간격 집합의 4배입니다.

단계 **6** 인터페이스의 암호화 유형을 지정합니다.

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**}

예제**:**

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

ipsec 키워드는 IP 보안 프로토콜을 지정합니다. **spi** *spi* 키워드 인수 쌍은 보안 정책 색인을 지정하며, 이 값의 범위는 256 ~ 42949667295이고 십진수로 입력해야 합니다.

esp 키워드는 보안 페이로드 암호화를 지정합니다. *encryption-algorithm* 인수는 ESP와 함께 사용할 암호화 알고리즘을 지정합니다. 유효한 값은 다음과 같습니다.

- aes-cdc — AES-CDC 암호화를 활성화합니다.
- 3des — 3DES 암호화를 활성화합니다.
- des — DES 암호화를 활성화합니다.
- null — 암호화 없이 ESP를 지정합니다.

key-encryption-typee 인수는 다음 2개의 값 중 하나가 될 수 있습니다.

- 0 — 키가 암호화되지 않습니다.
- 7 — 키가 암호화됩니다.

key 인수는 메시지 다이제스트의 계산에 사용되는 숫자를 지정합니다. 이 숫자는 32자 길이의 16진수 숫자(16바이트)입니다. 키의 크기는 사용되는 암호화 알고리즘에 따라 달라집니다. AES-CDC 같은 일부 알고리즘의 경우 키의 크기를 선택할 수 있습니다. *authentication-algorithm* 인수는 사용할 암호화 인증 알고리즘을 지정하며, 다음 중 하나가 될 수 있습니다.

- md5 — 메시지 다이제스트 5(MD5)를 활성화합니다.
- sha1 — SHA-1를 활성화합니다.

null 키워드는 영역 암호화를 재정의합니다.

인터페이스에서 OSPFv3 암호화가 활성화되어 있고 네이버가 다른 영역(예: 영역 0)에 있는 경우, ASA에서 해당 영역과의 인접성을 형성하려면 ASA에서 영역을 변경해야 합니다. ASA에서 영역을 0으로 변경하면 OSPFv3 인접성이 가동되기 전에 2분간의 지연이 발생합니다.

단계 **7** 인터페이스에 대한 LSA의 플러딩 감소를 지정합니다.

ipv6 ospf flood-reduction

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

단계 **8** 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다.

ipv6 ospf hello-interval *seconds*

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

```
ipv6 ospf hello-interval 15
```

이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1 ~ 65535입니다. 기본 간격은 이더넷 인터페이스의 경우 10초이고, 비 브로드캐스트 인터페이스의 경우 30초입니다.

단계 **9** DBD 패킷이 수신될 때 OSPF MTU 불일치 감지를 비활성화합니다.

ipv6 ospf mtu-ignore

예제**:**

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf mtu-ignore
```

OSPF MTU 불일치 감지는 기본적으로 활성화되어 있습니다.

단계 **10** OSPF 네트워크 유형을 기본값 이외의 유형으로 설정하며, 이 경우 네트워크 유형에 따라 달라집니다.

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

예제**:**

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf network point-to-point non-broadcast
```

point-to-point non-broadcast 키워드를 사용하면 네트워크 유형이 포인트 투 포인트 비 브로드캐스트로 설정됩니다. **broadcast** 키워드는 네트워크 유형을 브로드캐스트로 설정합니다.

단계 **11** 네트워크의 전용 라우터를 결정하는 데 도움이 되는 라우터 우선순위를 설정합니다.

ipv6 ospf priority *number-value*

예제**:**

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
```

```
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
```

유효한 값의 범위는 0 ~ 255입니다.

단계 **12** 브로드캐스트 이외 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성합니다.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

단계 **13** 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다.

ipv6 ospf retransmit-interval *seconds*

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 5초입니다.

단계 **14** 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 설정합니다.

ipv6 ospf transmit-delay *seconds*

예제:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-delay 3
```

유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 1초입니다.

OSPFv3 라우터 파라미터 구성

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPFv3 영역 파라미터를 구성합니다.

area

예제:

```
ciscoasa(config-rtr)# area 10
```

지원되는 매개변수에는 십진수 숫자(0 ~ 4294967295)로 된 영역 ID 및 IP 주소 형식(**A.B.C.D**)으로 된 영역 ID가 포함됩니다.

단계 **3** 명령을 기본값으로 설정합니다.

default

예제:

```
ciscoasa(config-rtr)# default originate
```

originate 매개변수는 기본 경로를 배포합니다.

단계 **4** 기본 정보의 배포를 제어합니다.

default-information

단계 **5** 경로 유형을 기준으로 OSPFv3 경로 관리 영역을 정의합니다.

distance

예제**:**

```
ciscoasa(config-rtr)# distance 200
```

지원되는 매개변수에는 관리 영역 값(1 ~ 254) 및 OSPFv3 영역에 대한 **ospf**가 포함됩니다.

단계 **6** 라우터에 유형 6 MOSPF(멀티캐스트 OSPF) 패킷에 대한 LSA(링크 상태 알림)가 수신될 경우, **lsa** 파라미터를 사용하여 syslog 메시지가 전송되는 것을 억제합니다.

ignore

예제**:**

```
ciscoasa(config-rtr)# ignore lsa
```

단계 **7** OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다.

log-adjacency-changes

예제**:**

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail 매개변수를 사용하면 모든 상태 변경 사항이 기록됩니다.

단계 **8** 인터페이스에서 라우팅 업데이트를 전송하고 수신하는 작업을 억제합니다.

passive-interface [*interface_name*]

예제**:**

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 인수는 OSPFv3 프로세스가 실행 중인 인터페이스의 이름을 지정합니다.

단계 **9** 하나의 라우팅 도메인에서 다른 도메인으로 경로를 재배포하도록 구성합니다.

redistribute {**connected** | **ospf** | **static**}

여기서 각 항목은 다음을 나타냅니다.

- **connected** - 연결된 경로를 지정합니다.
- **ospf** — OSPFv3 경로를 지정합니다.

- **static** - 고정 경로를 지정합니다.

예제:

```
ciscoasa(config-rtr)# redistribute ospf
```

단계 **10** 지정된 프로세스에 대한 고정된 라우터 ID를 생성합니다.

router-id {*A.B.C.D* | **cluster-pool** | **static**}

여기서 각 항목은 다음을 나타냅니다.

A.B.C.D - OSPF 라우터 ID를 IP 주소 형식으로 지정합니다.

cluster-pool — 개별 인터페이스 클러스터링이 구성될 때 IP 주소 풀을 구성합니다. 클러스터링에 사용되는 IP 주소 풀에 대한 자세한 내용은 클러스터링(OSPFv2 및 OSPFv3)에 대한 IP 주소 풀 구성, 915 페이지을(를) 참조하십시오.

예제:

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

단계 **11** IPv6 주소 요약을 0~128 사이의 유효한 값으로 구성합니다.

summary-prefix *X:X:X:X::X/*

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 192.168.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

X:X:X:X::X/ 매개변수는 IPv6 접두사를 지정합니다.

단계 **12** 라우팅 타이머를 조정합니다.

timers

라우팅 타이머 매개변수는 다음과 같습니다.

- **lsa** — OSPFv3 LSA 타이머를 지정합니다.
- **pacing** — OSPFv3 속도 타이머를 지정합니다.
- **throttle** — OSPFv3 속도 제한 타이머를 지정합니다.

예제:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

OSPFv3 영역 파라미터 구성

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다.

이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** NSSA 영역 또는 stub 영역의 요약 기본 비용을 설정합니다.

area *area-id* **default-cost** *cost*

예제:

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

단계 **3** 경계선 라우터 전용 주소 및 마스크와 일치하는 경로를 요약합니다.

area *area-id* **range** *ipv6-prefix*/ *prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

예제:

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- *area-id* 인수는 경로를 요약할 영역을 지정합니다. 이 값은 십진수 또는 IPv6 접두사로 지정할 수 있습니다.
- *ipv6-prefix* 인수는 IPv6 접두사를 지정합니다. *prefix-length* 인수는 접두사 길이를 지정합니다.
- **advertise** 키워드는 광고할 주소 범위 상태를 advertised로 설정하고 Type 3 요약 LSA를 생성합니다.
- **not-advertise** 키워드는 주소 범위 상태를 DoNotAdvertise로 설정합니다.
- Type 3 요약 LSA가 억제되고, 구성 요소 네트워크는 다른 네트워크에 숨겨진 상태로 유지됩니다.
- **cost** *cost* 키워드 인수 쌍은 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 요약 경로의 메트릭 또는 비용을 지정합니다.
- 유효한 값의 범위는 0 ~ 16777215입니다.

단계 **4** NSSA 영역을 지정합니다.

area *area-id* **nssa**

예제**:**

```
ciscoasa(config-rtr)# area 1 nssa
```

단계 **5** stub 영역을 지정합니다.

area *area-id* **stub**

예제**:**

```
ciscoasa(config-rtr)# area 1 stub
```

단계 **6** 가상 링크 및 파라미터를 정의합니다.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

예제**:**

```
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

- *area-id* 인수는 경로를 요약할 영역을 지정합니다. **virtual link** 키워드는 가상 링크 네이버의 생성을 지정합니다.
- *router-id* 인수는 가상 링크 네이버와 연결된 라우터 ID를 지정합니다.
- 라우터 ID를 표시하려면 **show ospf** 또는 **show ipv6 ospf** 명령을 입력합니다. 기본값은 없습니다.
- **hello-interval** 키워드는 인터페이스에서 전송되는 Hello 패킷 간의 시간을 초 단위로 지정합니다. Hello 간격은 Hello 패킷에 광고되는 무부호 정수입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1 ~ 8192입니다. 기본값은 10입니다.
- **retransmit-interval** *seconds* 키워드 인수 쌍은 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값은 예상 왕복 지연 시간보다 커야 하며 입력 가능한 범위는 1~8192입니다. 기본값은 5입니다.
- **transmit-delay** *seconds* 키워드 인수 쌍은 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 이 정수 값은 0보다 커야 합니다. 업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 입력 가능한 값의 범위는 1 ~ 8192입니다. 기본값은 1입니다.
- **dead-interval** *seconds* 키워드 인수 쌍은 네이버에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않은 시간을 초 단위로 지정합니다. Dead 간격은 무부호 정수입니다. 기본값은 Hello 간격의 4배이거나 40초입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1 ~ 8192입니다.

- **ttl-security hops** 키워드는 가상 링크에서 TTL(Time-to-Live) 보안을 구성합니다. *hop-count* 인수 값의 범위는 1~254입니다.

OSPFv3 수동 인터페이스 구성

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process_id*

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 인터페이스에서 라우팅 업데이트를 전송하고 수신하는 작업을 억제합니다.

passive-interface [*interface_name*]

예제:

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 인수는 OSPFv3 프로세스가 실행 중인 인터페이스의 이름을 지정합니다. *no interface_name* 인수를 지정한 경우, OSPFv3 프로세스 *process_id*의 인터페이스는 모두 패시브가 됩니다.

OSPFv3 관리 영역 구성

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process_id*

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPFv3 경로에 대한 관리 영역을 설정합니다.

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

예제**:**

```
ciscoasa(config-rtr)# distance ospf external 200
```

ospf 키워드는 OSPFv3 경로를 지정합니다. **external** 키워드는 OSPFv3에 대한 외부 Type 5 및 Type 7 경로를 지정합니다. **inter-area** 키워드는 OSPVv3에 대한 영역 간 경로를 지정합니다. **inter-area** 키워드는 OSPVv3에 대한 영역 간 경로를 지정합니다. *distance* 인수는 관리 영역을 지정하며, 이 값은 10~254 사이의 정수입니다.

OSPFv3 타이머 구성

OSPFv3에 대한 LSA 도착, LSA 속도, 속도 제한 타이머를 설정할 수 있습니다.

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제**:**

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** ASA에서 OSPF 네이버의 동일한 LSA를 허용하는 최소 간격을 설정합니다.

timers lsa arrival *milliseconds*

예제**:**

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

milliseconds 인수는 네이버에서 도착하는 동일한 LSA를 수락하는 동안 소요될 수밖에 없는 최소 지연 시간을 밀리초 단위로 지정합니다. 범위는 0밀리초 ~ 6,000,000밀리초입니다. 기본값은 1000밀리초입니다.

단계 **3** LSA 플러드 패킷 속도 조절을 구성합니다.

timers pacing flood *milliseconds*

예제**:**

```
ciscoasa(config-rtr)# timers lsa flood 20
```

milliseconds 인수는 업데이트 중 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 컨피그레이션 가능한 범위는 5밀리초 ~ 100밀리초입니다. 기본값은 33밀리초입니다.

단계 **4** OSPFv3 LSA를 그룹으로 수집 및 새로 고치고, 체크섬 또는 시간 경과가 이루어지는 간격을 변경합니다.

timers pacing lsa-group *seconds*

예제**:**

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

seconds 인수는 LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 초 단위로 지정합니다. 이 값의 범위는 10초 ~ 1800초입니다. 기본값은 240초입니다.

단계 **5** LSA 재전송 패킷 속도 조절을 구성합니다.

timers pacing retransmission *milliseconds*

예제**:**

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

milliseconds 인수는 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 컨피그레이션 가능한 범위는 5밀리초 ~ 200밀리초입니다. 기본값은 66밀리초입니다.

단계 **6** OSPFv3 LSA 속도 제한을 구성합니다.

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

예제**:**

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- *milliseconds1* 인수는 LSA의 첫 번째 어커런스를 생성하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. *milliseconds2* 인수는 동일한 LSA를 시작하는 데 필요한 최대 지연 시간을 밀리초 단위로 지정합니다. *milliseconds3* 인수는 동일한 LSA를 시작하는 데 필요한 최소 지연 시간을 밀리초 단위로 지정합니다.
- LSA 제한의 경우 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3이 첫 번째 어커런스 값으로 자동으로 수정됩니다. 마찬가지로 지정된 최대 지연 시간이 최소 지연 시간보다 작으면 OSPFv3이 최소 지연 시간 값으로 자동으로 수정됩니다.
- *milliseconds1*의 경우 기본값은 0밀리초입니다.

- *milliseconds2* 및 *milliseconds3*의 경우 기본값은 5000밀리초입니다.

단계 **7** OSPFv3 SPF 속도 제한을 구성합니다.

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

예제:

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- *milliseconds1* 인수는 SPF 계산의 변경 사항을 수신하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. *milliseconds2* 인수는 첫 번째와 두 번째 SPF 계산 사이의 지연 시간을 밀리초 단위로 지정합니다. *milliseconds3* 인수는 SPF 계산에 소요되는 최대 대기 시간을 밀리초 단위로 지정합니다.
- SPF 제한의 경우 *milliseconds2* 또는 *milliseconds3*이 *milliseconds1*보다 작으면 OSPFv3이 *milliseconds1* 값으로 자동으로 수정됩니다. 마찬가지로 *milliseconds3*이 *milliseconds2*보다 작으면 OSPFv3이 *milliseconds2* 값으로 자동으로 수정됩니다.
- *milliseconds1*의 경우 SPF 속도 제한의 기본값은 5000밀리초입니다.
- *milliseconds2* 및 *milliseconds3*의 경우 SPF 속도 제한의 기본값은 10000밀리초입니다.

고정 OSPFv3 인접 디바이스 정의

고정 OSPFv3 네이버를 정의하여 포인트-투-포인트 비 브로드캐스트 네트워크를 통해 OSPF 경로를 광고할 수 있습니다. 이 기능을 사용하면 GRE 터널에 광고를 캡슐화하지 않고도 기존 VPN 연결 전체에 OSPFv3 광고를 브로드캐스트할 수 있습니다.

시작하기 전에, OSPFv3 네이버에 대한 고정 경로를 생성해야 합니다. 고정 경로 생성에 대한 자세한 내용은 고정 경로 구성, 817 페이지을 참조하십시오.

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 구성 모드를 시작합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 브로드캐스트 이외 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성합니다.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

예제:

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

OSPFv3 기본 파라미터 재설정

OSPFv3 매개변수를 기본값으로 되돌리려면 다음 단계를 수행합니다.

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 선택적 파라미터를 기본값으로 되돌립니다.

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route | distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

예제:

```
ciscoasa(config-rtr)# default metric 5
```

- **area** 키워드는 OSPFv3 영역 매개변수를 지정합니다. **auto-cost** 키워드는 대역폭에 따라 OSPFv3 인터페이스 비용을 지정합니다.
- **default-information** 키워드는 기본 정보를 배포합니다. **default-metric** 키워드는 재배포된 경로에 대한 메트릭을 지정합니다.
- **discard-route** 키워드는 discard-route 설치를 활성화하거나 비활성화합니다. **distance** 키워드는 관리 영역을 지정합니다.
- **distribute-list** 키워드는 라우팅 업데이트에서 네트워크를 필터링합니다.
- **ignore** 키워드는 특정 이벤트를 무시합니다. **log-adjacency-changes** 키워드는 인접성 상태의 변경 사항을 기록합니다.

- **maximum-paths** 키워드는 여러 경로를 통해 패킷을 전달합니다.
- **passive-interface** 키워드는 인터페이스에서 라우팅 업데이트를 억제합니다.
- **redistribute** 키워드는 다른 라우팅 프로토콜에서 IPv6 접두사를 재분배합니다.
- **router-id** 키워드는 지정된 라우팅 프로세스에 대한 라우터 ID를 지정합니다.
- **summary-prefix** 키워드는 IPv6 요약 접두사를 지정합니다.
- **timers** 키워드는 OSPFv3 타이머를 지정합니다.

Syslog 메시지 보내기

OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다.

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제**:**

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다.

log-adjacency-changes [**detail**]

예제**:**

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail 키워드는 OSPFv3 네이버가 작동 또는 중단되는 경우뿐만 아니라 각각의 상태에 대한 syslog 메시지를 전송합니다.

Syslog 메시지 억제

지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷이 경로에 전송될 경우 syslog 메시지가 전송되는 것을 억제하려면 다음 단계를 수행합니다.

프로시저

단계 **1** OSPFv2 라우팅 프로세스를 활성화합니다.

router ospf *process_id*

예제:

```
ciscoasa(config-if)# router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 지원되지 않는 LSA 유형 6 MOSPF(멀티캐스트 OSPF) 패킷이 경로에 전송될 경우 syslog 메시지가 전송되는 것을 억제합니다.

ignore lsa mospf

예제:

```
ciscoasa(config-rtr)# ignore lsa mospf
```

요약 경로 비용 계산

프로시저

RFC 1583에 따라 요약 경로 비용을 계산하는 데 사용된 방법을 복원합니다.

compatible rfc1583

예제:

```
ciscoasa (config-rtr)# compatible rfc1583
```

OSPFv3 라우팅 도메인에 기본 외부 경로 생성

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제**:**

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** OSPFv3 라우팅 도메인에 이르는 기본 외부 경로를 생성합니다.

default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

예제**:**

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- **always** 키워드는 기본 경로의 존재 여부에 상관없이 기본 경로를 광고합니다.
- **metric** *metric-value* 키워드 인수 쌍은 기본 경로를 생성하는 데 사용되는 메트릭을 지정합니다.
- **default-metric** 명령을 사용하여 값을 지정하지 않을 경우 기본값은 10입니다. 유효한 값의 범위는 0 ~ 16777214입니다.
- **metric-type** *type-value* 키워드 인수 쌍은 OSPFv3 라우팅 도메인에 광고되는 기본 경로와 연결된 외부 링크 유형을 지정합니다. 다음 중 하나를 유효한 값으로 사용할 수 있습니다.
  - 1 - Type 1 외부 경로
  - 2 - Type 2 외부 경로

  기본값은 Type 2 외부 경로입니다.
- **route-map** *map-name* 키워드 인수 쌍은 경로 맵이 충족될 경우 기본 경로를 생성하는 라우팅 프로세스를 지정합니다.

IPv6 요약 프리픽스 구성

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** IPv6 요약 프리픽스를 구성합니다.

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static
```

prefix 인수는 목적지의 IPv6 경로 접두사입니다. **not-advertise** 키워드는 지정된 접두사 및 마스크 쌍과 일치하는 경로를 억제합니다. 이 키워드는 OSPFv3에만 적용됩니다. **tag** *tag-value* 키워드 인수 쌍은 경로 맵을 통한 재분배를 제어하기 위한 일치 값으로 사용할 수 있는 태그 값을 지정합니다. 이 키워드는 OSPFv3에만 적용됩니다.

IPv6 경로 재배포

프로시저

단계 **1** OSPFv3 라우팅 프로세스를 활성화합니다.

ipv6 router ospf *process-id*

예제:

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1 ~ 65535의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** 하나의 OSPFv3 프로세스에서 다른 프로세스로 IPv6 경로를 재배포합니다.

redistribute *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* |**transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

예제**:**

```
ciscoasa(config-rtr)# redistribute connected 5 type-1
```

- *source-protocol* 인수는 경로가 재분배되는 소스 프로토콜을 지정하며, 선택 가능한 값은 static, connected 또는 OSPFv3입니다.
- *process-id* 인수는 OSPFv3 라우팅 프로세스가 활성화될 때 관리를 위해 할당되는 번호입니다.
- **include-connected** 키워드를 사용하면 대상 프로토콜에서는 소스 프로토콜 및 연결된 접두사를 통해 파악한 경로를 소스 프로토콜이 실행 중인 해당 인터페이스에 재분배할 수 있습니다.
- **level-1** 키워드는 Intermediate System-to-Intermediate System(IS-IS)의 경우, Level 1 경로가 다른 IP 라우팅 프로토콜에 개별적으로 재분배되도록 지정합니다.
- **level-1-2** 키워드는 IS-IS의 경우, Level 1 및 Level 2 경로가 모두 다른 IP 라우팅 프로토콜에 재분배되도록 지정합니다.
- **level-2** 키워드는 IS-IS의 경우, Level 2 경로가 다른 IP 라우팅 프로토콜에 개별적으로 재분배되도록 지정합니다.
- **metric** *metric-value* 키워드 인수 쌍의 경우, 하나의 OSPFv3 프로세스에서 동일한 라우터의 다른 OSPFv3 프로세스로 경로를 재분배할 때 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPFv3 프로세스에 다른 프로세스를 재분배할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.
- **metric transparent** 키워드는 RIP가 재분배된 경로에 라우팅 테이블 메트릭을 RIP 메트릭으로 사용하도록 합니다.
- **metric-type** *type-value* 키워드 인수 쌍은 OSPFv3 라우팅 도메인에 광고되는 기본 경로와 연결된 외부 링크 유형을 지정합니다. 유효한 값은 Type 1 외부 경로는 1, Type 2 외부 경로는 2이며 둘 중 하나를 선택할 수 있습니다. **metric-type** 키워드에 값을 지정하지 않을 경우 ASA에서는 Type 2 외부 경로를 적용합니다. IS-IS에 사용 가능한 링크 유형은 두 가지이며 하나를 선택할 수 있습니다. 63 이하의 IS-IS 메트릭에는 internal을 사용하고, 64 이상 128 미만의 IS-IS 메트릭에는 external을 사용합니다. 기본값은 internal입니다.
- **match** 키워드는 경로를 다른 라우팅 도메인에 재분배하며 다음 옵션 중 하나와 함께 사용됩니다. **external** [**1**|**2**]은 자동 시스템의 외부에 있지만 OSPFv3에 Type 1 또는 Type 2 외부 경로로서 가져온 경로에 사용됩니다. **internal**은 특정 자동 시스템의 내부에 있는 경로에 사용됩니다. **nssa-external** [**1**|**2**]은 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 1 외부 경로로서 가져온 경로에 사용됩니다.

- **tag** *tag-value* 키워드 인수 쌍은 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값을 지정합니다. 아무것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값의 범위는 0 ~ 4294967295.입니다.
- **route-map** 키워드는 경로 맵을 지정하여 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜까지 경로 가져오기의 필터링을 확인합니다. 이 키워드를 지정하지 않으면 모든 경로가 재분배됩니다. 이 키워드를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. *map-tag* 인수는 구성된 경로 맵을 식별합니다.

정상 재시작 구성

ASA에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(Non-Stop Forwarding) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 구성 요소에 오류가 발생하거나(예: 액티브 유닛이 장애 조치(HA) 모드 역할을 수행 중인 스탠바이 유닛과 충돌하거나, 마스터 유닛이 클러스터 모드에서 새 마스터로 선택된 슬레이브 유닛과 충돌한 경우), 무중단 소프트웨어 업그레이드가 예약된 경우 유용합니다.

Graceful Restart는 SPFv2 및 OSPFv3에서 모두 지원됩니다. NSF Cisco(RFC 4811 및 RFC 4812) 또는 NSF IETF(RFC 3623)를 사용하여 OSPFv2에서 Graceful Restart를 구성할 수 있습니다. graceful-restart(RFC 5187)를 사용하여 OSPFv3에서 Graceful Restart를 구성할 수 있습니다.

NSF Graceful Restart 기능을 구성하려면 기능을 구성하고, 디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. NSF 지원 디바이스는 해당 디바이스의 재시작 작업을 네이버에 나타낼 수 있으며, NSF 인식 디바이스는 네이버를 초기화하도록 지원할 수 있습니다.

디바이스는 몇 가지 조건에 따라 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다.

- 디바이스는 현재 속한 모드에 관계없이 NSF 인식 디바이스로 구성할 수 있습니다.
- NSF 지원 디바이스로 구성하려면 디바이스가 Failover 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.
- NSF 인식 또는 NSF 지원 디바이스가 되려면, 필요에 따라 불투명 LSA(Link State Advertisements)/LLS(Link Local Signaling) 블록 처리 기능과 함께 디바이스를 구성해야 합니다.

참고 OSPFv2에 Fast Hello를 구성한 경우, 액티브 유닛이 다시 로드된 후 스탠바이 유닛이 액티브 유닛이 될 때 Graceful Restart가 실행되지 않습니다. 이는 역할 변경에 소요되는 시간이 구성된 Dead 간격보다 더 많기 때문입니다.

기능 구성

Cisco NSF Graceful Restart 메커니즘은 LLS 기능을 기반으로 하며, 이는 LLS 블록을 Hello 패킷의 RS 비트 집합으로 전송하여 재시작 작업을 나타냅니다. IETF NSF 메커니즘은 불투명 LSA 기능을 기반으로 하며, 이는 Type 9 불투명 LSA를 전송하여 재시작 작업을 나타냅니다. 기능을 구성하려면 다음 명령을 입력합니다.

프로시저

단계 **1** OSPF 라우팅 프로세스를 생성하고 재배포하려는 OSPF 프로세스의 라우터 구성 모드를 시작합니다.

router ospf *process_id*

예제**:**

```
ciscoasa(config)# router ospf 2
```

process_id 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 어떠한 양수이든 사용 가능합니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

단계 **2** LLS 데이터 블록 또는 불투명 LSA를 사용하여 NSF를 활성화합니다.

capability {lls|opaque}

lls 키워드는 Cisco NSF Graceful Restart 메커니즘의 LLS 기능을 활성화하는 데 사용됩니다.

opaque 키워드는 IETF NSF Graceful Restart 메커니즘의 불투명 LSA 기능을 활성화하는 데 사용됩니다.

OSPFv2에 대한 정상 재시작 구성

OSPFv2에 사용할 수 있는 두 가지 Graceful Restart 메커니즘은 Cisco NSF 및 IETF NSF입니다. ospf 인스턴스에는 Graceful Restart 메커니즘을 한 번에 하나만 구성할 수 있습니다. NSF 인식 디바이스는 Cisco NSF 헬퍼 및 IETF NSF 헬퍼 모두로 구성할 수 있으나, NSF 지원 디바이스는 Cisco NSF 또는 IETF NSF 모드를 한 번에 하나씩 ospf 인스턴스에 구성할 수 있습니다.

OSPFv2용 Cisco NSF 정상 재시작 구성

NSF 지원 또는 NSF 인식 디바이스에 대해 OSPFv2용 Cisco NSF 정상 재시작을 구성합니다.

프로시저

단계 **1** NSF 지원 디바이스에서 Cisco NSF를 활성화합니다.

nsf cisco [enforce global]

예제:

```
ciscoasa(config-router)# nsf cisco
```

enforce global 키워드는 비 NSF 인식 인접 디바이스 디바이스가 감지될 경우 NSF 재시작을 취소합니다.

단계 **2** NSF 인식 디바이스에서 Cisco NSF 헬퍼 모드를 활성화합니다.

capability {lls|opaque}

예제:

```
ciscoasa(config-router)# capability lls
```

이 명령은 기본적으로 사용됩니다. 이 명령을 no 형식으로 사용하면 명령이 비활성화됩니다.

OSPFv2에 IETF NSF 정상 재시작 구성

NSF 지원 또는 NSF 인식 디바이스에 대해 OSPFv2용 IETF NSF 정상 재시작을 구성합니다.

프로시저

단계 **1** NSF 지원 디바이스에서 IETF NSF를 활성화합니다.

nsf ietf [restart interval seconds]

예제:

```
ciscoasa(config-router)# nsf ietf restart interval 80
```

restart interval seconds는 정상 재시작 간격의 길이를 초 단위로 지정합니다. 유효한 값은 1초 ~ 1800초입니다. 기본값은 120초입니다.

인접성이 가동되는 데 소요된 시간보다 재시작 간격이 작게 구성될 경우 정상 재시작이 종료될 수 있습니다. 예를 들어, 30초 미만의 재시작 간격은 지원되지 않습니다.

단계 **2** NSF 인식 디바이스에서 IETF NSF 헬퍼 모드를 활성화합니다.

nsf ietf helper [strict-lsa-checking]

예제:

```
ciscoasa(config-router)# nsf ietf helper
```

strict-LSA-checking 키워드는 재시작 라우터에 플러딩되는 LSA의 변경사항이 감지되거나, 정상 재시작 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.

이 명령은 기본적으로 사용됩니다. 이 명령을 no 형식으로 사용하면 명령이 비활성화됩니다.

OSPFv3에 정상 재시작 구성

OSPFv3에 NSF Graceful Restart 기능을 구성하려면 디바이스를 NSF 지원 디바이스로 구성하고, 디바이스를 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다.

프로시저

단계 **1** 명시적인 IPv6 주소로 구성되지 않은 인터페이스에서 IPv6 처리를 활성화합니다.

interface physical_interface ipv6 enable

예제**:**

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

physical_interface 인수는 OSPFv3 NSF에 참여하는 인터페이스를 나타냅니다.

단계 **2** NSF 지원 디바이스에서 OSPFv3에 대해 Graceful-Restart를 활성화합니다.

graceful-restart [restart interval seconds]

예제**:**

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

restart interval seconds는 정상 재시작 간격의 길이를 초 단위로 지정합니다. 유효한 값은 1초 ~ 1800초입니다. 기본값은 120초입니다.

인접성이 가동되는 데 소요된 시간보다 재시작 간격이 작게 구성될 경우 Graceful Restart가 종료될 수 있습니다. 예를 들어, 30초 미만의 재시작 간격은 지원되지 않습니다.

단계 **3** NSF 인식 디바이스에서 OSPFv3에 Graceful-Restart를 활성화합니다.

graceful-restart helper [strict-lsa-checking]

예제**:**

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

strict-LSA-checking 키워드는 재시작 라우터에 플러딩되는 LSA의 변경사항이 감지되거나, 정상 재시작 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.

Graceful-Restart 헬퍼 모드는 기본적으로 활성화되어 있습니다.

OSPFv2 구성 제거

OSPFv2 구성을 제거합니다.

프로시저

활성화한 전체 OSPFv2 구성을 제거합니다.

clear configure router ospf *pid*

예제:

```
ciscoasa(config)# clear configure router ospf 1000
```

컨피그레이션을 지운 후에는 **router ospf** 명령을 사용하여 OSPF를 다시 구성해야 합니다.

OSPFv3 구성 제거

OSPFv3 구성을 제거합니다.

프로시저

활성화한 전체 OSPFv3 구성을 제거합니다.

clear configure ipv6 router ospf *process-id*

예제:

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

구성을 지운 후에는 **ipv6 routerospf** 명령을 사용하여 OSPFv3를 다시 구성해야 합니다.

OSPFv2의 예

다음 예에는 다양한 선택적 프로세스로 OSPFv2를 활성화하고 구성하는 방법이 나와 있습니다.

1. OSPFv2를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2. (선택 사항) 하나의 OSPFv2 프로세스에서 다른 OSPFv2 프로세스로 경로를 재분배하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

3. (선택 사항) OSPFv2 인터페이스 매개변수를 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

4. (선택 사항) OSPFv2 영역 매개변수를 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

5. (선택 사항) 경로 계산 타이머를 구성하고 네이버 동작 및 중단 메시지 로그를 표시하려면 다음 명령을 입력합니다.

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6. (선택 사항) 현재 OSPFv2 컨피그레이션 설정을 표시하려면 **show ospf** 명령을 입력합니다.

   다음은 **show ospf** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show ospf

Routing Process “ospf 2” with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

7. OSPFv2 컨피그레이션을 지우려면 다음 명령을 입력합니다.

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 예

다음 예에는 인터페이스 수준에서 OSPFv3를 활성화하고 구성하는 방법이 나와 있습니다.

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

다음은 **show running-config ipv6** 명령의 샘플 출력입니다.

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

다음은 **show running-config interface** 명령의 샘플 출력입니다.

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

다음 예에는 OSPFv3별 인터페이스를 구성하는 방법이 나와 있습니다.

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
```

```
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
123456789012345678901234567890 12
```

```
ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

OSPFv3 가상 링크를 구성하는 방법의 예를 보려면 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

OSPF 모니터링

IP 라우팅 테이블, 캐시, 데이터베이스의 내용 같은 특정 통계를 표시할 수 있습니다. 제공된 정보를 사용하여 리소스 사용률을 결정하고 네트워크 문제를 해결할 수도 있습니다. 또한 노드 도달 범위에 대한 정보를 표시하고 디바이스 패킷이 네트워크를 통해 들어오는 라우팅 경로를 검색할 수 있습니다.

다양한 OSPFv2 경로 통계를 모니터링하거나 표시하려면 다음 명령 중 하나를 입력합니다.

명령어	목적
show ospf [*process-id* [*area-id*]]	OSPFv2 라우팅 프로세스에 대한 일반적인 정보가 표시됩니다.
show ospf border-routers	ABR 및 ASBR에 대한 내부 OSPFv2 라우팅 테이블 항목이 표시됩니다.
show ospf [*process-id* [*area-id*]] database	특정 라우터에 대해 OSPFv2 데이터베이스에 관련된 정보 목록이 표시됩니다.

명령어	목적
show ospf flood-list *if-name*	인터페이스를 통해 플러딩되는 대기 중인 LSA 목록이 표시됩니다(OSPF v2packet 속도 확인). OSPFv2 업데이트 패킷은 자동으로 속도를 조절하여 33밀리초 미만의 속도로는 전송되지 않도록 합니다. 속도가 조절되지 않을 경우 일부 업데이트 패킷은 링크 속도가 느려지거나, 업데이트가 네이버에 빠른 속도로 수신되지 않거나, 라우터의 버퍼 용량이 부족해질 수 있습니다. 예를 들어, 속도가 조절되지 않으면 다음과 같은 토폴로지가 있을 경우 패킷이 손실될 수 있습니다. • 속도가 빠른 라우터가 포인트-투-포인트 링크를 통해 느린 라우터에 연결됩니다. • 플러딩이 진행되는 동안, 일부 네이버에서 단일 라우터로 동시에 업데이트를 전송합니다. 효율성을 높이고 재전송 손실을 최소화하기 위해서는 재발송하는 동안에도 속도 조절을 사용해야 합니다. 또한 인터페이스 외부로 전송하기 위해 대기 중인 LSA를 표시할 수도 있습니다. 속도 조절을 사용하면 OSPFv2 업데이트 및 재전송 패킷을 더욱 효율적으로 전송할 수 있습니다. 이 기능을 사용하기 위한 컨피그레이션 작업이 필요하지 않으며, 자동으로 실행됩니다.
show ospf interface [*if_name*]	OSPFv2 관련 인터페이스 정보가 표시됩니다.
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	인터페이스당 OSPFv2 네이버 정보가 표시됩니다.
show ospf request-list *neighbor if_name*	라우터에서 요청한 모든 LSA 목록이 표시됩니다.
show ospf retransmission-list *neighbor if_name*	재전송 대기 중인 모든 LSA 목록을 표시합니다.
show ospf [*process-id*] summary-address	OSPFv2 프로세스에 따라 구성된 모든 요약 주소 재분배 정보의 목록이 표시됩니다.
show ospf [*process-id*] **traffic**	특정 OSPFv2 인스턴스에 의해 전송되거나 수신된 다양한 유형의 패킷 목록이 표시됩니다.
show ospf [*process-id*] virtual-links	OSPFv2 관련 가상 링크 정보가 표시됩니다.
show route cluster	클러스터링 시 추가적인 OSPFv2 경로 동기화 정보가 표시됩니다.

다양한 OSPFv3 경로 통계를 모니터링하거나 표시하려면 다음 명령 중 하나를 입력합니다.

명령어	목적
show ipv6 ospf [*process-id* [*area-id*]]	OSPFv3 라우팅 프로세스에 대한 일반적인 정보가 표시됩니다.
show ipv6 ospf [*process-id*] **border-routers**	ABR 및 ASBR에 대한 내부 OSPFv3 라우팅 테이블 항목이 표시됩니다.
show ipv6 ospf [*process-id* [*area-id*]] database [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	특정 라우터에 대해 OSPFv3 데이터베이스에 관련된 정보 목록이 표시됩니다.
show ipv6 ospf [*process-id* [*area-id*]] **events**	OSPFv3 이벤트 정보가 표시됩니다.
show ipv6 ospf [*process-id*] [*area-id*] flood-list *interface-type interface-number*	인터페이스를 통해 플러딩되는 대기 중인 LSA 목록이 표시됩니다(OSPFv3 패킷 속도 확인). OSPFv3 업데이트 패킷은 자동으로 속도를 조절하여 33밀리초 미만의 속도로는 전송되지 않도록 합니다. 속도가 조절되지 않을 경우 일부 업데이트 패킷은 링크 속도가 느려지거나, 업데이트가 네이버에 빠른 속도로 수신되지 않거나, 라우터의 버퍼 용량이 부족해질 수 있습니다. 예를 들어, 속도가 조절되지 않으면 다음과 같은 토폴로지가 있을 경우 패킷이 손실될 수 있습니다. • 속도가 빠른 라우터가 포인트-투-포인트 링크를 통해 느린 라우터에 연결됩니다. • 플러딩이 진행되는 동안, 일부 네이버에서 단일 라우터로 동시에 업데이트를 전송합니다. 효율성을 높이고 재전송 손실을 최소화하기 위해서는 재발송하는 동안에도 속도 조절이 사용됩니다. 또한 인터페이스 외부로 전송하기 위해 대기 중인 LSA를 표시할 수도 있습니다. 속도 조절을 사용하면 OSPFv3 업데이트 및 재전송 패킷을 더욱 효율적으로 전송할 수 있습니다. 이 기능을 사용하기 위한 컨피그레이션 작업이 필요하지 않으며, 자동으로 실행됩니다.
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	OSPFv3 관련 인터페이스 정보가 표시됩니다.
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	인터페이스당 OSPFv3 네이버 정보가 표시됩니다.

명령어	목적
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	라우터에서 요청한 모든 LSA 목록이 표시됩니다.
show ipv6 ospf [*process-id*] [*area-id*] retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	재전송 대기 중인 모든 LSA 목록을 표시합니다.
show ipv6 ospf statistic [*process-id*] [**detail**]	다양한 OSPFv3 통계가 표시됩니다.
show ipv6 ospf [*process-id*] summary-prefix	OSPFv3 프로세스에 따라 구성된 모든 요약 주소 재분배 정보의 목록이 표시됩니다.
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	OSPFv3 타이머 정보가 표시됩니다.
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	OSPFv3 트래픽 관련 통계가 표시됩니다.
show ipv6 ospf virtual-links	OSPFv3 관련 가상 링크 정보가 표시됩니다.
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	클러스터 내의 IPv6 라우팅 테이블 순서 번호, IPv6 재통합 타이머 상태, IPv6 라우팅 항목 순서 번호가 표시됩니다.

OSPF 내역

표 ***33: OSPF*** 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
OSPF 지원	7.0(1)	OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용한 데이터 라우팅, 인증, 라우팅 정보의 재분배 및 모니터링에 대한 지원이 추가되었습니다. 다음 명령을 도입했습니다. **route ospf**
다중 상황 모드의 동적 라우팅	9.0(1)	다중 상황 모드에서 OSPFv2 라우팅이 지원됩니다.
클러스터링	9.0(1)	클러스터링 환경에서 OSPFv2 및 OSPFv3에 대해 벌크 동기화, 경로 동기화, Spanned EtherChannel 로드 밸런싱이 지원됩니다. 다음 명령을 도입하거나 수정했습니다. **show route cluster**, **show ipv6 route cluster**, **debug route cluster, router-id cluster-pool**

기능 이름	플랫폼 릴리스	기능 정보
OSPFv3의 IPv6 지원	9.0(1)	OSPFv3 라우팅이 IPv6에서 지원됩니다. 다음 명령을 도입하거나 수정했습니다. **ipv6 ospf**, **ipv6 ospf area**, **ipv6 ospf cost, ipv6 ospf database-filter all out, ipv6 ospf dead-interval, ipv6 ospf encryption, ipv6 ospf hello-interval, ipv6 ospf mtu-ignore, ipv6 ospf neighbor, ipv6 ospf network, ipv6 ospf flood-reduction, ipv6 ospf priority, ipv6 ospf retransmit-interval, ipv6 ospf transmit-delay, ipv6 router ospf, ipv6 router ospf area, ipv6 router ospf default, ipv6 router ospf default-information, ipv6 router ospf distance, ipv6 router ospf exit, ipv6 router ospf ignore, ipv6 router ospf log-adjacency-changes, ipv6 router ospf no, ipv6 router ospf passive-interface, ipv6 router ospf redistribute, ipv6 router ospf router-id, ipv6 router ospf summary-prefix, ipv6 router ospf timers, area encryption, area range, area stub, area nssa, area virtual-link, default, default-information originate, distance, ignore lsa mospf, log-adjacency-changes, redistribute, router-id, summary-prefix, timers lsa arrival, timers pacing flood, timers pacing lsa-group, timers pacing retransmission, timers throttle, show ipv6 ospf, show ipv6 ospf border-routers, show ipv6 ospf database, show ipv6 ospf events, show ipv6 ospf flood-list, show ipv6 ospf graceful-restart, show ipv6 ospf interface, show ipv6 ospf neighbor, show ipv6 ospf request-list, show ipv6 ospf retransmission-list, show ipv6 ospf statistic, show ipv6 ospf summary-prefix, show ipv6 ospf timers, show ipv6 ospf traffic, show ipv6 ospf virtual-links, show ospf, show running-config ipv6 router, clear ipv6 ospf, clear configure ipv6 router, debug ospfv3, ipv6 ospf neighbor**
OSPF의 Fast Hellos 지원	9.2(1)	OSPF가 Fast Hello 패킷 기능을 지원하므로 OSPF 네트워크에서 통합 속도를 단축하는 컨피그레이션이 가능합니다. 수정된 명령: **ospf dead-interval**

기능 이름	플랫폼 릴리스	기능 정보
타이머	9.2(1)	새 OSPF 타이머가 추가되었으며, 기존 타이머는 사용이 중단되었습니다. 다음 명령을 도입했습니다. timers lsa arrival, timers pacing, timers throttle 다음 명령을 제거했습니다. Timers spf, timers lsa-grouping-pacing
액세스 목록을 사용한 경로 필터링	9.2(1)	이제 ACL을 사용한 경로 필터링이 지원됩니다. 다음 명령을 도입했습니다. distribute-list
OSPF 모니터링 개선 사항	9.2(1)	OSPF 모니터링 정보가 추가되었습니다. 다음 명령을 수정했습니다. show ospf events, show ospf rib, show ospf statistics, show ospf border-routers [detail], show ospf interface brief
OSPF 재분배 BGP	9.2(1)	OSPF 재분배 기능이 추가되었습니다. 다음 명령을 추가했습니다. redistribute bgp
NSF를 위한 OSPF 지원	9.3(1)	NSF를 위한 OSPFv2 및 OSPFv3 지원을 추가했습니다. 다음 명령을 추가했습니다. capability, nsf cisco, nsf cisco helper, nsf ietf, nsf ietf helper, nsf ietf helper strict-lsa-checking, graceful-restart, graceful-restart helper, graceful-restart helper strict-lsa-checking

30 장

IS-IS

이 장에서는 IS-IS(Intermediate System to Intermediate System) 라우팅 프로토콜에 대해 설명합니다.

IS-IS 정보

IS-IS 라우팅 프로토콜은 링크 상태 IGP(Interior Gateway Protocol)입니다. 링크 상태 프로토콜은 각 참여 디바이스에서 전체 네트워크 연결 맵을 작성하는 데 필요한 정보를 전파하는 것이 특징입니다. 그런 다음 해당 맵은 대상에 대한 최단 경로를 계산하는 데 사용됩니다. IS-IS 구현은 IPv4 및 IPv6를 지원합니다.

라우팅 도메인을 하나 이상의 하위 도메인으로 나눌 수 있습니다. 각 하위 도메인은 영역이라고 하며 영역 주소를 할당받습니다. 영역 내 라우팅을 수준-1 라우팅이라고 합니다. 수준-1 영역 간의 라우팅을 수준-2 라우팅이라고 합니다. 라우터를 IS(Intermediate System)라고도 합니다. IS는 수준 1, 수준 2 또는 둘 다에서 작동할 수 있습니다. 수준 1에서 작동하는 IS는 동일한 영역의 다른 수준-1 IS와 라우팅 정보를 교환합니다. 수준 2에서 작동하는 IS는 동일한 수준-1 영역에 있는지 여부와 관계없이 다른 수준-2 라우터와 라우팅 정보를 교환합니다. 수준-2 라우터 집합과 이를 상호 연결하는 링크는 수준-2 하위 도메인을 형성하며, 라우팅이 제대로 작동하려면 파티셔닝되지 않아야 합니다.

NET 정보

IS는 NET(Network Entity Title)이라고 알려져 있는 주소로 식별됩니다. NET은 NSAP(Network Service Access Point)의 주소이며 이는 IS에서 실행 중인 IS-IS 라우팅 프로토콜의 인스턴스를 식별합니다. NET은 길이가 8~20 옥텟이며 다음과 같이 3개의 부분으로 구성됩니다.

- Area address(영역 주소) — 이 필드는 길이가 1~13 옥텟이며 주소의 고차 옥텟으로 구성됩니다.

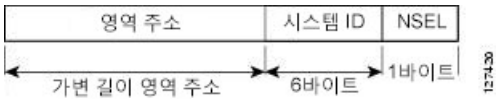
참고 IS-IS 인스턴스에 여러 영역 주소를 할당할 수 있습니다. 이 경우 모든 영역 주소가 동일하다고 간주됩니다. 여러 동일한 영역 주소는 도메인에서 영역을 병합하거나 분할할 때 유용합니다. 병합 또는 분할이 완료되면 IS-IS 인스턴스에 둘 이상의 영역 주소를 할당할 필요가 없습니다.

- System ID(시스템 ID) —이 필드는 6개의 옥텟이며 영역 주소를 바로 따릅니다. IS가 수준 1에서 작동할 경우 시스템 ID는 동일한 영역의 모든 수준-1 디바이스 간에 고유해야 합니다. IS가 수준 2에서 작동할 경우 시스템 ID는 도메인의 모든 디바이스 간에 고유해야 합니다.

참고 한 개의 시스템 ID를 IS 인스턴스에 할당합니다.

- NSEL — N-선택기 필드는 길이가 1옥텟이며 시스템 ID를 바로 따릅니다. 00으로 설정해야 합니다.

그림 ***62: NET*** 형식



IS-IS 동적 호스트 이름

IS-IS 라우팅 도메인에서 시스템 ID는 각 ASA를 나타내기 위해 사용됩니다. 시스템 ID는 각 IS-IS ASA에 대해 구성된 NET의 일부입니다. 예를 들어, 49.0001.0023.0003.000a.00의 NET으로 구성된 ASA에는 0023.0003.000a의 시스템 ID가 있습니다. ASA-name-to-system-ID 매핑은 ASA에서 네트워크 관리자가 유지 보수 및 트러블슈팅을 수행하는 동안 기억하기 어렵습니다.

show isis hostname 명령을 입력하면 system-ID-to-ASA-name 매핑 테이블에 항목이 표시됩니다.

동적 호스트 이름 메커니즘은 LSP(Link-State Protocol) 플러딩을 사용하여 전체 네트워크에서 ASA-name-to-system-ID 매핑 정보를 배포합니다. 네트워크에 있는 모든 ASA에서는 system ID-to-ASA 이름 매핑 정보를 라우팅 테이블에 설치하려고 시도합니다.

네트워크에서 동적 이름 유형, 길이, 값(TLV)을 알렸던 ASA에서 갑자기 알림을 중지하는 경우, 마지막으로 수신한 매핑 정보가 최대 1시간 동안 동적 호스트 매핑 테이블에 남아 있어 네트워크 관리자가 네트워크에 문제가 발생하는 동안 매핑 테이블에 항목을 표시할 수 있습니다.

IS-IS PDU 유형

IS는 PDU(프로토콜 데이터 단위)를 사용하여 라우팅 정보를 피어와 교환합니다. PDU의 IIH(Intermediate System-to-Intermediate System Hello PDU), LSP(Link-State PDU) 및 SNP(시퀀스 번호 PDU) 유형이 사용됩니다.

IIH

IIH는 IS-IS 프로토콜이 활성화되어 있는 회로에서 IS 네이버 간에 교환됩니다. IIH에는 발신자의 시스템 ID, 할당된 영역 주소 및 발신 IS에 알려져 있는 해당 회로의 네이버 ID가 포함됩니다. 추가적인 정보(선택 사항)도 포함될 수 있습니다.

두 가지 유형의 IIH가 있습니다.

- 수준-1 LAN IIH — 발신 IS가 해당 회로에 있는 수준-1 디바이스로 작동하는 경우 멀티 액세스 회로에서 발신됩니다.
- 수준-2 LAN IIH — 발신 IS가 해당 회로에 있는 수준-2 디바이스로 작동하는 경우 멀티 액세스 회로에서 발신됩니다.

LSP

IS는 LSP를 생성하여 IS에 직접 연결되어 있는 대상 및 네이버를 알립니다. LSP는 다음을 사용하여 고유하게 식별됩니다.

- LSP를 생성한 IS의 시스템 ID
- 의사 노드 ID — LSP가 의사 노드 LSP인 경우를 제외하고 이 값은 항상 0입니다.
- LSP 번호(0~255)
- 32비트 시퀀스 번호

LSP의 새 버전이 생성될 때마다 시퀀스 번호는 증가합니다.

수준-1 LSP는 수준 1을 지원하는 IS에서 생성됩니다. 수준-1 LSP는 수준-1 영역 전체에서 플러딩됩니다. 한 영역에 있는 모든 수준-1 IS에서 생성한 수준-1 LSP 집합은 수준-1 LSP 데이터베이스(LSPDB)입니다. 한 영역에 있는 모든 수준-1 IS에는 동일한 수준-1 LSPDB가 있으므로 영역에 대해 동일한 네트워크 연결성 맵이 있습니다.

수준-2 LSP는 수준 2를 지원하는 IS에서 생성됩니다. 수준-2 LSP는 수준-2 하위 도메인 전체에서 플러딩됩니다. 도메인에 있는 모든 수준-2 IS에서 생성한 수준-2 LSP 집합은 수준-2 LSP 데이터베이스(LSPDB)입니다. 모든 수준-2 IS에는 동일한 수준-2 LSPDB가 있으므로 수준-2 하위 도메인에 대해 동일한 연결성 맵이 있습니다.

SNP

SNP는 하나 이상의 LSP에 대한 요약 설명을 포함합니다. 수준 1 및 수준 2 둘 다에 대해 두 가지 유형의 SNP가 있습니다.

- CSNP(전체 시퀀스 번호 PDU)는 IS가 특정 수준에 대해 보유한 LSPDB의 요약을 전송하는 데 사용됩니다.
- PSNP(부분 시퀀스 번호 PDU)는 IS가 데이터베이스에 있거나 획득해야 하는 특정 수준에 대한 LSP의 하위 집합의 요약을 전송하는 데 사용됩니다.

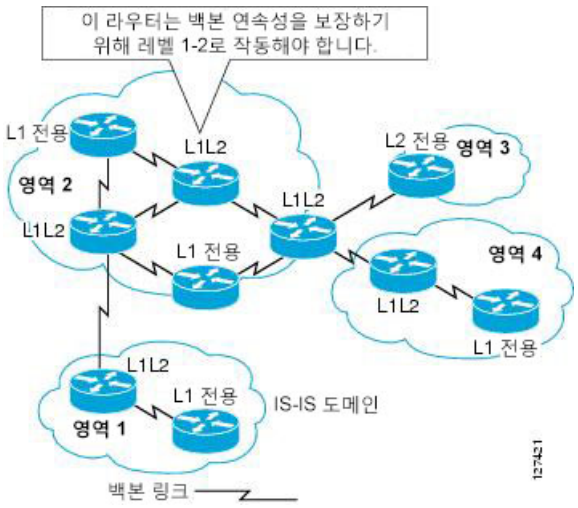
멀티 액세스 회로에서의 IS-IS 작업

멀티 액세스 회로는 여러 IS 즉, 회로에서 작동하는 2개 이상의 IS를 지원합니다. 멀티 액세스 회로의 필수 사전 요구 사항은 멀티캐스트 또는 브로드캐스트 주소를 사용하여 여러 시스템의 주소를 지정하는 기능입니다. 멀티 액세스 회로에서 수준 1을 지원하는 IS는 회로에서 수준-1 LAN IIH를 전송합니다. 멀티 액세스 회로에서 수준 2를 지원하는 IS는 회로에서 수준-2 LAN IIH를 전송합니다. IS는 회로에서 네이버 IS가 있는 각 수준에 대해 개별 인접성을 형성합니다.

IS는 회로의 수준 1을 지원하는 다른 IS와 수준 1 인접성을 형성하며 일치하는 영역 주소를 가집니다. 동일한 멀티 액세스 회로에서 수준 1을 지원하는 영역 주소 집합이 분리된 두 개의 IS는 지원되지 않습니다. IS는 회로의 수준 2를 지원하는 다른 IS와 수준-2 인접성을 형성합니다.

다음 그림의 IS-IS 네트워크 토폴로지에 있는 디바이스는 네트워크의 백본을 따라 수준 1, 수준 2 또는 수준 1 및 수준 2 라우팅을 수행합니다.

그림 ***63: IS-IS*** 네트워크 토폴로지의 수준***-1,*** 수준***-2,*** 수준 ***1-2*** 디바이스



지정된 IS의 IS-IS 선택

각 IS가 LSP의 멀티 액세스 회로에 모든 인접성을 알린 경우, 필요한 총 알림 수는 N 2가 됩니다(여기서 N은 회로에서 주어진 수준에서 작동하는 IS의 수). 이 확장성 문제를 해결하기 위해 IS-IS는 멀티 액세스 회로를 나타내는 의사 노드를 정의합니다. 지정된 수준의 회로에서 작동하는 모든 IS는 IS 중 하나를 선택하여 해당 회로에서 DIS(Designated Intermediate System)로 작동합니다. DIS는 회로에서 액티브 상태인 각 수준에 대해 선택됩니다.

DIS는 의사 노드 LSP의 실행을 담당합니다. 의사 노드 LSP는 해당 회로에서 작동하는 모든 네이버 알림을 포함합니다. 회로에서 작동하는 모든 IS(DIS 포함)는 비 의사 노드 LSP의 의사 노드에 네이버 알림을 제공하고 멀티 액세스 회로에서 네이버를 알리지 않습니다. 이러한 방법으로 필요한 알림의 총 수는 IS의 회로에서 작동되는 N-번호의 기능으로 다양합니다.

의사 노드 LSP는 다음 식별자를 사용하여 고유하게 분류됩니다.

- LSP를 생성한 DIS의 시스템 ID

- 의사 노드 ID(항상 0이 아님)
- LSP 번호(0~255)
- 32비트 시퀀스 번호

0이 아닌 의사 노드 ID는 비 의사 노드의 LSP와 의사 노드 LSP를 구별하는 것으로, DIS에 의해 선택되며 이 수준에서 DIS이기도 한 다른 LAN 회로 중에서 고유합니다.

DIS는 또한 회로에서 주기적으로 CSNP의 전송을 담당합니다. 이는 DIS에 있는 LSPDB의 현재 내용에 대한 전체 요약 설명을 제공합니다. 그런 다음 회로의 다른 IS가 멀티 액세스 회로의 모든 IS의 LSPDB를 효율적이고 안정적으로 동기화할 수 있는 다음 작업을 수행합니다.

- DIS에서 보낸 CSNP에 설명되어 있는 것보다 최신이거나 없는 플러드 LSP입니다.
- 로컬 데이터베이스에 없거나 CSNP 집합에 설명된 것보다 오래된 DIS가 보낸 CSNP에 설명된 LSP에 대해 PSNP를 전송하여 LSP를 요청합니다.

IS-IS LSPDB 동기화

IS-IS를 올바르게 작동하려면 각 IS의 LSPDB를 동기화할 수 있는 안정적이고 효율적인 프로세스가 필요합니다. IS-IS에서 이 프로세스를 업데이트 프로세스라고 부릅니다. 업데이트 프로세스는 각각의 지원되는 수준에서 개별적으로 작동합니다. 로컬에서 생성된 LSP는 항상 새로운 LSP입니다. 회로에서 네이버로부터 수신한 LSP는 다른 IS에 의해 생성되거나 로컬 IS에 의해 생성된 LSP의 복사본일 수 있습니다. 수신된 LSP는 로컬 LSPDB의 현재 내용보다 더 오래되었거나 동일하거나 더 최신일 수 있습니다.

새 **LSP** 처리

로컬 LSPDB에 새 LSP가 추가되면 LSPDB에서 동일한 LSP의 이전 사본을 대체합니다. 새 LSP는 IS가 현재 새 LSP와 관련된 수준(새 LSP가 수신된 회로를 제외)에서 작동 상태에 있는 모든 회로에 전송되도록 표시되어 있습니다.

멀티 액세스 회로의 경우 IS는 새 LSP를 한 번 플러딩합니다. IS는 멀티 액세스 회로를 위해 DIS에 의해 주기적으로 전송되는 CNSP 집합을 조사합니다. 로컬 LSPDB에 CSNP 집합에 설명된 것보다 최신 LSP가 하나 이상 포함되어 있는 경우(CSNP 집합에 없는 LSP도 포함됨), 이러한 LSP는 멀티 액세스 회로를 통해 다시 플러딩됩니다. 로컬 LSPDB에 CSNP 집합에 설명된 것보다 오래된 LSP가 하나 이상 포함되어 있는 경우(로컬 LSPDB에 없는 CSNP 집합에 설명되어 있는 LSP도 포함됨), PSNP는 업데이트가 필요한 LSP에 대한 설명과 함께 멀티 액세스 회로를 통해 전송됩니다. 멀티 액세스 회로용 DIS는 요청된 LSP를 전송하여 응답합니다.

오래된 **LSP** 처리

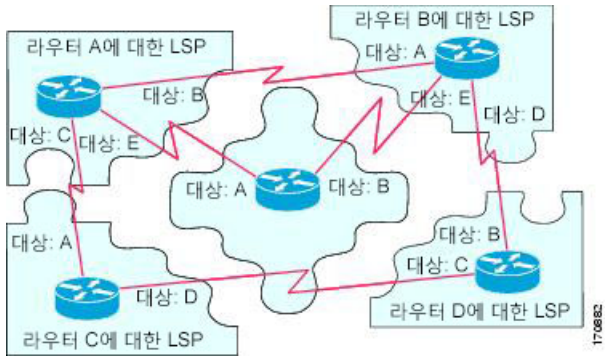
IS는 로컬 LSPDB의 복사본보다 오래된 LSP를 수신할 수 있습니다. IS는 로컬 LSPDB의 복사본보다 오래된 LSP를 설명하는 SNP(전체 또는 부분)를 수신할 수 있습니다. 두 경우 모두 IS는 이전 LSP를 포함하는 이전 LSP 또는 SNP가 수신된 회로에서 로컬 데이터베이스의 LSP를 플러딩하도록 표시합니다. 수행한 작업은 로컬 데이터베이스에 새 LSP를 추가한 후 위에 설명된 내용과 동일합니다.

동일 시기의 **LSP** 처리

업데이트 프로세스의 분산된 특성 때문에 IS가 로컬 LSPDB의 현재 내용과 동일한 LSP의 복사본을 수신할 수 있는 것보다 더 가능성이 있습니다. 멀티 액세스 회로에서 동일 시기의 LSP를 수신할 경우 무시됩니다. DIS에 의해 설정된 CSNP의 주기적 전송은 LSP가 수신되었다는 것을 송신자에게 암시하는 역할을 합니다.

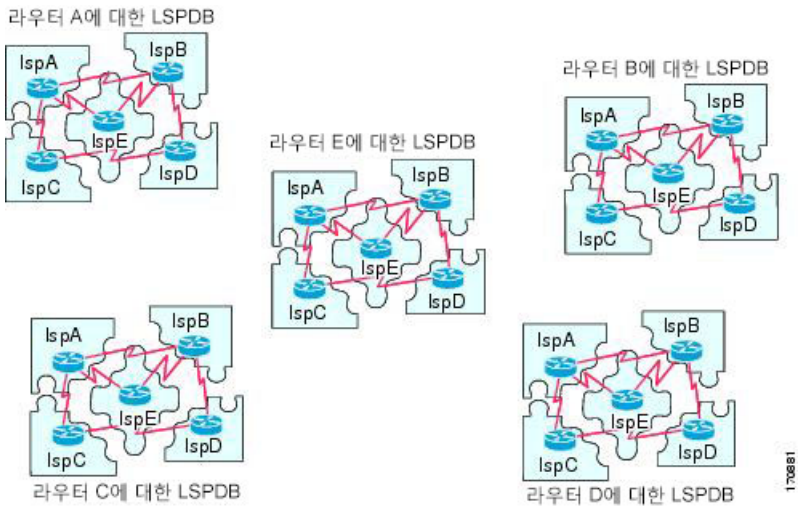
다음 그림에는 LSP를 사용하여 네트워크 맵을 생성하는 방법이 나와 있습니다. 네트워크 토폴로지를 조각 그림 퍼즐로 생각해 보십시오. 각 LSP(IS를 나타냄)는 조각 중 하나입니다. 수준-2 하위 도메인의 모든 수준-2 디바이스 또는 영역에 있는 모든 수준-1 디바이스에 적용될 수 있습니다.

그림 ***64: IS-IS*** 네트워크 맵



다음 그림에는 네이버 디바이스 간에 인접성이 형성된 후 완전히 업데이트된 링크 상태 데이터베이스와 함께 IS-IS 네트워크의 각 디바이스가 나와 있습니다. 레벨-2 하위 도메인의 모든 레벨-2 디바이스 또는 영역에 있는 모든 레벨-1 디바이스에 적용될 수 있습니다.

그림 ***65:*** 동기화된 ***LSPDB***를 사용하는 ***IS-IS*** 디바이스



IS-IS 최단 경로 계산

LSPDB의 내용을 변경하는 경우 각 IS는 독립적으로 최단 경로 계산을 다시 실행합니다. 이 알고리즘은 IS가 그래프의 정점이고 IS 사이의 링크가 음수가 아닌 가중치를 지닌 가장자리인 지시된 그래프를 따라 최단 경로를 찾기 위해 잘 알려진 Dijkstra 알고리즘을 기반으로 합니다. 그래프의 일부로 두 IS 사이의 링크를 고려하기 전에 양방향 연결 검사가 수행됩니다. 이렇게 하면 한 IS가 더 이상 네트워크에서 작동하지 않지만 작동을 중지하기 전에 생성한 LSP 집합을 삭제하지 않은 경우 등 LSPDB에서 오래된 정보를 사용하는 것을 방지할 수 있습니다.

SPF의 출력은 튜플(대상, next hop) 집합입니다. 대상은 프로토콜별로 다릅니다. 여러 개의 동일한 비용 경로가 지원되며, 이 경우 여러 개의 next hop이 동일한 대상에 연결됩니다.

독립적인 SPF는 IS에서 지원되는 각 수준에 대해 수행됩니다. 수준-1 경로와 수준-2 경로 모두에서 동일한 대상에 연결할 수 있는 경우 수준-1 경로를 사용하는 것이 좋습니다.

다른 영역에 하나 이상의 수준-2 네이버가 있음을 나타내는 수준-2 IS는 기본 경로라고도 하는 마지막 리조트의 경로와 동일한 영역에 있는 수준-1 디바이스에서 사용할 수 있습니다. 수준-2 IS는 수준-1 LSP 0에 첨부 비트(ATT)를 설정하여 다른 영역에 대한 첨부 파일을 표시합니다.

참고 IS는 각 수준에서 최대 256개의 LSP를 생성할 수 있습니다. LSP는 숫자 0~255로 식별됩니다. 다른 영역에 대한 첨부 파일을 나타내기 위한 ATT 비트 설정의 중요성 등 LSP 0에는 특정한 속성이 있습니다. 1에서 255까지 번호가 매겨진 LSP에 ATT 비트가 설정되어 있으면 이는 중요하지 않습니다.

IS-IS 종료 프로토콜

IS-IS를 종료(관리 중단 상태로 배치)하여 구성 파라미터를 잃지 않고 IS-IS 프로토콜 구성을 변경할 수 있습니다. IS-IS는 전역 IS-IS 프로세스 수준 또는 인터페이스 수준에서 종료할 수 있습니다. 프로토콜이 해제된 경우 디바이스가 재부팅되면 프로토콜은 비활성화된 상태에서 다시 시작할 것으로 예상됩니다. 프로토콜을 관리 중단 상태로 설정하면 네트워크 관리자가 프로토콜 구성을 잃지 않고 관리상 IS-IS 프로토콜의 작동을 해제할 수 있으며, 매개체를 통한 프로토콜 전환 작업 없이 프로토콜 구성을 연속하여 변경하고 바람직한 상태를 유지하고 적절한 시간에 프로토콜을 다시 활성화할 수 있습니다.

IS-IS에 대한 사전 요구 사항

IS-IS를 구성하기 전에 다음 사전 요구 사항이 필요합니다.

- IPv4 및 IPv6의 정보
- 네트워크 설계 기술 및 IS-IS를 구성하기 전에 트래픽을 통과하는 방식
- 영역을 정의하고, 디바이스에 대한 주소 지정 계획(NET 정의 포함)을 준비하고, IS-IS를 실행할 인터페이스를 결정합니다.

- 디바이스를 구성하기 전에 인접성 표에서 예상해야 하는 네이버를 보여주는 인접성 매트릭스를 준비합니다. 이때 확인 기능을 이용합니다.

IS-IS에 대한 지침

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

클러스터 지침

개별 인터페이스 모드에서만 지원됩니다. Spanned EtherChannel 모드는 지원되지 않습니다.

추가 지침

IS-IS는 양방향 포워딩에서 지원되지 않습니다.

IS-IS 구성

이 섹션에서는 시스템에서 IS-IS 프로세스를 활성화하고 구성하는 방법을 설명합니다.

프로시저

단계 **1** IS-IS 라우팅 전체 활성화, 960 페이지.
단계 **2** IS-IS 인증 활성화, 965 페이지.
단계 **3** IS-IS LSP 구성, 968 페이지
단계 **4** IS-IS 요약 주소 구성, 972 페이지.
단계 **5** IS-IS 패시브 인터페이스 구성, 973 페이지.
단계 **6** IS-IS 인터페이스 구성, 974 페이지.
단계 **7** IS-IS 인터페이스 Hello 패딩 구성, 979 페이지
단계 **8** IS-IS IPv4 주소군 구성, 981 페이지.
단계 **9** IS-IS IPv6 주소군 구성, 986 페이지.

IS-IS 라우팅 전체 활성화

IS-IS 구성은 두 부분으로 수행됩니다. 먼저 전역 구성 모드에서 IS-IS 프로세스를 구성한 다음 라우터 구성 모드에서 IS-IS에 대한 NET 및 라우팅 수준을 지정합니다. 라우터 구성 모드에서 구성할 수 있는 일반 파라미터는 인터페이스별로 구성하는 것보다 네트워크에 더 적합할 수 있습니다. 이 섹션은 이러한 명령을 포함합니다.

두 번째로, 인터페이스 구성 모드의 개별 인터페이스에서 IS-IS 프로토콜을 활성화하여 인터페이스가 동적 라우팅에 참여하고 네이버 디바이스와의 인접성을 형성하도록 할 수 있습니다. 하나 이상의 인터페이스에서 라우팅을 활성화해야 인접성을 설정하고 동적 라우팅을 사용할 수 있습니다. 인터페이스에서 IS-IS를 구성하는 절차는 IS-IS 인터페이스 구성, 974 페이지의 내용을 참조하십시오.

이 절차에서는 ASA 및 라우터 구성 모드의 기타 일반 옵션에서 IS-IS를 IP 라우팅 프로토콜로 활성화하는 방법을 설명합니다.

시작하기 전에

다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context***name* 명령을 입력합니다.

프로시저

단계 **1** ASA에서 라우팅 프로토콜로 IS-IS를 활성화합니다.

router isis

예제:

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

단계 **2** 라우팅 프로세스에 대한 NET를 지정합니다.

net *network-entity-title*

예제:

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

NET는 IS-IS에 대한 디바이스를 식별합니다. NET 정보는 NET 정보, 953 페이지의 내용을 참조하십시오.

단계 **3** (선택 사항) IS-IS 라우팅 프로세스에 대한 라우팅 수준을 할당합니다.

is-type [level-1 | level-2-only | level-1-2]

예제:

```
ciscoasa(config-router)# is-type level-1
```

- (선택 사항) **level-1**— 영역 내 라우팅을 나타냅니다. ASA에서는 해당 영역 내 대상만 파악합니다.
- (선택 사항) **level-2-only**— 영역 간 라우팅을 나타냅니다. ASA는 백본의 일부이며 고유 영역의 수준-1 라우터와 통신하지 않습니다.
- (선택 사항) **level-1-2**— ASA에서는 수준 1 및 수준 2 라우팅을 수행합니다. 이 라우터는 라우팅 프로세스의 인스턴스 2개를 실행합니다. 영역 내의 대상에 대해 하나의 LSDB(수준 1 라우팅)가

있으며 SPF 계산을 실행하여 영역 토폴로지를 검색합니다. 또한 다른 모든 백본(수준 2) 라우터의 LSP가 포함된 다른 LSDB가 있고, 다른 SPF 계산을 실행하여 백본의 토폴로지 및 다른 모든 영역의 존재를 검색합니다.

기존의 IS-IS 구성에서 ASA는 수준 1(영역 내) 및 수준 2(영역 간) 라우터로 작동합니다. 다중 영역 IS-IS 구성에서 구성된 IS-IS 라우팅 프로세스의 첫 번째 인스턴스는 기본적으로 수준 1-2(영역 내 및 영역 간) 라우터입니다. 기본적으로 구성된 IS-IS 프로세스의 나머지 인스턴스는 수준 1 라우터입니다.

참고 IS-IS 라우팅 프로세스의 유형을 구성하는 것이 좋습니다.

단계 **4** ASA에서 IS-IS 동적 호스트 이름 기능을 활성화합니다.

hostname dynamic

이 명령은 기본적으로 사용됩니다. IS-IS에서 동적 호스트 이름에 대한 자세한 내용은 IS-IS 동적 호스트 이름, 954 페이지을 참조하십시오.

단계 **5** ASA에서 모든 인터페이스에 대한 hello 패딩을 구성합니다.

hello padding multi-point

이 명령은 기본적으로 사용됩니다. IS-IS hello를 전체 MTU 크기로 구성합니다. 이를 통해 큰 프레임의 전송 문제 또는 인접 인터페이스의 일치하지 않는 MTU로 인해 발생하는 오류를 조기에 탐지할 수 있습니다.

두 인터페이스의 MTU가 동일한 경우 또는 변환 브리징의 경우 Hello 패딩(IS-IS 라우팅 프로세스용 라우터의 모든 인터페이스에 대해 **no hello padding multi-point**)이 네트워크 대역폭을 낭비하지 않도록 비활성화할 수 있습니다. Hello 패딩이 비활성화된 경우에도 ASA에서는 MTU 불일치 발견의 이점을 유지하기 위해 전체 MTU 크기에 패딩된 처음 5개의 IS-IS hello를 여전히 전송합니다.

특권 EXEC 모드에서 **show clns interface** 명령을 입력하여 hello 패딩이 라우터 수준에서 해제되었음을 표시합니다. 자세한 내용은 IS-IS 모니터링, 992 페이지을 참조하십시오.

단계 **6** (선택 사항) NLSP IS-IS 인접성 상태가 변경(작동 또는 중단)될 경우 ASA에서 로그 메시지를 생성하도록 활성화합니다.

log-adjacency-changes [all]

이 명령은 기본적으로 비활성화되어 있습니다. 인접성 변경 사항 로깅은 대규모 네트워크를 모니터링하는 경우 유용합니다. 메시지는 다음 형식입니다.

예제**:**

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all— (선택 사항) 비_IIH 이벤트에 의해 생성된 변경 사항을 포함합니다.

단계 **7** (선택 사항) 모든 인터페이스에서 임의의 인접성을 형성할 수 없으므로 IS-IS 프로토콜을 비활성화하고 LSP 데이터베이스를 지웁니다.

protocol shutdown

이 명령을 사용하면 모든 기존 IS-IS 명령 파라미터를 제거하지 않고 특정 라우팅 인스턴스에 대한 IS-IS 프로토콜을 비활성화할 수 있습니다. 이 명령을 입력하면 IS-IS 프로토콜이 라우터에서 계속 실행되고 현재 IS-IS 구성을 사용할 수 있지만 IS-IS는 어떤 인터페이스에서도 인접성을 형성하지 않으며 IS-IS LSP 데이터베이스도 지워집니다. 특정 인터페이스에 대해 IS-IS를 비활성화하려면 **isis protocol shutdown** 명령을 사용합니다. 절차는 IS-IS 인터페이스 구성, 974 페이지를 참조하십시오.

단계 **8** (선택 사항) IS-IS IP 접두사에 높은 우선순위를 할당합니다.

route priority high tag *tag-value*

예제:

```
ciscoasa(config-router)# route priority high tag 100
```

tag *tag-value* — 특정 경로 태그를 사용하는 접두사가 있는 IS-IS IP에 높은 우선순위를 할당합니다. 범위는 1~4294967295입니다.

이 명령을 사용하여 전역 라우팅 테이블에서 더 빠른 처리 및 설치를 위해 우선순위가 높은 IS-IS IP 접두사에 태그를 지정하여 더 빠르게 통합할 수 있습니다. 예를 들어, VoIP 게이트웨이 주소는 VoIP 트래픽이 다른 유형의 패킷보다 빠르게 업데이트되도록 먼저 처리됩니다.

단계 **9** (선택 사항) 전역적으로 모든 IS-IS 인터페이스에 대한 메트릭 값을 변경합니다.

metric *default-value* **[level-1 | level-2]**

예제:

```
ciscoasa(config-router)# metric 55 level-1
```

- *default-value* — 링크에 할당되고 대상에 대한 링크를 통해 경로 비용을 계산하는 데 사용되는 메트릭 값입니다. 범위는 1~63입니다. 기본값은 10입니다.
- (선택 사항) **level-1** — 수준 1 IPv4 또는 IPv6 메트릭을 설정합니다.
- (선택 사항) **level-2** — 수준 2 IPv4 또는 IPv6 메트릭을 설정합니다.

모든 IS-IS 인터페이스에 대한 기본 메트릭을 변경해야 하는 경우 **metric** 명령을 사용하는 것이 좋습니다. 이렇게 하면 새 값을 구성하지 않고 인터페이스에서 의도하지 않게 설정된 메트릭을 제거하고 의도하지 않게 인터페이스를 기본 메트릭 10으로 되돌릴 수 있도록 허용하는 등의 사용자 오류를 방지하여 네트워크에서 높은 선호도의 인터페이스가 됩니다.

단계 **10** (선택 사항) 새로운 스타일, 길이, 값 개체(TLV)만 허용하고 생성하도록 ASA를 구성합니다.

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

예제:

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**— 좁은 범위의 메트릭을 사용하는 이전 스타일의 TVL를 사용합니다.

- **transition**— ASA에서 이전 스타일의 TVL와 새로운 스타일의 TVL를 둘 다 허용하도록 지시합니다.
- **wide**— 넓은 범위의 메트릭을 전달하도록 TVL의 새로운 스타일을 사용합니다.
- (선택 사항) **level-1**— 라우팅 수준 1에서 이 명령을 활성화합니다.
- (선택 사항) **level-2**— 라우팅 수준 2에서 이 명령을 활성화합니다.
- (선택 사항) **level-1-2**— 라우팅 수준 1과 수준 2에서 이 명령을 활성화합니다.

이 명령을 실행하면 ASA에서 새로운 스타일의 TLV만 생성하고 허용하므로 이전 스타일의 TLV와 새로운 스타일의 TLV를 모두 생성하는 경우보다 메모리 및 기타 리소스를 적게 사용합니다.

단계 **11** (선택 사항) 모든 인터페이스에서 지정된 ASA의 우선순위를 구성합니다.

priority *number-value*

예제:

```
ciscoasa(config-router)# priority 80
```

number-value — ASA의 우선순위입니다. 범위는 0~127입니다. 기본값은 64입니다.

단계 **12** (선택 사항) IS-IS 영역에 대한 추가적인 수동 주소를 구성합니다.

max-area-addresses *number*

예제:

```
ciscoasa(config-router)# max-area-addresses 3
```

number — 추가할 수동 주소의 수입니다. 범위는 3~254입니다. 기본값은 없습니다.

이 명령을 사용하면 추가 수동 주소를 구성하여 IS-IS 영역의 크기를 최대화할 수 있습니다. 각 수동 주소를 생성하려면 NET 주소를 추가하고 할당할 주소 수를 지정합니다. NET 정보는 NET 정보, 953 페이지의 내용을 참조하십시오.

단계 **13** IS-IS에 대해 다중 경로 로드 공유를 구성합니다.

maximum-paths *number-of-paths*

예제:

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths — 라우팅 테이블에 설치할 경로의 수를 지정합니다. 범위는 1~8입니다. 기본값은 1입니다.

maximum-path 명령은 ECMP가 ASA에서 구성된 경우 IS-IS 다중 로드 공유를 구성하는 데 사용됩니다.

IS-IS 인증 활성화

IS-IS 경로 인증은 승인되지 않은 소스로부터 허가되지 않거나 잘못된 라우팅 메시지가 수신되는 것을 방지할 수 있습니다. 인증되지 않은 라우터가 링크 상태 데이터베이스에 잘못된 라우팅 정보를 주입하지 못하도록 각 IS-IS 영역 또는 도메인에 대한 비밀번호를 설정하거나 IS-IS MD5 또는 향상된 투명 텍스트 인증 유형을 구성할 수 있습니다. 인터페이스별로 인증을 설정할 수도 있습니다. IS-IS 메시지 인증에 구성된 인터페이스의 모든 IS-IS 네이버는 인접성을 위해 동일한 인증 모드와 키로 구성되어야 설정 가능합니다.

영역 및 도메인에 대한 자세한 내용은 IS-IS 정보, 953 페이지를 참조하십시오.

시작하기 전에

IS-IS 경로 인증을 활성화하기 전에 IS-IS를 활성화하고 영역을 설정해야 합니다. 절차는 IS-IS 라우팅 전체 활성화, 960 페이지를 참조하십시오.

프로시저

단계 **1** IS-IS 라우터 구성 모드로 들어가고 IS-IS 영역 인증 비밀번호를 구성합니다.

area-password *password* [**authenticate snp {validate | send-only}**]

예제:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password* — 할당하는 비밀번호입니다.
- (선택 사항) **authenticate snp**— 시스템에서 비밀번호를 SNP에 삽입합니다.
- **validate**— 시스템이 SNP에 비밀번호를 삽입하고 이를 수신하는 SNP에서 비밀번호를 확인합니다.
- **send-only**— 시스템이 SNP에 비밀번호만 삽입하지만, 이를 수신하는 SNP에서 비밀번호를 확인하지는 않습니다. 변환을 지우려면 소프트웨어 업그레이드 중에 이 키워드를 사용합니다.

영역에 있는 모든 ASA에서 이 명령을 사용하면 무단 라우터가 링크 상태 데이터베이스에 잘못된 라우팅 정보를 주입하는 것을 방지할 수 있습니다. 하지만, 이 비밀번호는 일반 텍스트 형식으로 교환되므로 제한된 보안만 제공합니다.

비밀번호는 수준 1(스테이션 라우터 수준) PDU LSP, CSNP 및 PSNP에서 삽입됩니다. **authenticate snp** 키워드를 **validate** 또는 **send-only** 키워드와 함께 지정하지 않을 경우, IS-IS 프로토콜은 SNP에 비밀번호를 삽입하지 않습니다.

단계 **2** IS-IS 라우터 구성 모드로 들어가고 IS-IS 도메인 인증 비밀번호를 구성합니다.

domain-password *password* [**authenticate snp {validate | send-only}**]

예제:

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password* — 할당하는 비밀번호입니다.
- (선택 사항) **authenticate snp**— 시스템에서 시퀀스 번호 PDU(SNP)에 비밀번호를 삽입합니다.
- **validate**— 시스템이 SNP에 비밀번호를 삽입하고 이를 수신하는 SNP에서 비밀번호를 확인합니다.
- **send-only**— 시스템이 SNP에 비밀번호만 삽입하고 SNP에서 수신되는 비밀번호는 확인하지 않습니다. 변환을 지우려면 소프트웨어 업그레이드 중에 이 키워드를 사용합니다.

이 비밀번호는 일반 텍스트 형식으로 교환되므로 제한된 보안만 제공합니다.

비밀번호는 수준 2(영역 라우터 수준) PDU LSP, CSNP 및 PSNP에서 삽입됩니다. **authenticate snp** 키워드를 **validate** 또는 **send-only** 키워드와 함께 지정하지 않을 경우, IS-IS 프로토콜은 SNP에 비밀번호를 삽입하지 않습니다.

단계 **3** 전송 중인 IS-IS 패킷에 대해서만 인증을 수행하도록 전역적으로 또는 인터페이스별로 IS-IS 인스턴스를 구성합니다(수신되지 않음).

라우터 모드:**authentication send-only [level-1 | level-2]**

예제**:**

```
ciscoasa(config-router)# authentication send-only level-1
```

인터페이스 모드:**isis authentication send-only [level-1 | level-2]**

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- (선택 사항) **level-1** — 인증은 전송 중인(수신되지 않음) 인증 수준 1 패킷에서만 수행됩니다.
- (선택 사항) **level-2** — 인증은 전송 중인(수신되지 않음) 인증 수준 2 패킷에서만 수행됩니다.

인증 구현이 원활하게 진행되도록 인증 모드 및 인증 키 체인을 구성하기 전에 이 명령을 사용합니다. 수준 1 또는 수준 2를 지정하지 않으면 두 수준에만 전송이 적용됩니다.

참고 인증이 수신 중인 패킷에서 확인되지 않고 전송 중인 패킷에만 삽입된 경우 ASA는 각 ASA에서 키를 구성하는 데 더 많은 시간을 할애합니다. 이 명령을 사용하여 통신해야 하는 모든 ASA를 구성한 후 각 ASA에서 인증 모드와 키 체인을 사용하도록 활성화합니다.

단계 **4** 전역적으로 또는 인터페이스별로 IS-IS 인스턴스에 대해 IS-IS 패킷에 사용되는 인증 모드 유형을 지정합니다.

라우터 모드:**authentication mode {md5 | text} [level-1 | level-2]**

예제**:**

```
ciscoasa(config-router)# authentication mode md5 level-1
```

인터페이스 모드:**isis authentication mode {md5 | text} [level-1 | level-2]**

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5**— Message Digest 5 인증을 활성화합니다.
- **text**— 일반 텍스트 인증을 사용합니다.
- (선택 사항) **level-1**— 수준 1 패킷에 대해서만 지정된 인증을 활성화합니다.
- (선택 사항) **level-2**— 수준 2 패킷에 대해서만 지정된 인증을 활성화합니다.

area-password 또는 **domain-password**를 사용하여 일반 텍스트 인증을 구성한 경우, IS-IS 인증 모드는 이러한 명령을 재정의합니다. **isis authentication mode**를 구성한 다음 **area-password** 또는 **domain-password**를 구성하려고 시도하는 경우, 해당 작업은 허용되지 않습니다. 수준 1 또는 수준 2를 지정하지 않으면 두 수준 모두에 모드가 적용됩니다.

단계 **5** 전역적으로 또는 인터페이스별로 IS-IS에 대한 인증을 활성화합니다.

라우터 모드: **authentication key [0 | 8]** *password* **[level-1 | level-2]**

예제**:**

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

인터페이스 모드: **isis authentication key [0 | 8]** *password* **[level-1 | level-2]**

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0**— 암호화되지 않은 비밀번호가 뒤따르도록 지정합니다.
- **8**— 암호화된 비밀번호가 뒤따르도록 지정합니다.
- *password*— 인증을 활성화하고 키를 지정합니다.
- (선택 사항) **level-1**— 수준 1 패킷에 대해서만 인증을 활성화합니다.
- (선택 사항) **level-2**— 수준 2 패킷에 대해서만 인증을 활성화합니다.

key 명령을 사용하여 비밀번호가 구성되지 않은 경우, 키 인증이 수행되지 않습니다. 키 인증은 일반 텍스트 또는 MD5 인증에 적용할 수 있습니다. 모드를 설정하려면 4단계를 참조하십시오. 한 번에 한 개의 인증 키가 IS-IS에 적용됩니다. 두 번째 키를 구성하는 경우 첫 번째 키가 재정의됩니다. 수준 1 또는 수준 2를 지정하지 않으면 두 수준 모두에 비밀번호가 적용됩니다.

단계 **6** 인터페이스에 대한 인증 비밀번호를 구성합니다.

isis password *password* **[level-1 | level-2]**

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis password analyst level-1
```

- *password* — 인터페이스에 할당하는 인증 비밀번호입니다.
- (선택 사항) **level-1** — 수준 1에 대해 독립적으로 인증 비밀번호를 구성합니다. 수준 1 라우팅의 경우 ASA는 스테이션 라우터로만 작동합니다.
- (선택 사항) **level-2** — 수준 2에 대해 독립적으로 인증 비밀번호를 구성합니다. 수준 2 라우팅의 경우 ASA는 영역 라우터로만 작동합니다.

이 명령을 사용하면 무단 라우터가 이 ASA와 인접성을 형성하는 것을 방지하여 침입자로부터 네트워크를 보호할 수 있습니다. 비밀번호는 일반 텍스트 형식으로 교환되므로 제한된 보안을 제공합니다. **level-1** 및 **level-2** 키워드를 사용하여 서로 다른 라우팅 수준에 대해 다른 비밀번호를 할당할 수 있습니다.

예

다음 예에는 수준 1 패킷에 대해 MD5 인증을 수행하고 site1이라는 키 체인에 속한 키를 전송하는 IS-IS 인스턴스가 나와 있습니다.

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

IS-IS LSP 구성

IS는 LSP를 생성하여 IS-IS에 직접 연결되어 있는 대상 및 네이버를 알립니다. LSP에 대한 자세한 내용은 IS-IS PDU 유형, 954 페이지을 참조하십시오.

빠른 통합 구성을 갖도록 하려면 다음 명령을 사용하여 LSP를 구성합니다.

시작하기 전에

다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context***name* 명령을 입력합니다.

프로시저

단계 **1** 라우터 구성 모드로 들어갑니다.

router isis

예제**:**

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

단계 **2** LSP를 삭제하는 대신 내부 체크섬 오류와 함께 수신된 IS-IS LSP를 무시하도록 ASA를 구성합니다.

ignore-lsp-errors

예제**:**

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS에서는 잘못된 데이터 링크 체크섬이 있는 LSP를 수신기에 의해 삭제해야 하므로 패킷의 이니시에이터가 이를 재생성합니다. 네트워크에 올바른 데이터 링크 체크섬을 사용하여 LSP를 제공하면서 데이터가 손상되는 링크가 있는 경우 많은 수의 패킷을 삭제하고 재생성하는 연속적인 주기가 발생할 수 있으므로 네트워크가 작동하지 않을 수 있습니다. 이 명령을 사용하여 LSP를 제거하는 대신 무시합니다. 기본값은 enabled입니다.

단계 **3** 수동 인터페이스에 속하는 접두사만 알리도록 IS-IS를 구성합니다.

advertise passive-only

이 명령을 사용하면 LSP 알림에서 연결된 네트워크의 IP 접두사가 제외되므로 라우터 비 의사 노드 LSP에 더 적은 접두사가 알려지기 때문에 IS-IS 통합 시간이 단축됩니다.

단계 **4** IS-IS LSP를 전체 설정으로 구성합니다.

fast-flood *lsp-number*

예제**:**

```
ciscoasa(config-router)# fast-flood 7
```

(선택 사항) *lsp-number* — SPF를 시작하기 전에 플러딩할 LSP 수입니다.

이 명령을 사용하면 ASA에서 지정된 LSP 수가 전송됩니다. LSP는 SPF를 실행하기 전에 SPF를 호출합니다. LSP 플러딩 프로세스 속도를 높이면 전체적인 통합 시간이 향상됩니다. 범위는 1~15입니다. 기본값은 5입니다.

참고 라우터가 SPF 계산을 실행하기 전에 LSP의 빠른 플러딩을 활성화하는 것이 좋습니다.

단계 **5** IS-IS LSP의 MTU 크기를 구성합니다.

lsp-mtu 바이트

예제**:**

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes — 최대 패킷 크기(바이트)입니다. 바이트 수는 네트워크에 있는 모든 링크의 가장 작은 MTU보다 작거나 같아야 합니다. 범위는 128~4352입니다.

단계 **6** 새로 고치지 않고 ASA의 데이터베이스에서 LSP를 유지할 최대 시간을 설정합니다.

max-lsp-lifetime *seconds*

예제**:**

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds — LSP 수명(초)입니다. 범위는 1~65,535입니다. 기본값은 1200입니다.

새로 고친 LSP가 도착하기 전에 수명이 초과되는 경우, LSP는 데이터베이스에서 삭제됩니다.

단계 **7** SPF 계산의 IS-IS 제한을 맞춤화합니다.

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

예제**:**

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (선택 사항) **level-1** — 수준 1 영역에만 간격을 적용합니다.
- (선택 사항) **level-2** — 수준 2 영역에만 간격을 적용합니다.
- *spf-max-wait* — 두 번 연속된 SPF 계산 사이의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 10초입니다.
- (선택 사항) *spf-initial-wait* — 토폴로지를 첫 번째 SPF 계산 이전에 변경한 후 첫 번째 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5500밀리초입니다(5.5초).

  이후 각 대기 간격은 대기 간격이 지정된 SPF 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.
- (선택 사항) *spf-second-wait* — 첫 번째와 두 번째 SPF 계산 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5500밀리초입니다(5.5초).

토폴로지가 변경된 경우에만 SPF 계산이 수행됩니다. 이 명령을 사용하면 소프트웨어가 SPF 계산을 수행하는 빈도가 제어됩니다.

참고 SPF 계산은 프로세서를 많이 사용합니다. 따라서 이 작업이 완료되는 빈도를 제한하는 데 유용하며 특히 영역이 크고 토폴로지가 자주 변경되는 경우 유용합니다. SPF 간격을 늘리면 ASA의 프로세서 로드가 줄어들지만 잠재적으로 통합 속도가 느려집니다.

단계 **8** LSP 생성의 IS-IS 제한을 맞춤화합니다.

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

예제**:**

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- (선택 사항) **level-1** — 레벨 1 영역에만 간격을 적용합니다.
- (선택 사항) **level-2** — 레벨 2 영역에만 간격을 적용합니다.
- *lsp-max-wait* — 생성되고 있는 2개의 연속 발생 LSP 간의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 5일입니다.
- (선택 사항) *lsp-initial-wait* — 첫 번째 LSP를 생성하기 전에 초기 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 50밀리초입니다.

  이후 각 대기 간격은 대기 간격이 지정된 LSP 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.
- (선택 사항) *lsp-second-wait* — 첫 번째와 두 번째 LSP 생성 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5000밀리초입니다(5초).

  이 명령을 사용하면 생성 중인 LSP 간의 지연 시간이 제어됩니다.

단계 **9** LSP 새로 고침 간격을 설정합니다.

lsp-refresh-interval *seconds*

예제**:**

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

(선택 사항) *seconds* — LSP의 새로 고침 간격입니다. 범위는 1~65535초입니다. 기본값은 900초(15분)입니다.

새로 고침 간격은 소프트웨어가 LSP에서 전송하는 경로 토폴로지 정보를 주기적으로 전송하는 속도를 결정합니다. 이 작업은 데이터베이스 정보가 너무 오래되는 것을 방지하기 위해 수행됩니다.

참고 LSP는 수명 만료 전에 주기적으로 새로 고칠 수 있어야 합니다. **lsp-refresh-interval** 명령에 대한 설정된 값은 **max-lsp-lifetime** 명령에 대해 설정된 값보다 작아야 합니다. 그렇지 않으면, LSP가 새로 고쳐지기 전에 시간 초과됩니다. LSP 새로 고침 간격에 비해 LSP 수명을 너무 낮게 설정하는 경우 소프트웨어는 LSP가 시간 초과되는 것을 방지하기 위해 LSP 새로 고침 간격을 줄입니다.

단계 **10** PRC의 IS-IS 제한을 맞춤화합니다.

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

예제**:**

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* — 두 번 연속된 PRC 계산 사이의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 5일입니다.

- (선택 사항) *prc-initial-wait* — 토폴로지 변경 이후 첫 번째 PRC 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 2000밀리초입니다.

  이후 각 대기 간격은 대기 간격이 지정된 PRC 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.

- (선택 사항) *prc-second-wait* — 첫 번째와 두 번째 PRC 계산 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5000밀리초입니다(5초).

  PRC는 SPF 계산을 수행하지 않고 경로를 계산하는 소프트웨어 프로세스입니다. 이는 라우팅 시스템 자체의 토폴로지가 변경되지 않았지만, 특정 IS가 발표한 정보에 변화가 탐지되거나 RIB에 이러한 경로를 재설치해야 할 때 가능합니다.

단계 **11** PDU가 가득 찼을 때 경로 억제를 구성합니다.

lsp-full suppress {external [interlevel] | interlevel [external] | none}

예제**:**

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external**— 이 ASA에서 재배포된 경로를 표시하지 않습니다.
- **interlevel**— 다른 수준에서 오는 모든 경로를 표시하지 않습니다. 예를 들어, 수준 2 LSP가 가득 차면 수준 1의 경로가 표시되지 않습니다.
- **none**— 경로를 억제하지 않습니다.

IS-IS로 재배포된 경로 수에 제한이 없는 네트워크(즉, **redistribute maximum-prefix** 명령이 구성되지 않음)에서는 LSP가 채워지고 경로가 삭제될 수 있습니다. **lsp-full suppress** 명령을 사용하여 LSP가 가득 찰 경우 미리 억제할 경로를 정의합니다.

IS-IS 요약 주소 구성

지정된 수준에 대해 여러 그룹의 주소를 요약할 수 있습니다. 다른 라우팅 프로토콜에서 확인된 경로도 요약할 수 있습니다. 요약 광고에 사용되는 메트릭은 특정 경로 중에서도 가장 작은 메트릭입니다. 이는 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

네트워크 숫자 경계에서 발생하지 않는 요약 주소를 생성하려는 경우 또는 자동 경로 요약을 비활성화하고 ASA에서 요약 주소를 사용하려는 경우 요약 주소를 수동으로 정의해야 합니다.

프로시저

단계 **1** 라우터 구성 모드로 들어갑니다.

router isis

예제**:**

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

단계 **2** IS-IS에 집계 주소를 생성합니다.

summary-address *address mask* **[level-1 | level-1-2 | level-2] tag** *tag-number* **metric** *metric-value*

예제**:**

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address* — IP 주소 범위에 대해 요약 주소를 지정합니다.
- *mask* — 요약 경로에 사용되는 IP 서브넷 마스크입니다.
- (선택 사항) **level-1**— 수준 1로 재배포된 경로만 구성된 주소 및 마스크 값으로 요약되어 있습니다.
- (선택 사항) **level-1-2**— 요약 경로는 경로를 수준 1과 수준 2로 재배포할 때, 수준 2 IS-IS가 수준 1 경로를 해당 영역에서 도달할 수 있는 것으로 알릴 때 적용됩니다.
- (선택 사항) **level-2**— 수준 1 라우팅을 통해 확인된 경로가 구성된 주소 및 마스크 값이 있는 수준 2 백본으로 요약되어 있습니다. 수준 2 IS-IS에 대한 재배포된 경로도 요약되어 있습니다.
- (선택 사항) **tag** *tag-number* — 요약 경로에 태그를 지정하는 데 사용된 수를 지정합니다. 범위는 1~4294967295입니다.
- (선택 사항) **metric** *metric-value* — 요약 경로에 적용된 메트릭 값을 지정합니다. **metric** 키워드는 링크에 할당되고 대상에 대한 링크를 통해 경로 비용을 계산하는 데 사용됩니다. 수준 1 또는 수준 2 라우팅에 대해서만 이 메트릭을 구성할 수 있습니다. 범위는 1~4294967295입니다. 기본값은 10입니다.

인터페이스에 대한 메트릭 값을 확인하려면 **show clns interface** 명령을 입력합니다. 자세한 내용은 IS-IS 모니터링, 992 페이지을 참조하십시오.

IS-IS 패시브 인터페이스 구성

인터페이스 주소를 토폴로지 데이터베이스에 계속 포함한 상태로 인터페이스에서 IS-IS hello 패킷과 라우팅 업데이트를 비활성화할 수 있습니다. 이러한 인터페이스는 IS-IS 네이버 인접성을 형성하지 않습니다.

IS-IS 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 패시브 인터페이스에서 IS-IS를 사용하지 않도록 패시브 인터페이스(**passive-interface** 명령 사용)를 구성합니다. 또한, 업데이트를 위해 ASA에서 사용되는 IS-IS의 버전을 지정할 수 있습니다. 패시브 라우팅에서는 IS-IS 라우팅 정보의 알림을 제어할 수 있도록 지원하고, 인터페이스에서 IS-IS 라우팅 업데이트의 전송 및 수신을 비활성화합니다.

프로시저

단계 **1** 라우터 구성 모드로 들어갑니다.

router isis

예제**:**

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

단계 **2** ASA에서 패시브 인터페이스를 구성합니다.

passive-interface *interface-name*

예제**:**

```
ciscoasa(config-router)# passive-interface inside
```

- **default**— 모든 인터페이스에서 라우팅 업데이트를 표시하지 않습니다.
- **management**— Management 0/1 인터페이스에서 업데이트를 표시하지 않습니다.
- **management2**— Management 0/2 인터페이스에서 업데이트를 표시하지 않습니다.
- **inside**— 내부 인터페이스에서 업데이트를 표시하지 않습니다.

이 명령은 인트페이스가 IS-IS 네이버 인접성을 형성하지 않지만 IS-IS 데이터베이스에 인터페이스 주소를 포함하도록 구성합니다.

단계 **3** 패시브 인터페이스를 알리도록 ASA를 구성합니다.

advertise passive-only

예제**:**

```
ciscoasa(config-router)# advertise passive-only
```

이 명령은 패시브 인터페이스에 속하는 접두사만 알리도록 IS-IS를 구성합니다. LSP 알림에서 연결된 네트워크의 IP 접두사를 제외하며 IS-IS 통합 시간이 줄어듭니다.

IS-IS 인터페이스 구성

이 절차에서는 IS-IS 라우팅을 위해 개별 ASA 인터페이스를 수정하는 방법을 설명합니다. 다음을 수정할 수 있습니다.

- 인터페이스에서의 IS-IS 활성화, IS-IS 종료 프로토콜 활성화, 우선순위, 태그 및 인접성 필터 등의 일반 설정.

- 인증 키 및 모드 — 인터페이스에서 인증을 구성하는 절차에 대한 내용은 IS-IS 인증 활성화, 965 페이지를 참고하십시오.
- Hello 패딩 값 — 인터페이스에서 hello 패딩을 구성하는 절차에 대한 내용은 IS-IS 인터페이스 Hello 패딩 구성, 979 페이지을 참고하십시오.
- LSP 설정
- IS-IS 메트릭 계산에 사용되는 인터페이스 지연 메트릭.

시작하기 전에

IS-IS 라우팅 프로세스를 유용하게 사용하려면 먼저 NET을 할당하고 일부 인터페이스에 IS-IS가 활성화되어 있어야 합니다. 레벨 2(영역 간) 라우팅을 수행하기 위해 프로세스를 하나만 구성할 수 있습니다. 레벨 2 라우팅이 특정 프로세스에서 구성된 경우, 모든 추가 프로세스가 자동으로 레벨 1로 구성됩니다. 영역 내(레벨 1) 라우팅을 동시에 수행하기 위해 이 프로세스를 구성할 수 있습니다. 인터페이스는 연결된 라우팅 프로세스가 레벨 1과 레벨 2 라우팅을 모두 수행하는 경우를 제외하고 둘 이상의 영역에 속할 수 없습니다. 절차는 IS-IS 라우팅 전체 활성화, 960 페이지를 참조하십시오.

프로시저

단계 **1** 인터페이스 구성 모드로 들어갑니다.

interface *interface_id*

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

단계 **2** IS-IS 인접성 설정을 필터링합니다.

isis adjacency-filter *name* **[match-all]**

예제**:**

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- *name(*이름*)* — 적용할 필터 집합 또는 식의 이름입니다.
- (선택 사항) **match-all** — 인접성을 수락하기 위해서는 모든 NSAP 주소가 필터와 일치해야 합니다. 이 설정이 지정되지 않은 경우(기본값), 인접성 수락을 위해 한 개의 주소만 필터와 일치하면 됩니다.

필터링은 hello의 각 영역 주소를 시스템 ID와 결합하고 수신 IS-IS hello 패킷에서부터 NSAP 주소를 구축하여 수행됩니다. 그런 다음 이러한 NSAP 주소 각각은 필터를 통해 전달됩니다. 일치하는 NSAP가 있는 경우, 모든 주소를 전달해야 하는 **match-all** 키워드가 지정된 경우를 제외하고 필터는 전달된 것으로 간주됩니다. **match-all** 키워드의 기능은 특정 주소가 없는 경우에만 인접성을 수락하는 등의 음성 테스트를 수행할 때 유용합니다.

단계 **3** 연결된 네트워크의 IS-IS 접두사를 IS-IS 인터페이스에서 LSP 알림으로 알립니다.

isis advertise prefix

예제**:**

```
ciscoasa(config-if)# isis advertise prefix
```

IS-IS 통합 시간을 개선하려면 **no isis advertise prefix** 명령을 사용합니다. 이렇게 하면 LSP 알림에서 연결된 네트워크의 IP 접두사를 제외하며 IS-IS 통합 시간이 줄어듭니다. 기본값은 enabled입니다.

참고 IS-IS 인터페이스별로 이 명령의 **no** 형식을 구성하면 라우터의 비 의사 노드 LSP에서 더 적은 수의 접두사를 알립니다. 따라서 이러한 방식은 IS-IS 통합 시간을 줄이는 소규모 해결 방법입니다. **isis advertise prefix** 명령 대신 **advertise passive-only** 명령을 사용할 수 있습니다. 이는 IS-IS 인스턴스별로 구성되어 있으므로 확장 가능한 해결 방법입니다.

단계 **4** IS-IS 인터페이스에서 IPv6를 활성화합니다.

ipv6 router isis

예제**:**

```
ciscoasa(config-if)# ipv6 router isis
```

단계 **5** 인터페이스별로, 연속되는 IS-IS LSP 전송 간의 지연 시간 간격을 구성합니다.

isis lsp-interval 밀리초

예제**:**

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds — 연속되는 LSP의 시간 지연입니다. 범위는 1~4294967298입니다. 기본값은 33밀리초입니다.

많은 IS-IS 네이버 및 인터페이스가 있는 토폴로지에서 ASA는 LSP 전송 및 수신 시 발생하는 CPU 로드로 인해 어려움을 겪을 수 있습니다. 이 명령은 LSP 전송 속도(및 묵시적으로 다른 시스템의 수신 속도)를 줄여 줍니다

단계 **6** IS-IS 메트릭의 값을 구성합니다.

isis metric {*metric-value* | **maximum**} [**level-1 | level-2**]

예제**:**

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value* — 링크에 할당되고 네트워크에 있는 다른 대상에 대한 링크를 통해 서로 간의 라우터 비용을 계산하는 데 사용되는 메트릭입니다. 레벨 1 또는 레벨 2 라우팅에 대해 이 메트릭을 구성할 수 있습니다. 범위는 1~63입니다. 기본값은 10입니다.
- **maximum**— SPF 계산에서 링크 또는 인접성을 제외합니다.

- (선택 사항) **level-1** — 이 메트릭을 레벨 1(영역 내) 라우팅의 SPF 계산에만 사용해야 한다고 지정합니다. 선택 사항 키워드가 지정되지 않은 경우, 메트릭이 라우팅 레벨 1과 레벨 2에서 활성화됩니다.
- (선택 사항) **level-2** — 이 메트릭을 레벨 2(영역 간) 라우팅의 SPF 계산에만 사용해야 한다고 지정합니다. 선택 사항 키워드가 지정되지 않은 경우, 메트릭이 라우팅 레벨 1과 레벨 2에서 활성화됩니다.

단계 **7** 인터페이스에서 지정된 ASA의 우선순위를 구성합니다.

isis priority *number-value* **[level-1 | level-2]**

예제:

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value* — ASA의 우선순위를 설정합니다. 범위는 0~127입니다. 기본값은 64입니다.
- (선택 사항) **level-1** — 레벨 1의 우선순위를 개별적으로 설정합니다.
- (선택 사항) **level-2** — 레벨 2의 우선순위를 개별적으로 설정합니다.

우선순위는 LAN에서 어떤 ASA가 전용 라우터 또는 DIS가 될지 결정하는 데 사용됩니다. 우선순위는 hello 패킷에서 알려집니다. 우선순위가 가장 높은 ASA는 DIS가 됩니다.

참고 IS-IS에는 백업 전용 라우터가 없습니다. 우선순위를 0으로 설정하면 이 시스템이 DIS가 될 가능성이 작아지지만 DIS가 되지 못하는 것은 아닙니다. 더 높은 우선순위를 지닌 라우터가 작동 상태가 되면 현재 DIS로부터 역할을 인계받습니다. 우선순위가 동일한 경우 가장 높은 우선순위를 지닌 MAC 주소가 선택됩니다.

단계 **8** IS-IS 프로토콜이 지정된 인터페이스에서 인접성을 형성할 수 없도록 하기 위해 IS-IS 프로토콜을 비활성화하고 해당 인터페이스의 IP 주소를 ASA에서 생성된 LSP에 추가합니다.

isis protocol shutdown

예제:

```
ciscoasa(config-if)# isis protocol shutdown
```

이 명령을 사용하면 구성 파라미터를 제거하지 않고 지정된 인터페이스에 대해 IS-IS 프로토콜을 비활성화할 수 있습니다. IS-IS 프로토콜은 이 명령이 구성되어 있는 인터페이스에 대해 인접성을 형성하지 않으며 해당 인터페이스의 IP 주소는 라우터에서 생성된 LSP에 추가됩니다. IS-IS가 모든 인터페이스에서 인접성을 형성하지 않고 IS-IS LSP 데이터베이스를 지우지 않도록 하려면 **protocol shutdown** 명령을 사용합니다. 절차는 IS-IS 라우팅 전체 활성화, 960 페이지를 참조하십시오.

단계 **9** 각 IS-IS LSP의 재전송 간 시간 간격을 구성합니다.

isis retransmit-interval *seconds*

예제:

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

(선택 사항) *seconds* — 각 LSP의 재전송 간 시간 간격입니다. 이 숫자는 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 범위는 0~65535입니다. 기본값은 5일입니다.

seconds 인수가 보존되지 않으면 불필요한 재전송이 일어나게 됩니다. 이 명령은 LAN(멀티 포인트) 인터페이스에 영향을 미치지 않습니다.

단계 **10** 각 IS-IS LSP의 재전송 간 시간 간격을 구성합니다.

isis retransmit-throttle-interval 밀리초

예제**:**

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

(선택 사항) *milliseconds* — 인터페이스에서의 LSP 재전송 간 최소 지연 시간입니다. 범위는 0~65535입니다.

이 명령은 LSP와 인터페이스가 많은 대규모 네트워크에서 LSP 재전송 트래픽을 제어할 때 유용할 수 있습니다. 이 명령은 인터페이스에서 LSP가 재전송될 수 있는 속도를 제어합니다.

이 명령은 LSP가 인터페이스에서 전송되는 속도(**isis lsp-interval** 명령을 통해 제어됨)와 단일 LSP의 재전송 간 시간 간격(**isis retransmit-interval** 명령을 통해 제어됨)과는 구별됩니다. 한 ASA에서 네이버로 이동하는 라우팅 트래픽의 제공된 로드를 제어하기 위해 이러한 명령을 조합할 수 있습니다.

단계 **11** IP 접두사가 IS-IS LSP에 추가되는 경우 인터페이스에 대해 구성된 IP 주소에 태그를 설정합니다.

isis tag *tag-number*

예제**:**

```
ciscoasa(config-if)# isis tag 100
```

tag-number — IS-IS 경로에서 태그 역할을 하는 번호입니다. 범위는 1~4294967295입니다.

예를 들어, 경로를 재배포하거나 경로를 요약하기 위해 태그가 사용될 때까지 태그가 지정된 경로에서는 아무런 동작이 일어나지 않습니다. 이 태그는 패킷의 새로운 정보이므로, 이 명령을 구성하면 ASA에서 새 LSP를 생성하게 됩니다.

예

이 예에서 두 개의 인터페이스는 서로 다른 태그 값으로 태그가 지정됩니다. 기본적으로 이러한 두 IP 주소는 IS-IS 레벨 1 및 레벨 2 데이터베이스에 추가되어 있습니다. 그러나 경로 맵에서 **redistribute** 명령을 사용하여 태그 110을 일치시키는 경우, 유일한 IP 주소는 172.16입니다. 0.0은 레벨 2 데이터베이스에 추가됩니다.

```
ciscoasa (config)# interface GigabitEthernet1/0
```

```
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

IS-IS 인터페이스 Hello 패딩 구성

Hello 패킷은 네이버 검색 및 유지 관리를 담당합니다. 다음 hello 패딩 파라미터를 인터페이스 수준에서 구성할 수 있습니다. 전체 IS-IS에 대해 hello 패딩을 활성화/비활성화하려면 IS-IS 라우팅 전체 활성화, 960 페이지을 참고하십시오.

프로시저

단계 **1** 인터페이스 구성 모드로 들어갑니다.

interface *interface_id*

예제:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

단계 **2** ASA에서 모든 인터페이스에 대해 IIH PDU(IS-IS Hello Protocol Data Unit)에서 패딩을 구성하려면 인터페이스 구성 모드로 들어갑니다.

isis hello padding

예제:

```
ciscoasa(config-if)# isis hello padding
```

전체 MTU에 hello를 패딩하면 큰 프레임의 전송 문제 또는 인접 인터페이스의 일치하지 않는 MTU로 인해 발생하는 오류를 조기에 탐지할 수 있습니다. IS-IS hello 패딩은 기본적으로 활성화되어 있습니다.

참고 두 인터페이스의 MTU가 동일하거나 변환 브리징의 경우 Hello 패딩이 네트워크 대역폭을 낭비하지 않도록 비활성화할 수 있습니다. Hello 패딩이 비활성화되어 있는 동안에도 ASA는 MTU 불일치 항목을 발견하는 이점을 유지하기 위해 전체 MTU 크기에 패딩된 처음 5개의 IS-IS hello를 계속해서 전송합니다.

단계 **3** IS-IS에서 보낸 연속 hello 패킷 간의 시간 간격을 지정합니다.

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

예제:

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds(초)* — hello 패킷 간의 시간 간격입니다. 기본적으로 Hello 간격(초)의 3배인 값은 전송된 Hello 패킷의 보류 시간으로 알려집니다. **isis hello-multiplier** 명령을 구성하여 승수 3을 변경할 수 있습니다. hello 간격이 작을수록 토폴로지 변경 사항이 더 빨리 탐지되지만 라우팅 트래픽이 많아집니다. 범위는 0~65535입니다. 기본값은 10입니다.
- **minimal** — 시스템에서 hello 승수에 기반하여 hello 간격을 계산하므로(**isis hello-multiplier** 명령으로 지정됨) 결과 보류 시간이 1초가 됩니다.
- (선택 사항) **level-1** — 레벨 1에 대한 hello 간격을 개별적으로 구성합니다. X.25, SMDS(Switched Multimegabit Data Service), 프레임 릴레이 멀티 액세스 네트워크에서 이 옵션을 사용합니다.
- (선택 사항) **level-2** — 레벨 2에 대한 hello 간격을 개별적으로 구성합니다. X.25, SMDS, 프레임 릴레이 멀티 액세스 네트워크에서 이 옵션을 사용합니다.

참고 hello 간격이 느리면 대역폭과 CPU 사용량이 절약되지만 예를 들어, TE(TrafficEngineering) 터널을 사용하는 대규모 구성과 같이 빠른 hello 간격이 선호되는 경우가 있습니다. TE 터널이 IS-IS를 IGP(Interior Gateway Protocol)로 사용하는 경우, IP 라우팅 프로세스가 네트워크의 인그레스 포인트(헤드엔드)의 라우터에서 다시 시작되면 모든 TE 터널이 기본 hello 간격으로 다시 알려집니다. hello 간격이 빠르면 이렇게 다시 알려지는 것이 방지됩니다. 빠른 hello 간격을 구성하려면 **isis hello-multiplier** 명령을 사용하여 IS-IS hello 간격을 수동으로 늘려야 합니다.

단계 **4** ASA가 인접성이 중단되었음을 선언하기 전에 네이버가 누락해야 하는 IS-IS hello 패킷의 수를 지정합니다.

isis hello-multiplier *multiplier* **[level-1 | level-2]**

예제:

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler* — IS-IS hello 패킷에서 알려진 보류 시간은 hello 승수 곱하기 hello 간격으로 설정됩니다. 네이버는 알려진 보류 시간 동안 IS-IS hello 패킷을 수신하지 않은 후에 이 ASA에 대한 인접성이 중단됨을 선언합니다. 인터페이스별로 보류 시간(따라서 hello 승수와 hello 간격)을 설정할 수 있으며 보류 시간은 한 영역에 있는 여러 라우터 간에 다를 수 있습니다. 범위는 3~1000입니다. 기본값은 3입니다.
- (선택 사항) **level-1** — 레벨 1 인접성에 대한 hello 승수를 개별적으로 구성합니다.
- (선택 사항) **level-2** — 레벨 2 인접성에 대한 hello 승수를 개별적으로 구성합니다.

Hello 패킷이 자주 손실되고 IS-IS 인접성이 불필요하게 실패하는 경우 이 명령을 사용합니다.

참고 작은 hello 승수를 사용하면 빠른 통합이 가능하지만 라우팅이 더 불안정해질 수 있습니다. Hello 승수를 더 큰 값으로 변경하여 필요한 경우 네트워크 안정성을 지원합니다. hello 승수를 기본값인 3보다 작게 구성하지 마십시오.

단계 **5** IS-IS에 사용되는 인접성 유형을 구성합니다.

isis circuit-type [level-1 | level-1-2 | level-2-only]

예제:

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- (선택 사항) **level-1** — 레벨 1 인접성에 대해서만 ASA를 구성합니다.
- (선택 사항) **level-1-2** — 레벨 1 및 레벨 2 인접성에 대해 ASA를 구성합니다.
- (선택 사항) **level-2** — 레벨 2 인접성에 대해서만 ASA를 구성합니다.

일반적으로 이 명령은 구성할 필요가 없습니다. 올바른 방법은 ASA에서 레벨을 구성하는 것입니다. 절차는 IS-IS 라우팅 전체 활성화, 960 페이지를 참조하십시오. 영역(레벨 1-2 라우터) 사이에 있는 ASA의 일부 인터페이스만 레벨 2로 구성해야 합니다. 이 경우 사용되지 않는 레벨 1 hello 패킷을 전송하여 대역폭이 절약됩니다.

단계 **6** 브로드캐스트 인터페이스에서 정기적인 CSNP 패킷이 전송되는 간격을 구성합니다.

isis csnp-interval *seconds* **[level-1 | level-1-2 | level-2]**

예제:

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds* — 멀티 액세스 네트워크에서의 CSNP 전송 간 시간 간격입니다. 이 간격은 지정된 ASA에만 적용됩니다. 범위는 0~65,535입니다. 기본값은 10초입니다.
- (선택 사항) **level-1** — 레벨 1에 대한 CSNP 전송 간 시간 간격을 개별적으로 구성합니다.
- (선택 사항) **level-2** — 레벨 2에 대한 CSNP 전송 간 시간 간격을 개별적으로 구성합니다.

이 명령의 기본값을 변경해야 할 경우는 거의 없습니다.

이 명령은 지정된 인터페이스에 대한 DR에만 적용됩니다. DR만 데이터베이스 동기화를 유지하기 위해 CSNP 패킷을 전송합니다. 레벨 1 및 레벨 2에 대한 CSNP 간격을 개별적으로 구성할 수 있습니다.

IS-IS IPv4 주소군 구성

라우터는 다른 라우팅 프로토콜, 고정 구성 또는 연결된 인터페이스에서 확인한 외부 접두사 또는 경로를 재배포할 수 있습니다. 재배포된 경로는 레벨 1 라우터 또는 레벨 2 라우터에서 허용됩니다.

인접성, SPF(Shortest Path First)를 설정할 수 있으며, 다른 라우팅 도메인에서 IPv4 주소용 ISIS(재배포)로의 경로를 재배포하는 조건을 정의할 수 있습니다.

시작하기 전에

IS-IS 경로 인증을 활성화하기 전에 IS-IS를 활성화하고 영역을 설정해야 합니다. 절차는 IS-IS 라우팅 전체 활성화, 960 페이지를 참조하십시오.

프로시저

단계 **1** IPv4 주소군을 구성하려면 라우터 구성 모드로 들어갑니다.

router isis

예제:

```
ciscoasa(config)# router isis
cisco(config-router)#
```

단계 **2** IS-IS 프로토콜 지원을 확인하려면 인접성 확인을 수행합니다.

adjacency-check

예제:

```
cisco(config-router)# adjacency-check
```

단계 **3** IS-IS 프로토콜에 의해 발견된 경로에 할당되는 관리 거리를 정의합니다.

distance *weight*

weight — IS-IS 경로에 할당되는 관리 거리입니다. 범위는 1~255입니다. 기본값은 115입니다.

예제:

```
ciscoasa(config-router)# distance 20
```

이 명령은 IS-IS 경로가 RIB에 삽입되어 다른 프로토콜을 통해 발견된 동일한 대상 주소에 대한 경로보다 이 경로가 우선시 될 가능성이 있는 경우 IS-IS 경로에 적용되는 거리를 구성합니다.

참고 일반적으로, 관리 거리 값이 높을수록 신뢰 등급이 더 낮습니다. 관리 거리가 255라면 이 라우팅 정보 소스는 전혀 신뢰할 수 없으므로 무시해야 합니다. 가중치 값은 주관적이며 가중치 값을 선택하는 정량적인 방법은 없습니다.

단계 **4** IS-IS에 대해 다중 경로 로드 공유를 구성합니다.

maximum-paths *number-of-paths*

예제:

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths — 라우팅 테이블에 설치할 경로의 수입니다. 범위는 1~8입니다. 기본값은 1입니다.

maximum-path 명령은 ECMP가 ASA에서 구성된 경우 IS-IS 다중 로드 공유를 구성하는 데 사용됩니다.

단계 **5** IS-IS 라우팅 도메인에 대한 기본 경로를 생성합니다.

default-information originate [**route-map** *map-name*]

예제**:**

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

(선택 사항) **route-map** *map-name* — 경로 맵이 충족되면 라우팅 프로세스에서 기본 경로를 생성합니다.

이 명령을 사용하여 구성된 ASA의 라우팅 테이블에 0.0.0.0에 대한 경로가 있는 경우, IS-IS는 LSP에서 0.0.0.0에 대한 알림을 생성합니다. 경로 맵이 없는 경우, 기본값은 레벨 2 LSP에서만 알려집니다. 레벨 1 라우팅의 경우 기본 경로를 찾는 또 다른 메커니즘이 있습니다. 이는 가장 가까운 레벨 1 또는 레벨 2 라우터를 찾는 것입니다. 가장 가까운 레벨 1 또는 레벨 2 라우터는 레벨 1 LSP에서 ATT를 확인하여 찾을 수 있습니다. **match ip address** *standard-access-list* 명령을 사용하여 ASA가 0/0을 알리기 전에 반드시 있어야 하는 하나 이상의 IP 경로를 지정할 수 있습니다.

단계 **6** 레벨 1 및 레벨 2에 대해 IS-IS 메트릭을 전역으로 설정합니다.

metric *default-value* **[level-1 | level-2]**

예제**:**

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- *default-value* — 링크에 할당되고 대상에 대한 링크를 통해 경로 비용을 계산하는 데 사용되는 메트릭 값입니다. 범위는 1~63입니다. 기본값은 10입니다.
- (선택 사항) **level-1** — 레벨 1 IPv4 또는 IPv6 메트릭을 설정합니다.
- (선택 사항) **level-2** — 레벨 2 IPv4 또는 IPv6 메트릭을 설정합니다.

단계 **7** 메트릭 스타일 및 메트릭 스타일을 적용할 레벨을 지정합니다.

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

예제**:**

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**— ASA가 좁은 범위의 메트릭을 사용하는 이전 TLV 스타일을 사용하게 합니다.
- **transition**— ASA가 전환 중에 이전 스타일의 TLV와 새로운 스타일의 TLV를 둘 다 허용하게 합니다.
- **wide**— ASA가 넓은 범위의 메트릭을 전달하도록 TLV의 새로운 스타일을 사용하게 합니다.
- (선택 사항) **level-1** — 레벨 1 IPv4 또는 IPv6 메트릭을 설정합니다.
- (선택 사항) **level-2** — 레벨 2 IPv4 또는 IPv6 메트릭을 설정합니다.

- (선택 사항) **level-1-2** — 레벨 1 및 레벨 2 IPv4 또는 IPv6 메트릭을 설정합니다.

단계 **8** 레벨 1-레벨 2 라우터가 연결된 비트를 설정해야 할 경우에 대한 제약 조건을 지정합니다.

set-attached-bit route-map *map-tag*

예제**:**

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag* — 구성된 경로 맵의 식별자입니다. 지정된 경로 맵이 일치하는 경우, 라우터는 계속해서 연결된 비트를 설정합니다. 이 명령은 기본적으로 비활성화되어 있습니다.

현재 IS-IS 구현에서는 ISO 10589에 지정된 대로, 레벨 1-레벨 2 라우터가 자신의 고유한 도메인에서 다른 영역을 확인하거나 다른 도메인을 확인하는 경우 레벨 1 LSP의 연결된 비트를 설정합니다. 그러나 일부 네트워크 토폴로지에서 서로 다른 영역에 있는 인접한 레벨 1-레벨 2 라우터는 레벨 2 백본에 대한 연결을 잃을 수 있습니다. 그런 다음 레벨 1 라우터는 영역 또는 도메인 외부를 향하는 트래픽을 이러한 연결이 없는 레벨 1-레벨 2 라우터로 전송할 수 있습니다.

이 명령을 사용하면 레벨 1-레벨 2 라우터에 대해 연결된 비트 설정을 더 잘 제어할 수 있습니다. 경로 맵은 하나 이상의 CLNS 경로를 지정할 수 있습니다. 하나 이상의 '일치 주소 경로 맵' 절이 레벨 2 CLNS 라우팅 테이블의 경로와 일치하거나, 연결된 비트 설정을 위한 기타 모든 요구 사항이 충족되는 경우, 레벨 1-레벨 2 라우터가 계속해서 레벨 1 LSP에서 연결된 비트를 설정합니다. 요구 사항이 충족되지 않거나 '일치 주소 경로 맵' 절이 레벨 2 CLNS 라우팅 테이블의 경로와 일치하는 경우, 연결된 비트가 설정되지 않습니다.

단계 **9** SPF 계산 시 ASA를 중간 홉으로 사용하지 않으려면 다른 라우터에 신호를 보내도록 ASA를 구성합니다.

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

예제**:**

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (선택 사항) **on-startup** — 시스템 시작 시 오버로드 비트를 설정합니다. 오버로드 비트는 지정된 후속 인수 또는 키워드에 따라서, 구성된 시간(초) 동안 또는 BGP가 통합될 때까지 설정된 상태로 유지됩니다.
- (선택 사항) *seconds* — 오버로드 비트가 시스템 시작 시 설정되고 설정된 상태로 유지되는 시간(초)입니다. 범위는 5~86400입니다.
- (선택 사항) **wait-for-bgp** — **on-startup** 키워드가 구성된 경우, 오버로드 비트가 시스템 시작 시 설정되고 BGP가 통합될 때까지 설정된 상태로 유지됩니다.
- (선택 사항) **suppress** — 후속 키워드 또는 키워드로 식별된 접두사 유형이 표시되지 않게 합니다.
- (선택 사항) **interlevel** — **suppress** 키워드가 구성된 경우, 다른 IS-IS 수준에서 확인한 IP 접두사를 알리지 않습니다.

- (선택 사항) **external** — **suppress** 키워드가 구성된 경우, 다른 프로토콜에서 확인한 IP 접두사를 알리지 않습니다.

이 명령은 ASA가 비 의사 노드 LSP의 오버로드 비트(hippity 비트라고도 함)를 강제로 설정하게 합니다. 일반적으로, 오버로드 비트의 설정은 ASA에서 문제가 발생하는 경우에만 허용됩니다. 예를 들어 ASA에서 메모리가 부족한 경우, 링크 상태 데이터베이스가 불완전하여 라우팅 테이블이 불완전하거나 부정확해질 수 있습니다. LSP의 오버로드 비트를 설정하면, 다른 라우터에서는 SPF 계산 시 신뢰할 수 없는 라우터를 문제가 복구될 때까지 무시할 수 있습니다. 그 결과, 이 라우터를 통하는 어떤 경로도 IS-IS 영역의 다른 경로에서 볼 수 없습니다. 그러나 IP 및 CLNS 접두사는 이 라우터에 직접 연결되어 있습니다.

단계 **10** PRC의 IS-IS 제한을 맞춤화합니다.

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

예제**:**

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* — 두 번 연속된 PRC 계산 사이의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 5일입니다.
- (선택 사항) *prc-initial-wait* — 토폴로지 변경 이후 첫 번째 PRC 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 2000밀리초입니다.

  이후 각 대기 간격은 대기 간격이 지정된 PRC 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.
- (선택 사항) *prc-second-wait* — 첫 번째와 두 번째 PRC 계산 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5000밀리초입니다(5초).

  PRC는 SPF 계산을 수행하지 않고 경로를 계산하는 소프트웨어 프로세스입니다. 이는 라우팅 시스템 자체의 토폴로지가 변경되지 않았지만, 특정 IS가 발표한 정보에 변화가 탐지되거나 RIB에 이러한 경로를 재설치해야 할 때 가능합니다.

단계 **11** SPF 계산의 IS-IS 제한을 맞춤화합니다.

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

예제**:**

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (선택 사항) **level-1** — 레벨 1 영역에만 간격을 적용합니다.
- (선택 사항) **level-2** — 레벨 2 영역에만 간격을 적용합니다.
- *spf-max-wait* — 연속된 두 SPF 계산 사이의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 10초입니다.
- (선택 사항) *spf-initial-wait* — 첫 SPF 계산 이전에 토폴로지를 변경한 후 초기 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5500밀리초입니다(5.5초).

이후 각 대기 간격은 대기 간격이 지정된 SPF 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.

- (선택 사항) *spf-second-wait* — 첫 번째와 두 번째 SPF 계산 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5500밀리초입니다(5.5초).

토폴로지가 변경된 경우에만 SPF 계산이 수행됩니다. 이 명령은 소프트웨어가 SPF 계산을 수행하는 빈도를 제어합니다.

참고 SPF 계산은 프로세서를 많이 사용합니다. 따라서 이 작업이 완료되는 빈도를 제한하는 데 유용하며 특히 영역이 크고 토폴로지가 자주 변경되는 경우 유용합니다. SPF 간격을 늘리면 ASA의 프로세서 로드가 줄어들지만 잠재적으로 통합 속도가 느려집니다.

단계 **12** SFP 계산 중에 외부 메트릭을 준수하도록 IS-IS를 구성합니다.

use external-metrics

단계 **13** BGP, 연결된 IS-IS, OSPF 또는 고정 경로 재배포를 구성합니다.

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

예제**:**

```
ciscoasa(config-router)# redistribute static level-1 metric-type internal metric 6
```

metric *number* — 메트릭 값입니다. 범위는 1~4294967295입니다.

연결된 비트 구성

다음 예에서는 라우터가 L2 CLNS 라우팅 테이블의 49.00aa와 일치하는 경우 연결된 비트가 설정된 상태를 유지합니다.

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

IS-IS IPv6 주소군 구성

인접성, SPF를 설정할 수 있으며, 다른 라우팅 도메인에서 IPv6 주소용 ISIS(재배포)로의 경로를 재배포하는 조건을 정의할 수 있습니다.

시작하기 전에

IS-IS 경로 인증을 활성화하기 전에 IS-IS를 활성화하고 영역을 설정해야 합니다. 절차는 IS-IS 라우팅 전체 활성화, 960 페이지를 참조하십시오.

프로시저

단계 **1** 라우터 구성 모드로 들어갑니다.

router isis

예제:

```
cisco(config-router)#
```

단계 **2** 메트릭 스타일을 넓은 범위로 지정합니다.

metric-style wide [transition] [level-1 | level-2 | level-1-2]

예제:

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- (선택 사항) **transition** — 라우터가 이전 스타일의 TLV와 새로운 스타일의 TLV를 둘 다 허용하게 합니다.
- (선택 사항) **level-1** — 레벨 1 IPv4 또는 IPv6 메트릭을 설정합니다.
- (선택 사항) **level-2** — 레벨 2 IPv4 또는 IPv6 메트릭을 설정합니다.
- (선택 사항) **level-1-2** — 레벨 1 및 레벨 2 IPv4 또는 IPv6 메트릭을 설정합니다.

모든 IS-IS 인터페이스에 대한 기본 메트릭을 변경해야 하는 경우 **metric** 명령을 사용하는 것이 좋습니다. 이렇게 하면 새 값을 구성하지 않은 채 설정된 메트릭을 의도치 않게 인터페이스에서 제거하거나, 인터페이스가 기본 메트릭 10으로 되돌아가도록 허용하는 등의 사용자 오류를 방지하게 되므로 네트워크에서 높은 선호도를 가진 인터페이스가 됩니다.

단계 **3** 주소군 구성 모드로 들어가 표준 IPv4 또는 IPv6 주소 접두사를 사용하는 IS-IS 라우팅 세션을 구성합니다.

address-family ipv6 [unicast]

예제:

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

단계 **4** IS-IS 프로토콜 지원을 확인하려면 인접성 확인을 수행합니다.

adjacency-check

예제:

```
cisco(config-router-af)# adjacency-check
```

단계 **5** IS-IS에 대해 다중 경로 로드 공유를 구성합니다.

maximum-paths *number-of-paths*

예제:

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths — 라우팅 테이블에 설치할 경로의 수입니다. 범위는 1~8입니다. 기본값은 1입니다.

maximum-path 명령은 ECMP가 ASA에서 구성된 경우 IS-IS 다중 로드 공유를 구성하는 데 사용됩니다.

단계 **6** IS-IS 프로토콜에 의해 발견된 경로에 할당되는 관리 거리를 정의합니다.

distance *weight*

weight — IS-IS 경로에 할당되는 관리 거리입니다. 범위는 1~255입니다. 기본값은 115입니다.

예제:

```
ciscoasa(config-router-af)# distance 20
```

이 명령은 IS-IS 경로가 RIB에 삽입되어 다른 프로토콜을 통해 발견된 동일한 대상 주소에 대한 경로보다 이 경로가 우선시 될 가능성이 있는 경우 IS-IS 경로에 적용되는 거리를 구성합니다.

참고 일반적으로, 관리 거리 값이 높을수록 신뢰 등급이 더 낮습니다. 관리 거리가 255라면 이 라우팅 정보 소스는 전혀 신뢰할 수 없으므로 무시해야 합니다. 가중치 값은 주관적이며 가중치 값을 선택하기 위한 정량적인 방법은 없습니다.

단계 **7** IS-IS 라우팅 도메인에 기본 경로를 생성합니다.

default-information originate [**route-map** *map-name*]

예제:

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

(선택 사항) **route-map** *map-name* — 경로 맵이 충족되면 라우팅 프로세스에서 기본 경로를 생성합니다.

이 명령을 사용하여 구성된 ASA에 라우팅 테이블의 0.0.0.0에 대한 경로가 있는 경우, IS-IS는 LSP에서 0.0.0.0에 대한 알림을 생성합니다. 경로 맵이 없는 경우, 기본값은 레벨 2 LSP에서만 알려집니다. 레벨 1 라우팅의 경우, 기본 경로를 찾기 위한 다른 메커니즘이 있는데 이는 가장 가까운 레벨 1 또는 레벨 2 라우터를 찾기 위한 메커니즘입니다. 가장 가까운 레벨 1 또는 레벨 2 라우터는 레벨 1 LSP에서 ATT를 확인하여 찾을 수 있습니다. **match ip address** *standard-access-list* 명령을 사용하여 ASA가 0/0을 알리기 전에 존재해야 하는 하나 이상의 IP 경로를 지정할 수 있습니다.

단계 **8** 다른 라우터에 SPF 계산 시 중간 홉으로 연결된 비트를 사용하지 않도록 신호를 보내도록 ASA를 구성합니다.

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external]]]**

예제**:**

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (선택 사항) **on-startup** — 시스템 시작 시 오버로드 비트를 설정합니다. 오버로드 비트는 구성된 시간(초) 동안 또는 BGP가 통합될 때까지 지정된 후속 인수 또는 키워드에 따라 오버로드 비트는 이후 지정된 인수 또는 키워드에 따라 구성된 시간(초) 동안 또는 BGP가 통합될 때까지 설정된 상태로 유지됩니다.
- (선택 사항) *seconds* — 오버로드 비트가 시스템 시작 시 설정되고 이 상태로 유지되는 시간(초)입니다. 범위는 5~86400입니다.
- (선택 사항) **wait-for-bgp** — **on-startup** 키워드가 구성된 경우, 오버로드 비트가 시스템 시작 시 설정되고 BGP가 통합될 때까지 설정된 상태로 유지됩니다.
- (선택 사항) **suppress** — 후속 키워드 또는 표시할 키워드로 접두사 유형을 식별합니다.
- (선택 사항) **interlevel** — **suppress** 키워드가 구성된 경우, 다른 IS-IS 레벨에서 확인한 IP 접두사가 알려지는 것을 방지합니다.
- (선택 사항) **external** — **suppress** 키워드가 구성된 경우, 다른 프로토콜에서 확인한 IP 접두사가 알려지는 것을 방지합니다.

이 명령은 비 의사 노드 LSP에서 오버로드 비트(hippity 비트라고도 함)를 설정하도록 ASA를 강제로 실행 합니다. 일반적으로, 오버로드 비트의 설정은 ASA에서 문제가 발생하는 경우에만 허용됩니다. 예를 들어 ASA에서 메모리가 부족한 경우, 링크 상태 데이터베이스가 완료되지 않아서 일 수 있으므로 이로 인해 불완전하거나 부정확한 라우팅 테이블이 생성될 수 있습니다. 해당 LSP에서 오버로드 비트를 설정하여 기타 라우터에서는 해당 라우터가 문제에서 복구될 때까지 SPF 계산 시 신뢰할 수 없는 라우터를 무시할 수 있습니다. 그 결과, 이 라우터를 통하는 어떤 경로도 IS-IS 영역의 다른 경로에서 볼 수 없습니다. 그러나, IP 및 CLNS 접두사는 이 라우터에 직접 연결되어 있습니다.

단계 **9** PRC의 IS-IS 제한을 맞춤화합니다.

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

예제**:**

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait* — 두 번 연속된 PRC 계산 사이의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 5일입니다.
- (선택 사항) *prc-initial-wait* — 토폴로지 변경 이후 첫 번째 PRC 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 2000밀리초입니다.

이후 각 대기 간격은 대기 간격이 지정된 PRC 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.

- (선택 사항) *prc-second-wait* — 첫 번째와 두 번째 PRC 계산 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5000밀리초입니다(5초).

  PRC는 SPF 계산을 수행하지 않고 경로를 계산하는 소프트웨어 프로세스입니다. 이는 라우팅 시스템 자체의 토폴로지가 변경되지 않았지만, 특정 IS가 발표한 정보에 변화가 탐지되거나 RIB에 이러한 경로를 재설치해야 할 때 가능합니다.

단계 **10** SPF 계산의 IS-IS 제한을 맞춤화합니다.

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

예제**:**

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- (선택 사항) **level-1** — 레벨 1 영역에만 간격을 적용합니다.
- (선택 사항) **level-2** — 레벨 2 영역에만 간격을 적용합니다.
- *spf-max-wait* — 두 번 연속된 SPF 계산 사이의 최대 간격을 나타냅니다. 범위는 1~120초입니다. 기본값은 10초입니다.
- (선택 사항) *spf-initial-wait* — 토폴로지를 첫 번째 SPF 계산 이전에 변경한 후 첫 번째 대기 시간을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5500밀리초입니다(5.5초).

  이후 각 대기 간격은 대기 간격이 지정된 SPF 최대 대기 간격에 도달할 때까지 이전 대기 간격보다 두 배 더 깁니다.

- (선택 사항) *spf-second-wait* — 첫 번째와 두 번째 SPF 계산 사이의 간격을 나타냅니다. 범위는 1~120,000밀리초입니다. 기본값은 5500밀리초입니다(5.5초).

토폴로지가 변경된 경우에만 SPF 계산이 수행됩니다. 이 명령은 소프트웨어가 SPF 계산을 수행하는 빈도를 제어합니다.

참고 SPF 계산은 프로세서를 많이 사용합니다. 따라서 이 작업이 완료되는 빈도를 제한하는 데 유용하며 특히 영역이 크고 토폴로지가 자주 변경되는 경우 유용합니다. SPF 간격을 늘리면 ASA의 프로세서 로드가 줄어들지만 잠재적으로 통합 속도가 느려집니다.

단계 **11** BGP, 연결된 IS-IS, OSPF 또는 고정 경로 재배포를 구성합니다.

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

예제**:**

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number* — 메트릭 값입니다. 범위는 1~4294967295입니다.

단계 **12** IS-IS 경로를 구체적으로 레벨 1에서 레벨 2로 또는 레벨 2에서 레벨 1로 재배포합니다.

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag***]]**

예제**:**

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2**— IS-IS 경로가 어떤 레벨에서 어떤 레벨로 재배포되는지를 나타냅니다.
- **into**— 이 키워드는 재배포 중인 경로가 시작되는 레벨과 끝나는 레벨을 구분해 줍니다.
- (선택 사항) **distribute-list** *list-number* — IS-IS 재배포를 제어하는 배포 목록의 수입니다. 배포 목록 또는 경로 맵 중 하나만 지정할 수 있으며 둘 다 지정할 수는 없습니다.
- (선택 사항) **route-map** *map-tag* — IS-IS 재배포를 제어하는 경로 맵의 이름입니다. 배포 목록 또는 경로 맵 중 하나만 지정할 수 있으며 둘 다 지정할 수는 없습니다.

참고 **redistribute isis** 명령을 실행하려면 **metric-style wide** 명령을 지정해야 합니다. 이 절차의 1 단계를 참고하십시오.

모든 영역이 스텁 영역인 IS-IS의 경우, 이는 백본(레벨 2)에서 영역(레벨 1)으로 라우팅 정보가 유출되지 않았음을 의미합니다. 레벨 1 전용 라우터는 해당 영역에서 가장 가까운 레벨 1-레벨 2 라우터의 기본 라우팅을 사용합니다. 이 명령을 사용하여 레벨 1 영역에 레벨 2 IP 경로를 재배포할 수 있습니다. 이러한 재배포를 통해 레벨 1-전용 라우터는 IP 접두사가 해당 영역에서 벗어나는 데 가장 적합한 경로를 선택할 수 있습니다. 이는 IP 전용 기능이며 CLNS 라우팅이 계속해서 스텁 라우팅을 수행합니다.

참고 더 우수한 제어 및 안정성을 확보하기 위해 배포 목록 또는 경로 맵을 구성하여 어떤 레벨 2 IP 경로를 레벨 1로 재배포할지 제어할 수 있습니다. 이렇게 하면 대규모 IS-IS-IP 네트워크가 확장성이 향상된 영역을 사용할 수 있습니다.

단계 **13** IS-IS IPv6 경로에 대해 집계 접두사를 생성합니다.

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

예제**:**

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address* — X.X.X.X.::X/0-128 형식의 IPv6 접두사입니다.
- (선택 사항) **level-1** — 레벨 1로 재배포되는 경로만 구성된 주소 및 마스크 값으로 요약되어 있습니다.
- (선택 사항) **level-1-2** — 요약 경로는 경로를 레벨 1과 레벨 2 IS-IS로 재배포할 때와 레벨 2 IS-IS가 레벨 1 경로를 해당 영역에서 도달할 수 있는 것으로 알릴 때 적용됩니다.

- (선택 사항) **level-2** — 레벨 1 라우팅을 통해 확인된 경로가 구성된 주소 및 마스크 값이 있는 레벨 2 백본으로 요약되어 있습니다. 레벨 2 IS-IS에 재배포된 경로도 요약되어 있습니다.

IS-IS 모니터링

다음 명령을 사용하여 IS-IS 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조를 참고하십시오.

IS-IS 데이터베이스 모니터링

다음 명령을 사용하여 IS-IS 데이터베이스를 모니터링합니다.

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** — 레벨 1, 레벨 2에 대한 IS-IS 링크 상태 데이터베이스와 각 LSP의 자세한 내용을 표시합니다.
- **show isis database verbose** — 시퀀스 번호, 체크섬 및 LSP 보류 시간 등 IS-IS 데이터베이스에 대한 자세한 정보를 표시합니다.

IS-IS 매핑 테이블 항목 모니터링

다음 명령을 사용하여 IS-IS 호스트 이름을 모니터링합니다.

show isis hostname— IS-IS 라우터에 대한 router-name-to-system-ID 매핑 테이블 항목을 표시합니다.

IS-IS IPv4 모니터링

다음 명령을 사용하여 IS-IS IPv4를 모니터링합니다.

- **show isis ip rib**— IS-IS 라우팅 프로세스에 대한 IPv4 주소군 특정 RIB를 표시합니다.
- **show isis ip spf-log**— IS-IS 라우팅 프로세스에 대한 IPv4 주소군 특정 SPF 로그를 표시합니다.
- **show isis ip topology**— IS-IS 라우팅 프로세스에 대한 IPv4 주소군 특정 토폴로지를 표시합니다.
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*] — IS-IS가 확인 및 설치한 IPv6 경로를 표시합니다.
- **show isis ip unicast**— IPv4 주소군 특정 RIB, SPF 로그 및 IS에 대한 경로를 표시합니다.

IS-IS IPv6 모니터링

다음 명령을 사용하여 IS-IS IPV6를 모니터링합니다.

- **show isis ipv6 rib**— IS-IS 라우팅 프로세스에 대한 IPv6 주소군 특정 RIB를 표시합니다.
- **show isis ipv6 spf-log**— IS-IS 라우팅 프로세스에 대한 IPv6 주소군 특정 SPF 로그를 표시합니다.

- **show isis ipv6 topology**— IS-IS 라우팅 프로세스에 대한 IPv6 주소군 특정 토폴로지를 표시합니다.
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*] — IS-IS의 확인 및 설치된 IPv6 경로를 표시합니다.
- **show isis ipv6 unicast**— IPv6 주소군 특정 RIB, SPF 로그 및 IS에 대한 경로를 표시합니다.

IS-IS 로그 모니터링

다음 명령을 사용하여 IS-IS 로그를 모니터링합니다.

- **show isis lsp-log**— 새 LSP를 트리거한 인터페이스의 레벨 1 및 레벨 2 IS-IS LSP 로그를 표시합니다.
- **show isis spf-log**— ASA가 SPF 계산을 실행한 빈도와 이유를 표시합니다.

IS-IS 프로토콜 모니터링

다음 명령을 사용하여 IS-IS 프로토콜을 모니터링합니다.

show clns protocol — ASA의 각 IS-IS 라우팅 프로세스에 대한 프로토콜 정보를 표시합니다.

IS-IS 네이버 및 경로 모니터링

다음 명령을 사용하여 IS-IS 네이버를 모니터링합니다.

- **show isis topology** — 모든 영역에서 연결된 모든 라우터의 목록을 표시합니다. 이 명령은 모든 영역에 있는 모든 라우터 간의 연결성과 프레즌스를 확인합니다.
- **show isis neighbors [detail]** — IS-IS 인접성 정보를 표시합니다.
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**] — ES(최종 시스템), IS(중간 시스템) 및 M-ISIS(다중 토폴로지 IS-IS) 네이버를 표시합니다. 이 명령은 IPv6용 다중 토폴로지 IS-IS를 통해 확인된 인접성을 표시합니다.
- **show clns is-neighbors** *[interface-name]* **[detail]** — IS-IS 디바이스 인접성에 대한 IS-IS 정보를 표시합니다.

IS-IS RIB 모니터링

다음 명령을 사용하여 IS-IS RIB를 모니터링합니다.

- **show isis rib** [*ip-address* | *ip-address-mask*] — RIB에 저장되어 있으며 주요 네트워크에 있는 모든 경로 또는 특정 경로에 대한 경로를 표시합니다.
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*] — 로컬 재배포 캐시에 있는 접두사를 표시합니다.
- **show route isis** 라우팅 테이블의 현재 상태를 표시합니다.

IS-IS 트래픽 모니터링

다음 명령을 사용하여 IS-IS 트래픽을 모니터링합니다.

show clns traffic [since {bootup | show}] — ASA가 확인한 CLNS 트래픽 통계를 표시합니다.

IS-IS 디버깅

다음 명령을 사용하여 IS-IS를 디버깅합니다.

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets]— IS-IS 라우팅 프로토콜의 다양한 측면을 디버깅합니다.

IS-IS에 대한 기록

표 *34: IS-IS*에 대한 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
IS-IS 라우팅	9.6(1)	이제 ASA에서 IS-IS(Intermediate System to Intermediate System) 라우팅 프로토콜을 지원합니다. 데이터 라우팅, 인증 수행, IS-IS 라우팅 프로토콜을 사용한 라우팅 정보 재배포 및 모니터링에 대한 지원이 추가되었습니다. 다음 명령을 도입했습니다. **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

IS-IS의 예

이 섹션에서는 토폴로지가 있는 구성 예를 통해 IS-IS의 다양한 측면을 살펴봅니다.

IS-IS 라우팅 구성

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

IS-IS IPv6 라우팅 구성

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

동일한 영역에서의 동적 라우팅

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
```

```
 router isis
  net 49.1234.2035.2035.2035.00
  is-type level-1
  metric-style wide

 oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis

 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

둘 이상의 영역에서의 동적 라우팅

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120
```

```
iRouter
interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

중복 영역에서의 동적 라우팅

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
```

```
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

경로 재배포

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
```

```
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

요약 주소

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
```

```
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

수동 인터페이스

```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default
```

```
IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis

 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

 oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis

 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

인증

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
```

```
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```

31 장

EIGRP

이 장에서는 EIGRP(Enhanced Interior Gateway Routing Protocol)를 이용하여 데이터를 라우팅하고, 인증을 수행하고, 라우팅 정보 재배포하도록 Cisco ASA를 구성하는 방법을 설명합니다.

EIGRP 소개

EIGRP는 Cisco에서 개발한 IGRP의 향상된 버전입니다. IGRP 및 RIP와 달리 EIGRP는 주기적인 경로 업데이트를 전송하지 않습니다. EIGRP 업데이트는 네트워크 토폴로지가 변경될 때만 전송됩니다. EIGRP를 다른 라우팅 프로토콜과 차별화하는 핵심 기능으로는 빠른 컨버전스, variable-length 서브넷 마스크 지원, 부분 업데이트 지원, 다중 네트워크 계층 프로토콜 지원이 있습니다.

EIGRP를 실행하는 라우터는 모든 네이버 라우팅 테이블을 저장하여 다른 경로에 빠르게 적응할 수 있습니다. 적절한 경로가 존재하지 않는 경우 EIGRP는 네이버를 쿼리하여 대체 경로를 찾습니다. 이 쿼리는 대체 경로를 발견할 때까지 전파됩니다. variable-length 서브넷 마스크 지원을 통해 네트워크 숫자 경계에서 경로를 자동으로 요약할 수 있습니다. 또한 EIGRP는 모든 인터페이스의 모든 비트 경계에서 요약되도록 구성할 수 있습니다. EIGRP는 주기적인 업데이트를 만들지 않습니다. 대신 경로의 메트릭이 변경될 때만 부분적인 업데이트를 전송합니다. 부분 업데이트 전파가 자동으로 바운딩되므로 정보가 필요한 라우터만 업데이트됩니다. 이 두 기능 덕분에 EIGRP는 IGRP보다 훨씬 적은 대역폭을 사용합니다.

네이버 검색은 ASA가 직접 연결된 네트워크의 다른 라우터를 동적으로 학습하기 위해 사용하는 프로세스입니다. EIGRP 라우터는 멀티캐스트 hello 패킷을 전송하여 네트워크에서 존재를 알립니다. ASA가 새로운 네이버에서 hello 패킷을 수신하면 초기화 비트 집합과 함께 토폴로지 테이블을 네이버로 보냅니다. 초기화 비트 집합과 함께 토폴로지 업데이트를 수신한 네이버는 토폴로지 테이블을 ASA로 다시 전달합니다.

hello 패킷은 멀티캐스트 메시지로 전달됩니다. hello 메시지에는 응답할 필요가 없습니다. 고정으로 정의된 네이버의 경우 예외입니다. **neighbor** 명령을 사용하거나 ASDM에서 hello 간격을 구성하여 네이버를 구성할 경우 네이버로 전송되는 hello 메시지는 유니캐스트 메시지로 전송됩니다. 라우팅 업데이트 및 확인은 유니캐스트 메시지로 전송됩니다.

이 네이버 관계가 설정되면 네트워크 토폴로지의 변화가 없는 한 라우팅 업데이트가 교환되지 않습니다. 네이버 관계는 hello 패킷을 통해 유지됩니다. 네이버에서 수신된 각 hello 패킷은 보류 시간을 포함합니다. 이 시간은 ASA가 해당 네이버로부터 hello 패킷을 수신할 것으로 예상하는 시간입니다. ASA가 해당 네이버가 알린 보류 시간 이내에 네이버로부터 hello 패킷을 수신하지 않으면 ASA는 해당 네이버를 사용할 수 없는 것으로 간주합니다.

EIGRP 프로토콜은 경로 연산에 중요한 네이버 검색/복구, RTP(Reliable Transport Protocol) 및 DUAL을 포함하여 4가지 주요 알고리즘 기술을 사용합니다. DUAL은 least-cost 경로뿐 아니라 토폴로지 테이블의 대상에 대한 모든 경로를 저장합니다. least-cost 경로가 라우팅 테이블로 삽입됩니다. 다른 경로는 토폴로지 테이블에 남아 있습니다. 기본 경로가 실패할 경우 가능한 successor에서 다른 경로가 선택됩니다. successor는 대상에 대한 least-cost 경로를 가진 패킷 전달에 사용되는 네이버 라우터입니다. 가능성 계산은 경로가 라우팅 루프의 일부가 아님을 보장합니다.

토폴로지 테이블에서 가능한 successor를 찾을 수 없는 경우 경로 재계산이 이루어져야 합니다. 경로 재계산 중 DUAL이 EIGRP 네이버에 경로를 쿼리하면 EIGRP 네이버가 다시 자신의 네이버에 쿼리합니다. 경로에 대한 가능한 successor가 없는 라우터는 도달할 수 없음 메시지를 반환합니다.

경로 재계산 중 DUAL은 경로를 활성으로 표시합니다. 기본적으로 ASA는 네이버로부터 응답을 수신하기 위해 3분을 대기합니다. ASA가 네이버로부터 응답을 수신하지 않는 경우 경로가 stuck-in-active로 표시됩니다. 가능한 successor로서 응답이 없는 네이버를 가리키는 토폴로지 테이블의 모든 경로는 제거됩니다.

참고 EIGRP 네이버 관계는 GRE 터널 없이 IPsec 터널을 통해 지원되지 않습니다.

EIGRP를 위한 지침

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

클러스터 지침

EIGRP는 개별 인터페이스 모드에서 클러스터 피어와 네이버 관계를 형성하지 않습니다.

IPv6 지침

IPv6를 지원하지 않습니다.

상황 지침

- EIGRP 인스턴스는 기본적으로 공유 인터페이스 전반에서 멀티캐스트 트래픽의 상황 간 교환이 지원되지 않기 때문에 공유 인터페이스 전반에서 서로 인접성을 형성할 수 없습니다. 그러나 특정 공유 인터페이스에서 EIGRP 인접 관계를 가져오기 위해 EIGRP 프로세스의 EIGRP 프로세서 구성에서 고정 네이버 구성을 사용할 수 있습니다.
- 별도 인터페이스에서의 상황 간 EIGRP가 지원됩니다.

추가 지침

- 최대 하나의 EIGRP 프로세스가 지원됩니다.
- 구성 변경 사항이 적용될 때마다 EIGRP 인접성 플랩이 발생하며, 이로 인해 특히 배포 목록, 오프셋 목록 및 요약 변경 사항에서 네이버로부터 전송 또는 수신된 라우팅 정보가 수정됩니다. 라우터를 동기화한 후 EIGRP는 네이버 간에 인접성을 재설정합니다. 인접성이 해제되고 재설정되면 네이버 간에 확인한 모든 경로가 지워지고, 새 배포 목록을 통해 네이버 간의 전체 동기화가 새로 수행됩니다.

EIGRP 구성

이 섹션에서는 시스템에서 EIGRP 프로세스를 활성화하는 방법을 설명합니다. EIGRP를 활성화한 후에는 다음 섹션을 참조하여 시스템에서 EIGRP 프로세스를 사용자 정의하는 방법을 알아보십시오.

EIGRP 활성화

ASA에서 하나의 EIGRP 라우팅 프로세스만 활성화할 수 있습니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제**:**

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

network ip-addr [mask]

예제**:**

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

이 명령으로 하나 이상의 **network** 구문을 구성할 수 있습니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 인터페이스 구성, 1010 페이지을(를) 참조하십시오.

EIGRP stub 라우팅 활성화

ASA를 EIGRP 스텁 라우터로 활성화하고 구성할 수 있습니다. 스텁 라우팅은 ASA에 대한 메모리 및 처리 요구 사항을 줄여 줍니다. 스텁 라우터인 ASA는 모든 비 로컬 트래픽을 배포 라우터로 전달하기 때문에 전체 EIGRP 라우팅 테이블을 유지할 필요가 없습니다. 일반적으로 배포 라우터는 기본 경로 외에 아무것도 stub 라우터로 보낼 필요가 없습니다.

지정된 경로만 stub 라우터에서 배포 라우터로 전파됩니다. 스텁 라우터인 ASA는 요약, 연결된 경로, 재배포된 고정 경로, 외부 경로, 내부 경로에 대한 모든 쿼리에 "액세스 불가" 메시지로 응답합니다. ASA가 스텁으로 구성되면 모든 네이버 라우터에 특별한 피어 정보 패킷을 보내 자신이 스텁 라우터임을 알립니다. stub 상태를 알려주는 패킷 정보를 수신하는 모든 네이버는 경로에 대해 일체 stub 라우터에 쿼리하지 않고 stub 피어가 있는 라우터는 피어에 쿼리하지 않습니다. stub 라우터는 올바른 업데이트를 모든 피어에 전송하기 위해 배포 라우터에 의지합니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제**:**

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

network ip-addr [mask]

예제**:**

```
ciscoasa(config)# router eigrp 2
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

이 명령으로 하나 이상의 **network** 구문을 구성할 수 있습니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 패시브 인터페이스 구성, 1012 페이지 섹션을 참조하십시오.

단계 **3** stub 라우팅 프로세스를 구성합니다.

eigrp stub {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]}

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static]
[summary]}
```

stub 라우팅 프로세스가 어떤 네트워크를 배포 라우터로 알릴지 지정해야 합니다. 고정 네트워크 및 연결 네트워크는 stub 라우팅 프로세스로 자동 재분배되지 않습니다.

참고 stub 라우팅 프로세스는 전체 토폴로지 테이블을 유지하지 않습니다. stub 라우팅은 최소한 라우팅 결정을 내리는 배포 라우터로의 기본 경로를 필요로 합니다.

EIGRP 사용자 지정

이 섹션에서는 EIGRP 라우팅을 사용자 정의하는 방법을 설명합니다.

EIGRP 라우팅 프로세스를 위한 네트워크 정의

네트워크 테이블을 통해 EIGRP 라우팅 프로세스가 사용하는 네트워크를 지정할 수 있습니다. 인터페이스가 EIGRP 라우팅에 참여하려면 네트워크 엔트리에 의해 정의된 주소 범위에 해당해야 합니다. 직접 연결 및 고정 네트워크를 알리려면 네트워크 엔트리 범위에 해당해야 합니다.

네트워크 테이블은 EIGRP 라우팅 프로세스에 대해 지정된 네트워크를 표시합니다. 테이블의 각 행은 네트워크 주소와 지정된 EIGRP 라우팅 프로세스에 대해 구성된 연결된 마스크를 표시합니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

network ip-addr [mask]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

이 명령으로 하나 이상의 **network** 구문을 구성할 수 있습니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 패시브 인터페이스 구성, 1012 페이지을(를) 참조하십시오.

EIGRP 인터페이스 구성

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있는 경우, 이 인터페이스가 연결된 네트워크를 포함하는**network** 명령을 구성하고, **passive-interface** 명령을 사용하여 이 인터페이스가 EIGRP 업데이트를 보내거나 받지 않게 할 수 있습니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

network ip-addr [mask]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

이 명령으로 하나 이상의 network 구문을 구성할 수 있습니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 라우팅 프로세스를 위한 네트워크 정의, 1009 페이지을(를) 참조하십시오.

단계 **3** 후보 기본 경로 정보의 송수신을 제어합니다.

no default-information {**in** | **out** | **WORD**}

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

no default-information in 명령을 입력하면 후보 기본 경로 비트가 수신 경로에서 차단됩니다.

no default-information out 명령을 입력하면 알려진 경로에서 기본 경로 비트 설정이 비활성화됩니다.

자세한 내용은 EIGRP에서 기본 정보 구성, 1021 페이지를 참조하십시오.

단계 **4** EIGRP 패킷의 MD5 인증을 활성화합니다.

authentication mode eigrp as-num **md5**

예제:

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 인수는 ASA에 구성된 EIGRP 라우팅 프로세스의 자율 시스템의 수입니다. EIGRP가 활성화되지 않았거나 잘못된 수를 입력한 경우 ASA가 다음 오류 메시지를 반환합니다.

```
% Asystem(100) specified does not exist
```

자세한 내용은 인터페이스에서 EIGRP 인증 활성화, 1014 페이지를 참조하십시오.

단계 **5** 지연 값을 설정합니다.

delay 값

예제:

```
ciscoasa(config-if)# delay 200
```

value 인수는 10마이크로초 단위로 입력합니다. 2000마이크로초 지연을 설정하려면 *value*를 200으로 입력합니다.

인터페이스에 할당된 지연 값을 보려면 **show interface** 명령을 사용합니다.

자세한 내용은 인터페이스 지연 값 변경, 1014 페이지를 참고하십시오.

단계 **6** hello 간격을 변경합니다.

hello-interval eigrp as-num seconds

예제:

```
ciscoasa(config)# hello-interval eigrp 2 60
```

자세한 내용은 EIGRP hello 간격 및 보류 시간 사용자 지정, 1020 페이지를 참조하십시오.

단계 **7** 보류 시간을 변경합니다.

hold-time eigrp as-num seconds

예제:

```
ciscoasa(config)# hold-time eigrp 2 60
```

자세한 내용은 EIGRP hello 간격 및 보류 시간 사용자 지정, 1020 페이지를 참조하십시오.

패시브 인터페이스 구성

하나 이상의 인터페이스를 패시브 인터페이스로 구성할 수 있습니다. EIGRP에서 패시브 인터페이스는 라우팅 업데이트를 보내거나 받지 않습니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 이 명령으로 하나 이상의 **network** 구문을 구성할 수 있습니다.

network ip-addr [mask]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 라우팅 프로세스를 위한 네트워크 정의, 1009 페이지을(를) 참조하십시오.

단계 **3** 인터페이스가 EIGRP 라우팅 메시지를 보내거나 받지 못하게 합니다.

passive-interface {**default** | if-name}

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# passive-interface {default}
```

default 키워드를 사용하면 모든 인터페이스의 EIGRP 라우팅 업데이트가 비활성화됩니다. **nameif** 명령에 정의된 대로 인터페이스 이름을 지정하면 지정된 인터페이스에서 EIGRP 라우팅 업데이트가 비활성화됩니다. EIGRP 라우터 구성에서 여러 **passive-interface** 명령을 사용할 수 있습니다.

인터페이스에서 요약 종합 주소 구성

인터페이스별로 요약 주소를 구성할 수 있습니다. 네트워크 숫자 경계에서 발생하지 않는 요약 주소를 생성하려는 경우 또는 자동 경로 요약을 비활성화하고 ASA에서 요약 주소를 사용하려는 경우 요약 주소를 수동으로 정의해야 합니다. 라우팅 테이블에 다른 특정 경로가 있는 경우 EIGRP는 모든 추가 경로의 최소값과 동등한 메트릭을 통해 인터페이스로 요약 주소를 알립니다.

프로시저

단계 **1** EIGRP에서 사용하는 지연 값을 변경하는 인터페이스에 대한 인터페이스 컨피그레이션 모드에 진입합니다.

interface phy_if

예제:

```
ciscoasa(config)# interface inside
```

단계 **2** 요약 주소를 생성합니다.

summary-address eigrp *as-num address mask* [*distance*]

예제:

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

기본적으로 EIGRP 요약 주소를 정의하면 관리 거리는 5입니다. 이 값은 선택적인 *distance* 인수를 **summary-address** 명령에 지정하여 변경할 수 있습니다.

인터페이스 지연 값 변경

인터페이스 지연 값은 EIGRP 거리 계산에 사용됩니다. 인터페이스별로 이 값을 수정할 수 있습니다.

프로시저

단계 **1** EIGRP에서 사용하는 지연 값을 변경하는 인터페이스에 대한 인터페이스 컨피그레이션 모드에 진입합니다.

interface phy_if

예제:

```
ciscoasa(config)# interface inside
```

단계 **2** 지연 값을 설정합니다.

delay 값

예제:

```
ciscoasa(config-if)# delay 200
```

value 인수는 10마이크로초 단위로 입력합니다. 2000마이크로초 지연을 설정하려면 *value*를 200으로 입력합니다.

참고 인터페이스에 할당된 지연 값을 보려면 **show interface** 명령을 사용합니다.

인터페이스에서 **EIGRP** 인증 활성화

EIGRP 경로 인증은 EIGRP 라우팅 프로토콜로부터 라우팅 업데이트의 MD5 인증을 제공합니다. 각 EIGRP 패킷의 MD5 키 입력 다이제스트를 사용하여 승인되지 않은 소스로부터 허가되지 않거나 잘못된 라우팅 메시지가 수신되는 것을 방지할 수 있습니다.

EIGRP 경로 인증은 인터페이스별로 구성됩니다. EIGRP 메시지 인증에 구성된 인터페이스의 모든 EIGRP 네이버는 인접성을 위해 동일한 인증 모드와 키로 구성되어야 설정 가능합니다.

참고 EIGRP 경로 인증을 활성화하기 전에 EIGRP를 활성화해야 합니다.

프로시저

단계 1 EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp *as-num*

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 2 EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

network *ip-addr* [*mask*]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

- 이 명령으로 하나 이상의 network 구문을 구성할 수 있습니다.
- 정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.
- EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 구성, 1007 페이지을(를) 참조하십시오.

단계 3 EIGRP 메시지 인증을 구성하는 인터페이스에 대한 인터페이스 컨피그레이션 모드를 시작합니다.

interface *phy_if*

예제:

```
ciscoasa(config)# interface inside
```

단계 4 EIGRP 패킷의 MD5 인증을 활성화합니다.

authentication mode eigrp *as-num* md5

예제:

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 인수는 ASA에 구성된 EIGRP 라우팅 프로세스의 자율 시스템 개수입니다. EIGRP가 활성화되지 않았거나 잘못된 번호를 입력한 경우 ASA가 다음 오류 메시지를 반환합니다.

```
% Asystem(100) specified does not exist
```

단계 **5** MD5 알고리즘에서 사용하는 키를 구성합니다.

authentication key eigrp *as-num key* key-id *key-id*

예제**:**

```
ciscoasa(config)# authentication key eigrp 2 cisco key-id 200
```

- as-num 인수는 ASA에 구성된 EIGRP 라우팅 프로세스의 자율 시스템 개수입니다. EIGRP가 활성화되지 않았거나 잘못된 번호를 입력한 경우 ASA가 다음 오류 메시지를 반환합니다.

  ```
  % Asystem(100) specified does not exist%
  ```

- key 인수에는 영문자, 숫자 및 특수 문자를 포함하여 최대 16자가 포함될 수 있습니다. key 인수에는 공백을 사용할 수 없습니다.
- key-id 인수는 0~255 범위의 숫자입니다.

EIGRP 네이버 정의

EIGRP hello 패킷은 멀티캐스트 패킷으로 전송됩니다. EIGRP 네이버가 터널과 같이 브로드캐스트가 아닌 네트워크에 위치한 경우 해당 네이버를 수동으로 정의해야 합니다. EIGRP 네이버를 수동으로 정의할 경우 hello 패킷은 유니캐스트 메시지로 해당 네이버에 전송됩니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제**:**

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** 고정 네이버를 정의합니다.

neighbor *ip-addr* **interface** *if_name*

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

ip-addr 인수는 네이버의 IP 주소입니다.

if-name 인수는 **nameif** 명령으로 지정된 인터페이스 이름이며 이 이름을 통해 네이버를 이용할 수 있습니다. EIGRP 라우팅 프로세스에 여러 네이버를 정의할 수 있습니다.

EIGRP로 경로 재분배

RIP 및 OSPF에서 검색된 경로를 EIGRP 라우팅 프로세스로 재분배할 수 있습니다. 고정 경로 및 연결된 경로도 EIGRP 라우팅 프로세스로 재분배할 수 있습니다. 연결된 경로가 EIGRP 구성에서 **network** 구문 범위에 해당하는 경우 연결된 경로를 재배포할 필요가 없습니다.

참고 RIP만 해당: 이 절차를 시작하기 전에 지정된 라우팅 프로토콜에서 어떤 경로가 RIP 라우팅 프로세스로 재분배될지 정의하기 위해 경로 지도를 생성해야 합니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** (선택 사항) EIGRP 라우팅 프로세스로 재분배된 경로에 적용할 기본 메트릭을 지정합니다.

default-metric bandwidth delay reliability loading mtu

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

EIGRP 라우터 구성에서 기본 메트릭을 지정하지 않은 경우 각 **redistribute** 명령에서 메트릭 값을 지정해야 합니다. EIGRP 메트릭을 **redistribute** 명령에 지정하고 EIGRP 라우터 구성에 **default-metric** 명령이 있는 경우 **redistribute** 명령의 메트릭이 사용됩니다.

단계 **3** 연결된 경로를 EIGRP 라우팅 프로세스로 재분배합니다.

redistribute connected [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

예제**:**

```
ciscoasa(config-router): redistribute connected [metric bandwidth delay reliability loading
 mtu] [route-map map_name]
```

EIGRP 라우터 구성에 **default-metric** 명령이 없는 경우 **redistribute** 명령에서 EIGRP 메트릭 값을 지정해야 합니다.

단계 **4** 고정 경로를 EIGRP 라우팅 프로세스로 재분배합니다.

redistribute static [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

예제**:**

```
ciscoasa(config-router): redistribute static [metric bandwidth delay
reliability loading mtu] [route-map map_name]
```

단계 **5** OSPF 라우팅 프로세스의 경로를 EIGRP 라우팅 프로세스로 재분배합니다.

redistribute ospf pid [**match** {**internal | external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

예제**:**

```
ciscoasa(config-router): redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

단계 **6** RIP 라우팅 프로세스의 경로를 EIGRP 라우팅 프로세스로 재분배합니다.

redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

예제**:**

```
ciscoasa(config-router): redistribute rip [metric bandwidth delay
reliability load mtu] [route-map map_name]
```

EIGRP 네트워크 필터링

참고 이 프로세스를 시작하기 전에 알리고자 하는 경로를 정의하는 표준 ACL을 생성해야 합니다. 업데이트 송신 또는 수신에서 필터링하려는 경로를 정의하는 표준 ACL을 생성하는 것입니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

ciscoasa(config-router)# **network** ip-addr [mask]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

이 명령으로 하나 이상의 network 구문을 구성할 수 있습니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 인터페이스 구성, 1010 페이지을(를) 참조하십시오.

단계 **3** EIGRP 라우팅 업데이트에서 전송되는 네트워크를 필터링합니다.

distribute-list acl **out** [**connected** | **ospf** | **rip** | **static** | **interface** if_name]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl out [connected]
```

해당 특정 인터페이스에서 전송되는 업데이트에만 필터를 적용하도록 인터페이스를 지정할 수 있습니다.

EIGRP 라우터 구성에서 여러 **distribute-list** 명령을 입력할 수 있습니다.

단계 **4** EIGRP 라우팅 업데이트에서 수신되는 네트워크를 필터링합니다.

distribute-list acl **in** [**interface** if_name]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

```
ciscoasa(config-router): distribute-list acl in [interface interface1]
```

해당 특정 인터페이스에서 수신되는 업데이트에만 필터를 적용하도록 인터페이스를 지정할 수 있습니다.

EIGRP hello 간격 및 보류 시간 사용자 지정

ASA는 정기적으로 hello 패킷을 전송하여 네이버를 발견하고 네이버가 도달 불가 또는 작동 불능 상태가 되는 시간을 파악합니다. 기본적으로 hello 패킷은 5초 간격으로 전송됩니다.

hello 패킷은 ASA 보류 시간을 알립니다. 보류 시간은 EIGRP 네이버에 ASA를 도달 가능으로 간주할 시간을 알려 줍니다. 네이버가 알려진 보류 시간 내에 hello 패킷을 수신하지 못하면 ASA는 도달 불가로 간주됩니다. 기본적으로 알려지는 보류 시간은 15초(hello 간격의 3배)입니다.

hello 간격과 알려진 보류 시간은 인터페이스별로 구성됩니다. 보류 시간은 hello 간격의 최소 3배로 설정하는 것이 좋습니다.

프로시저

단계 **1** hello 간격 또는 알려진 보류 시간을 구성하는 인터페이스에 대한 인터페이스 컨피그레이션 모드를 시작합니다.

interface phy_if

예제**:**

```
ciscoasa(config)# interface inside
```

단계 **2** hello 간격을 변경합니다.

hello-interval eigrp as-num seconds

예제**:**

```
ciscoasa(config)# hello-interval eigrp 2 60
```

단계 **3** 보류 시간을 변경합니다.

hold-time eigrp as-num seconds

예제**:**

```
ciscoasa(config)# hold-time eigrp 2 60
```

자동 경로 요약 비활성화

기본적으로 자동 경로 요약이 활성화되어 있습니다. EIGRP 라우팅 프로세스는 네트워크 번호 경계에서 요약됩니다. 불연속 네트워크를 가진 경우 라우팅 문제가 발생할 수 있습니다.

예를 들어 네트워크 192.168.1.0, 192.168.2.0 및 192.168.3.0이 연결된 라우터가 있고 이러한 네트워크가 모두 EIGRP에 참여하는 경우 EIGRP 라우팅 프로세스가 해당 경로에 대해 요약 주소 192.168.0.0을 생성합니다. 네트워크 192.168.10.0 및 192.168.11.0으로 라우터가 추가되고 해당 네트워크가 EIGRP에 참여할 경우에도 192.168.0.0으로 요약됩니다. 잘못된 위치에 트래픽이 라우팅될 가능성을 방지하려면 충돌하는 요약 주소를 만드는 라우터에서 자동 경로 요약을 비활성화해야 합니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제**:**

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** 자동 경로 요약을 비활성화합니다.

no auto-summary

예제**:**

```
ciscoasa(config-router)# no auto-summary
```

자동 요약 주소의 기본 관리 영역은 5입니다.

EIGRP에서 기본 정보 구성

EIGRP 업데이트에서 기본 경로 정보의 송수신을 제어할 수 있습니다. 기본적으로 기본 경로가 전송되고 승인됩니다. 기본 정보 수신을 금지하도록 ASA를 구성하면 수신된 경로에서 후보 기본 경로 비트가 차단됩니다. 기본 정보 전송을 금지하도록 ASA를 구성하면 알려진 경로에서 기본 경로 비트 설정이 비활성화됩니다.

프로시저

단계 **1** EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.

router eigrp as-num

예제:

```
ciscoasa(config)# router eigrp 2
```

as-num 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

단계 **2** EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다.

network ip-addr [mask]

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

이 명령으로 하나 이상의 network 구문을 구성할 수 있습니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 고정 네트워크는 ASA에 의해 알려집니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 인터페이스 구성, 1010 페이지을(를) 참조하십시오.

단계 **3** 후보 기본 경로 정보의 송수신을 제어합니다.

no default-information {**in** | **out** | **WORD**}

예제:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

참고 **no default-information in** 명령을 입력하면 후보 기본 경로 비트가 수신 경로에서 차단됩니다. **no default-information out** 명령을 입력하면 알려진 경로에서 기본 경로 비트 설정이 비활성화됩니다.

EIGRP Split Horizon 비활성화

Split horizon은 EIGRP 업데이트 및 쿼리 패킷의 전송을 제어합니다. 인터페이스에서 split horizon이 활성화된 경우 업데이트 및 쿼리 패킷이 이 인터페이스가 next hop인 대상으로 전송되지 않습니다. 이 방식으로 업데이트 및 쿼리 패킷을 제어하면 라우팅 루프 가능성이 줄어듭니다.

기본적으로 split horizon은 모든 인터페이스에서 활성화되어 있습니다.

Split horizon은 경로 정보를 해당 정보가 발생하는 인터페이스 밖의 라우터가 알릴 수 없도록 합니다. 이러한 행동은 일반적으로 특히 링크가 깨졌을 때 여러 라우팅 디바이스 간 통신을 최적화합니다. 하

지만 비브로드캐스트 네트워크의 경우 이 행동이 필요하지 않은 상황이 있을 수 있습니다. 이 경우 EIGRP를 구성한 네트워크를 포함하여 split horizon을 비활성화할 수 있습니다.

인터페이스에서 split horizon을 비활성화하는 경우 해당 인터페이스의 모든 라우터와 액세스 서버에서 비활성화해야 합니다.

EIGRP split horizon을 비활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** EIGRP에서 사용하는 지연 값을 변경하는 인터페이스에 대한 인터페이스 컨피그레이션 모드에 진입합니다.

interface phy_if

예제**:**

```
ciscoasa(config)# interface phy_if
```

단계 **2** split horizon을 비활성화합니다.

no split-horizon eigrp *as-number*

예제**:**

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

EIGRP 프로세스 재시작

EIGRP 프로세스를 다시 시작하거나 재분배 또는 카운터를 지웁니다.

프로시저

EIGRP 프로세스를 다시 시작하거나 재분배 또는 카운터를 지웁니다.

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

예제**:**

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

EIGRP 모니터링

다음 명령을 사용하여 EIGRP 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조를 참고하십시오. 또한 네이버 변경 메시지 및 네이버 경고 메시지의 로깅을 비활성화할 수 있습니다.

다양한 EIGRP 라우팅 통계를 모니터링하거나 비활성화하려면 다음 명령 중 하나를 입력하십시오.

- **router-id**

  이 EIGRP 프로세스에 대한 router-id를 표시합니다.

- **show eigrp** [*as-number*] **events** [{*start end*} | **type**]

  EIGRP 이벤트 로그를 표시합니다.

- **show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

  EIGRP 라우팅에 참여하는 인터페이스를 표시합니다.

- **show eigrp** [as-number] **neighbors** [**detail** | **static**] [*if-name*]

  EIGRP 네이버 테이블을 표시합니다.

- **show eigrp** [*as-number*] **topology** [*ip-addr* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  EIGRP 토폴로지 테이블을 표시합니다.

- **show eigrp** [*as-number*] **traffic**

  EIGRP 트래픽 통계를 표시합니다.

- **show mfib cluster**

  전달 항목 및 인터페이스와 관련된 MFIB 정보를 표시합니다.

- **show route cluster**

  클러스터링을 위한 추가 경로 동기화 정보를 표시합니다.

- **no eigrp log-neighbor-changes**

  네이버 변경 메시지 로깅을 비활성화합니다. 이 명령을 EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드에 입력합니다.

- **no eigrp log-neighbor-warnings**

  네이버 경고 메시지 로깅을 비활성화합니다.

EIGRP의 예

다음 예는 다양한 프로세스 옵션으로 EIGRP를 활성화하고 구성하는 방법을 보여줍니다.

프로시저

단계 **1** EIGRP를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

단계 **2** 인터페이스의 EIGRP 라우팅 메시지 송수신을 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# passive-interface {default}
```

단계 **3** EIGRP 네이버를 정의하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

단계 **4** EIGRP 라우팅에 참여하는 인터페이스 및 네트워크를 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

단계 **5** EIGRP 거리 계산에 사용되는 인터페이스 지연 값을 변경하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

EIGRP 기록

표 ***35: EIGRP*** 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
EIGRP 지원	7.0(1)	데이터 라우팅, 인증 수행, EIGRP(Enhanced Interior Gateway Routing Protocol)을 사용한 라우팅 정보 재분배 및 모니터링에 대한 지원이 추가되었습니다. 다음 명령을 도입했습니다. **route eigrp**.
다중 상황 모드의 동적 라우팅	9.0(1)	EIGRP 라우팅이 다중 상황 모드에서 지원됩니다.

기능 이름	플랫폼 릴리스	기능 정보
클러스터링	9.0(1)	EIGRP의 경우 일괄 동기화, 경로 동기화 및 계층 2 로드 밸런싱은 클러스터링 환경에서 지원됩니다. 다음 명령을 도입하거나 수정했습니다. **show route cluster**, **debug route cluster, show mfib cluster, debug mfib cluster**.
EIGRP Auto-Summary	9.2(1)	EIGRP의 경우, 이제 Auto-Summary 필드가 기본적으로 비활성화됩니다.

32 장

멀티캐스트 라우팅

이 장에서는 멀티캐스트 라우팅 프로토콜을 사용하도록 Cisco ASA를 구성하는 방법을 설명합니다.

멀티캐스트 라우팅 정보

멀티캐스트 라우팅은 단일 정보 스트림을 수천 개의 기업 수신자와 가정으로 동시에 제공함으로써 트래픽을 줄이는 대역폭 절약 기술입니다. 멀티캐스트 라우팅을 활용하는 분야로는 화상 회의, 기업 통신, 원거리 학습, 소프트웨어 배포, 주식 시세 및 뉴스가 있습니다.

멀티캐스트 라우팅 프로토콜은 소스나 수신자에 추가적인 부담을 주지 않고 경쟁 기술 중에서도 가장 적은 네트워크 대역폭을 사용하여 소스 트래픽을 여러 수신자에게 보냅니다. 멀티캐스트 패킷은 PIM(Protocol Independent Multicast) 및 기타 지원 멀티캐스트 프로토콜로 활성화되는 ASA에 의해 네트워크에서 복제되어 여러 수신자에게 데이터를 가장 효율적으로 제공할 수 있습니다.

ASA는 stub 멀티캐스트 라우팅과 PIM 멀티캐스트 라우팅을 모두 지원합니다. 하지만 두 라우팅을 하나의 ASA에 동시에 구성할 수는 없습니다.

참고 멀티캐스트 라우팅에 대해 UDP 및 비 UDP 전송이 모두 지원됩니다. 그러나 비 UDP 전송에는 FastPath 최적화가 없습니다.

stub 멀티캐스트 라우팅

Stub 멀티캐스트 라우팅은 동적 호스트 등록을 제공하고 멀티캐스트 라우팅을 촉진합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 ASA는 IGMP 프록시 에이전트 역할을 합니다. 멀티캐스트 라우팅에 완전히 참여하는 대신 ASA는 IGMP 메시지를 업스트림 멀티캐스트 라우터로 전송하고 이 라우터가 멀티캐스트 데이터 전송을 설정합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 ASA는 PIM 스파스 또는 양방향 모드에 대해 구성될 수 없습니다. IGMP 스텁 멀티캐스트 라우팅에 참여 중인 인터페이스에서 PIM을 활성화해야 합니다.

ASA는 PIM-SM과 양방향 PIM을 모두 지원합니다. PIM-SM은 기본 유니캐스트 라우팅 정보 기반 또는 별도의 멀티캐스트 지원 라우팅 정보 기반을 사용하는 멀티캐스트 라우팅 프로토콜입니다. 또한 멀티캐스트 그룹당 단일 RP(랑데부 포인트)를 루트로 삼는 단방향 공유 트리를 구축하고 선택적으로 멀티캐스트 소스별로 최단 경로 트리를 생성합니다.

PIM 멀티캐스트 라우팅

양방향 PIM은 멀티캐스트 소스와 수신자를 연결하는 양방향 공유 트리를 구축하는 PIM-SM의 변형입니다. 양방향 트리는 멀티캐스트 토폴로지의 각 링크에서 작동하는 DF(Designated Forwarder) 선택 프로세스를 사용하여 구축됩니다. 멀티캐스트 데이터는 DF의 도움을 받아 소스에서 RP(랑데부 포인트)로 전달되고 따라서 소스별 상태 없이도 공유 트리에서 수신자를 따르게 됩니다. DF 선택은 RP 검색 중에 이루어지고 RP에 대한 기본 경로를 제공합니다.

참고 ASA가 PIM RP인 경우 ASA의 변환되지 않은 외부 주소를 RP 주소로 사용합니다.

PIM 소스별 멀티캐스트 지원

ASA는 PIM SSM(Source Specific Multicast) 기능 및 관련된 구성을 지원하지 않습니다. 그러나 ASA는 마지막 홉 라우터로 배치되는 경우를 제외하고 SSM 관련 패킷이 통과하도록 허용합니다.

SSM은 IPTV 같은 일대다 애플리케이션에 대한 데이터 전달 메커니즘으로 분류됩니다. SSM 모델은 (S,G) 쌍으로 표시된 "채널"의 개념을 사용하며, 여기서 S는 소스 주소이고 G는 SSM 대상 주소입니다. 채널 가입은 IGMPv3 같은 그룹 관리 프로토콜을 사용하여 수행됩니다. SSM이 특정 멀티캐스트 소스를 확인한 경우, 수신 클라이언트가 공유 RP(랑데부 포인트)에서 수신하는 대신 소스에서 직접 멀티캐스트 스트림을 수신하게 합니다. 액세스 제어 메커니즘은 현재 SM(Sparse Mode) 또는 SDM(Sparse-Dense Mode) 구현으로 사용할 수 없는 보안 향상을 제공하는 SSM 내에서 도입되었습니다.

PIM-SSM은 RP 또는 공유 트리를 사용하지 않는 점에서 PIM-SM과 다릅니다. 대신, 멀티캐스트 그룹의 소스 주소에 대한 정보가 IGMPv3(로컬 리시버십 프로토콜)를 통해 리시버에서 제공되고 소스별 트리를 직접 구축하는 데 사용됩니다.

PIM BSR(부트스트랩 라우터)

PIM BSR(부트스트랩 라우터)은 그룹에 대해 RP 정보를 릴레이하기 위해, 그리고 RP 기능을 위해 후보 라우터를 사용하는 동적 RP(랑데부 포인트) 선택 모델입니다. RP 기능은 RP 검색을 포함하며 RP에 대한 기본 경로를 제공합니다. RP 기능은 이를 위해 디바이스 집합을 BSR 선택 프로세스에 참여하는 C-BSR(후보 BSR)로 구성하여 후보 중에서 BSR을 선택하는 방식을 이용합니다. BSR을 선택한 후 C-RP(후보 랑데부 포인트)로 구성된 디바이스는 선택한 BSR로 그룹 매핑을 전송하기 시작합니다. 그런 다음 BSR은 홉에 기반하여 PIM 라우터 간에 이동하는 BSR 메시지를 통해 멀티캐스트 트리 아래의 모든 기타 디바이스로 그룹-RP 매핑 정보를 배포합니다.

이 기능은 RP를 동적으로 확인하는 수단을 제공하는데, 이는 RP가 정기적으로 아래위로 이동할 수 있는 대규모의 복잡한 네트워크에서 매우 필수적입니다.

PIM BSR(부트스트랩 라우터) 용어

다음 조건은 PIM BSR 구성에서 자주 참조됩니다.

- BSR(부트스트랩 라우터) — BSR은 PIM을 사용하여 RP(랑데부 포인트) 정보를 다른 라우터에 홉별로 알립니다. 선택 프로세스 이후에 여러 후보 BSR 중에서 단일 BSR이 선택됩니다. 이 부트스트랩 라우터의 주목적은 모든 C-RP(Candidate-RP) 알림을 RP-set(RP 집합)이라고 하는 데이터베이스에 수집하고 이를 BSR 메시지로 60초마다 네트워크에 있는 다른 모든 라우터에 정기적으로 전송하는 것입니다.
- BSR(부트스트랩 라우터) 메시지 — BSR 메시지는 All-PIM-Routers(모든 PIM 라우터) 그룹에 대한 멀티캐스트입니다(TTL이 1). 이러한 메시지를 수신하는 모든 PIM 네이버는 메시지를 수신한 인터페이스를 제외한 모든 인터페이스 외부로 해당 메시지를 TTL을 1로 재전송합니다. BSR 메시지는 RP 집합 및 현재 활성 BSR의 IP 주소를 포함합니다. 이를 통해 C-RP는 자신의 C-RP 메시지를 유니캐스트할 위치를 확인합니다.
- C-BSR(후보 부트스트랩 라우터) — 후보-BSR로 구성된 디바이스는 BSR 선택 메커니즘에 참여합니다. 우선순위가 가장 높은 C-BSR은 BSR로 선택됩니다. C-BSR의 우선순위가 가장 높은 IP 주소는 타이 브레이커로 사용됩니다. BSR 선택 프로세스는 선점형입니다. 예를 들어, 우선순위가 더 높은 새로운 C-BSR이 가동되면 새로운 선택 프로세스가 트리거됩니다.
- C-RP(후보 랑데부 포인트) — RP는 소스 및 멀티캐스트 데이터의 수신자가 만나는 공간의 역할을 합니다. C-RP로 구성된 디바이스는 정기적으로 유니캐스트를 통해 선택한 BSR로 직접 멀티캐스트 그룹 매핑 정보를 알립니다. 이러한 메시지에는 그룹 범위, C-RP 주소 및 보류 시간이 포함되어 있습니다. 현재 BSR의 IP 주소는 네트워크의 모든 라우터에서 수신하는 정기적인 BSR 메시지에서 확인됩니다. 이러한 방법으로 BSR은 현재 작동 중이며 연결 가능한 RP를 확인합니다.

  참고 C-RP가 BSR 트래픽에 대한 필수 요구 사항인 경우에도 ASA는 C-RP로 작동하지 않습니다. 라우터만 C-RP로 작동할 수 있습니다. 따라서 BSR 테스트 기능을 위해 라우터를 토폴로지에 추가해야 합니다.

- BSR 선택 메커니즘 — 각 C-BSR은 BSR Priority(BSR 우선순위) 필드를 포함하는 부트스트랩 메시지(BSM)를 시작합니다. 도메인 내의 라우터는 도메인 전체에서 BSM을 플러딩합니다. 자신보

다 우선순위가 높은 C-BSR를 알고 있는 C-BSR은 일정 기간 동안 추가 BSM 전송을 표시하지 않습니다. 나머지 단일 C-BSR은 선택된 BSR이 되며 해당 BSM은 도메인에 있는 모든 기타 라우터에 자신이 선택된 BSR임을 알립니다.

멀티캐스트 그룹 개념

멀티캐스트는 그룹 개념을 기반으로 합니다. 임의의 수신자 그룹이 특정 데이터 스트림 수신에 관심을 표현합니다. 이 그룹은 물리적 또는 지리적 경계가 없이 호스트가 인터넷의 어디에나 위치할 수 있습니다. 특정 그룹으로 향하는 데이터 수신에 관심이 있는 호스트는 IGMP를 사용하여 그룹에 참여해야 합니다. 호스트가 그룹의 일원이어야만 데이터 스트림을 받을 수 있습니다.

멀티캐스트 주소

멀티캐스트 주소는 그룹에 참여하고 이 그룹으로 전송된 트래픽을 수신하고자 하는 임의의 IP 호스트 그룹입니다.

클러스터링

멀티캐스트 라우팅은 클러스터링을 지원합니다. Spanned EtherChannel 클러스터링에서 기본 유닛은 빠른 경로 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 전송합니다. 빠른 경로 전달이 설정된 후에는 종속 유닛이 멀티캐스트 데이터 패킷을 전송할 수 있습니다. 모든 데이터 흐름은 완전한 흐름입니다. Stub 전달 흐름도 지원됩니다. Spanned EtherChannel 클러스터링에서는 하나의 유닛만 멀티캐스트 패킷을 받기 때문에 기본 유닛으로의 리디렉션이 일반적입니다. 개별 인터페이스 클러스터링에서는 유닛이 독립적으로 작동하지 않습니다. 모든 데이터 및 라우팅 패킷은 기본 유닛에 의해 처리 및 전달됩니다. 종속 유닛은 전송된 모든 패킷을 삭제합니다.

클러스터링에 대한 자세한 내용은 ASA 클러스터, 351 페이지를 참고하십시오.

멀티캐스트 라우팅 지침

상황 모드

단일 컨텍스트 모드에서 지원됩니다.

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

IPv6

IPv6를 지원하지 않습니다.

클러스터링

IGMP 및 PIM에 대한 클러스터링에서 이 기능은 기본 유닛에서만 지원됩니다.

추가 지침

멀티캐스트 호스트(예: 224.1.2.3)에 대한 트래픽을 허용하려면 인바운드 인터페이스에서 액세스 제어 규칙을 구성해야 합니다. 그러나 규칙에 대한 대상 인터페이스를 지정하거나 초기 연결을 검증하는 동안 이를 멀티캐스트 연결에 적용할 수는 없습니다.

멀티캐스트 라우팅 활성화

ASA에서 멀티캐스트 라우팅을 활성화하면 기본적으로 모든 데이터 인터페이스에서 IGMP 및 PIM을 활성화하지만 5506-X~5555-X 모델의 관리 인터페이스에서는 활성화하지 않습니다. IGMP는 그룹에서 어떤 멤버가 직접 연결된 서브넷에 존재하는지 학습하는 데 사용됩니다. 호스트는 IGMP 보고 메시지를 전송함으로써 멀티캐스트 그룹에 참여합니다. PIM은 멀티캐스트 데이터 그램을 전달하기 위한 전달 테이블 유지에 사용됩니다.

5506-X~5555-X 모델의 관리 인터페이스에서 멀티캐스트 라우팅를 활성화하려면 관리 인터페이스에서 멀티캐스트 경계를 명시적으로 설정해야 합니다.

참고 멀티캐스트 라우팅에 대해서는 UDP 전송 레이어만 지원됩니다.

다음 표에는 ASA의 RAM양을 기준으로 특정 멀티캐스트 테이블에 대한 최대 항목 수가 나와 있습니다. 이 제한에 도달하면 새로운 엔트리가 삭제됩니다.

표 ***36:*** 멀티캐스트 테이블에 대한 항목 제한***(***통합된 고정 및 동적 항목에 대한 제한***)***

표	**16MB**	**128 MB**	**128+MB**
MFIB	1000	3000	30000
IGMP 그룹	1000	3000	30000
PIM 경로	3000	7000	72000

프로시저

멀티캐스트 라우팅을 활성화합니다.

multicast-routing

예제**:**

```
ciscoasa(config)# multicast-routing
```

멀티캐스트 라우팅 테이블의 항목 수는 ASA의 RAM양에 따라 제한됩니다.

멀티캐스트 라우팅 사용자 정의

이 섹션에서는 멀티캐스트 라우팅을 사용자 정의하는 방법을 설명합니다.

stub 멀티캐스트 라우팅 구성 및 IGMP 메시지 전달

참고 스텁 멀티캐스트 라우팅은 PIM 스파스 모드 및 양방향 모드에서 동시에 지원되지 않습니다.

스텁 영역에 대한 게이트웨이 역할을 하는 ASA는 PIM 스파스 모드 또는 양방향 모드에 참여할 필요가 없습니다. 대신 IGMP 프록시 에이전트 역할을 하고 IGMP 메시지를 하나의 인터페이스에 연결된 호스트에서 다른 인터페이스에 연결된 업스트림 멀티캐스트 라우터로 전달하도록 구성할 수 있습니다. IGMP 프록시 에이전트로 ASA를 구성하려면 호스트 조인을 전달하고 스텁 영역 인터페이스에서 업스트림 인터페이스로 메시지를 남깁니다. 또한 스텁 모드 멀티캐스트 라우팅에 참여 중인 인터페이스에서 PIM을 활성화해야 합니다.

프로시저

stub 멀티캐스트 라우팅 구성 및 IGMP 메시지를 전달합니다.

igmp forward interface if_name

예제**:**

```
ciscoasa(config-if)# igmp forward interface interface1
```

고정 멀티캐스트 경로 구성

고정 멀티캐스트 경로를 구성함으로써 유니캐스트 트래픽에서 멀티캐스트 트래픽을 분리할 수 있습니다. 예를 들어 소스와 목적지 사이의 경로가 멀티캐스트 라우팅을 지원하지 않을 경우 해결책은 두 멀티캐스트 디바이스 사이에 GRE 터널을 구성하여 멀티캐스트 패킷을 터널을 통해 전송하는 것입니다.

PIM을 사용하는 경우 ASA는 유니캐스트 패킷을 다시 소스로 보내는 인터페이스와 같은 인터페이스에서 패킷을 수신할 것으로 기대합니다. 멀티캐스트 라우팅을 지원하지 않는 경로를 바이패스할 때와 같이 일부 경우에서는 유니캐스트 패킷이 하나의 경로를 따르고 멀티캐스트 패킷이 다른 경로를 따르도록 할 수 있습니다.

고정 멀티캐스트 경로가 알려지거나 재배포되지 않습니다.

프로시저

단계 **1** 고정 멀티캐스트 경로를 구성합니다.

mroute src_ip src_mask {input_if_name | *rpf_neighbor*} [distance]

예제**:**

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
```

단계 **2** stub 영역에 대한 고정 멀티캐스트 경로를 구성합니다.

mroute src_ip src_mask input_if_name [**dense** output_if_name] [distance]

예제**:**

```
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

dense *output_if_name* 키워드와 인수 쌍은 스텁 멀티캐스트 라우팅에 대해서만 지원됩니다.

IGMP 기능 구성

IP 호스트가 IGMP를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터에 보고합니다. IGMP는 특정 LAN의 멀티캐스트 그룹에서 개별 호스트를 동적으로 등록하는 데 사용됩니다. 호스트는 IGMP 메시지를 로컬 멀티캐스트 라우터로 전송함으로써 그룹 멤버십을 식별합니다. IGMP에서 라우터가 IGMP 메시지를 듣고 주기적으로 쿼리를 보내 특정 서브넷에서 어떤 그룹이 활성 상태이고 어떤 그룹이 비활성 상태인지 파악합니다.

이 섹션에서는 인터페이스별로 선택적인 IGMP 설정을 구성하는 방법을 설명합니다.

인터페이스에서 IGMP 비활성화

특정 인터페이스에서 IGMP를 비활성화할 수 있습니다. 이 정보는 특정 인터페이스에 멀티캐스트 호스트가 없음을 알고 있고 ASA가 해당 인터페이스로 호스트 쿼리 메시지를 보내는 것을 막고 싶을 때 유용합니다.

프로시저

인터페이스에서 IGMP 비활성화:

no igmp

예제**:**

```
ciscoasa(config-if)# no igmp
```

인터페이스에서 IGMP를 다시 활성화하려면 **igmp** 명령을 사용합니다.

참고 인터페이스 구성에 **no igmp** 명령만 표시됩니다.

IGMP 그룹 멤버십 구성

ASA를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. ASA를 멀티캐스트 그룹에 조인하도록 구성하면 업스트림 라우터가 해당 그룹에 대한 멀티캐스트 라우팅 테이블 정보를 유지하고 해당 그룹에 대한 경로를 액티브 상태로 유지하게 됩니다.

참고 특정 그룹에 대한 멀티캐스트 패킷을 인터페이스로 전달하면서 ASA가 해당 패킷을 해당 그룹의 일부로 수락하지 않도록 하려면 고정 참여 IGMP 그룹 구성, 1034 페이지을 참고하십시오.

프로시저

ASA를 멀티캐스트 그룹의 멤버로 구성합니다.

igmp join-group group-address

예제:

```
ciscoasa(config-if)# igmp join-group mcast-group
```

group-address 인수는 그룹의 IP 주소입니다.

고정 참여 IGMP 그룹 구성

때로는 일부 구성으로 인해 또는 네트워크 세그먼트의 그룹에 멤버가 없기 때문에 그룹 멤버가 멤버십을 보고할 수 없는 경우도 있습니다. 그러나 해당 네트워크 세그먼트로 여전히 해당 그룹에 대한 멀티캐스트 트래픽을 보내려고 합니다. 고정 참여 IGMP 그룹을 구성하면 해당 그룹에 대한 멀티캐스트 트래픽을 해당 세그먼트로 보낼 수 있습니다.

igmp static-group 명령을 입력합니다. ASA는 멀티캐스트 패킷을 수락하지 않지만 대신 지정된 인터페이스로 전달합니다.

프로시저

ASA가 인터페이스에서 멀티캐스트 그룹에 고정으로 조인하도록 구성합니다.

igmp static-group

예제:

```
ciscoasa(config-if)# igmp static-group group-address
```

group-address 인수는 그룹의 IP 주소입니다.

멀티캐스트 그룹에 대한 액세스 제어

액세스 제어 목록을 사용하여 멀티캐스트 그룹에 대한 액세스를 제어할 수 있습니다.

프로시저

단계 **1** 멀티캐스트 트래픽에 대한 표준 ACL을 생성합니다.

access-list name **standard** [**permit | deny]** ip_addr mask

예제**:**

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

단일 ACL에 대해 하나 이상의 엔트리를 생성할 수 있습니다. 확장 또는 표준 ACL을 사용할 수 있습니다.

ip_addr mask 인수는 허용 또는 거부되는 멀티캐스트 그룹의 IP 주소입니다.

단계 **2** 확장 ACL을 생성합니다.

access-list name **extended** [**permit | deny]** protocol src_ip_addr src_mask dst_ip_addr dst_mask

예제**:**

```
ciscoasa(config)# access-list acl2 extended permit protocol
src_ip_addr src_mask dst_ip_addr dst_mask
```

dst_ip_addr 인수는 허용 또는 거부되는 멀티캐스트 그룹의 IP 주소입니다.

단계 **3** ACL을 인터페이스에 적용합니다.

igmp access-group acl

예제**:**

```
ciscoasa(config-if)# igmp access-group acl
```

acl 인수는 표준 또는 확장 IP ACL의 이름입니다.

인터페이스에서 IGMP 상태의 개수 제한

인터페이스별로 IGMP 멤버십 보고에서 비롯되는 IGMP 멤버십 상태의 수를 제한할 수 있습니다. 구성된 제한을 초과하는 멤버십 보고는 IGMP 캐시에 입력되지 않고 초과된 멤버십 보고에 대한 트래픽은 전달되지 않습니다.

프로시저

인터페이스에서 IGMP 상태의 개수 제한

igmp limit number

예제**:**

```
ciscoasa(config-if)# igmp limit 50
```

유효한 값의 범위는 0 ~ 500이고 기본값은 500입니다.

이 값을 0으로 설정하면 학습된 그룹이 추가되지 않지만 수동으로 정의한 그룹(**igmp join-group** 및 **igmp static-group** 명령 사용)은 여전히 허용됩니다. 이 명령의 **no** 양식은 기본값을 복원합니다.

멀티캐스트 그룹으로의 쿼리 메시지 수정

ASA는 쿼리 메시지를 보내 어떤 멀티캐스트 그룹이 인터페이스에 연결된 네트워크의 멤버인지 확인합니다. 멤버는 특정 그룹에 대한 멀티캐스트 패킷을 받고 싶다는 의미의 IGMP 보고 메시지로 응답합니다. 쿼리 메시지는 주소가 224.0.0.1이고 time-to-live 값이 1인 전체 시스템 멀티캐스트 그룹으로 전달됩니다.

이 메시지는 정기적으로 전송되어 ASA에 저장된 멤버십 정보를 새로 고침합니다. ASA가 아직 인터페이스에 연결된 멀티캐스트 그룹의 로컬 멤버가 없다고 확인하면 해당 그룹의 멀티캐스트 패킷을 연결된 네트워크로 더 이상 전달하지 않고 prune 메시지를 다시 패킷 소스로 전송합니다.

기본적으로 서브넷의 PIM 지정 라우터가 쿼리 메시지 전송을 담당합니다. 기본적으로 125초마다 한 번 전송됩니다.

쿼리 응답 시간을 변경할 경우 IGMP 쿼리에서 알려지는 최대 쿼리 응답 시간은 기본적으로 10초입니다. 이 시간 내에 ASA가 호스트 쿼리에 대한 응답을 받지 못하면 해당 그룹이 삭제됩니다.

참고 **igmp query-timeout** 및 **igmp query-interval** 명령에는 IGMP 버전 2가 필요합니다.

쿼리 간격, 쿼리 응답 시간 및 쿼리 시간 초과 값을 변경하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 쿼리 간격 시간을 초로 설정합니다.

igmp query-interval *seconds*

예제**:**

```
ciscoasa(config-if)# igmp query-interval 30
```

유효한 값 범위는 0~3600이고 기본값은 125입니다.

ASA가 인터페이스에서 지정된 시간 초과 값(기본값: 255초)의 시간 동안 쿼리 메시지를 수신하지 못하면 ASA가 지정된 라우터가 되고 쿼리 메시지를 전송하기 시작합니다.

단계 **2** 쿼리의 시간 초과 값을 변경합니다.

igmp query-timeout *seconds*

예제**:**

```
ciscoasa(config-if)# igmp query-timeout 30
```

유효한 값 범위는 60~300이고 기본값은 225입니다.

단계 **3** 최대 쿼리 응답 시간을 변경합니다.

igmp query-max-response-time *seconds*

유효한 값 범위는 1~25이고 기본값은 10입니다.

예제**:**

```
ciscoasa(config-if)# igmp query-max-response-time 20
```

IGMP 버전 변경

기본적으로 ASA는 **igmp query-timeout**및 **igmp query-interval** 명령 같은 몇 가지 추가 기능을 지원하는 IGMP 버전 2를 실행합니다.

서브넷의 모든 멀티캐스트 라우터는 같은 버전의 IGMP를 지원해야 합니다. ASA는 자동으로 버전 1 라우터를 탐지하여 버전 1로 전환하지 않습니다. 그러나 IGMP 버전 1과 2 호스트를 서브넷에서 혼용할 수는 있습니다. IGMP 버전 2를 실행 중인 ASA는 IGMP 버전 1 호스트가 있을 때에도 정상 작동합니다.

프로시저

인터페이스에서 실행하려는 IGMP 버전을 제어합니다.

igmp version {**1** | **2**}

예제:

```
ciscoasa(config-if)# igmp version 2
```

PIM 기능 구성

라우터는 PIM을 사용하여 멀티캐스트 다이어그램 전달에 사용할 전달 테이블을 유지합니다. ASA에서 멀티캐스트 라우팅을 활성화할 경우 PIM 및 IGMP가 모든 인터페이스에서 자동으로 활성화됩니다.

참고 PIM은 PAT에서 지원되지 않습니다. PIM 프로토콜은 포트를 사용하지 않고 PAT는 포트를 사용하는 프로토콜에서만 작동합니다.

이 섹션은 선택적인 PIM 설정을 구성하는 방법을 설명합니다.

인터페이스에서 PIM 활성화 및 비활성화

특정 인터페이스에서 PIM을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 **1** 특정 인터페이스에서 PIM을 활성화하거나 다시 활성화합니다.

PIM

예제:

```
ciscoasa(config-if)# pim
```

단계 **2** 특정 인터페이스에서 PIM을 비활성화합니다.

no pim

예제:

```
ciscoasa(config-if)# no pim
```

참고 인터페이스 구성에 **no pim** 명령만 표시됩니다.

고정 **Rendezvous Point** 주소 구성

일반 PIM sparse mode 또는 bidir 도메인을 가진 모든 라우터는 PIM RP 주소를 알아야 합니다. 이 주소는 **pim rp-address** 명령을 사용하여 고정으로 구성됩니다.

참고 ASA는 자동 RP 또는 PIM BSR을 지원하지 않습니다. **pim rp-address** 명령을 사용하여 RP 주소를 지정해야 합니다.

ASA가 두 개 이상의 그룹에 대해 RP 역할을 하도록 구성할 수 있습니다. ACL에 지정된 그룹 범위가 PIM RP 그룹 매핑을 결정합니다. ACL이 지정되지 않은 경우 해당 그룹에 대한 RP가 전체 멀티캐스트 그룹 범위(224.0.0.0/4)에 적용됩니다.

프로시저

특정 인터페이스에서 PIM을 활성화하거나 다시 활성화합니다.

pim rp-address ip_address [acl] [**bidir**]

ip_address 인수는 PIM RP에 할당된 라우터의 유니캐스트 IP 주소입니다.

acl 인수는 RP가 사용할 멀티캐스트 그룹을 정의하는 표준 ACL의 이름이나 번호입니다. 호스트 ACL을 이 명령과 함께 사용하지 마십시오.

bidir 키워드를 제외하면 그룹이 PIM 스파스 모드로 작동하게 됩니다.

참고 실제 양방향 구성에 관계없이 ASA는 PIM hello 메시지에서 항상 양방향 기능을 알립니다.

예제**:**

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

지정된 라우터 우선순위 구성

DR은 PIM 등록, 참여 및 prune 메시지를 RP로 보내는 것을 담당합니다. 네트워크 세그먼트에 멀티캐스트 라우터가 하나 이상 있는 경우 DR 선택은 DR 우선 순위를 따릅니다. 여러 디바이스의 DR 우선순위가 동일한 경우 IP 주소가 가장 높은 디바이스가 DR이 됩니다.

기본적으로 ASA의 DR 우선순위는 1입니다. 이 값을 변경할 수 있습니다.

프로시저

지정된 라우터 우선순위를 변경합니다.

pim dr-priority num

예제:

```
ciscoasa(config-if)# pim dr-priority 500
```

num 인수는 1 ~ 4294967294 범위의 아무 숫자나 될 수 있습니다.

PIM 레지스터 메시지 구성 및 필터링

ASA가 RP 역할을 수행하는 경우 특정 멀티캐스트 소스의 등록을 제한하여 권한이 없는 소스가 RP에 등록하지 못하도록 할 수 있습니다. Request Filter(요청 필터) 창을 통해 ASA가 PIM 등록 메시지를 수락하는 멀티캐스트 소스를 정의할 수 있습니다.

프로시저

PIM 레지스터 메시지를 필터링하도록 ASA를 구성합니다.

pim accept-register {**list** acl | **route-map** map-name}

예제:

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

예에서 ASA는 PIM 레지스터 메시지 *acl1* 및 경로 맵 *map2*를 필터링합니다.

PIM 메시지 간격 구성

PIM DR 선택을 위해 라우터 쿼리 메시지가 사용될 수 있습니다. PIM DR은 라우터 쿼리 메시지 전송을 담당합니다. 기본적으로 라우터 쿼리 메시지는 30초마다 전송됩니다. 또한 ASA는 60초마다 PIM 조인 또는 prune 메시지를 보냅니다.

프로시저

단계 **1** 라우터 쿼리 메시지를 전송합니다.

pim hello-interval seconds

예제:

```
ciscoasa(config-if)# pim hello-interval 60
```

seconds 인수에 유효한 값은 1 ~ 3600초입니다.

단계 **2** ASA가 PIM 조인 또는 prune 메시지를 전송하는 시간(초)을 변경합니다.

pim join-prune-interval seconds

예제:

```
ciscoasa(config-if)# pim join-prune-interval 60
```

seconds 인수에 유효한 값은 10 ~ 600초입니다.

PIM 인접 디바이스 필터링

PIM 네이버가 될 수 있는 라우터를 정의할 수 있습니다. PIM 네이버가 될 수 있는 라우터를 필터링함으로써 다음을 할 수 있습니다.

- 권한이 없는 라우터가 PIM 네이버가 되는 것을 막습니다.
- 연결된 stub 라우터가 PIM에 참여하는 것을 막습니다.

프로시저

단계 **1** 표준 ACL을 사용하여 PIM에 참여시킬 라우터를 정의합니다.

access-list pim_nbr deny *router-IP_addr PIM neighbor*

예제:

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

이 예에서 다음 ACL은 **pim neighbor-filter** 명령과 함께 사용할 경우 10.1.1.1 라우터가 PIM 네이버가 되는 것을 방지합니다.

단계 **2** 인접 디바이스 라우터를 필터링합니다.

pim neighbor-filter pim_nbr

예제:

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

이 예에서 10.1.1.1 라우터는 GigabitEthernet0/3 인터페이스에서 PIM 네이버가 될 수 없습니다.

양방향 인접 디바이스 필터 구성

Bidirectional Neighbor Filter(양방향 네이버 필터) 창은 ASA에 구성된 PIM 양방향 네이버 필터를 표시합니다(있는 경우). PIM 양방향 네이버 필터는 네이버가 DF 선택에 참여할 수 있다고 정의하는 ACL입니다. 인터페이스에 대해 PIM 양방향 네이버 필터가 구성되지 않은 경우에는 제한 사항이 없습니다. PIM 양방향 네이버 필터가 구성된 경우 ACL에서 허용된 네이버만 DF 선택 프로세스에 참여할 수 있습니다.

PIM 양방향 네이버 필터 구성이 ASA에 적용된 경우 ACL이 *interface-name*_multicast라는 이름으로 실행 중인 구성에 표시되며, 여기서 *interface-name*은 멀티캐스트 경계 필터가 적용되는 인터페이스의 이름입니다. 이 이름의 ACL이 이미 존재하는 경우 이름 앞에 숫자가 추가됩니다(예: inside_multicast_1). 이 ACL은 ASA의 PIM 네이버가 될 수 있는 디바이스를 정의합니다.

양방향 PIM은 멀티캐스트 라우터가 축소된 상태 정보를 유지할 수 있게 합니다. 세그먼트의 모든 멀티캐스트 라우터가 bidir에 대해 양방향으로 활성화되어 있어야 DF를 선택할 수 있습니다.

PIM 양방향 네이버 필터는 DF 선택에 참여할 라우터 지정을 허용하는 동시에 모든 라우터가 sparse-mode 도메인에 참여할 수 있게 함으로써 sparse-mode-only 네트워크에서 bidir 네트워크로의 전환을 가능하게 합니다. bidir-enabled 라우터는 bidir 라우터가 세그먼트에 없어도 자기들끼리 DF를 선택할 수 있습니다. non-bidir 라우터의 멀티캐스트 경계는 bidir 그룹의 PIM 메시지 및 데이터가 bidir 그룹이나 bidir 서브셋 클라우드에서 유출되지 않도록 합니다.

PIM 양방향 네이버 필터가 활성화된 경우 ACL에 의해 허용된 라우터는 양방향을 지원하는 것으로 간주됩니다. 따라서 다음은 참입니다.

- 허용된 네이버가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 네이버 장치가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 네이버가 bidir을 지원하지 않을 경우 DF 선택이 일어날 수 있습니다.

프로시저

단계 **1** 표준 ACL을 사용하여 PIM에 참여시킬 라우터를 정의합니다.

access-list pim_nbr deny *router-IP_addr PIM neighbor*

예제**:**

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

이 예에서 다음 ACL은 **pim neighbor-filter** 명령과 함께 사용할 경우 10.1.1.1 라우터가 PIM 네이버가 될 수 없도록 막습니다.

단계 **2** 인접 디바이스 라우터를 필터링합니다.

pim bidirectional-neighbor-filter pim_nbr

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

이 예에서 10.1.1.1 라우터는 GigabitEthernet0/3 인터페이스에서 PIM 양방향 네이버가 될 수 없습니다.

ASA를 후보 BSR로 구성

ASA를 후보 BSR로 구성할 수 있습니다.

프로시저

단계 **1** BSR(부트스트랩 라우터)로 해당 후보를 알리도록 라우터를 구성합니다.

pim bsr-candidate*interface_name* [*hash_mask_length* [*priority*]]

예제**:**

```
ciscoasa(config)# pim bsr-candidate inside 12 3
```

단계 **2** (선택 사항) ASA를 보더 부트스트랩 라우터로 구성합니다.

interface *interface_name*

pim bsr-border

예제**:**

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# pim bsr-border
```

이 명령이 인터페이스에 구성되어 있는 경우, BSR(부트스트랩 라우터) 메시지가 인터페이스를 통해 전송 또는 수신되지 않습니다.

멀티캐스트 경계 구성

주소 범위 지정은 도메인 경계를 정의하여 같은 IP 주소를 가진 RP 도메인이 서로 섞이지 않도록 합니다. 범위 지정은 대형 도메인 내 서브넷 경계와 도메인과 인터넷 사이의 경계에서 이루어집니다.

멀티캐스트 그룹 주소에 대한 인터페이스에서 관리적으로 범위가 지정된 경계를 설정할 수 있습니다. IANA는 관리적으로 범위가 지정된 주소로 239.0.0.0~239.255.255.255의 멀티캐스트 주소 범위를 지정했습니다. 이 주소 범위는 다른 조직이 관리하는 도메인에서 재사용될 수 있습니다. 주소는 전역에서 고유한 주소가 아닌 로컬 주소로 간주됩니다.

표준 ACL은 영향을 받는 주소의 범위를 정의합니다. 경계를 설정할 때 어느 방향으로도 경계를 건너는 멀티캐스트 데이터 패킷 흐름은 허용되지 않습니다. 경계를 통해 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있습니다.

filter-autorp 키워드를 입력하면 자동 RP 검색 및 알림 메시지를 관리적으로 범위가 지정된 경계에서 구성, 검사 및 필터링할 수 있습니다. 경계 ACL에 의해 거부된 Auto-RP 패킷의 모든 Auto-RP 패킷 그룹 범위 알림은 삭제됩니다. Auto-RP 그룹 범위 알림은 Auto-RP 그룹 범위의 모든 주소가 경계 ACL에 의해 허용된 경우에만 경계에서 허용 및 통과됩니다. 주소가 하나라도 허용되지 않은 경우 전체 그룹 범위가 필터링되고 Auto-RP 메시지가 전달되기 전에 Auto-RP 메시지에서 삭제됩니다.

프로시저

멀티캐스트 경계 구성:

multicast boundary acl [**filter-autorp**]

예제**:**

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

PIM에 대한 모니터링

다음 명령을 사용하여 PIM 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조를 참고하십시오.

다양한 PIM 라우팅 통계를 모니터링하거나 비활성화하려면 다음 명령 중 하나를 입력하십시오.

- **show pim bsr-router**

  부트스트랩 라우터 정보를 표시합니다.

- **show mroute**

  멀티캐스트 라우팅 테이블의 내용을 표시합니다.

- **show mfib summary**

  IPv4 PIM 멀티캐스트 전달 정보의 기본 항목 및 인터페이스의 수에 대한 요약 정보를 표시합니다.

- **show mfib active**

  액티브 멀티캐스트 소스가 멀티캐스트 그룹으로 전송하고 있는 속도에 대한 MFIB(Multicast Forwarding Information Base)의 정보를 표시합니다.

- **show pim group-map**

  그룹-PIM 모드 매핑을 표시합니다. 그룹에 대해 선택된 RP를 표시하려면 그룹 주소 또는 이름을 지정합니다.

- **show pim group-map rp-timers**

  각 그룹에 대한 타이머 만료 및 업타임을 PIM 모드 매핑 항목에 표시합니다.

- **show pim neighbor**

  PIM(Protocol Independent Multicast) 네이버를 표시합니다.

멀티캐스트 라우팅 예

다음 예는 다양한 프로세스 옵션으로 멀티캐스트 라우팅을 활성화하고 구성하는 방법을 보여줍니다.

1. 멀티캐스트 라우팅을 활성화합니다.

```
ciscoasa(config)# multicast-routing
```

2. 고정 멀티캐스트 경로를 구성합니다.

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

3. ASA를 멀티캐스트 그룹의 멤버로 구성합니다.

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

멀티캐스트 라우팅 내역

표 ***37:*** 멀티캐스트 라우팅 기록

기능 이름	플랫폼 릴리스	기능 정보
멀티캐스트 라우팅 지원	7.0(1)	멀티캐스트 라우팅 데이터, 인증 및 재배포, 멀티캐스트 라우팅 프로토콜을 이용한 라우팅 정보의 재배포와 모니터링에 대한 지원이 추가되었습니다. **multicast-routing** 명령을 도입했습니다.
클러스터링 지원	9.0(1)	클러스터링 지원이 추가되었습니다. 다음 명령을 도입했습니다. **debug mfib cluster**, **show mfib cluster**.

기능 이름	플랫폼 릴리스	기능 정보
PIM-SSM(Protocol Independent Multicast Source-Specific Multicast) 통과 지원	9.5(1)	ASA가 마지막 홉 라우터인 경우를 제외하고, 멀티캐스트 라우팅을 활성화할 때 PIM-SSM 패킷이 통과하도록 허용하는 지원이 추가되었습니다. 이렇게 하면 다른 공격을 차단하면서 멀티캐스트 그룹을 훨씬 유연하게 선택할 수 있으며, 호스트는 명시적으로 요청된 소스에서만 트래픽을 수신합니다. 명령은 변경하지 않았습니다.
PIM(Protocol Independent Multicast) BSR(부트스트랩 라우터)	9.5(2)	그룹에 대해 랑데부 포인트(RP) 정보를 릴레이하기 위해, 그리고 RP 기능을 위해 후보 라우터를 사용하는 동적 랑데부 포인트(RP) 선택 모델에 대한 지원이 추가되었습니다. 이 기능은 RP(랑데부 포인트)를 동적으로 확인하는 수단을 제공하는데, 이는 RP가 정기적으로 아래위로 이동할 수 있는 대규모의 복잡한 네트워크에서 매우 필수적입니다. 다음 명령을 도입했습니다. clear pim group-map, debug pim bsr, pim bsr-border, pim bsr-candidate, show pim bsr-router, show pim group-map rp-timers

VI 부

AAA 서버 및 로컬 데이터베이스

33 장

AAA 및 로컬 데이터베이스

이 장에서는 인증, 권한 부여, (AAA, “트리플 A”로 발음)에 대해 설명합니다. AAA는 컴퓨터 리소스에 대한 액세스 제어를 위한 서비스의 집합으로 정책을 구현하고, 사용량을 평가하고 서비스에 대한 청구에 필요한 정보를 제공합니다. 이 과정은 효과적인 네트워크 관리 및 보안을 위해 중요한 부분으로 간주됩니다.

이 장에서는 AAA 기능을 위해 로컬 데이터베이스를 구성하는 방법에 대해서도 설명합니다. 외부 AAA 서버의 경우 서버 유형에 대한 장을 참조하십시오.

AAA 및 로컬 데이터베이스

이 섹션에서는 AAA 및 로컬 데이터베이스에 대해 설명합니다.

인증

인증은 액세스를 부여하기 전에 보통 사용자 이름과 비밀번호를 입력하도록 요구하는 방식으로 효과적인 사용자 확인 방법을 제공합니다. AAA 서버는 사용자의 인증 크리덴셜을 데이터베이스에 저장된 다른 사용자의 크리덴셜과 비교합니다. 크리덴셜이 일치하면 사용자는 네트워크에 액세스할 수 있습니다. 크리덴셜이 일치하지 않으면, 인증에 실패하고 네트워크 액세스가 거부됩니다.

Cisco ASA가 다음 항목을 인증하도록 구성할 수 있습니다.

- 다음 세션을 포함한 ASA에 대한 모든 관리 연결:
  - 텔넷
  - SSH
  - 시리얼 콘솔

  - HTTPS를 사용하는 ASDM
  - VPN 관리 액세스
- **enable** 명령
- 네트워크 액세스
- VPN 접속

권한 부여

권한 부여는 정책을 구현하는 프로세스로 사용자의 액세스가 허용된 활동, 리소스 또는 서비스 유형을 판단하는 것입니다. 사용자가 인증되면 해당 사용자는 다양한 액세스 또는 활동 유형에 대한 허가를 받을 수 있습니다.

ASA가 다음 항목에 권한을 부여하도록 구성할 수 있습니다.

- 관리 명령
- 네트워크 액세스
- VPN 접속

어카운팅

어카운팅은 사용자가 액세스 중 소비하는 리소스를 측정합니다. 여기에는 시스템 사용 시간, 사용자가 세션 중 보내거나 받는 데이터의 양 등이 포함됩니다. 어카운팅은 세션 통계 및 사용량 정보 기록을 통해 이루어지며 이는 권한 부여 제어, 청구, 경향 분석, 리소스 활용도 및 용량 계획 활동에 사용됩니다.

인증, 권한 부여 및 어카운팅 간 상호 작용

인증을 단독으로 사용하거나 권한 부여 및 어카운팅과 함께 사용할 수 있습니다. 권한 부여에서는 항상 먼저 사용자의 인증 여부를 확인해야 합니다. 어카운팅을 단독으로 사용하거나 인증 및 권한 부여와 함께 사용할 수 있습니다.

AAA 서버

AAA 서버는 액세스 제어를 위해 사용되는 네트워크 서버입니다. 인증은 사용자를 식별합니다. 권한 부여는 사용자가 액세스할 수 있는 리소스와 서비스를 결정하는 정책을 구현합니다. 어카운팅은 청구 및 분석을 위해 사용되는 시간과 데이터를 추적합니다.

AAA 서버 그룹

인증, 권한 부여 또는 어카운팅을 위해 외부 AAA 서버를 사용하려면 먼저 AAA 프로토콜당 최소 1개의 AAA 서버 그룹을 만들고 하나 이상의 서버를 각 그룹에 추가해야 합니다. AAA 서버 그룹은 이름으로 구분합니다. 각 서버 그룹은 1가지 유형의 서버 또는 서비스에만 해당됩니다.

다음 주제를 참고하십시오.

- RADIUS 서버 그룹 구성, 1077 페이지
- TACACS+ 서버 그룹 구성, 1087 페이지
- LDAP 서버 그룹 구성, 1100 페이지

Kerberos, SDI 및 HTTP 양식에 대한 서버 그룹을 구성할 수도 있습니다. 이러한 그룹은 VPN 구성에 사용됩니다. 이러한 그룹 유형 사용에 대한 자세한 내용은 VPN 구성 가이드를 참고하십시오.

로컬 데이터베이스 정보

ASA는 사용자가 사용자 프로필을 저장할 수 있는 로컬 데이터베이스를 유지합니다. AAA 서버 대신 로컬 데이터베이스를 사용하여 사용자 인증, 권한 부여 및 어카운팅을 제공할 수 있습니다.

다음 기능에 로컬 데이터베이스를 사용할 수 있습니다.

- ASDM 사용자별 액세스
- 콘솔 인증
- 텔넷 및 SSH 인증
- **enable** 명령 인증

  이 설정은 CLI 액세스에만 적용되며 Cisco ASDM 로그인에는 영향을 미치지 않습니다.
- 명령 권한 부여

  로컬 데이터베이스를 사용하여 명령 권한 부여를 켜면 Cisco ASA에서는 사용자 권한 레벨을 참고하여 어떤 명령을 사용할 수 있는지 확인합니다. 그렇지 않을 경우 권한 레벨은 일반적으로 사용되지 않습니다. 기본적으로 모든 명령의 권한 레벨은 0 또는 15입니다.
- 네트워크 액세스 인증
- VPN 클라이언트 인증

다중 상황 모드의 경우, 시스템 실행 영역에서 사용자 이름을 구성하면 **login** 명령을 사용하여 CLI에서 개별 로그인을 제공할 수 있습니다. 그러나 시스템 실행 영역에서 로컬 데이터베이스를 사용하는 AAA 규칙은 구성할 수 없습니다.

참고 네트워크 액세스 권한 부여에는 로컬 데이터베이스를 사용할 수 없습니다.

장애 조치 지원

로컬 데이터베이스는 몇 가지 기능을 지원하기 위한 폴백 방법으로서의 역할을 수행할 수 있습니다. 이러한 동작은 ASA가 실수로 잠기는 것을 방지하기 위해 고안된 것입니다.

사용자가 로그인할 경우 그룹의 서버는 한 번에 하나씩 차례로 액세스되고, 컨피그레이션에서 지정한 첫 번째 서버부터 시작되며 서버가 응답할 때까지 계속됩니다. 그룹의 모든 서버를 사용할 수 없는 경우, 로컬 데이터베이스가 폴백 방법(관리 인증 및 권한 부여만 해당)으로 구성되어 있으면 ASA에서는 로컬 데이터베이스를 사용하려고 시도합니다. 폴백 방법이 없는 경우, ASA에서는 AAA 서버를 사용하기 위한 시도를 계속합니다.

폴백 지원이 필요한 사용자의 경우, 로컬 데이터베이스의 사용자 이름 및 비밀번호가 AAA 서버의 사용자 이름 및 비밀번호와 일치하는 것이 좋습니다. 이러한 방식을 사용하면 투명 폴백 지원이 제공됩니다. 사용자는 서비스를 제공하는 것이 AAA 서버인지 또는 로컬 데이터베이스인지 확인할 수 없으므로, 로컬 데이터베이스의 사용자 이름 및 비밀번호와 다른 사용자 이름 및 비밀번호를 AAA 서버에서 사용할 경우, 해당 사용자는 어떤 사용자 이름 및 비밀번호를 제공하는 게 맞는지 정확히 알 수 없게 됩니다.

로컬 데이터베이스에서는 다음과 같은 폴백 기능을 지원합니다.

- 콘솔 및 enable 비밀번호 인증 — 그룹의 서버를 모두 사용할 수 없는 경우 ASA에서는 로컬 데이터베이스를 사용하여 관리 액세스 권한을 인증하며, 여기에는 enable 비밀번호 인증도 포함될 수 있습니다.
- 명령 권한 부여 — 그룹의 TACACS+ 서버를 모두 사용할 수 없는 경우, 로컬 데이터베이스를 사용하여 권한 레벨을 기준으로 명령에 권한을 부여합니다.
- VPN 인증 및 권한 부여 — 정상적으로 VPN 인증 및 권한 부여를 지원하는 AAA 서버를 사용할 수 없는 경우, ASA에 원격 액세스할 수 있도록 이러한 VPN 서비스가 지원됩니다. 로컬 데이터베이스로 폴백을 수행하도록 구성된 터널 그룹을 관리자의 VPN 클라이언트에서 지정할 경우, 로컬 데이터베이스가 필요한 속성으로 구성되어 있으면 AAA 서버 그룹을 사용할 수 없는 경우에도 VPN 터널을 설정할 수 있습니다.

그룹의 여러 서버에서 장애 조치가 작동하는 방식

서버 그룹에 여러 개의 서버를 구성하고 서버 그룹의 로컬 데이터베이스에 폴백을 사용하도록 설정할 경우, 해당 그룹의 서버가 ASA의 인증 요청에 응답하지 않으면 폴백이 실행됩니다. 다음 시나리오를 이해를 돕기 위한 것입니다.

2개의 Active Directory 서버가 서버 1, 서버 2의 순서대로 포함된 LDAP 서버 그룹을 구성합니다. 원격 사용자가 로그인하면 ASA에서는 서버 1 인증을 시도합니다.

서버 1이 인증 오류로 응답할 경우(예: 사용자가 없음), ASA에서는 서버 2 인증을 시도하지 않습니다.

서버 1이 제한 시간 내에 응답하지 않을 경우(또는 인증 시도 횟수가 구성된 최대 횟수를 초과할 경우), ASA에서는 서버 2 인증을 시도합니다.

그룹의 두 서버가 모두 응답하지 않고 로컬 데이터베이스에 폴백을 수행하도록 ASA가 구성된 경우, ASA에서는 로컬 데이터베이스 인증을 시도합니다.

로컬 데이터베이스에 대한 지침

인증 또는 권한 부여를 위해 로컬 데이터베이스를 사용할 경우 ASA가 잠기는 것을 방지해야 합니다.

로컬 데이터베이스에 사용자 어카운트 추가

로컬 데이터베이스에 사용자를 추가하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 사용자 계정을 생성합니다.

username *username* [**password** *password*] [**privilege** *priv_level*]

예제**:**

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

username *username* 키워드는 공백 및 물음표를 제외하고 인쇄 가능 ASCII 문자(문자 코드 32~126)를 조합한 3~64자의 문자열입니다. **password** *password* 키워드는 공백 및 물음표를 제외하고 인쇄 가능 ASCII 문자(문자 코드 32~126)를 조합한 3~127자의 문자열입니다. 예를 들어 SSH 공개 키 인증을 사용하는 경우 비밀번호 없이 사용자 이름을 생성할 수 있습니다. **privilege** *priv_level* 키워드는 0~15의 범위에서 권한 레벨을 설정합니다. 기본값은 2입니다. 이 권한 레벨은 명령 권한 부여와 함께 사용됩니다.

주의 명령 권한 부여(**aaa authorization console LOCAL** 명령)를 사용하지 않을 경우 기본 레벨 2에서 특권 EXEC 모드에 대한 관리 액세스가 허용됩니다. 특별 권한 EXEC 모드에 대한 액세스를 제한하려면 권한 레벨을 0 또는 1로 설정하거나, **service-type** 명령을 사용합니다.

이렇게 사용도가 낮은 옵션은 위 구문에서 표시되지 않습니다. **nopassword** 키워드는 모든 비밀번호를 수락하는 사용자 어카운트를 생성하므로 이 옵션은 안전하지 않으며 권장되지 않습니다.

encrypted 키워드(9.6 이하 버전에서 32자 이하의 비밀번호용) 또는 **pbkdf2** 키워드(9.6 이상 버전에서 32자 보다 긴 비밀번호 및 9.7 이상 버전에서 모든 길이의 비밀번호용)는 비밀번호가 암호화되어 있음을 나타냅니다(MD5 기반 해시 또는 PBKDF2(비밀번호 기반 키 파생 함수 2) 해시 사용). 새 비밀번호를 입력하지 않는 한, 기존 비밀번호에서는 MD5 기반 해시를 계속해서 사용합니다. **username** 명령에서 비밀번호를 정의하는 경우 ASA에서는 비밀번호를 구성에 저장할 때 암호화하여 보안을 강화합니다. **show running-config** 명령을 입력하면 **username** 명령에서는 실제 비밀번호를 표시하지 않습니다. 암호화된 비밀번호 뒤에 **encrypted** 또는 **pbkdf2** 키워드가 표시됩니다. 예를 들어 "test"라는 비밀번호를 입력할 경우 다음과 비슷한 내용의 **show running-config** 명령 출력이 표시됩니다.

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

CLI에서 **encrypted** 또는 **pbkdf2** 키워드를 실제로 입력하는 유일한 경우는 다른 ASA에서 사용할 구성 파일을 잘라서 붙여넣은 다음, 동일한 비밀번호를 사용하는 경우입니다.

단계 **2** (선택 사항) 사용자 이름 특성을 구성합니다.

username *username(*사용자 이름*)* **attributes**

예제**:**

```
ciscoasa(config)# username exampleuser1 attributes
```

username 인수는 첫 번째 단계에서 생성한 사용자 이름입니다.

기본적으로 이 명령을 사용하여 추가하는 VPN 사용자에게는 특성 또는 그룹 정책 연결이 없습니다. **username attributes** 명령을 사용하여 모든 값을 명시적으로 구성해야 합니다. 자세한 내용은 VPN 구성 가이드를 참고하십시오.

단계 **3** (선택 사항) **aaa authorization exec** 명령을 사용하여 관리 권한 부여를 구성한 경우 사용자 레벨을 구성합니다.

service-type{**admin** | **nas-prompt** | **remote-access**}

예제**:**

```
ciscoasa(config-username)# service-type admin
```

admin 키워드의 경우 **aaa authentication console LOCAL** 명령으로 지정된 모든 서비스에 대한 전체 액세스를 허용합니다. **admin** 키워드는 기본값입니다.

nas-prompt 키워드의 경우 **aaa authentication** {**telnet** | **ssh** | **serial**} **console** 명령을 구성할 때 CLI에 대한 액세스를 허용하지만, **aaa authentication http console** 명령을 구성할 경우 ASDM 구성 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **aaa authentication enable console** 명령으로 인증을 활성화할 경우, 사용자는 **enable** 명령(또는 **login** 명령)을 사용하여 특권 EXEC 모드에 액세스할 수 없습니다.

remote-access 키워드는 관리 액세스를 거부합니다. **aaa authentication console** 명령으로 지정된 모든 서비스를 사용할 수 없습니다(**serial** 키워드는 제외이며 직렬 액세스는 허용됨).

단계 **4** (선택 사항) 사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증에 대한 내용은 SSH 액세스 구성, 1107 페이지을 참고하십시오.

단계 **5** (선택 사항) VPN 인증에 이 사용자 이름을 사용할 경우 해당 사용자에 대해 여러 VPN 속성을 구성할 수 있습니다. 자세한 내용은 VPN 구성 가이드를 참조하십시오.

예

다음 예에서는 권한 레벨 15를 관리자 계정에 할당합니다.

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

다음 예에서는 관리 권한 부여를 활성화하고 비밀번호가 있는 사용자 어카운트를 생성하고 사용자 이름 구성 모드로 들어가고 **nas-prompt**의 **service-type**을 지정합니다.

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

로컬 데이터베이스 모니터링

로컬 데이터베이스를 모니터링하려면 다음 명령을 참고하십시오.

- **show aaa-server**

  이 명령을 사용하면 구성된 데이터베이스 통계가 표시됩니다. AAA 서버 컨피그레이션을 지우려면 **clear aaa-server statistics** 명령을 입력합니다.

- **show running-config aaa-server**

  이 명령을 사용하면 컨피그레이션을 실행 중인 AAA 서버가 표시됩니다. AAA 서버 통계를 지우려면 **clear configure aaa-server** 명령을 입력합니다.

로컬 데이터베이스에 대한 기록

표 ***38:*** 로컬 데이터베이스에 대한 기록

기능 이름	플랫폼 릴리스	설명
AAA의 로컬 데이터베이스 컨피그레이션	7.0(1)	AAA 사용을 위해 로컬 데이터베이스를 구성하는 방법에 대해 설명합니다. 다음 명령을 도입했습니다. **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, aaa authentication {telnet | ssh | serial} console LOCAL**, **aaa authenticationhttp console LOCAL**, **aaa authentication enable console LOCAL**, **showrunning-config aaa-server**, **show aaa-server**, **clear configure aaa-server**, **clear aaa-server statistics**.

기능 이름	플랫폼 릴리스	설명
SSH 공개 키 인증 지원	9.1(2)	이제 사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증을 활성화할 수 있습니다. PKF 형식의 키 또는 Base64 키를 지정할 수 있습니다. PKF 키는 최대 4096비트입니다. ASA의 Base64 형식 지원 범위(최대 2048비트)보다 너무 큰 키에는 PKF 형식을 사용합니다. We introduced the following commands: **ssh authentication**. *8.4(4.1)*에서도 사용 가능. *PKF* 키 형식은 *9.1(2)*에서만 지원됩니다.
로컬 **username** 및 **enable** 비밀번호에 대한 더 긴 비밀번호 지원(최대 127자)	9.6(1)	이제 로컬 **username** 및 **enable** 비밀번호를 최대 127자(이전 제한: 32자)로 생성할 수 있습니다. 32자 보다 긴 비밀번호를 생성하는 경우, 비밀번호는 PBKDF2(비밀번호 기반 키 파생 함수 2) 해시를 사용하여 구성에 저장됩니다. 더 짧은 비밀번호는 계속해서 MD5 기반 해싱 방법을 사용합니다. 다음 명령을 수정했습니다. **enable, username**
SSH 공개 키 인증 개선 사항	9.6(2)	이전 릴리스에서는 로컬 사용자 데이터베이스 (**aaa authentication ssh console LOCAL**)에서 AAA SSH 인증을 활성화하지 않고도 SSH 공개 키 인증(**ssh authentication**)을 활성화할 수 있었습니다. 이제 AAA SSH 인증을 명시적으로 활성화해야 하는 것으로 구성이 수정되었습니다. 사용자가 개인 키 대신 비밀번호를 사용하는 것을 허용하지 않기 위해 이제 정의된 비밀번호 없이 사용자 이름을 생성할 수 없습니다. 다음 명령을 수정했습니다. **ssh authentication, username**

기능 이름	플랫폼 릴리스	설명
모든 로컬 **username** 및 **enable** 비밀번호에 대한 PBKDF2 해싱	9.7(1)	모든 길이의 로컬 **username** 및 **enable** 비밀번호는 PBKDF2(비밀번호 기반 키 파생 함수 2) 해시를 사용하여 구성에 저장됩니다. 이전에는 32자 이하의 비밀번호에서 MD5 기반 해싱 방법을 사용했습니다. 이미 있는 기존 비밀번호는 새 비밀번호를 입력하지 않으면 MD5 기반 해시를 계속해서 사용합니다. 다운그레이드 지침을 확인하려면 일반적인 작업 구성 가이드의 "소프트웨어 및 구성" 장을 참조하십시오. 다음 명령을 수정했습니다. **enable, username**
SSH 공개 키 인증을 사용하는 사용자와 비밀번호를 사용하는 사용자에 대한 개별 인증	9.6(3)/9.8(1)	9.6(2) 이전 릴리스에서는 로컬 사용자 데이터베이스(**aaa authentication ssh console LOCAL**)에서 AAA SSH 인증을 명시적으로 활성화하지 않고도 SSH 공개 키 인증(**ssh authentication**)을 활성화할 수 있습니다. 9.6(2)에서 ASA는 AAA SSH 인증을 명시적으로 활성화하도록 요구했습니다. 이 릴리스에서는 더 이상 AAA SSH 인증을 명시적으로 활성화할 필요가 없습니다. 즉 **ssh authentication** 명령을 사용자에 대해 구성할 때 이 유형의 인증을 사용하는 사용자에 대해 기본적으로 로컬 인증이 활성화됩니다. 게다가 AAA SSH 인증을 명시적으로 구성하는 경우, 이 구성은 비밀번호를 사용하는 사용자 이름에만 적용되며 모든 AAA 서버 유형(예: **aaa authentication ssh console radius_1**)을 사용할 수 있습니다. 예를 들어, 일부 사용자는 로컬 데이터베이스를 사용하여 공개 키 인증을 사용할 수 있으며 다른 사용자는 RADIUS에서 비밀번호를 사용할 수 있습니다. 명령은 수정하지 않았습니다.

34 장

AAA를 위한 RADIUS 서버

이 장에서는 AAA를 위한 RADIUS 서버를 구성하는 방법을 설명합니다.

AAA를 위한 RADIUS 서버 정보

Cisco ASA에서는 AAA를 위해 다음의 RFC 규격 RADIUS 서버를 지원합니다.

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2, 5.x
- Cisco ISE(Identity Services Engine)
- RSA Authentication Manager 5.2, 6.1 및 7.x의 RSA RADIUS
- Microsoft

지원되는 인증 방법

ASA는 RADIUS 서버에서 다음 인증 방법을 지원합니다.

- PAP—모든 연결 유형에 대해 지원됩니다.
- CHAP 및 MS-CHAPv1—L2TP-over-IPsec 연결에 대해 지원됩니다.
- MS-CHAPv2—L2TP-over-IPsec 연결 및 일반 IPsec 원격 액세스 연결(비밀번호 관리 기능이 활성화된 경우)에 대해 지원됩니다. 클라이언트 없는 연결로 MS-CHAPv2를 사용할 수도 있습니다.
- 인증 프록시 모드—RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS- to-Token 서버, RSA/SDI-to-RADIUS 연결에 대해 지원됩니다.

참고 VPN 연결을 위해 ASA와 RADIUS 서버 사이에서 사용할 프로토콜로 MS-CHAPv2를 활성화하려면 터널 그룹 일반 속성에서 비밀번호 관리가 활성화되어 있어야 합니다. 비밀번호 관리를 활성화하면 ASA에서 RADIUS 서버로의 MS-CHAPv2 인증 요청이 생성됩니다. 자세한 내용은 **password-management** 명령의 설명을 참고하십시오.

터널 그룹에서 이중 인증을 사용하고 비밀번호 관리를 활성화하는 경우 기본 및 보조 인증 요청은 MS-CHAPv2 요청 특성을 포함합니다. RADIUS 서버가 MS-CHAPv2를 지원하지 않는 경우 **no mschapv2-capable** 명령을 사용하여 서버가 non-MS-CHAPv2 인증 요청을 보내도록 구성할 수 있습니다.

VPN 연결 사용자 인증

ASA는 동적 ACL 또는 사용자별 ACL 이름을 사용하여 VPN 원격 액세스 및 방화벽 cut-through-proxy 세션의 사용자 인증에 RADIUS 서버를 이용할 수 있습니다. 동적 ACL을 구현하려면 이를 지원하도록 RADIUS 서버를 구성해야 합니다. 사용자가 인증되면 RADIUS 서버가 다운로드 가능한 ACL 또는 ACL 이름을 ASA로 전송합니다. 주어진 서비스에 대한 액세스가 ACL에 의해 허용 또는 거부됩니다. 인증 세션이 만료되면 ASA가 ACL을 삭제합니다.

ACL 외에도 ASA는 VPN 원격 액세스 및 방화벽 cut-through proxy 세션에 대한 권한 부여 및 권한 설정을 위한 다른 여러 속성도 지원합니다.

지원되는 RADIUS 속성 집합

ASA는 다음 RADIUS 속성 집합을 지원합니다.

- RFC 2138에 정의된 인증 특성
- RFC 2139에 정의된 어카운팅 특성
- RFC 2868에 정의된 터널링된 프로토콜 지원을 위한 RADIUS 특성
- RADIUS 공급업체 ID 9로 식별되는 Cisco IOS VSA(Vendor-Specific Attributes)
- RADIUS 공급업체 ID 3076으로 식별되는 Cisco VPN 관련 VSA
- RFC 2548에 정의된 Microsoft VSA

지원되는 RADIUS 권한 부여 속성

권한 부여는 권한 또는 특성을 적용하는 프로세스를 가리킵니다. RADIUS 서버는 권한이나 특성이 구성된 경우 이를 적용하는 인증 서버로 정의됩니다. 이러한 특성은 공급업체 ID가 3076입니다.

다음 표에는 사용자 권한 부여에 사용 가능한 지원되는 RADIUS 속성이 나와 있습니다.

참고 RADIUS 특성 이름은 cVPN3000 접두사를 포함하지 않습니다. Cisco Secure ACS 4.x는 이 새로운 명명법을 지원하지만 4.0 이전 ACS 릴리스의 특성은 여전히 cVPN3000 접두사를 포함합니다. ASA는 속성 이름이 아닌 속성 숫자 ID를 기반으로 RADIUS 속성을 적용합니다.

다음 표에 나열된 모든 속성은 146, 150, 151 및 152 속성 번호를 제외하고 RADIUS 서버에서 ASA로 전송되는 다운스트림 속성입니다. 이러한 속성 번호는 ASA에서 RADIUS 서버로 전송되는 업스트림 속성입니다. RADIUS 속성 146과 150은 인증과 권한 부여 요청을 위해 ASA에서 RADIUS 서버로 전송됩니다. 이전에 나열한 4개의 속성은 모두 어카운팅 시작, 임시 업데이트 및 중단 요청을 위해 ASA에서 RADIUS 서버로 전송됩니다. 업스트림 RADIUS 특성 146, 150, 151, 152는 버전 8.4(3)에서 도입되었습니다.

Cisco ACS 5.x 및 Cisco ISE는 버전9.0(1)에서 RADIUS 인증을 사용하는 IP 주소 할당을 위한 IPv6 프레임 IP 주소를 지원하지 않습니다.

표 ***39:*** 지원되는 ***RADIUS*** 권한 부여 속성

특성 이름	**ASA**	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
Access-Hours	Y	1	문자열	단일	시간 범위의 이름 (예: 업무 시간)
Access-List-Inbound	Y	86	문자열	단일	ACL ID
Access-List-Outbound	Y	87	문자열	단일	ACL ID
Address-Pools	Y	217	문자열	단일	IP 로컬 풀의 이름
Allow-Network-Extension-Mode	Y	64	부울	단일	0 = 비활성화됨 1 = 활성화됨
Authenticated-User-Idle-Timeout	Y	50	정수	단일	1분 ~ 35791394분
Authorization-DN-Field	Y	67	문자열	단일	가능한 값: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name
Authorization-Required		66	정수	단일	0 = 아니요 1 = 예
Authorization-Type	Y	65	정수	단일	0 = 없음 1 = RADIUS 2 = LDAP

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
Banner1	Y	15	문자열	단일	Cisco VPN 원격 액세스 세션에 대해 표시할 배너 문자열: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, Clientless SSL
Banner2	Y	36	문자열	단일	Cisco VPN 원격 액세스 세션에 대해 표시할 배너 문자열: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, Clientless SSL Banner2 문자열은 Banner1 문자열과 연결됩니다(구성된 경우).
Cisco-IP-Phone-Bypass	Y	51	정수	단일	0 = 비활성화됨 1 = 활성화됨
Cisco-LEAP-Bypass	Y	75	정수	단일	0 = 비활성화됨 1 = 활성화됨
Client Type	Y	150	정수	단일	1 = Cisco VPN Client(IKEv1) 2 = AnyConnect Client SSL VPN 3 = 클라이언트리스 SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN(IKEv2)
Client-Type-Version-Limiting	Y	77	문자열	단일	IPsec VPN 버전 번호 문자열
DHCP-Network-Scope	Y	61	문자열	단일	IP 주소
Extended-Authentication-On-Rekey	Y	122	정수	단일	0 = 비활성화됨 1 = 활성화됨

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
Group-Policy	Y	25	문자열	단일	원격 액세스 VPN 세션에 대한 그룹 정책을 설정합니다. 버전 8.2.x 이상에서는 IETF-Radius-Class 대신 이 특성을 사용하십시오. 다음 형식 중 하나를 사용할 수 있습니다. • 그룹 정책 이름 • OU=그룹 정책 이름 • OU=그룹 정책 이름;
IE-Proxy-Bypass-Local		83	정수	단일	0 = 없음 1 = 로컬
IE-Proxy-Exception-List		82	문자열	단일	줄바꿈(\n)으로 구분된 DNS 도메인 목록
IE-Proxy-PAC-URL	Y	133	문자열	단일	PAC 주소 문자열
IE-Proxy-Server		80	문자열	단일	IP 주소
IE-Proxy-Server-Policy		81	정수	단일	1 = 수정 없음 2 = 프록시 없음 3 = 자동 탐지 4 = 집중 장치 설정 사용
IKE-KeepAlive-Confidence-Interval	Y	68	정수	단일	10초 ~ 300초
IKE-Keepalive-Retry-Interval	Y	84	정수	단일	2초 ~ 10초
IKE-Keep-Alives	Y	41	부울	단일	0 = 비활성화됨 1 = 활성화됨
Intercept-DHCP-Configure-Msg	Y	62	부울	단일	0 = 비활성화됨 1 = 활성화됨

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
IPsec-Allow-Passwd-Store	Y	16	부울	단일	0 = 비활성화됨 1 = 활성화됨
IPsec-Authentication		13	정수	단일	0 = 없음 1 = RADIUS 2 = LDAP(권한 부여만 해당) 3 = NT 도메인 4 = SDI 5 = 내부 6 = 만료 기간이 있는 RADIUS 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	부울	단일	0 = 비활성화됨 1 = 활성화됨
IPsec-Backup-Server-List	Y	60	문자열	단일	서버 주소(공백 구분)
IPsec-Backup-Servers	Y	59	문자열	단일	1 = 클라이언트 구성 목록 사용 2 = 클라이언트 목록 비활성화 및 지우기 3 = 백업 서버 목록 사용
IPsec-Client-Firewall-Filter-Name		57	문자열	단일	클라이언트에 방화벽 정책으로 푸시할 필터의 이름을 지정합니다.
IPsec-Client-Firewall-Filter-Optional	Y	58	정수	단일	0 = 필수 1 = 선택 사항
IPsec-Default-Domain	Y	28	문자열	단일	클라이언트로 보낼 단일 기본 도메인 이름을 지정합니다(1자 ~ 255자).
IPsec-IKE-Peer-ID-Check	Y	40	정수	단일	1 = 필수 2 = 피어 인증서별로 지원되는 경우 3 = 확인하지 않음

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
IPsec-IP-Compression	Y	39	정수	단일	0 = 비활성화됨 1 = 활성화됨
IPsec-Mode-Config	Y	31	부울	단일	0 = 비활성화됨 1 = 활성화됨
IPsec-Over-UDP	Y	34	부울	단일	0 = 비활성화됨 1 = 활성화됨
IPsec-Over-UDP-Port	Y	35	정수	단일	4001 ~ 49151. 기본값은 10000입니다.
IPsec-Required-Client-Firewall-Capability	Y	56	정수	단일	0 = 없음 1 = 원격 FW AYT(Are-You-There)에 의해 정의된 정책 2 = 정책 푸시됨 CPP 4 = 서버의 정책
IPsec-Sec-Association		12	문자열	단일	보안 연결의 이름
IPsec-Split-DNS-Names	Y	29	문자열	단일	클라이언트로 보낼 보조 도메인 이름의 목록을 지정합니다(1자 ~ 255자).
IPsec-Split-Tunneling-Policy	Y	55	정수	단일	0 = 스플릿 터널링 없음 1 = 스플릿 터널링 2 = 로컬 LAN 허용됨
IPsec-Split-Tunnel-List	Y	27	문자열	단일	스플릿 터널 포함 목록을 설명하는 네트워크 또는 ACL의 이름을 지정합니다.
IPsec-Tunnel-Type	Y	30	정수	단일	1 = LAN-to-LAN 2 = 원격 액세스
IPsec-User-Group-Lock		33	부울	단일	0 = 비활성화됨 1 = 활성화됨
IPv6-Address-Pools	Y	218	문자열	단일	IP 로컬 풀(IPv6)의 이름

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
IPv6-VPN-Filter	Y	219	문자열	단일	ACL 값
L2TP-Encryption		21	정수	단일	비트맵: 1 = 암호화 필수 2 = 40비트 4 = 128비트 8 = 스테이트리스 필수 15 = 40/128 암호화/스테이트리스 필수
L2TP-MPPC-Compression		38	정수	단일	0 = 비활성화됨 1 = 활성화됨
Member-Of	Y	145	문자열	단일	쉼표로 구분된 문자열, 예: `Engineering, Sales` 동적 액세스 정책에서 사용할 수 있는 관리 특성입니다. 이는 그룹 정책을 설정하지 않습니다.
MS-Client-Subnet-Mask	Y	63	부울	단일	IP 주소
NAC-Default-ACL		92	문자열		ACL
NAC-Enable		89	정수	단일	0 = 아니요 1 = 예
NAC-Revalidation-Timer		91	정수	단일	300초 ~ 86400초
NAC-Settings	Y	141	문자열	단일	NAC 정책의 이름
NAC-Status-Query-Timer		90	정수	단일	30초 ~ 1800초
Perfect-Forward-Secrecy-Enable	Y	88	부울	단일	0 = 아니요 1 = 예
PPTP-Encryption		20	정수	단일	비트맵: 1 = 암호화 필수 2 = 40비트 4 = 128비트 8 = 스테이트리스 필수 15 = 40/128 암호화/스테이트리스 필수
PPTP-MPPC-Compression		37	정수	단일	0 = 비활성화됨 1 = 활성화됨

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
Primary-DNS	Y	5	문자열	단일	IP 주소
Primary-WINS	Y	7	문자열	단일	IP 주소
Privilege-Level	Y	220	정수	단일	0과 15 사이의 정수입니다.
Required-Client-Firewall-Vendor-Code	Y	45	정수	단일	1 = Cisco Systems(Cisco Integrated Client) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems(Cisco Intrusion Prevention Security Agent)
Required-Client-Firewall-Description	Y	47	문자열	단일	문자열
Required-Client-Firewall-Product-Code	Y	46	정수	단일	Cisco Systems 제품: 1 = Cisco Intrusion Prevention Security Agent 또는 Cisco Integrated Client(CIC) Zone Labs 제품: 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 제품: 1 = BlackIce Defender/Agent Sygate 제품: 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	정수	단일	0 = 비활성화됨 1 = 활성화됨
Require-HW-Client-Auth	Y	48	부울	단일	0 = 비활성화됨 1 = 활성화됨
Secondary-DNS	Y	6	문자열	단일	IP 주소

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
Secondary-WINS	Y	8	문자열	단일	IP 주소
SEP-Card-Assignment		9	정수	단일	사용되지 않음
세션 하위 유형	Y	152	정수	단일	0 = 없음 1 = 클라이언트리스 2 = 클라이언트 3 = 클라이언트 전용 세션 하위 유형은 세션 유형(151) 특성에 1, 2, 3, 4의 값이 포함될 때만 적용됩니다.
세션 유형	Y	151	정수	단일	0 = 없음 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN(IKEv2) 3=클라이언트리스 SSL VPN 4 = 클라이언트리스 이메일 프록시 5 = Cisco VPN Client(IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN 로드 밸런싱
Simultaneous-Logins	Y	2	정수	단일	0 ~ 2147483647
Smart-Tunnel	Y	136	문자열	단일	스마트 터널의 이름
Smart-Tunnel-Auto	Y	138	정수	단일	0 = 비활성화됨 1 = 활성화됨 2 = 자동 시작
Smart-Tunnel-Auto-Signon-Enable	Y	139	문자열	단일	도메인 이름이 추가된 스마트 터널 자동 로그인 목록의 이름
Strip-Realm	Y	135	부울	단일	0 = 비활성화됨 1 = 활성화됨

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
SVC-Ask	Y	131	문자열	단일	0 = 비활성화됨 1 = 활성화됨 3 = 기본 서비스 활성화 5 = 기본 클라이언트리스 활성화(2 및 4는 사용되지 않음)
SVC-Ask-Timeout	Y	132	정수	단일	5초 ~ 120초
SVC-DPD-Interval-Client	Y	108	정수	단일	0 = 꺼짐 5~3600초
SVC-DPD-Interval-Gateway	Y	109	정수	단일	0 = 꺼짐) 5~3600초
SVC-DTLS	Y	123	정수	단일	0 = False 1 = True
SVC-Keepalive	Y	107	정수	단일	0 = 꺼짐 15~600초
SVC-Modules	Y	127	문자열	단일	문자열(모듈 이름)
SVC-MTU	Y	125	정수	단일	MTU 값 256~1406(바이트)
SVC-Profiles	Y	128	문자열	단일	문자열(프로필 이름)
SVC-Rekey-Time	Y	110	정수	단일	0 = 비활성화됨 1~10080분
터널 그룹 이름	Y	146	문자열	단일	1자 ~ 253자
Tunnel-Group-Lock	Y	85	문자열	단일	터널 그룹의 이름 또는 “none”
Tunneling-Protocols	Y	11	정수	단일	1 = PPTP 2 = L2TP 4 = IPSec(IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec(IKEv2) 8 및 4는 상호 배타적임. 0 - 11, 16 - 27, 32 - 43, 48 - 59는 올바른 값임.
Use-Client-Address		17	부울	단일	0 = 비활성화됨 1 = 활성화됨
VLAN	Y	140	정수	단일	0 ~ 4094

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
WebVPN-Access-List	Y	73	문자열	단일	액세스 목록 이름
WebVPN ACL	Y	73	문자열	단일	디바이스의 WebVPN ACL 이름
WebVPN-ActiveX-Relay	Y	137	정수	단일	0 = 비활성화됨 기타 = 활성화됨
WebVPN-Apply-ACL	Y	102	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Auto-HTTP-Signon	Y	124	문자열	단일	예약
WebVPN-Citrix-Metaframe-Enable	Y	101	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Content-Filter-Parameters	Y	69	정수	단일	1 = Java ActiveX 2 = Java Script 4 = 이미지 8 = 이미지의 쿠키
WebVPN-Customization	Y	113	문자열	단일	사용자 정의의 이름
WebVPN-Default-Homepage	Y	76	문자열	단일	http://example-example.com과 같은 URL
WebVPN-Deny-Message	Y	116	문자열	단일	유효한 문자열(최대 500자)
WebVPN-Download_Max-Size	Y	157	정수	단일	0x7fffffff
WebVPN-File-Access-Enable	Y	94	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-File-Server-Browsing-Enable	Y	96	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-File-Server-Entry-Enable	Y	95	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	문자열	단일	와일드카드(*) 옵션을 포함한 쉼표로 구분된 DNS/IP(예: *.cisco.com, 192.168.1.*, wwwin.cisco.com)

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
WebVPN-Hidden-Shares	Y	126	정수	단일	0 = 없음 1 = 표시
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	부울	단일	클라이언트리스 홈 페이지가 스마트 터널을 통해 만들어지는 경우 활성화됩니다.
WebVPN-HTML-Filter	Y	69	비트맵	단일	1 = Java ActiveX 2 = 스크립트 4 = 이미지 8 = 쿠키
WebVPN-HTTP-Compression	Y	120	정수	단일	0 = 꺼짐 1 = Deflate 압축
WebVPN-HTTP-Proxy-IP-Address	Y	74	문자열	단일	http= 또는 https= 접두사를 포함한 쉼표로 구분된 DNS/IP:port(예: http=10.10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	Y	148	정수	단일	0~30. 0 = 비활성화됨
WebVPN-Keepalive-Ignore	Y	121	정수	단일	0 ~ 900
WebVPN-Macro-Substitution	Y	223	문자열	단일	무제한
WebVPN-Macro-Substitution	Y	224	문자열	단일	무제한
WebVPN-Port-Forwarding-Enable	Y	97	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Port-Forwarding-List	Y	72	문자열	단일	포트 전달 목록 이름

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
WebVPN-Port-Forwarding-Name	Y	79	문자열	단일	문자열 이름(예: "Corporate-Apps"). 이 텍스트는 클라이언트리스 포털 홈페이지에서 기본 문자열인 "Application Access"를 대체합니다.
WebVPN-Post-Max-Size	Y	159	정수	단일	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	정수	단일	0~30. 0 = 비활성화됨
WebVPN Smart-Card-Removal-Disconnect	Y	225	부울	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-Smart-Tunnel	Y	136	문자열	단일	스마트 터널의 이름
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	문자열	단일	도메인 이름이 추가된 스마트 터널 자동 로그인 목록의 이름
WebVPN-Smart-Tunnel-Auto-Start	Y	138	정수	단일	0 = 비활성화됨 1 = 활성화됨 2 = 자동 시작
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	문자열	단일	"e networkname", "i networkname" 또는 "a" 중 하나입니다. 여기서 networkname은 스마트 터널 네트워크 목록의 이름을, e는 제외된 터널을, i는 지정된 터널을, a는 모든 터널을 나타냅니다.
WebVPN-SSL-VPN-Client-Enable	Y	103	정수	단일	0 = 비활성화됨 1 = 활성화됨

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-SSL-VPN-Client-Required	Y	104	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-SSO-Server-Name	Y	114	문자열	단일	유효한 문자열
WebVPN-Storage-Key	Y	162	문자열	단일	
WebVPN-Storage-Objects	Y	161	문자열	단일	
WebVPN-SVC-Keepalive-Frequency	Y	107	정수	단일	15초 ~ 600초, 0 = 꺼짐
WebVPN-SVC-Client-DPD-Frequency	Y	108	정수	단일	5초 ~ 3600초, 0 = 꺼짐
WebVPN-SVC-DTLS-Enable	Y	123	정수	단일	0 = 비활성화됨 1 = 활성화됨
WebVPN-SVC-DTLS-MTU	Y	125	정수	단일	MTU 값은 256바이트 ~ 1406바이트입니다.
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	정수	단일	5초 ~ 3600초, 0 = 꺼짐
WebVPN-SVC-Rekey-Time	Y	110	정수	단일	4분 ~ 10080분, 0 = 꺼짐
WebVPN-SVC-Rekey-Method	Y	111	정수	단일	0(꺼짐), 1(SSL), 2(새 터널)
WebVPN-SVC-Compression	Y	112	정수	단일	0(꺼짐), 1(Deflate 압축)
WebVPN-UNIX-Group-ID (GID)	Y	222	정수	단일	유효한 UNIX 그룹 ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	정수	단일	유효한 UNIX 사용자 ID
WebVPN-Upload-Max-Size	Y	158	정수	단일	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	정수	단일	0 = 비활성화됨 1 = 활성화됨

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
WebVPN-URL-List	Y	71	문자열	단일	URL 목록 이름
WebVPN-User-Storage	Y	160	문자열	단일	
WebVPN-VDI	Y	163	문자열	단일	설정 목록

지원되는 IETF RADIUS 권한 부여 속성

다음 표에는 지원되는 IETF RADIUS 특성이 나와 있습니다.

표 *40:* 지원되는 *IETF RADIUS* 특성

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
IETF-Radius-Class	Y	25		단일	버전 8.2.x 이상에서는 Group-Policy 특성(VSA 3076, #25)을 사용하십시오. • 그룹 정책 이름 • OU=그룹 정책 이름 • OU=그룹 정책 이름
IETF-Radius-Filter-Id	Y	11	문자열	단일	ASA에 정의된 ACL 이름으로, 전체 터널 IPsec 및 SSL VPN 클라이언트에만 적용됩니다.
IETF-Radius-Framed-IP-Address	Y	해당 없음	문자열	단일	IP 주소
IETF-Radius-Framed-IP-Netmask	Y	해당 없음	문자열	단일	IP 주소 마스크
IETF-Radius-Idle-Timeout	Y	28	정수	단일	시간(초)

특성 이름	ASA	특성 번호	구문/유형	단일 또는 다중 값 지정	설명 또는 값
IETF-Radius-Service-Type	Y	6	정수	단일	초. 가능한 서비스 유형 값: • .Administrative—사용자에게 구성 프롬프트 액세스가 허용됩니다. • .NAS-Prompt—사용자에게 실행 프롬프트 액세스가 허용됩니다. • .remote-access—사용자에게 네트워크 액세스가 허용됩니다.
IETF-Radius-Session-Timeout	Y	27	정수	단일	시간(초)

RADIUS 어카운팅 연결 종료 사유 코드

이 코드는 ASA가 패킷 전송 중 연결이 끊길 때 반환됩니다.

연결 종료 사유 코드
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9

연결 종료 사유 코드
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA를 위한 RADIUS 서버에 대한 지침

이 섹션에서는 AAA를 위한 RADIUS 서버를 구성하기 전에 확인해야 하는 제한 사항 및 지침에 대해 설명합니다.

- 단일 모드로 최대 100개의 서버 그룹 또는 다중 모드로 상황당 4개의 서버 그룹을 포함할 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다.

AAA를 위한 RADIUS 서버 구성

이 섹션에서는 AAA를 위한 RADIUS 서버를 구성하는 방법을 설명합니다.

프로시저

단계 **1** RADIUS 서버에 ASA 속성을 로드합니다. 특성을 로드하는 방법은 사용하는 RADIUS 서버 유형에 따라 다릅니다.

- Cisco ACS를 사용하는 경우 서버에 이미 이러한 특성이 통합되어 있습니다. 이 단계를 건너뛸 수 있습니다.
- 다른 공급업체의 RADIUS 서버(예: Microsoft Internet Authentication Service)의 경우 각 ASA 속성을 수동으로 정의해야 합니다. 특성을 정의하려면 특성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

단계 **2** RADIUS 서버 그룹 구성, 1077 페이지.

단계 **3** 그룹에 RADIUS 서버 추가, 1080 페이지.

RADIUS 서버 그룹 구성

인증, 권한 부여, 어카운팅에 외부 RADIUS 서버를 사용하려면 먼저 AAA 프로토콜당 1개 이상의 RADIUS 서버 그룹을 생성하고 각 그룹에 서버를 1개 이상 추가해야 합니다.

프로시저

단계 **1** RADIUS AAA 서버 그룹을 생성합니다.

aaa-server *group_name* **protocol radius**

예제:

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol 명령을 입력하면 aaa-server 그룹 구성 모드로 들어갑니다.

단계 **2** (선택 사항). 다음 서버를 시도하기 전에 그룹의 RADIUS 서버로 보낼 수 있는 최대 요청 횟수를 지정합니다.

max-failed-attempts *number*

범위는 1~5입니다. 기본값은 3입니다.

로컬 데이터베이스를 사용하여 장애 조치 방법을 구성한 경우(관리 액세스에만 해당) 그룹의 모든 서버가 응답하지 않으면 그룹이 응답하지 않는 것으로 간주되고 장애 조치 방법이 시도됩니다. 서버 그룹은 10분(기본값) 동안 무응답으로 표시됩니다. 그러면 이 기간에 다른 AAA 요청에서 서버 그룹 접속을 시도하지 않으며 즉시 대비책이 사용됩니다. 무응답 기간을 기본값이 아닌 값으로 변경하려면 다음 단계의 **reactivation-mode** 명령을 참조하십시오.

대비책이 없는 경우 ASA는 그룹의 서버를 계속 재시도합니다.

예제:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

단계 **3** (선택 사항). 그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

여기서 각 항목은 다음을 나타냅니다.

- **depletion** [**deadtime** *minutes*]는 그룹의 모든 서버가 비활성되어야만 실패한 서버를 재활성화합니다. 이것이 기본 재활성화 모드입니다. 그룹의 마지막 서버를 비활성화한 시점부터 나중에 모든 서버를 다시 활성화한 시점까지 경과한 시간을 0~1440분 범위에서 지정할 수 있습니다. 기본은 10분입니다.
- **timed** 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.

예제**:**

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

단계 **4** (선택 사항). 그룹의 모든 서버에 어카운팅 메시지를 전송합니다.

accounting-mode simultaneous

활성 서버로만 메시지를 전송하는 기본 설정을 복원하려면 **accounting-mode single** 명령을 입력합니다.

예제**:**

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

단계 **5** (선택 사항). RADIUS interim-accounting-update 메시지를 정기적으로 생성하도록 활성화합니다.

interim-accounting-update [**periodic** [*hours*]]

ISE는 ASA와 같은 NAS 디바이스에서 수신하는 어카운팅 레코드를 기반으로 하는 활성 세션의 디렉터리를 유지합니다. 그러나 ISE가 5일 동안 세션이 여전히 활성 상태(어카운팅 메시지 또는 포스처 트랜잭션)임을 나타내는 메시지를 수신하지 않은 경우 데이터베이스에서 세션 레코드를 제거합니다. 장기 VPN 연결이 제거되지 않도록 하려면 모든 활성 세션에 대해 정기적으로 ISE에 interim-accounting-update 메시지를 전송하도록 그룹을 구성합니다.

- **periodic** [*hours*]는 문제의 서버 그룹으로 계정 관리 기록을 전송하도록 구성된 모든 VPN 세션에 대한 계정 관리 기록의 주기적 생성 및 전송을 활성화합니다. 선택적으로 이러한 업데이트를 전송할 간격을 시간 단위로 포함할 수 있습니다. 기본값은 24시간, 범위는 1~120입니다.
- (매개변수가 없습니다.) **periodic** 키워드 없이 이 명령을 사용하는 경우 VPN 터널 연결이 클라이언트리스 VPN 세션에 추가될 경우에만 ASA에서 interim-accounting-update 메시지를 전송합니다. 이 경우 어카운팅 업데이트가 생성되어 RADIUS 서버에 새로 할당된 IP 주소를 알려줍니다.

예제**:**

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

단계 **6** (선택 사항). AAA 서버 그룹에 대해 RADIUS 동적 권한 부여(ISE CoA(Change of Authorization)) 서비스를 활성화합니다.

dynamic-authorization [**port** *number*]

포트를 지정하는 것은 선택 사항입니다. 기본값은 1700이고, 범위는 1024~65535입니다.

VPN 터널에서 서버 그룹을 사용하면 RADIUS 서버 그룹이 CoA 알림에 등록되고 ASA는 ISE에서 보내는 CoA 정책 업데이트를 포트에서 수신합니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

예제:

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

단계 **7** (선택 사항). 인증에 ISE를 사용하지 않으려면 RADIUS 서버 그룹에 대해 권한 부여 전용 모드를 활성화합니다. (ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 권한 부여 전용 모드를 활성화합니다.)

authorize-only

이것은 이 서버 그룹이 권한 부여에 사용될 때 RADIUS Access Request 메시지가 AAA 서버에 대해 정의된 구성된 비밀번호 방식이 아니라 "Authorize Only" 요청으로 작성됨을 의미합니다. RADIUS 서버에 대한 **radius-common-pw** 명령을 사용하여 공통 비밀번호를 구성하지 않으면 무시됩니다.

예를 들어, 인증에 이 서버 그룹보다 인증서를 사용하려면 권한 부여 전용 모드를 사용합니다. VPN 터널에서 권한 부여 및 어카운팅에 대한 이 서버 그룹을 계속 사용합니다.

예제:

```
ciscoasa(config-aaa-server-group)# authorize-only
```

단계 **8** (선택 사항). RADIUS 패킷에서 Cisco AV 쌍으로 수신된 ACL과 다운로드 가능한 ACL을 병합합니다.

merge-dacl {**before-avpair** | **after-avpair**}

예제:

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

이 옵션은 VPN 연결에만 적용됩니다. VPN 사용자의 경우 ACL은 Cisco AV 쌍 ACL, 다운로드 가능한 ACL 및 ASA에서 구성된 ACL의 형식이 될 수 있습니다. 이 옵션은 다운로드 가능한 ACL과 AV 쌍 ACL의 병합 여부를 결정하며 ASA에 구성된 ACL에는 적용되지 않습니다.

기본 설정은 다운로드 가능한 ACL을 Cisco AV 쌍 ACL과 병합하지 않도록 지정하는 **no merge dacl** 입니다. AV 쌍과 다운로드 가능한 ACL이 모두 수신되는 경우 AV 쌍이 우선 사용됩니다.

before-avpair 옵션은 다운로드 가능한 ACL 항목이 Cisco AV 쌍 항목 앞에 배치되도록 지정합니다.

after-avpair 옵션은 다운로드 가능한 ACL 항목이 Cisco AV 쌍 항목 뒤에 배치되도록 지정합니다.

예

다음 예에서는 단일 서버로 하나의 RADIUS 그룹을 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

다음 예는 동적 권한 부여(CoA) 업데이트 및 시간별 주기적 계정 관리를 위해 ISE 서버 그룹을 구성하는 방법을 보여 줍니다. ISE와 비밀번호 인증을 구성하는 터널 그룹 구성이 포함됩니다.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

다음 예는 ISE를 사용하여 로컬 인증서 검증 및 권한 부여를 위한 터널 그룹을 구성하는 방법을 보여줍니다. 서버 그룹이 인증에 사용되지 않으므로 서버 그룹 구성에서 권한 부여 전용 명령을 포함합니다.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

그룹에 **RADIUS** 서버 추가

그룹에 RADIUS 서버를 추가하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** RADIUS 서버와 해당 서버가 속한 AAA 서버 그룹을 식별합니다.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

예제:

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name*)을 지정하지 않는 경우, ASA는 기본적으로 **inside**interface을 사용합니다.

단계 **2** ASA가 RADIUS 서버의 다운로드 가능 ACL로부터 수신한 넷마스크를 취급하는 방법을 지정합니다.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

예제:

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

auto-detect 키워드는 ASA가 사용된 넷마스크 식의 유형 확인을 시도하도록 지정합니다. ASA가 와일드카드 넷마스크 표현을 발견하면 이를 표준 넷마스크 표현으로 변환합니다.

standard 키워드는 ASA가 RADIUS 서버로부터 수신한 다운로드 가능한 ACL에 표준 넷마스크 식만 포함되어 있다고 가정한다고 지정합니다. 와일드카드 넷마스크 표현에 대한 변환이 이루어지지 않습니다.

wildcard 키워드는 ASA가 RADIUS 서버로부터 수신한 다운로드 가능한 ACL에 와일드카드 넷마스크 식만 포함되어 있다고 가정하고 ACL가 다운로드될 때 모두 표준 넷마스크 식으로 변환한다고 지정합니다.

단계 **3** ASA를 통해 RADIUS 권한 부여 서버에 액세스하는 모든 사용자에 대해 사용되는 공통 비밀번호를 지정합니다.

radius-common-pw 문자열

예제:

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

string 인수는 대/소문자를 구분하는 최대 127자의 영숫자 키워드이며, RADIUS 서버와의 모든 권한 부여 트랜잭션에서 공통 비밀번호로 사용됩니다.

단계 **4** RADIUS 서버로의 MS-CHAPv2 인증 요청을 활성화합니다.

mschapv2-capable

예제:

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

단계 **5** ASA가 백업 서버에 요청을 보내기 전에 기본 서버에서 응답을 기다리는 시간을 초 단위로 지정합니다.

timeout *hh:mm:ss*

예제:

```
ciscoasa(config-aaa-server-host)# timeout 15
```

단계 **6** 이전 명령에서 지정된 특정 AAA 서버의 재시도 간 시간 간격을 구성합니다.

retry-interval *seconds*

예제:

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

seconds 인수는 요청에 대한 재시도 간격(1초 ~ 10초)을 지정합니다. 연결 요청 재시도에 앞서 ASA가 기다리는 시간입니다.

참고 다음 재시도까지의 간격은 입력한 재시도 간격 설정과 무관하게 항상 50밀리초 또는 100밀리초입니다. 이는 정상적인 동작입니다.

단계 **7** 그룹의 모든 서버에 어카운팅 메시지를 전송합니다.

accounting-mode simultaneous

예제:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

활성 서버에만 메시지 전송의 기본값을 복원하려면 **accounting-mode single** 명령을 입력합니다.

단계 **8** 인증 포트를 포트 번호 1645 또는 사용자 인증에 사용되는 서버 포트로 지정합니다.

authentication-port *port*

예제:

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

단계 **9** 어카운팅 포트를 포트 번호 1646 또는 이 호스트에 대한 어카운팅에 사용되는 서버 포트로 지정합니다.

accounting-port *port*

예제:

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

단계 **10** RADIUS 서버를 ASA에 인증하는 데 사용하는 서버 암호 값을 지정합니다. 서버 비밀번호는 RADIUS 서버에서 구성한 것과 일치해야 합니다. 서버 비밀번호를 모르는 경우 RADIUS 서버 관리자에게 문의하십시오. 최대 길이는 64자입니다.

key

예제:

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

서버 비밀번호는 RADIUS 서버에서 구성한 것과 일치해야 합니다. 서버 비밀번호를 모르는 경우 RADIUS 서버 관리자에게 문의하십시오. 최대 길이는 64자입니다.

예

다음 예는 RADIUS 서버를 기존 RADIUS 서버 그룹에 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

AAA를 위한 RADIUS 서버 모니터링

AAA를 위한 RADIUS 서버의 상태를 모니터링하려면 다음의 명령을 참고하십시오.

- **show aaa-server**

  이 명령은 구성된 RADIUS 서버 통계를 보여 줍니다. 카운터를 0으로 재설정하려면 **clear aaa-server statistics** 명령을 사용할 수 있습니다.

- **show running-config aaa-server**

  이 명령은 구성을 실행 중인 RADIUS 서버를 보여 줍니다.

AAA를 위한 RADIUS 서버 내역

표 *41: AAA*를 위한 *RADIUS* 서버 내역

기능 이름	플랫폼 릴리스	설명
AAA를 위한 RADIUS 서버	7.0(1)	AAA를 위한 RADIUS 서버를 구성하는 방법을 설명합니다. 다음 명령을 도입했습니다. **aaa-server protocol**, **max-failed-attempts**, **reactivation-mode**, **accounting-mode simultaneous**, **aaa-server host**, **show aaa-server**, **show running-config aaa-server**, **clear aaa-server statistics**, **authentication-port**, **accounting-port**, **retry-interval**, **acl-netmask-convert**, **clear configure aaa-server**, **merge-dacl**, **radius-common-pw, key**.
ASA에서 RADIUS 액세스 요청 및 어카운팅 요청 패킷으로 전송되는 주요 VSA(Vendor-Specific Attribute)	8.4(3)	4개의 새로운 VSA — 터널 그룹 이름(146) 및 클라이언트 유형(150)은 ASA에서 RADIUS 액세스 요청 패킷으로 전송됩니다. 세션 유형(151) 및 세션 하위 유형(152)은 ASA에서 RADIUS 어카운팅 요청 패킷으로 전송됩니다. 4가지 특성은 모두 모든 어카운팅 요청 패킷 유형(Start, Interim-Update 및 Stop)에 대해 전송됩니다. 그러면 RADIUS 서버(예: ACS 및 ISE)가 권한 부여 또는 정책 특성을 시행하거나 이를 어카운팅 및 청구 목적으로 사용할 수 있습니다.

35 장

AAA를 위한 TACACS+ 서버

이 장에서는 AAA에서 사용되는 TACACS+ 서버 구성 방법을 설명합니다.

AAA를 위한 TACACS+ 서버 정보

ASA는 ASCII, PAP, CHAP 및 MS-CHAPv1 프로토콜을 통한 TACACS+ 서버 인증을 지원합니다.

TACACS+ 특성

Cisco ASA에서는 TACACS+ 속성을 지원합니다. TACACS+ 특성은 인증, 권한 부여, 어카운팅 기능을 분리합니다. 이 프로토콜은 필수 및 선택의 두 가지 특성 유형을 지원합니다. 서버와 클라이언트가 모두 필수 특성을 이해해야 하고 필수 특성이 사용자에게 적용되어야 합니다. 선택 특성은 이해되거나 사용될 수 있고 그렇지 않을 수도 있습니다.

참고 TACACS+ 특성을 사용하려면 NAS에서 AAA 서비스를 활성화해야 합니다.

다음 표는 컷스루 프록시 연결을 위해 지원되는 TACACS+ 권한 부여 응답 특성을 나열합니다.

표 ***42:*** 지원되는 ***TACACS+*** 권한 부여 응답 특성

속성	설명
acl	연결에 적용할 로컬 구성된 ACL을 식별합니다.
idletime	비활성 상태가 얼마나 지속되면 인증된 사용자 세션을 종료할지 분 단위로 나타냅니다.

속성	설명
timeout	인증된 사용자 세션을 종료하기 전에 인증 자격 증명을 활성 상태로 유지할 절대 시간(분)을 지정합니다.

다음 표는 지원되는 TACACS+ 어카운팅 특성을 나열합니다.

.

표 ***43:*** 지원되는 ***TACACS+*** 어카운팅 특성

속성	설명
bytes_in	이 연결 중에 전송된 입력 바이트의 수를 지정합니다(중단 레코드만 해당).
bytes_out	이 연결 중에 전송된 출력 바이트의 수를 지정합니다(중단 레코드만 해당).
cmd	실행되는 명령을 정의합니다(명령 어카운팅만 해당).
disc-cause	연결이 끊긴 원인을 식별하는 숫자 코드를 나타냅니다(중단 레코드만 해당).
elapsed_time	연결에서 경과한 시간을 초 단위로 정의합니다(중단 레코드만 해당).
foreign_ip	터널 연결을 위한 클라이언트의 IP 주소를 지정합니다. cut-through-proxy 연결을 위한 가장 낮은 수준의 보안 인터페이스 주소를 정의합니다.
local_ip	클라이언트가 터널 연결을 위해 연결된 IP 주소를 지정합니다. cut-through-proxy 연결을 위한 가장 높은 수준의 보안 인터페이스 주소를 정의합니다.
NAS port	해당 연결을 위한 세션 ID를 포함합니다.
packs_in	이 연결 중에 전송되는 입력 패킷의 수를 지정합니다.
packs_out	이 연결 중에 전송되는 입력 패킷의 수를 지정합니다.
priv-level	명령 어카운팅 요청에 대한 사용자 권한 수준으로 설정합니다. 그렇지 않으면 1로 설정합니다.
rem_iddr	클라이언트의 IP 주소를 나타냅니다.

속성	설명
service	사용하는 서비스를 지정합니다. 명령 어카운팅에 한해 항상 “shell”로 설정합니다.
task_id	어카운팅 거래에 대한 고유한 작업 ID를 지정합니다.
username	사용자의 이름을 나타냅니다.

AAA를 위한 TACACS+ 서버에 대한 지침

이 섹션에서는 AAA를 위한 TACACS+ 서버를 구성하기 전에 확인해야 하는 제한 사항 및 지침에 대해 설명합니다.

IPv6

AAA 서버는 IPv4 또는 IPv6 주소를 사용할 수 있습니다.

추가 지침

- 단일 모드로 최대 100개의 서버 그룹 또는 다중 모드로 상황당 4개의 서버 그룹을 포함할 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다.

TACACS+ 서버 구성

이 섹션에서는 TACACS+ 서버 구성 방법에 대해 설명합니다.

프로시저

단계 **1** TACACS+ 서버 그룹 구성, 1087 페이지.
단계 **2** 그룹에 TACACS+ 서버 추가, 1089 페이지.

TACACS+ 서버 그룹 구성

인증, 권한 부여 또는 어카운팅을 위해 TACACS+ 서버를 사용하려면 먼저 1개 이상의 TACACS+ 서버 그룹을 생성하고 각 그룹에 하나 이상의 서버를 추가해야 합니다. TACACS+ 서버 그룹은 이름으로 구분합니다.

TACACS+ 서버 그룹을 추가하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 서버 그룹 이름과 프로토콜을 식별합니다.

aaa-server *server_tag* **protocol tacacs+**

예제:

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

aaa-server protocol 명령을 입력하면 aaa-server 그룹 구성 모드로 들어갑니다.

단계 **2** 다음 서버를 시도하기 전에 그룹의 AAA 서버로 보낼 수 있는 최대 요청 횟수를 지정합니다.

max-failed-attempts *number*

예제:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 인수의 범위는 1부터 5까지입니다. 기본값은 3입니다.

로컬 데이터베이스를 사용하여 장애 조치 방법을 구성한 경우(관리 액세스에만 해당) 그룹의 모든 서버가 응답하지 않으면 그룹이 응답하지 않는 것으로 간주되고 장애 조치 방법이 시도됩니다. 서버 그룹은 10분(기본값) 동안 무응답으로 표시됩니다. 그러면 이 기간에 다른 AAA 요청에서 서버 그룹 접속을 시도하지 않으며 즉시 대비책이 사용됩니다. 무응답 기간을 기본값이 아닌 값으로 변경하려면 다음 단계의 **reactivation-mode** 명령을 참조하십시오.

대비책이 없는 경우 ASA는 그룹의 서버를 계속 재시도합니다.

단계 **3** 그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

예제:

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 키워드는 그룹의 모든 서버가 비활성 상태가 되어야 실패한 서버를 재활성화합니다.

deadtime *minutes* 키워드-인수 쌍은 그룹의 마지막 서버를 비활성화한 시점부터 이후에 모든 서버를 다시 활성화한 시점까지 경과하는 시간(분)을 0~1440 범위에서 지정합니다. 기본은 10분입니다.

timed 키워드는 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.

단계 **4** 그룹의 모든 서버에 어카운팅 메시지를 전송합니다.

accounting-mode simultaneous

예제:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

활성 서버에만 메시지 전송의 기본값을 복원하려면 **accounting-mode single** 명령을 입력합니다.

예

다음 예는 기본 서버와 백업 서버를 하나씩 포함한 TACACS+ 그룹을 1개 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

그룹에 **TACACS+** 서버 추가

그룹에 RADIUS 서버를 추가하려면 다음 단계를 수행합니다.

프로시저

단계 **1** TACACS+ 서버와 해당 서버가 속한 서버 그룹을 식별합니다.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

예제**:**

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)**을 지정하지 않는 경우, ASA는 기본적으로 **inside**interface을 사용합니다.

서버는 IPv4 또는 IPv6 주소를 사용할 수 있습니다.

단계 **2** ASA가 백업 서버에 요청을 보내기 전에 기본 서버에서 응답을 기다리는 시간을 초 단위로 지정합니다.

timeout *hh:mm:ss*

예제**:**

```
ciscoasa(config-aaa-server-host)# timeout 15
```

단계 **3** 서버 포트를 포트 번호 49로 지정하거나 ASA에서 TACACS+ 서버와 통신에 사용하는 TCP 포트 번호로 지정합니다.

server-port *port_number*

예제**:**

```
ciscoasa(config-aaa-server-host)# server-port 49
```

단계 **4** TACACS+ 서버에서 NAS를 인증하는 데 사용하는 서버 비밀 값을 지정합니다.

key

예제**:**

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

이 값은 대/소문자를 구별하는 최대 127자의 영숫자 키워드로 TACACS+ 서버의 키와 같은 값입니다. 127자를 넘는 문자는 무시됩니다. 키는 클라이언트와 서버 사이에서 데이터 암호화에 사용되며 클라이언트와 서버 시스템에서 동일해야 합니다. 키는 공백을 포함할 수 없지만 다른 특수 문자는 허용됩니다.

AAA를 위한 TACACS+ 서버 모니터링

AAA를 위한 TACACS+ 서버 모니터링에 대해서는 다음 명령을 참고하십시오.

- **show aaa-server**

  이 명령은 구성된 TACACS+ 서버 통계를 보여 줍니다. TACACS+ 서버 통계를 지우려면 **clear aaa-server statistics** 명령을 입력합니다.

- **show running-config aaa-server**

  이 명령은 구성을 실행 중인 TACACS+ 서버를 보여 줍니다. TACACS+ 서버 구성을 지우려면 **clear configure aaa-server** 명령을 입력합니다.

AAA를 위한 TACACS+ 서버 내역

표 *44: AAA*를 위한 *TACACS+* 서버 내역

기능 이름	플랫폼 릴리스	설명
TACACS+ 서버	7.0(1)	AAA에 대한 TACACS+ 서버를 구성하는 방법을 설명합니다. 다음 명령을 도입했습니다. **aaa-server protocol**, **max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, aaa authorization exec authentication-server**, **server-port, key**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **username**, **service-type**, **timeout**.
AAA를 위해 IPv6 주소를 사용하는 TACACS+ 서버	9.7(1)	이제 AAA 서버에 IPv4 또는 IPv6 주소를 사용할 수 있습니다.

36 장

AAA를 위한 LDAP 서버

이 장에서는 AAA에서 사용되는 LDAP 서버의 구성 방법을 설명합니다.

LDAP과 ASA 소개

Cisco ASA는 다음을 포함하여 대부분의 LDAPv3 디렉터리 서버와 호환됩니다.

- Sun Microsystems JAVA System Directory Server - 현재는 Oracle Directory Server Enterprise Edition에 포함됨. 이전 이름은 Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

기본적으로 ASA는 Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP 또는 일반 LDAPv3 디렉터리 서버와의 연결 여부를 자동으로 탐지합니다. 그러나 자동 감지 기능에서 LDAP 서버 유형을 확인하지 못한 경우 수동으로 구성할 수 있습니다.

인증이 LDAP에서 작동하는 방식

ASA는 인증 과정에서 해당 사용자의 LDAP 서버에 대한 클라이언트 프록시 역할을 하며, 일반 텍스트 또는 SASL 프로토콜을 사용하여 LDAP 서버를 인증합니다. 기본적으로 ASA는 인증 파라미터(대개 사용자 이름과 비밀번호)를 일반 텍스트 형식으로 LDAP 서버에 전달합니다.

ASA는 강도가 낮은 순서로 나열되어 있는 다음 SASL 메커니즘을 지원합니다.

- Digest-MD5 — ASA는 사용자 이름과 비밀번호로 계산한 MD5 값을 사용하여 LDAP 서버에 응답합니다.

- Kerberos — ASA는 GSSAPI Kerberos 메커니즘을 사용하여 사용자 이름과 영역을 보내는 방법으로 LDAP 서버에 응답합니다.

ASA와 LDAP 서버는 이러한 SASL 메커니즘이 결합된 방식을 지원합니다. 여러 메커니즘을 구성한 경우, ASA는 해당 서버에 구성된 SASL 메커니즘의 목록을 검색하고 ASA와 서버에 모두 구성되어 있는 가장 강력한 방식으로 인증 메커니즘을 설정합니다. 예를 들어, LDAP 서버와 ASA 모두 두 메커니즘을 지원할 경우 ASA는 둘 중 더 강력한 Kerberos를 선택합니다.

사용자 인증이 성공했으면 LDAP 서버는 인증된 사용자의 특성을 반환합니다. VPN 인증의 경우, 일반적으로 이 특성에는 VPN 세션에 적용된 권한 부여 데이터가 포함됩니다. 이러한 경우 LDAP를 사용하면 단일 단계에서 인증과 권한 부여가 이루어집니다.

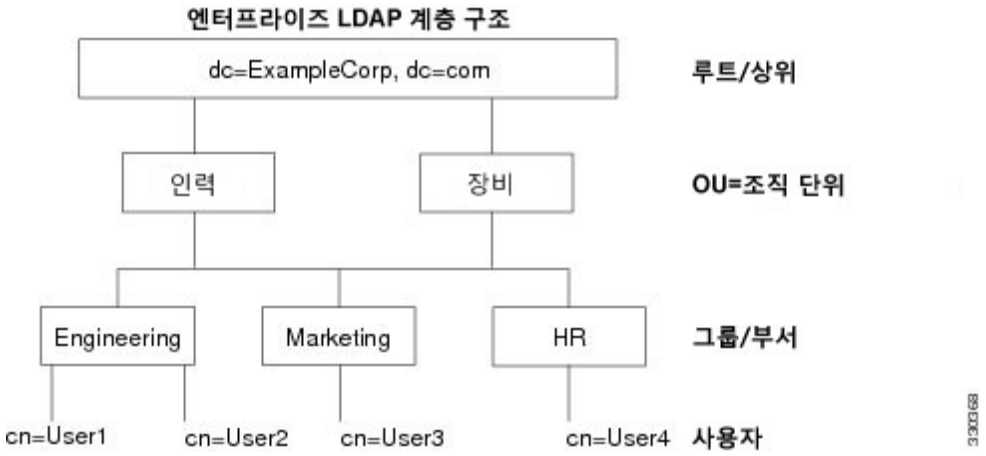
참고 LDAP 프로토콜에 대한 자세한 내용은 RFC 1777, 2251, 2849를 참조하십시오.

LDAP 계층 구조

LDAP 컨피그레이션은 조직의 논리적 계층 구조를 반영해야 합니다. Example Corporation이라는 회사에 Employee1이라는 직원이 있다고 가정합니다. Employee1은 Engineering 그룹에서 일합니다. LDAP 계층 구조는 단일 단계 또는 여러 단계를 포함할 수 있습니다. 단일 단계 계층 구조로 설정할 경우 Employee1은 Example Corporation의 멤버로 간주됩니다. 또는 다단계 계층 구조로 설정할 수 있는데, 그러면 Employee1은 Engineering 부서의 멤버이고 이 부서는 People이라는 조직 단위의 멤버이며, People은 Example Corporation의 멤버입니다. 다단계 계층 구조의 예는 다음 그림을 참조하십시오.

다단계 계층 구조가 더 상세한 내용을 포함하지만, 검색 결과는 단일 단계 계층 구조에서 더 빨리 얻을 수 있습니다.

그림 *66:* 다단계 ***LDAP*** 계층 구조



LDAP 계층 구조 검색

ASA에서는 LDAP 계층 구조 내 검색을 맞춤 구성할 수 있습니다. ASA의 다음 3개 필드를 구성하여 LDAP 계층 구조에서 검색을 시작할 위치, 범위, 찾으려는 정보 유형을 정의합니다. 이 필드가 종합적으로 작용하여 사용자 권한을 포함하는 부분으로만 계층 구조 검색을 한정합니다.

- LDAP Base DN(LDAP 기본 DN)은 서버가 ASA로부터 권한 부여 요청을 받았을 때 LDAP 계층 구조의 어디에서 사용자 정보 검색을 시작할 것인가를 정의합니다.
- Search Scope(검색 범위)는 LDAP 계층 구조에서 검색의 범위를 정의합니다. 검색에서는 계층 구조상 LDAP 기본 DN 아래의 여러 단계에서 이 작업을 진행합니다. 서버가 바로 아래 단계만 검색하게 하거나, 전체 하위 트리를 검색할 수도 있습니다. 단일 레벨 검색이 더 빠르지만, 하위 트리 검색은 더 광범위합니다.
- Naming Attribute(s)(명명 특성)는 LDAP 서버의 항목을 고유하게 식별하는 RDN을 정의합니다. cn(Common Name), sAMAccountName, userPrincipalName과 같은 명명 특성이 주로 사용됩니다.

다음 그림에서는 Example Corporation의 샘플 LDAP 계층 구조를 보여줍니다. 이 계층 구조에서 여러 가지 방법으로 검색을 정의할 수 있습니다. 다음 표에서는 2개의 샘플 검색 컨피그레이션을 보여줍니다.

첫 번째 구성 예에서는 Employee1이 LDAP 권한 부여가 필요한 IPsec 터널을 설정하자 ASA에서는 LDAP 서버에 검색 요청을 보내면서 Engineering 그룹에서 Employee1을 찾도록 지시합니다. 이 검색은 빠르게 수행됩니다.

두 번째 구성 예에서는 ASA가 검색 요청을 보내면서 서버가 Example Corporation 내에서 Employee1을 검색하도록 지시합니다. 이 검색은 더 오래 걸립니다.

표 ***45:*** 검색 컨피그레이션의 예

번호	**LDAP** 기본 **DN**	검색 범위	명명 특성	결과
1	group=Engineering,ou=People,dc=ExampleCorporation,dc=com	단일 레벨	cn=Employee1	더 빠른 검색
2	dc=ExampleCorporation,dc=com	하위 트리	cn=Employee1	더 오래 걸리는 검색

LDAP 서버에 바인딩

ASA에서는 로그인 DN과 로그인 비밀번호를 사용하여 LDAP 서버와의 신뢰(바인딩)를 설정합니다. Microsoft Active Directory 읽기 전용 작업(예: 인증, 권한 부여, 그룹 검색)을 수행할 때 ASA는 더 적은 권한을 가진 로그인 DN을 사용하여 바인딩할 수 있습니다. 이를테면 로그인 DN은 AD "Member Of" 지정이 Domain Users의 일부인 사용자일 수 있습니다. VPN 비밀번호 관리 작업의 경우 로그인 DN은 상승된 권한이 필요하며 Account Operators AD 그룹의 일원이어야 합니다.

다음은 로그인 DN의 예입니다.

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA에서는 다음 인증 방식을 지원합니다.

- 포트 389에서 암호화되지 않은 비밀번호를 사용하는 단순 LDAP 인증
- 포트 636의 LDAP-S(Secure LDAP)
- SASL(Simple Authentication and Security Layer) MD5
- SASL Kerberos

ASA에서는 익명 인증을 지원하지 않습니다.

참고 LDAP 클라이언트인 ASA는 익명 바인딩 또는 요청의 전송을 지원하지 않습니다.

LDAP 특성 맵

ASA에서는 사용자 인증을 위해 LDAP 디렉터리를 사용할 수 있습니다.

- VPN 원격 액세스 사용자
- 방화벽 네트워크 액세스/컷스루 프록시 세션
- 정책 권한(권한 부여 특성이라고도 함) 설정(예: ACL, 북마크 목록, DNS 또는 WINS 설정, 세션 타이머)
- 로컬 그룹 정책의 키 특성 설정

ASA에서는 기본 LDAP 사용자 속성을 Cisco ASA 속성으로 변환하는 데 LDAP 속성 맵을 사용합니다. 이 특성 맵을 LDAP 서버에 바인딩하거나 삭제할 수 있습니다. 특성 맵을 표시하거나 지울 수도 있습니다.

LDAP 특성 맵은 다중값 특성을 지원하지 않습니다. 예를 들어, 사용자가 여러 AD 그룹의 멤버이고 LDAP 특성 맵이 둘 이상의 그룹에 매칭할 경우, 매칭된 항목의 알파벳순에 따라 값이 선택됩니다.

특성 매핑 기능을 올바르게 사용하려면 LDAP 특성의 이름 및 값 그리고 사용자 정의 특성의 이름 및 값까지 알고 있어야 합니다.

자주 매핑되는 LDAP 특성의 이름 및 일반적으로 이 특성이 매핑되는 사용자 정의 특성의 유형에는 다음이 포함됩니다.

- IETF-Radius-Class(ASA 버전 8.2 이상의 Group_Policy) — 디렉터리 부서 또는 사용자 그룹(예: Microsoft Active Directory memberOf) 속성 값을 기반으로 그룹 정책을 설정합니다. 이 그룹 정책 특성은 IETF-Radius-Class 특성을 ASDM 버전 6.2/ASA 버전 8.2 이상으로 대체합니다.
- IETF-Radius-Filter-Id—액세스 제어 목록, 즉 ACL을 VPN 클라이언트, IPsec, SSL에 적용합니다.

- IETF-Radius-Framed-IP-Address—VPN 원격 액세스 클라이언트, IPsec, SSL에 할당되는 정적 IP 주소를 지정합니다.
- Banner1—VPN 원격 액세스 사용자가 로그인할 때 문자 배너를 표시합니다.
- Tunneling-Protocols—액세스 유형에 따라 VPN 원격 액세스 세션을 허용하거나 거부합니다.

참고 단일 LDAP 특성 맵은 하나 이상의 특성을 포함할 수 있습니다. 특정 LDAP 서버에서 하나의 LDAP 특성만 매핑할 수 있습니다.

AAA를 위한 LDAP 서버를 위한 지침

이 섹션에서는 AAA를 위한 LDAP 서버를 구성하기 전에 확인해야 하는 지침 및 제한 사항을 설명합니다.

IPv6

AAA 서버는 IPv4 또는 IPv6 주소를 사용할 수 있습니다.

추가 지침

- Sun 디렉터리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉터리 관리자 또는 디렉터리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACL을 배치할 수 있습니다.
- Microsoft Active Directory 및 Sun 서버로 비밀번호를 관리할 수 있도록 SSL을 통한 LDAP를 구성해야 합니다.
- ASA에서는 Novell, OpenLDAP, 기타 LDAPv3 디렉터리 서버를 사용한 비밀번호 관리를 지원하지 않습니다.
- 버전 7.1(x)부터 ASA는 기본 LDAP 스키마를 사용하여 인증 및 권한 부여를 수행하므로 Cisco 스키마가 더 이상 필요하지 않습니다.
- 단일 모드에서는 최대 100개의 LDAP 서버 그룹을, 다중 모드에서는 컨텍스트당 4개의 LDAP 서버 그룹을 가질 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 LDAP 서버를, 다중 모드에서는 4개의 LDAP 서버를 가질 수 있습니다.
- 사용자가 로그인하면, 컨피그레이션에서 지정한 첫 번째 LDAP 서버부터 시작하여 서버가 응답할 때까지 한 번에 하나씩 서버에 액세스합니다. 그룹의 모든 서버를 사용할 수 없는 경우, 로컬 데이터베이스가 폴백 방법(관리 인증 및 권한 부여만 해당)으로 구성되어 있으면 ASA에서는 로컬 데이터베이스를 사용하려고 시도합니다. 폴백 방법이 없는 경우, ASA에서는 LDAP 서버를 사용하기 위한 시도를 계속합니다.

AAA를 위한 LDAP 서버 구성

이 섹션에서는 AAA를 위한 LDAP 서버를 구성하는 방법을 설명합니다.

프로시저

단계 1 LDAP 특성 맵을 구성합니다. LDAP 특성 맵 구성, 1098 페이지을 참조하십시오.

단계 2 LDAP 서버 그룹을 추가합니다. LDAP 서버 그룹 구성, 1100 페이지을 참조하십시오.

단계 3 (선택 사항) 인증 메커니즘과는 별개인 LDAP 서버의 권한 부여를 구성합니다. VPN을 위해 LDAP를 사용하는 권한 부여 구성, 1102 페이지를 참조하십시오.

LDAP 특성 맵 구성

LDAP 특성 맵을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 1 채워지지 않은 LDAP 특성 맵 테이블을 만듭니다.

ldap-attribute-map *map-name*

예제:

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

단계 2 사용자 정의 특성 이름 부서를 Cisco 특성에 매핑합니다.

map-name *user-attribute-name Cisco-attribute-name*

예제:

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

단계 3 사용자 정의 맵 값 부서를 사용자 정의 특성 값 및 Cisco 특성 값에 매핑합니다.

map-value *user-attribute-name Cisco-attribute-name*

예제:

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

단계 4 서버 및 그 서버가 속한 AAA 서버 그룹을 식별합니다.

aaa-server *server_group* [*interface_name*] **host** *server_ip*

예제:

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

단계 **5** 특성 맵을 LDAP 서버에 바인딩합니다.

ldap-attribute-map *map-name*

예제:

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

예

다음 예에서는 accessType이라는 LDAP 속성을 기반으로 ASA에 대한 관리 세션을 제한하는 방법을 보여 줍니다. accessType 특성은 다음 값 중 하나를 가질 수 있습니다.

- VPN
- admin
- helpdesk

다음 예에서는 각 값이 ASA에서 지원하는 유효한 IETF-Radius-Service-Type 속성, 즉 remote-access(Service-Type 5) Outbound, admin(Service-Type 6) Administrative, nas-prompt(Service-Type 7) NAS Prompt 중 하나에 매핑되는 방법을 보여 줍니다.

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

다음 예에서는 Cisco LDAP 특성 이름의 전체 목록을 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
```

```
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

LDAP 서버 그룹 구성

LDAP 서버 그룹을 생성하고 구성한 다음 LDAP 서버를 추가하려면 다음 단계를 수행합니다.

시작하기 전에

LDAP 서버 그룹에 LDAP 서버를 추가하기 전에 특성 맵을 추가해야 합니다.

프로시저

단계 **1** 서버 그룹 이름과 프로토콜을 식별합니다.

aaa-server *server_tag* **protocol ldap**

예제**:**

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol 명령을 입력하면 aaa-server 그룹 구성 모드를 시작합니다.

단계 **2** 그룹의 어떤 LDAP 서버에 최대 몇 번의 요청을 보낸 후 다음 서버를 시도할지 지정합니다.

max-failed-attempts *number*

예제**:**

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 인수의 범위는 1부터 5까지입니다. 기본값은 3입니다.

로컬 데이터베이스를 사용하여 폴백 방법을 구성하여 폴백 매커니즘을 구성한 경우(관리 액세스만 해당) 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 폴백 방법이 시도됩니다. 서버 그룹은 10분(기본값) 동안 무응답으로 표시됩니다. 그러면 이 기간에 다른 AAA 요청에서 서버 그룹 접속을 시도하지 않으며 즉시 대비책이 사용됩니다. 무응답 기간을 기본값이 아닌 값으로 변경하려면 다음 단계의 **reactivation-mode** 명령을 참조하십시오.

대비책이 없는 경우 ASA는 그룹의 서버를 계속 재시도합니다.

단계 **3** 그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

예제:

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 키워드는 그룹의 모든 서버가 비활성 상태가 되어야 실패한 서버를 재활성화합니다.

deadtime *minutes* 키워드-인수 쌍은 그룹의 마지막 서버를 비활성화한 시점부터 나중에 모든 서버를 다시 활성화한 시점까지 경과한 시간(분)을 0~1440 범위에서 지정합니다. 기본은 10분입니다.

timed 키워드는 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.

단계 **4** LDAP 서버 및 그 서버가 속한 AAA 서버 그룹을 지정합니다.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

예제:

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)**을 지정하지 않는 경우, ASA는 기본적으로 **inside**interface을 사용합니다.

aaa-server host 명령을 입력하면 aaa-server 호스트 구성 모드로 들어갑니다. 필요하다면 호스트 컨피그레이션 모드 명령을 사용하여 AAA 서버를 추가 구성합니다.

다음 표에서는 LDAP 서버를 위해 사용 가능한 명령 및 그 명령에 대해 새로운 LDAP 서버 정의가 기본값을 갖는지 보여줍니다. 기본값이 제공되지 않은 경우("—"로 표시) 명령을 사용하여 값을 지정합니다.

표 ***46:*** 호스트 모드 명령 및 기본값

명령	기본값	설명
ldap-attribute-map	—	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	설정되지 않은 경우 ASA에서는 LDAP 요청에 sAMAccountName을 사용합니다. SASL 또는 일반 텍스트를 사용하더라도 ASA와 LDAP 서버 간의 통신을 SSL로 보호할 수 있습니다. SASL을 구성하지 않은 경우 LDAP 통신을 SSL로 보호하는 것이 좋습니다.
ldap-scope	—	—

명령	기본값	설명
sasl-mechanism	—	—
server-port	389	—
server-type	autodiscovery	자동 감지에서 LDAP 서버 유형을 확인하지 못한 경우, 그 서버가 Microsoft, Sun 또는 일반 LDAP 서버인지 알고 있다면 직접 서버 유형을 구성할 수 있습니다.
timeout	10초	—

예

다음 예에서는 watchdog이라는 LDAP 서버 그룹을 구성하고 그 그룹에 LDAP 서버를 추가하는 방법을 보여줍니다. 이 예에서는 재시도 간격 또는 LDAP 서버가 수신하는 포트를 정의하지 않으므로 ASA는 이 두 서버별 파라미터에 기본값을 사용합니다.

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

VPN을 위해 LDAP를 사용하는 권한 부여 구성

VPN 액세스를 위한 사용자 LDAP 인증이 성공하면 ASA는 LDAP 서버를 쿼리하여 LDAP 속성을 받습니다. 대개 이 특성에는 VPN 세션에 적용되는 권한 부여 데이터가 들어 있습니다. 이와 같이 LDAP를 사용하면 단일 단계에서 인증과 권한 부여가 이루어집니다.

그러나 인증 메커니즘과 별개인 LDAP 디렉터리 서버의 권한 부여가 필요할 때가 있습니다. 예를 들어 인증에 SDI 또는 인증서 서버를 사용하는 경우 어떤 권한 부여 정보도 반환되지 않습니다. 이러한 사용자 권한 부여의 경우 인증에 성공한 후 LDAP 디렉토리를 조회하면 인증 및 권한 부여를 두 단계로 완료할 수 있습니다.

LDAP을 사용하여 VPN 사용자 권한 인증을 설정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 이름이 remotegrp인 IPsec 원격 액세스 터널 그룹을 생성합니다.

tunnel-group *groupname*

예제**:**

```
ciscoasa(config)# tunnel-group remotegrp
```

단계 **2** 서버 그룹과 터널 그룹을 연결합니다.

tunnel-group *groupname* **general-attributes**

예제**:**

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

단계 **3** 권한 부여를 위해 앞서 생성한 AAA 서버 그룹에 새 터널 그룹을 지정합니다.

authorization-server-group *group-tag*

예제**:**

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

예

특정 요구 사항을 위한 다른 권한 부여 관련 명령과 옵션도 있지만, 다음 예에서는 LDAP를 통한 사용자 권한 부여를 활성화하는 명령을 보여줍니다. 그런 다음 remote-1이라는 IPsec 원격 액세스 터널 그룹을 만들고, 권한 부여를 위해 앞서 만든 ldap_dir_1 AAA 서버 그룹에 새 터널 그룹을 지정합니다.

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

이 구성 작업을 완료했으면 다음 명령을 사용하여 디렉터리 비밀번호, 디렉터리 검색의 시작점, 디렉터리 검색의 범위와 같은 추가 LDAP 권한 부여 매개변수를 구성할 수 있습니다.

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

AAA를 위한 LDAP 서버 모니터링

AAA를 위한 LDAP 서버를 모니터링하려면 다음 명령을 참고하십시오.

- **show aaa-server**

이 명령은 구성된 LDAP 서버의 통계를 표시합니다. AAA 서버 구성을 지우려면 **clear aaa-server statistics** 명령을 사용합니다.

- **show running-config aaa-server**

  이 명령은 AAA 서버에서 실행 중인 컨피그레이션을 표시합니다. AAA 서버 통계를 지우려면 **clear configure aaa-server** 명령을 사용합니다.

AAA를 위한 LDAP 서버 기록

표 ***47: AAA*** 서버 기록

기능 이름	플랫폼 릴리스	설명
AAA를 위한 LDAP 서버	7.0(1)	LDAP 서버에서 AAA 지원과 LDAP 서버 구성 방법에 대해 설명합니다. 다음 명령을 도입했습니다. **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, ldap attribute-map**, **aaa-server protocol**, **aaa authentication telnet | ssh | serial} console LOCAL**, **aaa authentication http consoleLOCAL**, **aaa authentication enable console LOCAL**, **max-failed-attempts**, **reactivation-mode**, **accounting-mode simultaneous**, **aaa-server host**, **authorization-server-group**, **tunnel-group**, **tunnel-group general-attributes**, **map-name**, **map-value**, **ldap-attribute-map**
AAA를 위한 IPv6 주소를 사용하는 LDAP 서버	9.7(1)	이제 AAA 서버에 IPv4 또는 IPv6 주소를 사용할 수 있습니다.

VII 부

시스템 관리

37 장

관리 액세스

이 장에서는 텔넷, SSH, HTTPS(ASDM 사용)를 통한 시스템 관리를 위해 Cisco ASA에 액세스하는 방법, 사용자를 인증하고 사용자에게 권한을 부여하는 방법, 로그인 배너를 만드는 방법을 설명합니다.

관리 원격 액세스 구성

이 섹션에서는 ASDM, 텔넷 또는 SSH 및 로그인 배너와 같은 기타 관리 파라미터를 위한 ASA 액세스를 구성하는 방법을 설명합니다.

SSH 액세스 구성

클라이언트 IP 주소를 확인하고 SSH를 사용하여 ASA에 연결할 수 있는 사용자를 정의하려면 다음 단계를 수행합니다. 다음 지침을 참조하십시오.

- SSH 액세스를 위해 ASA 인터페이스에 액세스할 때 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 SSH 액세스를 구성하면 됩니다.
- ASA를 시작할 때 사용한 것과 다른 인터페이스에 대한 SSH 액세스는 지원되지 않습니다. 예를 들어, SSH 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다. 이 규칙의 유일한 예외는 VPN 연결을 거치는 경우입니다. VPN 터널을 통한 관리 액세스 구성, 1118 페이지을 참조하십시오.
- ASA에서는 상황/단일 모드당 최대 5개의 동시 SSH 연결이 가능하며 모든 상황에서 최대 100개의 연결 할당이 가능합니다.
- (8.4 이상) SSH 기본 사용자 이름은 더 이상 지원하지 않습니다. 이제는 **pix** 또는 **asa** 사용자 이름 및 로그인 비밀번호를 사용하여 SSH를 통해 ASA에 연결할 수 없습니다. SSH를 사용하려면 **aaa authentication ssh console LOCAL** 명령을 사용하여 AAA 인증을 구성한 다음 **username** 명령을

입력하여 로컬 사용자를 정의해야 합니다. 로컬 데이터베이스 대신에 AAA 서버를 인증에 사용하려는 경우, 만일에 대비하여 로컬 인증도 구성하는 것이 좋습니다.

시작하기 전에

- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context** *name*을 입력합니다.

프로시저

단계 **1** SSH에 필요한 RSA 키 쌍을 생성합니다(물리적인 ASA만 해당).

crypto key generate rsa modulus *modulus_size*

예제**:**

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

ASAv에서는 구축 후 자동으로 RSA 키 쌍이 생성됩니다.

모듈러스 값(비트)은 512, 768, 1024, 2048, 3072 또는 4096입니다. 지정하는 키 모듈러스 크기가 클수록 RSA 키 쌍을 생성하는 데 오래 걸립니다. 권장되는 값은 최소 2048입니다.

단계 **2** 지속형 플래시 메모리에 RSA 키를 저장합니다.

write memory

예제**:**

```
ciscoasa(config)# write memory
```

단계 **3** SSH 액세스에 사용할 수 있는 사용자를 로컬 데이터베이스에 만듭니다. 또는 사용자 액세스를 위해 AAA 서버를 사용할 수 있지만 로컬 사용자 이름을 사용하는 것이 좋습니다.

username *name* [**password** *password*] **privilege** *level*

예제**:**

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

기본적으로 권한 레벨은 2입니다. 0~15 사이의 레벨을 입력합니다. 이때 15는 모든 권한을 갖습니다. 사용자가 비밀번호 인증 대신 공개 키 인증**(ssh authentication)**을 강제로 사용하도록 하려는 경우, 비밀번호가 없는 사용자를 생성할 수 있습니다. **username** 명령에서 비밀번호 뿐만 아니라 공개 키 인증을 구성하는 경우, 이 절차에서 AAA 인증을 명시적으로 구성하는 경우 사용자는 두 가지 방법 중 하나로 로그인할 수 있습니다. 참고**: username** 명령 **nopassword** 옵션을 사용하지 마십시오. **nopassword** 옵션을 사용하면 비밀번호가 아니라 모든 비밀번호를 입력할 수 있습니다.

단계 **4** (선택 사항) 비밀번호 인증 대신/뿐만 아니라 사용자에 대한 공개 키 인증을 허용하려면 ASA에서 공개 키를 입력합니다.

username *name* **attributes**

ssh authentication {**pkf** | **publickey** *key*}

예제**:**

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

로컬 **username**의 경우, 비밀번호 인증 대신/뿐만 아니라 공개 키 인증을 활성화할 수 있습니다. SSH-RSA 원시 키(즉, 인증서가 없음)를 생성할 수 있는 SSH 키 생성 소프트웨어(예: ssh keygen)를 사용하여 공개 키/개인 키 쌍을 생성할 수 있습니다. ASA에서 공개 키를 입력합니다. 그런 다음 SSH 클라이언트는 개인 키(및 키 쌍을 생성하는 데 사용한 패스프레이즈)를 사용하여 ASA에 연결합니다.

pkf 키의 경우 PKF 형식의 키에 붙여넣으라는 메시지가 표시됩니다(최대 4096비트). 너무 커서 Base64 형식으로 인라인으로 붙여넣을 수 없는 키에 이 형식을 사용합니다. 예를 들어 ssh keygen을 사용하여 4096비트 키를 생성하여 PKF로 변환한 다음 **pkf** 키워드를 사용하여 해당 키에 대한 메시지를 표시할 수 있습니다. 참고**:** 페일오버가 있는 **pkf** 옵션을 사용할 수 있지만 PKF 키가 스탠바이 시스템에 자동으로 복제되지는 않습니다. **write standby** 명령을 입력하여 PKF 키를 동기화해야 합니다.

publickey *key*의 경우 키는 Base64 인코딩 공개 키입니다. SSH-RSA 원시 키(즉, 인증서가 없음)를 생성할 수 있는 SSH 키 생성 소프트웨어(예: ssh keygen)를 사용하여 키를 생성할 수 있습니다.

단계 **5** (비밀번호 액세스용) SSH 액세스를 위해 로컬(또는 AAA 서버) 인증을 활성화합니다.

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

예제**:**

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

이 명령은 **ssh authentication** 명령을 사용하는 사용자 이름에 대한 로컬 공개 키 인증에 영향을 미치지 않습니다. ASA는 암시적으로 공개 키 인증을 위해 로컬 데이터베이스를 사용합니다. 이 명령은 비밀번호가 있는 사용자 이름에만 영향을 미칩니다. 공개 키 인증 또는 비밀번호를 로컬 사용자가 사용하도록 허용하려는 경우, 비밀번호 액세스를 허용하도록 이 명령을 사용하여 로컬 인증을 명시적으로 구성해야 합니다.

단계 **6** ASA가 각 주소 또는 서브넷에 대한 연결을 수락하는 IP 주소와 SSH를 사용할 수 있는 인터페이스를 식별합니다.

ssh *source_IP_address mask source_interface*

- *source_interface* — 이름이 있는 인터페이스를 지정합니다. 브리지 그룹의 경우, 브리지 그룹 멤버 인터페이스를 지정합니다.VPN 관리 액세스의 경우에만(VPN 터널을 통한 관리 액세스 구성, 1118 페이지 참조), 명명된 BVI 인터페이스를 지정합니다.

텔넷과 달리 SSH는 가장 낮은 보안 수준 인터페이스에서 가능합니다.

예제:

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

단계 **7** (선택 사항) ASA에서 세션 연결을 끊기 전에 얼마 동안 SSH 세션을 유휴 상태로 유지할 수 있는지 설정합니다.

ssh timeout *minutes*

예제:

```
ciscoasa(config)# ssh timeout 30
```

1분~60분 범위에서 시간 제한을 설정합니다. 기본값은 5분입니다. 이 기본값은 대개 너무 짧으므로 모든 프로덕션 전 단계 테스트 및 문제 해결을 완료할 수 있도록 늘려야 합니다.

단계 **8** (선택 사항) SSH 버전 1 또는 2로 액세스를 제한합니다. 기본적으로 SSH는 버전 1과 2 모두 허용합니다.

ssh version *version_number*

예제:

```
ciscoasa(config)# ssh version 2
```

단계 **9** (선택 사항) SSH 암호 암호화 알고리즘을 구성합니다.

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_encryption_ciphers*}

예제:

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

기본값은 **medium**입니다.

- **all** 키워드는 모든 암호를 사용하도록 지정합니다. 예: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **custom** 키워드는 콜론으로 구분된 맞춤형 암호 암호화 구성 문자열을 지정합니다.
- **fips** 키워드는 FIPS 호환 암호만 지정합니다. 예: aes128-cbc aes256-cbc

- **high** 키워드는 보안 수준이 높은 암호만 지정합니다. 예: aes256-cbc aes256-ctr
- **low** 키워드는 보안 수준이 낮은 암호, 보통인 암호, 높은 암호를 지정합니다. 예: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **medium** 키워드는 보안 수준이 보통인 암호 및 높은 암호(기본값)를 지정합니다. 예: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

단계 **10** (선택 사항) SSH 암호 무결성 알고리즘을 구성합니다.

ssh cipher integrity {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_integrity_ciphers*}

예제**:**

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

기본값은 **medium**입니다.

- **all** 키워드는 모든 암호를 사용하도록 지정합니다. 예: hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
- **custom** 키워드는 콜론으로 구분된 맞춤형 암호 암호화 구성 문자열을 지정합니다.
- **fips** 키워드는 FIPS 호환 암호만 지정합니다. 예: hmac-sha1
- **high** 키워드는 보안 수준이 높은 암호만 지정합니다. 예: hmac-sha1
- **low** 키워드는 보안 수준이 낮은 암호, 보통인 암호, 높은 암호를 지정합니다. 예: hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
- **medium** — 보안 수준이 보통인 암호와 높은 암호(기본값)를 지정합니다. 예: hmac-sha1 hmac-sha1-96

단계 **11** (선택 사항) DH(Diffie-Hellman) 키 교환 모드를 설정합니다.

ssh key-exchange group {**dh-group1-sha1** | **dh-group14-sha1**}

예제**:**

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

기본값 - **dh-group1-sha1**

DH 키 교환에서는 어느 한쪽에서 단독으로 확인할 수 없는 공유 암호를 제공합니다. 이 키 교환은 서명 및 호스트 키와 연계하여 호스트 인증을 수행합니다. 이 키 교환 방식은 명시적 서버 인증을 수행합니다. DH 키 교환 방법 사용에 대한 자세한 내용은 RFC 4253을 참조하십시오.

예

다음 예에서는 PKF 형식의 키를 사용하여 인증하는 방법을 보여 줍니다.

```
ciscoasa(config)# crypto key generate rsa modulus 4096
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
```

다음 예에서는 Linux 또는 Macintosh 시스템에서 SSH용 공유 키를 생성하고 이를 ASA에 가져옵니다.

1. 4096비트용 ssh-rsa 공개 및 개인 키를 컴퓨터에 생성합니다.

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. 다음과 같이 키를 PKF 형식으로 변환합니다.

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. 키를 클립보드에 복사합니다.
4. ASA CLI에 연결하고 공개 키를 사용자 이름에 추가합니다.

```
ciscoasa(config)# username test attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file completed successfully.
```

5. 사용자(테스트)가 ASA에 SSH를 수행할 수 있는지 확인합니다.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

암호를 입력하라는 다음과 같은 대화 상자가 나타납니다.

한편 터미널 세션에는 다음과 같은 메시지가 표시됩니다.

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

텔넷 액세스 구성

텔넷을 사용하여 ASA에 연결하는 것이 허용된 클라이언트 IP 주소를 지정하려면 다음 단계를 수행합니다. 다음 지침을 참조하십시오.

- 텔넷 액세스를 위해 ASA 인터페이스에 액세스할 때 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 텔넷 액세스를 구성하면 됩니다.
- ASA를 시작할 때 사용한 것과 다른 인터페이스에 대한 텔넷 액세스는 지원되지 않습니다. 예를 들어, 텔넷 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 텔넷 연결만 시작할 수 있습니다. 이 규칙의 유일한 예외는 VPN 연결을 거치는 경우입니다. VPN 터널을 통한 관리 액세스 구성, 1118 페이지을 참조하십시오.
- VPN 터널 내에서 텔넷을 사용하지 않는 한 텔넷을 최하위 보안 인터페이스에서 사용할 수 없습니다.
- ASA에서는 상황/단일 모드당 최대 5개의 동시 텔넷 연결이 가능하며 모든 상황에서 최대 100개의 연결 할당이 가능합니다.

시작하기 전에

- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context** *name*을 입력합니다.
- 텔넷을 사용하여 ASA CLI에 액세스하려면**password** 명령으로 설정한 로그인 비밀번호를 입력하십시오. 텔넷을 사용하기 전에 직접 비밀번호를 설정해야 합니다.

프로시저

단계 1 ASA가 지정된 인터페이스에서 각 주소 또는 서브넷에 대한 연결을 수락하는 IP 주소를 식별합니다.

telnet *source_IP_address mask source_interface*

- *source_interface* — 이름이 있는 인터페이스를 지정합니다. 브리지 그룹의 경우, 브리지 그룹 멤버 인터페이스를 지정합니다.VPN 관리 액세스의 경우에만(VPN 터널을 통한 관리 액세스 구성, 1118 페이지 참조), 명명된 BVI 인터페이스를 지정합니다.

인터페이스가 하나뿐일 경우, 그 인터페이스의 보안 수준이 100이라면 텔넷에서 그 인터페이스에 액세스하도록 구성할 수 있습니다.

예제:

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

단계 2 ASA에서 세션 연결을 끊기 전에 얼마 동안 텔넷 세션을 유휴 상태로 유지할 수 있는지 설정합니다.

telnet timeout *minutes*

예제:

```
ciscoasa(config)#  telnet timeout 30
```

1분~1440분 범위에서 시간 제한을 설정합니다. 기본값은 5분입니다. 이 기본값은 대개 너무 짧으므로 모든 프로덕션 전 단계 테스트 및 문제 해결을 완료할 수 있도록 늘려야 합니다.

예

다음 예는 주소가 192.168.1.2인 내부 인터페이스의 호스트가 ASA에 액세스하도록 허용하는 방법을 보여 줍니다.

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

다음 예는 내부 인터페이스에서 192.168.3.0 네트워크의 모든 사용자가 ASA에 액세스하도록 허용하는 방법을 보여 줍니다.

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

ASDM을 위한 HTTPS 액세스 구성, 기타 클라이언트

ASDM 또는 기타 HTTPS 클라이언트(예: CSM)를 사용하려면 HTTPS 서버를 활성화하고 ASA와의 HTTPS 연결을 허용해야 합니다. HTTPS 액세스는 공장 기본 구성에서 활성화됩니다. HTTPS 액세스를 구성하려면 다음 단계를 수행하십시오. 다음 지침을 참조하십시오.

- HTTPS 액세스를 위해 ASA 인터페이스에 액세스할 때 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 HTTPS 액세스를 구성하면 됩니다. 하지만 HTTPS에 HTTP 연결을 리디렉션하도록 지정하기 위해 HTTP 리디렉션을 구성하는 경우, HTTP를 허용하도록 액세스 규칙을 활성화해야 합니다. 액세스 규칙을 활성화하지 않으면 인터페이스가 HTTP 포트를 수신 대기할 수 없습니다.
- ASA를 시작할 때 사용한 것과 다른 인터페이스에 대한 관리 액세스는 지원되지 않습니다. 예를 들어, 관리 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다. 이 규칙의 유일한 예외는 VPN 연결을 거치는 경우입니다. VPN 터널을 통한 관리 액세스 구성, 1118 페이지을 참조하십시오.
- ASA를 사용하면 상황당 최대 5개의 동시 ASDM 인스턴스가 허용되며 가능한 경우 모든 상황에서 최대 32개의 ASDM 인스턴스가 가능합니다.

  ASDM 세션에서는 2개의 HTTPS 연결을 사용합니다. 하나는 모니터링용으로 항상 실행되며 다른 하나는 구성 변경용으로, 변경할 때만 실행됩니다. 예를 들어, 시스템 제한이 32개의 ASDM 세션이라면 64개의 HTTPS 세션을 의미합니다.

시작하기 전에

- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 구성으로 변경하려면 **changeto context** *name*을 입력합니다.

프로시저

단계 **1** ASA가 지정된 인터페이스에서 각 주소 또는 서브넷에 대한 HTTPS 연결을 수락하는 IP 주소를 식별합니다.

http *source_IP_address mask source_interface*

- *source_interface* — 이름이 있는 인터페이스를 지정합니다. 브리지 그룹의 경우, 브리지 그룹 멤버 인터페이스를 지정합니다.VPN 관리 액세스의 경우에만(VPN 터널을 통한 관리 액세스 구성, 1118 페이지 참조), 명명된 BVI 인터페이스를 지정합니다.

예제:

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

단계 **2** HTTPS 서버를 활성화합니다.

http server enable [*port*]

예제:

```
ciscoasa(config)# http server enable 444
```

기본적으로 port는 443입니다. 포트 번호를 변경한 경우 ASDM 액세스 URL에 포함시켜야 합니다. 예를 들어, 포트 번호를 444로 변경한 경우 다음 URL을 입력합니다.

https://10.1.1.1:444

예

다음 예는 HTTPS 서버를 활성화하는 방법 및 주소가 192.168.1.2인 내부 인터페이스의 호스트가 ASDM에 액세스하도록 허용하는 방법을 보여 줍니다.

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

다음 예는 내부 인터페이스에서 192.168.3.0/24 네트워크의 모든 사용자가 ASDM에 액세스하도록 허용하는 방법을 보여 줍니다.

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

ASDM 액세스 또는 클라이언트리스 SSL VPN을 위한 HTTP 리디렉션 구성

ASDM 또는 클라이언트리스 SSL VPN을 사용하여 ASA에 연결하려면 HTTPS를 사용해야 합니다. 편의를 위해 HTTP 관리 연결을 HTTPS로 리디렉션할 수 있습니다. 예를 들어, HTTP를 리디렉션하여 **http://10.1.8.4/admin/** 또는 **https://10.1.8.4/admin/** 중 어느 것을 입력하더라도 HTTPS 주소의 ASDM 시작 페이지에서 계속 연결됩니다.

IPv4 및 IPv6 트래픽을 둘 다 리디렉션할 수 있습니다.

시작하기 전에

일반적으로 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 하지만 HTTP 리디렉션을 위해 HTTP를 허용하도록 액세스 규칙을 활성화해야 합니다. 액세스 규칙을 활성화하지 않으면 인터페이스가 HTTP 포트를 수신 대기할 수 없습니다.

프로시저

HTTP 리디렉션을 활성화합니다.

http redirect *interface_name* [*port*]

예제**:**

```
ciscoasa(config)# http redirect outside 88
```

*port*는 인터페이스가 HTTP 연결을 리디렉션하는 포트를 식별합니다. 기본값은 80입니다.

VPN 터널을 통한 관리 액세스 구성

VPN 터널이 어떤 인터페이스에서 종료했지만 다른 인터페이스에 액세스하여 ASA를 관리하려는 경우, 해당 인터페이스를 관리 액세스 인터페이스로 식별해야 합니다. 예를 들어, 외부 인터페이스에서 ASA에 들어올 경우, 이 기능을 이용하면 ASDM, SSH, Telnet 또는 SNMP를 통해 내부 인터페이스에 연결할 수 있습니다. 또는 외부 인터페이스에서 들어올 때 내부 인터페이스를 ping할 수 있습니다.

ASA를 시작할 때 사용한 것과 다른 인터페이스에 대한 VPN 액세스는 지원되지 않습니다. 예를 들어, VPN 액세스가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 연결만 시작할 수 있습니다. ASA의 직접 액세스가 가능한 인터페이스에서 VPN을 활성화하고 이름 확인을 사용해야 여러 주소를 기억할 필요가 없습니다.

관리 액세스는 IPsec 클라이언트, IPsec 사이트 대 사이트, Easy VPN 및 AnyConnect SSL VPN 클라이언트의 VPN 터널 유형을 통해 사용할 수 있습니다.

시작하기 전에

별도 관리 및 데이터 라우팅 테이블에 관련 라우팅 고려 사항으로 인해 VPN 종료 인터페이스 및 관리 액세스 인터페이스는 동일한 유형이어야 합니다. 즉, 모두 관리 전용 인터페이스이거나 모두 일반 데이터 인터페이스여야 합니다.

프로시저

다른 인터페이스에서 ASA에 들어갈 때 액세스하려는 관리 인터페이스의 이름을 지정합니다.

management-access *management_interface*

Easy VPN 및 사이트 대 사이트 터널의 경우 라우팅 모드에서 명명된 BVI를 지정할 수 있습니다.

예제:

```
ciscoasa(config)# management-access inside
```

Firepower 2100 데이터 인터페이스에서 FXOS에 대한 관리 액세스 구성

데이터 인터페이스의 Firepower 2100에서 FXOS를 관리하려는 경우 SSH, HTTPS 및 SNMP 액세스를 구성할 수 있습니다. 이 기능은 디바이스를 원격으로 관리하려는 경우와 격리된 네트워크에서 FXOS에 액세스하는 기본 방법으로 관리 1/1을 유지하려는 경우 유용합니다. 이 기능을 활성화하는 경우 로컬 액세스를 위해 관리 1/1을 계속해서 사용할 수 있습니다. 이 기능을 사용할 때는 동시에 FXOS에 대한 관리 1/1에서 원격 액세스를 허용할 수 없습니다. 이 기능을 사용하려면 내부 경로(기본값)를 사용하여 ASA 데이터 인터페이스에 트래픽을 전달해야 하며 하나의 FXOS 관리 게이트웨이만 지정할 수 있습니다.

ASA는 FXOS 액세스용으로 비표준 포트를 사용합니다. 표준 포트는 동일한 인터페이스에 있는 ASA에서 사용하기 위해 예약되어 있습니다. ASA가 FXOS로 트래픽을 전달할 때 비표준 대상 포트를 각 프로토콜(FXOS에서 HTTPS 포트를 변경하지 않음)에 대한 FXOS 포트로 변환합니다. 패킷 대상 IP

주소(ASA 인터페이스 IP 주소)도 FXOS에서 사용하기 위해 내부 주소로 변환됩니다. 소스 주소는 변경되지 않습니다. 트래픽을 반환하기 위해 ASA는 데이터 라우팅 테이블을 사용하여 올바른 이그레스 인터페이스를 결정합니다. 관리 애플리케이션용 ASA 데이터 IP 주소에 액세스할 때 FXOS 사용자 이름을 사용하여 로그인해야 합니다. ASA 사용자 이름은 ASA 관리 액세스에만 적용됩니다.

또한, FXOS 관리 트래픽 시작 기능을 ASA 데이터 인터페이스에서 활성화할 수 있습니다. 이 기능은 예를 들어 SNMP 트랩 또는 NTP 및 DNS 서버 액세스에 필요합니다. 기본적으로 FXOS 관리 트래픽 시작 기능은 DNS 및 NTP 서버 통신(Smart Software Licensing 통신에 필요)을 위한 ASA 외부 인터페이스에 대해 활성화됩니다.

시작하기 전에

- 단일 상황 모드만 해당합니다.
- ASA 관리 전용 인터페이스는 제외됩니다.
- VPN 터널을 ASA 데이터 인터페이스에 사용할 수 없으며 FXOS에 직접 액세스할 수 없습니다. SSH를 위한 해결 방법으로, ASA에 VPN을 사용하고 *ASA* CLI에 액세스한 다음 **connect fxos** 명령을 사용하여 FXOS CLI에 액세스할 수 있습니다. SSH, HTTPS 및 SNMPv3는 암호화될 수 있으므로 데이터 인터페이스에 직접 연결하는 것이 안전합니다.

프로시저

단계 **1** FXOS 원격 관리를 활성화합니다.

fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address*/*prefix_length*} *interface_name*

예제**:**

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

단계 **2** (선택 사항) 서비스에 대한 기본 포트를 변경합니다.

fxos {**https** | **ssh** | **snmp**} **port** *port*

다음 기본값을 참고하십시오.

- HTTPS 기본 포트 — 3443
- SNMP 기본 포트 — 3061
- SSH 기본 포트 — 3022

예제**:**

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

단계 **3** FXOS가 ASA 인터페이스에서 관리 연결을 시작하도록 허용합니다.

ip-client *interface_name*

기본적으로 외부 인터페이스는 활성화되어 있습니다.

예제**:**

```
ciscoasa(config)# ip-client outside
ciscoasa(config)# ip-client services
```

단계 **4** 관리 1/1에서 Firepower Chassis Manager(기본값: https://192.168.45.45, 사용자 이름: **admin**, 비밀번호: **Admin123**)에 연결합니다.

단계 **5** **Platform Settings(**플랫폼 설정**)** 탭을 클릭하고 **SSH**, **HTTPS** 또는 **SNMP**를 활성화합니다.

SSH와 HTTPS는 기본적으로 활성화되어 있습니다.

단계 **6** **Platform Settings(**플랫폼 설정**)** 탭의 **Access List(**액세스 목록**)**를 구성하여 관리 주소를 허용합니다. SSH와 HTTPS는 기본적으로 관리 1/1 192.168.45.0 네트워크만 허용합니다. ASA의 **FXOS Remote Management(FXOS** 원격 관리**)** 컨피그레이션에서 지정한 주소를 허용해야 합니다.

콘솔 시간 초과 변경

콘솔 시간 초과는 어떤 연결에서 특별 권한 EXEC 모드 또는 컨피그레이션 모드가 얼마나 오래 유지될 수 있는가를 설정합니다. 시간 초과에 도달하면 세션은 사용자 EXEC 모드로 전환됩니다. 기본적으로 세션은 시간 제한이 없습니다. 이 설정은 사용자가 얼마나 오랫동안 콘솔 포트와의 연결 상태를 유지할 수 있는가에 영향을 주지 않습니다. 이 연결 상태는 시간 제한이 없습니다.

프로시저

특별 권한 세션이 끝난 이후의 유휴 시간(분, 0~60)을 지정합니다.

console timeout *number*

예제**:**

```
ciscoasa(config)# console timeout 0
```

기본 시간 제한은 0입니다. 즉 세션에 시간 제한이 없습니다.

CLI 프롬프트 사용자 정의

프롬프트에 정보를 추가하는 기능 덕분에 여러 모듈이 있는 경우 어떤 ASA에 로그인했는지를 한눈에 알 수 있습니다. 페일오버 중에 두 ASA의 호스트 이름이 동일한 경우 이 기능이 유용합니다.

다중 상황 모드에서 시스템 실행 공간 또는 관리 상황에 로그인하면 확장 프롬프트를 볼 수 있습니다. 비관리 상황 내에서는 호스트 이름 및 상황 이름인 기본 프롬프트만 볼 수 있습니다.

기본적으로 프롬프트는 ASA의 호스트 이름을 표시합니다. 다중 상황 모드에서는 프롬프트가 상황 이름도 표시합니다. CLI 프롬프트에서 다음 항목을 표시할 수 있습니다.

cluster-unit	클러스터 유닛 이름을 표시합니다. 클러스터의 각 유닛은 고유한 이름을 가질 수 있습니다.
context	(다중 모드만) 현재 상황의 이름을 표시합니다.
domain	도메인 이름을 표시합니다.
hostname	호스트 이름을 표시합니다.
priority	장애 조치 우선순위를 pri(1차) 또는 sec(2차)로 표시합니다.

state	유닛의 트래픽 전달 상태 또는 역할을 표시합니다. 페일오버의 경우 state 키워드에 대해 다음 값이 표시됩니다. • **act** - 장애 조치가 활성화되었으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • **stby** — 페일오버가 활성화되었으며, 해당 유닛은 트래픽을 전달하는 중이 아니며, 스탠바이, 실패 또는 액티브가 아닌 상태입니다. • **actNoFailover** - 장애 조치가 활성화되지 않았으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • **stbyNoFailover** — 페일오버가 활성화되지 않았으며, 해당 유닛은 트래픽을 전달하는 중이 아닙니다. 스탠바이 유닛의 임계값을 초과하는 인터페이스 오류가 있을 경우 이러한 상황이 발생할 수 있습니다. 클러스터링의 경우 state 키워드에 대해 다음 값이 표시됩니다. • **master** • **slave** 예를 들어, **prompt hostname cluster-unit state**를 설정하는 경우 프롬프트 "ciscoasa/cl2/slave>"에서 호스트 이름은 ciscoasa, 유닛 이름은 cl2, 상태 이름은 slave입니다.

프로시저

다음 명령을 입력하여 CLI 프롬프트를 사용자 정의합니다.
prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

예제:

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

키워드를 입력하는 순서는 프롬프트에서 요소가 나타나는 순서를 결정하며, 슬래시(/)로 구분됩니다.

로그인 배너 구성

사용자가 ASA에 연결할 때 사용자 로그인 전에 또는 사용자가 특별 권한 EXEC 모드를 시작하기 전에 표시할 메시지를 구성할 수 있습니다.

시작하기 전에

- 보안의 관점에서는 배너에서 무단 액세스를 방지하는 것이 중요합니다. 침입자를 초대하는 것처럼 보이는 "환영" 또는 "부탁"에 해당하는 단어를 사용하지 마십시오. 다음 배너는 무단 액세스에 대해 올바른 톤을 설정합니다.

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- 배너가 추가된 후 다음과 같은 경우에 ASA에 대한 텔넷 또는 SSH 세션이 종료될 수 있습니다.
  - 배너 메시지를 처리하기에는 시스템 메모리가 충분하지 않을 경우
  - 배너 메시지를 표시하려 할 때 TCP 쓰기 오류가 발생한 경우
- 배너 메시지에 대한 자세한 내용은 RFC 2196을 참조하십시오.

프로시저

사용자가 처음 연결할 때(message-of-the-day(motd)), 사용자가 로그인할 때(login), 사용자가 특별 권한 EXEC 모드에 액세스할 때(exec)의 3가지 경우 중 하나에 표시할 배너를 추가합니다.

banner {**exec** | **login** | **motd**} *text*

예제**:**

```
ciscoasa(config)# banner motd Welcome to $(hostname).
```

사용자가 ASA에 연결할 때 message-of-the-day 배너가 먼저 표시되고 뒤이어 로그인 배너와 프롬프트가 나타납니다. 사용자가 ASA에 성공적으로 로그인하면 EXEC 배너가 나타납니다.

두 라인 이상 추가하려면 각 라인의 앞에 **banner** 명령을 넣습니다.

배너 텍스트:

- CLI에서 공백은 허용되지만 탭은 입력할 수 없습니다.
- RAM 및 플래시 메모리에 대한 제한을 제외하면 배너 길이에 대한 제한은 없습니다.
- ASA의 호스트 이름 또는 도메인 이름을 동적으로 추가할 수 있습니다. 문자열 **$(hostname)**과 **$(domain)**을 포함시키면 됩니다.

- 시스템 구성에서 배너를 구성한 경우, 상황 구성에서 **$(system)** 문자열을 사용하여 상황 내에 배너 텍스트를 사용할 수 있습니다.

예

다음 예는 message-of-the-day 배너를 추가하는 방법을 보여 줍니다.

```
ciscoasa(config)# banner motd Welcome to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

관리 세션 할당량 설정

ASA에서 허용되는 동시 ASDM, SSH, 텔넷 세션의 최대 수를 설정할 수 있습니다. 최대 개수에 도달하면 더 이상 추가 세션이 허용되지 않으며 syslog 메시지가 생성됩니다. 시스템 잠금을 방지하는 차원에서 관리 세션 할당량 메커니즘이 콘솔 세션을 차단할 수 없습니다.

시작하기 전에

다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황에서 시스템 구성으로 변경하려면 **changeto system** 명령을 입력합니다.

프로시저

단계 **1** 다음의 명령을 입력합니다.

quota management-session *number*

- *number* — 0(무제한)~10000 사이의 집계 세션 수를 설정합니다.

예제**:**

예제**:**

```
ciscoasa(config)# quota management-session 1000
```

단계 **2** 사용 중인 현재 세션을 확인합니다.

show quota management-session

예제**:**

```
ciscoasa(config)# show quota management-session

quota management-session limit 3
quota management-session warning level 2
quota management-session level 0
```

```
quota management-session high water 2
quota management-session errors 0
quota management-session warnings 0
```

시스템 관리자를 위한 **AAA** 구성

이 섹션에서는 시스템 관리자를 위해 인증, 관리 권한 부여 및 명령 권한 부여를 구성하는 방법을 설명합니다.

관리 인증 구성

CLI 및 ASDM 액세스를 위한 인증 구성

관리 인증 정보

ASA에 로그인하는 방법은 인증을 활성화했는지에 따라 달라집니다.

SSH 인증 정보

인증 사용 여부와 관계없이 SSH 액세스를 위한 다음 동작을 참고하십시오.

- 인증 없음 — 인증 없이는 SSH를 사용할 수 없습니다.
- 인증 — SSH 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. ASA는 공개 키 인증을 위해 로컬 데이터베이스만 지원합니다. SSH 공개 키 인증을 구성하는 경우, ASA는 암시적으로 로컬 데이터베이스를 사용합니다. 사용자 이름 및 비밀번호를 사용하여 로그인하는 경우, SSH 인증만 명시적으로 구성하면 됩니다. 사용자 EXEC 모드에 액세스할 수 있습니다.

텔넷 인증 정보

인증 사용 여부와 관계없이 텔넷 액세스를 위한 다음 동작을 참고하십시오.

- 인증 없음 — 텔넷에 대해 어떤 인증도 활성화하지 않을 경우 사용자 이름을 입력하지 않습니다. 로그인 비밀번호를 입력합니다(**password** 명령으로 설정). 기본 비밀번호가 없는 경우, ASA에 텔넷으로 연결하려면 기본 비밀번호를 설정해야 합니다. 사용자 EXEC 모드에 액세스할 수 있습니다.
- 인증 — 텔넷 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. 사용자 EXEC 모드에 액세스할 수 있습니다.

ASDM 인증 정보

인증 사용 여부와 관계없이 ASDM 액세스를 위한 다음 동작을 참고하십시오. 또는 AAA 인증 사용 여부와 관계없이 인증서 인증을 구성할 수도 있습니다.

- 인증 없음 — 기본적으로 빈 사용자 이름과 enable 비밀번호를 사용하여(**enable password** 명령을 통해 설정됨) ASDM에 로그인할 수 있습니다. 비밀번호가 비어 있지 않도록 가능한 한 빨리 enable 비밀번호를 변경하는 것이 좋습니다. 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정, 681 페이지의 내용을 참고하십시오. 로그인 화면에서 (사용자 이름을 비워 두지 않고) 사용자 이름과 비밀번호를 입력한 경우 ASDM은 로컬 데이터베이스에 일치하는 항목이 있는지 확인합니다.
- 인증서 인증 — (단일, 라우팅 모드 전용) 사용자에게 유효한 인증서를 보유하도록 요구할 수 있습니다. 인증서 사용자 이름 및 비밀번호를 입력합니다. ASA는 PKI 신뢰 지점에 대해 인증서를 검증합니다.
- AAA 인증 — ASDM(HTTPS) 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. 더 이상 빈 사용자 이름과 enable 비밀번호로 ASDM을 사용할 수 없습니다.
- AAA 인증 및 인증서 인증 — (단일, 라우팅 모드 전용) ASDM(HTTPS) 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. 인증서 인증용 사용자 이름 및 비밀번호가 다른 경우, 이를 입력하라는 프롬프트가 표시됩니다. 인증서에서 가져온 사용자 이름을 미리 채우도록 선택할 수 있습니다.

시리얼 인증 정보

인증 사용 여부와 관계없이 시리얼 콘솔 포트에 액세스하기 위한 다음 동작을 참고하십시오.

- 인증 없음 — 시리얼 액세스를 위해 어떤 인증도 활성화하지 않을 경우 사용자 이름 또는 비밀번호를 입력하지 않습니다. 사용자 EXEC 모드에 액세스할 수 있습니다.
- 인증 — 시리얼 액세스를 위해 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. 사용자 EXEC 모드에 액세스할 수 있습니다.

인증 활성화 정보

로그인한 다음 특별 권한 EXEC 모드를 시작하려면 **enable** 명령을 입력합니다. 이 명령의 작동 방식은 인증을 활성화했는지에 따라 달라집니다.

- 인증 없음 — enable 인증을 구성하지 않은 경우, **enable** 명령을 입력할 때 기본적으로 비어 있는 시스템 enable 비밀번호(**enable password** 명령으로 설정)를 입력합니다. 그러나 enable 인증을 사용하지 않을 경우, **enable** 명령을 입력한 다음에는 더 이상 특정 사용자로 로그인한 상태가 아니므로 명령 권한 부여 같은 사용자 기반 기능에 영향을 줄 수 있습니다. 사용자 이름을 유지하려면 enable 인증을 사용합니다.
- 인증 — enable 인증을 구성한 경우 ASA는 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력하라는 프롬프트를 표시합니다. 사용자가 입력 가능한 명령을 확인하는 데 사용자 이름이 중요한 역할을 하는 명령 권한 부여에서 이 기능은 매우 유용합니다.

로컬 데이터베이스를 사용하는 enable 인증에서는 **login** 명령을 **enable** 명령 대신 사용할 수 있습니다. **login** 명령은 사용자 이름을 유지하지만, 인증을 실행하는 데 어떤 구성도 필요하지 않습니다.

주의 CLI에 대한 액세스는 허용되지만 특별 권한 EXEC 모드 액세스는 허용되지 않는 사용자를 로컬 데이터베이스에 추가하려는 경우 명령 권한 부여를 구성해야 합니다. 명령 권한 부여가 없으면, 권한 수준이 2 이상(2가 기본값)인 사용자는 CLI에서 각자의 비밀번호를 사용하여 특별 권한 EXEC 모드(및 모든 명령)에 액세스할 수 있습니다. 또는 로컬 데이터베이스 대신 인증에 AAA 서버를 사용하여 로그인 명령을 사용하지 않을 수 있습니다. 또는 모든 로컬 사용자를 레벨 1로 설정해 놓고 누가 시스템 enable 비밀번호를 사용하여 특별 권한 EXEC 모드에 액세스할 수 있는가를 제어하는 방법도 있습니다.

호스트 운영 체제부터 **ASA**까지의 세션

일부 플랫폼은 별도의 애플리케이션으로 ASA의 실행을 지원합니다. 예를 들어 Catalyst 6500에서는 ASASM이 해당하고 Firepower 4100/9300에서는 ASA가 해당합니다. 호스트 운영 체제에서 ASA로 연결되는 세션의 경우, 연결 유형에 따라 시리얼 또는 텔넷 인증을 구성할 수 있습니다. 예를 들어, Firepower 2100의 FXOS에서 **connect asa** 명령은 시리얼 연결을 사용합니다.

다중 상황 모드에서는 시스템 구성에서 어떤 AAA 명령도 구성할 수 없습니다. 그러나 관리 상황에서 텔넷 또는 시리얼 인증을 구성한 경우, 이러한 세션에도 인증이 적용됩니다. 이 경우에는 관리 상황 AAA 서버 또는 로컬 사용자 데이터베이스가 사용됩니다.

CLI 및 ASDM 액세스를 위한 인증 구성

시작하기 전에

- 텔넷, SSH 또는 HTTP 액세스를 구성합니다.
- 외부 인증의 경우, AAA 서버 그룹을 구성합니다. 로컬 인증의 경우, 로컬 데이터베이스에 사용자를 추가합니다.
- HTTP 관리 인증에서는 AAA 서버 그룹에 대해 SDI 프로토콜을 지원하지 않습니다.
- 이 기능은 **ssh authentication** 명령을 사용하는 로컬 사용자 이름에 대한 SSH 공개 키 인증에 영향을 미치지 않습니다. ASA는 암시적으로 공개 키 인증을 위해 로컬 데이터베이스를 사용합니다. 이 기능은 비밀번호가 있는 사용자 이름에만 영향을 미칩니다. 공개 키 인증 또는 비밀번호를 로컬 사용자가 사용하도록 허용하려는 경우, 비밀번호 액세스를 허용하도록 이 절차대로 로컬 인증을 명시적으로 구성해야 합니다.

프로시저

관리 액세스를 위해 사용자를 인증합니다.

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

예제:

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
```

```
ciscoasa(config)# aaa authentication serial console LOCAL
```

telnet 키워드가 텔넷 액세스를 제어합니다. ASASM에서는 이 키워드가 **session** 명령을 사용하는 스위치로부터의 세션에도 영향을 줍니다. **ssh** 키워드는 SSH 액세스를 제어합니다(비밀번호만 해당, 공개 키 인증 시 로컬 데이터베이스를 암시적으로 사용). **http** 키워드는 ASDM 액세스를 제어합니다. **serial** 키워드는 콘솔 포트 액세스를 제어합니다. ASASM에서는 예를 들어, 이 키워드가 **service-module session** 명령을 사용하여 스위치로부터 액세스하는 가상 콘솔에 영향을 줍니다.Firepower 2100에서는 이 키워드가 **connect asa** 명령을 사용하여 FXOS로부터 액세스하는 가상 콘솔에 영향을 줍니다.

인증에 AAA 서버 그룹을 사용하는 경우, AAA 서버를 사용할 수 없을 때 로컬 데이터베이스를 폴백 방법으로 사용하도록 ASA를 구성할 수 있습니다. **LOCAL**(대/소문자 구분) 다음에 서버 그룹 이름을 지정합니다. 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다. **LOCAL**만 입력하여 로컬 데이터베이스를 기본 인증 방법으로(폴백 없이) 사용할 수도 있습니다.

인증 활성화 구성(특권 **EXEC** 모드)

사용자가 **enable** 명령을 입력할 때 사용자를 인증할 수 있습니다.

시작하기 전에

인증 활성화 정보, 1126 페이지을 참조하십시오.

프로시저

사용자 인증을 위해 다음 옵션 중 하나를 선택합니다.

- AAA 서버 또는 로컬 데이터베이스를 통해 사용자를 인증하려면, 다음 명령을 입력하십시오.

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  예**:**

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  사용자는 사용자 이름과 비밀번호를 입력해야 합니다.

  인증에 AAA 서버 그룹을 사용하는 경우, AAA 서버를 사용할 수 없을 때 로컬 데이터베이스를 대신 사용하도록 ASA를 구성할 수 있습니다. **LOCAL**(대/소문자 구분) 다음에 서버 그룹 이름을 지정합니다. 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다.

  LOCAL만 입력하여 (대체 방법 없이) 로컬 데이터베이스를 기본 인증 방법으로 사용할 수도 있습니다.

- 로컬 데이터베이스의 사용자로 로그인하려면 다음 명령을 입력합니다.

  login

예:

```
ciscoasa# login
```

ASA에서는 사용자 이름과 비밀번호를 묻습니다. 비밀번호를 입력하면 ASA에서는 로컬 데이터베이스에 지정된 권한 레벨을 부여합니다.

사용자는 자신의 사용자 이름과 비밀번호로 로그인하여 특별 권한 EXEC 모드에 액세스할 수 있습니다. 따라서 모든 사람에게 시스템 enable 비밀번호를 알려줘야 하는 부담이 없습니다. 사용자가 로그인할 때 특별 권한 EXEC 모드(및 모든 명령)에 액세스할 수 있게 하려면 사용자 권한 수준을 2(기본값)~15로 설정합니다. 로컬 명령 권한 부여를 구성한 경우, 사용자는 해당 권한 수준 이하에 할당된 명령만 입력할 수 있습니다.

ASDM 인증서 인증 구성

AAA 인증 사용 여부와 관계없이 인증서 인증이 필요할 수 있습니다. ASA는 PKI 신뢰 지점에 대해 인증서를 검증합니다.

시작하기 전에

이 기능은 단일 라우팅 모드에서만 지원됩니다.

프로시저

단계 **1** 인증서 인증을 활성화합니다.

http authentication-certificate *interface_name*[**match** *certificate_map_name*]

예제:

```
ciscoasa(config)# crypto ca certificate map map1 10
ciscoasa(config-ca-cert-map)# subject-name eq www.example.com
ciscoasa(config)# http authentication-certificate outside match map1
```

각 인터페이스에 대해 인증서 인증을 구성함으로써 신뢰받는/내부 인터페이스의 연결은 인증서를 제공할 필요가 없습니다. 이 명령을 여러 번 사용하여 여러 인터페이스에서 인증서 인증을 활성화할 수 있습니다.

인증서 맵과 일치하는 인증서를 요구하려면 **match** 키워드와 맵 이름을 지정합니다. **crypto ca certificate map** 명령을 사용하여 맵을 구성합니다.

단계 **2** (선택 사항) ASDM에서 사용한 속성이 인증서에서 사용자 이름을 파생하도록 설정합니다.

http username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

예제:

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

기본적으로 ASDM에서는 CN OU 속성을 사용합니다.

- *primary-attr* 인수는 사용자 이름을 파생하는 데 사용할 속성을 지정합니다. *secondary-attr* 인수는 사용자 이름을 파생하기 위해 기본 속성과 함께 사용할 추가 속성을 지정합니다. 다음 속성을 사용할 수 있습니다.
  - C — 국가
  - CN — 공통 이름
  - DNQ — DN 한정자
  - EA — 이메일 주소
  - GENQ — 세대 한정자
  - GN — 이름
  - I — 이니셜
  - L — 구/군/시
  - N — 이름
  - O — 조직
  - OU — 조직 단위
  - SER — 시리얼 번호
  - SN — 성
  - SP — 시/도
  - T — 직함
  - UID — 사용자 ID
  - UPN — 사용자 계정 이름
- **use-entire-name** 키워드는 전체 DN 이름을 사용합니다.
- **use-script** 키워드는 ASDM에서 생성한 Lua 스크립트를 사용합니다.
- **pre-fill-username** 키워드는 인증에 대한 프롬프트가 표시되면 사용자 이름을 미리 채웁니다. 사용자 이름이 처음에 입력한 이름과 다른 경우, 사용자 이름이 미리 채워진 새 대화 상자가 나타납니다. 그런 다음 인증을 위해 비밀번호를 입력합니다.

관리 권한 부여로 **CLI** 및 **ASDM** 액세스 제어

ASA를 사용하면 관리 및 원격 액세스 사용자가 인증할 때 이들 사용자를 구분할 수 있습니다. 사용자 역할 차별화를 통해 원격 액세스 VPN 및 네트워크 액세스 사용자가 ASA와의 관리 연결을 설정하는 것을 방지할 수 있습니다.

시작하기 전에

RADIUS 또는 **LDAP(**매핑됨**)** 사용자

사용자가 LDAP을 통해 인증되면 기본 LDAP 속성과 해당 값이 Cisco ASA 속성에 매핑되어 특정 권한 부여 기능을 제공할 수 있습니다. 값이 0~15인 Cisco VSA CVPN3000-Privilege-Level로 구성한 다음 **ldap map-attributes** 명령을 사용하여 LDAP 속성을 Cisco VAS CVPN3000-Privilege-Level에 매핑합니다.

RADIUS IETF **service-type** 특성은, RADIUS 인증 및 권한 부여 요청의 결과인 access-accept 메시지를 통해 전송될 때, 어떤 서비스 유형이 인증된 사용자에게 부여될지 지정하는 데 사용됩니다.

RADIUS Cisco VSA **privilege-level** 특성(Vendor ID 3076, sub-ID 220)은, access-accept 메시지를 통해 전송될 때, 사용자의 권한 수준을 지정하는 데 쓰입니다.

TACACS+ 사용자

"service=shell"로 권한 부여가 요청되고, 서버는 PASS 또는 FAIL로 응답합니다.

로컬 사용자

지정된 사용자 이름에 대해 **service-type** 명령을 설정합니다. 기본적으로 service-type은 admin이며, 이는 **aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.

관리 권한 부여 속성

AAA 서버 유형 및 관리 권한 부여에 유효한 값은 다음 표를 참고하십시오. ASA에서는 이러한 값을 사용하여 관리 액세스 레벨을 결정합니다.

관리 레벨	**RADIUS/LDAP(**매핑됨**)** 속성	**TACACS+** 특성	로컬 데이터베이스 속성
전체 액세스 — **aaa authentication console**명령에서 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.	서비스-유형 6(관리자), 권한-레벨 1	PASS, 권한 레벨 1	admin
부분 액세스 — **aaa authentication console**명령을 구성하는 경우 CLI 또는 ASDM에 대한 액세스를 허용합니다. 그러나 **enable** 인증을 구성하는 데 **aaa authentication enable console** 명령을 사용한 경우, CLI 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다.	서비스 유형 7(NAS 프롬프트), 권한 레벨 2 이상 Framed (2) 서비스 유형과 Login (1) 서비스 유형은 동일하게 처리됩니다.	PASS, 권한 레벨 2 이상	nas-prompt

관리 레벨	**RADIUS/LDAP**(매핑됨) 속성	**TACACS+** 특성	로컬 데이터베이스 속성
액세스 없음 — 관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령에서 지정된 임의의 서비스를 사용할 수 없습니다(**serial** 키워드 제외, 시리얼 액세스는 허용됨). 원격 액세스(IPSec 및 SSL) 사용자는 원격 액세스 세션을 계속 인증하고 종료할 수 있습니다. 그 밖의 모든 서비스 유형(Voice, FAX 등)은 동일하게 처리됩니다.	서비스-유형 5(아웃바운드)	실패	remote-access

추가 지침

- 시리얼 콘솔 액세스는 관리 권한 부여에 포함되지 않습니다.
- 또한 이 기능을 사용하려면 관리 액세스에 대한 AAA 인증을 구성해야 합니다. CLI 및 ASDM 액세스를 위한 인증 구성, 1127 페이지을 참조하십시오.
- 외부 인증을 사용하는 경우, 이 기능을 활성화하기 전에 AAA 서버 그룹을 사전에 구성해야 합니다.
- HTTP 권한 부여는 단일 라우팅 모드에서만 지원됩니다.

프로시저

단계 **1** 텔넷 및 SSH에 대한 관리 권한 부여를 활성화합니다.

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

auto-enable 키워드를 사용하면 충분한 권한 부여 특권을 지닌 관리자가 로그인할 때 특별 권한 EXEC 모드로 자동으로 들어갈 수 있습니다.

예제**:**

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

단계 **2** HTTPS(ASDM)에 대한 관리 권한 부여를 활성화합니다.

aaa authorization http console {**authentication-server** | **LOCAL**}

예제**:**

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

단계 **3**

예

다음 예는 LDAP 특성 맵을 정의하는 방법을 보여 줍니다. 이 예에서 보안 정책은 LDAP을 통해 인증되는 사용자가 사용자 레코드 필드 또는 파라미터 제목 및 회사를 각각 IETF-RADIUS service-type 및 privilege-level에 매핑하도록 지정합니다.

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

다음 예는 LDAP AAA 서버에 LDAP 특성 맵을 적용합니다.

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

명령 권한 부여 구성

명령에 대한 액세스를 제어하고 싶은 경우 ASA에서 명령 권한 부여를 구성할 수 있습니다. 이는 사용자가 어떤 명령을 사용할 수 있는가를 결정하는 것입니다. 기본적으로 로그인할 때 사용자 EXEC 모드에 액세스할 수 있습니다. 이 모드는 최소한의 명령만 제공합니다. **enable** 명령(또는 로컬 데이터베이스를 사용할 때는 **login** 명령)을 입력하면 특별 권한 EXEC 모드와 고급 명령(구성 명령 포함)에 액세스할 수 있습니다.

다음 두 가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 수준
- TACACS+ 서버 권한 수준

명령 권한 부여 정보

권한 있는 사용자만 명령을 입력할 수 있도록 명령 권한 부여를 활성화할 수 있습니다.

지원되는 명령 권한 부여 방식

다음 두 가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 레벨 — ASA에서 명령 권한 레벨을 구성합니다. 로컬, RADIUS 또는 LDAP(LDAP 속성을 RADIUS 속성에 매핑한 경우) 사용자가 CLI 액세스를 위해 인증할 경우, ASA에서는 로컬 데이터베이스, RADIUS 또는 LDAP 서버에서 정의한 권한 레벨을 사용자에게 부여합니다. 사용자는 할당된 권한 수준 이하의 명령에 액세스할 수 있습니다. 모든 사용자가 처음 로그인할 때는 사용자 EXEC 모드에 액세스합니다(수준 0 또는 1의 명령). 사용자는 **enable** 명령을 사용하여 다시 인증해야 특별 권한 EXEC 모드(수준 2 이상의 명령)에 액세스할 수 있습니다. 또는 **login** 명령을 사용하여 로그인할 수 있습니다(로컬 데이터베이스만).

참고 로컬 데이터베이스에 어떤 사용자도 없는 상태에서, CLI 또는 **enable** 인증 없이 로컬 명령 권한 부여를 사용할 수 있습니다. 그 대신 **enable** 명령을 입력할 때는 시스템 enable 비밀번호를 입력합니다. 그러면 ASA에서는 레벨 15를 부여합니다. 그러면 각 레벨의 enable 비밀번호를 생성할 수 있습니다. 즉 **enable** *n*(2~15)을 입력하면 ASA에서는 레벨 *n*을 부여합니다. 이러한 수준은 로컬 명령 권한 부여를 활성화한 경우에만 사용됩니다.

- TACACS+ 서버 권한 수준—TACACS+ 서버에서 사용자 또는 그룹이 CLI 액세스를 위한 인증 이후에 사용할 수 있는 명령을 구성합니다. 사용자가 CLI에서 입력하는 모든 명령에 대해 TACACS+ 서버를 사용한 유효성 검사가 실시됩니다.

보안 컨텍스트 및 명령 권한 부여

AAA 설정은 컨텍스트끼리 공유되지 않으며 컨텍스트마다 다릅니다.

명령 권한 부여를 구성할 때 각 보안 상황을 따로 구성해야 합니다. 이러한 구성에서는 여러 보안 상황에서 각기 다른 명령 권한 부여를 적용하는 것이 가능합니다.

보안 상황 간 전환에서 관리자는 로그인 시 지정된 사용자 이름에 대해 허용된 명령이 새 상황 세션에서는 다를 수 있음을 또는 새 상황에서는 명령 권한 부여가 아예 구성되지 않았을 수도 있음을 알고 있어야 합니다. 명령 권한 부여가 보안 상황마다 다를 수 있음을 모르는 관리자는 혼란스러워 할 수도 있습니다. 이는 다음 사항 때문에 더욱 복잡해집니다.

참고 시스템 실행 영역에서는 AAA 명령을 지원하지 않습니다. 따라서 시스템 실행 영역에서는 명령 권한 부여를 사용할 수 없습니다.

명령 권한 수준

기본적으로 다음 명령에 권한 수준 0이 할당됩니다. 다른 모든 명령은 권한 수준 15에 할당됩니다.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**

- **clear pager**
- **quit**
- **show version**

어떤 구성 모드 명령을 15보다 낮은 수준으로 이동한 경우, **configure** 명령도 해당 수준으로 이동해야 합니다. 그러지 않으면 사용자가 구성 모드를 시작할 수 없습니다.

로컬 명령 권한 부여 구성

로컬 명령 권한 부여에서는 16가지 권한 수준(0 ~ 15) 중 하나에 명령을 할당할 수 있습니다. 기본적으로 각 명령은 권한 수준 0 또는 15 중 하나에 할당됩니다. 각 사용자를 특정 권한 수준으로 정의할 수 있으며, 각 사용자는 할당된 권한 수준 이하의 어떤 명령도 입력할 수 있습니다. ASA에서는 로컬 데이터베이스, RADIUS 서버 또는 (LDAP 속성을 RADIUS 속성에 매핑한 경우) LDAP 서버에 정의된 사용자 권한 레벨을 지원합니다.

프로시저

단계 **1** 어떤 명령을 어떤 권한 수준에 할당합니다.

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command*

예제**:**

```
ciscoasa(config)# privilege show level 5 command filter
```

다시 할당하고 싶은 명령 각각에 대해 이 명령을 반복합니다.

이 명령의 옵션은 다음과 같습니다.

- **show** | **clear** | **cmd** — 이 선택적 키워드를 사용하여 해당 명령의 show, clear 또는 configure 형식에 대해서만 권한을 설정할 수 있습니다. 명령의 configure 형식은 일반적으로 구성 변경을 일으키는 형식으로서 수정되지 않은 명령(**show** 또는 **clear** 접두사 없음)이거나 **no** 형식입니다. 이 키워드 중 하나를 사용하지 않을 경우 해당 명령의 모든 형식이 영향을 받습니다.
- **level** *level* — 0~15의 레벨입니다.
- **mode** {**enable** | **configure**} — 사용자 EXEC 모드 또는 특별 권한 EXEC 모드뿐 아니라 구성 모드에서도 어떤 명령을 입력할 수 있고 이 명령이 각 모드에서 다른 작업을 수행할 경우, 이 모드 각각에 대한 권한 레벨을 설정할 수 있습니다.
  - **enable**— 사용자 EXEC 모드와 특별 권한 EXEC 모드를 모두 지정합니다.
  - **configure** — **configure terminal** 명령을 사용하여 액세스하는 구성 모드를 지정합니다.
- **command** *command* — 구성 중인 명령입니다. 기본 명령의 권한 수준만 구성할 수 있습니다. 예를 들어 모든 **aaa** 명령의 수준을 구성할 수 있으나, **aaa authentication** 명령과 **aaa authorization** 명령의 수준을 각각 구성할 수는 없습니다.

단계 **2** (선택 사항) 명령 권한 부여를 위해 AAA 사용자를 활성화합니다. 이 명령을 사용하지 않을 경우 ASA에서는 로컬 데이터베이스 사용자의 권한 레벨만 지원하며, 그 밖의 모든 사용자 유형은 기본적으로 레벨 15가 됩니다.

aaa authorization exec authentication-server [auto-enable]

예제**:**

```
ciscoasa(config)# aaa authorization exec authentication-server
```

이 명령은 관리 권한 부여도 활성화합니다. 관리 권한 부여로 CLI 및 ASDM 액세스 제어, 1131 페이지을 참조하십시오.

단계 **3** 로컬 명령 권한 레벨의 사용을 활성화합니다.

aaa authorization command LOCAL

예제**:**

```
ciscoasa(config)# aaa authorization command LOCAL
```

명령 권한 수준을 설정한 경우, 이 명령으로 명령 권한 부여를 구성하지 않으면 명령 권한 부여가 수행되지 않습니다.

예

filter 명령은 다음 형식을 갖습니다.

- **filter(configure** 옵션으로 표시됨)
- **show running-config filter**
- **clear configure filter**

각 형식의 권한 수준을 개별적으로 설정하거나, 이 옵션을 생략하여 모든 형식에 동일한 권한 수준을 설정할 수 있습니다. 다음 예는 각 형식을 개별적으로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

한편 다음 예는 모든 filter 명령을 동일한 수준에 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 명령은 화면에서 형식을 구분합니다.

다음 예는 **mode** 키워드의 사용 방법을 보여 줍니다. **enable** 명령은 사용자 EXEC 모드에서 입력해야 하지만, 구성 모드에서 액세스 가능한 **enable password** 명령은 최고 권한 레벨을 필요로 합니다.

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

다음 예는 또 다른 명령인 **configure** 명령을 보여주는데, 여기서는 **mode** 키워드를 사용합니다.

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

참고 이 마지막 줄은 **configure terminal** 명령에 사용됩니다.

TACACS+ 서버의 명령 구성

Cisco Secure ACS(Access Control Server) TACACS+ 서버의 명령을 어떤 그룹 또는 개별 사용자를 위한 공유 프로필 구성 요소로 구성할 수 있습니다. 타사 TACACS+ 서버의 경우 명령 권한 부여 지원에 대한 자세한 내용은 서버 설명서를 참조하십시오.

Cisco Secure ACS Version 3.1의 명령 구성에 대한 다음 지침을 참조하십시오. 그중 상당수는 타사 서버에도 적용됩니다.

- ASA에서 셸 명령으로 권한 부여될 명령을 보냅니다. 즉 TACACS+ 서버의 명령을 셸 명령으로 구성합니다.

  참고 Cisco Secure ACS는 "pix-shell"이라는 명령 유형을 포함할 수 있습니다. ASA 명령 권한 부여를 위해 이 유형을 사용하지 마십시오.

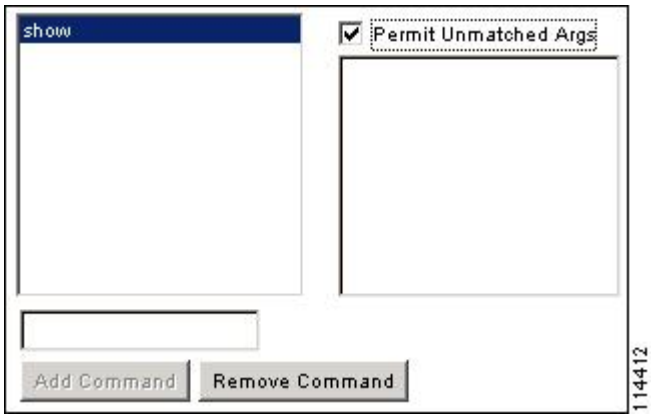
- 이 명령의 첫 단어를 주 명령으로 간주합니다. 모든 추가 단어는 인수로 간주하는데, 앞에 **permit** 또는 **deny**를 붙여야 합니다.

  예를 들어, **show running-configuration aaa-server** 명령을 허용하려면 command 필드에 **show running-configuration**을 추가하고 인수 필드에 **permit aaa-server**를 입력합니다.

- **Permit Unmatched Args(**일치하지 않는 인수**)** 확인란을 선택하면 명시적으로 거부하지 않은 명령의 모든 인수를 허용할 수 있습니다.

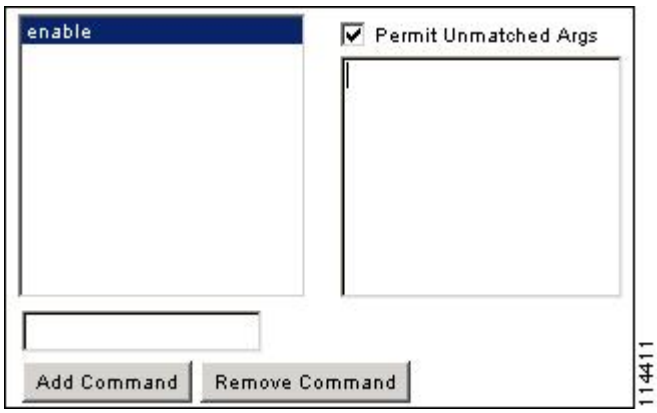
  예를 들어, **show** 명령만 구성할 수 있으며, 그러면 모든 **show** 명령이 허용됩니다. 이 방법을 사용하는 것이 좋습니다. 그러면 약어와 물음표(CLI 사용법 표시)를 비롯하여 명령의 모든 버전을 예상할 필요 없습니다(다음 그림 참조).

그림 *67:* 모든 관련 명령 허용



- 하나의 단어인 명령에 대해서는 반드시 일치하지 않음 인수를 허용해야 합니다. **enable**, **help**처럼 인수가 없는 경우도 해당됩니다(다음 그림 참조).

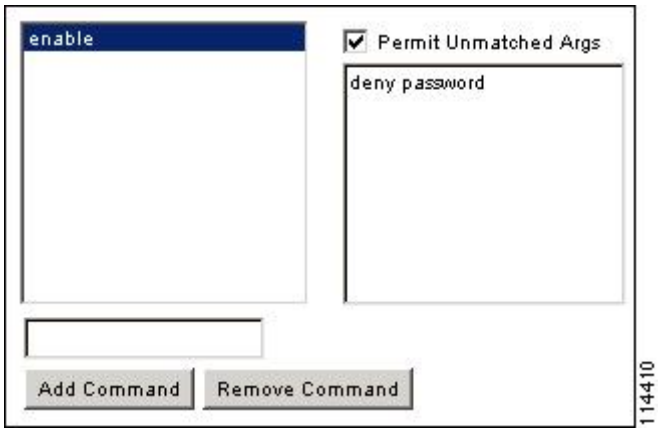
  그림 *68:* 단일 단어 명령 허용



- 일부 인수를 허용하지 않으려면 그 인수 앞에 **deny**를 입력합니다.

  예를 들어, **enable**을 허용하되 **enable password**는 허용하지 않으려면 명령 필드에 **enable**을 입력하고 인수 필드에 **deny password**라고 입력합니다. 반드시 **Permit Unmatched Args(**일치하지 않는 인수 허용**)** 확인란을 선택하여 **enable**만 계속 허용되게 해야 합니다(다음 그림 참조).

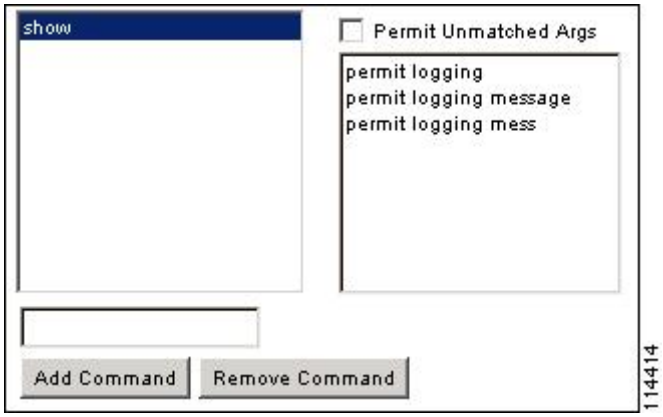
그림 ***69:*** 인수를 허용하지 않기



- 명령줄에서 어떤 명령을 축약하면 ASA는 접두사와 주 명령을 전체 텍스트로 확장합니다. 그러나 추가 인수는 입력하는 대로 TACACS+ 서버에 보냅니다.

  예를 들어, **sh log**를 입력하면 ASA에서는 전체 명령, 즉 **show logging**을 TACACS+ 서버에 보냅니다. 그러나 **sh log mess**를 입력하면 ASA는 확장된 명령인 **show logging message**가 아닌 **show logging mess**를 TACACS+ 서버에 보냅니다. 약어를 예상하여 동일 인수의 여러 철자를 구성할 수 있습니다(다음 그림 참조).

  그림 ***70:*** 약어 지정



- 모든 사용자에게 다음 기본 명령을 허용하는 것이 좋습니다.
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

TACACS+ 명령 권한 부여 구성

TACACS+ 명령 권한 부여를 활성화한 경우 어떤 사용자가 CLI에서 명령을 입력하면 ASA에서는 TACACS+ 서버에 명령과 사용자 이름을 보내 권한 부여된 명령인지 확인합니다.

TACACS+ 명령 권한 부여를 활성화하려면 먼저 TACACS+ 서버에 정의된 사용자로 ASA에 로그인해야 하며 ASA 구성을 계속 진행하는 데 필요한 명령 권한이 있어야 합니다. 예를 들어, 모든 명령 권한을 갖는 관리 사용자로 로그인해야 합니다. 그러지 않으면 뜻하지 않게 잠기게 될 수 있습니다.

원하는 대로 구성이 작동할 때까지는 구성을 저장하지 마십시오. 실수로 잠긴 경우 대개는 ASA를 다시 시작하면 액세스를 복구할 수 있습니다.

TACACS+ 시스템이 확실히 안정적이고 신뢰할 수 있는지 확인합니다. 필요한 레벨의 신뢰도에 이르기 위해서는 일반적으로 완전 이중 TACACS+ 서버 시스템이 있고 ASA와 완전 이중 방식으로 연결되어야 합니다. 예를 들어, TACACS+ 서버 풀에서 인터페이스 1과 연결된 서버 1대와 인터페이스 2와 연결된 또 다른 서버를 포함합니다. TACACS+ 서버를 사용할 수 없을 경우를 위한 장애 조치로 로컬 명령 권한 부여를 구성할 수도 있습니다.

TACACS+ 서버를 사용하여 명령 권한 부여를 구성하려면 다음 단계를 수행하십시오.

프로시저

다음의 명령을 입력합니다.

aaa authorization command *tacacs+_server_group* [**LOCAL**]

예제**:**

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

ASA에서 TACACS+ 서버를 사용할 수 없을 때 로컬 데이터베이스를 폴백 방법으로 사용하도록 구성할 수 있습니다. 폴백을 활성화하려면 **LOCAL** 다음에 서버 그룹 이름을 지정합니다(**LOCAL**은 대/소문자 구분). 로컬 데이터베이스에서 TACACS+ 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다. 반드시 로컬 데이터베이스의 사용자와 명령 권한 수준을 구성해야 합니다.

로컬 데이터베이스 사용자를 위한 비밀번호 정책 구성

로컬 데이터베이스를 사용하여 CLI 또는 ASDM 액세스를 위한 인증을 구성할 때, 일정한 시간이 지나면 사용자가 비밀번호를 변경해야 하고 최소 길이, 변경된 문자의 최소 개수와 같은 비밀번호 기준의 준수를 요구하는 비밀번호 정책을 구성할 수 있습니다.

비밀번호 정책은 로컬 데이터베이스를 사용하는 관리 사용자에게만 적용됩니다. 로컬 데이터베이스를 사용할 수 있는 기타 트래픽 유형(예: 네트워크 액세스를 위한 VPN 또는 AAA) 및 AAA 서버에서 인증한 사용자에게는 적용되지 않습니다.

비밀번호 정책을 구성한 다음 (본인의 또는 다른 사용자의) 비밀번호를 변경할 때 비밀번호 정책이 새 비밀번호에 적용됩니다. 기존 비밀번호는 상위 계층에서 상속 받습니다. 새 정책은 **username** 명령 및 **change-password** 명령을 사용하여 비밀번호를 변경하는 경우에 적용됩니다.

시작하기 전에

- 로컬 데이터베이스를 사용하여 CLI 또는 ASDM 액세스를 위해 AAA 인증을 구성합니다.
- 로컬 데이터베이스에 사용자 이름을 지정합니다.

프로시저

단계 **1** (선택사항) 원격 사용자에 대해 비밀번호가 만료된 이후의 날짜 간격을 설정합니다.

password-policy lifetime 일

예제**:**

```
ciscoasa(config)# password-policy lifetime 180
```

참고 콘솔 포트에서 사용자가 비밀번호 만료 때문에 절대로 잠기지 않습니다.

유효한 값의 범위는 0~65536일입니다. 기본값은 0일입니다. 즉 비밀번호가 절대 만료되지 않습니다.

비밀번호가 만료되기 7일 전에 경고 메시지가 나타납니다. 비밀번호가 만료되면 원격 사용자는 시스템 액세스가 거부됩니다. 만료 후 액세스 권한을 얻으려면 다음 중 하나를 수행합니다.

- 다른 관리자가 **username** 명령을 사용하여 비밀번호를 변경하게 합니다.
- 물리적 콘솔 포트에 로그인하여 비밀번호를 변경합니다.

단계 **2** (선택사항) 새 비밀번호에서 기존 비밀번호와 다르게 해야 할 문자의 최소 개수를 설정합니다.

password-policy minimum-changes *value*

예제**:**

```
ciscoasa(config)# password-policy minimum-changes 2
```

유효한 값의 범위는 0~64자입니다. 기본값은 0입니다.

문자 일치는 위치와 상관없습니다. 즉 새 비밀번호 문자가 기존 비밀번호의 어느 위치에도 없어야 변경된 것으로 간주됩니다.

단계 **3** (선택사항) 비밀번호의 최소 길이를 설정합니다.

password-policy minimum-length 값

예제**:**

```
ciscoasa(config)# password-policy minimum-length 8
```

유효한 값의 범위는 3~64자입니다. 권장되는 비밀번호 최소 길이는 8자입니다.

단계 **4** (선택사항) 비밀번호에 포함해야 할 대문자의 최소 개수를 설정합니다.

password-policy minimum-uppercase 값

예제**:**

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

유효한 값의 범위는 0~64자입니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.

단계 **5** (선택사항) 비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다.

password-policy minimum-lowercase 값

예제**:**

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

유효한 값의 범위는 0~64자입니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.

단계 **6** (선택사항) 비밀번호에 포함해야 할 숫자의 최소 개수를 설정합니다.

password-policy minimum-numeric *value*

예제**:**

```
ciscoasa(config)# password-policy minimum-numeric 1
```

유효한 값의 범위는 0~64자입니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.

단계 **7** (선택사항) 비밀번호에 포함해야 할 특수 문자의 최소 개수를 설정합니다.

password-policy minimum-special 값

예제**:**

```
ciscoasa(config)# password-policy minimum-special 2
```

유효한 값의 범위는 0~64자입니다. 특수 문자에는 !, @, #, $, %, ^, &, *, '(' 및 ')'가 포함됩니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.

단계 **8** 비밀번호 재사용을 금지합니다.

password-policy reuse-interval 값

예제**:**

```
ciscoasa(config)# password-policy reuse-interval 5
```

2~7개의 이전 비밀번호에서 이전에 사용한 비밀번호와 일치하는 비밀번호의 재사용을 금지할 수 있습니다. 이전 비밀번호는 **password-history** 명령을 사용하여 암호화된 형식으로 각 사용자 이름 아래의 구성에 저장되어 있습니다. 이 명령은 사용자가 구성할 수 없습니다.

단계 **9** 사용자 이름과 일치하는 비밀번호를 금지합니다.

password-policy username-check

단계 **10** (선택 사항) 사용자가 **username** 명령으로 비밀번호를 변경하는 것을 허용하지 않고 반드시 **change-password** 명령으로 비밀번호를 변경하게 할 것인지 설정합니다.

password-policy authenticate enable

예제**:**

```
ciscoasa(config)# password-policy authenticate enable
```

기본 설정은 disabled입니다. 즉 사용자는 두 방법 중 어느 쪽이든 사용하여 비밀번호를 변경할 수 있습니다.

이 기능을 활성화한 경우, **username** 명령으로 비밀번호를 변경하려고 시도하면 다음 오류 메시지가 나타납니다.

```
ERROR: Changing your own password is prohibited
```

또한 **clear configure username** 명령으로 자신의 어카운트를 삭제할 수 없습니다. 시도하면 다음 오류 메시지가 나타납니다.

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

비밀번호 변경

비밀번호 정책에서 비밀번호 수명을 구성한 경우, 기존 비밀번호가 만료되면 비밀번호를 새로운 비밀번호로 변경해야 합니다. 이 비밀번호 변경 방법은 비밀번호 정책 인증을 활성화한 경우 필요합니다. 비밀번호 정책 인증이 활성화되지 않은 경우에는 이 방법을 사용하거나 사용자 어카운트를 직접 변경할 수 있습니다.

사용자 이름 비밀번호를 변경하려면 다음 단계를 수행하십시오.

프로시저

다음의 명령을 입력합니다.

change-password [**old-password** *old_password* [**new-password** *new_password*]]

예제**:**

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

명령에 기존 비밀번호와 새 비밀번호를 입력하지 않으면 ASA에서는 입력하라는 메시지를 표시합니다.

로그인 기록 활성화 및 보기

기본적으로 로그인 기록은 90일 동안 저장됩니다. 이 기능을 비활성화하거나 최대 365일로 기간을 변경할 수 있습니다.

시작하기 전에

- 로그인 기록은 유닛별로만 저장되며 페일오버 및 클러스터링 환경에서 각 유닛은 고유한 로그인 기록만 유지합니다.
- 로그인 기록 데이터는 다시 로드를 통해 유지되지 않습니다.
- 이 기능은 하나 이상의 CLI 관리 방법(SSH, 텔넷, 시리얼 콘솔)에 대해 로컬 AAA 인증을 활성화하는 경우 로컬 데이터베이스 또는 AAA 서버의 사용자 이름에 적용됩니다. ASDM 로그인은 기록에 저장되지 않습니다.

프로시저

단계 **1** 로그인 기록의 기간을 설정합니다.

aaa authentication login-history duration 일

예제**:**

```
ciscoasa(config)# aaa authentication login-history duration 365
```

1~365 사이의 일을 설정할 수 있습니다. 기본값은 90입니다. 로그인 기록을 비활성화하려면 **no aaa authentication login-history**를 입력합니다.

사용자가 로그인할 때 자신의 로그인 기록(예: 이 SSH 예)을 확인합니다.

```
cugel@10.86.194.108's password:
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
```

```
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

단계 **2** 로그인 기록을 확인합니다.

show aaa login-history [**user** *name*]

예제**:**

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
```

관리 액세스 어카운팅 구성

CLI에서 **show** 명령이 아닌 임의의 명령을 입력할 때 TACACS+ 어카운팅 서버에 어카운팅 메시지를 보낼 수 있습니다. 사용자가 로그인할 때, 사용자가 **enable** 명령을 입력할 때 또는 사용자가 명령을 실행할 때 어카운팅을 구성할 수 있습니다.

명령 어카운팅에는 TACACS+ 서버만 사용할 수 있습니다.

관리 액세스를 구성하고 명령 어카운팅을 활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 다음의 명령을 입력합니다.

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

예제**:**

```
ciscoasa(config)# aaa accounting telnet console group_1
```

유효한 서버 그룹 프로토콜은 RADIUS와 TACACS+입니다.

단계 **2** 명령 어카운팅을 활성화합니다. TACACS+ 서버만 명령 어카운팅을 지원합니다.

aaa accounting command [**privilege** *level*] *server-tag*

예제**:**

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

privilege *level* 키워드 인수 쌍은 최소 권한 레벨이며 *server-tag* 인수는 TACACS+ 서버 그룹의 이름입니다. ASA에서 이 서버 그룹에 명령 어카운팅 메시지를 보내야 합니다.

잠금에서 복구

명령 권한 부여 또는 CLI 인증을 활성화할 때 ASA CLI에서 잠기는 경우가 있습니다. 대개는 ASA를 다시 시작하여 액세스를 복구할 수 있습니다. 그러나 이미 구성을 저장한 경우 잠길 수 있습니다.

다음 표에서는 대표적인 잠금 조건과 잠금으로부터 복구하는 방법을 소개합니다.

표 ***48: CLI*** 인증 및 명령 권한 부여 잠금 시나리오

기능	잠금 조건	설명	해결 방법: 단일 모드	해결 방법: 다중 모드
로컬 CLI 권한 부여	로컬 데이터베이스에 어떤 사용자도 구성되지 않았습니다.	로컬 데이터베이스에 사용자가 없을 경우 로그인할 수 없고 어떤 사용자도 추가할 수 없습니다.	로그인하고 비밀번호 및 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 영역에서 상황으로 변경하고 사용자를 추가할 수 있습니다.
TACACS+ 명령 권한 부여 TACACS+ CLI 인증 RADIUS CLI 인증	서버가 중지했거나 연결 불가한 상태이며, 구성된 장애 조치가 없습니다.	서버가 연결 불가한 상태라면 로그인할 수 없고 어떤 명령도 입력할 수 없습니다.	**1.** 로그인하고 비밀번호 및 AAA 명령을 재설정합니다. **2.** 로컬 데이터베이스를 장애 조치로 구성하여 서버가 중지하더라도 잠기지 않게 합니다.	**1.** ASA에서 네트워크 구성이 올바르지 않아 서버 연결이 불가할 경우 스위치에서 ASA로 세션 연결을 수행합니다. 시스템 실행 영역에서 상황으로 변경하고 네트워크 설정을 재구성할 수 있습니다. **2.** 로컬 데이터베이스를 장애 조치로 구성하여 서버가 중지하더라도 잠기지 않게 합니다.
TACACS+ 명령 권한 부여	충분한 권한이 없는 사용자 또는 존재하지 않는 사용자로 로그인한 상태입니다.	명령 권한 부여를 활성화했지만, 해당 사용자가 더 이상 어떤 명령도 입력할 수 없음을 알게 되었습니다.	TACACS+ 서버 사용자 어카운트의 문제를 해결합니다. TACACS+ 서버에 대한 액세스 권한이 없는데 즉시 ASA를 구성해야 하는 경우, 유지보수 파티션으로 로그인하고 비밀번호와 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 공간에서 상황으로 변경하고 구성 변경 사항을 완료할 수 있습니다. 또한 TACACS+ 구성의 문제를 해결할 때까지 명령 권한 부여를 비활성화할 수도 있습니다.

기능	잠금 조건	설명	해결 방법: 단일 모드	해결 방법: 다중 모드
로컬 명령 권한 부여	충분한 권한이 없는 사용자로 로그인했습니다.	명령 권한 부여를 활성화했지만, 해당 사용자가 더 이상 어떤 명령도 입력할 수 없음을 알게 되었습니다.	로그인하고 비밀번호 및 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 공간에서 상황으로 변경하고 사용자 수준을 변경할 수 있습니다.

디바이스 액세스 모니터링

디바이스 액세스 모니터링에 대한 내용은 다음 명령을 참고하십시오.

- **show running-config all privilege all**

  이 명령은 모든 명령에 대한 권한 수준을 보여 줍니다.

  show running-config all privilege all 명령의 경우, ASA는 현재 각 CLI 명령에 어떤 권한 레벨이 할당되었는지 표시합니다. 다음은 이 명령 출력의 샘플입니다.

```
ciscoasa(config)# show running-config all  privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** 레벨

  이 명령은 특정 권한 수준에 대한 명령을 보여 줍니다. level 인수는 0~15의 정수입니다.

  다음 예는 권한 수준 10의 명령 할당을 보여 줍니다.

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** 명령

  이 명령은 특정 명령의 권한 수준을 보여 줍니다.

  다음 예는 **access-list** 명령의 명령 할당을 보여 줍니다.

```
ciscoasa(config)# show running-config all privilege command access-list
```

```
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  이 명령은 현재 로그인한 사용자를 보여 줍니다.

  다음은 **show curpriv** 명령의 샘플 출력입니다.

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

  다음 표는 **show curpriv** 명령 출력을 설명합니다.

  표 ***49: show curpriv*** 명령 출력 설명

필드	설명
사용자 이름	사용자 이름 기본 사용자로 로그인할 경우 이름은 enable_1(사용자 EXEC) 또는 enable_15(특별 권한 EXEC)입니다.
Current privilege level	수준은 0부터 15까지입니다. 로컬 명령 권한 부여를 구성하고 중간 권한 수준에 명령을 할당하지 않는 한, 수준 0과 15만 사용됩니다.
현재 모드	사용 가능한 액세스 모드는 다음과 같습니다. • P_UNPR—사용자 EXEC 모드(수준 0과 1) • P_PRIV—특별 권한 EXEC 모드(수준 2~15) • P_CONF—구성 모드

- **show quota management-session**

  이 명령은 사용 중인 현재 세션을 보여 줍니다.

  다음은 **show quota management-session** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show quota management-session

quota management-session limit 3
quota management-session warning level 2
quota management-session level 0
quota management-session high water 2
quota management-session errors 0
quota management-session warnings 0
```

- **show aaa login-history** [**user** *name*]

이 명령은 사용자당 로그인 기록을 보여 줍니다.

다음은 **show aaa login-history** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
```

관리 액세스 기록

표 ***50:*** 관리 액세스 기록

기능 이름	플랫폼 릴리스	설명
RSA 키 쌍의 3072비트 키 지원	9.9(2)	이제 모듈러스 크기를 3072로 설정할 수 있습니다. 신규 또는 수정된 명령: **crypto key generate rsa modulus**
BVI(Bridged Virtual Interfaces)에서의 VPN 관리 액세스	9.9(2)	VPN **management-access**가 BVI에서 활성화된 경우 이제 관리 서비스(**telnet**, **http**, **ssh** 등)를 BVI에서 활성화할 수 있습니다. 비 VPN 관리 액세스를 위해 브리지 그룹 멤버 인터페이스에서 이러한 서비스를 구성하려면 계속 진행해야 합니다. 신규 또는 수정된 명령: **https**, **telnet**, **ssh**, **management-access**

기능 이름	플랫폼 릴리스	설명
SSH 공개 키 인증을 사용하는 사용자와 비밀번호를 사용하는 사용자에 대한 개별 인증	9.6(3)/9.8(1)	9.6(2) 이전 릴리스에서는 로컬 사용자 데이터베이스(**aaa authentication ssh console LOCAL**)에서 AAA SSH 인증을 명시적으로 활성화하지 않고도 SSH 공개 키 인증(**ssh authentication**)을 활성화할 수 있습니다. 9.6(2)에서 ASA는 AAA SSH 인증을 명시적으로 활성화하도록 요구했습니다. 이 릴리스에서는 더 이상 AAA SSH 인증을 명시적으로 활성화할 필요가 없습니다. 즉 **ssh authentication** 명령을 사용자에 대해 구성할 때 이 유형의 인증을 사용하는 사용자에 대해 기본적으로 로컬 인증이 활성화됩니다. 게다가 AAA SSH 인증을 명시적으로 구성하는 경우, 이 구성은 비밀번호를 사용하는 사용자 이름에만 적용되며 모든 AAA 서버 유형(예: **aaa authentication ssh console radius_1**)을 사용할 수 있습니다. 예를 들어, 일부 사용자는 로컬 데이터베이스를 사용하여 공개 키 인증을 사용할 수 있으며 다른 사용자는 RADIUS에서 비밀번호를 사용할 수 있습니다. 명령은 수정하지 않았습니다.
로그인 기록	9.8(1)	기본적으로 로그인 기록은 90일 동안 저장됩니다. 이 기능을 비활성화하거나 최대 365일로 기간을 변경할 수 있습니다. 하나 이상의 관리 방법(SSH, ASDM, 텔넷 등)에 대해 로컬 AAA 인증을 활성화하면 이 기능은 로컬 데이터베이스의 사용자 이름에만 적용됩니다. 다음 명령을 도입했습니다. **aaa authentication login-history, show aaa login-history**

기능 이름	플랫폼 릴리스	설명
비밀번호의 재사용을 금지하고 사용자 이름과 일치하는 비밀번호의 사용을 금지하기 위한 비밀번호 정책 시행	9.8(1)	이제 최대 7번 생성하는 동안 이전 비밀번호를 재사용하는 것을 금지할 수 있으며 사용자 이름과 일치하는 비밀번호를 사용하는 것을 금지할 수도 있습니다. 다음 명령을 도입했습니다. **password-history, password-policy reuse-interval, password-policy username-check**
ASDM에 대한 ASA SSL 서버 모드 일치	9.6(2)	인증서로 인증하는 ASDM 사용자를 대상으로, 이제 인증서 맵과 일치하는 인증서를 요구할 수 있습니다. 다음 명령을 수정했습니다. **http authentication-certificate match**
SSH 공개 키 인증 개선 사항	9.6(2)	이전 릴리스에서는 로컬 사용자 데이터베이스 (**aaa authentication ssh console LOCAL**)에서 AAA SSH 인증을 활성화하지 않고도 SSH 공개 키 인증(**ssh authentication**)을 활성화할 수 있었습니다. 이제 AAA SSH 인증을 명시적으로 활성화해야 하는 것으로 구성이 수정되었습니다. 사용자가 개인 키 대신 비밀번호를 사용하는 것을 허용하지 않기 위해 이제 정의된 비밀번호 없이 사용자 이름을 생성할 수 있습니다. 다음 명령을 수정했습니다. **ssh authentication, username**
ASDM 관리 권한 부여	9.4(1)	텔넷 및 SSH 액세스와 별도로 HTTP 액세스에 대해 관리 권한 부여를 구성할 수 있습니다. 다음 명령을 도입했습니다. **aaa authorization http console**
인증서 구성의 ASDM 사용자 이름	9.4(1)	ASDM 인증서 인증을 활성화하면(**http authentication-certificate**) ASDM에서 인증서로부터 사용자 이름을 추출하는 방식을 구성할 수 있습니다. 또한 로그인 프롬프트에 사용자 이름 미리 채우기를 활성화할 수도 있습니다. 다음 명령을 도입했습니다. **http username-from-certificate**

기능 이름	플랫폼 릴리스	설명
일회용 비밀번호 인증 향상	9.2(1)	충분한 권한이 있는 관리자는 인증 자격 증명을 한 번 입력하면 특별 권한 EXEC 모드에 들어갈 수 있습니다. **auto-enable** 옵션이 **aaa authorization exec** 명령에 추가되었습니다. 다음 명령을 수정했습니다. **aaa authorization exec**.
IPv6에 대한 HTTP 리디렉션 지원	9.1(7)/9.6(1)	ASDM 액세스 또는 클라이언트리스 SSL VPN에 대해 HTTPS로의 HTTP 리디렉션을 활성화할 때 이제 IPv6 주소로 전송된 트래픽을 리디렉션할 수 있습니다. 다음 명령에 기능을 추가했습니다. **http redirect**
구성 가능한 SSH 암호화 및 무결성 암호	9.0/9.5(3)/9.6 (1)	사용자는 SSH 암호화 관리를 수행할 때 암호화 모드를 선택할 수 있으며 다양한 키 교환 알고리즘을 위해 HMAC 및 암호화를 구성할 수 있습니다. 애플리케이션에 따라 암호를 더 엄격하게 또는 덜 엄격하게 변경할 수 있습니다. 보안 사본의 성능은 사용되는 암호화 암호에 따라 부분적으로 달라집니다. 기본적으로 ASA에서는 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr 알고리즘 중 하나를 순서대로 협상합니다. 제안된 첫 번째 알고리즘(3des-cbc)을 선택하는 경우, 성능이 aes128-cbc와 같은 더 효율적인 알고리즘보다 훨씬 느려집니다. 제안된 암호를 변경하려면 예를 들어 **ssh cipher encryption custom aes128-cbc**를 사용하십시오. 다음 명령을 도입했습니다. **ssh cipher encryption, ssh cipher integrity**.
SSH를 위한 AES-CTR 암호화	9.1(2)	ASA의 SSH 서버 구현에서 이제 AES-CTR 모드 암호화를 지원합니다.

기능 이름	플랫폼 릴리스	설명
SSH rekey 간격 향상	9.1(2)	SSH 연결은 연결 시간이 60분이 지났거나 데이터 트래픽이 1GB를 초과하면 키가 다시 생성됩니다. 다음 명령을 도입했습니다. **show ssh sessions detail**
다중 상황 모드의 ASASM에서는 스위치로부터의 텔넷 및 가상 콘솔 인증을 지원합니다.	8.5(1)	다중 상황 모드의 스위치에서 ASASM으로의 연결이 시스템 실행 영역으로 연결되지만, 관리 상황에서 이러한 연결에 적용할 인증을 구성할 수 있습니다.
로컬 데이터베이스를 사용할 때 관리자 비밀번호 정책 지원	8.4(4.1), 9.1(2)	로컬 데이터베이스를 사용하여 CLI 또는 ASDM 액세스를 위한 인증을 구성할 때, 일정한 시간이 지나면 사용자가 비밀번호를 변경해야 하고 최소 길이, 변경된 문자의 최소 개수와 같은 비밀번호 기준의 준수를 요구하는 비밀번호 정책을 구성할 수 있습니다. 다음 명령을 도입했습니다. **change-password**, **password-policy lifetime**, **password-policy minimum changes**, **password-policy minimum-length**, **password-policy minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minimum-numeric**, **password-policy minimum-special**, **password-policy authenticate enable**, **clear configure password-policy**, **showrunning-config password-policy**.
SSH 공개 키 인증 지원	8.4(4.1), 9.1(2)	사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증을 활성화할 수 있습니다. PKF 형식의 키 또는 Base64 키를 지정할 수 있습니다. PKF 키는 최대 4096비트입니다. ASA의 Base64 형식 지원 범위(최대 2048비트)보다 너무 큰 키에는 PKF 형식을 사용합니다. We introduced the following commands: **ssh authentication**. *PKF 키 형식은 9.1(2) 이상에서만 지원됩니다.*

기능 이름	플랫폼 릴리스	설명
SSH 키 교환에 Diffie-Hellman 그룹 14 지원	8.4(4.1), 9.1(2)	SSH 키 교환을 위한 Diffie-Hellman 그룹 14 지원이 추가되었습니다. 이전에는 그룹 1만 지원되었습니다. 다음 명령을 도입했습니다. **ssh key-exchange**.
관리 세션 최대 개수 지원	8.4(4.1), 9.1(2)	동시 ASDM, SSH, 텔넷 세션의 최대 개수를 설정할 수 있습니다. 다음 명령을 도입했습니다. **quota management-session**, **show running-config quota management-session**, **show quota management-session**.
SSH 보안이 강화되었습니다. SSH 기본 사용자 이름은 더 이상 지원되지 않습니다.	8.4(2)	8.4(2)부터는 pix 또는 asa 사용자 이름 및 로그인 비밀번호를 사용하여 SSH를 통해 ASA에 연결할 수 없습니다. SSH를 사용하려면 **aaa authentication ssh console LOCAL** 명령(CLI)을 사용하거나 Configuration(구성(> Device Management(디바이스 관리) > Users/AAA(사용자/AAA) > AAA Access(AAA 액세스) > Authentication(ASDM)(인증(ASDM))을 사용하여 AAA 인증을 구성해야 합니다. 그런 다음 **username** 명령(CLI)을 입력하거나 Configuration(구성) > Device Management(디바이스 관리)> Users/AAA(사용자/AAA) > User Accounts(ASDM)(사용자 어카운트(ASDM))를 사용하여 로컬 사용자를 정의합니다. 로컬 데이터베이스 대신에 AAA 서버를 인증에 사용하려는 경우, 만일에 대비하여 로컬 인증도 구성하는 것이 좋습니다.

기능 이름	플랫폼 릴리스	설명
관리 액세스	7.0(1)	이 기능을 도입했습니다. 다음 명령을 도입했습니다. **show running-config all privilege all**, **show running-config privilege level**, **show running-config privilege command**, **telnet**, **telnet timeout**, **ssh**, **ssh timeout**, **http**, **http server enable**, **asdm image disk, banner**, **console timeout**, **icmp**, **ipv6 icmp**, **management access**, **aaa authentication console**, **aaa authenticationenable console**, **aaa authentication telnet | ssh console**, **service-type**, **login**, **privilege**, **aaa authentication exec authentication-server**, **aaa authentication command LOCAL**, **aaa accounting serial | telnet | ssh | enable console**, **show curpriv**, **aaa accounting command privilege**.

38 장

소프트웨어 및 컨피그레이션

이 장에서는 Cisco ASA 소프트웨어 및 구성을 관리하는 방법을 설명합니다.

소프트웨어 업그레이드

전체 업그레이드 절차에 대한 내용은 Cisco ASA 업그레이드 가이드를 참고하십시오.

ROMMON을 사용하여 이미지 로드

ROMMON을 사용하여 새 이미지를 로드할 수 있습니다.

ROMMON을 사용하여 ASA 5500-X Series의 이미지 로드

TFTP를 사용하여 ROMMON 모드에서 ASA로 소프트웨어 이미지를 로드하려면 다음 단계를 수행하십시오.

프로시저

단계 1 또는 어플라이언스 콘솔 액세스, 13 페이지의 지침에 따라 ASA 콘솔 포트에 연결합니다.

단계 **2** ASA의 전원을 끈 후 전원을 켭니다.

단계 **3** 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

단계 **4** ROMMOM 모드에서 다음과 같이 ASA에 대한 인터페이스 설정을 정의합니다. 여기에는 IP 주소, TFTP 서버 주소, 게이트웨이 주소, 소프트웨어 이미지 파일, 포트 등이 포함됩니다.

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

참고 네트워크에 연결된 상태여야 합니다.

interface 명령은 ASA 5506-X, ASA 5508-X 및 ASA 5516-X 플랫폼에서 무시되므로 관리 1/1 인터페이스의 해당 플랫폼에서 TFTP 복구를 수행해야 합니다.

단계 **5** 설정을 검증합니다.

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

단계 **6** TFTP 서버를 ping합니다.

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

단계 **7** 나중에 사용하기 위해 네트워크 설정을 저장합니다.

```
rommon #8> sync
Updating NVRAM Parameters...
```

단계 **8** 소프트웨어 이미지를 로드합니다.

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
```

```
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

소프트웨어 이미지가 성공적으로 로드되면 ASA는 자동으로 ROMMON 모드를 종료합니다.

단계 **9** ROMMON 모드에서 ASA를 부팅해도 다시 로드를 통해 시스템 이미지가 보존되지 않습니다. 플래시 메모리에 이미지를 계속해서 다운로드해야 합니다. 소프트웨어 업그레이드, 1157 페이지를 참조하십시오.

ROMMON을 사용하여 ASASM의 이미지 로드

TFTP를 사용하여 ROMMON 모드에서 ASASM으로 소프트웨어 이미지를 로드하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 또는 ASA 서비스 모듈 콘솔 액세스, 18 페이지의 지침에 따라 ASA 콘솔 포트에 연결합니다.

단계 **2** ASASM 이미지를 다시 로드해야 합니다.

단계 **3** 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

단계 **4** ROMMOM 모드에서 다음과 같이 ASASM에 대한 인터페이스 설정을 정의합니다. 여기에는 IP 주소, TFTP 서버 주소, 게이트웨이 주소, 소프트웨어 이미지 파일, 포트, VLAN 등이 포함됩니다.

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
rommon #5> interface Data0
rommon #6> vlan 1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

참고 네트워크에 연결된 상태여야 합니다.

단계 **5** 설정을 검증합니다.

```
rommon #7> set
ROMMON Variable Settings:
```

```
  ADDRESS=10.86.118.4
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

단계 **6** TFTP 서버를 ping합니다.

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

단계 **7** 소프트웨어 이미지를 로드합니다.

```
rommon #9> tftpdnld
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
Starting download. Press ESC to abort.
```

소프트웨어 이미지가 성공적으로 로드되면 ASASM은 자동으로 ROMMON 모드를 종료합니다.

단계 **8** ROMMON 모드에서 모듈을 부팅해도 다시 로드를 통해 시스템 이미지가 보존되지 않습니다. 플래시 메모리에 이미지를 계속해서 다운로드해야 합니다. 소프트웨어 업그레이드, 1157 페이지를 참조하십시오.

ROMMON 이미지 업그레이드(ASA 5506-X, 5508-X 및 5516-X)

ASA 5506-X Series, ASA 5508-X 및 ASA 5516 X용 ROMMON 이미지를 업그레이드하려면 아래 단계를 수행합니다.

시작하기 전에

새 버전으로 업그레이드만 가능하며 다운그레이드할 수 없습니다. 현재 버전을 보려면 **show module** 명령을 입력하고 MAC 주소 범위 테이블의 Mod 1에 대한 출력에서 Fw 버전을 확인하십시오.

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

프로시저

단계 **1** Cisco.com에서 새 ROMMON 이미지를 가져와 ASA에 복사할 서버에 둡니다. 이 절차에서는 TFTP 복사에 대해 설명합니다.

다음 위치에서 이미지를 다운로드합니다.

https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

단계 **2** ASA 플래시 메모리에 ROMMON 이미지를 복사합니다.

copy tftp://*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

단계 **3** ROMMON 이미지를 업그레이드합니다.

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

예제:

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
```

```
Proceed with reload? [confirm]
```

단계 **4** 프롬프트가 표시되면 ASA 다시 로드를 확인합니다.

ASA가 ROMMON 이미지를 업그레이드한 다음 ASA OS를 다시 로드합니다.

ASA 5506W-X Wireless Access Point용 이미지 복구 및 로드

TFTP를 사용하여 ASA 5506W-X에서 소프트웨어 이미지를 복구하고 로드하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 액세스 포인트(AP)에 대한 세션 및 AP ROMMON(ASA ROMMON 아님)을 입력합니다.

```
ciscoasa# hw-module module wlan recover image
```

단계 **2** Cisco Aironet 액세스 포인트의 Cisco IOS 소프트웨어 구성 가이드의 절차를 따르십시오.

소프트웨어 다운그레이드

다운그레이드 기능을 사용하면 다음 기능을 간단하게 완수할 수 있습니다.

- 부트 이미지 구성 지우기(**clear configure boot**).
- 부트 이미지를 기존 이미지가 되게 설정(**boot system**).
- (선택 사항) 새 액티베이션 키 입력(**activation-key**).
- 실행 중인 구성을 시작에 저장(**write memory**). 이는 BOOT 환경 변수를 기존 이미지로 설정합니다. 따라서 다시 로드할 때 기존 이미지가 로드됩니다.
- 이전 구성을 시작 구성에 복사(**copy old_config_url startup-config**).
- 다시 로드(**reload**).

시작하기 전에

- 클러스터링에 대해 공식적인 제로 다운타임 다운그레이드 지원이 없습니다. 그러나 일부 경우에서 제로 다운타임 다운그레이드가 작동합니다. 다운그레이드에 대해 다음의 알려진 문제를 참고하십시오. 클러스터 유닛을 다시 로드해야 하는 다른 문제가 있을 수 있으므로 다운타임이 발생할 수 있습니다.

- 스마트 라이선싱을 위해 9.10(1)에서 다운그레이드 — 스마트 에이전트의 변경으로 인해 다운그레이드하면 Cisco Smart Software Manager에 디바이스를 다시 등록해야 합니다. 새 스마트 에이전트는 암호화된 파일을 사용하므로 이전 스마트 에이전트에서 필요로 하는 암호화되지 않은 파일을 사용하려면 다시 등록해야 합니다.
- 클러스터링을 통해 9.9(1) 이전 릴리스로 다운그레이드 — 9.9(1) 이후 버전에는 백업 배포에 개선 사항이 포함되어 있습니다. 클러스터에 3개 이상의 유닛이 있는 경우, 다음 단계를 수행해야 합니다.
  1. 클러스터에서 모든 보조 유닛을 제거합니다(따라서 클러스터가 기본 유닛으로만 구성됨).
  2. 1개의 보조 유닛을 다운그레이드하고 이를 클러스터에 다시 조인시킵니다.
  3. 기본 유닛에서 클러스터링을 비활성화하고 다운그레이드한 후 클러스터에 다시 조인시킵니다.
  4. 한 번에 하나씩 나머지 보조 유닛을 다운그레이드하고 클러스터에 다시 참가시킵니다.
- 클러스터 사이트 이중화를 활성화할 때 9.9(1) 이전 릴리스로 다운그레이드 — 다운그레이드하려면(또는 9.9(1) 이전 유닛을 클러스터에 추가하려는 경우) 사이트 이중화를 비활성화해야 합니다. 그렇지 않으면 예를 들어 이전 버전을 실행 중인 유닛의 더미 전달 플로우 같은 부작용이 나타날 수 있습니다.
- 클러스터링과 암호화 맵을 통해 9.8(1)에서 다운그레이드 — 암호화 맵이 구성되었을 때 9.8(1)에서 다운그레이드할 경우 제로 다운타임 다운그레이드 지원이 없습니다. 다운그레이드 전에 암호화 맵 구성을 지운 다음 다운그레이드 후에 이 구성을 다시 적용해야 합니다.
- 클러스터링 유닛 상태 검사가 0.3~0.7초로 설정되어 있는 9.8(1)에서 다운그레이드 — 대기 시간을 0.3~0.7초(**health-check holdtime**)로 설정한 후에 ASA 소프트웨어를 다운그레이드하는 경우, 새로운 설정이 지원되지 않으므로 이 설정은 3초의 기본값으로 되돌아갑니다.
- 클러스터링(CSCuv82933)을 통해 9.5(2) 이상 버전에서 9.5(1) 이하 버전으로 다운그레이드 — 9.5(2)에서 다운그레이드할 경우 제로 다운타임 다운그레이드는 지원되지 않습니다. 유닛이 온라인 상태로 돌아올 때 새로운 클러스터가 형성되도록 거의 동시에 모든 유닛을 다시 로드해야 합니다. 유닛을 순차적으로 다시 로드하기 위해 대기하는 경우 클러스터를 형성할 수 없습니다.
- 클러스터링을 통해 9.2(1) 이상 버전에서 9.1 이하 버전으로 다운그레이드 — 제로 다운타임 다운그레이드는 지원되지 않습니다.

- PBKDF2(비밀번호 기반 키 파생 함수 2)를 사용하여 비밀번호를 통해 9.5 이하 버전으로 다운그레이드 — 9.6 이전 버전은 PBKDF2 해싱을 지원하지 않습니다. 9.6(1)에서 32자보다 긴 **enable** 및 **username** 비밀번호는 PBKDF2 해싱을 사용합니다. 9.7(1)에서 모든 길이의 새 비밀번호는 PBKDF2 해싱을 사용합니다(기존 비밀번호는 계속해서 MD5 해싱을 사용함). 다운그레이드하는 경우, **enable** 비밀번호는 기본값(비어 있음)으로 되돌아갑니다. 사용자 이름은 정확하게 분석하지 않으며 **username** 명령은 제거됩니다. 로컬 사용자를 다시 생성해야 합니다.
- ASAv용 버전 9.5(2.200)에서 다운그레이드 — ASAv는 라이선싱 등록 상태를 유지하지 않습니다. **license smart register idtoken id_token force** 명령을 사용하여(ASDM용인 경우,

Configuration(구성**) > Device Management(**디바이스 관리**) > Licensing(**라이선싱**) > Smart Licensing(**스마트 라이선싱**)** 페이지를 참고하고 **Force registration(**강제 등록**)** 옵션 사용) 다시 등록하고 Smart Software Manager에서 ID 토큰을 얻어야 합니다.

- 구성 마이그레이션은 다운그레이드 기능에 영향을 미칠 수 있으므로 다운그레이드할 때 사용할 수 있는 이전 구성을 백업하는 것이 좋습니다. 8.3으로 업그레이드하는 경우 백업이 자동으로 생성됩니다(< old_version>_startup_cfg.sav). 다른 마이그레이션은 백업을 만들지 않습니다. 새 구성에 이전 버전에서 사용할 수 없는 명령이 포함된 경우, 구성이 로드될 때 이러한 명령에 대한 오류가 표시되지만 이 오류를 무시할 수 있습니다. 각 버전의 구성 마이그레이션 또는 중단에 대한 자세한 내용은 각 버전에 대한 업그레이드 가이드를 참고하십시오.
- VPN 터널은 스탠바이 유닛이 원래 터널이 협상했던 암호 그룹을 지원하지 않는 소프트웨어 버전을 실행 중인 경우라도 스탠바이 유닛으로 복제됩니다. 이 시나리오는 다운그레이드할 때 발생합니다. 이 경우 VPN 연결을 해제하고 다시 연결합니다.

프로시저

다음의 명령을 입력합니다.

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

예제**:**

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm 옵션을 사용하면 프롬프트 없이 다운그레이드합니다. *image_url*은 disk0, disk1, tftp, ftp 또는 smb에 있는 기존 이미지의 경로입니다. *old_config_url*은 저장된 마이그레이션 이전 구성의 경로입니다. 8.3 이전 액티베이션 키로 되돌려야 하는 경우 기존 액티베이션 키를 입력할 수 있습니다.

파일 관리

플래시 메모리의 파일 보기

플래시 메모리의 파일을 보고 해당 파일에 대한 정보를 확인할 수 있습니다.

프로시저

단계 **1** 플래시 메모리에서 파일: 보기

dir [**disk0:** | **disk1:**]

예제**:**

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

내부 플래시 메모리는 **disk0:**을 입력합니다. **disk1:** 키워드는 외부 플래시 메모리를 나타냅니다. 내부 플래시 메모리가 기본값입니다.

단계 **2** 특정 파일에 대한 보기 확장 정보:

show file information [path:/]*filename*

예제**:**

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

표시된 파일 크기는 예시용입니다.

기본 경로는 내부 플래시 메모리의 루트 디렉터리(disk0:/)입니다.

플래시 메모리의 파일 삭제

플래시 메모리에서 더 이상 필요 없는 파일을 삭제할 수 있습니다.

프로시저

플래시 메모리에서 파일을 삭제합니다.

delete disk0: 파일 이름

경로를 지정하지 않을 경우, 기본적으로 현재 작업 디렉터리에서 파일이 삭제됩니다. 파일 삭제 시 와일드카드를 사용할 수 있습니다. 삭제할 파일 이름을 묻는 메시지에 응답하고 삭제를 확인해야 합니다.

플래시 파일 시스템 지우기

플래시 파일 시스템을 지우려면 다음 단계를 수행하십시오.

프로시저

단계 **1** ASA 서비스 모듈 콘솔 액세스, 18 페이지 또는 어플라이언스 콘솔 액세스, 13 페이지의 지침에 따라 ASA 콘솔 포트에 연결합니다.

단계 **2** ASA의 전원을 끈 후 전원을 켭니다.

단계 **3** 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

단계 **4** **erase** 명령을 입력합니다. 그러면 모든 파일을 덮어쓰고 숨겨진 시스템 파일을 포함하여 파일 시스템을 지웁니다.

rommon #1> **erase** [**disk0:** | **disk1:** | **flash:**]

파일 액세스 구성

ASA는 FTP 클라이언트, SCP(Secure Copy) 클라이언트 또는 TFTP 클라이언트를 사용할 수 있습니다. 또한 컴퓨터에서 SCP(Secure Copy) 클라이언트를 사용할 수 있도록 ASA를 SCP(Secure Copy) 서버로 구성할 수도 있습니다.

FTP 클라이언트 모드 구성

ASA에서는 FTP를 사용하여 FTP 서버에 이미지 파일이나 구성 파일을 업로드하거나 FTP 서버로부터 다운로드할 수 있습니다. 패시브 FTP에서는 클라이언트가 제어 연결과 데이터 연결을 모두 시작합니다. 패시브 모드에서 데이터 연결의 수신자가 되는 서버는 해당 연결을 수신하는 포트의 번호를 알려주며 응답합니다.

프로시저

FTP 모드를 수동으로 설정합니다.

ftp mode passive

예제:

```
ciscoasa(config)# ftp mode passive
```

ASA를 SCP 서버로 구성

ASA에서 SCP(Secure Copy) 서버를 활성화할 수 있습니다. SSH를 사용하여 ASA에 액세스하는 것이 허용된 클라이언트만 SCP 연결을 설정할 수 있습니다.

시작하기 전에

- 이 서버에서는 디렉터리가 지원되지 않습니다. 디렉터리가 지원되지 않으므로 ASA 내부 파일에 대한 원격 클라이언트 액세스가 제한됩니다.
- 이 서버는 배너 또는 와일드카드를 지원하지 않습니다.
- SSH 액세스 구성, 1107 페이지에 따라 ASA에서 SSH를 활성화합니다.
- ASA 라이선스에 강력한 암호화(3DES/AES) 라이선스가 있어야 SSH 버전 2 연결을 지원할 수 있습니다.
- 달리 지정되지 않은 경우, 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다.상황에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.
- SCP(Secure Copy)의 성능은 사용되는 암호화 암호에 따라 부분적으로 달라집니다. 기본적으로 ASA에서는 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr 알고리즘 중 하나를 순서대로 협상합니다. 제안된 첫 번째 알고리즘(3des-cbc)을 선택하는 경우, 성능이 aes128-cbc와 같은 더 효율적인 알고리즘보다 훨씬 느려집니다. 제안된 암호를 변경하려면 **ssh cipher encryption** 명령을 사용합니다. 예를 들어, **ssh cipher encryption custom aes128-cbc**

프로시저

단계 **1** SCP 서버를 활성화합니다.

ssh scopy enable

단계 **2** (선택사항) 서버와 해당 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제합니다.

ssh pubkey-chain [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

예제:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

ASA에서는 연결되는 각 SCP 서버의 SSH 호스트 키를 저장합니다. 원하는 경우 키를 수동으로 관리할 수 있습니다.

각 서버에 대해 SSH 호스트의 **key-string**(공개 키) 또는 **key-hash**(해시된 값)를 지정할 수 있습니다.

*key_string*은 원격 피어의 Base64 인코딩 RSA 공개 키입니다. 열린 SSH 클라이언트에서, 즉 .ssh/id_rsa.pub 파일에서 공개 키 값을 얻을 수 있습니다. Base64 인코딩 공개 키를 전송하면 그 키가 SHA-256을 통해 해시됩니다.

key-hash {**md5** | **sha256**} *fingerprint*는 이미 해시된 키를 (MD5 또는 SHA-256 키를 사용하여) 입력합니다. 이를테면 **show** 명령 출력에서 복사한 키입니다.

단계 **3** (선택 사항) SSH 호스트 키 검사를 활성화하거나 비활성화합니다. 다중 상황 모드의 경우, 관리 상황에서 이 명령을 입력합니다.

[**no**] **ssh stricthostkeycheck**

예제**:**

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

기본적으로 이 옵션은 활성화되어 있습니다. 이 옵션을 활성화하면 호스트 키를 허용할지 또는 거부할지 묻는 메시지가 표시됩니다(ASA에 이미 저장되지 않은 경우). 이 옵션이 비활성화된 경우, 호스트 키가 아직 저장되지 않았다면 ASA는 자동으로 호스트 키를 승인합니다.

예

외부 호스트의 클라이언트에서 SCP 파일 전송을 수행합니다. 예를 들어, Linux에서는 다음 명령을 입력합니다.

scp -v -pw *password source_filename username@asa_address***:{disk0|disk1}:/***dest_filename*

-v는 상세 표시를 의미하며, **-pw**가 지정되지 않은 경우 비밀번호를 입력해야 합니다.

다음 예에서는 10.86.94.170에서 서버의 이미 해시된 호스트 키를 추가합니다.

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

다음 예에서는 10.7.8.9에서 서버의 호스트 문자열을 추가합니다.

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

ASA TFTP 클라이언트 경로 구성

TFTP는 단일 클라이언트/서버 파일 전송 프로토콜이며, RFC 783 및 RFC 1350 Rev 2에 기술되어 있습니다. ASA를 TFTP 클라이언트로 구성하여 TFTP 서버에 파일을 복사하거나 복사해 오도록 할 수 있습니다. 이와 같은 방법으로 구성 파일을 백업하여 여러 ASA에 배포할 수 있습니다.

이 섹션에서는 TFTP 서버의 경로를 미리 정의하는 방법을 알아봅니다. 그러면 **copy**, **configure net**과 같은 명령에서 그 경로를 입력하지 않아도 됩니다.

프로시저

---

configure net 및 **copy** 명령에서 사용할 TFTP 서버 주소와 파일 이름을 미리 정의합니다.

tftp-server *interface_name server_ip filename*

예제**:**

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

명령을 입력할 때 파일 이름을 재정의할 수 있습니다. 예를 들어, **copy** 명령을 사용할 때 미리 정의된 TFTP 서버 주소를 사용할 수 있으나 대화형 프롬프트에서 임의의 파일 이름을 입력하는 것도 가능합니다.

copy 명령의 경우 **tftp:**를 입력하면 **tftp://***url* 대신 tffp-server 값을 사용할 수 있습니다.

ASA에 파일 복사

이 섹션에서는 애플리케이션 이미지, ASDM 소프트웨어, 컨피그레이션 파일 또는 내부/외부 플래시 메모리에 다운로드해야 할 기타 파일을 TFTP, FTP, SMB, HTTP, HTTPS 또는 SCP 서버로부터 복사하는 방법을 설명합니다.

시작하기 전에

- IPS SSP 소프트웨어 모듈의 경우, disk0에 IPS 소프트웨어를 다운로드하기 전에 플래시 메모리의 50% 이상이 비어 있는지 확인합니다. IPS를 설치할 때 IPS는 내부 플래시 메모리의 50%를 파일 시스템용으로 예약합니다.
- 플래시 메모리의 같은 디렉터리에서 두 파일이 대/소문자가 다르더라도 같은 이름을 가질 수 없습니다. 예를 들어, Config.cfg 파일을 다운로드하려는 위치에 config.cfg라는 파일이 있을 경우 다음과 같은 오류 메시지가 나타납니다.

```
%Error opening disk0:/Config.cfg (File exists)
```

- Cisco SSL VPN 클라이언트 설치에 대한 자세한 내용은 *Cisco AnyConnect VPN* 클라이언트 관리자 설명서를 참조하십시오. ASA에 Cisco Secure Desktop을 설치하는 것에 대한 자세한 내용은 *Cisco ASA 5500 Series* 관리자를 위한 *Cisco Secure Desktop* 구성 가이드를 참고하십시오.
- ASA에서 특정 애플리케이션 이미지 또는 ASDM 이미지를 사용하도록 구성하려면(둘 이상을 설치했거나 외부 플래시 메모리에 설치한 경우) ASA 이미지, ASDM 및 시작 구성설정, 1174 페이지의 내용을 참고하십시오.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에 있어야 합니다.
- (선택 사항) ASA가 서버와 통신하는 데 사용되는 인터페이스를 지정합니다. 인터페이스를 지정하지 않은 경우, ASA는 관리 전용 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 데이터 라우팅 테이블을 확인합니다.

프로시저

다음 서버 유형 중 하나를 사용하여 파일을 복사합니다.

- TFTP 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* {**disk0**|**disk1**}**:**/[*path*/]*dest_filename*

  예:

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- FTP 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* {**disk0**|**disk1**}**:**/[*path*/]*dest_filename*

예:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?

Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- HTTP(S) 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

  예:

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SMB 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

  예:

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SCP 서버에서 복사합니다.

  ;int=*interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.

copy [**/noconfirm**] [*interface_name*]
scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*]
{**disk0**|**disk1**}**:/**[*path/*]*dest_filename*

예:

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?

Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

시작 또는 실행 중인 구성에 파일 복사

TFTP, FTP, SMB, HTTP(S), SCP 서버로부터 또는 플래시 메모리로부터 실행 중인 컨피그레이션 또는 시작 컨피그레이션에 텍스트 파일을 다운로드할 수 있습니다.

시작하기 전에

어떤 컨피그레이션을 실행 중인 컨피그레이션에 복사하면 두 컨피그레이션을 병합하는 것입니다. 병합은 새 컨피그레이션의 새로운 명령을 실행 중인 컨피그레이션에 추가합니다. 컨피그레이션이 동일할 경우 어떤 변경도 없습니다. 명령이 충돌하거나 명령이 상황 실행에 영향을 줄 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다.

(선택 사항) ASA가 서버와 통신하는 데 사용되는 인터페이스를 지정합니다. 인터페이스를 지정하지 않은 경우, ASA는 관리 전용 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 데이터 라우팅 테이블을 확인합니다.

프로시저

어떤 파일을 시작 컨피그레이션에 또는 실행 중인 컨피그레이션에 복사하려면 적합한 다운로드 서버에 대해 다음 명령 중 하나를 입력합니다.

- TFTP 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **tftp://***server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  예:

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- FTP 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  예:

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- HTTP(S) 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  예:

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- SMB 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  예:

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- SCP 서버에서 복사합니다.

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  예:

  ```
  ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
  ```

  ;int=*interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.

예

예를 들어, TFTP 서버로부터 컨피그레이션을 복사하려면 다음 명령을 입력합니다.

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP 서버로부터 컨피그레이션 파일을 복사하려면 다음 명령을 입력합니다.

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP 서버로부터 컨피그레이션 파일을 복사하려면 다음 명령을 입력합니다.

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

ASA 이미지, ASDM 및 시작 구성설정

둘 이상의 ASA 또는 ASDM 이미지가 있을 경우 부팅할 이미지를 지정해야 합니다. 이미지를 설정하지 않은 경우 기본 부트 이미지가 사용되는데, 원하는 이미지가 아닐 수 있습니다. 시작 컨피그레이션에서는 선택 사항으로 컨피그레이션 파일을 지정할 수 있습니다.

다음 기본 설정을 확인합니다.

- ASA 이미지:
  - 물리적 ASA — 내부 플래시 메모리에서 발견한 첫 번째 애플리케이션 이미지를 부팅합니다.
  - ASAv — 최초로 구축했을 때 생성한 읽기 전용 boot:/ 파티션의 이미지를 부팅합니다.
  - Firepower 4100/9300 섀시의 ASA — FXOS 시스템은 부팅할 ASA 이미지를 결정합니다. ASA 이미지를 설정하는 데 이 절차를 사용할 수 없습니다.
  - Firepower 2100 — FXOS 시스템은 부팅할 ASA/FXOS 패키지를 결정합니다. ASA 이미지를 설정하는 데 이 절차를 사용할 수 없습니다.
- 모든 ASA의 ASDM 이미지 — 내부 플래시 메모리에서 발견한 첫 번째 ASDM 이미지를 부팅합니다. 내부 플래시 메모리에 없을 경우 외부 플래시 메모리의 첫 번째 ASDM 이미지를 부팅합니다.
- 시작 구성— 기본적으로 ASA는 숨겨진 파일인 시작 구성으로부터 부팅합니다.

시작하기 전에

- Firepower 4100/9300 섀시— ASA 업그레이드는 FXOS에 의해 관리됩니다. ASA 운영 체제 내에서 ASA를 업그레이드할 수 없으므로 ASA 이미지에 대해 이 절차를 사용하지 않습니다. ASA 및

FXOS를 서로 개별적으로 업그레이드할 수 있으며 이 둘은 FXOS 디렉터리 목록에 별도로 나열됩니다. ASA 패키지는 항상 ASDM을 포함합니다.

- Firepower 2100 — ASA, ASDM 및 FXOS 이미지는 단일 패키지에 번들로 제공됩니다. 패키지 업데이트는 FXOS에 의해 관리됩니다. ASA 운영 체제 내에서 ASA를 업그레이드할 수 없으므로 ASA 이미지에 대해 이 절차를 사용하지 않습니다. ASA와 FXOS는 각각 별도로 업그레이드할 수 없습니다. 이 두 가지는 항상 번들로 제공됩니다.
- Firepower 2100 및 Firepower 4100/9300 섀시용 ASDM — ASDM은 ASA 운영 체제 내에서 업그레이드될 수 있습니다. 따라서 번들로 제공된 ASDM 이미지만 사용할 필요는 없습니다. 수동으로 업로드하는 ASDM 이미지는 FXOS 이미지 목록에 나타나지 않습니다. ASA에서 ASDM 이미지를 관리해야 합니다.

  참고 FXOS에서 ASA 번들을 업그레이드하는 경우 번들 이미지가 동일한 이름(**asdm.bin**)을 지니고 있기 때문에 번들의 ASDM 이미지가 ASA에서 이전 ASDM 번들 이미지를 대체합니다. 단, 업로드한 다른 ASDM 이미지를 수동으로 선택하는 경우(예: **asdm-782.bin**) 번들 업그레이드 이후에도 계속 해당 이미지를 사용하십시오. ASDM의 호환 가능한 버전을 실행 중인지 확인하려면 번들을 업그레이드하기 전에 ASDM을 업그레이드하거나 ASA 번들을 업그레이드하기 바로 전에 번들로 제공된 ASDM 이미지(**asdm.bin**)를 사용하도록 ASA를 다시 구성해야 합니다.

- ASAv — 초기 구축 ASAv 패키지는 ASA 이미지를 읽기 전용 boot:/ 파티션에 배치합니다. ASAv를 업그레이드할 때 플래시 메모리에 서로 다른 이미지를 지정합니다. 나중에 구성을 지울 경우(**clear configure all**) ASAv는 원래로 돌아가 최초의 구축 이미지를 로드합니다. 초기 구축 ASAv 패키지는 플래시 메모리에 들어 있는 ASDM 이미지도 포함합니다. ASDM 이미지를 개별적으로 업그레이드할 수 있습니다.

프로시저

단계 **1** ASA 부팅 이미지 위치를 설정합니다.

boot system *url*

예제**:**

```
ciscoasa(config)# boot system disk:/images/asa921.bin
```

URL은 다음과 같을 수 있습니다.

- {**disk0:/** | **disk1:/**}[*path*/]*filename*
- **tftp://**[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*

  TFTP 옵션은 모든 모델에서 지원되지는 않습니다.

최대 4개의 **boot system** 명령 항목을 입력하여 각기 다른 이미지를 지정할 수 있습니다. 그 순서대로 부팅됩니다. ASA는 발견한 첫 번째 이미지를 부팅합니다. **boot system** 명령을 입력하면 목록의 맨 아래에 항목을 추가합니다. 부트 항목의 순서를 바꾸려면 **clear configure boot system** 명령으로 모든 항목을 삭제한 다음 원하는 순서대로 다시 입력해야 합니다. 하나의 **boot system tftp** 명령만 구성할 수 있으며, 이는 구성된 첫 번째 항목이어야 합니다.

참고 ASA가 부팅을 무한 반복할 경우 를 ROMMON 모드로 재부팅할 수 있습니다. ROMMON 모드에 대한 자세한 내용은 디버깅 메시지 보기, 1223 페이지를 참조하십시오.

단계 **2** 부팅할 ASDM 이미지를 설정합니다.

asdm image {**disk0:/** | **disk1:/**}[*path*/]*filename*

예제**:**

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

부팅할 이미지를 지정하지 않은 경우, 설치된 이미지가 하나밖에 없더라도 ASA는 **asdm image** 명령을 실행 중인 구성에 삽입합니다. 자동 업데이트가 구성된 경우 이와 관련된 문제를 방지하고 시작할 때마다 이미지를 검색하는 번거로움을 피하기 위해서는 부팅할 ASDM 이미지를 시작 컨피그레이션에 지정해야 합니다.

단계 **3** (선택사항) 시작 구성을 기본값인 숨겨진 파일 대신 확인된 파일로 설정합니다.

boot config {**disk0:/** | **disk1:/**}[*path*/]*filename*

예제**:**

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

구성 또는 기타 파일 백업 및 복원

구성 및 기타 시스템 파일의 시스템 장애로부터 보호하기 위해 일반 백업을 생성할 것을 권장합니다.

전체 시스템 백업 또는 복원 수행

이 절차에서는 구성과 이미지를 tar.gz 파일로 백업 및 복원하고 로컬 컴퓨터에 전송하는 방법을 설명합니다.

백업 또는 복원을 시작하기 전에

- 백업 또는 복원을 시작하기에 앞서 백업 또는 복원 위치에 300MB 이상의 사용 가능한 디스크 공간이 있어야 합니다.

- 백업 중에 또는 백업 후에 컨피그레이션을 변경할 경우, 이 변경 사항은 백업에 포함되지 않습니다. 백업한 후 컨피그레이션을 변경한 다음 복원을 수행할 경우, 이 컨피그레이션 변경 사항은 덮어쓰기됩니다. 따라서 ASA가 다르게 작동할 수 있습니다.
- 한 번에 하나의 백업 또는 복원만 시작할 수 있습니다.
- 최초의 백업을 수행했을 때와 동일한 ASA 버전에만 구성을 복원할 수 있습니다. 복원 툴을 사용하여 어떤 ASA 버전의 구성을 다른 버전으로 마이그레이션할 수 없습니다. 구성 마이그레이션이 필요할 경우, ASA에서는 새 ASA OS를 로드할 때 상주하는 시작 구성을 자동으로 업그레이드합니다.
- 클러스터링을 사용할 경우 시작 구성, 실행 중인 구성, ID 인증서만 백업 및 복원할 수 있습니다. 각 유닛에서 개별적으로 백업을 생성하고 복원해야 합니다.
- 장애 조치를 사용할 경우, 액티브 유닛과 스탠바이 유닛의 백업을 따로 생성하고 복원해야 합니다.
- ASA에 대해 마스터 패스프레이즈를 설정한 경우, 이 절차로 생성한 백업 컨피그레이션을 복원하는 데 마스터 패스프레이즈가 필요합니다. ASA의 마스터 패스프레이즈를 모를 경우, 백업을 진행하기 전에 마스터 패스프레이즈 구성, 689 페이지에서 재설정 방법을 확인하십시오.
- PKCS12 데이터를 가져왔고(**crypto ca trustpoint** 명령 사용) 신뢰 지점에서 RSA 키를 사용할 경우, 가져온 키 쌍에는 신뢰 지점과 동일한 이름이 지정됩니다. 이러한 제한 때문에 ASDM 컨피그레이션을 복원한 다음 신뢰 지점과 그 키 쌍의 이름을 다르게 지정할 경우, 시작 컨피그레이션은 원래의 컨피그레이션과 동일하지만 실행 중인 컨피그레이션은 다른 키 쌍 이름을 가지게 됩니다. 따라서 키 쌍과 신뢰 지점에 서로 다른 이름을 사용하는 경우 원래의 컨피그레이션을 복원할 수 없습니다. 이 문제를 해결하려면 신뢰 지점과 그 키 쌍에 동일한 이름을 사용해야 합니다.
- CLI로 백업했다가 ASDM으로 복원할 수 없습니다. 그 반대도 마찬가지입니다.
- 각 백업 파일에는 다음 내용이 들어 있습니다.
  - 실행 중인 컨피그레이션
  - 시작 컨피그레이션
  - 모든 보안 이미지

    Cisco Secure Desktop & Host Scan 이미지

    Cisco Secure Desktop & Host Scan 이미지

    AnyConnect(SVC) 클라이언트 이미지 및 프로필

    AnyConnect(SVC) 사용자 지정 및 변환
  - ID 인증서(ID 인증서와 연결된 RSA 키 쌍 포함, 독립형 키는 제외)
  - VPN 사전 공유 키
  - SSL VPN 컨피그레이션
  - APCF(Application Profile Custom Framework)
  - 북마크

- 사용자 지정
- DAP(Dynamic Access Policy)
- 플러그인
- 미리 채워진 연결 프로필 스크립트
- 프록시 자동 컨피그레이션
- 변환 테이블
- 웹 콘텐츠
- 버전 정보

시스템 백업

이 절차에서는 전체 시스템 백업을 수행하는 방법을 설명합니다.

프로시저

단계 **1** 시스템을 백업합니다.

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

예제**:**

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

인터페이스를 이름을 지정하지 않은 경우, ASA는 관리 전용 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 데이터 라우팅 테이블을 확인합니다.

다중 상황 모드에서는 시스템 실행 영역에서 **context** 키워드를 입력하여 지정된 상황을 백업합니다. 각 상황은 개별적으로 백업해야 합니다. 즉, 각 파일에 대해 **backup** 명령을 다시 입력합니다.

VPN 인증서 및 사전 공유 키의 백업 과정에서 **passphrase** 키워드로 식별되는 보안 키가 인증서 인코딩에 필요합니다. 인증서 인코딩 및 디코딩에 사용할 패스프레이즈를 PKCS12 형식으로 제공해야 합니다. 백업에는 인증서와 연결된 RSA 키 쌍만 포함되며 독립형 인증서는 제외됩니다.

백업 위치는 로컬 디스크 또는 원격 URL일 수 있습니다. 위치를 지정하지 않으면 다음 기본 이름이 사용됩니다.

- 단일 모드 - disk0:*hostname*.backup.*timestamp*.tar.gz
- 다중 모드 - disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

단계 **2** 프롬프트에 따라 수행합니다.

예제**:**

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

백업 복원

로컬 컴퓨터에 있는 zip tar.gz 파일에서 복원할 구성과 이미지를 지정할 수 있습니다.

프로시저

단계 **1** 백업 파일에서 시스템을 복원합니다.

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

예제**:**

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

다중 상황을 복원하기 위해 **context** 키워드를 사용하는 경우, 각 백업된 상황 파일은 개별적으로 복원되어야 합니다. 즉, 각 파일에 대해 **restore** 명령을 다시 입력합니다.

단계 **2** 프롬프트에 따라 수행합니다.

예제:

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
```

```
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

자동 백업 및 복원 구성(ISA 3000)

이 기능은 시스템 구성의 간소화 및 자동화된 백업 및 복원을 제공하며 이는 다음과 같은 상황에서 유용합니다.

- 초기 구성 – 구성 정보를 대상 디바이스에 전송하는 데 사용된 외부 미디어에 있는 디바이스 구성(하드웨어 및 소프트웨어)입니다.
- 디바이스 교체를 위한 구성 복제 – 교체 디바이스에 실패한 기존 디바이스의 백업 구성을 적용합니다.
- 작동 가능 상태로 롤백 – 소프트웨어 구성이 손상된 경우, 이전 작업 구성으로 롤백됩니다.

시작하기 전에

- 이 기능은 Cisco ISA 3000 어플라이언스에서만 사용할 수 있습니다.
- ISA 3000에서 자동 백업 및 복원을 설정하려면 특정 파라미터의 일회 구성을 수행합니다.
  - 백업 위치 위치 – SD 카드, USB 스토리지 또는 네트워크 위치와 같은 스토리지 미디어를 선택할 수 있습니다.
  - 백업 모드 – 수동 또는 자동입니다.
  - 패스프레이즈 – 백업 구성을 암호화하는 동안 사용할 패스프레이즈입니다.

  따라서 이러한 설정은 자동 백업 및 복원 작업을 수행하는 데 사용됩니다.
- 백업 및 복원 기능 둘 다 자동 모드 또는 수동 모드에서 작동하도록 개별적으로 구성될 수 있습니다.
- 원래 EXEC **backup** | **restore** 명령은 변경되지 않으며 백업 패키지 명령이 구성되면 EXEC 명령은 추가 명령줄 파라미터를 제공할 필요 없이 수동으로 백업 및 복원하는 데 사용될 수 있습니다.

프로시저

단계 **1** 백업 패키지 파라미터를 설정합니다.

backup-package backup [**interface** *name*] **location disk***n***:** [**passphrase** *string*]

예제**:**

```
ciscoasa(config)# backup-package backup GigabitEthernet1/1 location disk3: passphrase cisco
```

이 명령을 사용하여 후속 백업 작업에서 구성 데이터를 백업하는 데 사용할 파라미터를 지정합니다.

interface *name*은 백업 작업에 대한 발신 인터페이스를 지정합니다.

location disk*n*은 데이터 백업에 사용할 스토리지 미디어를 지정합니다.

passphrase *string*은 백업 데이터를 보호하는 데 사용됩니다.

단계 **2** 복원 패키지 파라미터를 설정합니다.

backup-package restore [**interface** *name*] **location disk***n***:** [**passphrase** *string*]

예제**:**

```
ciscoasa(config)# backup-package restore GigabitEthernet1/1 location disk3: passphrase cisco
```

이 명령을 사용하여 후속 복원 작업에서 사용될 복원 파라미터를 지정합니다. 복원 파라미터는 백업 작업을 위해 앞에서 설명한 파라미터를 미러링합니다.

단계 **3** 백업 및 복원을 위해 자동 모드를 활성화합니다.

backup-package {**backup** | **restore**} **auto**

예제**:**

```
ciscoasa(config)# backup-package backup auto
ciscoasa(config)# backup-package restore auto
```

이 명령을 사용하여 백업 또는 복원을 위해 자동 모드를 활성화/비활성화합니다. 복원 모드에 대한 선택 사항은 ROMMON 변수로도 저장됩니다.

단일 모드 구성 또는 다중 모드 시스템 구성백업

단일 상황 모드에서 또는 다중 모드의 시스템 구성에서 시작 구성이나 실행 중인 구성을 외부 서버에 또는 로컬 플래시 메모리에 복사할 수 있습니다.

시작하기 전에

(선택 사항) ASA가 서버와 통신하는 데 사용되는 인터페이스를 지정합니다. 인터페이스를 지정하지 않은 경우, ASA는 관리 전용 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 데이터 라우팅 테이블을 확인합니다.

프로시저

다음 서버 유형 중 하나를 사용하여 구성을 백업합니다.

- TFTP 서버에 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**startup-config** |**running-config**} **tftp:**//*server*[/*path*]/*dst_filename*

  예:

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- FTP 서버에 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**}
  ftp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  예:

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- SMB 서버에 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**}
  smb://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  예:

  ```
  ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
  ```

- SCP 서버에 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**}
  scp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*[**;int=***interface_name*]

  예:

  ```
  ciscoasa# copy startup-config
  scp://pilot:moya@10.86.94.170/new-startup.cfg
  ```

  ;int=*interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.

- 로컬 플래시 메모리에 복사합니다.

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  예:

  ```
  ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
  ```

  대상 디렉터리가 있어야 합니다. 없는 경우 먼저 **mkdir** 명령을 사용하여 디렉터리를 만듭니다.

플래시 메모리의 상황 구성 또는 기타 파일 백업

시스템 실행 영역에서 다음 명령 중 하나를 입력하여 로컬 플래시 메모리에 있는 컨텍스트 컨피그레이션이나 기타 파일을 복사합니다.

시작하기 전에

(선택 사항) ASA가 서버와 통신하는 데 사용되는 인터페이스를 지정합니다. 인터페이스를 지정하지 않은 경우, ASA는 관리 전용 라우팅 테이블을 확인합니다. 일치하는 항목이 없으면 데이터 라우팅 테이블을 확인합니다.

프로시저

다음 서버 유형 중 하나를 사용하여 상황 구성을 백업합니다.

- 플래시에서 TFTP 서버로 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[/*path*]/*dst_filename*

  예:

  ```
  ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
  ```

- 플래시에서 FTP 서버로 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  ftp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  예:

  ```
  ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
  ```

- 플래시에서 SMB 서버로 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  smb://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  예:

  ```
  ciscoasa# copy /noconfirm copy disk0:/asdm.bin
  smb://chiana:dargo@10.1.1.67/asdm.bin
  ```

- 플래시에서 SCP 서버로 복사합니다.

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  scp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*[**;int=***interface_name*]

  예:

  ```
  ciscoasa# copy disk0:/context1.cfg
  ```

```
scp://pilot:moya@10.86.94.170/context1.cfg
```

;int=*interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.

- 플래시에서 로컬 플래시 메모리로 복사합니다.

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  예:

  ```
  ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
  ```

  대상 디렉터리가 있어야 합니다. 없는 경우 먼저 **mkdir** 명령을 사용하여 디렉터리를 만듭니다.

상황 내에서 상황 구성백업

다중 상황 모드에서는 어떤 상황 내에서 다음 백업을 수행할 수 있습니다.

프로시저

단계 **1** 실행 중인 구성을 시작 구성서버(관리 상황에 연결됨)에 복사합니다.

```
ciscoasa/contexta# copy running-config startup-config
```

단계 **2** 실행 중인 구성을 상황 네트워크에 연결된 TFTP 서버에 복사합니다.

```
ciscoasa/contexta# copy running-config tftp:/server[/path]/filename
```

터미널 디스플레이에서 구성 복사

프로시저

단계 **1** 터미널에 구성을 인쇄합니다.

more system:running-config

단계 **2** 이 명령의 출력을 복사하고 텍스트 파일에 그 컨피그레이션을 붙여넣습니다.

내보내기 및 가져오기 명령을 사용하여 추가 파일 백업

다음과 같은 추가 파일이 컨피그레이션에 필요할 수 있습니다.

- **import webvpn** 명령을 사용하여 가져온 파일. 현재 이러한 파일에는 사용자 지정 설정, URL 목록, 웹 콘텐츠, 플러그인, 언어 번역 등이 포함됩니다.
- DAP 정책(dap.xml)
- CSD 컨피그레이션(data.xml)
- 디지털 키 및 인증서
- 로컬 CA 사용자 데이터베이스 및 인증서 상태 파일

CLI에서는 **export** 및 **import** 명령을 사용하여 컨피그레이션의 개별 요소를 백업하고 복원할 수 있습니다.

이러한 파일, 예를 들어 **import webvpn** 명령으로 가져온 파일이나 인증서를 백업하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 다음과 같이 알맞은 **show** 명령을 실행합니다.

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

단계 **2** 백업할 파일(여기서는 rdp 파일)에 대한 **export** 명령을 실행합니다.

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

파일 백업 및 복원에 스크립트 사용

import webvpn CLI로 가져온 모든 확장, CSD 구성 XML 파일, DAP 구성 XML 파일을 비롯한 ASA의 구성 파일을 백업하고 복원하는 데 스크립트를 사용할 수 있습니다. 보안상의 이유로 디지털 키와 인증서 또는 로컬 CA 키에 대해서는 자동 백업이 권장되지 않습니다.

이 섹션에서는 그 방법에 대한 설명과 샘플 스크립트를 제공합니다. 이 샘플 스크립트는 그대로 사용하거나 환경의 요구 사항에 따라 수정할 수 있습니다. 이 샘플 스크립트는 Linux 시스템 버전입니다. Microsoft Windows 시스템에서 사용하려면 샘플의 로직을 사용하여 수정해야 합니다.

참고 **backup** 및 **restore** 명령을 대신 사용할 수 있습니다. 자세한 내용은 전체 시스템 백업 또는 복원 수행, 1176 페이지를 참조하십시오.

백업 및 복원 스크립트 사용을 시작하기 전에

ASA 구성의 백업 및 복원에 스크립트를 사용하려면 먼저 다음 작업을 수행합니다.

- Expect 모듈로 Perl을 설치합니다.
- ASA에 연결할 수 있는 SSH 클라이언트를 설치합니다.
- ASA에서 백업 사이트에 파일을 보낼 수 있도록 TFTP 서버를 설치합니다.

또 다른 방법은 상용 툴을 사용하는 것입니다. 이 스크립트의 로직을 그 툴에 적용하면 됩니다.

스크립트 실행

백업 및 복원 스크립트를 실행하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 시스템의 임의의 위치에 스크립트 파일을 다운로드하거나 잘라내어 붙여넣습니다.

단계 **2** 명령줄에 **Perl***scriptname*을 입력합니다. 여기서 *scriptname*은 스크립트 파일의 이름입니다.

단계 **3** **Enter** 키를 누릅니다.

단계 **4** 시스템에서 각 옵션에 대한 값을 묻습니다. 또는 **Perl***scriptname* 명령을 입력할 때 옵션에 대한 값을 입력한 다음 **Enter** 키를 누르는 방법도 있습니다. 어느 쪽이든 스크립트에서는 각 옵션에 대한 값을 입력해야 합니다.

단계 **5** 스크립트가 실행되기 시작하고 생성되는 명령을 출력합니다. 이는 CLI의 기록이 됩니다. 이 CLI를 추후 복원에 사용할 수 있습니다. 이는 파일 한두 개만 복원하려는 경우 특히 유용합니다.

샘플 스크립트

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name. This file is produced
```

```
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);
```

```
   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
```

```
      print OUT "$ocli\n";
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
    }
}

sub url_list {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn url-list\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
      chop;
      next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
      $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
      $ocli = $cli;
      $ocli =~ s/^export/import/;
      print "$cli\n";
      print OUT "$ocli\n";
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
    }
}

sub dap {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("dir dap.xml\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub csd {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("dir sdesktop\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub webcontent {
    $obj = shift;
    $obj->clear_accum();
```

```
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
```

```
        $storage = "tftp://$tstr";
    }
    else {
        print "Enter TFTP host name or IP address:";
        chop($tstr=<>);
        $storage = "tftp://$tstr";
    }
    if (defined($options{h})) {
        $asa = $options{h};
    }
    else {
        print "Enter ASA host name or IP address:";
        chop($asa=<>);
    }

    if (defined ($options{u})) {
        $user= $options{u};
    }
    else {
        print "Enter user name:";
        chop($user=<>);
    }

    if (defined ($options{w})) {
        $password= $options{w};
    }
    else {
        print "Enter password:";
        chop($password=<>);
    }
    if (defined ($options{p})) {
        $prompt= $options{p};
    }
    else {
        print "Enter ASA prompt:";
        chop($prompt=<>);
    }
    if (defined ($options{e})) {
        $enable = $options{e};
    }
    else {
        print "Enter enable password:";
        chop($enable=<>);
    }

    if (defined ($options{r})) {
       $restore = 1;
       $restore_file = $options{r};
    }
}
```

자동 업데이트 구성

자동 업데이트는 자동 업데이트 서버에서 다수의 ASA에 구성 및 소프트웨어 이미지를 다운로드할 수 있게 하고 중앙에서 ASA에 대한 기본적인 모니터링을 제공할 수 있는 프로토콜 사양입니다.

자동 업데이트 정보

이 섹션에서는 자동 업데이트 구현 방법과 자동 업데이트를 사용하는 이유에 대해 설명합니다.

자동 업데이트 클라이언트 또는 서버

ASA는 클라이언트 또는 서버로 구성할 수 있습니다. 자동 업데이트 클라이언트일 경우 정기적으로 자동 업데이트 서버에 폴링하여 소프트웨어 이미지 및 컨피그레이션 파일에 대한 업데이트를 확인합니다. 자동 업데이트 서버는 자동 업데이트 클라이언트로 구성된 ASA를 위해 업데이트를 배포합니다.

자동 업데이트의 이점

자동 업데이트는 다음과 같이 관리자가 ASA 관리에서 겪는 여러 문제점을 해결하는 데 효과적입니다.

- 동적 주소 지정 및 NAT 문제 해결
- 하나의 작업으로 컨피그레이션 변경 사항 커밋
- 믿을 수 있는 소프트웨어 업데이트 방법 제공
- 잘 알려진 고가용성(장애 조치) 방식 활용
- 개방적인 인터페이스로 유연성 제공
- 서비스 공급자 환경을 위한 보안 솔루션 간소화

자동 업데이트 사양은 원격 관리 애플리케이션에서 ASA 구성과 소프트웨어 이미지를 다운로드하고 중앙에서 또는 여러 위치에서 기본적인 모니터링을 수행하는 데 필요한 인프라를 제공합니다.

자동 업데이트 사양은 자동 업데이트 서버가 ASA에 구성 정보를 푸시하고 정보 요청을 보내게 하거나, ASA가 정기적으로 자동 업데이트 서버를 폴링하게 하여 구성 정보를 가져오게 합니다. 또한 자동 업데이트 서버는 언제라도 ASA에 명령을 보내 즉각적인 폴링을 요청할 수 있습니다. 자동 업데이트 서버와 ASA가 통신하려면 각 ASA에 통신 경로 및 로컬 CLI 구성이 있어야 합니다.

장애 조치 구성에서 자동 업데이트 서버 지원

액티브/스탠바이 페일오버 구성에서 자동 업데이트 서버를 사용하여 ASA에 소프트웨어 이미지 및 구성 파일을 배포할 수 있습니다. 액티브/스탠바이 장애 조치 컨피그레이션에서 자동 업데이트를 활성화하려면 장애 조치 쌍의 기본 유닛에 자동 업데이트 서버 컨피그레이션을 입력합니다.

다음 제한 사항과 동작은 장애 조치 컨피그레이션에서의 자동 업데이트 서버 지원에 적용됩니다.

- 단일 모드에서만 액티브/스탠바이 컨피그레이션이 지원됩니다.
- 새 플랫폼 소프트웨어 이미지를 로드할 때 장애 조치 쌍은 트래픽 전달을 중지합니다.
- LAN 기반 장애 조치를 사용할 때 새로운 컨피그레이션이 장애 조치 링크 컨피그레이션을 변경해서는 안 됩니다. 그러면 유닛 간의 통신이 실패합니다.

- 기본 유닛만 자동 업데이트 서버에 대한 콜 홈을 수행합니다. 기본 유닛은 액티브 상태에서 콜 홈을 수행할 수 있습니다. 액티브 상태가 아닐 경우 ASA는 자동으로 기본 유닛에 장애 조치합니다.
- 기본 유닛만 소프트웨어 이미지 또는 컨피그레이션 파일을 다운로드합니다. 그런 다음 소프트웨어 이미지 또는 컨피그레이션 파일은 보조 유닛에 복사됩니다.
- 인터페이스 MAC 주소 및 하드웨어 시리얼 ID는 기본 유닛에서 나옵니다.
- 자동 업데이트 서버 또는 HTTP 서버에 저장된 컨피그레이션 파일은 기본 유닛만을 대상으로 합니다.

자동 업데이트 프로세스 개요

다음은 장애 조치 컨피그레이션의 자동 업데이트 프로세스에 대한 개요입니다. 이 프로세스에서는 장애 조치가 활성화되어 작동 중이라고 가정합니다. 유닛에서 컨피그레이션을 동기화하고 있는 경우, 대기 유닛이 SSM 카드 고장을 제외한 어떤 이유로든 고장 상태에 있는 경우 또는 장애 조치 링크가 중단된 경우에는 자동 업데이트 프로세스가 수행될 수 없습니다.

1. 두 유닛 모두 플랫폼 및 ASDM 소프트웨어 체크섬과 버전 정보를 주고받습니다.
2. 기본 유닛이 자동 업데이트 서버에 접속합니다. 기본 유닛이 액티브 상태가 아닌 경우 ASA는 먼저 기본 유닛에 장애 조치한 다음 자동 업데이트 서버에 접속합니다.
3. 자동 업데이트 서버가 응답하면서 소프트웨어 체크섬 및 URL 정보를 보냅니다.
4. 기본 유닛이 액티브 유닛 또는 스탠바이 유닛의 플랫폼 이미지 파일을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
    1. 기본 유닛이 자동 업데이트 서버가 보낸 URL을 사용하여 HTTP 서버에서 해당 파일을 검색합니다.
    2. 기본 유닛이 스탠바이 유닛에 이미지를 복사한 다음 자신의 이미지를 업데이트합니다.
    3. 두 유닛 모두 새 이미지를 가지고 있는 경우 보조(스탠바이) 유닛 먼저 다시 로드됩니다.
        - 보조 유닛이 부팅할 때 히트리스(hitless) 업그레이드를 수행할 수 있는 경우, 보조 유닛이 액티브 유닛이 되고 기본 유닛이 다시 로드됩니다. 기본 유닛이 로딩을 마치면 액티브 유닛이 됩니다.
        - 스탠바이 유닛이 부팅할 때 히트리스 업그레이드를 수행할 수 없는 경우에는 두 유닛이 동시에 다시 로드됩니다.
    4. 보조(스탠바이) 유닛에만 새 이미지가 있는 경우 보조 유닛만 다시 로드됩니다. 기본 유닛은 보조 유닛이 다시 로드되는 것이 끝날 때까지 기다립니다.
    5. 기본(액티브) 유닛에만 새 이미지가 있을 경우, 보조 유닛이 액티브 유닛이 되고 기본 유닛이 다시 로드됩니다.
    6. 업데이트 프로세스가 1단계부터 다시 시작합니다.

5. ASA에서 기본 유닛이나 보조 유닛 중 하나의 ASDM 파일을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   1. 기본 유닛이 자동 업데이트 서버가 보낸 URL을 사용하여 HTTP 서버에서 ASDM 이미지 파일을 검색합니다.
   2. 필요하다면 기본 유닛이 스탠바이 유닛에 ASDM 이미지를 복사합니다.
   3. 기본 유닛이 자신의 ASDM 이미지를 업데이트합니다.
   4. 업데이트 프로세스가 1단계부터 다시 시작합니다.
6. 기본 유닛에서 컨피그레이션을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   1. 기본 유닛이 지정된 URL을 사용하여 컨피그레이션 파일을 검색합니다.
   2. 두 유닛에서 동시에 새 컨피그레이션이 기존 컨피그레이션을 대체합니다.
   3. 업데이트 프로세스가 1단계부터 다시 시작합니다.
7. 모든 이미지 및 컨피그레이션 파일에서 체크섬이 일치할 경우 어떤 업데이트도 필요 없습니다. 다음 폴링 시간까지 프로세스는 종료됩니다.

자동 업데이트를 위한 지침

상황 모드

자동 업데이트는 단일 컨텍스트 모드에서만 지원됩니다.

클러스터링

클러스터링은 지원되지 않습니다.

모델

다음 모델에서 지원되지 않습니다.

- ASA 5506-X, 5508-X, 5516-X
- Firepower 2100, 4100 및 9300
- ASAv

추가 지침

- HTTPS가 자동 업데이트 서버와의 통신 프로토콜로 선택된 경우 ASA는 SSL을 사용합니다. 따라서 ASA에 DES 또는 3DES 라이선스가 있어야 합니다.

자동 업데이트 서버와의 통신 구성

프로시저

단계 **1** 자동 업데이트 서버의 URL을 지정하려면 다음 명령을 입력합니다.

auto-update server *url* [**source** *interface*] [**verify-certificate** | **no-verification**]

여기서 *url*의 구문은 다음과 같습니다.

http[**s**]**://**[*user*:*password*@]*server_ip*[**:***port*]/*pathname*

source *interface* 키워드와 인수는 자동 업데이트 서버에 요청을 보낼 때 사용할 인터페이스를 지정합니다. **management-access** 명령에서 지정한 것과 동일한 인터페이스를 지정할 경우 자동 업데이트 서버 요청은 관리 액세스에 사용되는 것과 동일한 IPsec VPN 터널을 통해 전달됩니다.

HTTPS의 경우 **verify-certificate** 키워드(기본값)가 자동 업데이트 서버에서 반환하는 인증서를 검증합니다. (권장 사항은 아니지만) 검증을 비활성화하려면 **no-verification** 키워드를 지정합니다.

단계 **2** (선택 사항) 자동 업데이트 서버와 통신할 때 보낼 디바이스 ID를 식별하려면 다음 명령을 입력합니다.

auto-update device-id {*hardware-serial* | **hostname** | **ipaddress** [*if-name*] | **mac-address** [*if-name*] | **string** *text*}

사용되는 식별자는 다음 매개변수 중 하나를 지정하여 결정합니다.

- hardware-serial 인수는 ASA 시리얼 번호를 지정합니다.
- hostname 인수는 ASA 호스트 이름을 지정합니다.
- **ipaddress** 키워드는 지정된 인터페이스의 IP 주소를 지정합니다. 인터페이스 이름이 지정되지 않은 경우 자동 업데이트 서버와의 통신에 쓰인 인터페이스의 IP 주소를 사용합니다.
- **mac-address** 키워드는 지정된 인터페이스의 MAC 주소를 나타냅니다. 인터페이스 이름이 지정되지 않은 경우 자동 업데이트 서버와의 통신에 쓰인 인터페이스의 IP 주소를 사용합니다.
- **string** 문자열은 지정된 텍스트 식별자를 나타냅니다. 공백이나 ‘, “, , >, &, ? 문자를 포함할 수 없습니다.

단계 **3** (선택 사항) 컨피그레이션 또는 이미지 업데이트를 위해 자동 업데이트 서버에 폴링하는 빈도를 지정하려면 다음 명령을 입력합니다.

auto-update poll-period *poll-period* [*retry-count* [*retry-period*]]

poll-period 인수는 업데이트 확인 빈도(분)를 지정합니다. 기본값은 720분(12시간)입니다.

retry-count 인수는 첫 번째 시도가 실패한 경우 서버와의 재연결을 시도할 횟수를 지정합니다. 기본값은 0입니다.

retry-period 인수는 재시도 사이의 대기 시간(분)을 지정합니다. 기본값은 5분입니다.

단계 **4** (선택 사항) 특정 시간에 ASA에서 자동 업데이트 서버에 폴링하도록 예약하려면 다음 명령을 입력합니다.

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

days-of-the-week 인수는 Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday 중 하나의 요일이거나 여러 요일의 조합입니다. 그 밖에도 daily (Monday through Sunday), weekdays (Monday through Friday), weekends (Saturday and Sunday)를 값으로 선택할 수 있습니다.

time 인수는 폴링을 시작할 시간을 HH:MM 형식으로 지정합니다. 예를 들어 8:00은 오전 8:00이며 20:00는 오후 8:00입니다.

randomize *minutes* 키워드와 인수는 지정된 시작 시간 이후에 폴링 시간을 무작위화하는 기간을 지정합니다. 범위는 1분부 ~ 1439분입니다.

retry-count 인수는 첫 번째 시도가 실패한 경우 자동 업데이트 서버와의 재연결을 시도할 횟수를 지정합니다. 기본값은 0입니다.

retry_period 인수는 연결 시도 사이의 대기 시간을 지정합니다. 기본값은 5분입니다. 범위는 1분 ~ 35791분입니다.

단계 **5** (선택 사항) 자동 업데이트 서버가 일정 기간 접속되지 않은 상태에서 다음 명령을 입력하면 트래픽 전송이 중단됩니다.

auto-update timeout 마침표

period 인수는 시간 초과 기간을 1분 ~ 35791분 범위에서 지정합니다. 기본값은 0분, 즉 시간 초과가 없습니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

auto-update timeout 명령을 사용하여 ASA에 가장 최신 버전의 이미지와 구성이 있는지 확인합니다. 이 조건은 시스템 로그 메시지 201008로 보고됩니다.

예

다음 예에서는 ASA가 외부 인터페이스에서 포트 번호 1742를 사용하여 IP 주소가 209.165.200.224인 자동 업데이트 서버에 폴링하고 인증서를 검증하도록 구성되었습니다.

ASA는 디바이스 ID를 호스트 이름으로 사용하고 자동 업데이트 서버를 매주 금요일과 토요일 밤 오후 10시와 오후 11시 사이의 임의의 시간에 폴링하도록 구성되었습니다. 실패한 폴링 시도 시 다음의 예에서와 같이 ASA는 10번 자동 업데이트 서버에 연결을 시도하고 재연결 시 시도 중간에 3분 동안 기다립니다.

```
ciscoasa(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside verify-certificate
ciscoasa (config)# auto-update device-id hostname
hostname (config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

자동 업데이트 서버로 클라이언트 업데이트 구성

client-update 명령을 입력하면 자동 업데이트 클라이언트로 구성된 ASA의 업데이트가 가능하며 소프트웨어 구성 요소의 유형(ASDM 또는 부트 이미지), ASA의 유형 또는 제품군, 업데이트가 적용되는 수정 버전 번호, 업데이트를 얻을 URL 또는 IP 주소를 지정할 수 있습니다.

ASA를 자동 업데이트 서버로 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 클라이언트 업데이트를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# client-update enable
```

단계 **2** ASA에 적용하려는 **client-update** 명령을 위한 다음 파라미터를 구성합니다.

client-update {**component** {**asdm** | **image**} | **device-id** dev_string | **family** family_name | **type** type} **url** url-string **rev-nums** rev-nums}

component {**asdm** | **image**} 파라미터는 ASA의 소프트웨어 구성 요소(ASDM 또는 부트 이미지)를 지정합니다.

device-id dev_string 파라미터는 자동 업데이트 클라이언트가 스스로를 식별하는 데 사용하는 고유한 문자열을 지정합니다. 최대 길이는 63자입니다.

family family_name 파라미터는 자동 업데이트 클라이언트가 스스로를 식별하는 데 사용하는 제품군 이름을 지정합니다. asa, pix 또는 최대 7자의 텍스트 문자열이 될 수 있습니다.

rev-nums rev-nums 파라미터는 이 클라이언트의 소프트웨어 또는 펌웨어 이미지를 지정합니다. 임의의 순서로 최대 4개를 입력하고 쉼표로 구분합니다.

type *type* 파라미터는 클라이언트 업데이트를 알릴 클라이언트의 유형을 지정합니다. 이 명령은 Windows 클라이언트를 업데이트하는 데에도 사용되므로 클라이언트 목록은 여러 Windows 운영 체제를 포함합니다.

url url-string 파라미터는 소프트웨어/펌웨어 이미지의 URL을 지정합니다. 이 URL은 해당 클라이언트에 적합한 파일을 가리켜야 합니다. 모든 자동 업데이트 클라이언트에서 프로토콜 “http://” 또는 “https://”를 URL의 접두사로 사용해야 합니다.

특정 유형의 모든 ASA에 적용할 클라이언트 업데이트의 파라미터를 구성합니다. 즉 ASA의 유형, 업데이트된 이미지 출처의 URL 또는 IP 주소를 지정합니다. 또한 수정 버전 번호를 지정해야 합니다. 원격 ASA의 수정 버전 번호가 지정된 수정 버전 번호 중 하나와 일치할 경우, 클라이언트를 업데이트할 필요가 없으며 업데이트는 무시됩니다.

Cisco 5525-X ASA의 클라이언트 업데이트를 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# client-update type asa5525 component asdm url
http://192.168.1.114/aus/asdm601.bin rev-nums 8.0(1)
```

자동 업데이트 모니터링

자동 업데이트 프로세스 모니터링

debug auto-update client 또는 **debug fover cmd-exe** 명령을 사용하여 자동 업데이트 프로세스에서 수행되는 작업을 표시합니다. 다음은 **debug auto-update client** 명령의 샘플 출력입니다.

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50
```

```
auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

다음 syslog 메시지는 자동 업데이트 프로세스가 실패하면 생성됩니다.

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

*file*은 어떤 업데이트가 실패했느냐에 따라 "image", "asdm" 또는 "configuration"이 됩니다. *version*은 업데이트의 버전 번호입니다. *reason*은 업데이트가 실패한 이유입니다.

자동 업데이트 상태 모니터링

자동 업데이트 상태를 모니터링하려면 다음 명령을 참조하십시오.

show auto-update

다음은 **show auto-update** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show auto-update

Server: https://********@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```

소프트웨어 및 구성 내역

기능 이름	플랫폼 릴리스	기능 정보
SCP(Secure Copy) 클라이언트	9.1(5)/9.2(1)	ASA에서 이제 SCP(Secure Copy) 클라이언트와 SCP 서버 간의 파일 전송을 지원합니다. 다음 명령을 도입했습니다. **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck** 다음 명령을 수정했습니다. **copy scp**

기능 이름	플랫폼 릴리스	기능 정보
구성 가능한 SSH 암호화 및 무결성 암호	9.1(7)9.4(3)9.5(3)9.6(1)	사용자는 SSH 암호화 관리를 수행할 때 암호화 모드를 선택할 수 있으며 다양한 키 교환 알고리즘을 위해 HMAC 및 암호화를 구성할 수 있습니다. 애플리케이션에 따라 암호를 더 엄격하게 또는 덜 엄격하게 변경할 수 있습니다. 보안 사본의 성능은 사용되는 암호화 암호에 따라 부분적으로 달라집니다. 기본적으로 ASA에서는 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr 알고리즘 중 하나를 순서대로 협상합니다. 제안된 첫 번째 알고리즘(3des-cbc)을 선택하는 경우, 성능이 aes128-cbc와 같은 더 효율적인 알고리즘보다 훨씬 느려집니다. 제안된 암호를 변경하려면 예를 들어 **ssh cipher encryption custom aes128-cbc**를 사용하십시오. 다음 명령을 도입했습니다. **ssh cipher encryption**, **ssh cipher integrity**
자동 업데이트 서버 인증서 검증이 기본적으로 활성화되었습니다.	9.2(1)	자동 업데이트 서버 인증서 검증이 기본적으로 활성화됩니다. 신규 컨피그레이션의 경우 명시적으로 인증서 검증을 비활성화해야 합니다. 이전 릴리스에서 업그레이드하는 경우, 인증서 검증을 활성화하지 않았다면 인증서 검증을 할 수 없고 다음 경고가 표시됩니다. `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 구성이 확인 없음을 명시적으로 구성하도록 마이그레이션됩니다. **auto-update server no-verification** 다음 명령을 수정했습니다. **auto-update server** {**verify-certificate** | **no-verification**}
CLI를 사용한 시스템 백업 및 복원	9.3(2)	CLI를 사용하여 이미지, 인증서를 포함한 전체 시스템 컨피그레이션을 백업하고 복원할 수 있습니다. 다음 명령을 도입했습니다. **backup** 및 **restore**
새로운 ASA 5506W-X 이미지 복구 및 로드	9.4(1)	현재 새로운 ASA 5506W-X 이미지 복구 및 로드를 지원하고 있습니다. 다음 명령을 도입했습니다. **hw-module module wlan recover image**

39 장

시스템 이벤트에 대한 응답 자동화

이 장에서는 EEM(Embedded Event Manager)을 구성하는 방법에 대해 설명합니다.

EEM 정보

EEM 서비스에서는 문제를 디버그할 수 있도록 지원하며 문제 해결을 위한 일반적인 용도의 로깅 기능을 제공합니다. 이 서비스는 두 가지 구성 요소로 구성됩니다. 하나는 EEM에서 응답 또는 수신하는 이벤트이며, 하나는 작업 및 EEM에서 응답하는 이벤트를 정의하는 이벤트 관리자 애플릿입니다. 여러 이벤트 관리자 애플릿을 구성하여 다양한 이벤트에 응답하고 여러 작업을 수행할 수 있습니다.

지원되는 이벤트

EEM에서는 다음과 같은 이벤트를 지원합니다.

- Syslog — ASA에서는 syslog 메시지 ID를 사용하여 이벤트 관리자 애플릿을 트리거하는 syslog 메시지를 식별합니다. 여러 syslog 이벤트를 구성할 수 있지만, syslog 메시지 ID는 단일 이벤트 관리자 애플릿에서 중복되지 않을 수 있습니다.
- Timers(타이머) — 타이머를 사용하여 이벤트를 트리거할 수 있습니다. 각 타이머는 각 이벤트 관리자 애플릿에 한 번만 구성할 수 있습니다. 각 이벤트 관리자 애플릿에는 최대 3개의 타이머가 포함될 수 있습니다. 타이머는 3가지 유형이 있습니다.
  - Watchdog(주기적) 타이머는 애플릿 작업이 완료된 후 지정된 기간이 지나면 이벤트 관리자 애플릿을 트리거하며 자동으로 다시 시작됩니다.
  - Countdown(일회성) 타이머는 지정된 기간이 지나면 이벤트 관리자 애플릿을 한 번 트리거하며 제거한 후 다시 추가하지 않으면 다시 시작되지 않습니다.

- Absolute(하루 한 번) 타이머는 지정된 시간에 하루 한 번씩 이벤트를 실행하며 자동으로 다시 시작됩니다. 시간 형식은 hh:mm:ss입니다.

  각 이벤트 관리자 애플릿에서 각 유형의 타이머 이벤트를 하나만 구성할 수 있습니다.

- None(없음) — CLI 또는 ASDM을 사용하여 수동으로 이벤트 관리자 애플릿을 실행할 경우 이벤트가 트리거됩니다.
- Crash(충돌) — ASA가 충돌할 경우 충돌 이벤트가 트리거됩니다. **output** 명령의 값과 상관없이 **action** 명령은 crashinfo 파일에 직접 적용됩니다. **show tech** 명령에 앞서 출력이 생성됩니다.

이벤트 관리자 애플릿에 대한 작업

이벤트 관리자 애플릿이 트리거되면 이벤트 관리자 애플릿에 대한 작업이 수행됩니다. 각 작업에는 작업의 순서를 지정하는 데 사용되는 번호가 있습니다. 이 순서 번호는 이벤트 관리자 애플릿에서 고유해야 합니다. 이벤트 관리자 애플릿에 여러 작업을 구성할 수 있습니다. 명령은 **show blocks** 같은 일반적인 CLI 명령입니다.

출력 대상

output 명령을 사용하여 지정된 위치에 작업의 출력을 보낼 수 있습니다. 한 번에 하나의 출력 값만 활성화할 수 있습니다. 기본값은 **output none**입니다. 이 값은 **action** 명령의 모든 출력을 무시합니다. 명령은 전역 컨피그레이션 모드에서 권한 수준이 15(가장 높음)인 사용자 권한으로 실행됩니다. 입력은 비활성화되었으므로 명령에서 어떤 입력도 불가합니다. 다음 3개의 위치 중 하나에 **action** CLI 명령의 출력을 보낼 수 있습니다.

- **None(**없음**)** - 기본값이며 출력을 무시합니다.
- **Console(**콘솔**)** - 출력을 ASA 콘솔로 보냅니다.
- **File(**파일**)** - 출력을 파일로 보냅니다. 다음 4가지 파일 옵션이 제공됩니다.
  - **Create a unique file(**고유한 파일 생성**)** - 이벤트 관리자 애플릿이 호출될 때마다 새로운 고유한 이름의 파일을 생성합니다.
  - **Create/overwrite a file(**파일 생성/덮어쓰기**)** - 이벤트 관리자 애플릿이 호출될 때마다 지정된 파일을 덮어씁니다.
  - **Create/append to a file(**파일 생성/파일에 추가**)** - 이벤트 관리자 애플릿이 호출될 때마다 지정된 파일에 추가합니다. 해당 파일이 아직 없는 경우 파일이 생성됩니다.
  - **Create a set of files(**파일 집합 생성**)** - 이벤트 관리자 애플릿이 호출될 때마다 순환되는 고유한 이름의 파일 집합을 생성합니다.

EEM에 대한 지침

이 섹션에서는 EEM을 구성하기 전에 확인해야 하는 지침 및 제한 사항에 대해 설명합니다.

상황 모드 지침

다중 상황 모드에서 지원되지 않습니다.

추가 지침

- 충돌이 진행되는 동안 일반적으로 ASA의 상태를 알 수 없습니다. 이러한 상황에서 일부 명령을 실행할 경우 안전하지 않을 수 있습니다.
- 이벤트 관리자 애플릿의 이름에는 공백을 포함할 수 없습니다.
- None 이벤트 및 Crashinfo 이벤트 매개변수는 수정할 수 없습니다.
- syslog 메시지가 EEM에 전송되어 처리되므로 성능에 영향을 미칠 수 있습니다.
- 각 이벤트 관리자 애플릿의 기본 출력은 **output none**입니다. 이 설정을 변경하려면 다른 출력 값을 입력해야 합니다.
- 각 이벤트 관리자 애플릿에는 출력 옵션을 하나만 정의할 수 있습니다.

EEM 구성

EEM 구성은 다음과 같은 작업으로 이루어집니다.

프로시저

단계 **1** 이벤트 관리자 애플릿 생성 및 이벤트 구성, 1205 페이지.
단계 **2** 작업 및 작업의 출력 대상 구성, 1207 페이지.
단계 **3** 이벤트 관리자 애플릿 실행, 1209 페이지.
단계 **4** 메모리 할당 및 메모리 사용량 추적, 1210 페이지.

이벤트 관리자 애플릿 생성 및 이벤트 구성

이벤트 관리자 애플릿을 생성하고 이벤트를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 이벤트 관리자 애플릿을 생성하고 이벤트 관리자 애플릿 컨피그레이션 모드로 들어갑니다.

event manager applet *name*

예제**:**

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 인수는 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다.

이벤트 관리자 애플릿을 제거하려면 이 명령의 **no** 형식을 입력합니다.

단계 **2** 이벤트 관리자 애플릿을 설명합니다.

description 텍스트

예제**:**

```
ciscoasa(config-applet)# description applet1example
```

text 인수는 최대 256자의 영숫자입니다. 설명 텍스트가 따옴표 안에 있는 경우 설명 텍스트에 공백을 포함할 수 있습니다.

단계 **3** 지정된 이벤트를 구성하려면 다음 명령 중 하나를 입력합니다. 구성된 이벤트를 제거하려면 각 명령의 **no** 형식을 사용합니다.

- syslog 이벤트를 구성하려면 이벤트 관리자 애플릿을 트리거하는 단일한 syslog 메시지 또는 다양한 syslog 메시지를 지정합니다.

  event syslog id *nnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

  예:

  ```
  ciscoasa(config-applet)# event syslog id 106201
  ```

  nnnnnn 인수는 syslog 메시지 ID를 식별합니다. **occurs** *n* 키워드-인수 쌍은 호출되는 이벤트 관리자 애플릿에 syslog 메시지가 발생해야 하는 횟수를 나타냅니다. 기본값은 0초 간격의 1회입니다. 유효한 값은 1 ~ 4294967295입니다. **period** *seconds* 키워드-인수 쌍은 이벤트가 발생해야 하는 시간 간격을 초 단위로 나타내며, 이벤트 관리자 애플릿의 호출 빈도를 구성된 기간 중 최대 1회로 제한합니다. 유효한 값은 0 ~ 604800입니다. 값이 0이면 어떤 기간도 정의되지 않은 것입니다.

- 구성된 기간마다 1회씩 이벤트가 발생하고 자동으로 다시 시작되도록 구성합니다.

  event timer watchdog time *seconds*

  예:

  ```
  ciscoasa(config-applet)# event timer watchdog time 30
  ```

1초 ~ 604800초로 지정할 수 있습니다.

- 이벤트가 한 번 발생하도록 구성하며 이벤트를 제거하고 다시 추가하지 않는 한 다시 시작되지 않습니다.

  event timer countdown time *seconds*

  예:

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  1초 ~ 604800초로 지정할 수 있습니다. Countdown 타이머 이벤트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

  참고 시작 컨피그레이션인 경우 재부팅 시 타이머가 다시 실행됩니다.

- 이벤트가 하루에 한 번 지정된 시간에 발생하고 자동으로 다시 시작되도록 구성합니다.

  event timer absolute time *hh:mm:ss*

  예:

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  시간 형식은 hh:mm:ss입니다. 시간 범위는 00:00:00(자정)부터 23:59:59까지입니다.

- ASA가 충돌할 경우 충돌 이벤트를 트리거합니다.

  event crashinfo

  예:

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

  output 명령의 값과 상관없이 **action** 명령은 crashinfo 파일에 직접 적용됩니다. **show tech** 명령에 앞서 출력이 생성됩니다.

작업 및 작업의 출력 대상 구성

작업 및 작업의 출력을 전송할 특정 대상을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 이벤트 관리자 애플릿에 대한 작업을 구성합니다.

action *n* **cli command** "*command*"

예제:

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

n 옵션은 작업 ID입니다. 유효한 ID 범위는 0 ~ 4294967295입니다. *command* 옵션의 값은 따옴표로 묶어야 합니다. 이렇게 하지 않으면 명령이 여러 개의 단어로 이루어진 경우 오류가 발생합니다. 명령은 전역 컨피그레이션 모드에서 권한 수준이 15(가장 높음)인 사용자 권한으로 실행됩니다. 입력은 비활성화되었으므로 명령에서 어떤 입력도 불가합니다. 명령에서 사용 가능하도록 설정한 경우 **noconfirm** 옵션을 사용합니다.

단계 **2** 사용 가능한 출력 대상 옵션 중 하나를 선택합니다. 출력 대상을 제거하려면 각 명령의 **no** 형식을 사용합니다.

- **None** 옵션은 **action** 명령의 모든 출력을 무시하며, 이는 기본 설정입니다.

  output none

  예:

  ```
  ciscoasa(config-applet)# output none
  ```

- **Console** 옵션은 **action** 명령의 출력을 콘솔에 전송합니다.

  output console

  예:

  ```
  ciscoasa(config-applet)# output console
  ```

  참고 이 명령을 실행할 경우 성능에 영향을 미칩니다.

- **New File** 옵션은 **action** 명령의 출력을 호출된 각 이벤트 관리자 애플릿을 위한 새 파일에 전송합니다.

  output file new

  예:

  ```
  ciscoasa(config-applet)# output file new
  ```

  파일 이름의 형식은 eem-*applet*-*timestamp*.log입니다. 여기서 *applet*은 이벤트 관리자 애플릿의 이름이고 *timestamp*는 YYYYMMDD-hhmmss 형식의 날짜 타임 스탬프입니다.

- **New Set of Rotated Files** 옵션은 순환되는 파일 집합을 생성합니다. 새 파일이 작성되면 가장 오래된 파일이 삭제되며, 첫 번째 파일이 작성되기 전에 모든 후속 파일의 번호가 다시 지정됩니다.

  output file rotate *n*

  예:

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

최신 파일은 0으로 표시되고 가장 오래된 파일은 가장 큰 숫자(*n*-1)로 표시됩니다. *n* 옵션은 순환 값입니다. 유효한 값의 범위는 2 ~ 100입니다. 파일 이름의 형식은 eem-*applet*-*x*.log이며, 여기서 *applet*은 애플릿의 이름이고 *x*는 파일 번호입니다.

- **Single Overwritten File** 옵션은 **action** 명령 출력을 단일 파일에 작성하며 매번 이 파일에 덮어쓰기합니다.

  output file overwrite 파일 이름

  예:

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  filename 인수는 로컬(ASA) 파일 이름입니다. 이 명령에서는 FTP, TFTP 및 SMB 대상 파일을 사용할 수도 있습니다.

- **Single Appended File** 옵션은 **action** 명령 출력을 단일 파일에 작성하되 매번 이 파일에 추가합니다.

  output file append 파일 이름

  예:

  ```
  ciscoasa(config-applet)# output file append examplefile1
  ```

  filename 인수는 로컬(ASA) 파일 이름입니다.

이벤트 관리자 애플릿 실행

이벤트 관리자 애플릿을 실행하려면 다음 단계를 수행합니다.

프로시저

이벤트 관리자 애플릿을 실행합니다.

event manager run 애플릿

예제**:**

```
ciscoasa# event manager run exampleapplet1
```

event none 명령으로 구성하지 않은 이벤트 관리자 애플릿을 실행하면 오류가 발생합니다. *applet* 인수는 이벤트 관리자 애플릿의 이름입니다.

메모리 할당 및 메모리 사용량 추적

메모리 할당 및 메모리 사용량을 기록하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 메모리 로깅을 활성화합니다.

memory logging [1024-4194304] [**wrap**] [**size** [1-2147483647]] [**process** *process-name*] [**context** *context-name*]

예제:

```
ciscoasa(config)# memory logging 202980
```

유일한 필수 인수는 메모리 로깅 버퍼의 항목 수입니다. **wrap** 옵션은 메모리 로깅 유틸리티가 래핑할 때 버퍼를 저장하도록 알려줍니다. 버퍼는 한 번만 저장할 수 있습니다.

메모리 로깅 버퍼가 여러 번 래핑하는 경우, 덮어쓰일 수 있습니다. 버퍼가 래핑할 때 데이터 저장을 활성화하도록 이벤트 관리자에게 트리거가 전송됩니다. **size** 옵션은 특정 크기를 모니터링합니다. **process** 옵션은 특정 프로세스를 모니터링합니다.

참고 Checkheaps 프로세스는 표준이 아닌 방식으로 메모리 할당자를 사용하기 때문에 프로세스로 완전히 무시됩니다.

context 옵션은 지정된 이름별로 지정된 가상 상황에 대해 메모리 로깅을 기록합니다.

메모리 로깅 파라미터를 변경하려면 이 파라미터를 비활성화한 다음 다시 활성화하십시오.

단계 **2** 메모리 로깅 결과를 표시합니다.

```
show memory logging [brief | wrap]
show memory logging include [address] [caller] [operator] [size] [process] [time] [context]
```

예제:

```
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
```

```
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b

ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free]
size=72 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server Process]
oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[ci/console] oper=[malloc] size=72 process=[ci/console]
oper=[free] size=72 ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
```

```
Number of realloc-new                    0
Number of realloc-free                   0
Number of realloc-null                   0
Number of realloc-same                   0
Number of calloc-fail                    0
Number of malloc-fail                    0
Number of realloc-fail                   0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

옵션이 없는 경우 **show memory logging**은 통계를 표시한 다음 기록한 작업을 표시합니다. **brief** 옵션은 통계만 보여 줍니다. **wrap** 옵션은 래핑 시 버퍼를 보여준 다음 중복 데이터가 나타나지 않거나 저장되지 않도록 데이터를 제거합니다. **include** 옵션은 출력에 지정된 필드만 포함합니다. 순서에 상관없이 필드를 지정할 수 있지만, 항상 다음 순서로 표시됩니다.

1. 프로세스
2. 시간
3. 상황(단일 모드가 아닌 경우)
4. 작업(free/malloc/등)
5. 주소
6. 크기
7. 발신자

출력 형식은 다음과 같습니다.

process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

최대 4개의 발신자 주소가 나타납니다. 작업 유형은 예에서 표시된 출력(...의 수)에 나열되어 있습니다.

단계 **3** 메모리 로깅 래핑 이벤트에 응답합니다.

event memory-logging-wrap

예제**:**

```
ciscoasa(config)# event manager applet memlog
ciscoasa(config)# event memory-logging-wrap
ciscoasa(config)# action 0 cli command "show memory logging wrap"
ciscoasa(config)# output file append disk0:/memlog.log
```

이 예는 모든 메모리 할당을 기록하는 애플릿을 보여 줍니다. 메모리 로깅에 대해 래핑을 활성화한 경우 메모리 로거가 구성된 애플릿을 트리거하기 위해 이벤트 관리자에게 이벤트를 전송합니다.

EEM의 예

다음 예에서는 매시간 누출 차단 정보를 기록하고 순환 로그 파일 집합에 출력을 작성하여 1일분의 로그를 보관하는 이벤트 관리자 애플릿을 보여줍니다.

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

다음 예에서는 매일 오전 1시에 ASA를 재부팅하고 필요하다면 구성을 저장하는 이벤트 관리자 애플릿을 보여 줍니다.

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

다음 예에서는 자정부터 오전 3시까지 지정된 인터페이스를 비활성화하는 이벤트 관리자 애플릿을 보여줍니다.

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

EEM 모니터링

EEM을 모니터링하려면 다음 명령을 참고하십시오.

- **clear configure event manager**

  이 명령은 이벤트 관리자에서 실행 중인 컨피그레이션을 제거합니다.

- **clear configure event manager applet** *appletname*

  이 명령은 명명된 이벤트 관리자 애플릿을 컨피그레이션에서 제거합니다.

- **show counters protocol eem**

  이 명령은 이벤트 관리자에 대한 카운터를 표시합니다.

- **show event manager**

  이 명령은 구성된 이벤트 관리자 애플릿에 대한 정보를 표시하며, 여기에는 히트 수 및 이벤트 관리자 애플릿이 마지막으로 호출된 시기 등이 포함됩니다.

- **show memory logging, show memory logging include**

  이 명령은 메모리 할당 및 메모리 사용량에 대한 통계를 보여 줍니다.

- **show running-config event manager**

  이 명령은 이벤트 관리자의 실행 중인 컨피그레이션을 표시합니다.

EEM에 대한 기록

표 ***51: EEM***에 대한 기록

기능 이름	플랫폼 릴리스	설명
EEM(Embedded Event Manager)	9.2(1)	EEM 서비스에서는 문제를 디버그할 수 있도록 지원하며 문제 해결을 위한 일반적인 용도의 로깅 기능을 제공합니다. 이 서비스는 두 가지 구성 요소로 구성됩니다. 하나는 EEM에서 응답 또는 수신하는 이벤트이며, 하나는 작업 및 EEM에서 응답하는 이벤트를 정의하는 이벤트 관리자 애플릿입니다. 여러 이벤트 관리자 애플릿을 구성하여 다양한 이벤트에 응답하고 여러 작업을 수행할 수 있습니다. 다음 명령을 도입하거나 수정했습니다. **event manager applet**, **description**, **event syslog id**, **event none**, **event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}, **event crashinfo**, **action cli command**, **output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}, **show running-config event manager**, **event manager run**, **show event manager**, **show counters protocol eem**, **clear configure event manager**, **debug event manager**, **debug menu eem**
EEM의 메모리 추적	9.4(1)	메모리 할당 및 메모리 사용량을 기록하고 메모리 로깅 래핑 이벤트에 응답하기 위해 새로운 디버깅 기능을 추가했습니다. 다음 명령을 도입 또는 수정했습니다. **memory logging**, **show memory logging**, **show memory logging include**, **event memory-logging-wrap**

40 장

테스트 및 트러블슈팅

이 장에서는 Cisco ASA를 트러블슈팅하고 기본 연결을 테스트하는 방법을 설명합니다.

Enable 비밀번호 및 텔넷 비밀번호 복구

enable 비밀번호나 텔넷 비밀번호를 잊은 경우 복구할 수 있습니다. 이 절차는 디바이스 유형에 따라 다릅니다. CLI를 사용하여 작업을 수행해야 합니다.

ASA의 비밀번호 복구

ASA의 비밀번호를 복구하려면 다음 단계를 수행합니다.

프로시저

단계 **1** ASA 콘솔 포트에 연결합니다.

단계 **2** ASA의 전원을 끈 후 전원을 켭니다.

단계 **3** 시작한 다음 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

단계 **4** 컨피그레이션 레지스터 값을 업데이트하려면 다음 명령을 입력합니다.

```
rommon #1> confreg 0x41
```

```
Update Config Register (0x41) in NVRAM...
```

단계 **5** ASA에서 시작 구성을 무시하도록 설정하려면 다음 명령을 입력합니다.

```
rommon #1> confreg
```

ASA는 현재 구성 레지스터 값을 표시하고 이를 변경할지 묻습니다.

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

단계 **6** 나중에 복원할 수 있도록 현재 컨피그레이션 레지스터 값을 기록해 둡니다.

단계 **7** 값을 변경하기 위해 프롬프트에서 **Y**를 입력합니다.

ASA 프롬프트에 새 값을 입력합니다.

단계 **8** "disable system configuration?" 값을 제외하고 모든 설정에 기본값을 적용합니다.

단계 **9** 프롬프트에 **Y**를 입력합니다.

단계 **10** 다음 명령을 입력하여 ASA를 다시 로드합니다.

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA는 시작 구성 대신 기본 구성을 로드합니다.

단계 **11** 다음 명령을 입력하여 특별 권한 EXEC 모드에 액세스합니다.

```
ciscoasa# enable
```

단계 **12** 비밀번호를 물으면 **Enter** 키를 누릅니다.

비밀번호는 비어 있습니다.

단계 **13** 다음 명령을 입력하여 시작 컨피그레이션을 로드합니다.

```
ciscoasa# copy startup-config running-config
```

단계 **14** 다음 명령을 입력하여 전역 컨피그레이션 모드에 액세스합니다.

```
ciscoasa# configure terminal
```

단계 **15** 필요하다면 다음 명령을 입력하여 기본 컨피그레이션에서 비밀번호를 변경합니다.

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

단계 **16** 다음 명령을 입력하여 기본 컨피그레이션을 로드합니다.

```
ciscoasa(config)# no config-register
```

기본 컨피그레이션 레지스터 값은 0x1입니다. 구성 레지스터에 대한 자세한 내용은 명령 참조를 참고하십시오.

단계 **17** 다음 명령을 입력하여 새 비밀번호를 시작 컨피그레이션에 저장합니다.

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506-X, ASA 5508-X 및 ASA 5516-X에서 비밀번호 복구

ASA 5506-X, ASA 5508-X 및 ASA 5516-X의 비밀번호를 복구하려면 다음 단계를 수행합니다.

프로시저

단계 **1** ASA 콘솔 포트에 연결합니다.

단계 **2** ASA의 전원을 끈 후 전원을 켭니다.

단계 **3** 시작한 다음 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

단계 **4** 컨피그레이션 레지스터 값을 업데이트하려면 다음 명령을 입력합니다.

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA는 현재 구성 레지스터 값과 구성 옵션의 목록을 표시합니다. 나중에 복원할 수 있도록 현재 컨피그레이션 레지스터 값을 기록해 둡니다.

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ..... auto-boot index 1 image in disks
```

단계 **5** 다음 명령을 입력하여 ASA를 다시 로드합니다.

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA는 시작 구성 대신 기본 구성을 로드합니다.

단계 **6** 다음 명령을 입력하여 특별 권한 EXEC 모드에 액세스합니다.

```
ciscoasa# enable
```

단계 **7** 비밀번호를 물으면 **Enter** 키를 누릅니다.

비밀번호는 비어 있습니다.

단계 **8** 다음 명령을 입력하여 시작 컨피그레이션을 로드합니다.

```
ciscoasa# copy startup-config running-config
```

단계 **9** 다음 명령을 입력하여 전역 컨피그레이션 모드에 액세스합니다.

```
ciscoasa# configure terminal
```

단계 **10** 필요하다면 다음 명령을 입력하여 기본 컨피그레이션에서 비밀번호를 변경합니다.

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

단계 **11** 다음 명령을 입력하여 기본 컨피그레이션을 로드합니다.

```
ciscoasa(config)# no config-register
```

기본 컨피그레이션 레지스터 값은 0x1입니다. 구성 레지스터에 대한 자세한 내용은 명령 참조를 참고하십시오.

단계 **12** 다음 명령을 입력하여 새 비밀번호를 시작 컨피그레이션에 저장합니다.

```
ciscoasa(config)# copy running-config startup-config
```

ASAv에서 비밀번호 또는 이미지 복구

ASAv의 비밀번호 또는 이미지를 복구하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 실행 중인 구성을 ASAv의 백업 파일에 복사합니다.

copy running-config 파일 이름

예제:

```
ciscoasa# copy running-config backup.cfg
```

단계 **2** ASAv를 다시 시작합니다.

reload

단계 **3** GNU GRUB 메뉴에서 아래쪽 화살표를 누르고 <**filename**> **with no configuration load** 옵션을 선택한 다음 **Enter** 키를 누릅니다. filename은 ASAv의 기본 부트 이미지 파일 이름입니다. 기본 부트 이미지는 **fallback** 명령을 통해 자동으로 부팅되지 않습니다. 그리고 선택된 부트 이미지를 로드합니다.

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

예제:

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

단계 **4** 백업 컨피그레이션 파일을 실행 중인 컨피그레이션에 복사합니다.

copy 파일 이름 **running-config**

예제:

```
ciscoasa (config)# copy backup.cfg running-config
```

단계 **5** 비밀번호를 초기화합니다.

enable password *password*

예제:

```
ciscoasa(config)# enable password cisco123
```

단계 **6** 새 컨피그레이션을 저장합니다.

write memory

예제:

```
ciscoasa(config)# write memory
```

비밀번호 복구 비활성화

참고 ASAv에서 비밀번호 복구를 비활성화할 수 없습니다.

허가받지 않은 사용자가 ASA를 공격할 목적으로 비밀번호 복구 메커니즘을 이용할 수 없도록 비밀번호 복구를 비활성화하려면 다음 단계를 수행합니다.

시작하기 전에

ASA에서 **no service password-recovery** 명령은 구성을 그대로 유지하면서 ROMMON 모드를 시작할 수 없게 합니다. ROMMON 모드에 들어가면 ASA에서는 모든 플래시 파일 시스템을 지우라는 메시지를 표시합니다. ROMMON 모드를 시작하려면 먼저 이 지우기를 수행해야 합니다. 플래시 파일 시스템을 지우지 않겠다고 선택하면 ASA가 다시 로드됩니다. 비밀번호를 복구하려면 ROMMON 모드를 사용하고 기존 컨피그레이션을 유지해야 하므로, 이와 같이 지우기를 수행하면 비밀번호를 복구할 수 없게 됩니다. 그러나 비밀번호 복구를 비활성화하면 권한 없는 사용자가 컨피그레이션을 보거나 다른 비밀번호를 삽입하지 못하게 됩니다. 이러한 경우 시스템을 정상 상태로 복원하려면 새 이미지와 백업 컨피그레이션 파일(있는 경우)을 로드합니다.

참고로 **service password-recovery** 명령이 구성 파일에 나타납니다. CLI 프롬프트에서 이 명령을 입력하면 설정이 NVRAM에 저장됩니다. 설정을 변경하는 방법은 CLI 프롬프트에 명령을 입력하는 방법밖에 없습니다. 다른 버전의 명령을 사용하여 새 컨피그레이션을 로드하면 설정이 변경되지 않습니다. (비밀번호 복구를 염두에 두고) ASA에서 시작할 때 시작 구성을 무시하도록 구성된 상태에서 비밀번호 복구를 비활성화하면 ASA는 설정을 변경하여 평소와 같이 시작 구성을 로드합니다. 페일오버를 사용하고 스탠바이 유닛이 시작 구성을 무시하도록 구성된 경우 **no service password- recovery** 명령이 스탠바이 유닛에 복제되면 동일한 변경사항이 구성 레지스터에 적용됩니다.

프로시저

비밀번호 복구를 비활성화합니다.

no service password-recovery

예제:

```
ciscoasa (config)# no service password-recovery
```

디버깅 메시지 보기

디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되기 때문에 시스템을 사용할 수 없게 만들 수 있습니다. 따라서 **debug** 명령은 특정 문제를 트러블슈팅하거나 Cisco TAC를 통해 세션 문제를 트러블슈팅하는 동안에만 사용해야 합니다. 또한 네트워크 트래픽 및 사용자 수가 적을 때 **debug** 명령을 사용하는 것이 가장 좋습니다. 그러한 기간에 디버깅하면 **debug** 명령의 처리 오버헤드 증가로 인해 시스템 사용에 지장이 생길 가능성이 줄어듭니다. 디버깅 메시지를 활성화하려면 명령 참조에서 **debug** 명령을 참고하십시오.

패킷 캡처

패킷 캡처는 연결 문제를 트러블슈팅하거나 의심스러운 활동을 모니터링할 때 유용할 수 있습니다. 패킷 캡처 서비스를 이용하려면 Cisco TAC에 문의하는 것이 좋습니다.

패킷 캡처 관련 지침

상황 모드

- 특정 상황 내에서 클러스터 제어 링크에 캡처를 구성할 수 있습니다. 클러스터 제어 링크에서 전송된 상황과 연결된 패킷만 캡처됩니다.
- 공유 VLAN에서는 하나의 캡처만 구성할 수 있습니다. 공유 VLAN에서 다중 상황 캡처를 구성할 경우, 구성된 마지막 캡처만 사용됩니다.
- 마지막으로 구성된 (활성) 캡처를 삭제하면, 어떤 캡처도 활성화되지 않습니다. 앞서 다른 컨텍스트에서 캡처를 구성했더라도 그렇습니다. 캡처를 삭제한 다음 다시 추가하여 활성 상태로 만들어야 합니다.
- 캡처가 연결된 인터페이스로 들어오는 모든 트래픽이 캡처됩니다. 공유 VLAN의 다른 컨텍스트로 가는 트래픽도 포함됩니다. 따라서 컨텍스트 B에서도 사용하는 VLAN에서 컨텍스트 A의 캡처를 활성화한 경우 컨텍스트 A와 컨텍스트 B의 인그레스 트래픽이 모두 캡처됩니다.
- 이그레스 트래픽의 경우 활성 캡처의 컨텍스트 트래픽만 캡처됩니다. 유일한 예외는 ICMP 검사를 활성화하지 않은 경우입니다. 그러면 ICMP 트래픽은 가속 경로에 세션이 없습니다. 그러한 경우 공유 VLAN의 모든 컨텍스트에 대한 인그레스 및 이그레스 ICMP 트래픽이 캡처됩니다.

추가 지침

- *invalid-tcp-hdr-length* ASP 폐기 사유로 인해 TCP 헤더의 형식이 잘못된 패킷이 ASA에 수신될 경우, 이러한 패킷이 수신되는 인터페이스의 **show capture** 명령 출력에서는 해당 패킷을 표시하지 않습니다.
- IP 트래픽만 캡처할 수 있습니다. ARP와 같은 비 IP 패킷은 캡처할 수 없습니다.

- 인라인 SGT 태그 처리된 패킷의 경우, 캡처된 패킷은 PCAP 뷰어에서 이해하지 못할 추가 CMD 헤더를 포함합니다.
- 패킷 캡처는 검사, NAT, TCP 정규화 또는 패킷의 콘텐츠를 조정하는 다른 기능 때문에 시스템이 연결에 삽입하거나 연결을 수정하는 패킷을 포함합니다.

패킷 캡처

패킷을 캡처하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화합니다.

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**match** *protocol* { **host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] { **host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

예제**:**

```
ciscoasa# capture captest interface inside
```

캡처할 모든 패킷에 대해 인터페이스를 구성해야 합니다. 여러 트래픽 유형을 캡처하려면 여러 **capture** 구문에 동일한 *capture_name*을 사용합니다.

type asp-drop 키워드는 가속화된 보안 경로에 의해 폐기된 패킷을 캡처합니다. 클러스터에서는 유닛 간의 드롭된 전달 데이터 패킷도 캡처합니다. 다중 상황 모드에서는 이 옵션을 시스템 실행 공간에서 실행하면 모든 드롭된 데이터 패킷이 캡처됩니다. 이 옵션을 상황에서 실행하면 해당 상황에 속한 인터페이스에서 들어온 드롭된 데이터 패킷만 캡처됩니다.

type raw-data 키워드는 인바운드 및 아웃바운드 패킷을 캡처합니다. 이 설정이 기본값입니다.

inline-tag *tag* 키워드-인수 쌍은 특정 SGT 값에 대한 태그를 지정하거나, 지정하지 않은 채로 두어 임의의 SGT 값을 갖는 태그 처리된 패킷을 캡처합니다.

buffer 키워드는 패킷 저장에 쓰이는 버퍼 크기를 정의합니다. 바이트 버퍼가 차면 패킷 캡처를 중지합니다. 클러스터에서 사용될 때는 모든 유닛의 합계가 아니라 유닛별 크기입니다. **circular-buffer** 키워드는 버퍼가 찼을 때 버퍼의 처음부터 덮어쓰기 시작합니다.

interface 키워드는 패킷 캡처를 사용하는 인터페이스의 이름을 설정합니다.

데이터 플레인에서 패킷을 캡처하려면 **asa_dataplane** 키워드를 사용합니다. 애드온 모듈 백플레인에서 캡처된 패킷을 필터링하려면 **asa_dataplane** 옵션을 사용하고 다음 지침을 준수하십시오. 단일 모드에서 백플레인 제어 패킷은 액세스 목록을 우회하고 캡처됩니다. 다중 상황 모드에서는 제어 패킷만 시스템 실행 공간에서 캡처됩니다. 데이터 패킷은 상황에서 캡처됩니다.

match 키워드는 프로토콜, 소스 및 대상 IP 주소, 선택적 포트 매칭을 캡처합니다. 하나의 명령에서 이 키워드를 최대 3번 사용할 수 있습니다. **any** 키워드는 IPv4 트래픽만 캡처합니다. 일치하는 IPv4 및 IPv6 네트워크 트래픽을 각각 캡처하려면 **any4** 및 **any6** 키워드를 사용할 수 있습니다. 연산자는 다음 중 하나일 수 있습니다.

- lt — 다음보다 작음
- gt — 다음보다 큼
- eq — 다음과 같음

real-time 키워드는 캡처된 패킷을 실시간으로 계속 표시합니다.

reinject-hide 키워드는 어떤 reinjected 패킷도 캡처하지 않게 하며, 클러스터링 환경에서만 적용됩니다.

참고 ACL 최적화가 구성된 경우 캡처에 **access-list** 명령을 사용할 수 없습니다. **access-group** 명령만 사용할 수 있습니다. 이 경우에 **access-list** 명령을 사용하려고 시도하면 오류가 표시됩니다.

단계 **2** 클러스터 제어 링크 트래픽 캡처:

capture *capture_name* { **type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* { **host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] { **host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

예제**:**

```
ciscoasa# capture ccl type lacp interface GigabitEthernet0/0
ciscoasa# capture ccl interface cluster match udp any eq 49495 any
ciscoasa# capture ccl interface cluster match udp any any eq 49495
```

두 가지 방법으로 클러스터 제어 링크 트래픽을 캡처할 수 있습니다. 클러스터 제어 링크에서 모든 트래픽을 캡처하려면 인터페이스 이름에 **cluster** 키워드를 사용합니다. cLACP 패킷만 캡처하려면 **type lacp**를 지정하고 인터페이스 이름 대신 물리적 인터페이스 ID를 지정합니다. 클러스터 제어 링크에는 2가지 패킷 유형이 있습니다. 컨트롤 플레인 패킷과 데이터 플레인 패킷입니다. 둘 다 전달 데이터 트래픽과 클러스터 LU 메시지를 포함합니다. IP 주소 헤더의 TTL 필드가 인코딩되어 이 두 패킷 유형을 구별합니다. 전달 데이터 패킷이 캡처될 때 디버깅을 위해 그 클러스터링 트레일러가 캡처 파일에 포함됩니다.

단계 **3** 패킷 클러스터 전체 캡처:

cluster exec capture *capture_name arguments*

단계 **4** 패킷 캡처를 중지합니다.

no capture *capture_name*

실시간 패킷 캡처를 종료하려면 **Ctrl + c**를 입력합니다**.** 캡처를 영구적으로 제거하려면 이 명령의 **no** 형식을 사용합니다. 실시간 옵션은 **raw-data** 및 **asp-drop** 캡처에만 적용됩니다.

단계 **5** 버퍼에서 패킷을 제거하지 않고 패킷 캡처를 수동으로 중지하려면 다음 작업을 수행합니다.

capture *name* **stop**

단계 **6** 캡처를 다시 시작합니다.

no capture *name* **stop**

단계 **7** 클러스터 유닛에서 영구 패킷 추적을 캡처합니다.

cluster exec *capture_test* **persist**

단계 **8** 영구 패킷 추적을 지웁니다.
cluster exec *clear* **packet-trace**

단계 **9** 암호 해독된 IPsec 패킷을 캡처합니다.

cluster exec *capture_test* **include-decrypted**

단계 **10** 캡처를 지웁니다.
clear capture *capture_name*

예

제어 플레인 패킷

제어 플레인을 오고 가는 패킷에 255의 TTL이 있고 포트 번호 49495는 제어-플레인 수신 대기에 사용됩니다. 다음 예에서는 클러스터링 환경에서 LACP 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa# capture lacp type lacp interface GigabitEthernet0/0
```

다음 예는 클러스터링 링크에서 제어 경로 패킷의 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa# capture cp interface cluster match udp any eq 49495 any
ciscoasa# capture cp interface cluster match udp any any eq 49495
```

데이터 플레인 패킷

데이터 패킷은 한 유닛에서 다른 유닛(연결 소유자)으로 전달되는 패킷과 클러스터 LU 메시지를 포함합니다. 일반 클러스터 LU 업데이트 메시지에는 254의 TTL이 있으며 253의 TTL이 있는 특수 LU 패킷이 있습니다. 이 특수 LU 패킷은 TCP 전용이며 관리자가 새 플로우 소유자를 선택하는 경우에만 발생합니다. 관리자는 CLU_FULL 업데이트 패킷과 함께 요청 패킷을 다시 보냅니다. LU 패킷은 수신자 측에서 잠재적인 경합 상태를 방지하기 위해 원래 패킷의 L3/L4 헤더로 채워집니다. 전달된 데이터 패킷은 4보다 작은 TTL을 갖습니다. 다음 예는 클러스터 제어 링크에서 데이터 경로 패킷의 캡처를 생성하는 방법을 보여 줍니다. 모든 클

러스터 간 데이터 플레인의 "플로우 논리적 업데이트" 메시지를 캡처하려면 4193 포트를 사용합니다.

```
ciscoasa# access-list cc1 extended permit udp any any eq 4193
ciscoasa# access-list cc1 extended permit udp any eq 4193 any
ciscoasa# capture dp interface cluster access-list ccl
```

패킷 캡처 보기

브라우저의 CLI에서 패킷 캡처를 보거나 선택한 서버로 캡처를 다운로드할 수 있습니다.

프로시저

단계 **1** CLI에서 캡처를 확인합니다.

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

예제**:**

```
ciscoasa# show capture capin

 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

access-list 키워드는 특정 액세스 목록 식별을 위해 IP 또는 해당 상위 필드를 기반으로 하는 패킷에 대한 정보를 표시합니다.

cluster exec 키워드를 사용하면 1개 유닛에서 **show capture** 명령을 실행하고 동시에 모든 다른 유닛에서 명령을 실행합니다.

count 키워드는 데이터가 지정된 패킷 수를 표시합니다.

decode 키워드는 **isakmp** 유형의 캡처를 인터페이스에 적용할 때 유용합니다. 이 인터페이스를 통과하는 모든 ISAKMP 데이터는 암호 해독 후에 캡처되며 필드를 디코딩한 후 추가 정보와 함께 표시됩니다. 패킷의 디코딩된 출력은 패킷의 프로토콜에 따라 달라집니다. 일반적으로 이 명령은 ICMP, UDP 및 TCP 프로토콜에 대한 IP 디코딩을 지원합니다. 버전 9.10(1)에서 이 명령은 또한 GRE 및 IPinIP에 대한 IP 디코딩을 지원합니다.

detail 키워드는 각 패킷에 대한 추가 프로토콜 정보를 표시합니다.

dump 키워드는 데이터 링크를 통해 전송되는 패킷의 16진수 덤프를 표시합니다.

packet-number 키워드는 지정된 패킷 번호에서 표시를 시작합니다.

단계 **2** 브라우저에서 패킷 캡처를 확인합니다.

https://*ip_of_asa*/**admin/capture/***capture_name*/**pcap**

pcap 키워드를 벗어나면 **show capture** *capture_name* 명령 출력과 동일한 내용만 제공됩니다.

다중 상황 모드에서는 시스템 실행 영역에서만 **copy capture** 명령을 사용할 수 있습니다.

단계 **3** 서버에 패킷 캡처를 복사합니다. 이 예에서는 FTP를 보여 줍니다.

[**cluster exec**] **copy /pcap capture:**[*context-name*/]*capture_name* **ftp://***username***:***password***@***server_ip*/*path*

pcap 키워드를 벗어나면 **show capture** *capture_name* 명령 출력과 동일한 내용만 제공됩니다.

예

다음 예에서는 type asp-drop 캡처를 보여 줍니다.

```
ciscoasa# capture asp-drop type asp-drop acl-drop
ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

다음 예에서는 ethernet-type 캡처를 보여 줍니다.

```
ciscoasa# capture arp ethernet-type arp interface inside
ciscoasa# show cap arp

22 packets captured

   1: 05:32:52.119485       arp who-has 10.10.3.13 tell 10.10.3.12
   2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
   3: 05:32:52.481878       arp who-has 192.168.10.50 tell 192.168.100.10
   4: 05:32:53.409723       arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085       arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429       arp who-has 10.106.44.135 tell 10.106.44.244
```

```
7: 05:32:54.784695       arp who-has 10.106.44.1 tell 11.11.11.112:
```

크래시 덤프 보기

ASA 또는 ASAv에 충돌이 발생한 경우 크래시 덤프 정보를 볼 수 있습니다. 크래시 덤프를 해석하려면 Cisco TAC에 문의하는 것이 좋습니다. 명령 참조에서 **show crashdump** 명령을 참고하십시오.

코어덤프 보기

코어덤프는 프로그램이 비정상적으로 종료했거나 충돌했을 때 실행 중이던 프로그램의 스냅샷입니다. 코어덤프는 오류를 진단하거나 디버깅하는 데 그리고 향후 오프사이트 분석을 위해 충돌 상황을 저장하는 데 사용합니다. Cisco TAC에서 ASA 또는 ASAv의 애플리케이션이나 시스템 충돌 문제를 트러블슈팅하기 위해 코어덤프 기능을 활성화하도록 요청할 수 있습니다. 명령 참조에서 **coredump** 명령을 참조하십시오.

ASAv의 vCPU 사용량

ASAv vCPU 사용량에서는 데이터 경로, 제어 지점, 외부 프로세스에 사용된 vCPU의 양을 보여 줍니다.

vSphere에서 보고하는 vCPU 사용량에는 앞서 설명한 ASAv 사용량과 함께 다음 항목도 포함되어 있습니다.

- ASAv 유휴 시간
- ASAv VM에 사용된 %SYS 오버헤드
- vSwitch, vNIC, pNIC 간 패킷 이동의 오버헤드. 이 오버헤드가 상당히 클 수 있습니다.

CPU 사용량의 예

다음은 보고된 vCPU 사용량이 상당한 차이를 보이는 예입니다.

- ASAv 보고서: 40%
- DP: 35%
- 외부 프로세스: 5%
- vSphere 보고서: 95%
- ASA(ASAv 보고서): 40%
- ASA 유휴 폴링: 10%

- 오버헤드: 45%

이 오버헤드는 하이퍼바이저 기능을 수행하고 vSwitch를 사용하여 NIC와 vNIC 간에 패킷을 이동하는 데 사용됩니다.

사용량이 100%를 초과하기도 합니다. ESXi 서버에서 ASAv 대신 추가 컴퓨팅 리소스를 오버헤드로 사용할 수 있기 때문입니다.

VMware CPU 사용량 보고

vSphere에서 **VM Performance(VM** 성능**)** 탭을 클릭하고 **Advanced(**고급**)**를 클릭하여 **Chart Options(**차트 옵션**)** 드롭다운 목록을 표시합니다. 여기서는 VM의 상태별 vCPU 사용량(%USER, %IDLE, %SYS 등)을 보여줍니다. 이 정보는 VMware의 관점에서 CPU 리소스 사용처를 파악하는 데 유용합니다.

ESXi 서버 셸(SSH로 호스트에 연결하는 방법으로 액세스)에서 esxtop을 사용할 수 있습니다. esxtop은 Linux **top** 명령과 비슷하게 생겼고 다음과 같이 vSphere 성능에 대한 VM 상태 정보를 제공합니다.

- vCPU, 메모리, 네트워크 사용량 세부 사항
- 각 VM의 상태별 vCPU 사용량
- 메모리(실행 중에 M 입력) 및 네트워크(실행 중에 N 입력), 통계, RX 드롭 수

ASAv 및 vCenter 그래프

ASAv와 vCenter의 CPU % 수치가 다릅니다.

- vCenter 그래프 수치가 항상 ASAv 수치보다 높습니다.
- vCenter에서는 이를 %CPU usage, ASAv에서는 %CPU utilization이라고 부릅니다.

용어 "%CPU utilization"과 "%CPU usage"의 의미는 서로 다릅니다.

- CPU utilization은 물리적 CPU의 통계를 제공합니다.
- CPU usage는 논리적 CPU의 통계로서 CPU 하이퍼스레딩을 기반으로 합니다. 그러나 단 하나의 vCPU가 사용되므로 하이퍼스레딩은 켜져 있지 않습니다.

vCenter는 %CPU usage를 다음과 같이 계산합니다.

활발하게 사용 중인 가상 CPU의 양 - 총 가용 CPU 기준 백분율로 표시

이 계산은 게스트 운영 체제가 아닌 호스트의 관점에서 본 CPU 사용량입니다. 그리고 가상 머신에 있는 사용 가능한 모든 가상 CPU의 평균 CPU 사용률입니다.

예를 들어, 가상 CPU 1개를 사용하는 가상 시스템이 4개의 물리적 CPU를 가진 호스트에서 실행되는 중이고 CPU usage가 100%라면 가상 머신에서 하나의 물리적 CPU를 온전히 사용하는 것입니다. 가상 CPU 사용량 계산: 사용량(MHz) / 가상 CPU 수 x 코어 주파수

사용량(MHz)을 비교하면 vCenter 수치와 ASAv 수치가 동일합니다. vCenter 그래프에 의거하여 MHz % CPU 사용량은 60/(2499 x 1 vCPU) = 2.4로 계산됩니다.

구성 테스트

이 섹션에서는 단일 모드 ASA 또는 각 보안 상황에 대한 연결을 테스트하는 방법, ASA 인터페이스를 ping하는 방법, 한 인터페이스의 호스트에서 다른 인터페이스의 호스트로 ping하도록 허용하는 방법에 대해 설명합니다.

기본 연결 테스트: 주소 **ping**하기

ping은 특정 주소가 활성 상태이고 응답할 수 있는지 확인하는 간단한 명령입니다. 다음 주제에서는 명령에 대한 자세한 내용과 ping을 통해 어떤 유형의 테스트를 완료할 수 있는지에 대해 설명합니다.

Ping을 사용하여 테스트할 수 있는 내용

디바이스를 ping하는 경우, 패킷이 디바이스로 전송되며 디바이스에서 응답을 반환합니다. 이 과정을 통해 네트워크 디바이스는 서로를 검색, 식별 및 테스트할 수 있습니다.

ping을 사용하여 다음 테스트를 수행할 수 있습니다.

- 두 인터페이스의 루프백 테스트 - 각 인터페이스의 기본 "가동" 상태 및 작동을 확인하는 외부 루프백 테스트로서 동일한 ASA의 한 인터페이스에서 다른 인터페이스로 ping을 시작할 수 있습니다.
- ASA로 ping하기 — 다른 ASA에 있는 인터페이스를 ping하여 가동 상태와 응답을 확인할 수 있습니다.
- ASA를 통해 ping하기 — ASA의 다른 쪽에 있는 디바이스를 ping하여 중간 ASA를 통해 ping할 수 있습니다. 패킷은 각 방향으로 들어간 대로 중간 ASA의 인터페이스 2개를 통과합니다. 이 작업은 중간 유닛의 인터페이스, 작동, 응답 시간에 대한 기본 테스트를 수행합니다.
- ping으로 네트워크 디바이스의 의심스러운 작동 테스트 — ASA 인터페이스에서 시작하여 오작동이 의심되는 네트워크 디바이스로 ping할 수 있습니다. 인터페이스 구성이 올바른데 에코를 수신할 수 없으면 디바이스에 문제가 있는 것일 수 있습니다.
- ping으로 중간 통신 테스트 — ASA 인터페이스에서 제대로 작동하는 것으로 알려진 네트워크 디바이스에 ping할 수 있습니다. 에코가 수신되면 중간 디바이스 및 물리적 연결이 올바르게 작동하는 것입니다.

ICMP 및 **TCP Ping** 중에서 선택

ASA에는 ICMP 에코 요청 패킷을 전송하고 에코 응답 패킷을 반환되게 하는 기존 ping이 포함되어 있습니다. 이것은 모든 중간 네트워크 디바이스가 ICMP 트래픽을 허용하는 경우 표준 툴이며 제대로 작동합니다. ICMP ping을 통해 IPv4 또는 IPv6 주소 또는 호스트 이름을 ping할 수 있습니다.

하지만, 일부 네트워크는 ICMP를 금지합니다. 네트워크가 해당하는 경우 대신 TCP ping을 사용하여 네트워크 연결을 테스트할 수 있습니다. TCP ping을 통해 ping은 TCP SYN 패킷을 전송하고 응답으로 SYN-ACK를 수신하는 경우 ping을 성공으로 간주합니다. TCP ping을 통해 IPv4 주소 또는 호스트 이름을 ping할 수 있지만, IPv6 주소를 ping할 수 없습니다.

성공적인 ICMP 또는 TCP ping은 사용 중인 주소가 활성 상태이며 해당하는 특정 유형의 트래픽에 응답 중임을 의미한다는 점을 기억하십시오. 이것은 기본 연결이 작동하고 있음을 의미합니다. 디바이스에서 실행 중인 기타 정책은 특정 유형의 트래픽이 디바이스를 성공적으로 통과하는 것을 방지할 수 있습니다.

ICMP 활성화

기본적으로 높은 보안 인터페이스에서 낮은 보안 인터페이스로 ping할 수 있습니다. 응답 트래픽 통과를 허용하려면 ICMP 검사를 활성화해야 합니다. 낮은 곳에서 높은 곳으로 ping하려면 트래픽을 허용하는 ACL을 적용해야 합니다.

ASA 인터페이스를 ping할 경우 해당 인터페이스에 적용된 ICMP 규칙은 에코 요청 및 에코 응답 패킷을 허용해야 합니다. ICMP 규칙은 선택사항입니다. 규칙을 구성하지 않은 경우, 인터페이스에 모든 ICMP 트래픽이 허용됩니다.

이 절차에서는 ASA 인터페이스의 ICMP ping하기 활성화를 완료하는 데 필요한 모든 ICMP 구성 또는 ASA를 통해 ping하기에 대해 설명합니다.

프로시저

단계 **1** ICMP 규칙이 에코 요청/에코 응답을 허용하는지 확인합니다.

ICMP 규칙은 선택사항이며 인터페이스로 직접 전송된 ICMP 패킷에 적용됩니다. ICMP 규칙을 적용하지 않는 경우, 모든 ICMP 액세스가 허용됩니다. 이 경우, 어떤 동작도 필요하지 않습니다.

그러나 ICMP 규칙을 구현하는 경우 “inside”를 디바이스에 있는 인터페이스 이름으로 대체하여 각 인터페이스에서 최소한 다음을 포함하도록 해야 합니다.

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

단계 **2** 액세스 규칙이 ICMP를 허용하는지 확인합니다.

ASA를 통해 호스트를 ping하는 경우, 액세스 규칙은 ICMP 트래픽을 남겨두고 반환하도록 허용해야 합니다. 액세스 규칙은 최소한 에코 요청/에코 응답 ICMP 패킷을 허용해야 합니다. 이러한 규칙을 전역 규칙으로 추가할 수 있습니다.

이미 액세스 규칙을 인터페이스에 적용했거나 전역적으로 적용한 경우, 이러한 규칙을 관련된 ACL에 간단하게 추가합니다. 예:

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any anyecho

ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho-reply
```

또는 모든 ICMP를 허용만 합니다.

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any any
```

액세스 규칙이 없는 경우, 인터페이스에 임의의 액세스 규칙을 적용하면 암시적으로 거부가 추가되어 다른 모든 트래픽이 드롭될 수 있으므로 원하는 다른 유형의 트래픽도 허용해야 합니다. ACL을 인터페이스 또는 전역적으로 적용하려면 **access-group** 명령을 사용합니다.

테스트용으로 간단하게 규칙을 추가 중인 경우 ACL에서 규칙을 제거하려면 **no** 형식의 **access-list** 명령을 사용할 수 있습니다. 전체 ACL이 간단하게 테스트용인 경우 인터페이스에서 ACL을 제거하려면 **no access-group** 명령을 사용하십시오.

단계 **3** ICMP 검사를 활성화합니다.

인터페이스를 ping하는 것과 반대로 ASA를 통해 ping할 때 ICMP 검사가 필요합니다. 검사를 통해 ping을 시작한 호스트로 반환하기 위해 트래픽을 반환(즉, 에코 응답 패킷)할 수 있으며 특수한 공격 유형을 방지하려면 패킷당 응답이 하나인지 확인하십시오.

간단하게 기본 전역 검사 정책에서 ICMP 검사를 활성화할 수 있습니다.

```
ciscoasa(config)# policy-map  global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

호스트 **ping**하기

모든 디바이스를 ping하려면 IP 주소 또는 호스트 이름과 함께 **ping**을 간단하게 입력합니다(예: **ping 10.1.1.1** 또는 **ping www.example.com**). TCP ping의 경우 **tcp** 키워드 및 대상 포트를 포함합니다(예: **ping tcp www.example.com 80**). 이는 실행해야 할 모든 테스트의 범위입니다.

성공적인 ping 출력의 예:

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping이 실패하는 경우 출력에 각각의 실패한 시도와 100% 미만의 성공률이 ?로 표시됩니다(완전한 실패는 0%임).

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

그러나, 또한 ping의 일부 측면을 제어하기 위해 파라미터를 추가할 수도 있습니다. 다음은 기본 옵션입니다.

- ICMP ping.

  ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  여기서 각 항목은 다음을 나타냅니다.

- *if_name*은 호스트가 액세스 가능한 인터페이스 이름입니다. 이름을 포함하지 않는 경우, 라우팅 테이블이 사용할 인터페이스를 결정하는 데 사용됩니다.
- *host*는 사용자가 ping하고 있는 IPv4, IPv6 또는 호스트의 호스트 이름입니다.
- **repeat** *count*는 전송할 패킷 수입니다. 기본값은 5입니다.
- **timeout** *seconds*는 응답이 발생하지 않는 경우 시간이 초과되는 각 패킷의 시간(초)입니다. 기본값은 2입니다.
- **data** *pattern*은 전송된 패킷에 사용할 16진수 패턴입니다. 기본값은 0xabcd입니다.
- **size** *bytes*는 전송된 패킷의 길이입니다. 기본값은 100바이트입니다.
- **validate**는 검증된 데이터에 응답할 것임을 나타냅니다.

- TCP ping.

  ping tcp [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host* [*ports*]

  여기서 각 항목은 다음을 나타냅니다.

  - *if_name*은 소스가 ping을 전송하는 데 사용하는 인터페이스입니다. 이름을 포함하지 않는 경우, 라우팅 테이블이 사용됩니다.
  - *host*는 사용자가 ping하고 있는 IPv4 주소 또는 대상의 호스트 이름입니다. IPv6 주소로 TCP ping을 사용할 수 없습니다.
  - *port*는 사용자가 ping하고 있는 호스트의 TCP 포트입니다.
  - **repeat** 및 **timeout**에는 위에서와 동일한 의미가 있습니다.
  - **source** *host port*는 ping을 위한 소스 호스트 및 포트를 나타냅니다. 임의 포트를 가져오기 위해 포트 0을 사용합니다.

- 인터랙티브 ping.

  ping

  파라미터 없이 ping을 입력하면 키워드로 사용할 수 없는 확장된 파라미터를 포함하는 인터페이스, 대상 및 기타 파라미터에 대해 프롬프트가 표시됩니다. ping 패킷을 광범위하게 제어해야 하는 경우 이 방법을 사용하십시오.

체계적인 **ASA** 연결 테스트

ASA 연결을 보다 체계적으로 테스트하려는 경우 다음의 일반적인 절차를 수행할 수 있습니다.

시작하기 전에

절차에서 언급한 syslog 메시지를 확인하려는 경우 로깅을 활성화합니다(**logging enable** 명령 또는 ASDM에서 **Configuration(**구성**) > Device Management(**디바이스 관리**) > Logging(**로깅**) > Logging Setup(**로깅 설정**)**).

필요하지 않은 경우에도 외부 디바이스에서 ASA 인터페이스를 ping할 때 ASA 콘솔에서 메시지를 표시하려면 ICMP 디버그를 활성화할 수 있습니다(ASA를 통과하는 ping에 대한 디버그 메시지는 확인 못함). 성능에 영향을 줄 수 있으므로 문제 해결 중에는 ping 및 디버깅 메시지만 활성화하는 것이 좋습니다. 다음 예는 ICMP 디버깅을 활성화하고 텔넷 또는 SSH 세션에 전송할 syslog 메시지를 설정한 다음 해당 세션에 이 메시지를 전송하고 로깅을 활성화합니다. **logging monitor debug** 명령을 사용하는 대신 **logging buffer debug** 명령을 사용하여 로그 메시지를 버퍼로 보낸 다음 나중에 **show logging** 명령을 사용하여 볼 수도 있습니다.

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

이 구성에서는 외부 호스트(209.165.201.2)에서 ASA 외부 인터페이스(209.165.201.1)로의 성공적인 ping에 대해 다음과 같은 내용이 표시됩니다.

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

출력에는 ICMP 패킷 길이(32바이트), ICMP 패킷 식별자(1) 및 ICMP 시퀀스 번호가 표시됩니다. ICMP 시퀀스 번호는 0에서 시작하여 요청이 전송될 때마다 증가합니다.

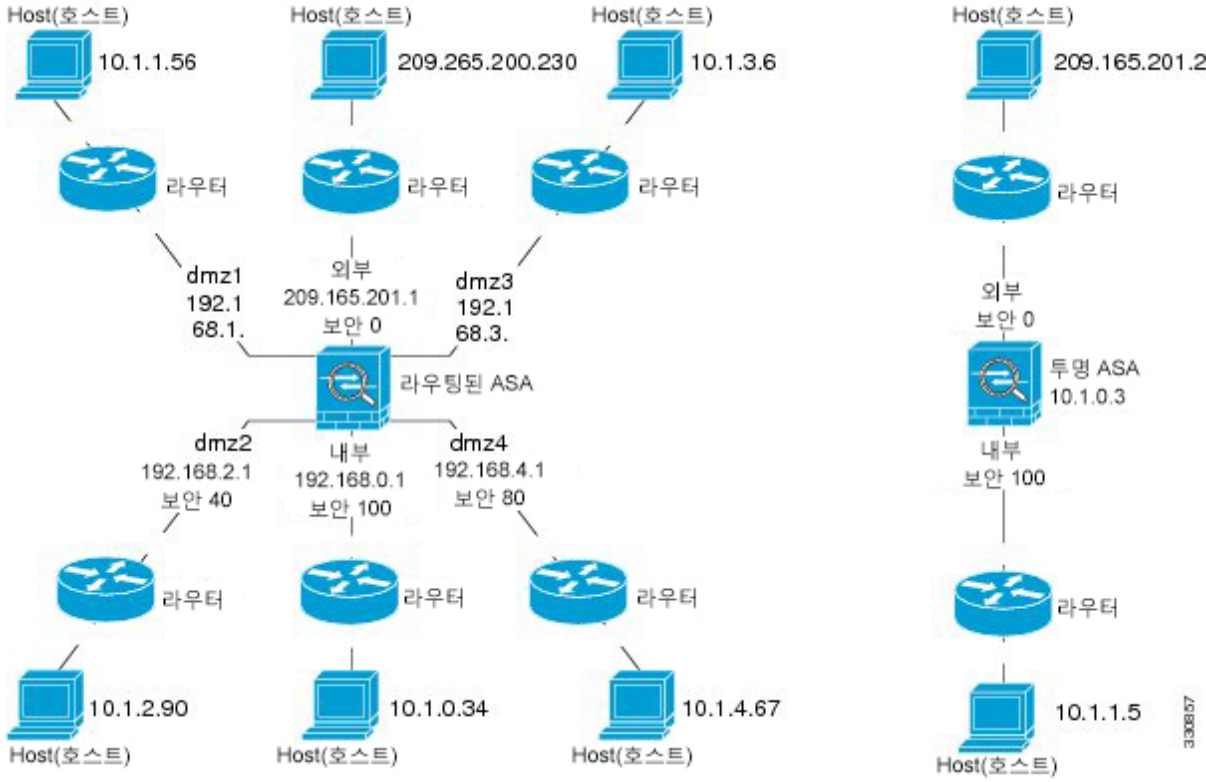
테스트를 완료한 경우, 디버깅을 비활성화합니다. 이 구성을 그대로 두면 성능 및 보안 위험을 초래할 수 있습니다. 테스트용으로만 로깅을 활성화한 경우, 다음과 같이 비활성화할 수도 있습니다.

```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
ciscoasa(config)# no terminal monitor
ciscoasa(config)# no logging enable
```

프로시저

단계 **1** 인터페이스 이름, 보안 레벨 및 IP 주소를 보여주는 단일 모드 ASA 또는 보안 상황의 다이어그램을 그립니다. 다이어그램에는 직접 연결된 라우터 및 ASA를 ping할 라우터의 다른 쪽에 있는 호스트도 포함되어 있습니다.

그림 71: 인터페이스, 라우터 및 호스트가 포함된 네트워크 다이어그램

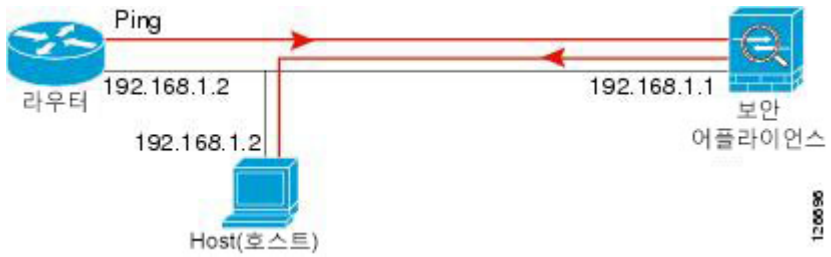


단계 2 직접 연결된 라우터에서 각 ASA 인터페이스를 ping합니다. 투명 모드의 경우 BVI IP 주소를 ping합니다. 이 테스트에서는 ASA 인터페이스가 활성 상태인지, 인터페이스 구성이 올바른지 확인합니다.

ASA 인터페이스가 활성 상태가 아니거나, 인터페이스 구성이 올바르지 않거나, ASA와 라우터 간 스위치가 다운된 경우 ping이 실패할 수 있습니다(다음 그림 참조). 이 경우 패킷이 ASA에 도달하지 않기 때문에 디버깅 메시지 또는 syslog 메시지가 표시되지 않습니다.

그림 72: ASA 인터페이스에서 Ping 실패

그림 73: IP 주소 지정 문제 때문에 Ping 실패



Ping 응답이 라우터로 반환되지 않으면 스위치 루프 또는 중복 IP 주소가 존재하는 것일 수 있습니다(다음 그림 참조).

단계 **3** 원격 호스트에서 각 ASA 인터페이스를 ping합니다. 투명 모드의 경우 BVI IP 주소를 ping합니다. 이 테스트에서는 직접 연결된 라우터가 호스트 및 ASA 간에 패킷을 라우팅할 수 있는지, ASA가 패킷을 정확하게 호스트로 다시 라우팅할 수 있는지 확인합니다.

ASA에 중간 라우터를 통해 호스트로 반환하는 경로가 없으면 ping이 실패할 수 있습니다(다음 그림 참조). 이 경우 디버깅 메시지에는 ping이 성공한 것으로 표시되지만, 라우팅이 실패했음을 나타내는 syslog 메시지 110001이 표시됩니다.

그림 ***74: ASA***에 반환 경로가 없기 때문에 ***Ping*** 실패

단계 **4** ASA 인터페이스에서 알고 있는 네트워크 디바이스로 ping하면 제대로 작동합니다.

- ping을 수신하지 못하면 전송 하드웨어 또는 인터페이스 컨피그레이션에 문제가 있는 것일 수 있습니다.
- ASA 인터페이스가 올바르게 구성되었지만 "정상 상태" 디바이스에서 에코 응답을 수신하지 못하는 경우, 인터페이스 하드웨어 수신 기능에 문제가 있기 때문일 수 있습니다. "정상 상태" 수신 기능이 있는 다른 인터페이스에서는 동일한 "정상 상태" 디바이스에서 에코를 수신할 수 있다면 첫 번째 인터페이스의 하드웨어 수신 기능에 문제가 있는 것입니다.

단계 **5** 호스트나 라우터에서 소스 인터페이스를 통해 다른 인터페이스의 다른 호스트나 라우터로 ping합니다. 확인하고 싶은 만큼의 인터페이스 쌍에 대해 이 단계를 반복합니다. NAT를 사용하는 경우 이 테스트에서는 NAT가 올바르게 작동하고 있음을 표시합니다.

Ping이 성공할 경우, syslog 메시지가 나타나서 라우팅된 모드의 주소 변환을 확인하고(305009 또는 305011), ICMP 연결이 설정되었는지를 확인합니다(302020). 이 정보를 보려면 **show xlate** 또는 **show conns** 명령을 입력할 수도 있습니다.

NAT가 올바르게 구성되지 않으면 ping이 실패할 수 있습니다. 이 경우 NAT가 실패했음을 알리는 syslog 메시지가 표시됩니다(305005 또는 305006). 외부 호스트에서 내부 호스트로 ping하는 경우 고정 변환이 없으면 106010 메시지가 표시됩니다.

그림 ***75: ASA***에서 주소를 변환하지 않기 때문에 ***Ping*** 실패

호스트에 대한 경로 추적

어떤 IP 주소에 트래픽을 보내는 데 문제가 있을 경우 호스트까지의 경로를 추적하여 네트워크 경로에 문제가 있는지 확인할 수 있습니다.

프로시저

단계 **1** 경로 추적 시 ASA 표시하기, 1238 페이지.

단계 **2** 패킷 경로 확인, 1239 페이지.

경로 추적 시 **ASA** 표시하기

기본적으로 ASA는 홉으로 트레이스라우트에 나타나지 않습니다. traceroute를 나타나게 하려면 ASA를 통과하는 패킷에서 TTL(Time-To-Live)을 줄이고 ICMP의 연결할 수 없는 메시지에 대한 속도 제한을 늘립니다.

프로시저

단계 **1** 연결 설정을 사용자 지정하려는 트래픽을 식별하기 위해 L3/L4 클래스 맵을 만듭니다.

class-map *name*

match 파라미터

예제**:**

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

일치 명령문에 대한 정보는 방화벽 구성 가이드에서 서비스 정책 장을 참고하십시오.

단계 **2** 클래스 맵 트래픽에 수행할 작업을 설정하는 정책 맵을 추가하거나 수정하고 클래스 맵을 식별합니다.

policy-map *name* **class** *name*

예제**:**

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

기본 구성에서 global_policy 정책 맵은 모든 인터페이스에 전역적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다. 클래스 맵의 경우 이 절차의 앞부분에서 작성한 클래스를 지정합니다.

단계 **3** 클래스에 일치하는 패킷의 TTL(Time-To-Live)을 줄입니다.

set connection decrement-ttl

단계 **4** 기존 서비스 정책(예: global_policy라는 기본 전역 정책)을 수정하는 경우 이 단계를 건너뛸 수 있습니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name* }

예제**:**

```
ciscoasa(config)# service-policy global_policy global
```

global 키워드는 모든 인터페이스에 정책 맵을 적용하고 **interface**는 하나의 인터페이스에 정책을 적용합니다. 전역 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 전역 정책을 재정의할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

단계 **5** ASA가 트레이스라우트 출력에 나타나도록 ICMP의 연결할 수 없는 메시지에 대한 속도 제한을 늘립니다.

icmp unreachable rate-limit *rate* **burst-size** *size*

예제**:**

```
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

속도 제한의 범위는 1 ~ 100이며 기본값은 1입니다. Burst size는 의미가 없지만 범위는 1~10이어야 합니다.

예

다음의 예는 모든 트래픽에 대한 TTL을 전역적으로 줄이고 ICMP 연결할 수 없는 제한을 50으로 늘립니다.

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

패킷 경로 확인

traceroute를 사용하면 패킷이 대상으로 이동하는 경로를 확인하는 데 도움이 됩니다. 트레이스라우트는 잘못된 포트의 UDP 패킷을 또는 ICMPv6 에코를 대상으로 전송하는 방식입니다. 포트가 유효

하지 않으므로 대상으로 가는 동안 라우터에서 ICMP 또는 ICMPv6 시간 초과 메시지로 응답하고 ASA에 오류를 보고합니다.

traceroute 명령은 전송된 각 프로브의 결과를 보여 줍니다. 출력 화면의 각 줄은 TTL 값에 해당합니다(오름차순). 다음 표는 출력 기호에 대해 설명합니다.

출력 기호	설명
*	프로브에 대한 응답을 받지 못한 채 시간이 초과되었습니다.
U	대상에 대한 경로가 없습니다.
nn msec	각 노드에서 지정된 수의 프로브가 왕복하는 데 걸린 시간(밀리초)입니다.
!N.	연결 불가한 ICMP 네트워크입니다. ICMPv6에 대한 주소 범위를 벗어났습니다.
!H	연결 불가한 ICMP 호스트입니다.
!P	ICMP 연결 불가입니다. ICMPv6에 포트를 연결할 수 없습니다.
!A	관리자가 ICMP를 금지했습니다.
?	알 수 없는 ICMP 오류입니다.

프로시저

대상에 대한 경로를 추적합니다.

traceroute [*destination_ip* | *hostname*} [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

예제**:**

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec

ciscoasa# traceroute 2002::130

Type escape sequence to abort.
```

```
Tracing the route to 2002::130

 1  5000::2 0 msec 0 msec 0 msec
 2  2002::130 10 msec 0 msec 0 msec
```

일반적으로 대상 IP 주소 또는 호스트 이름을 간단하게 포함시키면 됩니다(예: **traceroute www.example.com**). 그러나, 원하는 경우 추적의 특성을 조정할 수 있습니다.

- **source** {*source_ip* | *source-interface*}— 인터페이스를 추적의 소스로 사용하려면 지정합니다. 호스트 이름 또는 IP 주소로 인터페이스를 지정할 수 있습니다. IPv6의 경우 소스 인터페이스를 지정할 수 없습니다. 소스 IP 주소만 지정할 수 있습니다. IPv6 주소는 ASA 인터페이스에서 IPv6를 활성화하는 경우에만 유효합니다. 투명 모드에서, 관리 주소를 사용해야 합니다.
- **numeric** — IP 주소만 추적 경로에 표시되어야 한다는 점을 나타냅니다. 이 키워드를 사용하지 않으면 경로 추적 시 주소에 대해 DNS 조회를 수행하고 DNS 구성을 가정하는 DNS 이름이 포함됩니다.
- **timeout** *timeout_value*— 시간 초과 이전에 응답을 대기하는 시간입니다. 기본값은 3초입니다.
- **probe** *probe_num*— 각 TTL 수준에서 전송할 프로브 수입니다. 기본값은 3입니다.
- **ttl** *min_ttl max_ttl* — 프로브를 위한 최소 및 최대 TTL(time-to-live) 값입니다. 최소 기본값은 1이지만, 알려진 홉을 표시하지 않으려면 더 높은 값을 설정할 수 있습니다. 최대값은 기본적으로 30입니다. 패킷이 목적지에 도착하거나 최대값에 도달하면 트레이스라우트가 종료됩니다.
- **port** *port_value*— 사용할 UDP 포트입니다. 기본값은 33434입니다.
- **use-icmp**— 프로브에 대한 UDP 패킷 대신 ICMP 패킷을 전송합니다.

정책 구성을 테스트하기 위한 패킷 트레이서 사용

소스, 수신 주소 및 프로토콜 특성에 따라 패킷을 모델링하여 정책 구성을 테스트할 수 있습니다. 추적 시 액세스 규칙, NAT, 라우팅 등을 테스트하고 패킷이 허용 또는 거부되는지 여부를 확인하기 위해 정책 조회를 수행합니다.

이 방식으로 패킷을 테스트하면 정책의 결과를 확인하고 허용 또는 거부할 트래픽 유형이 사용자가 원하는 대로 처리되는지 여부를 테스트할 수 있습니다. 구성 확인 이외에도 추적기를 사용하여 패킷이 허용되어야 할 때 거부되고 있는지와 같이 예상하지 못한 동작을 디버깅할 수 있습니다.

프로시저

단계 **1** 명령이 복잡하므로 부분으로 세분화했습니다. 다음과 같이 추적을 위해 인터페이스 및 프로토콜을 선택하여 시작합니다.

packet-tracer input *ifc_name* [**vlan-id***vlan_id*] {**icmp** | **tcp** | **udp** | **rawip** | **sctp**} [**inline-tag** *tag*]...

여기서 각 항목은 다음을 나타냅니다.

- **input** *ifc_name* — 추적을 시작할 시작 인터페이스 이름입니다. 브리지 그룹의 경우, 브리지 그룹 멤버 인터페이스 이름을 지정합니다.
- **vlan-id** *vlan_id* — (선택 사항) 가상 LAN은 패킷 트레이서가 하위 인터페이스로 나중에 리디렉션되는 상위 인터페이스로 들어가는 위치입니다. VLAN id는 입력 인터페이스가 하위 인터페이스가 아닌 경우에만 사용할 수 있습니다. 유효한 값의 범위는 1~4096입니다.
- **icmp**, **tcp**, **udp**, **rawip**, **sctp** — 사용할 프로토콜입니다. "rawip" 는 raw IP, 즉 TCP/UDP가 아닌 IP 패킷입니다.
- **inline-tag** *tag*—(선택사항) Layer 2 CMD 헤더에 삽입된 보안 그룹 태그 값입니다. 유효한 값의 범위는 0 ~ 65533입니다.

단계 **2** 다음으로, 소스 주소와 프로토콜 기준을 입력합니다.

...{*src_ip* | **user** *username* | **security-group** { **name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}*...*

여기서 각 항목은 다음을 나타냅니다.

- *src_ip* — 패킷 추적을 위한 IPv4 또는 IPv6 소스 주소입니다.
- **user** *username* — domain\사용자의 형식으로 된 사용자 ID입니다. 사용자에 대해 가장 최근에 매핑된 주소(있는 경우)가 추적에 사용됩니다.
- **security-group** {**name** *name* | **tag** *tag*} — Trustsec에 대한 IP-SGT 조회에 기초한 소스 보안 그룹입니다. 보안 그룹 이름 또는 태그 번호를 지정할 수 있습니다.
- **fqdn** *fqdn-string* — 소스 호스트, IPv4 전용의 정규화된 도메인 이름입니다.

단계 **3** 다음으로, 프로토콜 특성을 입력합니다.

- ICMP — ICMP 유형(1-255), ICMP 코드(0-255) 및 선택사항인 ICMP Id를 입력합니다. 각 변수에 대해 숫자를 사용해야 합니다(예: 에코의 경우 8).

  type code... [ident]...

- TCP/UDP/SCTP — 소스 포트 번호를 입력합니다.

  ...src_port ...

- Raw IP — 0-255 사이의 프로토콜 번호를 입력합니다.

  ... protocol ...

단계 **4** 마지막으로, TCP/UDP 추적을 위해 수신 주소 기준, 대상 포트 및 선택사항 키워드를 입력하고 **Enter** 키를 누릅니다.

...dmac {*dst_ip* | **security-group** { **name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dst_port* [**detailed**] [**xml**]

여기서 각 항목은 다음을 나타냅니다.

- *dst_ip* — 패킷 추적을 위한 수신 IPv4 또는 Ipv6 주소입니다.
- **security-group** {**name** *name* | **tag** *tag*}— Trustsec에 대한 IP-SGT 조회에 기초한 대상 보안 그룹입니다. 보안 그룹 이름 또는 태그 번호를 지정할 수 있습니다.

- **fqdn** *fqdn-string* — 대상 호스트, IPv4 전용의 정규화된 도메인 이름입니다.
- *dst_port* — TCP/UDP/SCTP 추적을 위한 대상 포트입니다. ICMP 또는 raw IP 추적의 경우 이 값을 포함하지 마십시오.
- *dmac* — (투명 모드) 대상 MAC 주소입니다.
- **detailed** — 일반적인 출력 외에도 자세한 추적 결과 정보를 제공합니다.
- **xml** — 추적 결과를 XML 형식으로 표시합니다.

단계 **5** 클러스터 유닛 간에 패킷을 디버깅하려면 패킷 트레이서에 대한 **persist** 옵션에 내용을 입력합니다.

- **transmit(**전송**)** 옵션을 사용하여 ASA 이그레스를 위해 시뮬레이션된 패킷을 허용할 수 있습니다.
- ACL, VPN 필터, IPsec 스푸핑 및 uRPF 같은 보안 검사를 건너뛰려면 **bypass-checks** 옵션을 사용합니다.
- **decrypted** 옵션을 사용하여 VPN 터널에서 암호 해독된 패킷을 삽입하고 VPN 터널 전체에서 오는 패킷을 시뮬레이션할 수 있습니다.

단계 **6** 클러스터 유닛에서 특정 패킷을 추적하려면 **id** 및 **origin**에 내용을 입력합니다.

- **id**— 추적을 시작하는 유닛에서 할당된 ID 번호입니다.
- **origin** — 추적을 시작하는 클러스터 유닛을 나타냅니다.

예

다음 예는 10.100.10.10 ~ 10.100.11.11의 HTTP 포트에 대해 TCP 패킷을 추적합니다. 다음 결과는 패킷이 암시적 거부 액세스 규칙에 의해 드롭될 것임을 나타냅니다.

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11
 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
```

```
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

연결 모니터링

소스, 대상, 프로토콜 등에 대한 정보와 함께 현재 연결을 보려면 **show conn all detail** 명령을 사용합니다.

테스트 및 트러블슈팅에 대한 기록

기능 이름	플랫폼 릴리스	설명
트레이스라우트에 대한 IPv6 주소 지원	9.7(1)	**traceroute** 명령은 IPv6 주소를 허용하도록 수정되었습니다. 다음 명령을 수정했습니다. **traceroute**
브리지 그룹 멤버 인터페이스에 대한 패킷 트레이서 지원	9.7(1)	이제 브리지 그룹 멤버 인터페이스에 대한 패킷 트레이서를 사용할 수 있습니다. **packet-tracer** 명령에 **vlan-id** 및 **dmac**의 두 가지 새 옵션을 추가했습니다.
패킷 캡처 수동 시작 및 중지	9.7(1)	이제 수동으로 캡처를 중지하고 시작할 수 있습니다. 추가/수정된 명령: **capture stop**

기능 이름	플랫폼 릴리스	설명
향상된 패킷 트레이서 및 패킷 캡처 기능	9.9(1)	패킷 트레이서는 다음과 같은 기능을 지원하도록 개선되었습니다. • 클러스터 유닛 사이를 통과할 때 패킷을 추적합니다. • 시뮬레이션된 패킷이 ASA를 나갈 수 있습니다. • 시뮬레이션된 패킷에 대한 보안 검사를 우회합니다. • 시뮬레이션된 패킷을 IPsec/SSL의 암호 해독된 패킷으로 처리합니다. 패킷 캡처는 다음과 같은 기능을 지원하도록 개선되었습니다. • 암호가 해독된 후에 패킷을 캡처합니다. • 추적을 캡처하고 영구 목록에 보관합니다. 신규 또는 수정된 명령: **cluster exec capture test trace include-decrypted, clusterexec capture test trace persist, cluster exec clear packet-tracer, cluster exec show packet-tracer id, cluster exec show packet-tracer origin, packet-tracer persist, packet-tracer transmit, packet-tracer decrypted, packet-tracer bypass-checks**
ACL을 사용하지 않고 일치하는 IPv6 트래픽에 대한 패킷 캡처 지원	9.10(1)	**capture** 명령에 **match** 키워드를 사용하는 경우, **any** 키워드는 IPv4 트래픽하고만 일치합니다. 이제는 IPv4 또는 IPv6 트래픽을 캡처하기 위해 **any4**와 **any6** 키워드를 지정할 수 있습니다. **any** 키워드는 IPv4 트래픽하고만 계속 일치합니다. 신규/수정된 명령: **capture match**

VIII 부

모니터링

41 장

로깅

이 장에서는 시스템 메시지를 기록하고 문제 해결에 활용하는 방법을 설명합니다.

로깅 정보

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다. Cisco 디바이스는 로그 메시지를 UNIX 스타일 syslog 서비스로 전송할 수 있습니다. syslog 서비스는 메시지를 수신하고 파일로 저장하거나 간단한 구성 파일에 따라 인쇄합니다. 이 로깅 양식을 통해 로그를 안전하게 장기 보관할 수 있습니다. 로그는 일상적인 트러블슈팅과 사고 처리에 모두 유용합니다.

ASA 시스템 로그는 ASA 모니터링 및 트러블슈팅에 필요한 정보를 제공합니다. 로깅 기능을 사용하면 다음을 할 수 있습니다.

- 어떤 syslog 메시지를 기록해야 하는지 지정합니다.
- syslog 메시지의 심각도를 비활성화하거나 변경합니다.
- syslog 메시지를 보낼 한 개 이상의 위치를 다음을 포함하도록 지정합니다.
  - 내부 버퍼
  - 하나 이상의 syslog 서버
  - ASDM
  - SNMP 관리 스테이션
  - 지정된 이메일 주소
  - 콘솔

  - 텔넷 및 SSH 세션.

- 심각도 레벨 또는 메시지 클래스와 같은 그룹으로 syslog 메시지를 구성하고 관리합니다.
- syslog 생성에 속도 제한 적용 여부를 지정합니다.
- 내부 로그 버퍼가 가득 찰 때 작업을 지정합니다. 버퍼를 덮어쓰거나, FTP 서버에 버퍼 내용을 보내거나, 내부 플래시 메모리에 내용을 저장합니다.
- 위치, 심각도, 클래스 또는 맞춤형 메시지 목록별로 syslog 메시지를 필터링합니다.

다중 상황 모드에서의 로깅

각 보안 컨텍스트는 자체 로깅 컨피그레이션을 포함하고 자체 메시지를 생성합니다. 시스템 또는 관리자 컨텍스트에 로그인한 후 다른 컨텍스트로 변경하면 세션에서는 현재 컨텍스트와 관련된 메시지만 볼 수 있습니다.

장애 조치 메시지를 포함하여 시스템 실행 공간에서 생성된 syslog 메시지는 관리자 컨텍스트에서 생성된 메시지와 함께 관리자 컨텍스트에서 보게 됩니다. 시스템 실행 공간에서 로깅을 구성하거나 로깅 정보를 볼 수 없습니다.

각 메시지에 상황 이름을 포함하도록 ASA 및 ASASM을 구성하면 하나의 syslog 서버로 전송되는 상황 메시지를 구분하는 데 도움이 됩니다. 이 기능을 사용하면 관리자 컨텍스트에서 전송된 메시지와 시스템에서 전송된 메시지를 구분하는 데 도움이 됩니다. 시스템 실행 공간에서 발생한 메시지는 시스템의 디바이스 ID를 사용하고 관리자 컨텍스트에서 발생한 메시지는 관리자 컨텍스트의 이름을 디바이스 ID로 사용합니다.

Syslog 메시지 분석

다음은 다양한 syslog 메시지를 검토함으로써 얻을 수 있는 정보 유형의 예입니다.

- ASA 보안 정책에서 허용된 연결. 이러한 메시지는 보안 정책의 허점을 찾는 데 도움이 됩니다.
- ASA 보안 정책에서 거부된 연결. 이러한 메시지는 보안된 내부 네트워크로 어떤 유형의 활동이 전송되는지 보여줍니다.
- ACE 거부 속도 로깅 기능을 사용하면 ASA 또는 ASA 서비스 모듈에서 발생하는 공격을 볼 수 있습니다.
- IDS 활동 메시지는 발생한 공격을 보여줄 수 있습니다.
- 사용자 인증 및 명령 사용량은 보안 정책 변화에 대한 감사 추적을 제공합니다.
- 대역폭 사용량 메시지는 설정된 연결과 해제된 연결, 사용된 트래픽의 길이와 볼륨을 보여줍니다.
- 프로토콜 사용량 메시지는 각 연결에 대해 사용된 프로토콜 및 포트 번호를 보여줍니다.
- 주소 변환 감사 추적 메시지는 설정되거나 해제되는 NAT 또는 PAT 연결을 기록하여 네트워크 내부에서 외부로 악성 활동이 보고될 때 유용합니다.

Syslog 메시지 형식

Syslog 메시지는 백분율 기호(%)로 시작하며 다음과 같은 구조를 갖습니다.

```
%ASA Level Message_number: Message_text
```

필드 설명은 다음과 같습니다.

ASA	ASA 및 ASASM에서 생성된 메시지에 대한 syslog 메시지 기능 코드입니다. 이 값은 항상 ASA입니다.
Level	1부터 7까지입니다. 레벨은 syslog 메시지가 설명하는 상태의 심각도를 반영합니다. 숫자가 낮을수록 심각한 상태입니다.
Message_number	syslog 메시지를 식별하는 고유한 6자리 숫자입니다.
Message_text	상태를 설명하는 문자열입니다. syslog 메시지의 이 부분은 IP 주소, 포트 번호 또는 사용자 이름을 포함하기도 합니다.

심각도 수준

다음 표는 syslog 메시지 심각도 수준을 나열합니다. ASDM 로그 뷰어에서 구별하기 쉽도록 각 심각도에 컬러를 할당할 수 있습니다. syslog 메시지 컬러 설정을 컨피그레이션하려면 **Tools(**툴**) > Preferences(**기본 설정**) > Syslog** 탭을 선택하거나 로그 뷰어의 툴바에서 **Color Settings(**색상 설정**)**를 클릭하십시오.

표 ***52: Syslog*** 메시지 심각도 레벨

레벨 번호	심각도 레벨	설명
0	**emergencies(**비상**)**	시스템을 사용할 수 없습니다.
1	경고	즉각적인 행동이 필요합니다.
2	중요	심각한 상태입니다.
3	오류	오류 상태입니다.
4	경고	경고 상태입니다.
5	**notification(**알림**)**	일반적이지만 중요한 상태입니다.
6	정보	정보 메시지만 해당됩니다.
7	**debugging(**디버깅**)**	디버깅 메시지만 해당됩니다.

참고 ASA 심각도 레벨이 0(응급)인 syslog 메시지를 생성하지 않습니다.

Syslog 메시지 필터링

특정 syslog 메시지만 특정 출력 대상에 전송되도록 생성된 syslog 메시지를 필터링할 수 있습니다. 예를 들어 모든 syslog 메시지를 하나의 출력 대상으로 전송하고 이 syslog 메시지의 하위 집합을 다른 출력 대상으로 보내도록 ASA를 구성할 수 있습니다.

구체적으로 syslog 메시지가 다음 기준에 따라 출력 대상으로 전송되도록 지시할 수 있습니다.

- Syslog 메시지 ID 번호
- Syslog 메시지 심각도 레벨
- Syslog 메시지 클래스(기능 영역에 해당)

출력 대상을 설정할 때 지정할 수 있는 메시지 목록을 생성함으로써 이 기준을 사용자 정의할 수 있습니다. 또는 특정 메시지 클래스를 메시지 목록과는 별개로 각 출력 대상 유형으로 전송하도록 ASA를 구성할 수도 있습니다.

Syslog 메시지 클래스

syslog 메시지 클래스를 2가지 방법으로 사용할 수 있습니다.

- 전체 syslog 메시지 카테고리에 대한 출력 위치를 지정합니다. **logging class** 명령을 사용합니다.
- 메시지 클래스를 지정하는 메시지 목록을 생성합니다. **logging list** 명령을 사용합니다.

syslog 메시지 클래스는 디바이스의 기능에 해당하는 유형에 따라 syslog 메시지를 분류하는 방식을 제공합니다. 예를 들어 rip 클래스는 RIP 라우팅을 나타냅니다.

특정 클래스의 모든 syslog 메시지는 syslog 메시지 ID 번호의 첫 3자리가 같습니다. 예를 들어 611로 시작하는 모든 syslog 메시지 ID는 vpnc(VPN 클라이언트)와 연결되어 있습니다. VPN 클라이언트 기능에 연결된 syslog 메시지는 611101부터 611323까지입니다.

또한 대부분의 ISAKMP syslog 메시지는 터널 식별을 돕는 공통의 접두사가 있는 객체 세트를 갖습니다. 이러한 객체가 있는 경우 syslog 메시지의 설명 텍스트 앞에 위치합니다. syslog 메시지가 생성되는 시점에 객체를 알 수 없는 경우 구체적인 heading = value 조합은 표시되지 않습니다.

객체는 다음과 같이 접두사가 붙습니다.

그룹 = *groupname*, 사용자 이름 = *user*, IP = *IP_address*

그룹이 터널-그룹인 경우 사용자 이름은 로컬 데이터베이스 또는 AAA 서버의 사용자 이름이고 IP 주소는 원격 액세스 클라이언트 또는 레이어 2 피어의 공용 IP 주소입니다.

다음 표에는 메시지 클래스와 각 클래스의 메시지 ID 범위가 나와 있습니다.

표 ***53: Syslog*** 메시지 클래스와 연결된 메시지 ***ID*** 번호

클래스	정의	**Syslog** 메시지 **ID** 번호
auth	사용자 인증	109, 113
—	액세스 목록	106
—	애플리케이션 방화벽	415
bridge	투명한 방화벽	110, 220
ca	PKI 인증 기관	717
citrix	Citrix 클라이언트	723
—	클러스터링	747
—	카드 관리	323
config	CLI(Command Line Interface)	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	동적 액세스 정책	734
eap, eapoudp	Network Admission Control용 EAPoUDP 또는 EAP	333, 334
eigrp	EIGRP 라우팅	336
email	이메일 프록시	719
—	환경 모니터링	735
HA	페일오버	101, 102, 103, 104, 105, 210, 311, 709
—	ID 기반 방화벽	746
ids	Intrusion Detection System(침입 탐지 시스템)	400, 733
—	IKEv2 툴킷	750, 751, 752
ip	IP 스택	209, 215, 313, 317, 408
ipaa	IP 주소 할당	735
ips	Intrusion Protection System(침입 방지 시스템)	400, 401, 420
—	IPv6	325

클래스	정의	**Syslog** 메시지 **ID** 번호
—	블랙리스트, 화이트리스트 및 그레이리스트	338
—	라이선싱	444
mdm-proxy	MDM 프록시	802
nac	NAC(Network Admission Control)	731, 732
nacpolicy	NAC 정책	731
nacsettings	NAC 정책을 적용할 NAC 설정	732
—	네트워크 액세스 포인트	713
np	네트워크 프로세서	319
—	NP SSL	725
ospf	OSPF 라우팅	318, 409, 503, 613
—	비밀번호 암호화	742
—	전화 프록시	337
rip	RIP 라우팅	107, 312
rm	리소스 관리자	321
—	Smart Call Home	120
세션	사용자 세션	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL 스택	725
svc	SSL VPN 클라이언트	722
sys	시스템	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	위협 탐지	733
tre	트랜잭션 규칙 엔진	780
—	UC-IME	339

클래스	정의	**Syslog** 메시지 **ID** 번호
태그 스위칭	서비스 태그 스위칭	779
VM	VLAN 매핑	730
vpdn	PPTP 및 L2TP 세션	213, 403, 603
vpn	IKE 및 IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN 클라이언트	611
vpnfo	VPN 페일오버	720
vpnlb	VPN 로드 밸런싱	718
—	VXLAN	778
webfo	WebVPN 페일오버	721
webvpn	WebVPN 및 AnyConnect Client	716
—	NAT 및 PAT	305

사용자 지정 메시지 목록

사용자 정의 메시지 목록을 만드는 것은 어떤 syslog 메시지를 어떤 출력 대상으로 보낼지 제어하는 유연한 방법입니다. 맞춤형 syslog 메시지 목록에서 다음 기준 중 한 가지 또는 전체를 사용하여 syslog 메시지 그룹을 지정합니다.

- 심각도 레벨
- 메시지 ID
- Syslog 메시지 ID의 범위
- 메시지 클래스

예를 들어 다음 용도로 메시지 목록을 사용할 수 있습니다.

- 심각도 레벨이 1과 2인 syslog 메시지를 선택하고 하나 이상의 이메일 주소로 보냅니다.
- 메시지 클래스와 연결된 모든 syslog 메시지를 선택하고 내부 버퍼에 저장합니다.

메시지 목록은 메시지 선택을 위한 여러 기준을 포함할 수 있습니다. 하지만 새로운 명령 엔트리와 함께 각 메시지 선택 기준을 추가해야 합니다. 겹치는 메시지 선택 기준을 포함하는 메시지 목록을 만들 수 있습니다. 메시지 목록에서 2개의 기준이 같은 메시지를 선택하면 메시지는 한 번만 로깅됩니다.

클러스터링

syslog 메시지는 클러스터링 환경에서 어카운팅, 모니터링 및 문제 해결을 위한 필수 도구입니다. 클러스터의 각 ASA 유닛(최대 8개의 유닛이 허용됨)은 syslog 메시지를 독립적으로 생성합니다. 특정 **logging** 명령을 통해 타임 스탬프와 디바이스 ID를 포함하는 헤더 필드를 제어할 수 있습니다. syslog 서버는 디바이스 ID를 사용하여 syslog 생성기를 식별합니다. **logging device-id** 명령을 사용하면 디바이스 ID가 동일하거나 다른 syslog 메시지를 생성하여 클러스터의 동일한 또는 다른 유닛에서 메시지가 표시되도록 할 수 있습니다.

로깅 지침

이 섹션에는 로깅을 구성하기 전에 검토해야 할 지침 및 제한사항이 포함되어 있습니다.

IPv6 지침

- IPv6가 지원됩니다. TCP 또는 UDP를 사용하여 Syslog를 전송할 수 있습니다.
- Syslogs 전송에 대해 구성된 인터페이스가 활성화되어 있으며 IPv6를 지원 가능하며 syslog 서버에 지정된 인터페이스를 통해 연결할 수 있는지 확인합니다.
- IPv6를 통한 보안 로깅은 지원되지 않습니다.

추가 지침

- syslog 서버는 syslogd라는 서버 프로그램을 실행해야 합니다. Windows 운영 체제에는 syslog 서버가 포함되어 있습니다.
- ASA에서 생성된 로그를 보려면 로깅 출력 대상을 지정해야 합니다. 로깅 출력 대상을 지정하지 않고 로깅을 활성화하면 ASA는 메시지를 생성하지만 메시지를 볼 수 있는 위치에 저장하지 않습니다. 각 다른 로깅 출력 대상을 별도로 지정해야 합니다. 예를 들어 두 개 이상의 syslog 서버를 출력 대상으로 지정하려면 새로운 명령을 입력하여 .
- 스탠바이 디바이스에서는 TCP를 통한 syslog 전송이 지원되지 않습니다.
- 두 개의 서로 다른 목록 또는 다른 syslog 서버 또는 동일한 위치에 할당 중인 클래스를 갖는 것은 불가능합니다.
- 최대 16개의 syslog 서버를 구성할 수 있습니다. 그러나 다중 상황 모드에서는 상황당 서버 4개로 제한됩니다.
- syslog 서버는 ASA를 통해 연결할 수 있습니다. syslog 서버가 연결할 수 없는 인터페이스의 ICMP 연결 불가 메시지를 거부하고 syslog를 동일한 서버로 전송하도록 디바이스를 구성할 수 있습니다. 모든 심각도 레벨에 대해 로깅을 활성화했는지 확인합니다. syslog 서버가 충돌하지 않게 하려면 syslogs 313001, 313004 및 313005의 생성을 억제합니다.
- Syslog에 대한 UDP 연결 수는 하드웨어 플랫폼의 CPU 수와 구성하는 syslog 서버의 수와 직접 관련이 있습니다. 언제든지 구성된 Syslog 서버 수의 CPU보다 많은 UDP Syslog 연결이 있을 수 있습니다. 예를 들어, 각 syslog 서버에 대해서는 다음 연결이 가능합니다.

- ASA 5585-SSP-10에는 최대 4개의 UDP syslog 연결이 있을 수 있습니다.
- Firepower 4110에는 최대 22개의 UDP syslog 연결이 있을 수 있습니다.
- Firepower 4120에는 최대 46개의 UDP syslog 연결이 있을 수 있습니다.

이는 정상적인 동작입니다. 전역 UDP 연결 유휴 시간 초과가 이 세션에 적용되며 기본값은 2분입니다. 이러한 세션을 더욱 신속하게 종료하려면 설정을 조정할 수 있지만 시간 초과는 syslog뿐만 아니라 모든 UDP 연결에 적용됩니다.

- 액세스 목록만 일치하도록 사용자 정의 메시지 목록을 사용할 경우 로깅 심각도 레벨이 디버깅(레벨 7)으로 상승한 액세스 목록에 대해서 액세스 목록 로그가 생성되지 않습니다. 기본 로깅 심각도는 **logging list** 명령에 대해 6으로 설정됩니다. 이 기본 동작은 설계에 따른 것입니다. 액세스 목록 컨피그레이션의 심각도 레벨을 디버깅으로 확실히 변경할 경우 로깅 컨피그레이션 자체도 변경해야 합니다.

  다음은 로깅 심각도 레벨이 디버깅으로 변경되었기 때문에 액세스 목록 일치 결과를 포함하지 않는 **show running-config logging** 명령의 출력 샘플입니다.

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  다음은 액세스 목록 일치 결과를 포함하는 **show running-config logging** 명령의 출력 샘플입니다.

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

  이 경우 액세스 목록 컨피그레이션이 변경되지 않고 액세스 목록 일치 개수가 다음 예시와 같이 표시됩니다.

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- TCP를 통해 ASA가 syslogs를 전송할 때 syslogd 서비스가 재시작된 후에 연결을 초기화하는 데 약 1분 이상이 걸릴 수 있습니다.
- Syslog Server에서 받은 서버 인증서는 Extended Key Usage(확장 키 사용) 필드에서 "ServAuth"를 포함해야 합니다. 이 확인은 비 SSC(자가서명 인증서)에서만 수행됩니다. SSC(자가서명 인증서)는 이 필드에서 값을 제공하지 않습니다.

로깅 구성

이 섹션에서는 로깅 구성 방법을 설명합니다.

프로시저

단계 **1** 로깅을 활성화합니다.

단계 **2** syslog 메시지의 출력 대상을 구성합니다.

참고 최소 구성은 ASA 및 ASASM에서 하려고 하는 작업과 syslog 메시지 처리 요건이 무엇인지에 따라 달라집니다.

로깅 사용

로깅을 활성화하려면 다음 단계를 수행합니다.

프로시저

로깅을 활성화합니다.

logging enable

예제**:**

```
ciscoasa(config)# logging enable
```

출력 대상 구성

문제 해결 및 성능 모니터링을 위해 syslog 메시지 사용을 최적화하려면 syslog 메시지를 보낼 위치를 하나 이상 지정하는 것이 좋습니다(내부 로그 버퍼, 하나 이상의 외부 syslog 서버, ASDM, SNMP 관리 스테이션, 콘솔 포트, 지정된 이메일 주소 또는 텔넷 및 SSH 세션 포함).

Syslog 메시지를 외부 **Syslog** 서버로 전송

외부 syslog 서버의 사용 가능한 디스크 공간에 따라 메시지를 보관할 수 있으며, 저장한 후에 로그 데이터를 조작할 수 있습니다. 예를 들어 특정 유형의 syslog 메시지가 기록될 때 실행할 작업을 지정하고, 로그에서 데이터를 추출하고 보고를 위해 기록을 다른 파일에 저장하거나, 사이트별 스크립트를 사용하여 통계를 추적할 수 있습니다.

외부 syslog 서버로 syslog 메시지를 전송하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 메시지를 syslog 서버로 전송하도록 ASA를 구성합니다.

IPv4 또는 IPv6 syslog 서버에 메시지를 전송하도록 ASA를 구성할 수 있습니다.

logging host *interface_name syslog_ip* [**tcp**[/*port*] | **udp** [/*port*] [**format emblem**]]

예제**:**

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020
```

format emblem 키워드는 UDP만 있는 syslog 서버에 대한 EMBLEM 형식 로깅을 활성화합니다. *interface_name* 인수는 syslog 서버에 액세스할 인터페이스를 지정합니다. *syslog_ip* 인수는 syslog 서버의 IP 주소를 지정합니다. **tcp**[/*port*] 또는 **udp**[/*port*] 키워드 및 인수 쌍은 ASA가 TCP 또는 UDP를 사용하여 syslog 서버로 syslog 메시지를 전송하도록 지정합니다.

UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA를 구성할 수 있지만 둘 다 사용할 수는 없습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

TCP를 지정한 경우 ASA 및 ASASM이 syslog 서버 실패를 감지하고 보안 조치로서 ASA 및 ASA 서비스 모듈을 통한 새로운 연결이 차단됩니다. TCP syslog 서버에 연결에 관계없이 새로운 연결을 허용하려면 3단계를 참조하십시오. UDP를 지정한 경우 ASA는 syslog 서버 작동 여부에 관계없이 새로운 연결을 계속 허용합니다. 각 프로토콜에 대한 유효한 포트 값은 1025부터 65535입니다. 기본 UDP 포트는 514입니다. 기본 TCP 포트는 1470입니다.

단계 **2** 어떤 syslog 메시지를 syslog 서버에 전송할지 지정합니다.

logging trap {*severity_level* | *message_list*}

예제**:**

```
ciscoasa(config)# logging trap errors
```

심각도 레벨 숫자(1~7) 또는 이름을 지정할 수 있습니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 레벨 3, 2, 1에 대해 syslog 메시지를 보냅니다. syslog 서버로 전송할 syslog 메시지를 식별하는 사용자 정의 메시지 목록을 지정할 수 있습니다.

단계 **3** (선택 사항)TCP 연결 syslog 서버가 다운되었을 때 새로운 연결을 차단하려면 이 기능을 비활성화합니다.

logging permit-hostdown

예제**:**

```
ciscoasa(config)# logging permit-hostdown
```

ASA 또는 ASASM이 syslog 메시지를 TCP 기반 syslog 서버로 전송하도록 구성되어 있고 syslog 서버가 다운되었거나 로그 대기열이 가득 찬 경우 새로운 연결이 차단됩니다. syslog 서버가 백업되고 로그 대기열이 비워지면 새로운 연결이 다시 허용됩니다.

단계 **4** (선택 사항) 로깅 시설을 대부분의 UNIX 시스템이 기대하는 값인 20 외의 다른 값으로 설정합니다.

logging facility *number*

예제:

```
ciscoasa(config)# logging facility 21
```

안전한 로깅 활성화

프로시저

로깅 호스트 명령에서 **secure** 키워드를 지정하여 보안 로깅을 활성화합니다. 또한 선택적으로 **reference-identity**를 입력합니다.

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

여기서 각 항목은 다음을 나타냅니다.

- **logging host** *interface_name syslog_ip*는 syslog 서버의 IP 주소와 syslog 서버가 상주하고 있는 인터페이스를 지정합니다.
- [**tcp**/*port* | **udp**/*port*] 는 syslog 서버가 syslog 메시지에 대해 수신 대기하는 포트(TCP 또는 UDP)를 지정합니다. **tcp** 키워드는 ASA 또는 ASASM이 TCP를 사용하여 syslog 메시지를 syslog 서버로 전송하도록 지정합니다. **udp** 키워드는 ASA 또는 ASASM이 UDP를 사용하여 syslog 메시지를 syslog 서버로 전송하도록 지정합니다.
- **format emblem** 키워드는 syslog 서버에 대한 EMBLEM 형식 로깅을 활성화합니다.
- **secure** 키워드는 원격 로깅 호스트로의 연결이 TCP에 한해 SSL/TLS를 사용하도록 지정합니다. 보안 로깅은 UDP를 지원하지 않습니다. 이 프로토콜을 사용하려고 하면 오류가 발생합니다.
- [**reference-identity** *reference_identity_name*]을 사용하면 RFC 6125 참조 ID가 이전에 구성한 참조 ID 개체에 기반하여 인증서에서 확인을 수행합니다. 참조 ID 개체에 대한 자세한 내용은 참조 ID 구성, 754 페이지을 참고하십시오.

예제:

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

EMBLEM 형식 Syslog 메시지를 Syslog 서버에 생성

EMBLEM 형식의 syslog 메시지를 syslog 서버에 생성하려면 다음 단계를 수행합니다.

프로시저

포트 514를 사용하여 UDP를 통해 EMBLEM 형식의 syslog 메시지를 syslog 서버로 보냅니다.

logging host *interface_name ip_address*{**tcp** [/*port*] | **udp** [/ *port*]] [**format emblem**]

예제:

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

format emblem 키워드는 UDP만 있는 syslog 서버에 대한 EMBLEM 형식 로깅을 활성화합니다. *interface_name* 인수는 syslog 서버에 액세스할 인터페이스를 지정합니다. *ip_address* 인수는 syslog 서버의 IP 주소를 지정합니다. **tcp**[/*port*] 또는 **udp**[/*port*] 키워드 및 인수 쌍은 ASA가 TCP 또는 UDP를 사용하여 syslog 서버로 syslog 메시지를 전송하도록 지정합니다.

UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA를 구성할 수 있습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

여러 **logging host** 명령을 사용하여 모두 syslog 메시지를 수신하는 추가 서버를 지정할 수 있습니다. 로깅 서버를 2개 이상 구성한 경우 모든 로깅 서버에 대해 로깅 심각도 레벨을 경고로 제한합니다.

TCP를 지정한 경우 ASA 또는 ASASM은 syslog 서버의 장애를 감지하고 보호 조치로서 ASA를 통한 새로운 연결을 차단합니다. UDP를 지정한 경우 ASA 또는 ASASM은 syslog 서버 작동 여부에 관계없이 새로운 연결을 계속 허용합니다. 각 프로토콜에 대한 유효한 포트 값은 1025부터 65535입니다. 기본 UDP 포트는 514입니다. 기본 TCP 포트는 1470입니다.

다른 출력 대상으로 EMBLEM 형식 Syslog 메시지 생성

EMBLEM 형식의 syslog 메시지를 다른 출력 대상으로 생성하려면 다음 단계를 수행합니다.

프로시저

EMBLEM 형식의 syslog 메시지를 텔넷 또는 SSH 세션과 같은 syslog 서버 이외의 출력 대상으로 보냅니다.

logging emblem

예제:

```
ciscoasa(config)# logging emblem
```

Syslog 메시지를 내부 로그 버퍼로 전송

임시 저장 위치 역할을 하는 내부 로그 버퍼로 어떤 syslog 메시지를 전송할지 지정해야 합니다. 새 메시지가 목록의 끝에 추가됩니다. 버퍼가 가득 차는 경우, 즉 버퍼가 줄 바꿈되는 경우 가득 찬 버퍼를 다른 위치로 저장하도록 ASA 및 ASASM을 구성하지 않는 한 새로운 메시지가 생성되면서 이전 메시지를 덮어씁니다.

syslog 메시지를 내부 로그 버퍼로 보내려면 다음 단계를 수행합니다.

프로시저

단계 **1** 임시 저장 위치 역할을 하는 내부 로그 버퍼로 어떤 syslog 메시지를 전송할지 지정합니다.

logging buffered {*severity_level* | *message_list*}

예제**:**

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
ciscoasa(config)# logging buffered notif-list
```

새 메시지가 목록의 끝에 추가됩니다. 버퍼가 가득 차는 경우, 즉 버퍼가 줄 바꿈되는 경우 가득 찬 버퍼를 다른 위치로 저장하도록 ASA 및 ASASM을 구성하지 않는 한 새로운 메시지가 생성되면서 이전 메시지를 덮어씁니다. 내부 로그 버퍼를 비우려면 **clear logging buffer** 명령을 입력합니다.

단계 **2** 내부 로그 버퍼의 크기를 변경합니다. 기본 버퍼 크기는 4KB입니다.

logging buffer-size 바이트

예제**:**

```
ciscoasa(config)# logging buffer-size 16384
```

단계 **3** 다음 옵션 중 하나를 선택합니다.

- 새 메시지를 내부 로그 버퍼에 저장하고 전체 로그 버퍼 내용을 내부 플래시 메모리에 저장합니다.

  logging flash-bufferwrap

  예:

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

- 새 메시지를 내부 로그 버퍼에 저장하고 전체 로그 버퍼 내용을 FTP 서버에 저장합니다.

  logging ftp-bufferwrap

  예:

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

버퍼 내용을 다른 위치에 저장할 때는 ASA 및 ASASM이 다음 타임 스탬프 형식을 사용하는 이름으로 로그 파일을 생성합니다.

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

*YYYY*는 연도이고 *MM*는 달이며 *DD*는 날짜입니다. *HHMMSS*는 시간, 분, 초를 나타냅니다.

- 로그 버퍼 내용을 저장할 FTP 서버를 식별합니다.

  logging ftp-server *server pathusername password*

  예:

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  server 인수는 외부 FTP 서버의 IP 주소를 지정합니다. *path* 인수는 로그 버퍼 데이터를 저장할 FTP 서버에서 디렉터리 경로를 지정합니다. 이 경로는 FTP 루트 디렉터리에 대한 상대적인 경로입니다. *username* 인수는 FTP 서버 로그인에 유효한 사용자 이름을 지정합니다. *password* 인수는 지정된 사용자 이름에 대한 비밀번호를 나타냅니다.

- 현재 로그 버퍼 내용을 내부 플래시 메모리에 저장합니다.

  logging savelog [*savefile*]

  예:

  ```
  ciscoasa(config)# logging savelog latest-logfile.txt
  ```

로그에 사용할 수 있는 내부 플래시 메모리양 변경

로그에 사용할 수 있는 내부 플래시 메모리의 양을 변경하려면 다음 단계를 수행합니다.

프로시저

단계 1 로그 파일 저장에 사용 가능한 내부 플래시 메모리의 최대량을 지정합니다.

logging flash-maximum-allocation *KB*

예제**:**

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

기본적으로 ASA는 로그 데이터를 위해 최대 1MB의 내부 플래시 메모리를 사용할 수 있습니다. 로그 데이터 저장을 위해 ASA 및 ASASM에서 비어 있어야 하는 내부 플래시 메모리의 최소 용량은 3MB입니다.

내부 플래시 메모리에 저장되는 로그 파일로 인해 남을 내부 플래시 메모리가 구성된 최소 용량보다 작아질 경우 ASA 또는 ASASM은 가장 오래된 로그 파일을 삭제하여 새 로그 파일을 저장한 후에 최

소 여유 공간을 확보할 수 있도록 합니다. 삭제할 파일이 없거나 모든 오래된 파일을 삭제한 후에도 여유 메모리가 부족하면 ASA 또는 ASASM은 새 로그 파일을 저장할 수 없습니다.

단계 **2** ASA 또는 ASASM이 로그 파일을 저장하기 위해 필요한 최소 내부 플래시 메모리 여유 공간을 지정합니다.

logging flash-minimum-free *KB*

예제**:**

```
ciscoasa(config)# logging flash-minimum-free 4000
```

이메일 주소로 **Syslog** 메시지 전송

이메일 주소로 syslog 메시지를 전송하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 이메일 주소로 어떤 syslog 메시지를 보낼지 지정합니다.

logging mail {*severity_level* | *message_list*}

예제**:**

```
ciscoasa(config)# logging mail high-priority
```

이메일로 보낼 때는 이메일 메시지의 제목 줄에 syslog 메시지가 표시됩니다. 따라서 심각, 경고 및 긴급과 같이 높은 심각도 레벨으로 syslog 메시지를 관리자에게 알리도록 이 옵션을 구성하는 것이 좋습니다.

단계 **2** syslog 메시지를 이메일 주소로 보낼 때 사용할 소스 이메일 주소를 지정합니다.

logging from-address *email_address*

예제**:**

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

단계 **3** syslog 메시지를 이메일 주소로 보낼 때 사용할 소스 이메일 주소를 지정합니다.

logging recipient-address *e-mail_address*[*severity_level*]

예제**:**

```
ciscoasa(config)# logging recipient-address admin@example.com
```

단계 **4** syslog 메시지를 이메일 주소로 보낼 때 사용할 SMTP 서버를 지정합니다.

smtp-server *ip_address*

예제:

```
ciscoasa(config)# smtp-server 10.1.1.1
```

Syslog 메시지를 ASDM에 전송

syslog 메시지를 ASDM에 보내려면 다음 단계를 수행합니다.

프로시저

단계 **1** ASDM으로 어떤 syslog 메시지를 보낼지 지정합니다.

logging asdm {*severity_level* | *message_list*}

예제:

```
ciscoasa(config)# logging asdm 2
```

ASA 또는 ASASM은 ASDM으로 전송 대기 중인 syslog 메시지에 대한 버퍼 영역을 남겨두고 생성되는 메시지를 버퍼에 저장합니다. ASDM 로그 버퍼는 내부 로그 버퍼와 다른 버퍼입니다. ASDM 로그 버퍼가 가득 차면 ASA 또는 ASASM은 가장 오래된 syslog 메시지를 삭제하여 새로운 메시지를 위한 버퍼 공간을 확보합니다. ASDM의 기본 설정은 새로운 메시지를 위해 가장 오래된 syslog 메시지를 삭제하는 것입니다. ASDM 로그 버퍼에 보관되는 syslog 메시지의 수를 제어하려면 버퍼의 크기를 변경할 수 있습니다.

단계 **2** ASDM 로그 버퍼에 보존할 syslog 메시지의 수를 지정합니다.

logging asdm-buffer-size *num_of_msgs*

예제:

```
ciscoasa(config)# logging asdm-buffer-size 200
```

ASDM 로그 버퍼의 현재 내용을 비우려면 **clear logging asdm** 명령을 입력합니다.

로깅 대기열 구성

로깅 대기열을 구성하려면 다음 작업을 수행합니다.

프로시저

ASA 및 ASASM이 구성된 출력 대상으로 보내기 전에 대기열에 저장할 수 있는 syslog 메시지의 수를 지정합니다.

logging queue *message_count*

예제:

```
ciscoasa(config)# logging queue 300
```

ASA 및 ASASM은 메모리에 고정된 수의 블록을 가지고 있고 이 블록은 구성된 출력 대상으로 전송을 기다리는 동안 syslog 메시지 버퍼링을 위해 할당될 수 있습니다. 필요한 블록 개수는 syslog 메시지 대기열의 길이와 지정된 syslog 서버의 수에 따라 달라집니다. 기본 대기열 크기는 syslog 메시지 512개입니다. 대기열 크기는 이용 가능한 블록 메모리로만 제한됩니다. 유효한 값은 플랫폼에 따라 0~8192개의 메시지입니다. 로깅 대기열이 0으로 설정된 경우 대기열은 최대 구성 가능한 크기(메시지 8192개)가 됩니다.

Syslog 메시지를 콘솔 포트로 전송

syslog 메시지를 콘솔 포트로 보내려면 다음 단계를 수행합니다.

프로시저

콘솔 포트로 어떤 syslog 메시지를 보낼지 지정합니다.

logging console { *severity_level* | *message_list*}

예제:

```
ciscoasa(config)# logging console errors
```

Syslog 메시지를 SNMP 서버로 전송

SNMP 서버로 로깅을 활성화하려면 다음 단계를 수행합니다.

프로시저

SNMP 로깅을 활성화하고 어떤 메시지를 SNMP 서버로 보낼지 지정합니다.

logging history [*logging_list* | *level*]

예제:

```
ciscoasa(config)# logging history errors
```

SNMP 로깅을 비활성화하려면 **no logging history** 명령을 입력합니다.

Syslog 메시지를 텔넷이나 SSH 세션으로 전송

syslog 메시지를 텔넷이나 SSH 세션으로 전송하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 어떤 syslog 메시지를 텔넷 혹은 SSH 세션으로 보낼지 지정합니다.

logging monitor {*severity_level* | *message_list*}

예제**:**

```
ciscoasa(config)# logging monitor 6
```

단계 **2** 현재 세션에 대한 로깅만 허용합니다.

terminal monitor

예제**:**

```
ciscoasa(config)# terminal monitor
```

로그아웃하고 다시 로그인하면 이 명령을 다시 입력해야 합니다. 현재 세션에 대한 로깅을 비활성화하려면 **terminal no monitor** 명령을 입력합니다.

Syslog 메시지 구성

Syslogs에서 잘못된 사용자 이름 표시 또는 숨기기

로그인 시도가 실패하면 syslog 메시지에서 잘못된 사용자 이름을 표시하거나 숨길 수 있습니다. 기본 설정은 사용자 이름이 잘못되었거나 유효성을 알 수 없는 경우 사용자 이름을 숨기는 것입니다. 예를 들어 사용자가 사용자 이름 대신 비밀번호를 실수로 입력한 경우, 결과 syslog 메시지에서 "사용자 이름"을 숨기는 것이 훨씬 더 안전합니다. 로그인 문제를 트러블슈팅하는 데 도움을 주기 위해 잘못된 사용자 이름을 표시할 수 있습니다.

프로시저

단계 **1** 잘못된 사용자 이름을 표시합니다.

no logging hide username

단계 **2** 잘못된 사용자 이름을 숨깁니다.

logging hide username

Syslog 메시지에 날짜와 시간 포함

syslog 메시지에 날짜와 시간을 포함하려면 다음 단계를 수행합니다.

프로시저

---

syslog 메시지가 생성된 날짜 및 시간을 포함하도록 지정합니다.

logging timestamp

예제:

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

syslog 메시지에서 날짜 및 시간을 제거하려면 **no logging timestamp** 명령을 입력합니다.

Syslog 메시지 비활성화

지정된 syslog 메시지를 비활성화하려면 다음 단계를 수행합니다.

프로시저

ASA 또는 ASASM이 특정 syslog 메시지의 생성을 방지합니다.

no logging message *syslog_id*

예제:

```
ciscoasa(config)# no logging message 113019
```

비활성화된 syslog 메시지를 다시 활성화하려면 **logging message** *syslog_id* 명령을 입력합니다(예: **logging message 113019**). 모든 비활성화된 syslog 메시지 로깅을 다시 활성화하려면 **clear configure logging disabled** 명령을 입력합니다.

Syslog 메시지의 심각도 수준 변경

syslog 메시지의 심각도 레벨을 변경하려면 다음 단계를 수행합니다.

프로시저

Syslog 메시지의 심각도 레벨을 지정합니다.

logging message *syslog_id* **level** *severity_level*

예제**:**

```
ciscoasa(config)# logging message 113019 level 5
```

syslog 메시지의 심각도를 원래의 설정으로 되돌리려면 **no logging message** *syslog_id* **level***severity_level* 명령(예: **no logging message 113019 level 5**)을 입력합니다. 모든 수정된 syslog 메시지의 심각도를 원래의 설정으로 되돌리려면 **clear configure logging level** 명령을 사용합니다.

대기 유닛의 **Syslog** 메시지 차단

스탠바이 유닛에서 생성되는 특정 syslog 메시지를 차단하려면 다음 단계를 수행합니다.

프로시저

스탠바이 유닛에서 생성 차단되었던 특정 syslog 메시지를 차단 해제합니다.

logging message *syslog-id* **standby**

예제**:**

```
ciscoasa(config)# logging message 403503 standby
```

스탠바이 유닛에서 특정 syslog 메시지의 생성을 차단하려면 이 명령의 **no** 형식을 사용합니다.

logging standby 명령을 사용하여 페일오버가 발생할 경우 페일오버 스탠바이 ASA의 syslog 메시지가 동기화를 유지하도록 합니다.

참고 **logging standby** 명령을 사용하면 syslog 서버, SNMP 서버 및 FTP 서버와 같은 공유 로깅 대상에서 트래픽이 두 배 증가합니다.

디바이스 **ID**를 **EMBLEM** 이외 형식 **Syslog** 메시지에 포함

non-EMBLEM 형식 syslog 메시지에 디바이스 ID를 포함하려면 다음 단계를 수행합니다.

프로시저

EMBLEM 이외-형식 syslog 메시지에 디바이스 ID를 포함하도록 ASA 또는 ASASM을 구성합니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다.

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

예제**:**

```
ciscoasa(config)# logging device-id hostname
```

```
ciscoasa(config)# logging device-id context-name
```

context-name 키워드는 현재 상황의 이름을 디바이스 ID로 사용하도록 지정합니다(다중 상황 모드에만 적용). 다중 상황 모드에서 관리자 상황 모드를 위해 디바이스 ID 로깅을 활성화하는 경우 시스템 실행 공간에서 발생하는 메시지는 **system**의 디바이스 ID를 사용하고 관리자 상황에서 발생하는 메시지는 관리자 상황의 이름을 디바이스 ID로 사용합니다.

참고 ASA 클러스터에서는 항상 선택된 인터페이스에 대해 마스터 유닛 IP 주소를 사용합니다.

cluster-id 키워드는 클러스터에서 개별 ASA 유닛의 부트 구성 고유 이름을 디바이스 ID로 지정합니다. **hostname** 키워드는 ASA의 호스트 이름을 디바이스 ID로 사용하도록 지정합니다. **ipaddress** *interface_name* 키워드-인수 쌍은 *interface_name*으로 지정된 인터페이스 IP 주소를 디바이스 ID로 사용하도록 지정합니다. **ipaddress** 키워드를 사용하는 경우 syslog 메시지가 전송되는 인터페이스에 관계없이 디바이스 ID가 지정된 ASA 인터페이스 IP 주소가 됩니다. 클러스터 환경에서 **system** 키워드는 디바이스 ID가 인터페이스의 시스템 IP 주소가 되도록 만듭니다. 이 키워드는 디바이스에서 전송되는 모든 syslog 메시지에 대해 하나의 일관된 디바이스 ID를 제공합니다. **string** *text* 키워드-인수 쌍은 문자열이 디바이스 ID로 사용되도록 지정합니다. 문자열은 최대 16자를 포함할 수 있습니다.

공백 또는 다음 문자를 사용할 수 없습니다.

- &(앰퍼샌드)
- `(작은따옴표)
- "(큰따옴표)
- <(보다 작음)
- >(보다 큼)
- ? (물음표)

참고 활성화된 경우 디바이스 ID가 EMBLEM 형식 syslog 메시지나 SNMP 트랩에 표시되지 않습니다.

사용자 지정 이벤트 목록 생성

다음 3개의 기준을 이용하여 이벤트 목록을 정의합니다.

- 이벤트 클래스
- 심각도
- 메시지 ID

특정 로깅 대상(예: SNMP 서버)으로 보낼 사용자 지정 이벤트 목록을 생성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 내부 로그 버퍼에 저장할 메시지를 선택할 기준을 지정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 레벨 3, 2, 1에 대해 syslog 메시지를 보냅니다.

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

예제**:**

```
ciscoasa(config)# logging list list-notif level 3
```

name 인수는 목록의 이름을 지정합니다. **level** *level* 키워드 및 인수 쌍은 심각도 레벨을 지정합니다. **class** *message_class* 키워드-인수 쌍은 특정 메시지 클래스를 지정합니다. **message** *start_id* [*-end_id*] 키워드-인수 쌍은 개별 syslog 메시지 숫자 또는 숫자 범위를 지정합니다.

참고 심각도 레벨 이름을 syslog 메시지 목록의 이름으로 사용하지 마십시오. 금지된 이름에는 긴급, 경고, 중요 , 오류, 알림, 정보 및 디버깅이 포함됩니다. 마찬가지로 이벤트 목록 이름의 맨 앞에 이러한 단어의 처음 3개 글자를 사용하지 마십시오. 예를 들어 "err"로 시작하는 이벤트 목록 이름을 사용하지 마십시오.

단계 **2** (선택 사항) 목록에 메시지 선택 기준을 더 추가합니다.

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

예제**:**

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

이전 단계와 동일한 명령을 입력하여 기존 메시지 목록의 이름과 추가 기준을 지정합니다. 목록에 추가할 각 기준에 대한 새로운 명령을 입력합니다. 예를 들어 다음과 같이 목록에 포함할 syslog 메시지에 대한 기준을 지정할 수 있습니다.

- 104024~105999 범위에 해당하는 Syslog 메시지 ID.
- 심각도 레벨이 중요 이상인 모든 syslog 메시지(긴급, 경고 또는 중요).
- 심각도 레벨이 경고 이상인 모든 ha 클래스 syslog 메시지(긴급, 경고, 오류 또는 경고).

참고 다음 조건을 하나라도 충족하면 syslog 메시지가 로깅됩니다. syslog 메시지가 조건을 둘 이상 충족하는 경우 메시지는 한 번만 로깅됩니다.

로깅 필터 구성

클래스의 모든 **Syslog** 메시지를 지정된 출력 대상으로 전송

클래스의 모든 syslog 메시지를 지정된 출력 대상으로 전송하려면 다음 단계를 수행합니다.

프로시저

지정된 출력 대상 명령에서 컨피그레이션을 무시합니다. 예를 들어 심각도 레벨 7의 메시지가 내부 로그 버퍼로 전송되도록 지정하고 심각도 레벨 3의 ha 클래스 메시지가 내부 로그 버퍼로 전송되도록 지정한 경우 후자의 컨피그레이션이 우선합니다.

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

예제**:**

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered, **history**, **mail**, **monitor**, **trap** 키워드는 이 클래스의 syslog 메시지를 보낼 출력 대상을 지정합니다. **history** 키워드는 SNMP 로깅을 활성화합니다. **monitor** 키워드는 텔넷 및 SSH 로깅을 활성화합니다. **trap** 키워드는 syslog 서버 로깅을 활성화합니다. 명령 라인 항목당 하나의 대상을 선택합니다. 클래스가 2개 이상의 대상으로 전송되도록 지정하려면 각 출력 대상에 대해 새로운 명령을 입력합니다.

Syslog 메시지 생성 속도 제한

syslog 메시지 생성 속도를 제한하려면 다음 단계를 수행합니다.

프로시저

지정된 심각도 레벨(1~7)을 지정된 기간 내의 메시지 집합 또는 개별 메시지(대상 아님)에 적용합니다.

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

예제**:**

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

속도 제한은 모든 구성된 대상으로 전송되는 메시지의 양에 영향을 줍니다. 로깅 속도 제한을 기본값으로 재설정하려면 **clear running-config logging rate-limit** 명령을 입력합니다. 로깅 속도 제한을 재설정하려면 **clear configure logging rate-limit** 명령을 입력합니다.

로그 모니터링

로깅 상태 모니터링에 대해서는 다음 명령을 참고하십시오.

- **show logging**

  이 명령은 심각도 레벨을 포함하여 syslog 메시지를 표시합니다.

  참고 볼 수 있는 최대 syslog 메시지 수는 1000개로 기본 설정되어 있습니다. 볼 수 있는 최대 syslog 메시지 개수는 2000입니다.

- **show logging message**

  이 명령은 심각도 레벨이 수정된 syslog 메시지와 비활성화된 syslog 메시지 목록을 표시합니다.

- **show logging message** *message_ID*

  이 명령은 특정 syslog 메시지의 심각도 레벨을 보여줍니다.

- **show logging queue**

  이 명령은 로깅 대기열과 대기열 통계를 보여줍니다.

- **show running-config logging rate-limit**

  이 명령은 현재 로깅 속도 제한 설정을 보여줍니다.

로깅의 예

다음 예는 **show logging** 명령에 대해 표시되는 로깅 정보의 예를 보여 줍니다.

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address “10.1.1.1”
    Mail logging: disabled
    ASDM logging: disabled


ciscoasa (config)# show logging
Syslog logging: enabled
    Facility: 20
```

```
Timestamp logging: disabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: enabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 330272 messages logged
Trap logging: level debugging, facility 20, 325464 messages logged
    Logging to inside 2001:164:5:1::123
Permit-hostdown logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

다음 예는 syslog 메시지 활성화 여부와 지정된 syslog 메시지의 심각도 레벨을 제어하는 방법을 보여 줍니다.

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

로깅 내역

표 ***54:*** 로깅 내역

기능 이름	플랫폼 릴리스	설명
로깅	7.0(1)	다양한 출력 대상을 통해 ASA 네트워크 로깅 정보를 제공하며 로그 파일을 보고 저장할 수 있는 옵션을 포함합니다.
속도 제한	7.0(4)	syslog 메시지가 생성되는 속도를 제한합니다. 다음 명령을 도입했습니다. **logging rate-limit**

기능 이름	플랫폼 릴리스	설명
로깅 목록	7.2(1)	다른 명령에서 다양한 기준(로깅 레벨, 이벤트 클래스, 메시지 ID)으로 메시지를 지정하는 데 사용할 로깅 목록을 생성합니다. 다음 명령을 도입했습니다. **logging list**.
보안 로깅	8.0(2)	원격 로깅 호스트로의 연결이 SSL/TLS를 사용할지 지정합니다. 이 옵션은 선택된 프로토콜이 TCP인 경우에만 유효합니다. 다음 명령을 수정했습니다. **logging host**.
로깅 클래스	8.0(4), 8.1(1)	ipaa 이벤트 클래스 로깅 메시지에 대한 지원이 추가되었습니다. 다음 명령을 수정했습니다. **logging class**
로깅 클래스 및 저장된 로깅 버퍼	8.2(1)	dap 이벤트 클래스 로깅 메시지에 대한 지원이 추가되었습니다. 다음 명령을 수정했습니다. **logging class** 저장된 로깅 버퍼 지우기에 대한 지원이 추가되었습니다(ASDM, 내부, FTP 및 플래시). 다음 명령을 도입했습니다. **clear logging queue bufferwrap**
비밀번호 암호화	8.3(1)	비밀번호 암호화 지원이 추가되었습니다. 다음 명령을 수정했습니다. **logging ftp server**
로그 뷰어	8.3(1)	로그 뷰어에 소스 및 대상 IP 주소가 추가되었습니다.

기능 이름	플랫폼 릴리스	설명
향상된 로깅 및 연결 차단	8.3(2)	TCP를 사용하도록 syslog 서버를 구성하고 syslog 서버를 사용할 수 없는 경우 ASA는 서버를 다시 사용할 수 있을 때까지 syslog 메시지를 생성하는 새로운 연결을 차단합니다(예: VPN, 방화벽 및 cut-through-proxy 연결). 이 기능은 ASA의 로깅 대기열이 가득 찼을 때도 새로운 연결을 차단하도록 개선되었습니다. 로깅 대기열이 비워지면 연결이 재개됩니다. 이 기능은 EAL4 공통 평가 기준 준수를 위해 추가되었습니다. 요청이 없다면 syslog 메시지를 보내거나 받을 수 없을 때 연결을 허용할 것을 권장합니다. 연결을 허용하려면 계속해서 **logging permit-hostdown** 명령을 사용하십시오.. 다음 syslog 메시지를 도입했습니다. 414005, 414006, 414007 및 414008 다음 명령을 수정했습니다. **show logging**.
Syslog 메시지 필터링 및 정렬	8.4(1)	다음에 대한 지원이 추가되었습니다. • 다양한 열에 대응하는 여러 문자열을 기준으로 하는 Syslog 메시지 필터링 • 사용자 정의 필터의 생성 • 메시지의 열 정렬 세부적인 정보는 ASDM 구성 가이드를 참고하십시오. 이 기능은 모든 ASA 버전과 상호 운용됩니다.
클러스터링	9.0(1)	ASA 5580 및 5585-X에서의 클러스터링 환경에서 syslog 메시지 생성에 대한 지원을 추가했습니다. 다음 명령을 수정했습니다. **logging device-id**

기능 이름	플랫폼 릴리스	설명
스탠바이 유닛에서의 syslog 차단	9.4(1)	장애 조치 컨피그레이션에서 스탠바이 유닛의 특정 syslog 메시지 생성 차단에 대한 지원을 추가했습니다. 다음 명령을 도입했습니다. **logging message** *syslog-id* **standby**
보안 Syslog 서버 연결을 위한 참조 ID	9.6(2)	이제 TLS 클라이언트 처리 시 RFC 6125, 섹션 6에 정의되어 있는 서버 ID를 확인하기 위해 규칙을 지원합니다. ID 확인은 Syslog 서버에 대한 TLS 연결을 대상으로 PKI 검증을 하는 동안에만 수행됩니다. 표시되는 ID가 구성된 참조 ID에 대해 일치될 수 없는 경우 연결이 설정되지 않습니다. 다음 명령을 추가 또는 수정했습니다. **[no] crypto ca reference-identity**, **logging host**
Syslog 서버에 대한 IPv6 주소 지원	9.7(1)	이제 TCP 및 UDP를 통해 syslog를 기록, 전송 및 수신하기 위해 IPv6 주소로 syslog 서버를 구성할 수 있습니다. 다음 명령을 수정했습니다. **logging host**

42 장

SNMP

이 장에서는 Cisco ASA를 모니터링하기 위한 SNMP(Simple Network Management Protocol) 구성 방법을 설명합니다.

SNMP 정보

SNMP는 네트워크 디바이스 간의 관리 정보 교환을 촉진하기 위한 애플리케이션 계층 프로토콜이며 TCP/IP 프로토콜 군의 일부입니다. ASA는 SNMP 버전 1, 2c 및 3을 사용하여 네트워크 모니터링을 지원하고 모든 3개 버전의 동시 사용도 지원합니다. ASA 인터페이스에서 실행되는 SNMP 에이전트를 사용하면 HP OpenView와 같은 NMS(네트워크 관리 시스템)을 통해 네트워크 디바이스를 모니터링할 수 있습니다. ASA는 GET 요청 발행을 통해 SNMP 읽기 전용 액세스를 지원합니다. SNMP 쓰기 액세스는 허용되지 않으므로 SNMP를 사용하여 변경할 수는 없습니다. 또한 SNMP SET 요청은 지원되지 않습니다.

ASA를 NMS로의 특정 이벤트(알림 포함)에 대해 관리 디바이스에서 관리 스테이션으로 전송되는 요청하지 않은 메시지인 트랩을 보내도록 구성하거나 NMS를 사용하여 보안 디바이스에서 MIB(관리 정보 기반)를 찾아볼 수 있습니다. MIB는 정의 모음이고 ASA은 각 정의에 대한 값 데이터베이스를 유지합니다. MIB를 찾아보는 것은 NMS에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 발행하는 것을 의미합니다.

ASA에는 예를 들어 네트워크 링크가 실행 또는 중단 상태로 전환될 때 알림이 필요하도록 사전 정의된 이벤트가 발생하는 경우 지정된 관리 스테이션에 알려주는 SNMP 에이전트가 있습니다. 이때 보내는 알림은 관리 스테이션에 스스로를 식별하는 SNMP OID를 포함합니다. ASA 에이전트는 관리 스테이션이 정보를 요구할 때 응답하기도 합니다.

SNMP 용어

다음 표는 SNMP에서 작업할 때 일반적으로 사용되는 용어를 나열합니다.

표 *55: SNMP* 용어

용어	설명
에이전트	ASA에서 실행되는 SNMP 서버입니다. SNMP 에이전트는 다음과 같은 특징을 갖습니다. • 정보 요청 및 네트워크 관리 스테이션의 작업에 대해 응답합니다. • SNMP 관리자가 보거나 변경할 수 있는 객체 모음인 MIB(관리 정보 기반)에 대한 액세스를 제어합니다. • SET 작업을 허용하지 않습니다.
찾아보기	디바이스의 SNMP 에이전트에서 필요한 정보를 폴링함으로써 네트워크 관리 스테이션에서 해당 디바이스의 상태를 모니터링합니다. 이 작업은 값을 결정하기 위해 네트워크 관리 스테이션에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 생성하는 것을 포함할 수 있습니다.
MIB(관리 정보 기반)	패킷, 연결, 버퍼, 장애 조치 등에 관한 정보를 수집하기 위한 표준화된 데이터 구조입니다. MIB는 대부분의 네트워크 디바이스에서 사용되는 제품, 프로토콜 및 하드웨어 표준으로 정의됩니다. SNMP 네트워크 관리 스테이션은 MIB를 찾아보고 특정 데이터나 이벤트 전송을 실시간으로 요청할 수 있습니다.
NMS(네트워크 관리 스테이션)	SNMP 이벤트를 모니터링하고 ASA 등의 디바이스를 관리하도록 설정된 PC나 워크스테이션입니다.
OID(객체 식별자)	NMS에서 디바이스를 식별하고 사용자에게 모니터링 및 표시되는 정보의 소스를 보여주는 시스템입니다.
트랩	SNMP 에이전트에서 NMS로 메시지를 생성하는 사전 정의된 이벤트입니다. 이벤트는 linkup, linkdown, coldstart, warmstart, authentication 또는 syslog 메시지와 같은 경보 조건을 포함합니다.

MIB 및 트랩

MIB는 표준이거나 기업별로 구분됩니다. 표준 MIB는 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. 트랩은 네트워크 디바이스에서 발생하는 중요 이벤트(대부분 오류나 장애)를 보고합니다. SNMP 트랩은 표준 또는 기업별 MIB로 정의됩니다. 표준 트랩은 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. SNMP 트랩은 ASA, ASAv 또는 ASASM 소프트웨어로 컴파일됩니다.

필요한 경우 다음 위치에서 RFC, 표준 MIB 및 표준 트랩을 다운로드할 수 있습니다.

http://www.ietf.org/

다음 위치에서 Cisco MIB, 트랩 및 OID의 전체 목록을 검색하십시오.

ftp://ftp.cisco.com/pub/mibs/

또한 다음 위치에서 FTP를 통해 Cisco OID를 다운로드할 수 있습니다.

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

참고 소프트웨어 7.2(1), 8.0(2) 이후 버전에서는 SNMP를 통해 액세스하는 인터페이스 정보를 약 5초마다 새로 고칩니다. 따라서 연속 폴링 사이에 적어도 5초를 기다리는 것이 좋습니다.

MIB에 있는 모든 OID가 지원되지는 않습니다. 특정 ASA 또는 ASASM에 대해 지원되는 SNMP MIB 및 OID 목록을 얻으려면 다음 명령을 입력하십시오.

```
ciscoasa(config)# show snmp-server oidlist
```

참고 **oidlist** 키워드는 **show snmp-server** 명령 도움말에 대한 옵션 목록에 나타나지 않더라도 사용할 수 있습니다. 그러나 이 명령은 Cisco TAC 전용입니다. 이 명령을 사용하기 전에 Cisco TAC에 문의하십시오.

다음은 **show snmp-server oidlist** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
```

```
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

SNMP Object Identifier

모든 Cisco 시스템 레벨 제품에는 MIB II sysObjectID로 사용하기 위한 SNMP OID(object identifier)가 있습니다. CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB는 SNMPv2-MIB, Entity Sensor MIB 및 Entity Sensor Threshold Ext MIB에서 sysObjectID 개체로 보고될 수 있는 OID를 포함합니다. 이 값을 사용하여 모델 유형을 식별할 수 있습니다. 다음 표에는 ASA 및 ISA 모델의 sysObjectID OID가 나와 있습니다.

표 ***56: SNMP Object Identifier***

제품 **ID**	**sysObjectID**	모델 번호
ASA 5506 Adaptive Security Appliance	ciscoASA5506(ciscoProducts 2114)	ASA 5506-X
ASA 5506 Adaptive Security Appliance 보안 상황	ciscoASA5506sc(ciscoProducts 2115)	ASA 5506-X 보안 상황
ASA 5506 Adaptive Security Appliance 시스템 상황	ciscoASA5506sy(ciscoProducts 2116)	ASA 5506-X 시스템 상황

제품 **ID**	**sysObjectID**	모델 번호
ASA 5506W Adaptive Security Appliance	ciscoASA5506W(ciscoProducts 2117)	ASA 5506W-X
ASA 5506W Adaptive Security Appliance 보안 상황	ciscoASA5506Wsc(ciscoProducts 2118)	ASA 5506W-X 보안 상황
ASA 5506W Adaptive Security Appliance 시스템 상황	ciscoASA5506Wsy(ciscoProducts 2119)	ASA 5506W-X 시스템 상황
ASA 5508 Adaptive Security Appliance	ciscoASA5508(ciscoProducts 2120)	ASA 5508-X
ASA 5508 Adaptive Security Appliance 보안 상황	ciscoASA5508sc(ciscoProducts 2121)	ASA 5508-X 보안 상황
ASA 5508 Adaptive Security Appliance 시스템 상황	ciscoASA5508sy(ciscoProducts 2122)	ASA 5508-X 시스템 상황
ASA 5506 Adaptive Security Appliance(페이로드 암호화 없음)	ciscoASA5506K7(ciscoProducts 2123)	ASA 5506-X Adaptive Security Appliance(페이로드 암호화 없음)
ASA 5506 Adaptive Security Appliance 보안 상황(페이로드 암호화 없음)	ciscoASA5506K7sc(ciscoProducts 2124)	ASA 5506-X Adaptive Security Appliance 보안 상황(페이로드 암호화 없음)
ASA 5506 Adaptive Security Appliance 시스템 상황(페이로드 암호화 없음)	ciscoASA5506K7sy(ciscoProducts 2125)	ASA 5506-X Adaptive Security Appliance 시스템 상황(페이로드 암호화 없음)
ASA 5508 Adaptive Security Appliance(페이로드 암호화 없음)	ciscoASA5508K7(ciscoProducts 2126)	ASA 5508-X Adaptive Security Appliance 시스템 상황(페이로드 암호화 없음)
ASA 5508 Adaptive Security Appliance 보안 상황(페이로드 암호화 없음)	ciscoASA5508K7sc(ciscoProducts 2127)	ASA 5508-X Adaptive Security Appliance 보안 상황(페이로드 암호화 없음)
ASA 5508 Adaptive Security Appliance 시스템 상황(페이로드 암호화 없음)	ciscoASA5508K7sy(ciscoProducts 2128)	ASA 5508-X Adaptive Security Appliance 시스템 상황(페이로드 암호화 없음)
ASA5585-SSP10	ciscoASA5585Ssp10(ciscoProducts 1194)	ASA 5585-X SSP-10
ASA5585-SSP20	ciscoASA5585Ssp20(ciscoProducts 1195)	ASA 5585-X SSP-20
ASA5585-SSP40	ciscoASA5585Ssp40(ciscoProducts 1196)	ASA 5585-X SSP-40
ASA5585-SSP60	ciscoASA5585Ssp60(ciscoProducts 1197)	ASA 5585-X SSP-60
ASA5585-SSP10	ciscoASA5585Ssp10sc(ciscoProducts 1198)	ASA 5585-X SSP-10 보안 상황
ASA5585-SSP20	ciscoASA5585Ssp20sc(ciscoProducts 1199)	ASA 5585-X SSP-20 보안 상황
ASA5585-SSP40	ciscoASA5585Ssp40sc(ciscoProducts 1200)	ASA 5585-X SSP-40 보안 상황

제품 **ID**	**sysObjectID**	모델 번호
ASA5585-SSP60	ciscoASA5585Ssp60sc(ciscoProducts 1201)	ASA 5585-X SSP-60 보안 상황
ASA5585-SSP10	ciscoASA5585Ssp10sy(ciscoProducts 1202)	ASA 5585-X SSP-10 시스템 상황
ASA5585-SSP20	ciscoASA5585Ssp20sy(ciscoProducts 1203)	ASA 5585-X SSP-20 시스템 상황
ASA5585-SSP40	ciscoASA5585Ssp40sy(ciscoProducts 1204)	ASA 5585-X SSP-40 시스템 상황
ASA5585-SSP60	ciscoASA5585Ssp60sy(ciscoProducts 1205)	ASA 5585-X SSP-60 시스템 상황
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈	ciscoAsaSm1(ciscoProducts 1277)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈 보안 상황	ciscoAsaSm1sc(ciscoProducts 1275)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 보안 상황
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈 보안 상황(페이로드 암호화 없음)	ciscoAsaSm1K7sc(ciscoProducts 1334)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 보안 상황(페이로드 암호화 없음)
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈 시스템 상황	ciscoAsaSm1sy(ciscoProducts 1276)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 시스템 상황
Catalyst 스위치 시스템 상황/7600 라우터용 ASA 서비스 모듈(페이로드 암호화 없음)	ciscoAsaSm1K7sy(ciscoProducts 1335)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 시스템 상황(페이로드 암호화 없음)
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈 시스템 상황(페이로드 암호화 없음)	ciscoAsaSm1K7(ciscoProducts 1336)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈(페이로드 암호화 없음)
ASA 5512	ciscoASA5512(ciscoProducts 1407)	ASA 5512 Adaptive Security Appliance
ASA5525	ciscoASA5525(ciscoProducts 1408)	ASA 5525 Adaptive Security Appliance
ASA 5545	ciscoASA5545(ciscoProducts 1409)	ASA 5545 Adaptive Security Appliance
ASA 5555	ciscoASA5555(ciscoProducts 1410)	ASA 5555 Adaptive Security Appliance
ASA 5512 Security Context	ciscoASA5512sc(ciscoProducts 1411)	ASA 5512 Adaptive Security Appliance Security Context

제품 **ID**	**sysObjectID**	모델 번호
ASA 5525 Security Context	ciscoASA5525sc(ciscoProducts 1412)	ASA 5525 Adaptive Security Appliance Security Context
ASA 5545 Security Context	ciscoASA5545sc(ciscoProducts 1413)	ASA 5545 Adaptive Security Appliance Security Context
ASA 5555 Security Context	ciscoASA5555sc(ciscoProducts 1414)	ASA 5555 Adaptive Security Appliance Security Context
ASA 5512 System Context	ciscoASA5512sy(ciscoProducts 1415)	ASA 5512 Adaptive Security Appliance System Context
ASA 5515 System Context	ciscoASA5515sy(ciscoProducts 1416)	ASA 5515 Adaptive Security Appliance System Context
ASA 5525 System Context	ciscoASA5525sy(ciscoProducts1417)	ASA 5525 Adaptive Security Appliance System Context
ASA 5545 System Context	ciscoASA5545sy(ciscoProducts 1418)	ASA 5545 Adaptive Security Appliance System Context
ASA 5555 System Context	ciscoASA5555sy(ciscoProducts 1419)	ASA 5555 Adaptive Security Appliance System Context
ASA 5515 Security Context	ciscoASA5515sc(ciscoProducts 1420)	ASA 5515 Adaptive Security Appliance System Context
ASA 5515	ciscoASA5515(ciscoProducts 1421)	ASA 5515 Adaptive Security Appliance
ASAv	ciscoASAv(ciscoProducts 1902)	Cisco ASAv(Adaptive Security Virtual Appliance)
ASAv System Context	ciscoASAvsy(ciscoProducts 1903)	Cisco Adaptive Security Virtual Appliance(ASAv) System Context
ASAv Security Context	ciscoASAvsc(ciscoProducts 1904)	Cisco Adaptive Security Virtual Appliance(ASAv) Security Contex
ISA 30004C Industrial Security Appliance	ciscoProducts 2268	ciscoISA30004C
4GE Copper Security Context가 포함된 CISCO ISA30004C	ciscoProducts 2139	ciscoISA30004Csc
4GE Copper System Context가 포함된 CISCO ISA30004C	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F Industrial Security Appliance	ciscoProducts 2267	ciscoISA30002C2F
2GE 구리 포트 + 2GE Fiber Security Context가 포함된 CISCO ISA30002C2F	ciscoProducts 2142	ciscoISA30002C2Fsc

제품 **ID**	**sysObjectID**	모델 번호
2GE 구리 포트 + 2GE Fiber System Context가 포함된 CISCO ISA30002C2F	ciscoProducts 2143	ciscoISA30002C2Fsy
Cisco Industrial Security Appliance(ISA) 30004C Chassis	cevChassis 1677	cevChassisISA30004C
Cisco Industrial Security Appliance(ISA) 30002C2F Chassis	cevChassis 1678	cevChassisISA30002C2F
ISA30004C Copper SKU용 중앙 처리 장치 온도 센서	cevSensor 187	cevSensorISA30004CCpuTempSensor
ISA30002C2F Fiber용 중앙 처리 장치 온도 센서	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
ISA30004C Copper SKU용 프로세서 카드 온도 센서	cevSensor 192	cevSensorISA30004CPTS
ISA30002C2F Fiber SKU용 프로세서 카드 온도 센서	cevSensor 193	cevSensorISA30002C2FPTS
ISA30004C Copper SKU용 전력 카드 온도 센서	cevSensor 197	cevSensorISA30004CPowercardTS
ISA30002C2F Fiber SKU용 전력 카드 온도 센서	cevSensor 198	cevSensorISA30002C2FPowercardTS
ISA30004C용 포트 카드 온도 센서	cevSensor 199	cevSensorISA30004CPortcardTS
ISA30002C2F용 포트 카드 온도 센서	cevSensor 200	cevSensorISA30002C2FPortcardTS
ISA30004C Copper SKU용 중앙 처리 장치	cevModuleCpuType 329	cevCpuISA30004C
ISA30002C2F Fiber SKU용 중앙 처리 장치	cevModuleCpuType 330	cevCpuISA30002C2F
모듈 ISA30004C, ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C Industrial Security Appliance Solid State Drive	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F Industrial Security Appliance Solid State Drive	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Cisco ISA30004C/ISA30002C2F Hardware Bypass	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass

제품 **ID**	**sysObjectID**	모델 번호
FirePOWER 4140 Security Appliance, 포함된 보안 모듈 36이 있는 1U	ciscoFpr4140K9(ciscoProducts 2293)	FirePOWER 4140
FirePOWER 4120 Security Appliance, 포함된 보안 모듈 24가 있는 1U	ciscoFpr4120K9(ciscoProducts 2294)	FirePOWER 4120
FirePOWER 4110 Security Appliance, 포함된 보안 모듈 12가 있는 1U	ciscoFpr4110K9(ciscoProducts 2295)	FirePOWER 4110
FirePOWER 4110 Security Module 12	ciscoFpr4110SM12(ciscoProducts 2313)	FirePOWER 4110 Security Module 12
FirePOWER 4120 Security Module 24	ciscoFpr4120SM24(ciscoProducts 2314)	FirePOWER 4110 Security Module 24
FirePOWER 4140 Security Module 36	ciscoFpr4140SM36(ciscoProducts 2315)	FirePOWER 4110 Security Module 36
FirePOWER 4110 Chassis	cevChassis 1714	cevChassisFPR4110
FirePOWER 4120 Chassis	cevChassis 1715	cevChassisFPR4120
FirePOWER 4140 Chassis	cevChassis 1716	cevChassisFPR4140
FirePOWER 4K Fan Bay	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K Power Supply Bay	cevContainer 364	cevContainerFPR4KPowerSupplyBay
FirePOWER 4120 Supervisor Module	cevModuleFPRType 4	cevFPR4120SUPFixedModule
FirePOWER 4140 Supervisor Module	cevModuleFPRType 5	cevFPR4140SUPFixedModule
FirePOWER 4110 Supervisor Module	cevModuleFPRType 7	cevFPR4110SUPFixedModule
Cisco FirePOWER 4110 Security Appliance, Threat Defense	cevChassis 1787	cevChassisCiscoFpr4110td
Cisco FirePOWER 4120 Security Appliance, Threat Defense	cevChassis 1788	cevChassisCiscoFpr4120td
Cisco FirePOWER 4140 Security Appliance, Threat Defense	cevChassis 1789	cevChassisCiscoFpr4140td
Cisco 화력 9000 보안 모듈 24, 위협 방어	cevChassis 1791	cevChassisCiscoFpr9000SM24td
Cisco Firepower 9000 Security Module 24 NEBS, Threat Defense	cevChassis 1792	cevChassisCiscoFpr9000SM24Ntd
Cisco 화력 9000 보안 모듈 36, 위협 방어	cevChassis 1793	cevChassisCiscoFpr9000SM36td
Cisco Firepower Threat Defense Virtual, VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firepower Threat Defense Virtual, AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

물리적 공급업체 유형 값

각 Cisco 섀시 또는 독립형 시스템은 SNMP 사용을 위한 고유한 유형의 숫자를 갖습니다. entPhysicalVendorType OID는 CISCO-ENTITY-VENDORTYPE-OID-MIB에 정의되어 있습니다. 이 값은 ASA, ASAv 또는 ASASM SNMP 에이전트의 entPhysicalVendorType 개체에서 반환됩니다. 이 값을 사용하여 구성 요소의 유형(모듈, 전원 공급 장치, 팬, 센서, CPU 등)을 식별할 수 있습니다. 다음 표에는 ASA 및 ASASM 모델에 대한 실제 공급업체 유형 값이 나와 있습니다.

표 ***57:*** 물리적 공급업체 유형 값

항목	**entPhysicalVendorType OID** 설명
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈	cevCat6kWsSvcAsaSm1(cevModuleCat6000Type 169)
Catalyst 스위치/7600 라우터용 ASA 서비스 모듈(페이로드 암호화 없음)	cevCat6kWsSvcAsaSm1K7(cevModuleCat6000Type 186)
5506 Adaptive Security Appliance용 가속기	cevAcceleratorAsa5506(cevOther 10)
5506W Adaptive Security Appliance용 가속기	cevAcceleratorAsa5506W(cevOther 11)
5508 Adaptive Security Appliance용 가속기	cevAcceleratorAsa5508(cevOther 12)
5506(페이로드 암호화 없음) Adaptive Security Appliance용 가속기	cevAcceleratorAsa5506K7(cevOther 13)
5508(페이로드 암호화 없음) Adaptive Security Appliance용 가속기	cevAcceleratorAsa5508K7(cevOther 14)
Cisco ASA(Adaptive Security Appliance) 5506 섀시	cevChassisAsa5506(cevChassis 1600)
Cisco ASA(Adaptive Security Appliance) 5506W 섀시	cevChassisAsa5506W(cevChassis 1601)
Cisco ASA(Adaptive Security Appliance) 5508 섀시	cevChassisAsa5508(cevChassis 1602)
Cisco ASA(Adaptive Security Appliance) 5506 섀시(페이로드 암호화 없음)	cevChassisAsa5506K7(cevChassis 1603)
Cisco ASA(Adaptive Security Appliance) 5508 섀시(페이로드 암호화 없음)	cevChassisAsa5508K7(cevChassis 1604)
5506 Adaptive Security Appliance용 CPU	cevCpuAsa5506(cevModuleCpuType 312)
5506W Adaptive Security Appliance용 CPU	cevCpuAsa5506W(cevModuleCpuType 313)
5508 Adaptive Security Appliance용 CPU	cevCpuAsa5508(cevModuleCpuType 314)
5506(페이로드 암호화 없음) Adaptive Security Appliance용 CPU	cevCpuAsa5506K7(cevModuleCpuType 315)

항목	**entPhysicalVendorType OID** 설명
5508(페이로드 암호화 없음) Adaptive Security Appliance용 CPU	cevCpuAsa5508K7(cevModuleCpuType 316)
cevModuleASA5506 Type 섀시	cevModuleASA5506Type(cevModule 107)
5506 Adaptive Security Appliance 현장 교체 SSD	cevModuleAsa5506SSD(cevModuleASA5506Type 1)
5506W Adaptive Security Appliance 현장 교체 SSD	cevModuleAsa5506WSSD(cevModuleASA5506Type 2)
5506(페이로드 암호화 없음) Adaptive Security Appliance 현장 교체 SSD	cevModuleAsa5506K7SSD(cevModuleASA5506Type 3)
cevModuleASA5508 Type 섀시	cevModuleASA5508Type(cevModule 108)
5508 Adaptive Security Appliance 현장 교체 SSD	cevModuleAsa5508SSD(cevModuleASA5508Type 1)
5508(페이로드 암호화 없음) Adaptive Security Appliance 현장 교체 SSD	cevModuleAsa5508K7SSD(cevModuleASA5508Type 2)
Adaptive Security Appliance 5508용 섀시 냉각 팬	cevFanAsa5508ChassisFan(cevFan 247)
Adaptive Security Appliance 5508(페이로드 암호화 없음)용 섀시 냉각 팬	cevFanAsa5508K7ChassisFan(cevFan 248)
Adaptive Security Appliance 5508용 섀시 냉각 팬 센서	cevSensorAsa5508ChassisFanSensor(cevSensor 162)
Adaptive Security Appliance 5508(페이로드 암호화 없음)용 섀시 냉각 팬 센서	cevSensorAsa5508K7ChassisFanSensor(cevSensor 163)
5506 Adaptive Security Appliance용 CPU 온도 센서	cevSensorAsa5506CpuTempSensor(cevSensor 164)
5506W Adaptive Security Appliance용 CPU 온도 센서	cevSensorAsa5506WCpuTempSensor(cevSensor 165)
5508 Adaptive Security Appliance용 CPU 온도 센서	cevSensorAsa5508CpuTempSensor(cevSensor 166)
5506(페이로드 암호화 없음) Adaptive Security Appliance용 CPU 온도 센서	cevSensorAsa5506K7CpuTempSensor(cevSensor 167)
5508(페이로드 암호화 없음) Adaptive Security Appliance용 CPU 온도 센서	cevSensorAsa5508K7CpuTempSensor(cevSensor 168)
5506 Adaptive Security Appliance용 가속기 온도 센서	cevSensorAsa5506AcceleratorTempSensor(cevSensor 169)
5506W Adaptive Security Appliance용 가속기 온도 센서	cevSensorAsa5506WAcceleratorTempSensor(cevSensor 170)
5508 Adaptive Security Appliance용 가속기 온도 센서	cevSensorAsa5508AcceleratorTempSensor(cevSensor 171)
5506(페이로드 암호화 없음) Adaptive Security Appliance용 가속기 온도 센서	cevSensorAsa5506K7AcceleratorTempSensor(cevSensor 172)

항목	**entPhysicalVendorType OID** 설명
5508(페이로드 암호화 없음) Adaptive Security Appliance용 가속기 온도 센서	cevSensorAsa5508K7AcceleratorTempSensor(cevSensor 173)
5506 Adaptive Security Appliance용 섀시 주변 온도 센서	cevSensorAsa5506ChassisTempSensor(cevSensor 174)
5506W Adaptive Security Appliance용 섀시 주변 온도 센서	cevSensorAsa5506WChassisTempSensor(cevSensor 175)
5508 Adaptive Security Appliance용 섀시 주변 온도 센서	cevSensorAsa5508ChassisTempSensor(cevSensor 176)
5506(페이로드 암호화 없음) Adaptive Security Appliance용 섀시 주변 온도 센서	cevSensorAsa5506K7ChassisTempSensor(cevSensor 177)
5508(페이로드 암호화 없음) Adaptive Security Appliance용 섀시 주변 온도 센서	cevSensorAsa5508K7ChassisTempSensor(cevSensor 178)
Cisco ASA(Adaptive Security Appliance) 5512 Adaptive Security Appliance	cevChassisASA5512(cevChassis 1113)
Cisco ASA(Adaptive Security Appliance) 5512 Adaptive Security Appliance(페이로드 암호화 없음)	cevChassisASA5512K7(cevChassis 1108)
Cisco ASA(Adaptive Security Appliance) 5515 Adaptive Security Appliance	cevChassisASA5515(cevChassis 1114)
Cisco ASA(Adaptive Security Appliance) 5515 Adaptive Security Appliance(페이로드 암호화 없음)	cevChassisASA5515K7(cevChassis 1109)
Cisco ASA(Adaptive Security Appliance) 5525 Adaptive Security Appliance	cevChassisASA5525(cevChassis 1115)
Cisco ASA(Adaptive Security Appliance) 5525 Adaptive Security Appliance(페이로드 암호화 없음)	cevChassisASA5525K7(cevChassis 1110)
Cisco ASA(Adaptive Security Appliance) 5545 Adaptive Security Appliance	cevChassisASA5545(cevChassis 1116)
Cisco ASA(Adaptive Security Appliance) 5545 Adaptive Security Appliance(페이로드 암호화 없음)	cevChassisASA5545K7(cevChassis 1111)
Cisco ASA(Adaptive Security Appliance) 5555 Adaptive Security Appliance	cevChassisASA5555(cevChassis 1117)
Cisco ASA(Adaptive Security Appliance) 5555 Adaptive Security Appliance(페이로드 암호화 없음)	cevChassisASA5555K7(cevChassis 1112)
Cisco Adaptive Security Appliance 5512용 CPU	cevCpuAsa5512(cevModuleCpuType 229)
Cisco Adaptive Security Appliance 5512(페이로드 암호화 없음)용 CPU	cevCpuAsa5512K7(cevModuleCpuType 224)

항목	**entPhysicalVendorType OID** 설명
Cisco Adaptive Security Appliance 5515용 CPU	cevCpuAsa5515(cevModuleCpuType 230)
Cisco Adaptive Security Appliance 5515(페이로드 암호화 없음)용 CPU	cevCpuAsa5515K7(cevModuleCpuType 225)
Cisco Adaptive Security Appliance 5525용 CPU	cevCpuAsa5525(cevModuleCpuType 231)
Cisco Adaptive Security Appliance 5525(페이로드 암호화 없음)용 CPU	cevCpuAsa5525K7(cevModuleCpuType 226)
Cisco Adaptive Security Appliance 5545용 CPU	cevCpuAsa5545(cevModuleCpuType 232)
Cisco Adaptive Security Appliance 5545(페이로드 암호화 없음)용 CPU	cevCpuAsa5545K7(cevModuleCpuType 227)
Cisco Adaptive Security Appliance 5555용 CPU	cevCpuAsa5555(cevModuleCpuType 233)
Cisco Adaptive Security Appliance 5555(페이로드 암호화 없음)용 CPU	cevCpuAsa5555K7(cevModuleCpuType 228)
ASA 5585 SSP-10용 CPU	cevCpuAsa5585Ssp10(cevModuleCpuType 204)
ASA 5585 SSP-10(페이로드 암호화 없음)용 CPU	cevCpuAsa5585Ssp10K7(cevModuleCpuType 205)
ASA 5585 SSP-20용 CPU	cevCpuAsa5585Ssp20(cevModuleCpuType 206)
ASA 5585 SSP-20(페이로드 암호화 없음)용 CPU	cevCpuAsa5585Ssp20K7(cevModuleCpuType 207)
ASA 5585 SSP-40용 CPU	cevCpuAsa5585Ssp40(cevModuleCpuType 208)
ASA 5585 SSP-40(페이로드 암호화 없음)용 CPU	cevCpuAsa5585Ssp40K7(cevModuleCpuType 209)
ASA 5585 SSP-60용 CPU	cevCpuAsa5585Ssp60(cevModuleCpuType 210)
ASA 5585 SSP-60(페이로드 암호화 없음)용 CPU	cevCpuAsa5585Ssp60K(cevModuleCpuType 211)
Catalyst 스위치/7600 라우터용 Cisco ASA 서비스 모듈의 CPU	cevCpuAsaSm1(cevModuleCpuType 222)
Catalyst 스위치/7600 라우터용 Cisco ASA 서비스 모듈의 CPU(페이로드 암호화 없음)	cevCpuAsaSm1K7(cevModuleCpuType 223)
Adaptive Security Appliance 5512의 섀시 냉각 팬	cevFanASA5512ChassisFan(cevFan 163)
Adaptive Security Appliance 5512(페이로드 암호화 없음)의 섀시 냉각 팬	cevFanASA5512K7ChassisFan(cevFan 172)
Adaptive Security Appliance 5515의 섀시 냉각 팬	cevFanASA5515ChassisFan(cevFan 164)

항목	**entPhysicalVendorType OID** 설명
Adaptive Security Appliance 5515(페이로드 암호화 없음)의 섀시 냉각 팬	cevFanASA5515K7ChassisFan(cevFan 171)
Adaptive Security Appliance 5525의 섀시 냉각 팬	cevFanASA5525ChassisFan(cevFan 165)
Adaptive Security Appliance 5525(페이로드 암호화 없음)의 섀시 냉각 팬	cevFanASA5525K7ChassisFan(cevFan 170)
Adaptive Security Appliance 5545의 섀시 냉각 팬	cevFanASA5545ChassisFan(cevFan 166)
Adaptive Security Appliance 5545(페이로드 암호화 없음)의 섀시 냉각 팬	cevFanASA5545K7ChassisFan(cevFan 169)
Adaptive Security Appliance 5545(페이로드 암호화 없음)의 전원 공급 장치 팬	cevFanASA5545K7PSFan(cevFan 161)
Adapative Security Appliance 5545의 전원 공급 장치 팬	cevFanASA5545PSFan(cevFan 159)
Adaptive Security Appliance 5555의 섀시 냉각 팬	cevFanASA5555ChassisFan(cevFan 167)
Adaptive Security Appliance 5555(페이로드 암호화 없음)의 섀시 냉각 팬	cevFanASA5555K7ChassisFan(cevFan 168)
Adaptive Security Appliance 5555의 전원 공급 장치 팬	cevFanASA5555PSFan(cevFan 160)
Adaptive Security Appliance 5555(페이로드 암호화 없음)의 전원 공급 장치 팬	cevFanASA5555PSFanK7(cevFan 162)
ASA 5585-X용 전원 공급 장치 팬	cevFanASA5585PSFan(cevFan 146)
10기가비트 이더넷 인터페이스	cevPort10GigEthernet(cevPort 315)
기가비트 이더넷 포트	cevPortGe(cevPort 109)
Adaptive Security Appliance 5545의 전원 공급 장치	cevPowerSupplyASA5545PSInput(cevPowerSupply 323)
Adaptive Security Appliance 5545의 전원 공급 장치 입력용 감지 센서	cevPowerSupplyASA5545PSPresence(cevPowerSupply 321)
Adaptive Security Appliance 5555의 전원 공급 장치	cevPowerSupplyASA5555PSInput(cevPowerSupply 324)
Adaptive Security Appliance 5555의 전원 공급 장치 입력용 감지 센서	cevPowerSupplyASA5555PSPresence(cevPowerSupply 322)
ASA 5585용 전원 공급 장치 입력	cevPowerSupplyASA5585PSInput(cevPowerSupply 304)
Cisco ASA(Adaptive Security Appliance) 5512 섀시 팬 센서	cevSensorASA5512ChassisFanSensor(cevSensor 120)

항목	**entPhysicalVendorType OID** 설명
Cisco Adaptive Security Appliance 5512용 섀시 주변 온도 센서	cevSensorASA5512ChassisTemp(cevSensor 107)
Cisco Adaptive Security Appliance 5512용 CPU 주변 온도 센서	cevSensorASA5512CPUTemp(cevSensor 96)
Cisco ASA(Adaptive Security Appliance) 5512(페이로드 암호화 없음) 섀시 팬 센서	cevSensorASA5512K7ChassisFanSensor(cevSensor 125)
Cisco Adaptive Security Appliance 5512(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5512K7CPUTemp(cevSensor 102)
Adaptive Security Appliance 5512(페이로드 암호화 없음)의 섀시 냉각 팬용 센서	cevSensorASA5512K7PSFanSensor(cevSensor 116)
Adaptive Security Appliance 5512의 섀시 냉각 팬용 센서	cevSensorASA5512PSFanSensor(cevSensor 119)
Cisco ASA(Adaptive Security Appliance) 5515 섀시 팬 센서	cevSensorASA5515ChassisFanSensor(cevSensor 121)
Cisco Adaptive Security Appliance 5515용 섀시 주변 온도 센서	cevSensorASA5515ChassisTemp(cevSensor 98)
Cisco Adaptive Security Appliance 5515용 CPU 주변 온도 센서	cevSensorASA5515CPUTemp(cevSensor 97)
Cisco ASA(Adaptive Security Appliance) 5515(페이로드 암호화 없음) 섀시 팬 센서	cevSensorASA5515K7ChassisFanSensor(cevSensor 126)
Cisco Adaptive Security Appliance 5515(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5515K7CPUTemp(cevSensor 103)
Adaptive Security Appliance 5515(페이로드 암호화 없음)의 섀시 냉각 팬용 센서	cevSensorASA5515K7PSFanSensor(cevSensor 115)
Adaptive Security Appliance 5515의 섀시 냉각 팬용 센서	cevSensorASA5515PSFanSensor(cevSensor 118)
Cisco ASA(Adaptive Security Appliance) 5525 섀시 팬 센서	cevSensorASA5525ChassisFanSensor(cevSensor 122)
Cisco Adaptive Security Appliance 5525용 섀시 주변 온도 센서	cevSensorASA5525ChassisTemp(cevSensor 108)
Cisco Adaptive Security Appliance 5525용 CPU 주변 온도 센서	cevSensorASA5525CPUTemp(cevSensor 99)
Cisco ASA(Adaptive Security Appliance) 5525(페이로드 암호화 없음) 섀시 팬 센서	cevSensorASA5525K7ChassisFanSensor(cevSensor 127)

항목	**entPhysicalVendorType OID** 설명
Cisco Adaptive Security Appliance 5525(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5525K7CPUTemp(cevSensor 104)
Adaptive Security Appliance 5525(페이로드 암호화 없음)의 섀시 냉각 팬용 센서	cevSensorASA5525K7PSFanSensor(cevSensor 114)
Adaptive Security Appliance 5525의 섀시 냉각 팬용 센서	cevSensorASA5525PSFanSensor(cevSensor 117)
Cisco ASA(Adaptive Security Appliance) 5545 섀시 팬 센서	cevSensorASA5545ChassisFanSensor(cevSensor 123)
Cisco Adaptive Security Appliance 5545용 섀시 주변 온도 센서	cevSensorASA5545ChassisTemp(cevSensor 109)
Cisco Adaptive Security Appliance 5545용 CPU 주변 온도 센서	cevSensorASA5545CPUTemp(cevSensor 100)
Cisco ASA(Adaptive Security Appliance) 5545(페이로드 암호화 없음) 섀시 팬 센서	cevSensorASA5545K7ChassisFanSensor(cevSensor 128)
Cisco Adaptive Security Appliance 5545(페이로드 암호화 없음)용 섀시 주변 온도 센서	cevSensorASA5545K7ChassisTemp(cevSensor 90)
Cisco Adaptive Security Appliance 5545(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5545K7CPUTemp(cevSensor 105)
Adaptive Security Appliance 5545(페이로드 암호화 없음)의 섀시 냉각 팬용 센서	cevSensorASA5545K7PSFanSensor(cevSensor 113)
Adaptive Security Appliance 5545(페이로드 암호화 없음)의 전원 공급 장치 입력용 감지 센서	cevSensorASA5545K7PSPresence(cevSensor 87)
Adaptive Security Appliance 5545(페이로드 암호화 없음)의 전원 공급 장치 팬용 온도 센서	cevSensorASA5545K7PSTempSensor(cevSensor 94)
Adaptive Security Appliance 5545(페이로드 암호화 없음)의 전원 공급 장치 팬용 센서	cevSensorASA5545PSFanSensor(cevSensor 89)
Adaptive Security Appliance 5545의 전원 공급 장치 입력용 감지 센서	cevSensorASA5545PSPresence(cevSensor 130)
Adaptive Security Appliance 5555의 전원 공급 장치 입력용 감지 센서	cevSensorASA5545PSPresence(cevSensor 131)
Adaptive Security Appliance 5545의 전원 공급 장치 팬용 온도 센서	cevSensorASA5545PSTempSensor(cevSensor 92)
Cisco ASA(Adaptive Security Appliance) 5555 섀시 팬 센서	cevSensorASA5555ChassisFanSensor(cevSensor 124)

항목	**entPhysicalVendorType OID** 설명
Cisco Adaptive Security Appliance 5555용 섀시 주변 온도 센서	cevSensorASA5555ChassisTemp(cevSensor 110)
Cisco Adaptive Security Appliance 5555용 CPU 주변 온도 센서	cevSensorASA5555CPUTemp(cevSensor 101)
Cisco ASA(Adaptive Security Appliance) 5555(페이로드 암호화 없음) 섀시 팬 센서	cevSensorASA5555K7ChassisFanSensor(cevSensor 129)
Cisco Adaptive Security Appliance 5555(페이로드 암호화 없음)용 섀시 주변 온도 센서	cevSensorASA5555K7ChassisTemp(cevSensor 111)
Cisco Adaptive Security Appliance 5555(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5555K7CPUTemp(cevSensor 106)
Adaptive Security Appliance 5555(페이로드 암호화 없음)의 섀시 냉각 팬용 센서	cevSensorASA5555K7PSFanSensor(cevSensor 112)
Adaptive Security Appliance 5555(페이로드 암호화 없음)의 전원 공급 장치 입력용 감지 센서	cevSensorASA5555K7PSPresence(cevSensor 88)
Adaptive Security Appliance 5555(페이로드 암호화 없음)의 전원 공급 장치 팬용 온도 센서	cevSensorASA5555K7PSTempSensor(cevSensor 95)
Adaptive Security Appliance 5555의 전원 공급 장치 팬용 센서	cevSensorASA5555PSFanSensor(cevSensor 91)
Adaptive Security Appliance 5555의 전원 공급 장치 팬용 온도 센서	cevSensorASA5555PSTempSensor(cevSensor 93)
ASA 5585-X용 전원 공급 장치 팬용 센서	cevSensorASA5585PSFanSensor(cevSensor 86)
ASA 5585-X용 전원 공급 장치 입력용 센서	cevSensorASA5585PSInput(cevSensor 85)
ASA 5585 SSP-10용 CPU 온도 센서	cevSensorASA5585SSp10CPUTemp(cevSensor 77)
ASA 5585 SSP-10(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5585SSp10K7CPUTemp(cevSensor 78)
ASA 5585 SSP-20용 CPU 온도 센서	cevSensorASA5585SSp20CPUTemp(cevSensor 79)
ASA 5585 SSP-20(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5585SSp20K7CPUTemp(cevSensor 80)
ASA 5585 SSP-40용 CPU 온도 센서	cevSensorASA5585SSp40CPUTemp(cevSensor 81)
ASA 5585 SSP-40(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5585SSp40K7CPUTemp(cevSensor 82)
ASA 5585 SSP-60용 CPU 온도 센서	cevSensorASA5585SSp60CPUTemp(cevSensor 83)
ASA 5585 SSP-60(페이로드 암호화 없음)용 CPU 온도 센서	cevSensorASA5585SSp60K7CPUTemp(cevSensor 84)

항목	**entPhysicalVendorType OID** 설명
Adaptive Security Appliance 5555-X 현장 교체 SSD	cevModuleASA5555XFRSSD(cevModuleCommonCards 396)
Adaptive Security Appliance 5545-X 현장 교체 SSD	cevModuleASA5545XFRSSD(cevModuleCommonCards 397)
Adaptive Security Appliance 5525-X 현장 교체 SSD	cevModuleASA5525XFRSSD(cevModuleCommonCards 398)
Adaptive Security Appliance 5515-X 현장 교체 SSD	cevModuleASA5515XFRSSD(cevModuleCommonCards 399)
Adaptive Security Appliance 5512-X 현장 교체 SSD	cevModuleASA5512XFRSSD(cevModuleCommonCards 400)
Cisco Adaptive Security Virtual Appliance	cevChassisASAv(cevChassis 1451)

MIB에서 지원되는 테이블 및 객체

다음 표에서는 지정된 MIB에 대해 지원되는 테이블 및 객체를 소개합니다.

표 ***58: MIB***에서 지원되는 테이블 및 객체

MIB 이름	지원되는 테이블 및 객체
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid, cempMemPoolUsed, cempMemPoolFree, cempMemPoolUsedOvrflw, cempMemPoolHCUsed, cempMemPoolFreeOvrflw, cempMemPoolHCFree cempMemPoolPlatformMemory, cempMemPoolLargestFree, cempMemPoolLowestFree, cempMemPoolUsedLowWaterMark, cempMemPoolAllocHit, cempMemPoolAllocMiss, cempMemPoolFreeHit, cempMemPoolFreeMiss, cempMemPoolShared, cempMemPoolLargestFreeOvrflw, cempMemPoolHCLargestFree, cempMemPoolLowestFreeOvrflw, cempMemPoolHCLowestFree, cempMemPoolUsedLowWaterMarkOvrflw, cempMemPoolHCUsedLowWaterMark, cempMemPoolSharedOvrflw, cempMemPoolHCShared
CISCO-ENTITY-SENSOR-EXT-MIB 참고 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다.	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB 참고 Cisco Adaptive Security Virtual Appliance(ASAv)에서 지원되지 않습니다.	ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects

MIB 이름	지원되는 테이블 및 객체
DISMAN-EVENT-MIB	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB 참고 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다.	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB 참고 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다. 참고 섀시 온도, 팬 RPM, 전원 공급 장치 전압 등과 같은 물리적 센서와 관련된 정보를 제공합니다. Cisco ASAv 플랫폼에서는 지원되지 않습니다.	entPhySensorTable
NAT-MIB	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus
CISCO-PTP-MIB 참고 E2E 투명 클록 모드에 해당하는 MIB만 지원됩니다.	ciscoPtpMIBSystemInfo, cPtpClockDefaultDSTable, cPtpClockTransDefaultDSTable, cPtpClockPortTransDSTable

지원되는 트랩(알림)

다음 표에서는 지원되는 트랩(알림) 및 해당 MIB를 소개합니다.

표 ***59:*** 지원되는 트랩*(*알림*)*

트랩 및 **MIB** 이름	**Varbind** 목록	설명
authenticationFailure (SNMPv2-MIB)	—	SNMP 버전 1 또는 2의 경우 SNMP 요청에서 제공된 커뮤니티 문자열이 바르지 않습니다. SNMP Version 3의 경우 auth 또는 priv 비밀번호나 사용자 이름이 바르지 않은 경우 트랩 대신 보고서 PDU가 생성됩니다. **snmp-server enable traps snmp authentication** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	—	**snmp-server enable traps config** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	—	**snmp-server enable traps entity fru-insert** 명령은 이 알림을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	—	**snmp-server enable traps entity fru-remove** 명령은 이 알림을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB) 참고 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다.	ceSensorExtThresholdValue, entPhySensorValue, entPhySensorType, entPhysicalName	

트랩 및 **MIB** 이름	**Varbind** 목록	설명
		snmp-server enable traps entity [**power-supply-failure** | **fan-failure** | **cpu-temperature**] 명령은 엔티티 임계값 알림 전송을 활성화하는 데 사용됩니다. 이 알림은 전원 공급 장치 장애에 대해 전송됩니다. 전송된 객체는 팬과 CPU 온도를 파악합니다. **snmp-server enable traps entity fan-failure** 명령은 팬 장애 트랩 전송을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다. **snmp-server enable traps entity power-supply-failure** 명령은 전원 공급 장치 장애 트랩 전송을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다. **snmp-server enable traps entity chassis-fan-failure** 명령은 새시 팬 장애 트랩 전송을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다. **snmp-server enable traps entity cpu-temperature** 명령은 CPU 고온 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity power-supply-presence** 명령은 전원 공급 장치 감지 장애 트랩 전송을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다. **snmp-server enable traps entity power-supply-temperature** 명령은 전원 공급 장치 온도 임계값 트랩 전송을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다. **snmp-server enable traps entity chassis-temperature** 명령은 새시 주변 온도 트랩 전송을 활성화하는 데 사용됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
		snmp-server enable traps entity accelerator-temperature 명령은 섀시 가속기 온도 트랩 전송을 활성화하는 데 사용됩니다. 이 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다.
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	**snmp-server enable traps ipsec start** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	—	**snmp-server enable traps config** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions, crasNumUsers, crasMaxSessionsSupportable, crasMaxUsersSupportable, crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** 명령은 이 트랩 전송을 활성화하는 데 사용됩니다.
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp	Syslog 메시지가 생성됩니다. clogMaxSeverity 객체의 값은 어떤 syslog 메시지가 트랩으로 전송되는지 결정하는 데 사용됩니다. **snmp-server enable traps syslog** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	**snmp-server enable traps connection-limit-reached** 명령은 connection-limit-reached 알림 전송을 활성화하는 데 사용됩니다. clogOriginID 객체는 트랩이 시작하는 상황 이름을 포함합니다.
coldStart (SNMPv2-MIB)	—	SNMP 에이전트가 시작되었습니다. **snmp-server enable traps snmp coldstart** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** 명령은 CPU 임계값 상승 알림 전송을 활성화하는 데 사용됩니다. cpmCPURisingThresholdPeriod 객체가 다른 객체와 함께 전송됩니다.
entConfigChange (ENTITY-MIB)	—	**snmp-server enable traps entity config-change fru-insert fru-remove** 명령은 이 알림을 활성화하는 데 사용됩니다. 참고 이 알림은 보안 컨텍스트가 생성되거나 삭제될 때 멀티 모드로만 전송됩니다.
linkDown (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	인터페이스에 대한 linkdown 트랩. **snmp-server enable traps snmp linkdown** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
linkUp (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	인터페이스에 대한 linkup 트랩. **snmp-server enable traps snmp linkup** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** 명령은 메모리 임계값 알림을 활성화하는 데 사용됩니다. mteHotOID는 cempMemPoolHCUsed로 설정됩니다. cempMemPoolName 및 cempMemPoolHCUsed 객체는 다른 객체와 함께 전송됩니다.
mteTriggerFired (DISMAN-EVENT-MIB) 참고 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다.	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	**snmp-server enable traps interface-threshold** 명령은 인터페이스 임계값 알림을 활성화하는 데 사용됩니다. entPhysicalName 객체는 다른 객체와 함께 전송됩니다.

트랩 및 **MIB** 이름	**Varbind** 목록	설명
natPacketDiscard (NAT-MIB)	ifIndex	**snmp-server enable traps nat packet-discard** 명령은 NAT 패킷 폐기 알림을 활성화하는 데 사용됩니다. 이 알림은 5분으로 속도가 제한되어 있으며 매핑 공간이 제공되지 않으므로 NAT가 IP 패킷을 버릴 때 생성됩니다. ifIndex는 매핑된 인터페이스의 ID를 제공합니다.
warmStart (SNMPv2-MIB)	—	**snmp-server enable traps snmp warmstart** 명령은 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.

인터페이스 유형 및 예

SNMP 트래픽 통계를 생산하는 인터페이스 유형은 다음을 포함합니다.

- 논리—소프트웨어 드라이버가 수집한 통계로 물리적 통계의 하위 집합.
- 물리—하드웨어 드라이버가 수집한 통계. 각 물리적 이름 지정 인터페이스에는 논리적 통계와 물리적 통계 집합이 연결되어 있습니다. 각 물리적 인터페이스에는 연결된 VLAN 인터페이스가 두 개 이상 있습니다. VLAN 인터페이스에는 논리적 통계만 있습니다.

  참고 여러 VLAN 인터페이스가 연결된 물리적 인터페이스의 경우 ifInOctets 및 ifOutoctets OID에 대한 SNMP 카운터가 해당 물리적 인터페이스의 종합 트래픽 카운터와 일치하도록 주의하십시오.

- VLAN 전용—SNMP는 ifInOctets 및 ifOutOctets에 대해 논리적 통계를 사용합니다.

다음 표의 예에서는 SNMP 트래픽 통계의 차이점을 보여줍니다. 예 1은 **showinterface** 명령과 **show traffic** 명령에 대한 물리적 및 논리적 출력 통계의 차이를 보여 줍니다. 예 2는 **show interface** 명령과 **show traffic** 명령에 대한 VLAN 전용 인터페이스에 대한 출력 통계를 보여 줍니다. 예는 통계가 **show traffic** 명령에 대한 출력과 비슷함을 보여 줍니다.

표 *60:* 물리 및 ***VLAN*** 인터페이스에 대한 ***SNMP*** 트래픽 통계

예 **1**	예 **2**
ciscoasa# **show interface GigabitEthernet3/2** interface GigabitEthernet3/2 description fullt-mgmt nameif mgmt security-level 10 ip address 10.7.14.201 255.255.255.0 management-only ciscoasa# **show traffic** (Condensed output) Physical Statistics GigabitEthernet3/2: received (in 121.760 secs) **36 packets 3428 bytes** 0 pkts/sec 28 bytes/sec Logical Statistics mgmt: received (in 117.780 secs) **36 packets 2780 bytes** 0 pkts/sec 23 bytes/sec 다음 예는 관리 인터페이스 및 물리 인터페이스에 대한 SNMP 출력 통계를 보여줍니다. ifInOctets 값은 **show traffic** 명령 출력에 나타나는 물리적 통계와 비슷하지만 논리적 통계 출력과는 다릅니다. ifIndex of the mgmt interface: IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface 물리적 인터페이스 통계에 대응하는 ifInOctets: **IF-MIB::ifInOctets.6 = Counter32:3246**	ciscoasa# **show interface GigabitEthernet0/0.100** interface GigabitEthernet0/0.100 vlan 100 nameif inside security-level 100 ip address 10.7.1.101 255.255.255.0 standby 10.7.1.102 ciscoasa# **show traffic** inside received (in 9921.450 secs) **1977 packets 126528 bytes** 0 pkts/sec 12 bytes/sec transmitted (in 9921.450 secs) **1978 packets 126556 bytes** 0 pkts/sec 12 bytes/sec ifIndex of VLAN inside: IF-MIB::ifDescr.9 = Adaptive Security Appliance 'inside' interface **IF-MIB::ifInOctets.9 = Counter32: 126318**

SNMP Version 3 개요

SNMP Version 3에서는 SNMP Version 1 또는 Version 2c에 없는 향상된 보안을 제공합니다. SNMP 버전 1 및 2c는 일반 텍스트로 SNMP 서버와 SNMP 에이전트 간에 데이터를 전송합니다. SNMP 버전 3은 프로토콜 작동을 보호하기 위한 인증 및 프라이버시 옵션을 추가합니다. 또한 이 버전은 USM(사용자 기반 보안 모델) 및 VACM(보기 기반 제어 모델)을 통해 SNMP 에이전트와 MIB 객체에 대한 액세스를 제어합니다. ASA 및 ASASM 또한 SNMP 그룹 및 사용자는 물론 호스트 생성을 지원하며 이는 안전한 SNMP 통신을 위한 전송 인증 및 암호화 활성화를 위해 필요합니다.

보안 모델

구성을 위해 인증 및 프라이버시 옵션은 보안 모델로 그룹화됩니다. 보안 모델은 사용자와 그룹에 적용되며 다음 3개 유형으로 나누어집니다.

- NoAuthPriv—No Authentication and No Privacy(인증 없음 및 개인정보 보호 없음)로 메시지에 보안이 적용되지 않음을 의미합니다.
- AuthNoPriv—Authentication but No Privacy(인증 있음 및 개인정보 보호 없음)로 메시지가 인증을 받음을 의미합니다.
- AuthPriv—Authentication and Privacy(인증 있음 및 개인정보 보호 있음)로 메시지가 인증을 받고 암호화됨을 의미합니다.

SNMP 그룹

SNMP 그룹은 사용자를 추가할 수 있는 액세스 제어 정책입니다. 각 SNMP 그룹은 보안 모델로 구성되며 SNMP 보기와 연결됩니다. SNMP 그룹 내의 사용자는 SNMP 그룹의 보안 모델과 일치해야 합니다. 이러한 파라미터는 SNMP 그룹 내 사용자가 이용하는 인증 및 프라이버시 유형을 지정합니다. 각 SNMP 그룹 이름 및 보안 모델 쌍은 고유해야 합니다.

SNMP 사용자

SNMP 사용자는 지정된 사용자 이름, 사용자가 속하는 그룹, 인증 비밀번호, 암호화 비밀번호 및 승인, 그리고 사용할 암호화 알고리즘을 가져야 합니다. 인증 알고리즘 옵션은 MD5와 SHA입니다. 암호화 알고리즘 옵션은 DES, 3DES 및 AES(128, 192 및 256 버전으로 이용 가능)입니다. 사용자를 생성할 때 반드시 SNMP 그룹과 연결해야 합니다. 그러면 사용자에게 그룹의 보안 모델이 상속됩니다.

SNMP 호스트

SNMP 호스트는 SNMP 알림 및 트랩이 전송되는 IP 주소입니다. 트랩은 구성된 사용자에게만 전송되기 때문에 SNMP 버전 3 호스트를 대상 IP 주소와 함께 구성하려면 사용자 이름을 구성해야 합니다. SNMP 대상 IP 주소 및 대상 파라미터 이름은 ASA 및 ASA 서비스 모듈에서 고유해야 합니다. 각 SNMP 호스트는 연결된 하나의 사용자 이름만 가질 수 있습니다. SNMP 트랩을 수신하려면 **snmp-server host** 명령을 추가한 후,ASA 및 ASASM에 대한 크리덴셜과 일치하도록 NMS의 사용자 크리덴셜을 구성해야 합니다.

ASA, ASA 서비스 모듈 및 Cisco IOS Software의 구현 차이점

ASA 및 ASASM에서 SNMP 버전 3 구현은 Cisco IOS 소프트웨어에서의 SNMP 버전 3 구현과 다음과 같은 차이가 있습니다.

- 로컬 엔진 및 원격 엔진 ID를 구성할 수 없습니다. 로컬 엔진 ID는 ASA 또는 ASASM이 시작할 때 또는 상황이 생성될 때 생성됩니다.
- 무제한 MIB 찾아보기를 야기하는 보기 기반 액세스 제어는 지원되지 않습니다.
- 지원은 다음 MIB로 제한됩니다. USM, VACM, FRAMEWORK 및 TARGET
- 정확한 보안 모델로 사용자 및 그룹을 생성해야 합니다.

- 사용자, 그룹 및 호스트를 올바른 순서로 제거해야 합니다.
- snmp-server host 명령을 사용하면 SNMP 트래픽 허용을 위한 ASA, ASAv 또는 ASASM 규칙이 생성됩니다.

SNMP Syslog 메시징

SNMP는 212*nnn* 형식으로 번호가 매겨지는 상세한 syslog 메시지를 생성합니다. Syslog 메시지는 ASA 또는 ASASM에서 특정 인터페이스의 지정된 호스트로 SNMP 요청, SNMP 트랩, SNMP 채널 및 SNMP 응답의 상태를 알려 줍니다.

syslog 메시지에 대한 자세한 설명은 syslog 메시지 가이드를 참고하십시오.

참고 SNMP syslog 메시지가 높은 속도(초당 약 4000)를 초과하면 SNMP 폴링이 실패합니다.

애플리케이션 서비스 및 서드파티 툴

SNMP 지원에 대한 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP Version 3 MIB를 위한 서드파티 툴 사용에 대한 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP를 위한 지침

이 섹션에는 SNMP를 구성하기 전에 검토해야 할 지침 및 제한사항이 포함되어 있습니다.

장애 조치 지침

각 ASA, ASAv 또는 ASASM의 SNMP 클라이언트는 피어와 엔진 데이터를 공유합니다. 엔진 데이터는 SNMP-FRAMEWORK-MIB의 engineID, engineBoots 및 engineTime 객체를 포함합니다. 엔진 데이터는 flash:/snmp/*contextname*에 바이너리 파일로 저장됩니다.

IPv6 지침

IPv6 호스트가 IPv6 소프트웨어를 실행하는 디바이스에서 SNMP 쿼리를 수행하고 SNMP 알림을 수신할 수 있도록 IPv6 전송을 통해 SNMP를 구성할 수 있습니다. SNMP 에이전트 및 관련된 MIB는 IPv6 주소 지정을 지원하도록 기능이 향상되었습니다.

참고 **snmp-server host-group**이라는 네트워크 개체를 사용자 목록의 단일 사용자 또는 사용자 그룹과 연결하기 위한 명령은 IPv6를 지원하지 않습니다.

추가 지침

- Windows용 Cisco Works 또는 다른 SNMP MIB-II 규격 브라우저가 있어야 SNMP 트랩을 수신하거나 MIB를 찾아볼 수 있습니다.
- 보기 기반 액세스 제어를 지원하지 않지만 VACM MIB를 이용한 찾아보기로 기본 보기 설정을 결정할 수 있습니다.
- ENTITY-MIB는 관리 이외 상황에서 이용할 수 없습니다. 관리 이외 상황에서는 IF-MIB를 대신 사용하십시오.
- ENTITY-MIB는 Firepower 9300에서 사용할 수 없습니다. 대신 CISCO-FIREPOWER-EQUIPMENT-MIB 및 CISCO-FIREPOWER-SM-MIB를 사용하십시오.
- AIP SSM 또는 AIP SSC를 위한 SNMP 버전 3을 지원하지 않습니다.
- SNMP 디버깅을 지원하지 않습니다.
- ARP 정보 검색을 지원하지 않습니다.
- SNMP SET 명령을 지원하지 않습니다.
- NET-SNMP 버전 5.4.2.1을 사용할 때는 AES128 버전의 암호화 알고리즘만 지원합니다. AES256 또는 AES192의 암호화 알고리즘 버전은 지원하지 않습니다.
- 기존 구성을 변경했을 때 SNMP 기능이 일관성을 잃게 되면 변경이 거부됩니다.
- SNMP 버전 3의 경우 그룹, 사용자, 호스트 순서로 구성이 이루어져야 합니다.
- 그룹을 삭제하기 전에 해당 그룹에 연결된 모든 사용자가 삭제되었는지 확인해야 합니다.
- 사용자를 삭제하기 전에 해당 사용자 이름과 연결된 호스트가 구성되지 않았는지 확인해야 합니다.
- 사용자가 특정 보안 모델 내에서 특정 그룹에 속하도록 구성되어 있고 해당 그룹의 보안 수준이 변경되는 경우 다음을 순서대로 수행해야 합니다.
  - 해당 그룹에서 사용자를 제거합니다.
  - 그룹 보안 수준을 변경합니다.
  - 새 그룹에 속한 사용자를 추가합니다.
- MIB 객체 하위 집합에 대한 사용자 액세스를 제한하기 위한 맞춤 보기 생성은 지원되지 않습니다.
- 모든 요청 및 트랩은 기본 읽기/알림 보기에서만 이용 가능합니다.
- connection-limit-reached 트랩은 관리 상황에서 생성됩니다. 이 트랩을 생성하려면 연결 제한에 도달한 사용자 상황에서 SNMP 서버 호스트가 1개 이상 구성되어 있어야 합니다.
- ASA 5585 SSP-40(NPE)의 섀시 온도를 쿼리할 수 없습니다.
- 최대 4000개의 호스트를 추가할 수 있습니다. 하지만 이 중 128개만 트랩에 사용할 수 있습니다.

- 지원되는 액티브 폴링 대상의 총수는 128개입니다.
- 호스트 그룹으로 추가할 개별 호스트를 나타내는 네트워크 객체를 지정할 수 있습니다.
- 둘 이상의 사용자를 하나의 호스트와 연결할 수 있습니다.
- 다른 **host-group** 명령에서 겹치는 네트워크 객체를 지정할 수 있습니다. 마지막 호스트 그룹에 대해 지정하는 값은 다른 네트워크 객체의 호스트 공통 집합에서 적용됩니다.
- 다른 호스트 그룹과 겹치는 호스트 그룹 또는 호스트를 삭제할 경우 호스트는 구성된 호스트 그룹에서 지정된 값으로 다시 설정됩니다.
- 호스트가 획득하는 값은 명령 실행에 사용하는 지정된 순서에 따라 다릅니다.
- SNMP가 보내는 메시지 크기의 한도는 1472바이트입니다.
- 클러스터 구성원은 SNMPv3 엔진 ID를 동기화하지 않습니다. 따라서 클러스터의 각 유닛은 고유한 SNMPv3 사용자 구성을 가져야 합니다.
- 9.4(1) 버전에서 ASA는 상황당 무제한 SNMP 서버 트랩 호스트를 지원합니다. **show snmp-server host** 명령 출력에는 정적으로 구성한 호스트와 함께 ASA를 폴링 중인 활성 호스트만 표시됩니다.

문제 해결 정보

- NMS로부터의 수신 패킷을 수신하는 SNMP 프로세스가 실행되도록 하려면 다음 명령을 입력하십시오.

```
ciscoasa(config)# show process | grep snmp
```

- SNMP에서 syslog 메시지를 캡처하고 ASA, ASAv 또는 ASASM 콘솔에 표시하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- SNMP 프로세스가 패킷을 송수신하도록 하려면 다음 명령을 입력하십시오.

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  출력은 SNMPv2-MIB의 SNMP 그룹을 기준으로 합니다.

- SNMP 패킷이 확실히 ASA, ASAv 또는 ASASM을 통과하고 SNMP 프로세스를 거치도록 하려면 다음 명령을 입력하십시오.

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- NMS가 성공적으로 객체를 요청할 수 없거나 ASA, ASAv 또는 ASASM에서 수신 트랩을 바르게 처리하지 못하는 경우다음 명령을 입력함으로써 패킷 캡처를 사용하여 문제를 격리하십시오.

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- ASA, ASAv 또는 ASASM이 예상대로 작동하지 않으면 다음을 수행함으로써 네트워크 토폴로지 및 트래픽에 대한 정보를 확보하십시오.
  - NMS 구성의 경우 다음 정보를 확보합니다.

    시간 초과 횟수

    재시도 횟수

    엔진 ID 캐싱

    사용된 사용자 이름 및 비밀번호
  - 다음 명령을 수행:

    show block

    show interface

    show process

    show cpu

    show vm

- 치명적인 오류가 발생하는 경우 오류 재현에 도움이 되도록 역추적 파일과 **show tech-support** 명령 출력을 Cisco TAC로 보내십시오.
- SNMP 트래픽이 ASA, ASAv 또는 ASASM 인터페이스를 지날 수 없을 경우 **icmp permit** 명령을 사용하여 원격 SNMP 서버의 ICMP 트래픽도 허용해야 합니다.
- 추가적인 문제 해결 정보에 대해서는 다음 URL을 참조하십시오.
  http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

SNMP 구성

이 섹션에서는 SNMP 구성 방법을 설명합니다.

프로시저

단계 **1** SNMP 에이전트 및 SNMP 서버를 활성화합니다.

단계 **2** SNMP 트랩을 구성합니다.

단계 **3** SNMP 버전 1 및 2c 파라미터 또는 SNMP 버전 3 파라미터를 구성합니다.

SNMP 에이전트 및 SNMP 서버 활성화

SNMP 에이전트 및 SNMP 서버를 활성화하려면 다음 단계를 수행합니다.

프로시저

ASA, ASAv 또는 ASASM에서 SNMP 에이전트 및 SNMP 서버를 활성화합니다. SNMP 서버는 기본적으로 활성화되어 있습니다.

snmp-server enable

예제**:**

```
ciscoasa(config)# snmp-server enable
```

SNMP 트랩 구성

SNMP 에이전트가 생성하는 트랩 및 이를 수집하여 NMS로 전송하는 방법을 지정하려면 다음 단계를 수행합니다.

프로시저

개별 트랩, 트랩 집합 또는 모든 트랩을 NMS로 보냅니다.

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | *linkdown* | *coldstart* | *warmstart*] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan- failure** | **power-supply-failure**] | *chassis-temperature* | *power-supply-presence* | *power-supply-temperature* | *accelerator-temperature* | *l1-bypass-status*] | **ikev2** [*start* | *stop*] | **ipsec** [*start* | *stop*] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [*packet-discard*]

예제**:**

```
ciscoasa(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

이 명령을 통해 syslog 메시지를 트랩으로서 NMS에 보낼 수 있습니다. 기본 구성에는 예에서와 같이 모든 SNMP 표준 트랩이 활성화되어 있습니다. 이 트랩을 비활성화하려면 **no snmp-server enable traps snmp** 명령을 사용합니다. 이 명령을 입력하고 트랩 유형을 지정하지 않으면 기본값은 **syslog** 트랩입니다. 기본적으로 **syslog** 트랩이 활성화됩니다. 기본 SNMP 트랩이 **syslog** 트랩과 함께 활성화를 유지합니다. **logging history** 명령과 **snmp-server enable traps syslog** 명령을 모두 구성하여 syslog MIB

로부터 트랩을 생성해야 합니다. SNMP 트랩의 기본 활성화를 복원하려면 **clear configure snmp-server** 명령을 사용하십시오. 모든 다른 트랩은 기본적으로 비활성화되어 있습니다.

관리 상황에서만 이용 가능한 트랩:

- **connection-limit-reached**
- **entity**
- **memory-threshold**

시스템 상황에서 물리적으로 연결된 인터페이스에 대해서만 관리 상황을 통해 생성되는 트랩:

- **interface-threshold**

참고 **interface-threshold** 트랩은 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다.

모든 다른 트랩은 단일 모드의 관리자 및 사용자 상황에서 이용 가능합니다.

다중 상황 모드에서 **fan-failure** 트랩, **power-supply-failure** 트랩 및 **cpu-temperature** 트랩은 사용자 상황이 아닌 관리자 상황에서만 생성됩니다(ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에만 적용).

accelerator-temperature 임계값 트랩은 ASA 5506-X 및 ASA 5508-X에만 적용됩니다.

chassis-fan-failure 트랩은 ASA 5506-X에 적용되지 않습니다.

config 트랩은 구성 모드를 종료한 후에 생성되는 ciscoConfigManEvent 알림 및 ccmCLIRunningConfigChanged 알림을 활성화합니다.

다음 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다. **fan-failure**, **fru-insert**, **fru-remove**, **power-supply**, **power-supply-failure**, **power-supply-presence**, **power-supply-temperature**.

CPU 사용량이 구성된 모니터링 기간에 대한 구성된 임계값보다 큰 경우 **cpu threshold rising** 트랩이 생성됩니다.

사용된 시스템 상황 메모리가 전체 시스템 메모리의 80%에 도달하면 관리자 상황에서 **memory-threshold** 트랩이 생성됩니다. 다른 사용자 컨텍스트의 경우 이 트랩은 특정 컨텍스트에서 사용된 메모리가 전체 시스템 메모리의 80%에 도달할 때 생성됩니다.

참고 SNMP에서는 전압 센서를 모니터링하지 않습니다.

CPU 사용량 임계값 구성

CPU 사용량 임계값을 구성하려면 다음 단계를 수행합니다.

프로시저

높음 CPU 임계값과 임계값 모니터링 지속 시간에 대한 임계값을 구성합니다.

snmp cpu threshold rising *threshold_value monitoring_period*

예제:

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

CPU 사용률의 임계값 및 모니터링 기간을 지우려면 이 명령의 **no** 형식을 사용합니다. **snmp cpu threshold rising** 명령이 구성되지 않은 경우 높음 임계값의 기본값은 70% 이상이고 심각 임계값의 기본값은 95% 이상입니다. 기본 모니터링 지속 시간은 1분으로 설정됩니다.

항상 95%로 유지되는 위험 CPU 임계값 수준은 구성할 수 없습니다. 높음 CPU 임계값의 유효한 범위는 10~94%입니다. 모니터링 기간에 대한 유효한 값은 1~60분입니다.

물리적 인터페이스 임계값 구성

물리적 인터페이스 임계값을 구성하려면 다음 단계를 수행합니다.

프로시저

SNMP 물리적 인터페이스에 대한 임계값을 구성합니다.

snmp interface threshold *threshold_value*

예제:

```
ciscoasa(config)# snmp interface threshold 75%
```

SNMP 물리적 인터페이스에 대한 임계값을 지우려면 이 명령의 **no** 형식을 사용합니다. 임계값은 인터페이스 대역폭 사용량의 백분율로 정의됩니다. 유효한 임계값 범위는 30~99%입니다. 기본값은 70%입니다.

snmp interface threshold 명령은 관리 상황에서만 사용할 수 있습니다.

물리적 인터페이스 사용량은 단일 모드 및 다중 모드에서 모니터링되고 시스템 컨텍스트의 물리적 인터페이스에 대한 트랩은 관리 컨텍스트를 통해 전송됩니다. 임계값 사용량 계산에는 물리적 인터페이스만 사용됩니다.

참고 이 명령은 Catalyst 6500 스위치/7600 라우터용 ASA 서비스 모듈에서는 지원되지 않습니다.

SNMP 버전 1 또는 2c에 대한 매개변수 구성

SNMP 버전 1 또는 2c에 대한 파라미터를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 1 SNMP 알림 수신자를 지정하고 트랩이 전송되는 인터페이스를 표기하며 ASA에 연결 가능한 NMS 또는 SNMP 관리자의 이름과 IP 주소를 식별합니다.

snmp-server host{*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

예제:

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

trap 키워드는 NMS를 트랩 수신으로만 제한합니다. **poll** 키워드는 NMS를 요청 전송(폴링)으로만 제한합니다. 기본적으로 SNMP 트랩은 활성화되어 있습니다. 기본적으로, UDP 포트는 162입니다. 커뮤니티 문자열은 ASA, ASAv 또는 ASASM과 NMS 사이의 공유 비밀 키입니다. 키는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본 커뮤니티 문자열은 공개됩니다. ASA는 이 키를 사용하여 수신 SNMP 요청의 유효성을 판단합니다. 예를 들어, 커뮤니티 문자열로 사이트를 지정한 후 같은 문자열로 ASA 및 관리 스테이션을 구성할 수 있습니다. ASA, ASAv 및 ASASM은 지정된 문자열을 사용하여 커뮤니티 문자열이 바르지 않은 요청에는 응답하지 않습니다. 암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템(예: CLI, ASDM, CSM 등)에 표시됩니다. 일반 텍스트 비밀번호는 표시되지 않습니다. 암호화된 커뮤니티 문자열은 항상 ASA에서 생성됩니다. 대개 입력 형식은 일반 텍스트 형식입니다.

참고 버전 8.3(1)에서 하위 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우에는 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 변환한 다음 결과를 저장해야 합니다.

snmp-server host 명령을 추가한 후 트랩을 수신하려면 ASA, ASAv 및 ASASM에 구성된 크리덴셜과 같은 크리덴셜로 NMS의 사용자를 구성해야 합니다.

단계 2 SNMP 버전 1 또는 2c에 한해 사용할 커뮤니티 문자열을 설정합니다.

snmp-server community *community-string*

예제:

```
ciscoasa(config)# snmp-server community onceuponatime
```

단계 3 SNMP 서버 위치 또는 연락처 정보를 설정합니다.

snmp-server [**contact** | **location**] *text*

예제:

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 인수는 연락 담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며, 최대 127자까지 허용됩니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

단계 **4** SNMP 요청에 대한 듣기 포트를 설정합니다.

snmp-server listen-port *lport*

예제**:**

```
ciscoasa(config)# snmp-server lport 192
```

lport 인수는 수신 요청이 수락되는 포트입니다. 기본 수신 포트는 161입니다. **snmp-server listen-port** 명령은 관리자 상황에서만 사용 가능하며 시스템 상황에서는 사용할 수 없습니다. 현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성한 경우 다음 메시지가 표시됩니다.

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

기존 SNMP 스레드는 포트를 사용할 수 있을 때까지 60초마다 계속 폴링하며, 포트를 여전히 사용 중인 경우 syslog 메시지 %ASA-1-212001을 발행합니다.

SNMP Version 3에 대한 매개변수 구성

SNMP 버전 3에 대한 파라미터를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 새로운 SNMP 버전 3에 한하여 사용할 수 있는 새 SNMP 그룹을 지정합니다.

snmp-server group *group-name***v3** [**auth** | **noauth** | **priv**]

예제**:**

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

커뮤니티 문자열이 구성될 때 커뮤니티 문자열과 일치하는 이름의 추가 그룹 2개가 자동으로 생성됩니다. 하나는 버전 1 보안 모델을 위한 것이고 다른 하나는 버전 2 보안 모델을 위한 것입니다. **auth** 키워드는 패킷 인증을 활성화합니다. **noauth** 키워드는 패킷 인증 또는 암호화가 사용되지 않음을 의미합니다. **priv** 키워드는 패킷 암호화와 인증을 활성화합니다. **auth** 또는 **priv** 키워드에 대한 기본값은 존재하지 않습니다.

단계 **2** SNMP 버전 3에서만 사용할 SNMP 그룹을 위한 새 사용자를 구성합니다.

snmp-server user*username group-name* {**v3** [**engineID** *engineID*] [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv**] [**des** | **3des** | **aes**] [**128** | **192**| **256**] *priv-password*

예제:

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 인수는 SNMP 에이전트에 속하는 호스트의 사용자 이름입니다. group-name 인수는 사용자가 속하는 그룹의 이름입니다. **v3** 키워드는 SNMP 버전 3 보안 모델을 사용해야 함을 지정하고 **encrypted**, **priv** 및 **auth** 키워드의 사용을 활성화합니다. **engineID** 키워드는 선택 사항이며 사용자의 인증 및 암호화 정보를 현지화하는 데 사용된 ASA의 engineID를 지정합니다. EngineID 인수는 유효한 ASA engineID를 지정해야 합니다. **encrypted** 키워드는 암호화된 형식으로 비밀번호를 지정합니다. 암호화된 비밀번호는 16진수 형식이어야 합니다. **auth** 키워드는 사용할 인증 레벨(**md5** 또는 **sha**)을 지정합니다. **priv** 키워드는 암호화 레벨을 지정합니다. **auth** 또는 **priv** 키워드에 대한 기본값 또는 기본 비밀번호가 존재하지 않습니다. 암호화 알고리즘의 경우 **des**, **3des** 또는 **aes** 키워드를 지정할 수 있습니다. 또한 **128**, **192** 또는 **256** 중에서 사용할 AES 암호화 알고리즘 버전을 지정할 수 있습니다. auth-password 인수는 인증 사용자 비밀번호를 지정합니다. priv-password 인수는 암호화 사용자 비밀번호를 지정합니다.

참고 비밀번호를 잊어버린 경우 복구할 수 없으며 사용자를 다시 구성해야 합니다. 일반 텍스트 비밀번호 또는 현지화된 다이제스트를 지정할 수 있습니다. 현지화된 다이제스트는 MD5 또는 SHA 중 사용자에 대해 선택된 인증 알고리즘과 일치해야 합니다. 사용자 구성이 콘솔에 표시되거나 파일에 작성된 경우(예를 들어 startup-configuration 파일) 일반 텍스트 비밀번호 대신 항상 현지화된 인증 및 프라이버시 다이제스트가 표시됩니다(두 번째 예시 참고). 비밀번호 최소 길이는 영숫자 1자이나 보안을 위해 8자 이상으로 사용하는 것이 좋습니다.

클러스터링에서는 SNMPv3 사용자로 클러스터링된 각 ASA를 수동으로 업데이트해야 합니다. **snmp-server user** *username group-name* **v3** 명령을 마스터 유닛에 현지화되지 않은 형태의 *priv-password* 옵션 및 *auth-password* 옵션과 함께 입력하면 됩니다.

클러스터링 복제 또는 구성 중에는 SNMPv3 사용자 명령이 복제되지 않음을 알리는 오류 메시지가 표시됩니다. 그런 다음 슬레이브 ASA에서 독립적으로 SNMPv3 사용자 및 그룹 명령을 구성할 수 있습니다. 이는 복제 중에 기존 SNMPv3 사용자 및 그룹이 지워지지 않으며, 클러스터의 모든 슬레이브에서 SNMPv3 사용자 및 그룹 명령을 입력할 수 있음도 의미합니다. 예를 들면 다음과 같습니다.

이미 현지화된 키와 함께 입력된 명령을 사용하는 마스터 장의 경우

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

클러스터 복제 중인 슬레이브 디바이스의 경우(**snmp-server user** 명령이 구성에 있는 경우에만 표시됨)

```
ciscoasa(cfg-cluster)#
```

```
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

단계 **3** SNMP 알림 수신자를 지정하십시오. 트랩이 전송된 인터페이스를 지정합니다. ASA에 연결할 수 있는 NMS 또는 SNMP 관리자의 이름과 IP 주소를 식별합니다.

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

예제**:**

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

trap 키워드는 NMS를 트랩 수신으로만 제한합니다. **poll** 키워드는 NMS를 요청 전송(폴링)으로만 제한합니다. 기본적으로 SNMP 트랩은 활성화되어 있습니다. 기본적으로, UDP 포트는 162입니다. 커뮤니티 문자열은 ASA 및 NMS 사이의 공유 비밀 키입니다. 키는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본 커뮤니티 문자열은 public입니다. ASA, ASAv 및 ASASM은 이 키를 사용하여 수신 SNMP 요청이 유효한지 확인합니다. 예를 들어, 커뮤니티 문자열로 사이트를 지정한 후 같은 문자열로 ASA, ASAv 또는 ASASM 및 NMS를 구성할 수 있습니다. ASA, ASAv 및 ASASM은 지정된 문자열을 사용하여 커뮤니티 문자열이 바르지 않은 요청에는 응답하지 않습니다. 암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템(예: CLI, ASDM, CSM 등)에 표시됩니다. 일반 텍스트 비밀번호는 표시되지 않습니다. 암호화된 커뮤니티 문자열은 항상 ASA에서 생성됩니다. 대개 입력 형식은 일반 텍스트 형식입니다.

참고 버전 8.3(1)에서 하위 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우에는 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 변환한 다음 결과를 저장해야 합니다.

version 키워드는 SNMP 트랩 버전을 지정합니다. ASA에서는 SNMP 요청(폴링)을 기반으로 하는 필터링을 지원하지 않습니다.

SNMP 버전 3 호스트가 ASA, ASAv 및 ASASM에 구성된 경우 사용자가 해당 호스트와 연결되어야 합니다.

snmp-server host 명령을 추가한 후 트랩을 수신하려면 ASA, ASAv 또는 ASASM에 구성된 크리덴셜과 같은 크리덴셜로 NMS의 사용자를 구성해야 합니다.

단계 **4** SNMP 서버 위치 또는 연락처 정보를 설정합니다.

snmp-server [**contact** | **location**] *text*

예제**:**

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 인수는 연락 담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며, 최대 127자까지 허용됩니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

단계 **5** SNMP 요청에 대한 듣기 포트를 설정합니다.

snmp-server listen-port *lport*

예제**:**

```
ciscoasa(config)# snmp-server lport 192
```

lport 인수는 수신 요청이 수락되는 포트입니다. 기본 수신 포트는 161입니다. **snmp-server listen-port** 명령은 관리자 상황에서만 사용 가능하며 시스템 상황에서는 사용할 수 없습니다. 현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성한 경우 다음 메시지가 표시됩니다.

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

기존 SNMP 스레드는 포트를 사용할 수 있을 때까지 60초마다 계속 폴링하며, 포트를 여전히 사용 중인 경우 syslog 메시지 %ASA-1-212001을 발행합니다.

사용자 그룹 구성

지정된 사용자 그룹을 포함한 SNMP 사용자 목록을 구성하려면 다음 단계를 수행합니다.

프로시저

SNMP 사용자 목록을 구성합니다.

snmp-server user-list *list_name* **username** *user_name*

예제**:**

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 인수는 최대 33자 길이의 사용자 목록 이름을 지정합니다. **username** *user_name* 키워드-인수 쌍은 사용자 목록에 구성될 수 있는 사용자를 지정합니다. SNMP 버전 3을 사용하는 경우에만 이용 가능한 **snmp-server user** *username* 명령으로 사용자 목록에서 사용자를 구성할 수 있습니다. 사용자 목록은 둘 이상의 사용자가 있어야 하며, 호스트 이름 또는 IP 주소 범위와 연결될 수 있습니다.

사용자와 네트워크 객체 연결

사용자 목록의 단일 사용자 또는 사용자 그룹을 네트워크 객체와 연결하려면 다음 단계를 수행합니다.

프로시저

사용자 목록의 단일 사용자 또는 사용자 그룹을 네트워크 객체와 연결합니다.

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

예제**:**

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 인수는 사용자 또는 사용자 그룹이 연결된 인터페이스 네트워크 개체 이름을 지정합니다. **trap** 키워드는 트랩만 전송될 수 있으며 이 호스트는 찾아보기(폴링)가 허용되지 않음을 나타냅니다. **poll** 키워드는 이 호스트에서 찾아보기(폴링)가 허용되지만 트랩을 전송할 수 없음을 나타냅니다. **community** 키워드는 NMS에서 요청을 수신할 때 또는 NMS로 전송되는 트랩을 생성할 때 기본값이 아닌 문자열이 필요함을 나타냅니다. SNMP 버전 1 또는 2c에만 이 키워드를 사용할 수 있습니다. *community-string* 인수는 알림과 함께 전송되거나 NMS의 요청에서 전송되는 비밀번호와 비슷한 커뮤니티 문자열을 지정합니다. 커뮤니티 문자열은 최대 32자까지 허용됩니다. **version** 키워드는 버전 1, 2c 또는 3에 대해 트랩 전송에 사용할 SNMP 알림 버전을 설정합니다. *username* 인수는 SNMP 버전 3을 사용할 경우 사용자의 이름을 지정합니다. **user-list** *list_name* 키워드-인수 페어는 사용자 목록의 이름을 지정합니다. **udp-port** *port* 키워드-인수 쌍은 SNMP 트랩이 기본값이 아닌 포트의 NMS 호스트로 전송되어야 함을 지정하고 NMS 호스트의 UDP 포트 번호를 설정합니다. 기본 UDP 포트는 162입니다. 기본 버전은 1입니다. SNMP 트랩은 기본적으로 활성화되어 있습니다.

SNMP 모니터링

SNMP 모니터링에 대한 내용은 다음 명령을 참고하십시오.

- **show running-config snmp-server** [**default**]

  이 명령은 모든 SNMP 서버 구성 정보를 표시합니다.

- **show running-config snmp-server group**

  이 명령은 SNMP 그룹 구성 설정을 표시합니다.

- **show running-config snmp-server host**

  이 명령은 SNMP에서 원격 호스트로 전송되는 메시지 및 알림을 제어하는 데 사용되는 구성 설정을 표시합니다.

- **show running-config snmp-server host-group**

  이 명령은 SNMP 호스트 그룹 구성을 표시합니다.

- **show running-config snmp-server user**

이 명령은 SNMP 사용자 기반 구성 설정을 표시합니다.

- **show running-config snmp-server user-list**

  이 명령은 SNMP 사용자 목록 구성을 표시합니다.

- **show snmp-server engineid**

  이 명령은 구성된 SNMP 엔진의 ID를 표시합니다.

- **show snmp-server group**

  이 명령은 구성된 SNMP 그룹의 이름을 표시합니다. 커뮤니티 문자열이 이미 설정 구성된 경우 기본적으로 출력에 2개의 추가 그룹이 표시됩니다. 이는 정상입니다.

- **show snmp-server statistics**

  이 명령은 SNMP 서버의 구성된 특성을 표시합니다. 모든 SNMP 카운터를 0으로 재설정하려면 **clear snmp-server statistics** 명령을 사용하십시오.

- **show snmp-server user**

  이 명령은 사용자의 구성 특성을 표시합니다.

예

다음 예는 SNMP 서버 통계를 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

다음 예는 SNMP 서버 실행 구성을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP의 예

다음 섹션에서는 모든 SNMP Version의 참조로 사용할 수 있는 예를 제공합니다.

SNMP 버전 1 및 2c

다음 예는 ASA가 내부 인터페이스의 호스트 192.0.2.5으로부터 SNMP 요청을 받되 호스트로 SNMP syslog 요청을 전송하지 않는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP 버전 3

다음 예는 ASA가 SNMP 버전 3 보안 모델(그룹, 사용자, 호스트 순으로 구성해야 함)을 사용하여 SNMP 요청을 수신하는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP 기록

표 ***61: SNMP*** 기록

기능 이름	플랫폼 릴리스	설명
SNMP 버전 1 및 2c	7.0(1)	일반 텍스트 커뮤니티 문자열을 통해 SNMP 서버와 SNMP 에이전트 간에 데이터를 전송함으로써 ASA, ASAv 및 ASASM 네트워크 모니터링과 이벤트 정보를 제공합니다.

기능 이름	플랫폼 릴리스	설명
SNMP 버전 3	8.2(1)	3DES 또는 AES 암호화를 제공하고 지원 보안 모델 중 가장 안전한 SNMP 버전 3을 지원합니다. 이 버전에서는 USM을 사용하여 사용자, 그룹 및 호스트는 물론 인증 특성도 구성할 수 있습니다. 또한 이 버전은 에이전트 및 MIB 객체에 대한 액세스 제어가 가능하며 추가 MIB 지원을 포함합니다. 다음 명령을 도입 또는 수정했습니다. **show snmp-server engineid**, **show snmp-server group**, **show snmp-server user**, **snmp-server group**, **snmp-server user**, **snmp-server host**.
비밀번호 암호화	8.3(1)	비밀번호 암호화를 지원합니다. 다음 명령을 수정했습니다. **snmp-server community**, **snmp-server host**.

기능 이름	플랫폼 릴리스	설명
SNMP 트랩 및 MIB	8.4(1)	다음 추가 키워드를 지원합니다. **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. 센서, 팬, 전원 공급 장치 및 관련 구성 요소에 대한 entPhysicalTable 보고 항목. 다음 추가 MIB를 지원합니다. CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. 다음 추가 트랩을 지원합니다. ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. 다음 명령을 도입 또는 수정했습니다. **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
IF-MIB ifAlias OID 지원	8.2(5)/8.4(2)	이제 ASA가 ifAlias OID를 지원합니다. IF-MIB를 찾아볼 때 ifAlias OID는 인터페이스 설명에 설정된 값으로 설정됩니다.

기능 이름	플랫폼 릴리스	설명
ASA 서비스 모듈(ASASM)	8.5(1)	ASASM은 다음을 제외하고 8.4(1)의 모든 MIB 및 트랩을 지원합니다. 8.5(1)에서 지원되지 않는 MIB: • CISCO-ENTITY-SENSOR-EXT-MIB(entPhySensorTable그룹의 객체만 지원됨). • ENTITY-SENSOR-MIB(entPhySensorTable 그룹의 객체만 지원됨). • DISMAN-EXPRESSION-MIB(expExpressionTable, expObjectTable 및 expValueTable 그룹의 객체만 지원됨). 8.5(1)에서 지원되지 않는 트랩: • ceSensorExtThresholdNotification(CISCO-ENTITY-SENSOR-EXT-MIB). 이 트랩은 전원 공급 장치 및 팬 고장, CPU 고온 이벤트에만 사용됩니다. • InterfacesBandwidthUtilization.
SNMP 트랩	8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에 대해 다음 추가 키워드를 지원합니다. **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. 다음 명령을 수정했습니다. **snmp-server enable traps**

기능 이름	플랫폼 릴리스	설명
VPN 관련 MIB	9.0(1)	차세대 암호화 기능 지원을 위해 업데이트된 버전의 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB가 구현되었습니다. 다음 MIB가 ASASM에 대해 활성화되었습니다. • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	다음 MIB가 추가되었습니다. CISCO-TRUSTSEC-SXP-MIB.
SNMP OID	9.1(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 지원을 위해 5개의 새로운 SNMP 물리적 공급업체 유형 OID가 추가되었습니다.
NAT MIB	9.1(2)	xlate_count 및 max_xlate_count 항목 지원을 위해 cnatAddrBindNumberOfEntries 및 cnatAddrBindSessionCount OID가 추가되었습니다. 이는 **show xlate count** 명령을 사용한 폴링 허용과 대등합니다.
SNMP 호스트, 호스트 그룹 및 사용자 목록	9.1(5)	이제 호스트를 최대 4000개까지 추가할 수 있습니다. 지원되는 활성 폴링 대상 수는 128개입니다. 호스트 그룹으로 추가할 개별 호스트를 나타내는 네트워크 객체를 지정할 수 있습니다. 둘 이상의 사용자를 하나의 호스트와 연결할 수 있습니다. 다음 명령을 도입 또는 수정했습니다. **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.

기능 이름	플랫폼 릴리스	설명
SNMP 메시지 크기	9.2(1)	SNMP가 전송하는 메시지 크기 제한이 1472바이트로 증가했습니다.
SNMP OID 및 MIB	9.2(1)	이제 ASA가 cpmCPUTotal5minRev OID를 지원합니다. ASAv가 SNMP sysObjectID OID 및 entPhysicalVendorType OID에 새로운 제품으로 추가되었습니다. CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB가 업데이트되어 새로운 ASAv 플랫폼을 지원합니다. VPN 공유 라이센스 사용량 모니터링을 위한 새로운 SNMP MIB가 추가되었습니다.
SNMP OID 및 MIB	9.3(1)	ASASM에 대한 CISCO-REMOTE-ACCESS-MONITOR-MIB(OID 1.3.6.1.4.1.9.9.392) 지원이 추가되었습니다.

기능 이름	플랫폼 릴리스	설명
SNMP MIB 및 트랩	9.3(2)	CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB는 ASA 5506-X를 지원하도록 업데이트되었습니다. ASA 5506-X가 SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새로운 제품으로 추가되었습니다. 이제 ASA에서 CISCO-CONFIG-MAN-MIB를 지원하므로 다음 작업을 수행할 수 있습니다. • 특정 구성에 대해 어떤 명령이 입력되었는지 알 수 있습니다. • 구성 실행 중 변경이 발생하면 NMS에게 알립니다. • 실행 중인 구성이 마지막으로 변경되거나 저장된 시간에 대한 타임 스탬프를 추적합니다. • 터미널 정보 및 명령 소스와 같은 기타 명령 변경 사항을 추적합니다. 다음 명령을 수정했습니다. **snmp-server enable traps**
SNMP MIB 및 트랩	9.4(1)	ASA 5506W-X, ASA 5506H-X, ASA 5508-X 및 ASA 5516-X가 SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새 제품으로 추가되었습니다.
상황당 무제한 SNMP 서버 트랩 호스트	9.4(1)	ASA는 상황별로 무제한 SNMP 서버 트랩 호스트를 지원합니다. **show snmp-server host** 명령 출력에는 정적으로 구성한 호스트와 함께 ASA를 폴링 중인 활성 호스트만 표시됩니다. 다음 명령을 수정했습니다. **show snmp-server host**

기능 이름	플랫폼 릴리스	설명
ISA 3000에 대한 지원 추가됨	9.4(1.225)	ISA 3000 제품군이 이제 SNMP에 대해 지원됩니다. 이 플랫폼에 대한 새 OID를 추가했습니다. **snmp-server enable traps entity** 명령이 새로운 변수인 *l1-bypass-status*를 포함하도록 수정되었습니다. 이렇게 하면 하드웨어 우회 상태 변경이 활성화됩니다. 다음 명령을 수정했습니다. **snmp-server enable traps entity**.
CISCO-ENHANCED-MEMPOOL-MIB에서 cempMemPoolTable에 대한 지원	9.6(1)	이제 CISCO-ENHANCED-MEMPOOL-MIB의 cempMemPoolTable이 지원됩니다. 이는 매니지드 시스템의 모든 물리적 엔티티에 대한 항목을 모니터링하는 메모리 풀의 테이블입니다. 참고 CISCO-ENHANCED-MEMPOOL-MIB는 64비트 카운터를 사용하고 4GB 이상의 RAM을 사용하는 플랫폼에서 메모리 보고 기능을 지원합니다.
PTP(Precision Time Protocol)에 대한 E2E 투명 클록 모드 MIB를 지원합니다.	9.7(1)	E2E 투명 클록 모드에 해당하는 MIB가 이제 지원됩니다. 참고 SNMP get, bulkget, getnext, walk 작업만 지원됩니다.

기능 이름	플랫폼 릴리스	설명
IPv6를 통한 SNMP	9.9(2)	이제 ASA에서는 IPv6를 통한 SNMP 서버와의 통신, IPv6를 통한 쿼리 및 트랩 실행, 기존 MIB에 대한 IPv6 주소 지원을 비롯하여 IPv6를 통한 SNMP를 지원합니다. RFC 8096에 설명된 대로 다음과 같은 새로운 SNMP IPv6 MIB 개체가 추가되었습니다. • ipv6InterfaceTable(OID: 1.3.6.1.2.1.4.30) — 인터페이스별 IPv6 특정 정보를 포함합니다. • ipAddressPrefixTable(OID:1.3.6.1.2.1.4.32) — 이 엔티티에서 확인한 모든 접두사를 포함합니다. • ipAddressTable(OID: 1.3.6.1.2.1.4.34) — 엔티티의 인터페이스와 관련된 주소 지정 정보를 포함합니다. • ipNetToPhysicalTable(OID: 1.3.6.1.2.1.4.35) — IP 주소에서 실제 주소로의 매핑을 포함합니다. 신규 또는 수정된 명령: **snmp-server host** 참고 **snmp-server host-group** 명령은 IPv6를 지원하지 않습니다.

43 장

Cisco ISA 3000에 대한 알람

이 장에서는 ISA 3000의 알람 시스템 개요와 알람을 구성하고 모니터링하는 방법에 대해서도 설명합니다.

알람 정보

여러 조건에 대해 알람을 생성하도록 ISA 3000을 구성할 수 있습니다. 조건이 구성된 설정과 일치하지 않으면 시스템은 알람을 트리거합니다. 이러한 알람은 LED, syslog 메시지, SNMP 트랩 및 알람 출력 인터페이스에 연결된 외부 디바이스를 통해 보고됩니다. 기본적으로 알람이 트리거되면 syslog 메시지만 발급됩니다.

다음을 모니터링하도록 알람 시스템을 구성할 수 있습니다.

- 전원 공급 장치
- 기본 및 보조 온도 센서
- 알람 입력 인터페이스

ISA 3000에는 내부 센서와 알람 입력 인터페이스 2개, 알람 출력 인터페이스 1개가 있습니다. 도어 센서와 같은 외부 센서를 알람 입력에 연결할 수 있습니다. 버저나 표시등과 같은 외부 알람 디바이스를 알람 출력 인터페이스에 연결할 수 있습니다.

알람 출력 인터페이스는 릴레이 메커니즘입니다. 알람 조건에 따라 릴레이가 활성화되거나 비활성화됩니다. 릴레이가 활성화되면 인터페이스에 연결된 디바이스가 활성화됩니다. 릴레이가 비활성화되면 연결된 디바이스가 비활성 상태가 됩니다. 알람이 트리거되는 동안에는 릴레이가 활성화된 상태로 유지됩니다.

외부 센서와 알람 릴레이 연결에 대한 자세한 정보는 Cisco ISA 3000 Industrial Security Appliance 하드웨어 설치 가이드를 참조하십시오.

알람 입력 인터페이스

도어가 열린 상태를 탐지하는 센서 등의 외부 센서에 알람 입력 인터페이스나 접촉부를 연결할 수 있습니다.

각 알람 입력 인터페이스에는 해당하는 LED가 있습니다. 이러한 LED는 각 알람 입력의 알람 상태를 전달합니다. 각 알람 입력에 대해 트리거와 심각도를 구성할 수 있습니다. LED 외에도 출력 릴레이를 트리거하여 외부 알람을 활성화하고 syslog 메시지와 SNMP 트랩을 전송하는 접촉부를 구성할 수도 있습니다.

다음 표에서는 알람 입력에 대한 알람 조건에 대응하는 LED의 상태를 설명합니다. 또한 출력 릴레이, syslog 메시지 및 SNMP 트랩(알람 입력에 대해 이러한 응답을 활성화하는 경우)의 동작도 설명합니다.

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP Trap(SNMP 트랩)**
알람이 구성되지 않음	Off	—	—	—
알람이 트리거되지 않음	녹색	—	—	—
알람 활성화됨	경미한 알람 - 빨간색으로 켜짐 중요한 알람 - 빨간색으로 깜박임	릴레이 활성화됨	Syslog 생성됨	SNMP 트랩 전송됨
알람 종료됨	녹색	릴레이 비활성화됨	Syslog 생성됨	—

알람 출력 인터페이스

버저나 표시등과 같은 외부 알람을 알람 출력 인터페이스에 연결할 수 있습니다.

알람 출력 인터페이스는 릴레이로 작동하며 해당하는 LED도 가지고 있습니다. 이러한 LED는 입력 인터페이스에 연결된 외부 센서와 듀얼 전원 공급 장치 및 온도 센서 등의 내부 센서의 알람 상태를 전달합니다. 출력 릴레이(있는 경우)를 활성화하는 알람을 구성합니다.

다음 표에서는 알람 조건에 대응하는 LED 및 출력 릴레이의 상태를 설명합니다. 또한 syslog 메시지 및 SNMP 트랩(알람에 대해 이러한 응답을 활성화하는 경우)의 동작도 설명합니다.

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP Trap(SNMP 트랩)**
알람이 구성되지 않음	Off	—	—	—
알람이 트리거되지 않음	녹색	—	—	—

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP Trap(SNMP** 트랩**)**
알람 활성화됨	빨간색으로 켜짐	릴레이 활성화됨	Syslog 생성됨	SNMP 트랩 전송됨
알람 종료됨	녹색	릴레이 비활성화됨	Syslog 생성됨	—

알람 기본값

다음 표에는 알람 입력 인터페이스(접촉부), 예비 전원 공급 장치 및 온도의 기본값이 지정되어 있습니다.

	경보	트리거	**Severity(**심각도**)**	**SNMP Trap(SNMP** 트랩**)**	출력 릴레이	**Syslog** 메시지
알람 접촉부 1	활성화됨	닫힌 상태	Minor(경미)	비활성화됨	비활성화됨	활성화됨
알람 접촉부 2	활성화됨	닫힌 상태	Minor(경미)	비활성화됨	비활성화됨	활성화됨
예비 전원 공급 장치(활성화된 경우)	활성화됨	—	—	비활성화됨	비활성화됨	활성화됨
온도	기본 온도 알람에 대해 활성화됨(최고 임계값과 최저 임계값의 기본값은 각각 92°C 및 -40°C) 보조 알람에 대해 비활성화됨.	—	—	기본 온도 알람에 대해 활성화됨	기본 온도 알람에 대해 활성화됨	기본 온도 알람에 대해 활성화됨

알람 구성

ISA 3000에 대해 알람을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 1개 또는 모든 알람 접촉부의 심각도를 구성합니다.

alarm contact {*contact_number* | **all**} **severity {major | minor | none}**

예제**:**

```
ciscoasa(config)# alarm contact 1 severity major
```

접촉부 번호(**1** 또는 **2**)를 입력하거나 모든 알람을 구성하려면 **all**을 입력합니다. 심각도는 **major**, **minor** 또는 **none**으로 입력합니다. 기본값은 minor입니다.

단계 **2** 1개 또는 모든 알람 접촉부에 대한 트리거를 구성합니다.

alarm contact {*contact_number* | **all**} **trigger {closed | open}**

open을 지정하면 접촉부가 정상적으로 닫히거나(정상적인 전기 연결) 열려 있거나 전류 흐름이 중단된 경우 알람을 트리거합니다.

closed를 지정하면 접촉부가 정상적으로 열리고(전기 연결 없음) 닫히거나 전류 흐름이 시작된 경우 알람을 트리거합니다.

도어 센서를 알람 입력 접촉부에 연결하고 해당 접촉부의 정상적으로 열린 상태가 접촉부를 통해 전류가 흐르지 않고 있는 경우를 예로 들어 보겠습니다. 도어가 열리면 접촉부를 통해 전류가 흘러 알람이 활성화됩니다.

예제**:**

```
ciscoasa(config)# alarm contact 1 trigger open
```

접촉부 번호(**1** 또는 **2**)를 입력하거나 모든 알람을 구성하려면 **all**을 입력합니다. 트리거를 지정하려면 **open** 또는 **closed**를 입력합니다. 기본값은 closed입니다.

단계 **3** 알람 접촉부에 대해 릴레이, 시스템 로거 및 SNMP 트랩을 활성화합니다.

릴레이가 활성화되고 알람 조건이 발생하면 릴레이에 전원이 공급되고 릴레이에 연결된 디바이스가 활성화됩니다. 릴레이에 전원이 공급되면 알람 아웃 LED가 빨간색으로 켜집니다.

- 입력 알람에 대한 릴레이를 활성화합니다.

alarm facility input-alarm *contact_number* **relay**

예제**:**

```
ciscoasa(config)# alarm facility input-alarm 1 relay
```

접촉부 번호(**1** 또는 **2**)를 입력합니다. 알람 입력에 대한 릴레이는 기본적으로 비활성화되어 있습니다.

- 시스템 로거를 활성화합니다.

alarm facility input-alarm *contact_number* **syslog**

예제**:**

```
ciscoasa(config)# alarm facility input-alarm 1 syslog
```

접촉부 번호(**1** 또는 **2**)를 입력합니다.

- SNMP 트랩을 활성화합니다.

alarm facility input-alarm *contact_number* **notifies**

예제:

```
ciscoasa(config)# alarm facility input-alarm 1 notifies
```

접촉부 번호(**1** 또는 **2**)를 입력합니다.

단계 **4** (선택 사항) 입력 알람 접촉부에 대한 설명을 지정합니다.

alarm contact *contact_number* | **description** *string*

예제:

```
ciscoasa(config)# alarm contact 1 description Door_Open
```

contact_number는 설명이 구성되어 있는 알람 접촉부를 지정합니다. 설명은 최대 80자의 영숫자로 구성되며 syslog 메시지에 포함됩니다.

일치하는 접촉부 번호로 기본 설명을 설정하려면 **no alarmcontact contact_number description** 명령을 사용합니다.

단계 **5** 전원 공급 장치 알람 구성

참고 전원 공급 장치 알람이 작동하려면 예비 전원 공급 장치를 활성화해야 합니다.

전원 공급 장치 알람 구성에 대해서는 다음 명령을 참고하십시오.

- **power-supply dual**

  이 명령은 이중 전원 공급 장치를 활성화합니다.

- **alarm facility power-supply rps disable**

  이 명령은 전원 공급 장치 알람을 비활성화합니다. 기본 상태에서 이 알람은 비활성화되어 있습니다. 알람이 활성화되어 있는 경우 이 명령을 사용하여 비활성화합니다.

- **alarm facility power-supply rps notifies**

  이 명령은 SNMP 서버에 전원 공급 장치 알람 트랩을 전송합니다.

- **alarm facility power-supply rps relay**

  이 명령은 전원 공급 장치 알람을 릴레이에 연결합니다.

- **alarm facility power-supply rps syslog**

  이 명령은 syslog 서버에 전원 공급 장치 알람 트랩을 전송합니다.

단계 **6** 온도 임계값을 구성합니다.

alarm facility temperature {**primary | secondary**}{**high | low**} *threshold*

예제:

```
ciscoasa(config)# alarm facility temperature primary high 90
ciscoasa(config)# alarm facility temperature primary low 40
ciscoasa(config)# alarm facility temperature secondary high 85
ciscoasa(config)# alarm facility temperature primary low 35
```

기본 온도 알람의 경우 유효한 임계값은 −40°C ~ 92°C입니다. 보조 온도 알람의 경우 유효한 임계값은 −35°C ~ 85°C입니다. 보조 알람에 대해 온도 임계값이 구성된 경우 보조 알람만 활성화됩니다.

기본값을 비활성화하거나 되돌리려면 각 명령의 **no** 형식을 사용합니다. 기본 알람에 대한 명령의 **no** 형식을 사용하면 알람이 비활성화되지 않고 높은 임계값에 대한 기본값인 92°C로 되돌아가며 낮은 임계값에 대한 기본값인 −40°C로 되돌아갑니다. 보조 알람에 대한 명령의 **no** 형식을 사용하면 알람이 비활성화됩니다.

단계 **7** 온도 알람에 대해 SNMP 트랩, 릴레이 및 시스템 로거를 활성화합니다.

온도 알람에 대해 릴레이, SNMP 트랩, syslog를 활성화하는 데 대한 내용은 다음 명령을 참고하십시오.

- **alarm facility temperature {primary | secondary} notifies**

  이 명령은 SNMP 서버에 기본 온도 알람 또는 보조 온도 알람 트랩을 전송합니다.

- **alarm facility temperature {primary | secondary} relay**

  이 명령은 기본 또는 보조 온도 알람을 릴레이에 연결합니다.

- **alarm facility temperature {primary | secondary} syslog**

  이 명령은 syslog 서버에 기본 온도 알람 또는 보조 온도 알람 트랩을 전송합니다.

릴레이, SNMP 트랩 및 syslogs를 비활성화하려면 각 명령의 no 형식을 사용합니다.

알람 모니터링

알람을 모니터링하려면 다음 명령을 참고하십시오.

프로시저

- **show alarm settings**

  이 명령은 모든 전역 알람 설정을 표시합니다.

```
ciscoasa> show alarm settings
Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds            MAX: 92C                MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
```

```
         Syslog                  Disabled
Input-Alarm 1
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
Input-Alarm 2
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
```

- **show environment alarm-contact**

  이 명령은 모든 외부 알람 설정을 표시합니다.

```
ciscoasa> show environment alarm-contact
ALARM CONTACT 1
   Status:       not asserted
   Description:  external alarm contact 1
   Severity:     minor
   Trigger:      closed
ALARM CONTACT 2
   Status:       not asserted
   Description:  external alarm contact 2
   Severity:     minor
   Trigger:      closed
```

- **show facility-alarm status [info | major | minor]**

  이 명령은 지정된 심각도에 기반하는 모든 알람을 표시합니다.

  출력은 다음 정보를 표시합니다.

열	설명
소스	알람이 트리거된 디바이스입니다. 일반적으로 디바이스에 구성된 호스트 이름입니다.
심각도	Major 또는 Minor
설명	트리거되는 알람 유형입니다. 예: 온도, 외부 접촉부, 예비 전원 공급 장치 등입니다.
Relay	전원 공급됨 또는 전원 끊김
시간	트리거된 알람의 타임스탬프

```
ciscoasa> show facility-alarm status info
Source      Severity    Description                                    Relay
        Time
ciscoasa    minor       external alarm contact 1 triggered  Energized          06:56:50
 UTC Mon Sep 22 2014
ciscoasa    minor       Temp below Secondary Threshold De-energized            06:56:49
 UTC Mon Sep 22 2014
ciscoasa    major      Redundant pwr missing or failed    De-energized        07:00:19
 UTC Mon Sep 22 2014
ciscoasa    major       Redundant pwr missing or failed    De-energized        07:00:19
 UTC Mon Sep 22 2014
```

```
ciscoasa> show facility-alarm status major
Source      Severity    Description                                    Relay
        Time
ciscoasa    major       Redundant pwr missing or failed    De-energized     07:00:19
UTC Mon Sep 22 2014
ciscoasa   major        Redundant pwr missing or failed    De-energized     07:00:19
UTC Mon Sep 22 2014

ciscoasa> show facility-alarm status minor
Source      Severity    Description                                    Relay
        Time
ciscoasa   minor       external alarm contact 1 triggered  Energized         06:56:50
 UTC Mon Sep 22 2014
ciscoasa   minor        Temp below Secondary Threshold De-energized     06:56:49 UTC
Mon Sep 22 2014
```

- **show facility-alarm relay**

  이 명령은 전원이 공급된 상태의 모든 릴레이를 표시합니다.

```
ciscoasa> show facility-alarm relay
Source      Severity    Description                                    Relay
        Time
ciscoasa   minor        external alarm contact 1 triggered  Energized         06:56:50
 UTC Mon Sep 22 2014
```

알람에 대한 기록

기능 이름	플랫폼 릴리스	설명
ISA 3000에 대한 알람 포트 지원	9.7(1)	

기능 이름	플랫폼 릴리스	설명
		이제 ISA 3000은 알람 상태를 전달하는 LED를 사용하여 두 개의 알람 입력 핀과 한 개의 알람 출력 핀을 지원합니다. 외부 센서는 알람 입력에 연결할 수 있습니다. 외부 하드웨어 릴레이는 알람 출력 핀에 연결할 수 있습니다. 외부 알람에 대한 설명을 구성할 수 있습니다. 심각도 및 외부 및 내부 알람에 대한 트리거를 지정할 수도 있습니다. 모든 알람은 릴레이, 모니터링 및 로깅을 위해 구성될 수 있습니다. 다음 명령을 도입했습니다. **alarm contact description, alarm contactseverity, alarm contact trigger, alarm facility input-alarm, alarm facility power-supply rps, alarm facility temperature, alarm facility temperature high, alarm facility temperature low, clear configure alarm, clear facility-alarm output, show alarm settings, show environment alarm-contact** 추가된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Alarm Port(**알람 포트**)** > **Alarm Contact(**알람 접촉부**)** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Alarm Port(**알람 포트**)** > **Redundant Power Supply(**예비 전원 공급 장치**)** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Alarm Port(**알람 포트**)** > **Temperature(**온도**)** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Alarm(**알람**)** > **Alarm Settings(**알람 설정**)** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Alarm(**알람**)** > **Alarm Contact(**알람 접촉부**)** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Alarm(**알람**)** > **Facility Alarm**

기능 이름	플랫폼 릴리스	설명
		Status(설비 알람 상태**)**

44 장

Anonymous Reporting 및 Smart Call Home

이 장에서는 Anonymous Reporting 및 Smart Call Home 서비스를 구성하는 방법을 설명합니다.

Anonymous Reporting 정보

Anonymous Reporting을 활성화하면 Cisco가 안전하게 디바이스에서 최소 오류 및 상태 정보를 받을 수 있으므로 Cisco ASA 플랫폼을 개선하는 데 도움이 됩니다. 기능을 활성화해도 고객 ID가 익명으로 남으며 신원을 알 수 있는 정보는 전송되지 않습니다.

Anonymous Reporting을 활성화하면 신뢰 지점이 생성되고 인증서가 설치됩니다. CA 인증서는 ASA에서 Smart Call Home 웹 서버에 있는 서버 인증서를 확인하고 HTTPS 세션을 형성하여 ASA가 안전하게 메시지를 전송할 수 있도록 하기 위해 필요합니다. Cisco는 소프트웨어에서 미리 정의된 인증서를 가져옵니다. Anonymous Reporting을 활성화하기로 결정하면 인증서가 _SmartCallHome_ServerCA라는 하드 코딩된 신뢰 지점 이름으로 ASA에 설치됩니다. Anonymous Reporting을 활성화하면 이 신뢰 지점이 생성되고 적절한 인증서가 설치되며 이 활동에 대한 메시지를 받게 됩니다. 그런 다음 컨피그레이션에 인증서가 표시됩니다.

Anonymous Reporting을 활성화할 때 컨피그레이션에 이미 적절한 인증서가 존재하는 경우 신뢰 지점이 생성되지 않고 인증서가 설치되지 않습니다.

참고 Anonymous Reporting을 활성화할 때 Cisco 또는 Cisco의 공급업체로 지정된 데이터를 전송함에 동의합니다(미국 외부의 국가 포함). Cisco는 모든 고객의 개인 정보를 유지 관리합니다. Cisco의 개인 정보 관리 방법에 대한 자세한 내용은 다음 URL에 있는 Cisco의 개인 정보 보호 정책을 참고하십시오. http://www.cisco.com/web/siteassets/legal/privacy.html

ASA가 백그라운드에서 Smart Call Home 익명 보고를 구성할 경우, ASA는 Call Home 서버 인증서를 발급한 CA의 인증서를 포함하는 신뢰 지점을 자동으로 생성합니다. ASA는 이제 인증서 계층 구조를 변경하기 위해 고객이 개입할 필요 없이 발급하는 서버 인증서 계층 구조가 변경되는 경우 인증서 유효성 검사를 지원합니다. ASA는 수동 개입 없이 인증서 계층 구조를 갱신할 수 있도록 신뢰 풀 인증서를 자동으로 가져올 수 있습니다.

DNS 요건

Cisco Smart Call Home 서버에 연결하고 Cisco에 메시지를 전송할 수 있도록 ASA에 대한 DNS 서버가 올바르게 구성되어야 합니다. ASA가 사설 네트워크에 상주하고 공용 네트워크에 대한 액세스 권한이 없을 수 있기 때문에 Cisco는 DNS 설정을 확인한 다음 필요한 경우 다음과 같이 컨피그레이션을 대행합니다.

1. 구성된 모든 DNS 서버에 대한 DNS 조회 실시
2. 최고 수준의 보안 인터페이스에서 DHCPINFORM 메시지를 전송하여 DHCP 서버에서 DNS 서버로 연결
3. 조회용 Cisco DNS 서버 사용
4. 무작위로 tools.cisco.com에 대한 고정 IP 주소 사용

이러한 작업은 현재 컨피그레이션을 변경하지 않고 수행됩니다. 예를 들어 DHCP에서 학습된 DNS 서버는 컨피그레이션에 추가되지 않습니다.

구성된 DNS 서버가 없고 ASA가 Cisco Smart Call Home 서버에 연결 할 수 없는 경우 Cisco는 전송된 각 Smart Call Home 메시지에 대한 경고 심각도 수준과 함께 syslog 메시지를 생성하여 DNS를 바르게 구성하라고 알려줍니다.

syslog 메시지에 대한 정보는 syslog 메시지 가이드를 참고하십시오.

Smart Call Home 정보

완전히 구성된 Smart Call Home은 사이트의 문제를 감지하고 이를 Cisco 또는 다른 사용자 정의 채널(이메일이나 직접 연락)로 보고합니다. 문제가 있음을 알기도 전에 보고를 받는 경우도 많습니다. 이 문제의 심각성에 따라 Cisco에서는 다음 서비스를 제공하여 시스템 컨피그레이션 문제, 제품 단종 공지, 보안 권고 사항 등에 대응합니다.

- 지속적인 모니터링, 실시간 사전 경고 및 상세한 진단을 통해 신속하게 문제를 파악합니다.

- 서비스 요청이 등록되어 있고 모든 진단 데이터가 첨부된 Smart Call Home 알림을 통해 잠재적인 문제를 파악할 수 있습니다.
- Cisco TAC의 전문가와 직접적이고 자동적으로 연락함으로써 중요한 문제를 더 빨리 해결합니다.
- 문제 해결 시간을 단축하여 인력 자원을 더욱 효율적으로 활용합니다.
- Cisco TAC 서비스 요청을 자동으로 생성(서비스 계약을 체결한 경우)하고 적절한 지원 팀으로 라우팅하면 해당 팀이 자세한 진단 정보를 제공하여 문제 해결을 가속합니다.

Smart Call Home 포털은 다음을 수행하는 데 필요한 정보에 대한 빠른 액세스를 제공합니다.

- 모든 Smart Call Home 메시지, 진단 및 권장 사항을 한 곳에서 확인합니다.
- 서비스 요청 상태를 확인합니다.
- 모든 Smart Call Home 지원 디바이스에 대한 최신 인벤토리 및 컨피그레이션 정보를 확인합니다.

경고 그룹에 가입

경고 그룹은 ASA에서 지원되는 Smart Call Home 경고의 하위 집합으로 사전 정의됩니다. 다른 유형의 Smart Call Home 경고는 유형에 따라 다른 경고 그룹으로 그룹화됩니다. 각 경고 그룹은 특정 CLI 출력을 보고합니다. 지원되는 Smart Call Home 경고 그룹은 다음과 같습니다.

- syslog
- diagnostic
- environment
- inventory
- 구성
- threat
- snapshot
- telemetry
- 테스트

경보 그룹의 특성

경고 그룹 특성은 다음과 같습니다.

- 이벤트는 먼저 하나의 경고 그룹에 등록됩니다.
- 그룹은 여러 이벤트와 연결될 수 있습니다.
- 특정 경고 그룹에 등록할 수 있습니다.

- 문자 경고 그룹을 활성화 및 비활성화할 수 있습니다. 기본 설정은 모든 경고 그룹에 사용할 수 있습니다.
- 진단 및 환경 경고 그룹은 정기적 메시지에 대한 서브스크립션을 지원합니다.
- syslog 경고 그룹은 메시지 ID 기반 서브스크립션을 지원합니다.
- 환경 경고 그룹에 대한 CPU 및 메모리 사용량 한계값을 구성할 수 있습니다. 특정 매개 변수가 미리 정해진 한도를 초과할 때 메시지가 전송됩니다. 임계값의 대부분은 플랫폼에 따르며 변경할 수 없습니다.
- 스냅샷 경고 그룹을 지정하여 지정한 CLI의 출력을 전송합니다.

메시지가 경보 그룹별로 **Cisco**에 전송됨

ASA가 다시 로드될 때마다 메시지가 정기적으로 Cisco에 전송됩니다. 이 메시지는 경고 그룹별로 분류됩니다.

인벤토리 경고는 다음 명령의 출력으로 구성됩니다.

- **show version**—디바이스의 ASA 소프트웨어 버전, 하드웨어 컨피그레이션, 라이센스 키 및 관련 가동 시간 데이터를 표시합니다.
- **show inventory**—네트워킹 디바이스에 설치되어 있는 각 Cisco 제품에 대한 인벤토리 정보를 검색하고 표시합니다. 각 제품은 제품 ID(PID), 버전(VID) 및 일련 번호(SN)의 3가지 분리된 데이터 요소가 조합된 고유한 디바이스 정보인 UDI로 식별됩니다.
- **show failover state** - 장애 조치 쌍의 두 유닛의 장애 조치 상태를 표시합니다. 표시 정보는 유닛의 1차 또는 2차 상태, 유닛의 액티브/스탠바이 상태 및 장애 조치를 위해 마지막으로 보고된 이유를 포함합니다.
- **show module** - ASA 5585-X에 설치된 SSP에 대한 정보, ASA 5585-X에 설치된 IPS SSP에 대한 정보 등 ASA에 설치된 모든 모듈에 대한 정보를 제공합니다.
- **show environment** - 섀시, 드라이버, 팬 및 전력 공급 장치에 대한 하드웨어 동작 상태는 물론 온도 상태, 전압 및 CPU 사용량 등 ASA 시스템 구성 요소의 환경 정보를 표시합니다.

구성 경고는 다음 명령의 출력으로 구성됩니다.

- **show context**— 할당된 인터페이스 및 구성 파일 URL, 구성된 상황 수 또는 시스템 구현 영역에서 Anonymous Reporting을 설정한 경우 모든 상황 목록을 표시합니다.
- **show call-home registered-module status**— 등록된 모듈 상태를 표시합니다. 시스템 컨피그레이션 모드를 사용하는 경우 이 명령은 컨텍스트가 아니라 전체 디바이스를 기준으로 시스템 모듈 상태를 표시합니다.
- **show running-config** — 현재 ASA에서 실행 중인 구성을 표시합니다.
- **show startup-config** - 시작 컨피그레이션을 표시합니다.
- **show access-list | include elements** - 액세스 목록에 대한 계수기 및 타임 스탬프 값을 표시합니다.

진단 경고는 다음 명령의 출력으로 구성됩니다.

- **show failover**—유닛의 장애 조치 상태에 관한 정보를 표시합니다.
- **show interface** — 인터페이스 통계를 표시합니다.
- **show cluster info** — 클러스터 정보를 표시합니다.
- **show cluster history** — 클러스터 내역을 표시합니다.
- **show crashinfo(truncated)** - 소프트웨어가 예기치 않게 다시 로드된 후 디바이스가 파일의 역추적 섹션만 포함된 수정된 충돌 정보 파일을 전송하여 기능 호출, 등록 값, 스택 덤프만 Cisco에 보고됩니다.
- **show tech-support no-config** — 기술 지원 분석가가 진단을 위해 사용하는 정보를 표시합니다.

환경 경고는 다음 명령의 출력으로 구성됩니다.

- **show environment** - 섀시, 드라이버, 팬 및 전력 공급 장치에 대한 하드웨어 동작 상태는 물론 온도 상태, 전압 및 CPU 사용량 등 ASA 시스템 구성 요소의 환경 정보를 표시합니다.
- **show cpu usage** - CPU 사용량 정보를 표시합니다.
- **show memory detail** - 여유가 있는 할당된 시스템 메모리의 세부 정보를 표시합니다.

위협 경고는 다음 명령의 출력으로 구성됩니다.

- **show threat-detection rate** - 위협 감지 통계를 표시합니다.
- **show threat-detection shun** - 현재 회피 호스트를 표시합니다.
- **show shun** - 회피 정보를 표시합니다.
- **show dynamic-filter reports top** - 봇넷 트래픽 필터로 분류된 상위 10개의 악성 프로그램 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.

스냅샷 경고는 다음 명령의 출력으로 구성됩니다.

- **show conn count** - 현재 액티브 연결 수를 표시합니다.
- **show asp drop** - 가속화된 보안 경로 드롭 패킷 또는 연결을 표시합니다.

텔레메트리 경고는 다음 명령의 출력으로 구성됩니다.

- **show perfmon detail** — ASA 성능 정보를 표시합니다.
- **show traffic** — 인터페이스 송수신 활동을 표시합니다.
- **show conn count** - 현재 액티브 연결 수를 표시합니다.
- **show vpn-sessiondb summary** — **VPN** 세션 요약 정보를 표시합니다.
- **show vpn load-balancing** — **VPN** 로드 밸런싱 가상 클러스터 구성에 대한 런타임 통계를 표시합니다.

- **show local-host | include interface** — 로컬 호스트의 네트워크 상태를 표시합니다.
- **show memory** — 최대 물리적 메모리와 현재 운영 체제에서 이용 가능한 여유 메모리에 대한 요약 정보를 표시합니다.
- **show context**— 할당된 인터페이스 및 구성 파일 URL, 구성된 상황 수 또는 시스템 구현 영역에서 Anonymous Reporting을 설정한 경우 모든 상황 목록을 표시합니다.
- **show access-list | include elements** - 액세스 목록에 대한 계수기 및 타임 스탬프 값을 표시합니다.
- **show interface** — 인터페이스 통계를 표시합니다.
- **show threat-detection statistics protocol** — **IP** 프로토콜 통계를 표시합니다.
- **show phone-proxy media-sessions count** — 전화 프록시가 저장한 해당 미디어 세션 수를 표시합니다.
- **show phone-proxy secure-phones count** — 데이터베이스에 저장된 안전 모드를 지원하는 휴대폰 수를 표시합니다.
- **show route** — 라우팅 테이블을 표시합니다.
- **show xlate count** — **NAT** 세션**(xlates)** 수를 표시합니다.

메시지 심각도 임계값

특정 경고 그룹에 목적지 프로필을 등록하면 메시지 심각도 수준에 따라 경고 그룹 메시지를 보내는 임계값을 설정할 수 있습니다. 목적지 프로필의 지정 임계값보다 낮은 값을 가진 메시지는 목적지로 전송되지 않습니다.

다음 표는 메시지 심각도 수준 및 syslog 심각도 수준 간의 매핑을 보여 줍니다.

표 ***62:*** 메시지 심각도 수준 및 ***Syslog*** 수준 매핑

수준	메시지 심각도 레벨	**Syslog** 심각도 레벨	설명
9	치명	해당 없음	네트워크 전반의 치명적인 장애.
8	재해	해당 없음	중대한 네트워크 영향.
7	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** 경고 그룹 이름 심각도 심각도 레벨	0	긴급 시스템을 사용할 수 없습니다.

수준	메시지 심각도 레벨	**Syslog** 심각도 레벨	설명
6	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** 경고 그룹 이름 심각도 심각도 레벨	1	경고. 심각한 상태로 즉시 살펴봐야 합니다.
5	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** 경고 그룹 이름 심각도 심각도 레벨	2	심각. 중요한 문제.
4	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** 경고 그룹 이름 심각도 심각도 레벨	3	오류. 경미한 문제.
3	경고	4	경고 상태입니다.
2	알림	5	기본적인 알림 및 정보 메시지입니다. 단독으로는 중요하지 않습니다.
1	정상	6	정보: 일반적인 이벤트로 정상 상태 복귀를 의미합니다.
0	디버깅	7	디버깅 메시지(기본 설정)입니다.

서브스크립션 프로필

서브스크립션 프로필을 통해 목적지 수신자를 관심 그룹과 연계할 수 있습니다. 프로필의 서브스크립션 그룹에 이벤트가 등록되면 해당 이벤트와 연결된 메시지가 구성된 수신자에게 전송됩니다. 서브스크립션 프로필은 다음과 같은 특성을 갖습니다.

- 여러 프로필을 만들고 구성할 수 있습니다.
- 프로필은 여러 이메일 또는 HTTPS 수신자를 구성할 수 있습니다.
- 프로필은 지정된 심각도 수준에 여러 그룹을 등록할 수 있습니다.
- 프로필은 짧은 텍스트, 긴 텍스트 및 XML의 3가지 메시지 형식을 지원합니다.
- 특정 프로필을 활성화 및 비활성화할 수 있습니다. 프로필은 기본적으로 비활성화되어 있습니다.
- 최대 메시지 크기를 지정할 수 있습니다. 기본값은 3MB입니다.

기본 프로필 "Cisco TAC"가 제공됩니다. 기본 프로필에는 모니터 및 사전 정의된 목적지 이메일 및 HTTPS URL에 대한 사전 정의된 그룹 집합(진단, 환경, 인벤토리, 컨피그레이션 및 텔레메트리)이 있습니다. 기본 프로필은 Smart Call Home을 처음 구성할 때 자동으로 만들어집니다. 목적지 이메일은 callhome@cisco.com이고 목적지 URL은 https://tools.cisco.com/its/service/oddce/services/DDCEService입니다.

참고 기본 프로필의 이메일 또는 목적지 URL을 변경할 수 없습니다.

컨피그레이션, 인벤토리, 텔레메트리 또는 스냅샷 경고 그룹에 목적지 프로필을 등록할 때 경고 그룹 메시지를 비동기식으로 받을지 아니면 지정된 시간에 정기적으로 받을지 선택할 수 있습니다.

다음 표는 기본 경보 그룹을 심각도 수준 서브스크립션 및 기간에 매핑(해당하는 경우)합니다.

표 ***63:*** 심각도 수준 서브스크립션에 대한 경고 그룹 매핑

경고 그룹	심각도 수준	기간
구성	정보	매달
진단	정보 이상	해당 없음
환경	알림 이상	해당 없음
인벤토리	정보	매달
Snapshot	정보	해당 없음
Syslog	동일한 syslog	해당 없음
원격 측정	정보	매일
테스트	해당 없음	해당 없음
위협	알림	해당 없음

Anonymous Reporting 및 Smart Call Home에 대한 지침

이 섹션에는 Anonymous Reporting 및 Smart Call Home을 구성하기 전에 검토해야 할 지침 및 제한사항이 포함되어 있습니다.

Anonymous Reporting 지침

- DNS를 구성해야 합니다.
- Anonymous Reporting 메시지를 한 번에 전송할 수 없는 경우 ASA는 메시지를 삭제하기 전에 두 번 더 시도합니다.

- Anonymous Reporting은 기존 컨피그레이션을 변경하지 않고 다른 Smart Call Home 컨피그레이션과 공존할 수 있습니다. 예를 들어, Smart Call Home이 Anonymous Reporting을 활성화하기 전에 비활성화된 경우 Anonymous Reporting을 활성화한 후에도 비활성 상태를 유지합니다.
- Anonymous Reporting이 활성화되면 신뢰 지점을 제거할 수 없고 Anonymous Reporting이 비활성화되어도 신뢰 지점이 유지됩니다. Anonymous Reporting이 비활성화된 경우 신뢰 지점을 제거할 수 있으나 Anonymous Reporting을 비활성화한다고 신뢰 지점이 자동으로 삭제되지는 않습니다.
- 여러 컨텍스트 모드 컨피그레이션을 사용하는 경우 **dns**, **interface** 및 **trustpoint** 명령은 관리 컨텍스트에 상주하고 **call-home** 명령은 시스템 컨텍스트에 상주합니다.
- CA 서버의 자체 서명된 인증서가 변경되는 경우 해당 Smart Call Home이 활성 상태로 남아 있을 수 있도록 신뢰 풀 번들의 업데이트를 주기적으로 자동화할 수 있습니다. 다중 상황 구축에서는 이 신뢰 풀 자동 갱신 기능이 지원되지 않습니다.

Smart Call Home 지침

- 다중 컨텍스트 모드에서 subscribe-to-alert-group snapshot periodic 명령은 두 명령으로 분리됩니다. 하나는 시스템 컨피그레이션에서 정보를 가져오는 것이고 하나는 사용자 컨텍스트에서 정보를 가져오는 것입니다.
- Smart Call Home 백엔드 서버는 XML 형식의 메시지만 수락할 수 있습니다.
- 클러스터링을 활성화하고 위험 심각도 수준의 진단 경고 그룹에 등록하도록 Smart Call Home을 구성한 경우 Smart Call Home 메시지가 Cisco에 전달되어 중요한 클러스터 이벤트를 보고합니다. 다음 이벤트에 대해서만 Smart Call Home 클러스터링 메시지가 전송됩니다.
  - 유닛이 클러스터에 참여할 때
  - 유닛이 클러스터를 떠날 때
  - 클러스터 유닛이 클러스터 마스터가 될 때
  - 보조 유닛이 클러스터에서 실패할 때

  전송되는 각 메시지는 다음 정보를 포함합니다.
  - 액티브 클러스터 멤버 수
  - 클러스터 마스터에서 **show cluster info** 명령과 **show cluster history** 명령의 출력

Anonymous Reporting 및 Smart Call Home 구성

Anonymous Reporting은 Smart Call Home 서비스의 일부이며 Cisco가 디바이스로부터 최소한의 오류 및 상태 정보를 익명으로 수신할 수 있게 하지만 Smart Call Home 서비스는 Cisco TAC가 디바이스를 모니터링하고 문제가 있을 때 케이스를 열 수 있도록 시스템 상태에 대한 맞춤 지원을 제공하기도 합니다. 귀하가 문제 발생 사실을 알기 전에 케이스가 열리는 경우도 많습니다.

시스템에 대해 두 서비스 모두 동시에 구성할 수 있습니다. 다만 Smart Call Home 서비스를 구성하면 Anonymous Reporting과 동일한 기능에 맞춤 서비스가 추가로 제공됩니다.

컨피그레이션 모드로 들어가면 다음 지침에 따라 Anonymous Reporting 및 Smart Call Home을 활성화하라는 메시지가 표시됩니다.

- 프롬프트에서 [Y]es, [N]o 또는 [A]sk later를 선택할 수 있습니다. [A]sk later를 선택하면 7일 후 또는 ASA가 다시 로드될 때 다시 물어봅니다. 계속 [A]sk later를 선택하면 ASA가 7일 간격으로 두 번 더 물어본 후 [N]o로 응답한 것으로 간주하고 다시 물어보지 않습니다.
- 프롬프트를 받지 못한 경우 Anonymous Reporting 구성, 1350 페이지 또는 Smart Call Home 구성, 1350 페이지의 단계에 따라 Anonymous Reporting 또는 Smart Call을 활성화할 수 있습니다.

Anonymous Reporting 구성

Anonymous Reporting을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** Anonymous Reporting 기능을 활성화하고 새 익명 프로필을 만듭니다.

call-home reporting anonymous

예제:

```
ciscoasa(config)# call-home reporting anonymous
```

이 명령을 입력하면 신뢰 지점이 생성되고 Cisco 웹 서버의 ID를 확인하는 데 사용되는 인증서가 설치됩니다.

단계 **2** (선택 사항) 서버에 연결되어 있고 시스템이 메시지를 전송할 수 있는지 확인하십시오.

call-home test reporting anonymous

예제:

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

성공 또는 오류 메시지로 테스트 결과가 반환됩니다.

Smart Call Home 구성

ASA에서의 Smart Call Home 서비스 구성은 다음 작업을 포함합니다.

프로시저

단계 **1** Smart Call Home 서비스를 활성화합니다. Smart Call Home 활성화, 1351 페이지를 참조하십시오.

단계 **2** 가입자에게 Smart Call Home 메시지를 전달하는 메일 서버를 구성합니다. 메일 서버 구성, 1356 페이지를 참조하십시오.

단계 **3** Smart Call Home 메시지에 대한 연락 정보를 설정합니다. 고객 연락처 정보 구성, 1354 페이지를 참조하십시오.

단계 **4** 처리할 수 있는 최대 이벤트 속도와 같이 경고 처리 매개변수를 정의합니다. 경보 그룹 서브스크립션 구성, 1353 페이지를 참조하십시오.

단계 **5** 경고 서브스크립션 프로필을 설정합니다. 대상 프로필 구성, 1358 페이지를 참조하십시오.

각 경고 서브스크립션 프로필은 다음을 식별합니다.

- Cisco의 Smart Call Home 서버 또는 이메일 수신자 목록과 같이 Smart Call Home 메시지가 전송된 가입자.
- 컨피그레이션 또는 인벤토리 정보와 같이 경고를 받으려는 정보 범주.

Smart Call Home 활성화

Smart Call Home과 call-home 프로필을 활성화하려면 다음 단계를 수행합니다.

프로시저

단계 **1** Smart Call Home 서비스를 활성화합니다.

service call-home

예제:

```
ciscoasa(config)# service call-home
```

단계 **2** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제:

```
ciscoasa(config)# call home
```

CA 신뢰 포인트를 선언 및 인증

Smart Call Home이 HTTPS를 통해 웹 서버로 메시지를 보내도록 구성된 경우 웹 서버의 인증서 또는 인증서를 발급한 CA(Certificate Authority)의 인증서를 신뢰하도록 ASA를 구성해야 합니다. Cisco Smart Call Home 프로덕션 서버 인증서는 Verisign에서 발급합니다. Cisco Smart Call Home Staging 서버 인증서는 Digital Signature Trust Company에서 발급합니다.

참고 no client-types/no validation-usage에 대한 신뢰 지점을 설정하여 VPN 확인에 사용되지 않도록 해야 합니다.

Smart Call Home 서비스를 위해 Cisco 서버 보안 인증서를 선언 및 확인하고 HTTPS 서버와의 통신을 설정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** (다중 컨텍스트 모드에만 해당) 관리자 컨텍스트 내에서 인증서를 설치합니다.

changeto context *admincontext*

예제:

```
ciscoasa(config)# changeto context contextA
```

단계 **2** 신뢰 지점을 구성하고 인증서 등록을 준비합니다.

crypto ca trustpoint *trustpoint_name*

예제:

```
ciscoasa(config)# crypto ca trustpoint cisco
```

참고 전송 방법으로 HTTPS를 이용하는 경우 신뢰 지점을 통해 보안 인증서를 설치해야 합니다. 다음 URL에서 설치할 인증서를 찾을 수 있습니다.

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

단계 **3** 인증서 등록 방법으로 수동 붙여넣기를 지정합니다.

enroll terminal

예제:

```
ciscoasa(ca-trustpoint)# enroll terminal
```

단계 **4** 지정된 CA를 인증합니다. CA 이름이 **crypto ca trustpoint** 명령에 지정된 신뢰 지점 이름과 일치해야 합니다. 프롬프트에서 보안 인증서 텍스트를 붙여넣습니다.

crypto ca authenticate trustpoint

예제:

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

단계 **5** 보안 인증서 텍스트 끝을 지정하고 입력한 보안 인증서의 수락을 확인합니다.

quit

예제:

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

환경 및 스냅샷 경보 그룹 구성

환경 및 스냅샷 경고 그룹을 구성하려면 다음 단계를 수행합니다.

프로시저

경고 그룹 컨피그레이션 모드로 들어갑니다.

alert-group-config {**environment** | **snapshot**}

예제:

```
ciscoasa(config)# alert-group-config environment
```

경보 그룹 서브스크립션 구성

목적지 프로필을 경고 그룹에 등록하려면 다음 단계를 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제:

```
ciscoasa(config)# call-home
```

단계 **2** 지정된 Smart Call Home 경고 그룹을 활성화합니다.

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

예제**:**

```
ciscoasa(cfg-call-home)# alert-group syslog
```

모든 경고 그룹을 활성화하려면 **all** 키워드를 사용합니다. 기본적으로 모든 경고 그룹이 활성화됩니다.

단계 **3** 지정된 목적지 프로필에 대한 프로필 컨피그레이션 모드로 들어갑니다.

profile *profile-name*

예제**:**

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

단계 **4** 이용 가능한 모든 경고 그룹에 등록합니다.

subscribe-to-alert-group all

예제**:**

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

단계 **5** 이 목적지 프로필을 컨피그레이션 경고 그룹에 등록합니다.

subscribe-to-alert-group configuration periodic { **daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

예제**:**

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

periodic 키워드는 정기 알림을 위해 구성 알림 그룹을 구성합니다. 기본 기간은 매일입니다.

daily 키워드는 *hh:mm* 형식의 24시간제로 전송 시간을 지정합니다(예: 14:30).

weekly 키워드는 *day hh:mm* 형식으로 전송 요일과 시간을 지정하며 요일은 풀어서 씁니다(예: Monday).

monthly 키워드는 1부터 31까지의 숫자와 시간을 *date hh:mm* 형식으로 지정합니다.

고객 연락처 정보 구성

고객 연락처 정보를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제:

```
ciscoasa(config)# call-home
```

단계 **2** 고객 전화 번호를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

phone-number *phone-number-string*

예제:

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

단계 **3** 길이가 최대 255자인 자유 형식 문자열로 고객 주소를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

street-address *street-address*

예제:

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

단계 **4** 최대 128자 길이의 고객 이름을 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

contact-name *contact-name*

예제:

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

단계 **5** 최대 64자 길이의 Cisco 고객 ID를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

customer-id *customer-id-string*

예제:

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

단계 **6** 최대 64자 길이의 고객 사이트 ID를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

site-id *site-id-string*

예제:

```
ciscoasa(cfg-call-home)# site-id site1234
```

단계 **7** 최대 128자 길이의 고객 계약 ID를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

contract-id *contract-id-string*

예제**:**

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

예

다음 예는 연락처 정보 구성 방법을 보여줍니다.

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

메일 서버 구성

메시지 전송을 위해 가장 안전한 HTTPS를 사용하는 것이 좋습니다. 그러나 Smart Call Home을 위한 이메일 목적지를 구성한 다음 메일 서버가 이메일 메시지 전송을 사용하도록 구성할 수 있습니다.

메일 서버를 구성하려면 다음 작업을 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제**:**

```
ciscoasa(config)# call-home
```

단계 **2** SMTP 메일 서버를 지정합니다.

mail-server*ip-address* **name priority** [**1-100**] [**all**]

예제**:**

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

5개의 분리된 명령을 사용하여 최대 5개의 메일 서버를 지정할 수 있습니다. Smart Call Home 메시지 이메일 전송에 사용할 메일 서버를 하나 이상 구성해야 합니다.

숫자가 낮을수록 메일 서버의 우선 위가 높습니다.

ip-address 인수는 IPv4 또는 IPv6 메일 서버 주소가 될 수 있습니다.

예

다음 예는 기본 메일 서버(이름이 "smtp.example.com"로 지정됨)와 IP 주소 10.10.1.1의 보조 메일 서버를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

트래픽 속도 제한 구성

트래픽 속도 제한을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제**:**

```
ciscoasa(config)# call-home
```

단계 **2** Smart Call Home이 1분에 보낼 수 있는 메시지 수를 지정합니다. 기본값은 분당 10개의 메시지입니다.

rate-limit *msg-count*

예제**:**

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Smart Call Home 통신 전송

특정 Smart Call Home 통신을 보내려면, 다음 단계를 수행하십시오.

프로시저

다음 옵션 중 하나를 선택합니다.

- 옵션 1 — 프로필 구성을 사용하여 테스트 메시지를 수동으로 보냅니다.

  call-home test [*test-message*] **profile** *profile-name*

  예:

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- 옵션 2 — 대상 프로필이 지정되어 있다면 하나의 대상 프로필로 경보 그룹 메시지를 보냅니다. 프로필이 지정되지 않은 경우 인벤토리, 컨피그레이션, 스냅샷 또는 텔레메트리 경고 그룹에 등록된 모든 프로필로 메시지를 보냅니다.

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  예:

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- 옵션 3 — 명령 출력을 이메일 주소로 보냅니다. 지정된 CLI 명령은 모든 등록 모듈에 대한 명령을 포함하여 어떤 명령이라도 될 수 있습니다.

  call-home send*cli command* [**email** *email*]

  예:

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  이메일 주소를 지정하면 명령 출력이 해당 주소로 전송됩니다. 이메일 주소가 지정되지 않은 경우 출력이 Cisco TAC에 전송 됩니다. 이메일은 제목 줄에 서비스 번호(지정된 경우)를 포함하여 로그 텍스트 형식으로 전송됩니다.

  서비스 번호는 지정된 이메일 주소가 없거나 Cisco TAC 이메일 주소가 지정된 경우에만 필요합니다.

대상 프로필 구성

이메일 또는 HTTP에 대한 목적지 프로필을 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제:

```
ciscoasa(config)# call-home
```

단계 **2** 지정된 목적지 프로필에 대한 프로필 컨피그레이션 모드로 들어갑니다. 지정 목적지 프로필이 존재하지 않는 경우 프로필이 생성됩니다.

profile *profile-name*

예제:

```
ciscoasa(cfg-call-home)# profile newprofile
```

최대 10개의 액티브 프로필을 생성할 수 있습니다. 기본 프로필은 Cisco TAC로 다시 보고하는 것입니다. 콜 홈 정보를 다른 위치(예: 자체 서버)로 보내고 싶다면 별도의 프로필을 생성할 수 있습니다.

단계 **3** Smart Call Home 메시지 수신기의 목적지, 메시지 크기, 메시지 형식, 전송 방식을 구성합니다. 기본 메시지 형식은 XML이며 기본적으로 활성화된 라우팅 방법은 이메일입니다.

destination address { **email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

예제:

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

reference-identity 옵션은 수신한 서버 인증서에 대한 RFC 6125 참조 id 검사를 활성화합니다. 이 검사는 http 주소를 사용하여 구성된 대상에만 적용됩니다. ID 검사는 이전에 구성된 참조 id 개체를 기반으로 이루어집니다. 참조 ID 개체에 대한 자세한 내용은 참조 ID 구성, 754 페이지을 참조하십시오.

이메일 주소는 최대 100자가 될 수 있는 Smart Call Home 메시지 수신자의 이메일 주소입니다. 기본적으로 최대 URL 크기는 5MB입니다.

모바일 디바이스에서는 단문 형식으로 컴퓨터에서는 장문 형식으로 메시지를 보내고 읽으십시오.

메시지 수신자가 Smart Call Home 백엔드 서버인 경우 **preferred-msg-format** 값이 XML인지 확인하십시오. 백엔드 서버는 XML 형식의 메시지만 수신할 수 있습니다.

이 명령을 사용하여 전송 방식을 다시 이메일로 바꿀 수 있습니다.

대상 프로필 복사

기존 목적지 프로필을 복사하여 새 프로필을 생성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제**:**

```
ciscoasa(config)# call-home
```

단계 **2** 복사할 프로필을 지정합니다.

profile *profile-name*

예제**:**

```
ciscoasa(cfg-call-home)# profile newprofile
```

단계 **3** 기존 프로필 내용을 새 프로필에 복사합니다.

copy profile *src-profile-name dest-profile-name*

예제**:**

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

기존 프로필(*src-profile-name*)및 새 프로필(*dest-profile-name*)최대 길이는 23자입니다.

예

다음 예는 기존 프로필을 복사하는 방법을 보여줍니다.

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

대상 프로필 이름 변경

기존 프로필의 이름을 변경하려면 다음 단계를 수행합니다.

프로시저

단계 **1** call-home 컨피그레이션 모드로 들어갑니다.

call-home

예제**:**

```
ciscoasa(config)# call-home
```

단계 **2** 이름을 바꿀 프로필을 지정합니다.

profile *profilename*

예제**:**

```
ciscoasa(cfg-call-home)# profile newprofile
```

단계 **3** 기존 프로필 이름을 변경합니다.

rename profile *src-profile-name dest-profile-name*

예제**:**

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

기존 프로필(*src-profile-name*)및 새 프로필(*dest-profile-name*)최대 길이는 23자입니다.

예

다음 예는 기존 프로필 이름을 변경하는 방법을 보여줍니다.

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

Anonymous Reporting 및 Smart Call Home 모니터링

Anonymous Reporting 및 Smart Call Home 서비스 모니터링은 다음 명령을 참고하십시오.

- **show call-home detail**

  이 명령은 현재 Smart Call Home 세부 사항 컨피그레이션을 표시합니다.

- **show call-home mail-server status**

  이 명령은 현재 메일 서버 상태를 표시합니다.

- **show call-home profile** {profile name | **all**}

  이 명령은 Smart Call Home 프로필의 컨피그레이션을 보여줍니다.

- **show call-home registered-module status** [**all**]

  이 명령은 등록된 모듈 상태를 표시합니다.

- **show call-home statistics**

  이 명령은 콜 홈 세부 정보 상태를 표시합니다.

- **show call-home**

  이 명령은 현재 Smart Call Home 컨피그레이션을 표시합니다.

- **show running-config call-home**

  이 명령은 현재 Smart Call Home 실행 컨피그레이션을 표시합니다.

- **show smart-call-home alert-group**

  이 명령은 Smart Call Home 경고 그룹의 현재 상태를 표시합니다.

- **show running-config all**

  이 명령은 Anonymous Reporting 사용자 프로필에 대한 세부 정보를 표시합니다.

Smart Call Home의 예

다음 예는 Smart Call Home 서비스 구성 방법을 보여줍니다.

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly Monday
 23:30
```

Anonymous Reporting 및 Smart Call Home 내역

표 *64: Anonymous Reporting* 및 *Smart Call Home* 내역

기능 이름	플랫폼 릴리스	설명
Smart Call Home	8.2(2)	Smart Call Home 서비스는 ASA에 대한 사전 예방적 진단 및 실시간 경고를 제공하고 더욱 뛰어난 네트워크 가용성과 운영 효율성을 실현합니다. 다음 명령을 도입하거나 수정했습니다. **active (call home)**, **call-home, call-home send alert-group, call-home test, contact-email-addr**, **customer-id (call home)**, **destination (call home)**, **profile**, **rename profile**, **service call-home, show call-home, show call-home detail**, **show smart-call-home alert-group**, **show call-home profile**, **show call-home statistics**, **show call-home mail-server status**, **show running-config call-home**, **show call-home registered-module status all**, **site-id**, **street-address**, **subscribe-to-alert-group all**, **alert-group-config**, **subscribe-to-alert-group configuration**, **subscribe-to-alert-group diagnostic**, **subscribe-to-alert-group environment**, **subscribe-to-alert-group inventory periodic**, **subscribe-to-alert-group snapshot periodic**, **subscribe-to-alert-group syslog**, **subscribe-to-alert-group telemetry periodic**.
Anonymous Reporting	9.0(1)	Anonymous Reporting을 활성화하면 Cisco가 안전하게 디바이스에서 최소 오류 및 상태 정보를 받을 수 있으므로 ASA 플랫폼 개선에 도움이 됩니다. 다음 화면을 도입했습니다. **call-home reporting anonymous**, **call-home test reporting anonymous**.

기능 이름	플랫폼 릴리스	설명
Smart Call Home	9.1(2)	**show local-host** 명령이 텔레메트리 경고 그룹 보고를 위해 **show local-host | include interface** 명령으로 변경되었습니다.
Smart Call Home	9.1(3)	클러스터링을 활성화하고 위험 심각도 수준의 진단 경고 그룹에 등록하도록 Smart Call Home을 구성한 경우 Smart Call Home 메시지가 Cisco에 전달되어 중요한 클러스터 이벤트를 보고합니다. 다음 3가지 이벤트에 대해서만 Smart Call Home 클러스터링 메시지가 전송됩니다. • 유닛이 클러스터에 참여할 때 • 유닛이 클러스터를 떠날 때 • 클러스터 유닛이 클러스터 마스터가 될 때 전송되는 각 메시지는 다음 정보를 포함합니다. • 액티브 클러스터 멤버 수 • 클러스터 마스터에서 **show cluster info** 명령과 **show cluster history** 명령의 출력
보안 Smart Call Home 서버 연결을 위한 참조 ID	9.6(2)	이제 TLS 클라이언트 처리 시 RFC 6125, 섹션 6에 정의되어 있는 서버 ID를 확인하기 위해 규칙을 지원합니다. ID 확인은 Smart Call Home 서버에 대한 TLS 연결을 대상으로 PKI 검증을 하는 동안에만 수행됩니다. 표시되는 ID가 구성된 참조 ID에 대해 일치될 수 없는 경우 연결이 설정되지 않습니다. 추가 또는 수정된 명령: **[no] crypto ca reference-identity**, **call home profile destination address http**

IX 부

참조

45 장

명령줄 인터페이스 사용

이 장에서는 Cisco ASA에서 CLI를 사용하는 방법에 대해 설명합니다.

참고 CLI는 Cisco IOS CLI와 유사한 구문 및 규칙을 사용하지만 ASA 운영 체제는 Cisco IOS 소프트웨어 버전이 아닙니다. Cisco IOS CLI 명령이 ASA와 함께 작동하거나 동일한 기능을 갖추었다고 가정하지 마십시오.

방화벽 모드 및 보안 상황 모드

ASA는 다음 모드의 조합에서 실행됩니다.

- 투명 방화벽 또는 라우팅 방화벽 모드

  방화벽 모드는 ASA가 계층 2 방화벽으로 실행되는지 또는 계층 3 방화벽으로 실행되는지를 결정합니다.

- 다중 상황 또는 단일 상황 모드

  보안 상황 모드에서는 ASA가 단일 디바이스 또는 가상 디바이스 역할을 하는 다중 보안 상황으로 실행되는지 결정합니다.

일부 명령은 특정 모드에서만 사용할 수 있습니다.

명령 모드 및 프롬프트

ASA CLI에는 명령 모드가 포함되어 있습니다. 일부 명령은 특정 모드에서만 입력할 수 있습니다. 예를 들어 민감한 정보를 표시하는 명령을 입력하려면 비밀번호를 입력하고 특권 모드로 전환해야 합니다. 그런 다음 구성 변경을 실수로 입력하는 일이 없도록 우선 구성 모드로 전환해야 합니다. 상위 모드에서는 모든 하위 명령을 입력할 수 있습니다. 예를 들어 전역 구성 모드에서 특권 EXEC 명령을 입력할 수 있습니다.

참고 여러 유형의 프롬프트는 모두 기본 프롬프트이며, 구성된 경우에는 다를 수 있습니다.

- 시스템 구성 또는 단일 상황 모드에서는 프롬프트가 호스트 이름으로 시작합니다.

  ```
  ciscoasa
  ```

- 프롬프트 문자열을 인쇄할 때는 프롬프트 구성이 구문 분석되고 구성 키워드 값이 prompt 명령을 설정한 순서대로 인쇄됩니다. 키워드 인수는 hostname, domain, context, priority, state 중 하나일 수 있습니다(열거 순서와 무관).

  prompt hostname context priority state

- 상황 내에 있을 경우, 프롬프트는 호스트 이름으로 시작하고 그 다음 상황 이름이 옵니다.

  ```
  ciscoasa/context
  ```

프롬프트는 액세스 모드에 따라 변경됩니다.

- 사용자 EXEC 모드

  사용자 EXEC 모드에서는 최소 ASA 설정을 볼 수 있습니다. 먼저 ASA에 액세스한 경우 사용자 EXEC 모드 프롬프트는 다음과 같이 표시됩니다.

  ```
  ciscoasa>
  ciscoasa/context>
  ```

- 특권 EXEC 모드

  특권 EXEC 모드에서는 특권 수준까지의 모든 현재 설정을 볼 수 있습니다. 모든 사용자 EXEC 명령이 특권 EXEC 모드에서 작동합니다. 사용자 EXEC 모드에서 **enable** 명령을 입력하면(비밀

번호가 필요함) 특권 EXEC 모드가 시작됩니다. 프롬프트에는 번호 기호(#)가 포함되어 있습니다.

```
ciscoasa#

ciscoasa/context#
```

- 전역 구성 모드

  전역 구성 모드에서 ASA 구성을 변경할 수 있습니다. 모든 사용자 EXEC, 특권 EXEC 및 전역 구성 명령을 이 모드에서 사용할 수 있습니다. 특권 EXEC 모드에서 **configure terminal** 명령을 입력하면 전역 구성 모드가 시작됩니다. 프롬프트가 다음으로 변경됩니다.

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- 명령별 구성 모드

  전역 구성 모드에서 일부 명령은 명령별 구성 모드를 시작합니다. 모든 사용자 EXEC, 특권 EXEC, 전역 구성 및 명령별 구성 명령을 이 모드에서 사용할 수 있습니다. 예를 들어 **interface** 명령은 인터페이스 구성 모드를 시작합니다. 프롬프트가 다음으로 변경됩니다.

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

구문 형식 지정

명령 구문 설명에서는 다음 표에 나열된 규칙을 사용합니다.

표 ***65:*** 구문 규칙

표기 규칙	설명
굵은 글꼴	굵은 텍스트는 표시된 대로 입력할 명령 및 키워드를 나타냅니다.
기울임꼴	기울임꼴 텍스트는 값을 제공할 인수를 나타냅니다.
[x]	선택적 요소(키워드 또는 인수)를 대괄호로 묶습니다.
|	세로 막대는 선택적 또는 필수 키워드 또는 인수 집합 내에서 선택할 수 있음을 나타냅니다.
[x | y]	대괄호 안의 세로 막대로 구분된 키워드 또는 인수는 선택사항을 나타냅니다.
{x | y}	중괄호 안의 세로 막대로 구분된 키워드 또는 인수는 필수 선택 항목을 나타냅니다.

표기 규칙	설명
[x {y | z}]	중첩된 대괄호 또는 중괄호 집합은 선택 요소 또는 필수 요소 내의 선택사항 또는 필수 선택 항목을 나타냅니다. 대괄호 안의 중괄호 및 세로 막대는 선택 요소 내의 필수 선택 항목을 나타냅니다.

명령 약어 지정

대부분의 명령을 최소한의 고유한 명령 문자로 축약할 수 있습니다. 예를 들어 **wr t**를 전체 명령 **write terminal**을 입력하는 대신 입력하여 구성을 보거나, **en**을 입력하여 특권 모드를 시작하고 **conf t** 를 입력하여 구성 모드를 시작할 수 있습니다. 또한 **0**을 입력하여 **0.0.0.0**을 나타낼 수 있습니다.

명령줄 편집

ASA에서는 Cisco IOS 소프트웨어와 동일한 명령줄 편집 표기 규칙을 사용합니다. **show history** 명령을 사용하여 이전에 입력한 모든 명령을 보거나 위쪽 화살표 또는 **^p** 명령을 사용하여 개별적으로 볼 수 있습니다. 이전에 입력한 명령을 검토한 후에는 아래쪽 화살표 **^n** 명령을 사용하여 목록에서 앞으로 이동할 수 있습니다. 재사용할 명령에 도달하면 해당 명령을 편집하거나 **Enter** 키를 눌러 명령을 시작할 수 있습니다. 또한 **^w**를 사용하여 커서 왼쪽에 있는 단어를 삭제하거나 **^u**를 사용하여 행을 지울 수 있습니다.

ASA에서는 명령에 최대 512자를 입력할 수 있으며, 추가 문자는 무시됩니다.

명령 완성

부분 문자열을 입력한 후 명령 또는 키워드를 완성하려면 **Tab** 키를 누릅니다. ASA에서는 부분 문자열이 하나의 명령 또는 키워드와 일치하는 경우에만 명령 또는 키워드를 완성합니다. 예를 들어 **s**를 입력하고 **Tab** 키를 누른 경우 이는 둘 이상의 명령과 일치하므로 ASA에서 명령을 완성하지 않습니다. 그러나 **dis**를 입력하고 **Tab** 키를 누르면 **disable** 명령이 완성됩니다.

명령 도움말

다음 명령을 입력하여 커맨드 라인에서 도움말 정보를 사용할 수 있습니다.

- **help** *command_name*

  특정 명령에 대한 도움말을 표시합니다.

- *command_name* **?**

  사용 가능한 인수 목록을 표시합니다.

- *string***?** (공백 없음)

이 문자열로 시작할 수 있는 명령을 나열합니다.

- **?** 및 **+?**

  사용 가능한 모든 명령을 나열합니다. **?**를 입력한 경우 ASA에서는 현재 모드에 사용 가능한 명령만 표시합니다. 하위 모드의 명령을 포함하여 사용 가능한 모든 명령을 표시하려면 **+?**를 입력합니다.

참고 명령 문자열에 물음표(?)를 포함하려면 물음표를 입력하기 전에 **Ctrl-V**를 눌러서 CLI 도움말이 실수로 호출되지 않도록 해야 합니다.

실행 중인 구성 보기

실행 중인 구성을 보려면 다음 명령 중 하나를 사용합니다.

- **show running-config** [**all**] [*command*]

  all을 지정하면 모든 기본 설정도 표시됩니다. *command*를 지정하면 출력에 관련 명령만 포함됩니다.

  참고 대다수의 비밀번호는 *****로 표시됩니다. 비밀번호를 일반 텍스트로 보거나 마스터 패스프레이즈가 활성화된 경우 암호화된 형식으로 보려면 **more** 명령을 사용합니다.

- **more system:running-config**

필터 표시 및 추가 명령 출력

show 명령에서 세로 막대(|)를 사용하여 필터 옵션 및 필터링 식을 포함할 수 있습니다. 필터링은 Cisco IOS 소프트웨어와 마찬가지로 각 출력 행을 정규식과 일치하여 수행합니다. 다른 필터 옵션을 선택하여 식과 일치하는 모든 출력을 포함하거나 제외할 수 있습니다. 또한 해당 식과 일치하는 행으로 시작되는 모든 출력도 표시할 수 있습니다.

show 명령에서 필터링 옵션을 사용하는 구문은 다음과 같습니다.

show *command* | {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

또는

more system:running-config| {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

참고 **more** 명령을 입력하면 실행 중인 구성뿐만 아니라 모든 파일의 내용을 볼 수 있습니다. 자세한 내용은 명령 참조를 참고하십시오.

이 명령 문자열에서 첫 번째 세로 막대(|)는 연산자이며 명령에 꼭 포함되어야 합니다. 이 연산자는 **show** 명령의 출력을 필터링하도록 지시합니다. 구문 다이어그램에서 다른 세로 막대 (|)는 대체 옵션을 나타내며, 명령의 일부가 아닙니다.

include 옵션은 정규식과 일치하는 모든 출력 행을 포함합니다. **-v**가 포함되지 않은 **grep** 옵션도 동일한 효과를 가집니다. **exclude** 옵션은 정규식과 일치하는 모든 출력 행을 제외합니다. **-v**가 포함된 **grep** 옵션도 동일한 효과를 가집니다. **begin** 옵션은 정규식과 일치하는 행으로 시작하는 모든 출력 행을 표시합니다.

*regexp*를 Cisco IOS 정규식으로 대체합니다. 정규식은 따옴표 또는 큰따옴표로 묶이지 않으므로 후행 공백에 주의해야 합니다. 후행 공백은 정규식의 일부로 간주됩니다.

정규식을 만들 때 일치시킬 문자나 숫자를 사용할 수 있습니다. 또한 *metacharacters*라는 특정 키워드 문자는 정규식에서 사용될 때 특별한 의미를 가집니다.

CLI에서 물음표(?) 또는 탭 같은 모든 특수 문자를 이스케이프하려면 **Ctrl+V**를 사용합니다. 예를 들어 **d[Ctrl+V]?g**를 입력하여 구성에서 **d?g**를 입력할 수 있습니다.

show 명령 출력 리디렉션 및 추가

화면에 **show** 명령의 출력을 표시하는 대신 디바이스 또는 원격 위치에 있는 파일로 리디렉션할 수 있습니다. 디바이스에 있는 파일로 리디렉션하는 경우, 파일에 명령 출력을 추가할 수도 있습니다.

show *command* | {**append** | **redirect**} *url*

- **append** *url*은 출력을 기존 파일에 추가합니다. 다음 중 하나를 사용하여 파일을 지정합니다.
  - **disk0:**/[[*path/*]*filename*] 또는 **flash:**/[[*path/*]*filename*] — **flash** 및 **disk0** 모두 내부 플래시 메모리를 표시합니다. 옵션 중 하나를 사용할 수 있습니다.
  - **disk1:**/[[*path/*]*filename*] — 외부 메모리를 나타냅니다.
- **redirect** *url*은 지정된 파일을 생성하거나 파일이 이미 있는 경우 이를 덮어씁니다.
  - **disk0:**/[[*path/*]*filename*] 또는 **flash:**/[[*path/*]*filename*] — **flash** 및 **disk0** 모두 내부 플래시 메모리를 표시합니다. 옵션 중 하나를 사용할 수 있습니다.
  - **disk1:**/[[*path/*]*filename*] — 외부 메모리를 나타냅니다.
  - **smb:**/[[*path/*]*filename*] — 서버 메시지 블록, UNIX 서버 로컬 파일 시스템을 표시합니다.
  - **ftp:**//[[*user*[**:***password*]@] *server*[*:port*]/[*path/*] *filename*[**;type=***xx*]] — SCP 서버를 나타냅니다. **type**은 다음 키워드 중 하나가 될 수 있습니다. **ap**(ASCII 패시브 모드), **an**(ASCII 일반 모드), **ip**(기본값—바이너리 패시브 모드), **in**(바이너리 일반 모드).

- **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]] — **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다.
- **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] — TFTP 서버를 나타냅니다. 경로 이름은 공백을 포함할 수 없습니다. **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다.

show 명령 출력에 대한 라인 수 가져오기

show 명령 출력을 실제로 확인하는 대신 출력에서 행 수 또는 표현식과 일치하는 행 수를 간단하게 확인할 수 있습니다. 그런 다음 명령을 입력한 이전 횟수와 행 수를 쉽게 비교할 수 있습니다. 이렇게 하면 신속하게 구성하는 것처럼 빨리 확인할 수 있습니다. **count** 키워드를 사용하거나 **-c**를 grep 키워드에 추가할 수 있습니다.

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

*regular_expression*을 Cisco IOS 정규식으로 대체합니다. 정규식은 따옴표 또는 큰따옴표로 묶이지 않으므로 후행 공백에 주의해야 합니다. 후행 공백은 정규식의 일부로 간주됩니다. 정규식은 선택 사항입니다. 포함하지 않을 경우 카운트가 필터링되지 않은 출력의 총 행 수를 반환합니다.

정규식을 만들 때 일치시킬 문자나 숫자를 사용할 수 있습니다. 또한 metacharacters라는 특정 키워드 문자는 정규식에서 사용될 때 특별한 의미를 가집니다. CLI에서 물음표(?) 또는 탭 같은 모든 특수 문자를 이스케이프하려면 Ctrl+V를 사용합니다. 예를 들어 **d[Ctrl+V]?g**를 입력하여 구성에서 **d?g**를 입력할 수 있습니다.

예를 들어, **show running-config** 출력에서 모든 행의 총 수를 표시합니다.

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

다음 예에서는 가동 중인 인터페이스 수가 얼마나 많은지 신속하게 확인하는 방법을 보여 줍니다. 첫 번째 예에서는 가동 상태로 표시되는 행에서만 필터링하도록 정규식이 있는 **grep** 키워드를 사용하는 방법을 보여 줍니다. 다음 예에서는 출력의 실제 행 대신 카운트를 간단히 표시하기 위해 **-c** 옵션을 추가합니다.

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
Number of lines which match regexp = 2
```

명령 출력 페이징

help 또는 **?**, **show**, **show xlate** 또는 그 밖에 긴 목록을 제공하는 명령의 경우 정보가 화면에 표시되고 일시 중지되는지 또는 명령을 완성하도록 해주는지 확인할 수 있습니다. **pager** 명령을 사용하면 More(추가) 프롬프트가 나타나기 전에 표시할 행의 수를 선택할 수 있습니다.

페이징이 활성화된 경우 다음 프롬프트가 나타납니다.

```
<--- More --->
```

More 프롬프트에서는 UNIX **more** 명령과 유사한 구문을 사용합니다.

- 다른 화면을 보려면 스페이스바 키를 누릅니다.
- 다음 행을 보려면 **Enter** 키를 누릅니다.
- 명령줄로 돌아가려면 q 키를 누릅니다.

코멘트 추가

콜론(:)을 행 앞에 입력하여 주석을 만들 수 있습니다. 그러나 주석은 명령 기록 버퍼에만 표시되고 구성에는 표시되지 않습니다. 따라서 **show history** 명령을 사용하거나, 화살표 키를 눌러 이전 명령을 검색하여 주석을 볼 수는 있지만, 주석은 구성에 없으므로 **write terminal** 명령은 주석을 표시하지 않습니다.

텍스트 구성 파일

이 섹션에서는 ASA에 다운로드할 수 있는 텍스트 구성 파일의 형식을 지정하는 방법에 대해 설명합니다.

명령이 텍스트 파일의 행과 일치하는 방식

텍스트 구성 파일에는 이 가이드에 설명된 명령과 대응하는 행이 포함되어 있습니다.

예를 들어, 명령은 CLI 프롬프트 앞에 옵니다. 다음 예의 프롬프트는 “ciscoasa(config)#”입니다.

```
ciscoasa(config)# context a
```

텍스트 구성 파일에서는 명령을 입력하라는 프롬프트가 나타나지 않으므로 프롬프트가 생략됩니다.

```
context a
```

명령별 구성 모드 명령

명령별 구성 모드 명령은 명령줄에 입력할 경우 기본 명령 아래에 들여 쓴 형태로 표시됩니다. 텍스트 파일 행의 경우 명령이 기본 명령 다음에 바로 표시되기만 하면 들여 쓰지 않아도 됩니다. 예를 들어 다음 들여쓰기되지 않은 텍스트는 들여쓰기된 텍스트와 동일하게 해석됩니다.

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

자동 텍스트 항목

구성을 ASA에 다운로드할 경우, 일부 행이 자동으로 삽입됩니다. 예를 들어, ASA에서는 기본 설정 또는 구성이 수정된 시간에 대한 행을 삽입합니다. 텍스트 파일을 만들 때 이러한 자동 항목을 입력할 필요가 없습니다.

행 순서

대부분의 경우 명령은 파일에서 정해진 순서가 없습니다. 그러나 ACE 같은 일부 행의 경우 표시되는 순서대로 처리되며, 이러한 순서는 액세스 목록의 기능에 영향을 미칠 수 있습니다. 다른 명령에도 순서 요건이 있을 수 있습니다. 예를 들어 많은 후속 명령에서 인터페이스 이름을 사용하는 경우 먼저 인터페이스에 대한 **nameif** 명령을 입력해야 합니다. 또한 명령별 구성 모드의 명령은 기본 명령 바로 다음에 와야 합니다.

텍스트 구성에 포함되지 않은 명령

일부 명령의 경우 구성에 행을 삽입하지 않습니다. 예를 들어, **show running-config** 같은 런타임 명령의 경우 텍스트 파일에 해당 행이 없습니다.

비밀번호

로그인, 활성화 및 사용자 비밀번호는 구성에 저장되기 전에 자동으로 암호화됩니다. 예를 들어 비밀번호 “cisco”의 암호화된 형식은 jMorNbK0514fadBh처럼 나타날 수 있습니다. 구성 비밀번호를 암호화된 형식으로 다른 ASA에 복사할 수 있지만 비밀번호의 암호를 직접 해독할 수는 없습니다.

텍스트 파일에 암호화되지 않은 비밀번호를 입력한 경우 ASA는 구성을 ASA에 복사할 때 비밀번호를 자동으로 암호화하지 않습니다. ASA에서는 **copy running-config startup-config** 또는 **write memory** 명령을 사용하여 명령줄에서 실행 중인 구성을 저장할 경우에만 비밀번호를 암호화합니다.

다중 보안 상황 파일

다중 보안 상황의 경우, 전체 구성이 다음과 같은 여러 부분으로 구성됩니다.

- 보안 상황 구성

- 시스템 구성 - ASA의 기본 설정(상황 목록 포함) 식별
- 관리자 상황 - 시스템 구성에 대한 네트워크 인터페이스 제공

  시스템 구성에는 시스템 자체에 대한 인터페이스 또는 네트워크 설정이 포함되지 않습니다. 그 대신 시스템에서 네트워크 리소스에 액세스해야 할 경우(예: 서버에서 상황을 다운로드할 경우), 관리자 상황으로 지정된 상황을 사용합니다.

각 상황은 단일 상황 모드 구성과 유사합니다. 시스템 구성은 시스템 전용 명령(예: 모든 상황의 목록)을 포함하지만 기타 일반적인 명령(예: 대다수의 인터페이스 파라미터)은 없다는 점에서 상황 구성과 다릅니다.

지원되는 문자 집합

ASA CLI는 현재 UTF-8 인코딩만 지원합니다. UTF-8은 유니코드 기호에 대한 특정 인코딩 체계이며, ASCII 기호 하위 집합과 호환되도록 설계되었습니다. ASCII 문자는 1바이트 문자로 UTF-8에 표시됩니다. 나머지 모든 문자는 다중 바이트 기호로 UTF-8에 표시됩니다.

인쇄 가능한 ASCII 문자(0x20~0x7e)는 완전히 지원됩니다. 인쇄 가능한 ASCII 문자는 ISO 8859-1과 동일합니다. UTF-8은 ISO 8859-1의 상위 집합이므로 첫 번째 256자(0-255)는 ISO 8859-1과 동일합니다. ASA CLI는 ISO 8859-1의 최대 255자(다중 바이트 문자)를 지원합니다.

46 장

주소, 프로토콜, 포트

이 장에서는 IP 주소, 프로토콜, 애플리케이션에 대한 빠른 참조를 제공합니다.

IPv4 주소 및 서브넷 마스크

이 섹션에서는 Cisco ASA에서 IPv4 주소를 사용하는 방법에 대해 설명합니다. IPv4 주소는 점으로 구분된 십진수 표기법으로 나타낸 32비트 숫자입니다. 4개의 8비트 필드(옥텟)가 이진수에서 십진수로 변환된 것이며, 점으로 구분됩니다. IP 주소의 첫 번째 부분은 호스트가 상주하는 네트워크를 식별하고, 두 번째 부분은 제공된 네트워크의 특정 호스트를 식별합니다. 네트워크 번호 필드는 네트워크 접두사라고 합니다. 제공된 네트워크의 모든 호스트에서는 동일한 네트워크 접두사를 공유하지만 고유한 호스트 번호가 있어야 합니다. 클래스풀 IP의 경우, 주소의 클래스는 네트워크 접두사와 호스트 번호 간의 경계를 확인합니다.

클래스

IP 호스트 주소는 3가지 다른 주소 클래스인 클래스 A, 클래스 B, 클래스 C로 구분됩니다. 각 클래스는 32비트 주소 내에 있는 다른 지점에서 네트워크 프리픽스 및 호스트 번호 간의 경계를 수정합니다. 클래스 D 주소는 멀티캐스트 IP를 위해 남겨둡니다.

- 클래스 A 주소(1.xxx.xxx.xxx through 126.xxx.xxx.xxx)에서는 첫 번째 옥텟만 네트워크 접두사로 사용합니다.
- 클래스 B 주소(128.0.xxx.xxx through 191.255.xxx.xxx)에서는 처음 두 개의 옥텟을 네트워크 접두사로 사용합니다.
- 클래스 C 주소(192.0.0.xxx through 223.255.255.xxx)에서는 처음 세 개의 옥텟을 네트워크 접두사로 사용합니다.

클래스 A 주소에는 16,777,214개의 호스트 주소가 있고 클래스 B 주소에는 65,534개의 호스트가 있으므로, 서브넷 마스킹을 사용하여 대형 네트워크를 더 작은 서브넷으로 분할할 수 있습니다.

프라이빗 네트워크

네트워크에 많은 주소가 필요하고 인터넷에서 라우팅할 필요가 없는 경우, IANA(Internet Assigned Numbers Authority)에서 권장하는 사설 IP 주소를 사용할 수 있습니다(RFC 1918 참조). 다음 주소 범위는 광고할 수 없는 사설 네트워크로 지정됩니다.

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

서브넷 마스크

서브넷 마스크를 사용하면 단일 클래스 A, B, C 네트워크를 여러 네트워크로 변환할 수 있습니다. 서브넷 마스크를 통해 호스트 번호의 비트를 네트워크 접두사에 추가하는 확장된 네트워크 접두사를 생성할 수 있습니다. 예를 들어, 클래스 C 네트워크 접두사는 항상 IP 주소의 처음 3개의 옥텟으로 구성됩니다. 그러나 클래스 C 확장 네트워크 접두사에서는 네 번째 옥텟의 일부도 사용합니다.

점으로 구분된 십진수 대신 이진수 표기법을 사용하면 서브넷 마스킹을 쉽게 이해할 수 있습니다. 서브넷 마스크의 비트는 인터넷 주소에 일대일로 대응됩니다.

- IP 주소의 해당 비트가 확장된 네트워크 접두사의 일부일 경우 비트는 1로 설정됩니다.
- 비트가 호스트 번호의 일부일 경우 비트는 0으로 설정됩니다.

예 **1:** 클래스 B 주소가 129.10.0.0이고 세 번째 옥텟 전체를 호스트 번호 대신 확장된 네트워크 접두사로 사용하려면, 서브넷 마스크를 11111111.11111111.11111111.00000000으로 지정해야 합니다. 이러한 서브넷 마스크는 클래스 B 주소를 클래스 C 주소와 상응하게 변환하며, 여기에서는 호스트 번호가 마지막 옥텟으로만 구성됩니다.

예 **2:** 확장형 네트워크 접두사에 세 번째 옥텟의 일부만 사용하려면 서브넷 마스크를 11111111.11111111.11111000.00000000 형태로 지정해야 합니다. 여기에서는 확장된 네트워크 접두사에 세 번째 옥텟의 5비트만 사용합니다.

서브넷 마스크를 점으로 구분된 십진수 마스크 또는 /비트("슬래시 비트") 마스크로 작성할 수 있습니다. 예 1에서 점으로 구분된 십진수 마스크의 경우, 각 이진수 옥텟을 십진수 번호로 변환합니다(255.255.255.0). /비트 마스크의 경우 1s: /24 번호를 추가합니다. 예 2에서 십진수는 255.255.248.0이며 /비트는 /21입니다.

확장된 네트워크 접두사에 대한 세 번째 옥텟의 일부를 사용하여 여러 개의 클래스 C 네트워크를 대규모 네트워크로 수퍼네팅(supernet)할 수 있습니다. 예를 들면 192.168.0.0/20입니다.

서브넷 마스크 결정

다음 표를 참조하여 원하는 호스트 개수를 기준으로 서브넷 마스크를 결정합니다.

참고 단일 호스트를 식별하는 /32를 제외하고, 서브넷의 첫 번째 및 마지막 번호는 예약됩니다.

표 ***66:*** 호스트, 비트, 점으로 구분된 십진수 마스크

호스트	/비트 마스크	점으로 구분된 십진수 마스크
16,777,216	/8	255.0.0.0 클래스 A 네트워크
65,536	/16	255.255.0.0 클래스 B 네트워크
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 클래스 C 네트워크
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
사용하지 않음	/31	255.255.255.254
1	/32	255.255.255.255 단일 호스트 주소

서브넷 마스크와 함께 사용할 주소 결정

다음 섹션에서는 클래스 C 규모 및 클래스 B 규모 네트워크의 서브넷 마스크와 함께 사용할 네트워크 주소를 결정하는 방법에 대해 설명합니다.

클래스 C 규모 네트워크 주소

2개 ~ 254개의 호스트로 구성된 네트워크의 경우, 네 번째 옥텟은 0으로 시작하여 호스트 주소 개수의 배수가 됩니다. 예를 들어, 다음 표에는 192.168.0.x 형태의 호스트 서브넷(/29) 8개가 나와 있습니다.

참고 서브넷의 첫 번째 및 마지막 주소는 예약됩니다. 첫 번째 서브넷 예에서는 192.168.0.0 또는 192.168.0.7을 사용할 수 없습니다.

표 *67:* 클래스 *C* 규모 네트워크 주소

마스크 **/29**가 포함된 서브넷**(255.255.255.248)**	주소 범위
192.168.0.0	192.168.0.0 ~ 192.168.0.7
192.168.0.8	192.168.0.8 ~ 192.168.0.15
192.168.0.16	192.168.0.16 ~ 192.168.0.31
—	—
192.168.0.248	192.168.0.248 ~ 192.168.0.255

클래스 B 규모 네트워크 주소

호스트 수가 254개 ~ 65,534개인 네트워크의 서브넷 마스크와 함께 사용할 네트워크 주소를 결정하려면, 사용 가능한 각 확장된 네트워크 접두사의 세 번째 옥텟 값을 결정해야 합니다. 예를 들어, 주소 형태가 10.1.*x*.0 같은 서브넷을 원할 수 있습니다. 여기에서 처음 두 개의 옥텟은 확장된 네트워크 접두사에 사용되므로 고정되며, 네 번째 옥텟은 모든 비트가 호스트 번호에 사용되므로 0입니다.

세 번째 옥텟의 값을 결정하려면 다음 단계를 수행합니다.

1. 65,536(세 번째 및 네 번째 옥텟을 사용하는 총 주소 개수)을 원하는 호스트 주소의 수로 나누어 네트워크에서 생성할 수 있는 서브넷의 수를 계산합니다.

   예를 들어 65,536은 4096개의 호스트로 나뉘며 몫은 16입니다. 따라서 각 클래스 B 규모 네트워크에는 4096개의 주소로 구성된 16개의 서브넷이 있습니다.

2. 256(세 번째 옥텟의 값 수)을 서브넷 수로 나누어 세 번째 옥텟 값의 배수를 결정합니다.

   이 예에서는 256/16 = 16입니다.

   세 번째 옥텟은 0으로 시작하는 배수 16에 들어갑니다.

다음 표에는 네트워크 10.1의 서브넷 16개가 나와 있습니다.

참고 서브넷의 첫 번째 및 마지막 주소는 예약됩니다. 첫 번째 서브넷 예에서는 10.1.0.0 또는 10.1.15.255를 사용할 수 없습니다.

표 *68:* 네트워크의 서브넷

마스크 **/20**이 포함된 서브넷**(255.255.240.0)**	주소 범위
10.1.0.0	10.1.0.0 ~ 10.1.15.255
10.1.16.0	10.1.16.0 ~ 10.1.31.255
10.1.32.0	10.1.32.0 ~ 10.1.47.255
—	—
10.1.240.0	10.1.240.0 ~ 10.1.255.255

IPv6 주소

IPv6는 IPv4 이후의 차세대 인터넷 프로토콜입니다. IPv6 주소는 확장된 주소 공간, 간소화된 헤더 형식, 개선된 확장 및 옵션 지원, 흐름 레이블링 기능, 인증 및 개인 정보 보호 기능을 제공합니다. IPv6는 RFC 2460에 설명되어 있습니다. IPv6 주소 지정 아키텍처는 RFC 3513에 설명되어 있습니다.

이 섹션에서는 IPv6 주소 형식 및 아키텍처에 대해 설명합니다.

IPv6 주소 형식

IPv6 주소는 콜론(:)으로 구분된 16비트 16진수 필드 8개로 나타내며 x:x:x:x:x:x:x:x 형식으로 표시합니다. 다음은 IPv6 주소의 2가지 예입니다.

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

참고 IPv6 주소의 16진수 문자는 대소문자를 구분하지 않습니다.

주소의 개별 필드에 선행 0이 포함되지 않아도 되지만, 각 필드에는 최소 하나 이상의 숫자가 포함되어야 합니다. 왼쪽에서 세 번째 필드부터 여섯 번째 필드까지 선행 0을 제거하면 예시 주소 2001:0DB8:0000:0000:0008:0800:200C:417A는 2001:0DB8:0:0:8:800:200C:417A로 줄일 수 있습니다. 모두 0으로 된 필드는 0 하나로 줄일 수 있습니다(왼쪽에서 세 번째 및 네 번째 필드). 왼쪽에서 다섯 번째 필드는 3개의 선행 0이 제거되어 필드에 8 하나만 남았으며, 왼쪽에서 여섯 번째 필드는 1개의 선행 0이 제거되어 필드에 800이 남았습니다.

IPv6 주소에는 0으로 된 연속적인 16진수 필드가 몇 개 포함되는 것이 일반적입니다. 이중 콜론(::)을 사용하여 IPv6 주소의 맨 앞, 중간 또는 끝에 0이 연속으로 나오는 필드를 압축할 수 있습니다(콜론은 0이 연속으로 나오는 16진수 필드를 의미합니다). 다음 표에는 다른 유형의 IPv6 주소의 주소 압축에 대한 몇 가지 예가 나와 있습니다.

표 *69: IPv6* 주소 압축 예

주소 유형	표준 형식	압축된 형식
유니캐스트	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
멀티캐스트	FF01:0:0:0:0:0:0:101	FF01::101
루프백	0:0:0:0:0:0:0:1	::1
지정되지 않음	0:0:0:0:0:0:0:0	::

참고 이중 콜론(::)은 0이 연속으로 나오는 필드를 나타내기 위해 IPv6 주소에서 한 번만 사용할 수 있습니다.

IPv4 및 IPv6 주소가 모두 포함된 환경을 처리할 경우에는 IPv6 형식의 대체 형식이 자주 사용됩니다. 이러한 대체 형식은 x:x:x:x:x:x:y.y.y.y입니다. 여기서 x는 IPv6 주소의 높은 자리 부분 6개의 16진수 값을 나타내고, y는 주소의 32비트 IPv4 부분의 십진수 값을 나타냅니다(IPv6 주소의 나머지 2개의 16비트 부분을 대신함). 예를 들어, IPv4 주소 192.168.1.1은 IPv6 주소 0:0:0:0:0:0:FFFF:192.168.1.1 또는 ::FFFF:192.168.1.1로 표시할 수 있습니다.

IPv6 주소 유형

다음은 IPv6 주소의 3가지 기본 유형입니다.

- 유니캐스트 — 유니캐스트 주소는 단일 인터페이스의 식별자입니다. 유니캐스트 주소로 전송된 패킷은 해당 주소로 식별된 인터페이스에 전달됩니다. 인터페이스에는 할당된 것보다 여러 개의 유니캐스트 주소가 있을 수 있습니다.
- 멀티캐스트 — 멀티캐스트 주소는 인터페이스 집합의 식별자입니다. 멀티캐스트 주소로 전송된 패킷은 해당 주소로 식별된 인터페이스에 전달됩니다.
- 애니캐스트 — 애니캐스트 주소는 인터페이스 집합의 식별자입니다. 멀티캐스트 주소와 달리 애니캐스트 주소로 전송된 패킷은 라우팅 프로토콜의 거리를 측정하여 확인된 "가장 가까운" 인터페이스에만 전달됩니다.

참고 IPv6에는 브로드캐스트 주소가 없습니다. 멀티캐스트 주소에서는 브로드캐스트 기능을 제공합니다.

유니캐스트 주소

이 섹션에서는 IPv6 유니캐스트 주소에 대해 설명합니다. 유니캐스트 주소는 네트워크 노드의 인터페이스를 식별합니다.

전역 주소

IPv6 글로벌 유니캐스트 주소의 일반적인 형식은 전역 라우팅 접두사 뒤에 서브넷 ID가 오고 그 뒤에 인터페이스 ID가 옵니다. 전역 라우팅 접두사는 다른 IPv6 주소 유형에서 예약되지 않은 모든 접두사가 해당될 수 있습니다.

이진수 000으로 시작하는 주소를 제외한 모든 전역 유니캐스트 주소는 Modified EUI-64 형식의 64비트 인터페이스 ID가 포함됩니다.

이진수 000으로 시작하지 않는 전역 유니캐스트 주소에는 주소의 인터페이스 ID 부분에 아무런 제한 없이 모든 크기 또는 구조가 올 수 있습니다. 이러한 유형으로 된 주소의 한 가지 예는 IPv4 주소가 포함된 IPv6 주소입니다.

사이트-로컬 주소

사이트-로컬 주소는 사이트 내에서 주소를 지정하는 데 사용됩니다. 이러한 주소를 사용하면 전역에서 고유한 접두사를 사용하지 않고 전체 사이트의 주소를 지정할 수 있습니다. 사이트-로컬 주소에는 접두사 FEC0::/10이 포함되고 54비트 서브넷 ID가 뒤에 오며 Modified EUI-64 형식의 64비트 인터페이스 ID로 끝납니다.

사이트-로컬 라우터에서는 사이트 외부의 소스 또는 목적지에 대한 사이트-로컬 주소가 포함된 패킷을 전달하지 않습니다. 따라서 사이트-로컬 주소는 사설 주소로 간주할 수 있습니다.

링크-로컬 주소

모든 인터페이스에는 최소한 하나 이상의 링크-로컬 주소가 있어야 합니다. 인터페이스당 여러 개의 IPv6 주소를 구성할 수 있으나, 링크-로컬 주소는 하나만 구성 가능합니다.

링크-로컬 주소는 링크-로컬 접두사 FE80::/10 및 Modified EUI-64 형식의 인터페이스 식별자를 사용하여 모든 인터페이스에서 자동으로 구성할 수 있는 IPv6 유니캐스트 주소입니다. 링크-로컬 주소는 인접 검색 프로토콜 및 스테이트풀 자동 컨피그레이션 프로세스에서 사용됩니다. 링크-로컬 주소가 포함된 노드에서는 통신을 수행할 수 있으며, 통신을 위해 사이트-로컬 또는 전역에서 고유한 주소가 필요하지 않습니다.

라우터에서는 소스 또는 목적지의 링크-로컬 주소가 포함된 패킷은 전달하지 않습니다. 따라서 링크-로컬 주소는 사설 주소로 간주할 수 있습니다.

IPv4 호환 **IPv6** 주소

IPv4 주소를 포함할 수 있는 IPv6 주소에는 2가지 유형이 있습니다.

첫 번째 유형은 IPv4 호환 IPv6 주소입니다. IPv6 전환 메커니즘에는 IPv4 라우팅 인프라를 통해 IPv6 패킷을 동적으로 터널링할 수 있는 호스트 및 라우터를 지원하는 기술이 포함됩니다. 이러한 기술을 사용하는 IPv6 노드에는 낮은 자리 32비트 형식의 전역 IPv4 주소를 전달하는 특수 IPv6 유니캐스트 주소가 할당됩니다. 이러한 유형의 주소는 IPv4 호환 IPv6 주소라고 하며 ::y.y.y.y 형식으로 되어 있습니다. 여기서 y.y.y.y는 IPv4 유니캐스트 주소입니다.

참고 IPv4 호환 IPv6 주소에 사용되는 IPv4 주소는 전역에서 고유한 IPv4 유니캐스트 주소가 있어야 합니다.

두 번째 유형의 IPv6 주소는 내장된 IPv4 주소를 수용하며, IPv4 매핑 IPv6 주소라고 합니다. 이러한 주소 유형은 IPv4 노드의 주소를 IPv6 주소로 표현하는 데 사용됩니다. 이러한 주소 유형의 형식은 ::FFFF:y.y.y.y이며, 여기서 y.y.y.y는 IPv4 유니캐스트 주소입니다.

지정되지 않은 주소

지정되지 않은 주소 0:0:0:0:0:0:0:0은 IPv6 주소가 없음을 나타냅니다. 예를 들어, IPv6 네트워크에서 새로 초기화된 노드에서는 IPv6 주소를 수신할 때까지 해당 패킷에서 지정되지 않은 주소를 소스 주소로 사용할 수 있습니다.

참고 IPv6 지정되지 않은 주소는 인터페이스에 할당할 수 없습니다. 지정되지 않은 IPv6 주소를 IPv6 패킷 또는 IPv6 라우팅 헤더에서 목적지 주소로 사용해서는 안 됩니다.

루프백 주소

루프백 주소 0:0:0:0:0:0:0:1은 IPv6 패킷을 자신에게 전송하려는 노드에서 사용할 수 있습니다. IPv6의 루프백 주소는 IPv4 루프백 주소(127.0.0.1)와 동일한 기능을 수행합니다.

참고 IPv6 루프백 주소는 물리적 인터페이스에 할당할 수 없습니다. IPv6 루프백 주소를 소스 또는 목적지 주소로 포함한 패킷은 패킷이 생성된 노드 내에 그대로 있어야 합니다. IPv6 라우터에서는 IPv6 루프백 주소를 소스 또는 목적지 주소로 포함한 패킷을 전달하지 않습니다.

인터페이스 식별자

IPv6 유니캐스트 주소의 인터페이스 식별자는 링크의 인터페이스를 식별할 때 사용됩니다. 이러한 식별자는 서브넷 접두사에서 고유해야 합니다. 대부분의 경우, 인터페이스 식별자는 인터페이스 링크 계층 주소에서 파생됩니다. 동일한 인터페이스 식별자는 인터페이스가 다른 서브넷에 연결되어 있는 한 단일 노드의 여러 인터페이스에 사용될 수 있습니다.

이진수 000으로 시작하는 주소를 제외한 모든 유니캐스트 주소의 경우, 64비트 길이의 Modified EUI-64 형식으로 구성하려면 인터페이스 식별자가 필요합니다. Modified EUI-64 형식은 주소의 범용/로컬 비트를 변환하고, MAC 주소의 상위 3개 바이트와 하위 3개 바이트 사이에 16진수 숫자 FFFE를 삽입하는 방법을 통해 48비트 MAC 주소에서 생성됩니다.

예를 들어, MAC 주소가 00E0.b601.3B7A인 인터페이스의 64비트 인터페이스 ID는 02E0:B6FF:FE01:3B7A가 될 수 있습니다.

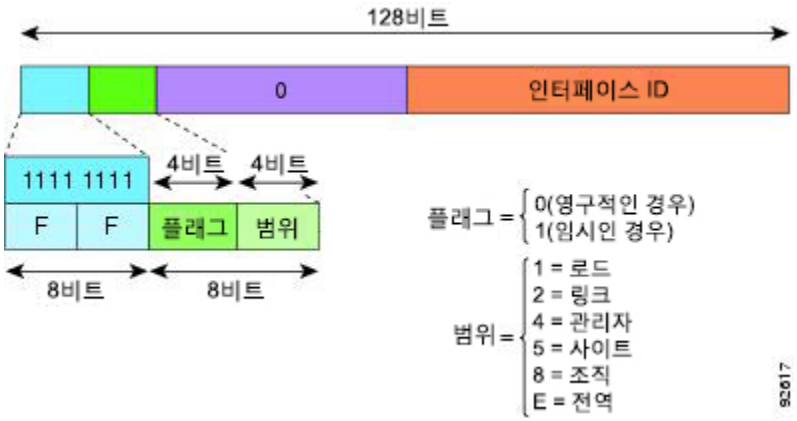
멀티캐스트 주소

IPv6 멀티캐스트 주소는 일반적으로 다른 노드에 있는 인터페이스 그룹의 식별자입니다. 멀티캐스트 주소로 전송된 패킷은 해당 주소로 식별된 모든 인터페이스에 전달됩니다. 인터페이스는 멀티캐스트 그룹에 얼마든지 속할 수 있습니다.

IPv6 멀티캐스트 주소의 접두사는 FF00::/8(1111 1111)입니다. 접두사 뒤의 옥텟은 멀티캐스트 주소의 유형과 범위를 정의합니다. 영구적으로 할당된(잘 알려진) 멀티캐스트 주소에는 0에 상응하는 플

래그 매개변수가 있습니다. 임시(일시적) 멀티캐스트 주소에는 1에 상응하는 플래그 매개변수가 있습니다. 노드, 링크, 사이트 또는 조직의 범위나 전역 범위가 포함된 멀티캐스트 주소에는 각각 1, 2, 5, 8 또는 E로 된 범위 매개변수가 포함됩니다. 예를 들어, 접두사가 FF02::/16인 멀티캐스트 주소는 링크 범위가 포함된 영구 멀티캐스트 주소입니다. 다음 그림에는 IPv6 멀티캐스트 주소의 형식이 나와 있습니다.

그림 ***76: IPv6*** 멀티캐스트 주소 형식



다음 멀티캐스트 그룹에 참여하려면 IPv6 노드(호스트 및 라우터)가 있어야 합니다.

- All Nodes 멀티캐스트 주소:
  - FF01::(인터페이스-로컬)
  - FF02::(링크-로컬)
- 노드의 각 IPv6 유니캐스트 및 애니캐스트 주소에 대한 Solicited-Node 주소이며 FF02:0:0:0:0:1:FFXX:XXXX/104 형식으로 되어 있습니다. 여기서 XX:XXXX는 유니캐스트 또는 애니캐스트 주소의 낮은 자리 24비트 부분입니다.

참고 Solicited-Node 주소는 Neighbor Solicitation 메시지에 사용됩니다.

다음 멀티캐스트 그룹에 참여하려면 IPv6 라우터가 있어야 합니다.

- FF01:: 2(인터페이스-로컬)
- FF02:: 2(링크-로컬)
- FF05:: 2(사이트-로컬)

멀티캐스트 주소는 IPv6 패킷에서 소스 주소로 사용해서는 안 됩니다.

참고 IPv6에는 브로드캐스트 주소가 없습니다. IPv6 멀티캐스트 주소는 브로드캐스트 주소 대신 사용됩니다.

애니캐스트 주소

IPv6 애니캐스트 주소는 일반적으로 다른 노드에 속한 여러 개의 인터페이스에 할당된 유니캐스트 주소입니다. 애니캐스트 주소에 라우팅된 패킷은 해당 주소가 포함된 가장 가까운 인터페이스에 라우팅되며, 인접성은 적용되는 라우팅 프로토콜에 의해 결정됩니다.

애니캐스트 주소는 유니캐스트 주소 영역에서 할당됩니다. 애니캐스트 주소는 여러 개의 인터페이스에 할당된 유니캐스트 주소이며, 인터페이스는 주소를 애니캐스트 주소로 인식할 수 있도록 구성해야 합니다.

애니캐스트 주소에는 다음과 같은 제한 사항이 적용됩니다.

- 애니캐스트 주소는 IPv6 패킷의 소스 주소로 사용할 수 없습니다.
- 애니캐스트 주소는 IPv6 호스트에 할당할 수 없으며, IPv6 라우터에만 할당할 수 있습니다.

참고 애니캐스트 주소는 ASA에서 지원되지 않습니다.

필수 주소

IPv6 호스트에서는 적어도 (자동 또는 수동으로) 다음 주소를 구성해야 합니다.

- 각 인터페이스의 링크-로컬 주소
- 루프백 주소
- All-Nodes 멀티캐스트 주소
- 각 유니캐스트 또는 애니캐스트 주소의 Solicited-Node 멀티캐스트 주소

IPv6 라우터에서는 적어도 (자동 또는 수동으로) 다음 주소를 구성해야 합니다.

- 필수 호스트 주소
- 라우터 역할을 수행하도록 구성된 모든 인터페이스의 Subnet-Router 애니캐스트 주소
- All-Routers 멀티캐스트 주소

IPv6 주소 프리픽스

ipv6-prefix/prefix-length 형식으로 된 IPv6 주소 접속사를 사용하여 전체 주소 영역의 비트 인접 블록을 표시할 수 있습니다. IPv6 접두사는 RFC 2373에 설명된 형식으로 구성해야 하며, 해당 주소는 콜론 사이에 16비트 값을 사용한 16진수로 지정해야 합니다. 접두사 길이는 접두사(주소의 네트워크 부분)로 구성된 주소의 높은 자리 인접 비트가 몇 개 있는지 나타내는 십진수 값입니다. 예를 들어, 2001:0DB8:8086:6502::/32는 올바른 IPv6 접두사입니다.

IPv6 접두사는 IPv6 주소의 유형을 식별합니다. 다음 표에는 각 IPv6 주소 유형의 프리픽스가 나와 있습니다.

표 ***70: IPv6*** 주소 유형 접두사

주소 유형	이진 접두사	**IPv6** 표기법
지정되지 않음	000...0(128비트)	::/128
루프백	000...1(128비트)	::1/128
멀티캐스트	11111111	FF00::/8
링크-로컬(유니캐스트)	1111111010	FE80::/10
사이트-로컬(유니캐스트)	1111111111	FEC0::/10
전역(유니캐스트)	기타 모든 주소	
애니캐스트	유니캐스트 주소 영역에서 가져옴	

프로토콜 및 애플리케이션

다음 표에는 프로토콜 리터럴 값 및 포트 번호가 나와 있으며, 이를 ASA 명령에 입력할 수 있습니다.

표 ***71:*** 프로토콜 리터럴 값

리터럴	값	설명
ah	51	IPv6용 Authentication Header, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	IPv6용 Encapsulated Security Payload, RFC 1827
gre	47	Generic Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
icmp6	58	IPv6용 Internet Control Message Protocol, RFC 2463
igmp	2	Internet Group Management Protocol, RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	IP-in-IP encapsulation
IPSec	50	IP Security. ipsec 프로토콜 리터럴을 입력할 경우 esp 프로토콜 리터럴을 입력하는 것에 상응합니다.
nos	94	Network Operating System(Novell의 NetWare)

리터럴	값	설명
ospf	89	Open Shortest Path First 라우팅 프로토콜, RFC 1247
pcp	108	Payload Compression Protocol
pim	103	Protocol Independent Multicast
pptp	47	Point-to-Point Tunneling Protocol. ipsec 프로토콜 리터럴을 입력할 경우 esp 프로토콜 리터럴을 입력하는 것에 상응합니다.
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768.

IANA 웹 사이트에서 프로토콜 번호를 볼 수 있습니다.

http://www.iana.org/assignments/protocol-numbers

TCP 및 UDP 포트

다음 표에는 리터럴 값 및 포트 번호가 나와 있으며, 이를 ASA 명령에 입력할 수 있습니다. 다음 주의 사항을 참조하십시오.

- ASA에서는 SQL*Net에 포트 1521을 사용합니다. 이는 SQL*Net용 Oracle에서 사용되는 기본 포트입니다. 그러나 이 값은 IANA 포트 할당과 일치하지 않습니다.
- ASA는 포트 1645 및 1646에서 RADIUS를 수신합니다. RADIUS 서버에서 표준 포트 1812 및 1813을 사용할 경우, **authentication-port** 및 **accounting-port** 명령을 사용하여 ASA에서 이러한 포트를 수신하도록 구성할 수 있습니다.
- DNS 액세스를 위한 포트를 할당하려면 **dns** 대신 **domain** 리터럴 값을 사용합니다. **dns**를 사용할 경우 ASA에서는 **dnsix** 리터럴 값을 사용하겠다는 것으로 간주합니다.

IANA 웹 사이트에서 포트 번호를 볼 수 있습니다.

http://www.iana.org/assignments/port-numbers

표 ***72:*** 포트 리터럴 값

리터럴	**TCP** 또는 **UDP?**	값	설명
aol	TCP	5190	America Online
bgp	TCP	179	Border Gateway Protocol, RFC 1163
biff	UDP	512	메일 시스템에서 새 메일이 수신되었음을 사용자에게 알리기 위해 사용됨
bootpc	UDP	68	Bootstrap Protocol Client

리터럴	TCP 또는 UDP?	값	설명
bootps	UDP	67	Bootstrap Protocol Server
chargen	TCP	19	Character Generator
CIFS	TCP, UDP	3020	Common Internet File System
citrix-ica	TCP	1494	Citrix ICA(Independent Computing Architecture) 프로토콜
cmd	TCP	514	cmd의 경우 자동 인증이 있다는 점을 제외하고 exec과 유사함
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time, RFC 867
discard	TCP, UDP	9	Discard
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
domain	TCP, UDP	53	DNS
echo	TCP, UDP	7	Echo
exec	TCP	512	Remote process execution
finger	TCP	79	Finger
ftp	TCP	21	File Transfer Protocol(제어 포트)
ftp-data	TCP	20	File Transfer Protocol(데이터 포트)
gopher	TCP	70	Gopher
h323	TCP	1720	H.323 호출 신호
hostname	TCP	101	NIC Host Name Server
http	TCP, UDP	80	World Wide Web HTTP
https	TCP	443	HTTP over SSL
ident	TCP	113	Ident 인증 서비스
imap4	TCP	143	Internet Message Access Protocol, 버전 4
irc	TCP	194	Internet Relay Chat protocol
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP, UDP	750	Kerberos

리터럴	TCP 또는 UDP?	값	설명
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	Lightweight Directory Access Protocol
ldaps	TCP	636	Lightweight Directory Access Protocol(SSL)
login	TCP	513	Remote login
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	Line Printer Daemon - printer spooler
mobile-ip	UDP	434	Mobile IP-Agent
nameserver	UDP	42	Host Name Server
netbios-dgm	UDP	138	NetBIOS Datagram Service
netbios-ns	UDP	137	NetBIOS Name Service
NetBIOS ssn	TCP	139	NetBIOS Session Service
NFS	TCP, UDP	2049	네트워크 파일 시스템 - Sun Microsystems
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	Network Time Protocol
pcanywhere-data	TCP	5631	pcAnywhere 데이터
pcanywhere-status	UDP	5632	pcAnywhere 상태
pim-auto-rp	TCP, UDP	496	Protocol Independent Multicast, reverse path flooding, dense mode
pop2	TCP	109	Post Office Protocol - 버전 2
pop3	TCP	110	Post Office Protocol - 버전 3
pptp	TCP	1723	Point-to-Point Tunneling Protocol
radius	UDP	1645	Remote Authentication Dial-In User Service
radius-acct	UDP	1646	Remote Authentication Dial-In User Service(accounting)
rip	UDP	520	Routing Information Protocol
rsh	TCP	514	원격 쉘
rtsp	TCP	554	Real Time Streaming Protocol

리터럴	**TCP** 또는 **UDP?**	값	설명
secureid-udp	UDP	5510	SecureID over UDP
sip	TCP, UDP	5060	세션 시작 프로토콜
smtp	TCP	25	Simple Mail Transport Protocol
snmp	UDP	161	Simple Network Management Protocol
snmptrap	UDP	162	Simple Network Management Protocol - Trap
sqlnet	TCP	1521	Structured Query Language Network
ssh	TCP	22	SSH(Secure Shell)
sunrpc	TCP, UDP	111	Sun Remote Procedure Call
syslog	UDP	514	System Log
tacacs	TCP, UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP, UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	Trivial File Transfer Protocol
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program
vxlan	UDP	4789	VXLAN(Virtual eXtensible Local Area Network)
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP, UDP	80	World Wide Web
xdmcp	UDP	177	X Display Manager Control Protocol

로컬 포트 및 프로토콜

다음 표에는 ASA에 지정된 트래픽을 처리하기 위해 ASA에서 열 수 있는 프로토콜, TCP 포트, UDP 포트가 나와 있습니다. 이 표에 나열된 기능 및 서비스를 활성화하지 않으면, ASA에서는 로컬 프로토콜이나 TCP 또는 UDP를 열지 않습니다. 수신하는 기본 프로토콜 또는 포트를 열려면 ASA에 대한 기능 또는 서비스를 구성해야 합니다. 대부분의 경우, 기능 또는 서비스를 활성화할 때 기본 포트 대신 여러 포트를 구성할 수 있습니다.

표 ***73:*** 기능 및 서비스를 통해 연 프로토콜 및 포트

기능 또는 서비스	프로토콜	포트 번호	코멘트
DHCP	UDP	67,68	—
장애 조치 제어	105	해당 없음	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	해당 없음	—
IGMP	2	해당 없음	목적지 IP 주소 224.0.0.1에서만 열리는 프로토콜
ISAKMP/IKE	UDP	500	구성 가능
IPsec(ESP)	50	해당 없음	—
IPsec over UDP(NAT-T)	UDP	4500	—
IPsec over TCP(CTCP)	TCP	—	기본 포트는 사용되지 않습니다. IPsec over TCP를 구성할 경우 포트 번호를 지정해야 합니다.
NTP	UDP	123	—
OSPF	89	해당 없음	목적지 IP 주소 224.0.0.5 및 224.0.0.6에서만 열리는 프로토콜
PIM	103	해당 없음	목적지 IP 주소 224.0.0.13에서만 열리는 프로토콜
RIP	UDP	520	—
RIPv2	UDP	520	목적지 IP 주소 224.0.0.9에서만 열리는 프로토콜
SNMP	UDP	161	구성 가능합니다.
SSH	TCP	22	—
스테이트풀 업데이트	8(비보안) 9(보안)	해당 없음	—
텔넷	TCP	23	—
VPN 로드 밸런싱	UDP	9023	구성 가능합니다.

기능 또는 서비스	프로토콜	포트 번호	코멘트
VPN 개별 사용자 인증 프록시	UDP	1645, 1646	VPN 터널을 통해서만 액세스할 수 있는 포트입니다.

ICMP 유형

다음 표에는 ASA 명령에 입력할 수 있는 ICMP 유형의 번호 및 이름이 나와 있습니다.

표 ***74: ICMP*** 유형

ICMP 번호	**ICMP** 이름
0	echo-reply
3	unreachable
4	source-quench
5	리디렉션
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect