Cisco ASA 시리즈 일반 운영 **CLI** 컨피그레이션 가이드

소프트웨어 버전9.3

릴리스: 2014년 7월 24일
업데이트: 2014년 9월 16일

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
주소, 전화 번호 및 팩스 번호는
Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

텍스트 파트 번호 : N/A, Online only

Cisco ASA 시리즈 일반 운영 CLI 컨피그레이션 가이드

목 차

설명서 정보

문서의 용도

이 설명서는 명령행 인터페이스를 사용하여 Cisco ASA 시리즈의 일반적인 운영을 구성하는 데 참조할 수 있습니다. 여기서는 모든 기능을 다루기보다는 가장 대표적인 컨피그레이션 시나리오에 대해서만 설명합니다.

웹 기반 GUI 애플리케이션인 ASDM(Adaptive Security Device Manager)을 사용하여 ASA를 구성하고 모니터링할 수도 있습니다. ASDM에서는 일반적인 컨피그레이션 시나리오를 안내하는 컨피그레이션 마법사 및 상대적으로 일반적이지 않은 시나리오를 위한 온라인 도움말을 제공합니다.

이 설명서에서 "ASA"는 달리 명시되지 않는 한 지원되는 모델을 총칭합니다.

관련 설명서

자세한 내용은 *Cisco ASA 시리즈 설명서(Navigating the Cisco ASA Series Documentation,* http://www.cisco.com/go/asadocs)를 참조하십시오.

표기 규칙

이 설명서는 다음과 같은 표기 규칙을 사용합니다.

표기 규칙	표시
굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은** 글꼴로 표시합니다.
기울임꼴	설명서 제목, 신규 용어 또는 강조된 용어, 사용자가 값을 지정해야 하는 인수는 *기울임꼴*로 표시합니다.
[ ]	대괄호로 묶인 요소는 선택 사항입니다.
{x | y | z }	필수 대체 키워드는 대괄호로 묶고 세로 선으로 구분합니다.

[x | y | z]	선택적 대체 키워드는 괄호로 묶고 세로 선으로 구분합니다.
문자열	따옴표 없는 문자의 집합입니다. 문자열 주변에 따옴표를 사용하지 마십시오. 그러지 않으면 따옴표도 문자열에 포함됩니다.
`courier` 글꼴	시스템에 표시되는 터미널 세션 및 정보는 `courier` 글꼴로 표시합니다.
`courier` 굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은 `courier`** 글꼴로 표시합니다.
`courier` 기울임꼴	사용자가 값을 지정하는 인수는 *`courier` 기울임꼴*로 표시합니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 우물 정자(#)는 코멘트 라인을 나타냅니다.

참고 *독자가 주목해야 하는 내용*을 가리킵니다.

팁 *다음 정보가 문제를 해결하는 데 도움이 된다는 것*을 의미합니다.

주의 *독자가 유의해야 하는 내용*을 말합니다. 이 경우, 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 합니다.

설명서 받기 및 서비스 요청 제출

설명서 다운로드, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, 추가 정보 수집에 대한 자세한 내용은 *Cisco 제품 설명서의 새로운 소식* (http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html)을 참조하십시오.

Cisco의 새로운 기술 문서 및 개정된 기술 문서를 모두 소개하는 *Cisco 제품 설명서의 새로운 소식*을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 배달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.

1 파 트

ASA 시작하기

Cisco ASA 소개

릴리스: 2014년 7월 24일
업데이트: 2014년 9월 16일

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 장치 기능을 하나의 디바이스에서 제공하며, 일부 모델의 경우 IPS 같은 통합된 서비스 모듈을 제공합니다. ASA에는 다중 보안 컨텍스트(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(레이어 2) 방화벽 또는 라우팅(레이어 3) 방화벽 가동, 고급 감시 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 호환성*을 참조 하십시오.
http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN 호환성

*지원되는 VPN 플랫폼, Cisco ASA Series*를 참조하십시오.
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

새로운 기능

참고 새 syslog 메시지, 변경된 syslog 메시지, 사용 중단된 syslog 메시지가 syslog 메시지 가이드에 나와 있습니다.

ASA 9.3(1)

릴리스 : 2014 년 7 월 24 일

표 1-1 에서는 ASA Version 9.3(1)의 새로운 기능을 소개합니다.

표 1-1 ASA 버전 9.3(1)

기능	설명
방화벽 기능	
SIP, SCCP, TLS 프록시에서 IPv6 지원	SIP, SCCP, TLS 프록시(SIP 또는 SCCP 사용)를 사용할 때 IPv6 트래픽을 검사할 수 있습니다. 어떤 명령도 수정하지 않았습니다.
Cisco Unified Communications Manager 8.6 지원	ASA가 Cisco Unified Communications Manager Version 8.6과의 상호 운용성을 제공합니다(SCCPv21 지원 포함). 어떤 명령도 수정하지 않았습니다.
액세스 그룹 및 NAT를 위한 규칙 엔진의 트랜잭션 커밋 모델	이 기능을 활성화한 경우, 규칙 매칭의 성능 저하 없이 규칙 컴파일이 완료되면 규칙 업데이트가 적용됩니다. 도입된 명령: **asp rule-engine transactional-commit**, **show running-config asp rule-engine transactional-commit**, **clear configure asp rule-engine transactional-commit**
원격 액세스 기능	
클라이언트리스 SSL VPN을 위한 XenDesktop 7 지원	클라언트리스 SSL VPN에 XenDesktop 7 지원을 추가했습니다. 자동 로그온의 북마크를 만들 때 랜딩 페이지 URL 또는 제어 ID를 지정할 수 있습니다. 어떤 명령도 수정하지 않았습니다.

표 1-1 ASA 버전 9.3(1)(계속)

기능	설명
Mobile Enablement 프록시	ISE Mobile Enablement 솔루션의 구성 요소인 Mobile Enablement 프록시를 사용하면 오프프레미스 모바일 디바이스에서 온프레미스 모바일 디바이스와 똑같은 방식으로 모바일 디바이스를 관리할 수 있습니다. **참고** Mobile Enablement 프록시는 2015년 초에 출시될 예정인 ISE 릴리스의 ISE 지원을 필요로 합니다. config-mdm-proxy 모드를 시작하는 **mdm-proxy** 명령을 도입했습니다. 이 새로운 모드에서는 **authentication-server-group, accounting-server-group, password-management, trusttpoint, port, session-limit, session-timeout, enable** 명령이 적용됩니다.
AnyConnect 사용자 지정 특성 확장	사용자 지정 특성으로 ASA에 통합되지 않은 AnyConnect 기능(예: Deferred Upgrade)을 정의하고 구성합니다. 사용자 지정 특성 컨피그레이션이 여러 값과 더 긴 값을 허용하도록 확장되었습니다. 또한 이제부터는 그 유형, 이름, 값을 지정해야 합니다. 동적 액세스 정책과 그룹 정책에 추가할 수 있습니다. 9.3.x로 업그레이드하면 이전에 정의했던 사용자 지정 특성이 이 확장된 컨피그레이션 형식으로 업데이트됩니다. 도입되거나 수정된 명령: **anyconnect-custom-attr**, **anyconnect-custom-data**, **anyconnect-custom**
데스크톱 플랫폼을 위한 ACIDex(AnyConnect Identity Extensions)	AnyConnect Endpoint Attributes 또는 Mobile Posture라고도 하는 ACIDex는 AnyConnect VPN 클라이언트에서 ASA에 포스처 정보를 전달하는 데 사용하는 방법입니다. 동적 액세스 정책에서는 사용자 권한 부여에 이 엔드포인트 특성을 사용합니다. AnyConnect VPN 클라이언트는 DAP에서 사용할 데스크톱 운영 체제(Windows, Mac OS X, Linux)용 플랫폼 식별자와 MAC 주소 풀을 제공합니다. 어떤 명령도 수정하지 않았습니다.
VPN을 위한 TrustSec SGT 지정	원격 사용자가 연결할 때 ASA에서 TrustSec SGT(Security Group Tag)가 SGT-IP 테이블에 추가될 수 있습니다. 새로 도입된 명령: **security-group-tag value**
고가용성 기능	
클러스터링의 모듈 상태 모니터링 지원 향상	클러스터링에서 모듈 상태의 모니터링을 더 효과적으로 지원합니다. 다음 명령을 수정했습니다. **show cluster info health**

표 1-1 ASA 버전 9.3(1)(계속)

기능	설명
하드웨어 모듈의 상태 모니터링 비활성화	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. 수정된 명령: **monitor-interface service-module**
플랫폼 기능	
ASP 로드 밸런싱	**asp load-balance per-packet** 명령의 새로운 **auto** 옵션은 ASA가 각 인터페이스 수신 링에서 패킷별로 ASP 로드 밸런싱을 켜고 끄면서 조정할 수 있게 합니다. 이 자동 메커니즘은 비대칭형 트래픽의 유입 여부를 감지하며, 다음과 같은 문제의 예방에 도움이 됩니다. • 흐름에서 산발적인 트래픽 급증으로 인한 오버런 • 특정 인터페이스 수신 링에 초과 유입되는 대량 흐름에 의한 오버런 • 비교적 과부하 상태인 인터페이스 수신 링으로 인한 오버런. 단일 코어에서 부하를 수용할 수 없음 도입되거나 수정된 명령: **asp load-balance per-packet auto**, **show asp load-balance per-packet**, **show asp load-balance per-packet history**, **clear asp load-balance history**
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB에서 ASASM를 지원합니다.
인터페이스 기능	
투명 모드 브리지 그룹 최대 개수 250개로 증가	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**
라우팅 기능	
ASA 클러스터링을 위한 BGP 지원	ASA 클러스터링에서 BGP 지원을 추가했습니다. 새로 도입된 명령: **bgp router-id clusterpool**
NSF를 위한 BGP 지원	BGP NSF(Nonstop Forwarding) 지원을 추가했습니다. 새로 도입된 명령: **bgp graceful-restart, neighbor ha-mode graceful-restart**
광고 맵을 위한 BGP 지원	BGPv4 광고 맵 지원을 추가했습니다. 새로 도입된 명령: **neighbor advertise-map**

표 1-1 ASA 버전 9.3(1)(계속)

기능	설명
NSF를 위한 OSPF 지원	NSF를 위한 OSPFv2 및 OSPFv3 지원을 추가했습니다. 추가된 명령: **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**
AAA 기능	
레이어 2 보안 그룹 태그 도입	보안 그룹 태그와 이더넷 태그를 함께 사용하면서 정책을 적용할 수 있습니다. Layer 2 SGT Imposition이라고도 하는 SGT plus Ethernet Tagging은 ASA가 기가비트 이더넷 인터페이스에서 Cisco 전용 이더넷 프레이밍(Ether Type 0x8909)을 사용하여 보안 그룹 태그를 보내고 받을 수 있게 합니다. 즉 일반 텍스트 이더넷 프레임에 소스 보안 그룹 태그를 삽입할 수 있습니다. 도입되거나 수정된 명령: **cts manual**, **policy static sgt**, **propagate sgt**, **cts role-based sgt-map**, **show cts sgt-map**, **packet-tracer**, **capture**, **show capture**, **show asp drop**, **show asp table classify**, **show running-config all**, **clear configure all**, **write memory**
AAA Windows NT 도메인 인증 종료	원격 액세스 VPN 사용자를 위한 NTLM 지원을 종료했습니다. **aaa-server protocol nt** 명령을 더 이상 사용하지 않습니다.
모니터링 기능	
물리적 인터페이스의 종합 트래픽 모니터링	**show traffic** 명령 출력이 업데이트되어 물리적 인터페이스의 종합 트래픽 정보를 포함합니다. 이 기능을 활성화하려면 먼저 **sysopt traffic detailed-statistics** 명령을 입력해야 합니다.

ASA Services Module에서 스위치 작업이 이루어지는 방식

Cisco IOS 소프트웨어를 사용하여 Catalyst 6500 Series 및 Cisco 7600 Series 스위치에서 스위치 수퍼바이저 및 통합 MSFC 양쪽에 대해 ASASM을 설치할 수 있습니다.

참고 Catalyst OS(운영 체제)는 지원되지 않습니다.

ASA에서는 자체적인 운영 체제를 실행합니다.

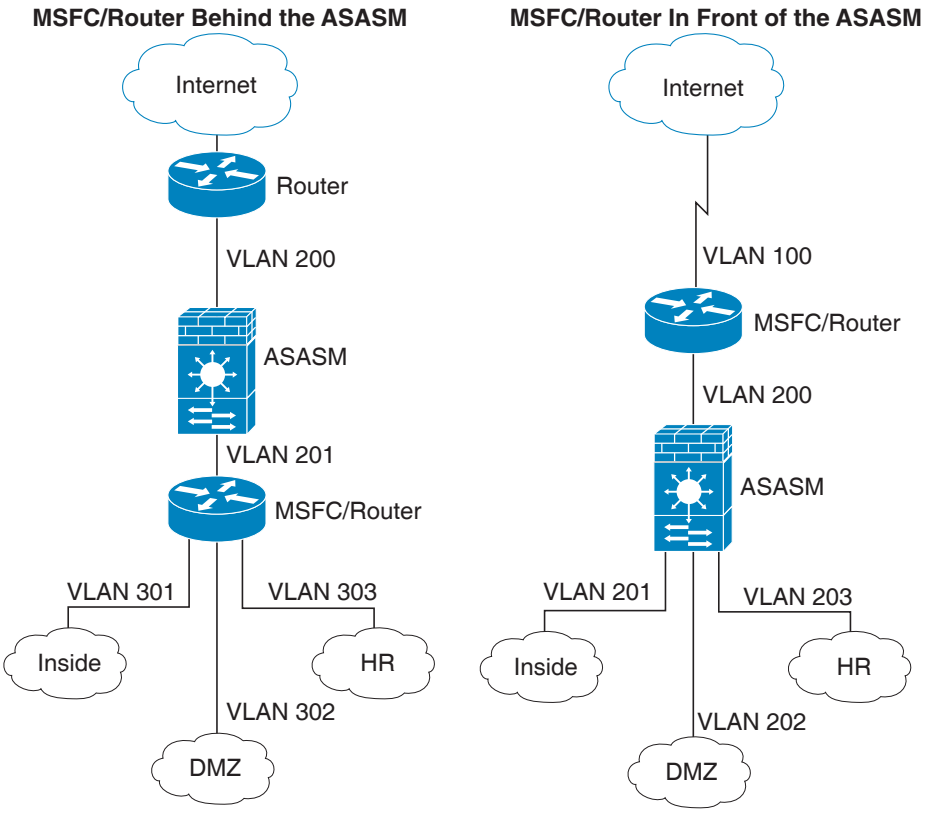
스위치에는 스위칭 프로세서(수퍼바이저) 및 라우터(MSFC)가 포함됩니다. 시스템에 MSFC가 있어야 하지만, 이를 사용할 필요는 없습니다. MSFC를 사용하도록 선택할 경우, MSFC에 하나 이상의 VLAN을 할당할 수 있습니다. 또는 MSFC 대신 외부 라우터를 사용할 수 있습니다.

단일 컨텍스트 모드의 경우 방화벽 앞이나 방화벽 뒤에 라우터를 배치할 수 있습니다(그림 1-1 참조).

라우터의 위치는 라우터에 할당하는 VLAN에 전적으로 달려 있습니다. 예를 들어, 왼쪽 그림 1-1 에 표시된 예에서 VLAN 201이 ASASM의 내부 인터페이스에 할당되었으므로 라우터가 방화벽의 뒤에 있습니다. 반대로 오른쪽 그림 1-1 에 표시된 예에서 VLAN 200이 ASASM의 외부 인터페이스에 할당되었으므로 라우터가 방화벽의 앞에 있습니다.

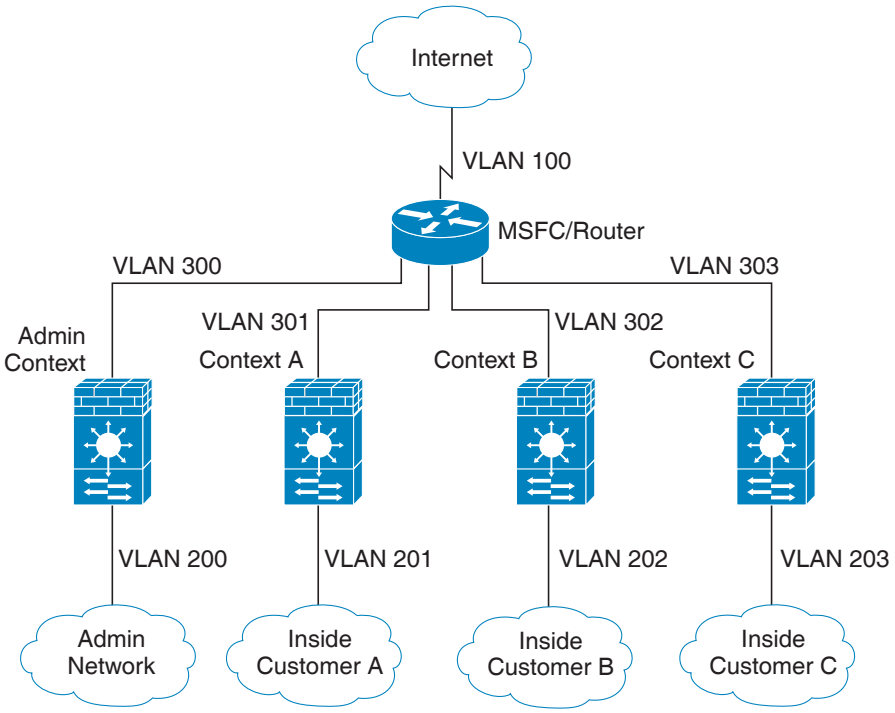
왼쪽 예에서 MSFC 또는 라우터는 VLAN 201, 301, 302, 303 사이를 라우팅하며, 내부 트래픽은 인터넷을 목적지로 하지 않는 한 ASASM을 통과하지 않습니다. 오른쪽 예의 경우 ASASM에서는 VLAN 201, 202, 203 간의 모든 트래픽을 처리하고 보호합니다.

그림 1-1 MSFC/라우터 배치



다중 컨텍스트 모드의 경우 ASASM 뒤에 라우터를 배치하면 이를 단일 컨텍스트로만 연결해야 합니다. 라우터를 다중 컨텍스트에 연결하면 라우터가 컨텍스트 간에 라우팅을 수행하며, 이는 원하는 작업 결과가 아닐 수 있습니다. 다중 컨텍스트의 일반적인 시나리오는 라우터를 모든 컨텍스트 앞에 사용하여 인터넷과 스위치 네트워크 간에 라우팅을 수행하는 것입니다(그림 1-2 참조)

그림 1-2 다중 컨텍스트로 MSFC/라우터 배치



방화벽 기능 개요

방화벽은 외부 네트워크의 사용자가 내부 네트워크에 무단 액세스하는 것을 차단합니다. 방화벽은 또한 내부 네트워크 사이에서도 상호 간 보호가 가능합니다. 인사부 네트워크를 사용자 네트워크로부터 분리하는 것 등이 그 예입니다. 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 있고, *내부* 네트워크는 방화벽 뒤에서 보호되고 있으며, *DMZ*는 방화벽 뒤에 있으나 외부 사용자에게 제한된 액세스를 허용하는 네트워크를 일컫습니다. 그러나 ASA에서는 여러 가지 보안 정책으로 많은 인터페이스(예: 다양한 내부 인터페이스, 다양한 DMZ, 다양한 외부 인터페이스)를 구성할 수 있도록 지원하므로, 이러한 용어는 일반적인 의미로만 사용됩니다.

- 1-8 페이지의 보안 정책 개요
- 1-10 페이지의 방화벽 모드 개요
- 1-10 페이지의 스테이트풀 감시 개요

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

액세스 목록을 적용하여 내부에서 외부로 나가는 트래픽을 제한하거나, 외부에서 내부로 들어오는 트래픽을 허용할 수 있습니다. 투명 방화벽 모드의 경우, EtherType 액세스 목록을 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 재결합하고, ASA를 통해 라우팅된 나머지 IP 프래그먼트를 가상으로 재결합하는 작업을 수행합니다. 보안 검사에 실패한 프래그먼트는 누락 및 기록됩니다. 가상 재결합은 비활성화할 수 없습니다.

통과 트래픽에 AAA 사용

HTTP 같은 특정 유형의 트래픽에 인증 및/또는 권한 부여를 요구할 수 있습니다. ASA에서는 RADIUS 또는 TACACS+ 서버에 대한 어카운팅 정보도 전송합니다.

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 정보를 포함하거나, 동적으로 할당된 포트에서 보조 채널을 여는 서비스에는 감시 엔진이 필요합니다. 이러한 프로토콜의 경우 ASA에서 심층 패킷 감시를 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

음성 및 스트리밍 비디오 같은 일부 네트워크 트래픽의 경우 긴 레이턴시 시간을 허용할 수 없습니다. 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. 초기 연결은 소스와 목적지 간에 필요한 핸드셰이크가 완료되지 않은 연결 요청입니다.

TCP 표준화는 정상으로 보이지 않는 패킷을 누락시키기 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 공격 검사는 서브넷에 있는 모든 IP 주소의 액세스 가능성을 테스트하는 호스트로 구성되어 있습니다(서브넷에 있는 다수의 호스트를 모두 검사하거나 호스트 또는 서브넷에 있는 다수의 포트를 모두 스위핑함). 위협 감지 검사 기능은 호스트가 언제 검사를 수행해야 할지 결정합니다. 트래픽 서명을 기반으로 하는 IPS 검사 감지와 달리, ASA 위협 감지 검사 기능의 경우 검사 활동을 분석할 수 있는 호스트 통계가 포함된 방대한 데이터베이스를 유지합니다.

호스트 데이터베이스에서는 반환 활동이 없는 연결, 닫힌 서비스 포트에 액세스, 취약한 TCP 동작(예: 임의적이지 않은 IPID) 등의 수많은 동작을 비롯한 의심스러운 활동을 추적합니다.

공격자에 대한 시스템 로그 메시지를 전송하도록 ASA를 구성하거나 호스트를 자동으로 피할 수 있습니다.

봇넷 트래픽 필터 활성화

악성코드는 알 수 없는 호스트에 설치되는 악성 소프트웨어입니다. 악성코드가 알려진 악성 IP 주소에 연결을 시작하면, 봇넷 트래픽 필터에서는 개인 데이터(비밀번호, 신용카드 번호, 키 스트로크, 독점 데이터) 전송 같은 네트워크 활동을 시도하는 악성코드를 감지할 수 있습니다. 봇넷 트래픽 필터에서는 알려진 악성 도메인 이름 및 IP 주소로 구성된 동적 데이터베이스(블랙리스트)를 기준으로, 들어오고 나가는 연결을 검사한 다음 모든 의심스러운 활동을 기록합니다. 악성코드 활동에 대한 syslog 메시지가 표시되면 해당 호스트를 격리하고 감염을 치료하기 위한 단계를 수행할 수 있습니다.

Cisco Unified Communications 구성

Cisco ASA Series는 유니파이드 커뮤니케이션 구축을 위한 프록시 기능을 제공하는 전략적 플랫폼입니다. 프록시의 용도는 클라이언트와 서버 간의 연결을 종료하고 다시 시작하기 위한 것입니다. 프록시에서는 트래픽 감시, 프로토콜 확인, 정책 제어 같은 다양한 보안 기능을 제공하여 내부 네트워크의 보안을 담당합니다. 점점 더 많이 사용되고 있는 프록시의 기능은 보안 정책을 적용하는 동시에 연결의 기밀성을 유지하기 위해 암호화된 연결을 종료하는 것입니다.

방화벽 모드 개요

ASA는 다음과 같은 두 가지 다른 방화벽 모드에서 실행됩니다.

- 라우팅
- 투명

라우팅 모드에서 ASA는 네트워크의 라우터 홉으로 간주합니다.

투명 모드에서 ASA는 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하며, 라우터 홉으로 간주하지 않습니다. ASA는 내부 및 외부 인터페이스에서 동일한 네트워크에 연결됩니다.

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

스테이트풀 감시 개요

ASA를 통과하는 모든 트래픽은 Adaptive Security Algorithm을 사용하여 감시되며 통과가 허용되거나 누락됩니다. 간단한 패킷 필터로 올바른 소스 주소, 목적지 주소, 포트를 확인할 수 있으나, 패킷 시퀀스 또는 플래그가 올바른지 여부는 확인할 수 없습니다. 또한 필터의 경우 해당 필터를 기준으로 *모든* 패킷을 확인하므로, 프로세스가 느릴 수 있습니다.

참고 TCP 상태 우회 기능을 사용하면 패킷 흐름을 맞춤화할 수 있습니다.

그러나 ASA 같은 스테이트풀 방화벽에서는 다음과 같은 패킷의 상태를 고려합니다.

- 새 연결인가?

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

  세션 관리 경로는 다음과 같은 작업에 직접적인 연관이 있습니다.

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

  ASA에서는 TCP 트래픽의 빠른 경로에서 전달 및 반대 흐름을 생성합니다. 또한 ASA에서는 UDP, ICMP(ICMP 감시를 활성화할 경우) 같은 무연결 프로토콜에 대한 연결 상태 정보도 생성하여, 마찬가지로 빠른 경로를 사용할 수 있도록 합니다.

  참고 ASA의 경우 SCTP 같은 다른 IP 프로토콜에 대해서는 반대 경로 흐름을 생성하지 않습니다. 결과적으로 이러한 연결을 참조하는 ICMP 오류 패킷은 누락됩니다.

  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 및 SNMP가 포함됩니다.

- 설정되어 있는 연결인가?

  연결이 기존에 설정되어 있는 경우 ASA에서는 패킷을 다시 확인할 필요가 없습니다. 일치하는 대부분의 패킷은 양방향에서 모두 "빠른" 경로를 통과할 수 있습니다. 빠른 경로는 다음과 같은 작업에 직접적인 연관이 있습니다.

  – 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. 이러한 보안 연결을 터널이라고 합니다. ASA에서는 터널링 프로토콜을 사용하여 보안 매개변수를 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 목적지로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 목적지로 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 할당
- 데이터 암호화 및 해독
- 보안 키 관리
- 터널 전반의 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로서 데이터 전송 인바운드 및 아웃바운드 관?

ASA에서는 다양한 표준 프로토콜을 호출하여 이러한 기능을 구현합니다.

보안 컨텍스트 개요

단일 ASA를 보안 컨텍스트라고 하는 다중 가상 디바이스로 분할할 수 있습니다. 각 컨텍스트는 고유한 보안 정책, 인터페이스 및 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 컨텍스트 모드에서는 ASA에 보안 정책, 인터페이스 및 독립형 디바이스에서 구성할 수 있는 거의 모든 옵션을 식별하는, 각 컨텍스트에 대한 컨피그레이션이 포함됩니다. 시스템 관리자는 시스템 컨피그레이션(단일 모드 컨피그레이션과 마찬가지로 시작 컨피그레이션)에서 컨텍스트를 구성하여 컨텍스트를 추가하고 관리할 수 있습니다. 시스템 컨피그레이션은 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 하며, 그 후 이러한 컨피그레이션은 컨피그레이션원 유닛으로 복제됩니다.

특별 레거시 서비스

일부 서비스의 설명서는 주요 컨피그레이션 설명서 및 온라인 도움말 이외의 위치에 있습니다. 전체 설명서 목록을 보려면 다음을 참조하십시오.

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

- 1-13 페이지의 특별 서비스 설명서
- 1-13 페이지의 레거시 서비스 설명서

특별 서비스 설명서

특별 서비스에서는 ASA와 기타 Cisco 제품 간의 상호 운용을 지원합니다. 이를테면 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 들 수 있습니다. 이러한 특별 서비스 중 일부는 별도의 설명서에서 다룹니다.

레거시 서비스 설명서

레거시 서비스는 ASA에서 계속 지원되지만, 해당 서비스 대신 사용할 수 있는 향상된 대체 서비스가 제공될 수 있습니다. 레거시 서비스에 대한 내용은 별도의 설명서에서 다룹니다.

2 장

시작하기

이 장에서는 Cisco ASA를 시작하는 방법에 대해 설명합니다.

Command-Line Interface용 콘솔 액세스

초기 컨피그레이션의 경우에는 콘솔 포트에서 CLI에 직접 액세스합니다. 나중에 35 장, "관리 액세스" 에 따라 텔넷이나 SSH를 사용하여 원격 액세스를 구성할 수 있습니다. 시스템이 이미 다중 컨텍스트 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.

절차

1단계 제공된 콘솔 케이블을 사용하여 PC를 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 설명서를 참조하십시오.

2단계 **Enter** 키를 누르면 다음 프롬프트가 표시됩니다.

```
ciscoasa>
```

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

3단계 특권 EXEC 모드에 액세스하려면 다음 명령을 입력합니다.

```
ciscoasa> enable
```

다음 프롬프트가 나타납니다.

```
Password:
```

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

4단계 프롬프트에서 enable 비밀번호를 입력합니다.

기본적으로 비밀번호는 비어 있으며 계속하려면 **Enter** 키를 누릅니다. enable 비밀번호를 변경하려면 13-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정을 참조하십시오.

프롬프트가 다음과 같이 변경됩니다.

```
ciscoasa#
```

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

5단계 전역 컨피그레이션 모드에 액세스하려면 다음 명령을 입력합니다.

```
ciscoasa# configure terminal
```

프롬프트가 다음과 같이 바뀝니다.

```
ciscoasa(config)#
```

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

ASA Services Module 콘솔 액세스

초기 컨피그레이션의 경우에는 스위치에 연결(콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음 ASASM에 연결하여 Command-Line Interface에 액세스합니다. 이 섹션에서는 ASASM CLI에 액세스하는 방법을 설명합니다.

- 2-2 페이지의 연결 방법 정보
- 2-3 페이지의 ASA Services Module에 로그인
- 2-5 페이지의 콘솔 세션에서 로그아웃
- 2-5 페이지의 활성화된 콘솔 연결 끊기
- 2-6 페이지의 텔넷 세션에서 로그아웃

연결 방법 정보

스위치 CLI에서 다음 두 가지 방법을 사용하여 ASASM에 연결할 수 있습니다.

- 가상 콘솔 연결 — **service-module session** 명령을 사용하여 ASASM에 대한 가상 콘솔 연결을 생성하며, 여기에는 실제 콘솔 연결의 이점과 제한 사항이 모두 포함됩니다.

혜택은 다음과 같습니다.

- 다시 로드하는 경우에도 전반적으로 연결이 지속적이며 시간이 초과되지 않습니다.
- ASASM 다시 로드를 통해 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.

- 연결 속도가 느립니다(9600baud).
- 한 번에 하나의 콘솔만 연결할 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 연결할 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 사용하십시오.

  참고 ASASM에서 올바르게 로그아웃하지 않을 경우 콘솔 연결 상태가 계속 유지되어 의도한 시간보다 오래 연결이 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 ASASM에 대한 텔넷 로그인 비밀번호를 구성해야 합니다(기본 비밀번호 없음). **passwd** 명령을 사용하여 비밀번호를 설정하면 이 방법을 사용할 수 있습니다.

  혜택은 다음과 같습니다.

  - ASASM에 대한 여러 세션을 동시에 받을 수 있습니다.
  - 텔넷 세션은 연결 속도가 빠릅니다.

  제한 사항은 다음과 같습니다.

  - ASASM이 다시 로드될 경우 텔넷 세션이 종료되며 시간이 초과될 수 있습니다.
  - 완전히 로드될 때까지 ASASM에 액세스할 수 없으며 ROMMON에 액세스할 수 없습니다.
  - 먼저 텔넷 로그인 비밀번호를 설정해야 합니다. 기본 비밀번호는 없습니다.

ASA Services Module에 로그인

초기 컨피그레이션의 경우에는 스위치에 연결(스위치 콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음 ASASM에 연결하여 Command-Line Interface에 액세스합니다.

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

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

절차

1단계 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 액세스합니다.

- 로그인 비밀번호 구성 후 사용 가능한 방법 — 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 로그인 비밀번호를 입력합니다. **passwd** 명령을 사용하여 비밀번호를 설정합니다. 기본 비밀번호가 없습니다.

  사용자 EXEC 모드에 액세스합니다.

2단계 가장 권한 수준이 높은 특권 EXEC 모드에 액세스합니다.

enable

예:

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

프롬프트에서 enable 비밀번호를 입력합니다. 기본적으로 비밀번호는 비어 있습니다.

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

3단계 전역 컨피그레이션 모드 액세스:

configure terminal

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

관련 주제

- 35-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성.
- 13-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정

콘솔 세션에서 로그아웃

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

다른 사용자가 의도치 않게 열어둔 활성화된 연결을 끊으려면 2-5 페이지의 활성화된 콘솔 연결 끊기를 참조하십시오.

절차

1단계 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 오래 연결이 지속될 수 있습니다. 다른 사람이 로그인하려면 기존 연결을 끊어야 합니다.

절차

1단계 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.

```
Router# 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
```

2단계 콘솔 연결이 포함된 행을 지우려면 다음 명령을 입력합니다.

```
Router# clear line number
```

예:

```
Router# clear line 0
```

텔넷 세션에서 로그아웃

텔넷 세션을 종료하고 스위치 CLI에 액세스하여 다음 단계를 수행합니다.

절차

1단계 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 컨피그레이션에 따라 시간이 초과될 수 있습니다.

ASDM 액세스 구성

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

- 2-6 페이지의 ASDM 액세스에 공장 기본 컨피그레이션 사용(어플라이언스, ASAv)
- 2-7 페이지의 어플라이언스 및 ASAv를 위한 ASDM 액세스 맞춤화
- 2-9 페이지의 ASA Services Module에 대한 ASDM 액세스 구성

ASDM 액세스에 공장 기본 컨피그레이션 사용(어플라이언스, ASAv)

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

절차

1단계 다음 인터페이스 및 네트워크 설정을 사용하여 ASDM에 연결합니다.

- 관리 인터페이스는 사용하는 모델에 따라 달라집니다.
  - ASA 5512-X 이상 — ASDM에 연결하는 인터페이스는 Management 0/0입니다.
  - ASAv— ASDM에 연결하는 인터페이스는 Management 0/0입니다.

- 기본 관리 주소는 다음과 같습니다.
  - ASA 어플라이언스 — 192.168.1.1.
  - ASAv— 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. ASAv에서는 연결된 클라이언트의 DHCP 서버로 작동하지 않습니다.

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

관련 주제

- 2-12 페이지의 공장 기본 컨피그레이션
- 6-15 페이지의 다중 컨텍스트 모드 활성화 또는 비활성화
- 2-11 페이지의 ASDM 시작

어플라이언스 및 ASAv를 위한 ASDM 액세스 맞춤화

다음 조건 중 *하나 이상*이 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.

절차

1단계 콘솔 포트에서 CLI에 액세스합니다.

2단계 (선택 사항) 투명 방화벽 모드를 활성화합니다.

이 명령을 실행하면 컨피그레이션이 지워집니다.

```
firewall transparent
```

3단계 관리 인터페이스를 구성합니다.

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

예:

```
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 1~100 사이의 숫자로 설정하며 100이 가장 안전한 수준입니다.

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

dhcpd address *ip_address-ip_address interface_name*
dhcpd enable *interface_name*

예:

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

범위에 관리 주소가 포함되어 있지 않은지 확인합니다.

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

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

예:

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

6단계 ASDM에 대한 HTTP 서버를 활성화합니다.

http server enable

7단계 관리 호스트에서 ASDM에 액세스하도록 허용합니다.

http *ip_address mask interface_name*

예:

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

8단계 컨피그레이션을 저장합니다.

write memory

9단계 (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 구성하고, 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 주제

- 2-13 페이지의 공장 기본 컨피그레이션 복원
- 5-9 페이지의 방화벽 모드 설정
- 2-1 페이지의 어플라이언스 콘솔 액세스
- 2-11 페이지의 ASDM 시작
- 6 장, "다중 컨텍스트 모드"

ASA Services Module에 대한 ASDM 액세스 구성

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

시작하기 전에

ASASM 빠른 시작 설명서에 따라 ASASM VLAN 인터페이스를 할당하십시오.

절차

1단계 ASASM에 연결하고 전역 컨피그레이션 모드에 액세스합니다.

2단계 (선택 사항) 투명 방화벽 모드를 활성화합니다.

firewall transparent

이 명령을 실행하면 컨피그레이션이 지워집니다.

3단계 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 — 브릿지 가상 인터페이스를 구성하고 브릿지 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.

4단계 (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
```

예:

```
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.

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

```
route management_ifc management_host_ip mask gateway_ip 1
```

예:

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

6단계 ASDM에 대한 HTTP 서버를 활성화합니다.

```
http server enable
```

7단계 관리 호스트에서 ASDM에 액세스하도록 허용합니다.

```
http ip_address mask interface_name
```

예:

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

8단계 컨피그레이션을 저장합니다.

```
write memory
```

9단계 (선택 사항) 모드를 다중 모드로 설정합니다.

```
mode multiple
```

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

예

다음 라우팅 모드 컨피그레이션에서는 VLAN 1 인터페이스를 구성하고 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 주제

- 2-2 페이지의 ASA Services Module 콘솔 액세스
- 6 장, "다중 컨텍스트 모드"
- 5-9 페이지의 방화벽 모드 설정

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. Launcher를 사용하면 로컬로 다운로드한 파일을 사용하여 데모 모드에서 가상 ASDM을 실행할 수도 있습니다.
- Java Web Start — ASA를 관리하는 모든 경우 웹 브라우저에 연결한 다음 Java Web Start 애플리케이션을 저장하거나 이 애플리케이션을 시작해야 합니다. 선택에 따라 PC에 바로 가기를 저장할 수는 있으나 ASA IP 주소마다 별도의 바로 가기를 지정해야 합니다.

ASDM 내에서는 여러 개의 ASA IP 주소를 선택하여 관리할 수 있습니다. Launcher와 Java Web Start 기능의 주요 차이점은 맨 처음 ASA에 연결하고 ASDM을 시작하는 방법에 있습니다.

ASDM을 사용하면 여러 개의 PC 또는 워크스테이션 간에 동일한 ASA 소프트웨어로 각각 하나의 브라우저 세션을 열 수 있습니다. 하나의 ASA에서는 단일 라우팅 모드에서 최대 5개의 동시 ASDM 세션을 지원할 수 있습니다. ASA에는 PC 또는 워크스테이션당 브라우저 하나에 1개의 세션만 지원됩니다. 다중 컨텍스트 모드의 경우, 컨텍스트당 5개의 동시 ASDM 세션이 지원되며, 각 ASA당 최대 총 32개의 연결이 지원됩니다.

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

절차

1단계 ASDM 클라이언트로 지정한 PC에서 다음 URL을 입력합니다.

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

다음 버튼이 있는 ASDM 시작 페이지가 나타납니다.

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

2단계 Launcher를 다운로드하려면

a. **Install ASDM Launcher and Run ASDM**을 클릭합니다.

b. 사용자 이름 및 비밀번호 필드를 비워 두고(신규 설치) **OK**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.

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

d. 관리 IP 주소를 입력하고 사용자 이름과 비밀번호는 비워 둔 다음(신규 설치의 경우) **OK**를 클릭합니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

3단계 Java Web Start를 사용하려면

a. **Run ASDM** 또는 **Run Startup Wizard**를 클릭합니다.

b. 프롬프트에 따라 바로가기를 PC에 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 비밀번호를 비워 두고(신규 설치) **OK**를 클릭합니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

공장 기본 컨피그레이션

공장 기본 컨피그레이션은 Cisco에서 신규 ASA에 적용하는 컨피그레이션입니다.

- ASA 어플라이언스 — 공장 기본 컨피그레이션을 통해 관리용 인터페이스가 구성되므로 ASDM을 함께 사용하여 ASA 어플라이언스에 연결하고 컨피그레이션을 완료할 수 있습니다.
- ASAv— 구축 과정에서 구축 컨피그레이션(초기 가상 구축 설정)을 통해 관리용 인터페이스가 구성되므로, ASDM을 함께 사용하여 ASAv에 연결하고 컨피그레이션을 완료할 수 있습니다. 또한 장애 조치 IP 주소를 구성할 수 있습니다. 필요한 경우 "공장 초기화" 컨피그레이션을 적용할 수 있습니다.
- ASASM— 기본 컨피그레이션이 없습니다. 컨피그레이션을 시작하려면 2-2 페이지의 ASA Services Module 콘솔 액세스를 참조하십시오.

공장 기본 컨피그레이션은 라우팅 방화벽 모드 및 단일 컨텍스트 모드에서만 사용할 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.

- 2-13 페이지의 공장 기본 컨피그레이션 복원
- 2-14 페이지의 ASAv 구축 컨피그레이션 복원
- 2-14 페이지의 ASA 어플라이언스 기본 컨피그레이션
- 2-15 페이지의 ASAv 구축 컨피그레이션

공장 기본 컨피그레이션 복원

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

참고 ASASM에서 공장 기본 컨피그레이션을 복원하면 컨피그레이션이 지워지며 공장 기본 컨피그레이션이 존재하지 않습니다.

시작하기 전에

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

절차

1단계 공장 기본 컨피그레이션을 복원합니다.

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

예:

```
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 명령어를 사용하면 **boot system** 명령과 함께 나머지 컨피그레이션도 지워집니다. **boot system** 명령을 사용하면 외부 플래시 메모리 카드의 이미지를 비롯한 특정 이미지에서 부팅할 수 있습니다. 공장 기본 설정을 복원한 후 다음번에 ASA를 다시 로드 할 경우, 내부 플래시 메모리의 첫 번째 이미지에서 부팅이 이루어집니다. 내부 플래시 메모리에 이미지가 없는 경우 ASA에서는 부팅을 수행하지 않습니다.

2단계 플래시 메모리에 기본 컨피그레이션을 저장합니다.

write memory

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

ASAv 구축 컨피그레이션 복원

이 섹션에서는 ASAv 구축 컨피그레이션을 복원하는 방법에 대해 설명합니다.

절차

1단계 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.

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

```
write erase
```

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

컨피그레이션을 저장하지 마십시오.

3단계 ASAv를 다시 로드하고 구축 컨피그레이션을 로드합니다.

```
reload
```

4단계 장애 조치를 수행하려면 스탠바이 유닛의 전원을 켭니다.

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

ASA 어플라이언스 기본 컨피그레이션

ASA 어플라이언스에 대한 공장 초기 컨피그레이션에서는 다음을 구성합니다.

  - 관리 인터페이스 — Management 0/0(관리).
- IP 주소 — 관리 주소는 192.168.1.1/24입니다.
- DHCP 서버 — 관리 호스트에 사용되며 관리 인터페이스에 연결된 PC에서는 192.168.1.2~192.168.1.254 사이의 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 100
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 lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASAv 구축 컨피그레이션

ASAv를 구성할 경우 ASDM을 사용하여 Management 0/0 인터페이스에 연결할 수 있도록 지원하는 다양한 매개변수를 사전 설정할 수 있습니다. 일반적인 컨피그레이션에는 다음과 같은 설정이 포함됩니다.

- Management 0/0 인터페이스:
  - 이름이 지정된 "관리"
  - IP 주소 또는 DHCP
  - 보안 수준 0
  - 관리 전용
- 기본 게이트웨이를 통해 관리 인터페이스에서 관리 호스트 IP 주소에 이르는 고정 경로
- ASDM 서버 사용
- 관리 호스트 IP 주소에 대한 ASDM 액세스
- (선택 사항) GigabitEthernet 0/8 및 Management 0/0 스탠바이 IP 주소에 대한 장애 조치 링크 IP 주소

독립형 유닛의 경우 다음 컨피그레이션을 참조하십시오.

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
```

장애 조치 쌍에 있는 기본 유닛의 경우 다음 컨피그레이션을 참조하십시오.

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address standby standby_ip
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
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 컨피그레이션이라는 텍스트 파일에서 컨피그레이션을 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.

컨피그레이션 변경 사항 저장

이 섹션에서는 컨피그레이션을 저장하는 방법에 대해 설명합니다.

단일 컨텍스트 모드에서 컨피그레이션 변경 사항 저장

실행 중인 컨피그레이션을 시작 컨피그레이션에 저장하려면 다음 절차를 수행합니다.

절차

1단계 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.

절차

1단계 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 컨텍스트 URL에서 확인된 서버에 컨피그레이션을 다시 저장합니다. 이때 HTTP 또는 HTTPS URL을 사용하면 컨피그레이션을 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.

절차

1단계 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 입력하면 ASA 에서는 시스템 컨피그레이션 및 각 컨텍스트를 저장합니다. 컨텍스트 시작 컨피그레이션은 외부 서버에 상주할 수 있습니다. 이 경우 ASA에서는 컨텍스트 URL에서 확인된 서버에 컨피그레이션을 다시 저장합니다. 이때 HTTP 또는 HTTPS URL을 사용하면 컨피그레이션을 서버에 저장할 수 없으므로 이러한 URL은 제외됩니다.

ASA에서 각 컨텍스트를 저장하면 다음 메시지가 표시됩니다.

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

일부 경우 오류로 인해 컨텍스트가 저장되지 않습니다. 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 목적지에 전달될 수 없어 컨텍스트가 저장되지 않은 경우 다음과 같은 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' .
  ```

다른 사용자가 이미 컨피그레이션을 저장했거나 삭제 중인 경우에만 컨텍스트가 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 컨텍스트 실행에 영향을 줄 경 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다.

- **reload**

  ASA을(를) 다시 로드하면 시작 컨피그레이션이 로드되고 실행 중인 컨피그레이션이 지워집니다.

- **clear configure all** 및 **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 컨피그레이션을 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 컨피그레이션을 지웁니다.

참고 ASAv에서 이 명령을 사용하면 다시 로드 후 구축 컨피그레이션이 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 명령어를 사용하면 **boot system** 명령과 함께 나머지 컨피그레이션도 지워집니다. **boot system** 명령을 사용하면 외부 플래시 메모리 카드의 이미지를 비롯한 특정 이미지에서 부팅할 수 있습니다. 다음번에 ASA를 다시 로드 할 경우, 내부 플래시 메모리의 첫 번째 이미지에서 부팅이 이루어집니다. 내부 플래시 메모리에 이미지가 없는 경우 ASA에서는 부팅을 수행하지 않습니다.

오프라인에서 텍스트 컨피그레이션파일 생성

이 설명서에서는 CLI를 사용하여 ASA을(를) 구성하는 방법에 대해 설명합니다. 명령을 저장하면 변경 사항이 텍스트 파일에 작성됩니다. 그러나 CLI를 사용하는 대신 PC에서 직접 텍스트 파일을 편집하여 컨피그레이션 모드 명령줄 프롬프트에 컨피그레이션을 전체 또는 한 줄씩 붙여넣을 수도 있습니다. 또는 ASA 내부 플래시 메모리에 텍스트 파일을 다운로드 할 수 있습니다. 36 장, "소프트웨어 및 컨피그레이션"에서 ASA에 컨피그레이션 파일을 다운로드하는 방법을 참조하십시오.

대부분의 경우, 이 설명서에 설명된 명령은 CLI 프롬프트 앞에 나옵니다. 다음 예의 프롬프트는 다음과 같습니다. "ciscoasa(config)#":

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

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

```
context a
```

파일 형식 지정에 대한 자세한 내용은 부록 42, "Command-Line Interface 사용"을(를) 참조하십시오.

연결에 컨피그레이션 변경 사항 적용

컨피그레이션에 대한 보안 정책을 변경하면 모든 *새* 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결을 설정할 당시 구성된 정책을 계속 사용합니다. 기존 연결에 대한 **show** 명령 출력에는 기존 컨피그레이션이 반영되며, 경우에 따라 기존 연결에 대한 데이터가 포함되지 않을 수도 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 참조합니다.

  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.

ASA다시 로드

ASA을(를) 다시 로드하려면 다음 절차를 완료하십시오.

절차

1단계 ASA를 다시 로드합니다.

```
reload
```

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

3 장

Cisco ASA Services Module에 대한 스위치 컨피그레이션

이 장에서는 Catalyst 6500 Series 또는 Cisco 7600 Series 스위치를 Cisco ASA Services Module (ASASM)과(와) 함께 사용하는 방법에 대해 알아봅니다. 이 장의 절차를 완료하기 전에, 해당 스위치와 함께 제공된 설명서에 따라 스위치 포트에 VLAN을 할당하는 작업을 비롯하여 스위치의 기본 속성을 구성하십시오.

스위치 정보

지원되는 스위치 하드웨어 및 소프트웨어

Catalyst 6500 Series 및 Cisco 7600 Series 스위치에서 ASASM을(를) 설치할 수 있습니다. 스위치에는 스위치(수퍼바이저 엔진)와 라우터(MSFC)가 포함됩니다.

스위치의 스위치 수퍼바이저 엔진 및 통합 MSFC 라우터에서는 모두 Cisco IOS 소프트웨어를 지원합니다.

참고 Catalyst 운영 체제 소프트웨어는 지원되지 않습니다.

ASASM에서는 자체적인 운영 체제를 실행합니다.

참고 ASASM에서 자체적인 운영 체제를 실행하므로 Cisco IOS 소프트웨어를 업그레이드해도 ASASM의 작동에 영향을 미치지 않습니다.

ASASM 및 Cisco IOS 버전의 하드웨어 및 소프트웨어 호환성 매트릭스를 보려면 *Cisco ASA Series 하드웨어 및 소프트웨어 호환성*을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

백플레인 연결

ASASM 과(와) 스위치 간의 연결은 단일한 20-GB 인터페이스입니다.

ASA 및 Cisco IOS 기능 상호 작용

일부 ASASM 기능은 Cisco IOS 기능과 상호 작용합니다. 다음 기능은 Cisco IOS 소프트웨어와 연동됩니다.

- VSS(Virtual Switching System) — ASASM 컨피그레이션이 필요하지 않습니다.
- Autostate — 제공된 VLAN의 마지막 인터페이스가 종료될 경우 수퍼바이저는 ASASM에 이를 알림으로써 장애 조치 스위치의 필요 여부를 결정할 수 있도록 지원합니다.
- 장애 조치 스위치에서 수퍼바이저 MAC 주소 테이블의 항목 지우기 — ASASM 컨피그레이션이 필요하지 않습니다.
- 버전 호환성 — 수퍼바이저/ASASM 버전 호환성 매트릭스 확인이 실패할 경우 ASASM의 전원이 자동으로 꺼집니다.

SVI 정보

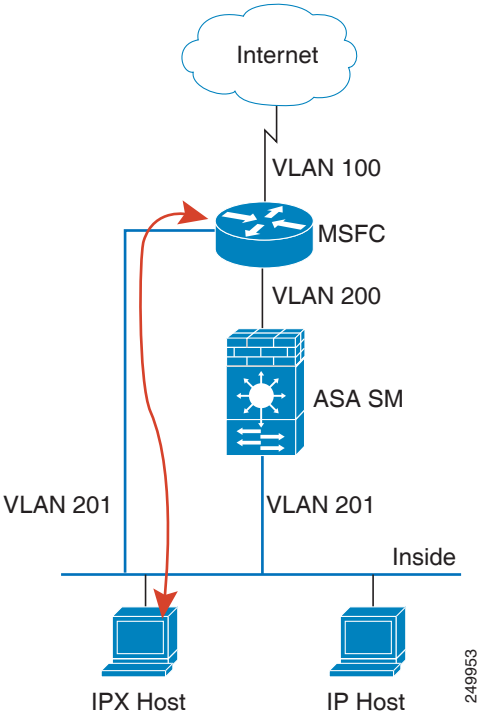
MSFC를 직접 연결된 라우터로 사용하려면(예: ASASM 외부 인터페이스에 연결된 기본 게이트웨이로 사용), ASASM VLAN 인터페이스를 SVI(스위치 가상 인터페이스)로서 MSFC에 연결합니다.

보안상의 이유로 인해, 기본적으로 MSFC와 ASASM 간에는 하나의 SVI를 구성할 수 있습니다. 다중 SVI를 사용할 수는 있으나 네트워크를 잘못 구성하지 않도록 주의해야 합니다.

예를 들어, 다중 SVI를 사용할 경우 내부 및 외부 VLAN을 MSFC에 할당하여 실수로 트래픽이 ASASM을(를) 지나 통과하도록 허용할 수 있습니다.

일부 네트워크 시나리오에서는 ASASM을(를) 우회해야 할 수 있습니다. 그림 3-1 에는 IP 호스트와 동일한 이더넷 세그먼트의 IPX 호스트가 나와 있습니다. 라우팅 방화벽 모드의 경우 ASASM에서는 IP 트래픽만 처리하고 IPX(투명 방화벽 모드에서는 선택에 따라 비 IP 트래픽을 허용할 수 있음) 같은 기타 프로토콜 트래픽은 누락하므로, IPX 트래픽을 위해 ASASM을(를) 우회하고자 할 수 있습니다. VLAN 201에서 IPX 트래픽만 통과하도록 허용하는 액세스 목록으로 MSFC를 구성해야 합니다.

그림 3-1 IPX에 다중 SVI 사용



다중 컨텍스트 모드에서 투명 방화벽을 지원하려면, 각 컨텍스트에는 외부 인터페이스의 고유한 VLAN이 필요하므로 다중 SVI를 사용해야 합니다. 라우팅 모드에서 다중 SVI를 사용하도록 선택하여 외부 인터페이스의 단일한 VLAN을 공유하지 않도록 할 수도 있습니다.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

VLAN 지침 및 제한 사항

- 1001에 VLAN ID 2개를 사용합니다.
- 사설 VLAN을 ASASM과(와) 함께 사용할 수 있습니다. 기본 VLAN을 ASASM에 할당합니다. ASASM에서는 보조 VLAN 트래픽을 자동으로 처리합니다. 이 기능을 사용하기 위해 ASASM에서 컨피그레이션을 수행하지 않아도 됩니다. 자세한 내용은 스위치 컨피그레이션 설명서를 참조하십시오. 3-5페이지의 ASA Services Module에 VLAN 할당의 예도 참조하십시오.
- 예약된 VLAN을 사용할 수 없습니다.
- VLAN 1을 사용할 수 없습니다.
- 동일한 스위치 섀시 내에서 ASASM 장애 조치를 사용할 경우, 장애 조치 및 스테이트풀 통신을 위해 예약된 VLAN을 스위치 포트에 할당하지 마십시오. 그런 섀시 간에 장애 조치를 사용할 경우에는 섀시 간의 트렁크 포트에 VLAN을 포함해야 합니다.
- ASASM에 할당하기 전에 VLAN을 스위치에 추가하지 않으면 VLAN이 수퍼바이저 엔진 데이터베이스에 저장되며 스위치에 추가되는 즉시 ASASM에 전송됩니다.

- 스위치에 할당하기 전에 ASASM 컨피그레이션에서 VLAN을 구성할 수 있습니다. 스위치에서 VLAN을 ASASM에 전송할 경우, VLAN은 기본적으로 ASASM에서 관리용으로 가동할 수 있는 상태가 되며 ASASM 컨피그레이션에서 VLAN을 종료한 경우에도 마찬가지입니다. 이 경우 VLAN을 다시 종료해야 합니다.

SPAN 리플렉터 지침

Cisco IOS 소프트웨어 버전 12.2SXJ1 이하에서는 스위치의 각 ASASM에 SPAN 리플렉터 기능이 활성화되어 있습니다. 이 기능을 사용하면 멀티캐스트 트래픽(및 중앙 리라이트 엔진이 필요한 기타 트래픽)이 ASASM에서 들어올 때 이를 전환할 수 있습니다. SPAN 리플렉터 기능에서는 하나의 SPAN 세션을 사용합니다. 이 기능을 비활성화하려면 다음 명령을 입력합니다.

```
Router(config)# no monitor session servicemodule
```

모듈 설치 확인

스위치에서 ASASM을(를) 인식하고 온라인 상태인지 확인하려면 다음 명령을 입력합니다.

세부 단계

명령	목적
show module [**switch** {**1** |**2**}] [*mod-num* | **all**]	모듈 정보가 표시됩니다. VSS의 스위치를 보려면 **switch** 키워드를 입력합니다.
예: `Router# show module 1`	Status 열에 ASASM의 상태가 "Ok"로 표시되는지 확인합니다.

예

다음은 **show module** 명령의 샘플 결과입니다.

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2     3  ASA Service Module                     WS-SVC-ASA-SM1     SAD143502E8
 4     3  ASA Service Module                     WS-SVC-ASA-SM1     SAD135101Z9
 5     5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6    16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e    0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655    0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13    2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f    1.0   12.2(18r)S1  12.2(2010121 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok
```

```
Base PID:
Mod  Model            Serial No.
---- ------------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2   Pass
2/0 Not Applicable
 4   Not Applicable
4/0 Not Applicable
 5   Pass
 6   Pass
```

ASA Services Module에 VLAN 할당

이 섹션에서는 ASASM에 VLAN을 할당하는 방법을 설명합니다. ASASM에는 외부 물리적 인터페이스가 포함되지 않습니다. 그 대신 VLAN 인터페이스를 사용합니다. VLAN을 ASASM에 할당하는 작업은 스위치 포트에 VLAN을 할당하는 것과 유사합니다. ASASM에는 스위치 패브릭 모듈(있는 경우) 또는 공유 버스에 대한 내부 인터페이스가 포함됩니다.

전제 조건

VLAN을 스위치에 추가하고 이를 스위치 포트에 할당하는 방법은 스위치 설명서를 참조하십시오.

지침

- 각 ASASM에 최대 16개의 방화벽 VLAN 그룹을 할당할 수 있습니다. (Cisco IOS 소프트웨어에서 16개 이상의 VLAN 그룹을 생성할 수 있지만, ASASM당 16개만 할당할 수 있습니다.) 예를 들어, 모든 VLAN을 하나의 그룹에 할당하거나, 내부 그룹 및 외부 그룹을 생성하거나, 각 고객에 대한 그룹을 하나씩 생성할 수 있습니다.
- 그룹당 VLAN 개수에는 제한이 없으나, ASASM에서는 ASASM 시스템 제한의 최대치에 해당하는 개수의 VLAN만 사용할 수 있습니다(자세한 내용은 ASASM 라이센스 설명서를 참조하십시오).
- 여러 방화벽 그룹에 같은 VLAN을 할당할 수 없습니다.
- 여러 ASASM에 단일한 방화벽 그룹을 할당할 수 있습니다. 예를 들어, 여러 ASASM에 할당하려는 VLAN은 ASASM마다 고유한 VLAN과 분리된 그룹에 상주할 수 있습니다.
- 3-3 페이지의 VLAN 지침 및 제한 사항을 참조하십시오.

세부 단계

	명령	목적
1단계	**firewall vlan-group** *firewall_group vlan_range* **예:** `Router(config)# firewall vlan-group 1 55-57`	방화벽 그룹에 VLAN을 할당합니다. *firewall_group* 인수는 정수입니다. *vlan_range* 인수는 다음 중 한 가지 방법을 통해 확인된 하나 이상의 VLAN(2 또는 1001)일 수 있습니다. • 단일 번호(*n*) • 범위(*n-x*) 다음 예에 나온 것처럼 쉼표로 분리된 별도의 번호 또는 범위: **5,7-10,13,45-100**
2단계	**firewall** [**switch** {**1** |**2**}] **module** *slot* **vlan-group** *firewall_group* **예:** `Router(config)# firewall module 5 vlan-group 1`	방화벽 그룹을 ASASM에 할당합니다. VSS에 있는 스위치의 경우 **switch** 인수를 입력합니다. ASASM이(가) 설치된 슬롯을 보려면 **show module** 명령을 입력합니다. *firewall_group* 인수는 다음 중 하나에 해당하는 하나 이상의 그룹 번호입니다. • 단일 번호(*n*) • 범위(*n-x*) 다음 예에 나온 것처럼 쉼표로 분리된 별도의 번호 또는 범위: **5,7-10**

예

다음 예에는 3개의 방화벽 VLAN 그룹을 생성하는 방법이 나와 있습니다. 각각 하나씩 ASASM에 사용되며 VLAN이 포함된 방화벽은 두 ASASM에 할당됩니다.

```
Router(config)# firewall vlan-group 10 55-57
Router(config)# firewall vlan-group 11 70-85
Router(config)# firewall vlan-group 12 100
Router(config)# firewall module 5 vlan-group 10,12
Router(config)# firewall module 8 vlan-group 11,12
```

다음 예에는 기본 VLAN을 ASASM에 할당하여 스위치에서 사설 VLAN을 구성하는 방법이 나와 있습니다.

1단계 기본 VLAN 200을 방화벽 VLAN 그룹에 추가하고 해당 그룹을 ASASM에 할당합니다.

```
Router(config)# firewall vlan-group 10 200
Router(config)# firewall module 5 vlan-group 10
```

2단계 VLAN 200을 기본 VLAN으로 지정합니다.

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan primary
```

3단계 분리된 보조 VLAN을 하나만 지정합니다. 하나 이상의 보조 커뮤니티 VLAN을 지정합니다.

```
Router(config)# vlan 501
Router(config-vlan)# private-vlan isolated
Router(config)# vlan 502
Router(config-vlan)# private-vlan community
Router(config)# vlan 503
Router(config-vlan)# private-vlan community
```

4단계 보조 VLAN을 기본 VLAN에 연결합니다.

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan association 501-503
```

5단계 포트 모드를 분류합니다. 인터페이스 f1/0/1의 모드는 호스트입니다. 인터페이스 f1/0/2의 모드는 프로미큐어스입니다.

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport mode private-vlan host
Router(config)# interface f1/0/2
Router(config-ifc)# switchport mode private-vlan promiscuous
```

6단계 호스트 포트에 VLAN 멤버십을 할당합니다. 인터페이스 f1/0/1은 기본 VLAN 200 및 분리된 보조 VLAN 501의 멤버입니다.

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport private-vlan host-association 200 501
```

7단계 VLAN 멤버십을 프로미큐어스 인터페이스에 할당합니다. 인터페이스 f1/0/2는 보조 VLAN 200의 멤버입니다. 보조 VLAN 501-503은 기본 VLAN에 매핑되어 있습니다.

```
Router(config)# interface f1/0/2
Router(config-ifc)# switchport private-vlan mapping 200 501-503
```

8단계 VLAN 간 라우팅이 필요한 경우, 기본 SVI를 구성한 다음 보조 VLAN을 기본에 매핑합니다.

```
Router(config)# interface vlan 200
Router(config-ifc)# private-vlan mapping 501-503
```

MSFC를 직접 연결된 라우터(SVI)로 사용

MSFC를 직접 연결된 라우터로 사용하려면(예: ASASM 외부 인터페이스에 연결된 기본 게이트웨이로 사용), ASASM VLAN 인터페이스를 SVI(스위치 가상 인터페이스)로서 MSFC에 연결합니다. 3-2 페이지의 SVI 정보를 참조하십시오.

제한 사항

보안상의 이유로 인해, 기본적으로 MSFC와 ASASM 간에는 하나의 SVI를 구성할 수 있습니다. 다중 SVI를 사용할 수는 있으나 네트워크를 잘못 구성하지 않도록 주의해야 합니다.

세부 단계

	명령	목적
1단계	(선택 사항) **firewall multiple-vlan-interfaces** 예: `Router(config)# firewall multiple-vlan-interfaces`	여러 개의 SVI를 ASASM에 추가할 수 있습니다.
2단계	**interface vlan** *vlan_number* 예: `Router(config)# interface vlan 55`	VLAN 인터페이스를 MSFC에 추가합니다.
3단계	**ip address** *address mask* 예: `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	MSFC에서 이 인터페이스의 IP 주소를 설정합니다.
4단계	**no shutdown** 예: `Router(config-if)# no shutdown`	인터페이스를 활성화합니다.

예

다음 예에는 다중 SVI의 일반적인 컨피그레이션이 나와 있습니다.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

ASA 장애 조치를 지원하는 스위치 구성

보조 ASA Services Module에 VLAN 할당

두 유닛에는 내부 및 외부 네트워크에 대한 동일한 액세스 권한이 필요하므로, 스위치에서 두 ASASM에 동일한 VLAN을 할당해야 합니다. 3-9 페이지의 보조 ASA Services Module에 VLAN 할당을 참조하십시오.

기본 스위치와 보조 스위치 간에 트렁크 추가

스위치 간 장애 조치를 사용할 경우, 장애 조치 및 상태 링크를 전송하려면 두 스위치 간에 802.1Q VLAN 트렁크를 구성해야 합니다. 트렁크에는 QoS를 활성화하여 CoS 값이 5인(상위 우선순위) 장애 조치 VLAN 패킷이 이러한 포트에서 상위 우선순위로 처리될 수 있도록 해야 합니다.

EtherChannel 및 트렁크를 구성하려면 스위치의 설명서를 참조하십시오.

투명 방화벽 모드와의 호환성 확인

투명 모드에서 장애 조치를 사용할 경우 루프를 방지하려면 BPDU 전달을 지원하는 스위치 소프트웨어를 사용합니다. ASASM이(가) 투명 모드에 있는 경우 LoopGuard를 스위치에서 전역으로 활성화하지 마십시오. LoopGuard는 스위치와 ASASM 간의 내부 EtherChannel에 자동으로 적용되므로, 장애 조치 및 장애 복구가 완료된 후에는 EtherChannel이 err-disable 상태가 되므로 LoopGuard로 인해 보조 유닛의 연결이 끊기는 결과를 초래할 수 있습니다.

Autostate 메시징 활성화로 신속한 링크 오류 감지 지원

수퍼바이저 엔진에서는 ASASM에 ASASM VLAN과 연결된 물리적 인터페이스의 상태에 대한 autostate 메시지를 전송할 수 있습니다. 예를 들어, VLAN과 연결된 모든 물리적 인터페이스가 중단되면 autostate 메시지에서는 VLAN이 중단되었음을 ASASM에 알립니다. ASASM에서는 이러한 정보를 사용하여 VLAN이 중단되었음을 선언할 수 있으며, 어느 쪽에 링크 오류가 발생한 것인지 확인하려면 인터페이스 모니터링 우회 테스트가 필요합니다. Autostate 메시징 기능은 ASASM에서 링크 오류를 감지하는 데 소요되는 시간을 대폭 개선합니다(autostate가 지원되지 않을 경우 최대 45초가 걸리는 것과 달리 몇 밀리초만 소요됨).

스위치 수퍼바이저에서는 다음과 같은 경우 ASASM에 autostate 메시지를 전송합니다.

- VLAN에 속한 마지막 인터페이스가 종료된 경우
- VLAN에 속한 첫 번째 인터페이스가 가동될 경우

세부 단계

명령	목적
firewall autostate 예: `Router(config)# firewall autostate`	Cisco IOS 소프트웨어에서 autostate 메시징을 활성화합니다. Autostate 메시징은 기본적으로 비활성화되어 있습니다.

ASA Services Module 초기화

이 섹션에서는 ASASM을(를) 초기화하는 방법에 대해 설명합니다. CLI 또는 텔넷 세션을 통해 ASASM에 접속할 수 없는 경우 초기화해야 할 수 있습니다. 초기화 프로세스는 몇 분 정도 걸릴 수 있습니다.

세부 단계

명령	목적
hw-module [**switch** {**1** |**2**}] **module** *slot* **reset** **예:** `Router# hw-module module 9 reset`	Resets the ASASM. VSS에 있는 스위치의 경우 **switch** 인수를 입력합니다. *slot* 인수는 모듈이 설치된 슬롯 번호를 나타냅니다. ASASM이(가) 설치된 슬롯을 보려면 **show module** 명령을 입력합니다. **참고** ASASM에 이미 로그인한 경우 이를 초기화합니다. **reload** 또는 **reboot** 명령을 입력합니다.

예

다음은 **hw-module module reset** 명령의 샘플 결과입니다.

```
Router# hw-module module 9 reset

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

ASA Services Module 모니터링

ASA을(를) 모니터링하려면,다음 명령 중 하나를 입력합니다.

명령	목적
show firewall module [*mod-num*] **state**	ASA의 상태를 확인합니다.
show firewall module [*mod-num*] **traffic**	ASA을(를) 통과하는 트래픽 흐름을 확인합니다.
show firewall module [*mod-num*] **version**	ASA의 소프트웨어 버전을 표시합니다.
show firewall multiple-vlan-interfaces	여러 VLAN 인터페이스의 상태를 나타냅니다(활성화 또는 비활성화).
show firewall vlan-group	구성된 모든 VLAN 그룹을 표시합니다.
show interface vlan	구성된 VLAN 인터페이스에 대한 상태 및 정보가 표시됩니다.

예

다음은 **show firewall module** [*mod-num*] **state** 명령의 샘플 결과입니다.

```
Router> show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

다음은 **show firewall module** [*mod-num*] **traffic** 명령의 샘플 결과입니다.

```
Router> show firewall module 11 traffic
Firewall module 11:

Specified interface is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

다음은 **show firewall multiple-vlan-interfaces** 명령의 샘플 결과입니다.

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

다음은 **show firewall module** 명령의 샘플 결과입니다.

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

다음은 **show firewall module** [*mod-num*] **version** 명령의 샘플 결과입니다.

```
Router# show firewall module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

다음은 **show firewall vlan-group** 명령의 샘플 결과입니다.

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

다음은 **show interface vlan** 명령의 샘플 결과입니다.

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ASA Services Module과 함께 사용할 수 있는 스위치의 기능 기록

표 3-1 에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다

표 3-1 ASASM과(와) 함께 사용할 수 있는 스위치의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
ASA Services Module은(는) Catalyst 6500 스위치에서 지원	8.5(1)	ASASM은(는) Catalyst 6500 Series 스위치에 사용되는 고성능 보안 서비스 모듈로, 이 장에 설명된 절차에 따라 구성합니다. 도입하거나 수정한 명령: **firewall transparent, mac address auto, firewall autostate** (IOS), **interface vlan**
ASA Services Module이 Cisco 7600 스위치에서 지원	9.0(1)	이제 Cisco 7600 Series에서 ASASM을(를) 지원합니다.
사설 VLAN 지원	9.1(2)	사설 VLAN을 ASASM과(와) 함께 사용할 수 있습니다. 기본 VLAN을 ASASM에 할당합니다. ASASM에서는 보조 VLAN 트래픽을 자동으로 처리합니다. 이 기능을 사용하기 위해 ASASM에서 컨피그레이션을 수행하지 않아도 됩니다. 자세한 내용은 스위치 컨피그레이션 설명서를 참조하십시오.

4 장

Cisco ASA Version 9.3의 기능

라이센스는 제공된 Cisco ASA에서 활성화되는 옵션을 지정합니다. 이 문서에서는 라이센스 활성화 키를 얻는 방법 및 이를 활성화하는 방법에 대해 설명합니다. 또한 각, 모델에 제공되는 라이센스에 대해서도 설명합니다.

참고 이 장에서는 버전 9.3의 라이센스에 대해 설명합니다. 다른 버전의 경우 해당 버전에 적용되는 라이센스 설명서를 참조하십시오.

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-licensing-information-listing.html

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.

- 4-6 페이지의 ASA 5545-X
- 4-7 페이지의 ASA 5555-X
- 4-8 페이지의 ASA 5585-X 및 SSP-10
- 4-9 페이지의 SSP-20이 포함된 ASA 5585-X
- 4-10 페이지의 SSP-40 및 -60이 포함된 ASA 5585-X
- 4-11 페이지의 ASA Services Module
- 4-12 페이지의 ASAv - 가상 CPU 1개 포함
- 4-13 페이지의 ASAv - 가상 CPU 4개 포함

*기울임 꼴*로 된 항목은 Base(또는 Security Plus 등) 라이센스 버전을 대체할 수 있는 별도로 선택 가능한 라이센스입니다. 라이센스는 여러 가지를 서로 조합할 수 있습니다. 예를 들어, Unified Communications 라이센스 24개에 Strong Encryption 라이센스를 더하거나, AnyConnect Premium 라이센스 500개에 GTP/GPRS 라이센스를 더할 수 있고, 네 가지 라이센스를 모두 조합할 수도 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 4-29 페이지의 No Payload Encryption 모델을 참조하십시오.

라이센스에 대한 자세한 내용은 4-14 페이지의 라이센스 참고 사항을 참조하십시오.

ASA 5512-X

표 4-1 ASA 5512-X 라이센스 기능

라이센스	Base 라이센스						Security Plus 라이센스					
Firewall 라이센스												
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*					비활성화됨	*선택적 기간별 라이센스: 사용 가능*				
동시 방화벽 연결 수	100,000						250,000					
GTP/GPRS	지원 안 함						비활성화됨	*선택적 라이센스: 사용 가능*				
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*					2	*옵션 라이센스:*				
		24	*50*	*100*	*250*	*500*		*24*	*50*	*100*	*250*	*500*
VPN 라이센스												
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능 (250개 세션)*					비활성화됨	*선택적 라이센스: 사용 가능 (250개 세션)*				
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				

표 4-1 ASA 5512-X 라이센스 기능(계속)

라이센스	Base 라이센스					Security Plus 라이센스				
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*				2	*선택적 영구 라이센스:*			
		10	*25*	*50*	*100*	*250*	*10*	*25*	*50*	*100*	*250*
		선택적 기간별(VPN Flex) 라이센스:				*250*	*선택적 기간별(VPN Flex) 라이센스:*				*250*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:						*선택적 공유 라이센스: 참가자 또는 서버. 서버용:*				
	500~50,000(500개 단위로 증분)			*50,000~545,000 (1,000개 단위로 증분)*			*500~50,000(500개 단위로 증분)*			*50,000~545,000 (1,000개 단위로 증분)*	
총 VPN(세션), 모든 유형 통합	250					250					
기타 VPN(세션)	250					250					
VPN 로드 밸런싱	지원 안 함					지원					
일반 라이센스											
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*				Base(DES)	*선택적 라이센스: Strong(3DES/AES)*				
장애 조치	지원 안 함					액티브/스탠바이 또는 액티브/액티브					
모든 유형의 인터페이스, 최대 개수	716					916					
보안 컨텍스트	지원 안 함					2	*옵션 라이센스:*				*5*
클러스터링	지원 안 함					2					
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*				비활성화됨	*선택적 라이센스: 사용 가능*				
VLAN, 최대 개수	50					100					

ASA 5515-X

표 4-2 ASA 5515-X 라이센스 기능

라이센스	Base 라이센스						
Firewall 라이센스							
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*					
동시 방화벽 연결 수	250,000						
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*					
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*					
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*	*24*	*50*	*100*	*250*	*500*
VPN 라이센스							
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*					
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*					
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(250개 세션)*					

표 4-2 ASA 5515-X 라이센스 기능(계속)

라이센스	Base 라이센스					
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*				
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*				
		10	*25*	*50*	*100*	*250*
		선택적 기간별(VPN Flex) 라이센스:				*250*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:					
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*
총 VPN(세션), 모든 유형 통합	250					
기타 VPN(세션)	250					
VPN 로드 밸런싱	지원					
일반 라이센스						
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*				
장애 조치	액티브/스탠바이 또는 액티브/액티브					
모든 유형의 인터페이스, 최대 개수	916					
보안 컨텍스트	2	*옵션 라이센스:*			*5*	
클러스터링	2					
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*				
VLAN, 최대 개수	100					

ASA 5525-X

표 4-3 ASA 5525-X 라이센스 기능

라이센스	Base 라이센스								
Firewall 라이센스									
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*							
동시 방화벽 연결 수	500,000								
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*							
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*							
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN 라이센스									
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(750개 세션)*							
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	
		선택적 기간별(VPN Flex) 라이센스:						*750*	
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:								
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*			
총 VPN(세션), 모든 유형 통합	750								
기타 VPN(세션)	750								
VPN 로드 밸런싱	지원								
일반 라이센스									
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*							
장애 조치	액티브/스탠바이 또는 액티브/액티브								
모든 유형의 인터페이스, 최대 개수	1316								
보안 컨텍스트	2	*옵션 라이센스:*	*5*	*10*	*20*				
클러스터링	2								
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*							
VLAN, 최대 개수	200								

ASA 5545-X

표 4-4 ASA 5545-X 라이센스 기능

라이센스	Base 라이센스									
Firewall 라이센스										
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*								
동시 방화벽 연결 수	750,000									
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*								
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*								
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN 라이센스										
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(2,500개 세션)*								
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
		선택적 기간별(VPN Flex) 라이센스:								*2500*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:									
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*				
총 VPN(세션), 모든 유형 통합	2500									
기타 VPN(세션)	2500									
VPN 로드 밸런싱	지원									
일반 라이센스										
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*								
장애 조치	액티브/스탠바이 또는 액티브/액티브									
모든 유형의 인터페이스, 최대 개수	1716									
보안 컨텍스트	2	*옵션 라이센스:*	*5*	*10*	*20*	*50*				
클러스터링	2									
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*								
VLAN, 최대 개수	300									

ASA 5555-X

표 4-5 ASA 5555-X 라이센스 기능

라이센스	Base 라이센스								
Firewall 라이센스									
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*							
동시 방화벽 연결 수	1,000,000								
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*							
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*							
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 라이센스									
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(5,000개 세션)*							
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		선택적 기간별(VPN Flex) 라이센스:								*5000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:								
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*			
총 VPN(세션), 모든 유형 통합	5000								
기타 VPN(세션)	5000								
VPN 로드 밸런싱	지원								
일반 라이센스									
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*							
장애 조치	액티브/스탠바이 또는 액티브/액티브								
모든 유형의 인터페이스, 최대 개수	2516								
보안 컨텍스트	2	*옵션 라이센스:*		*5*	*10*	*20*	*50*	*100*	
클러스터링	2								
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*							
VLAN, 최대 개수	500								

ASA 5585-X 및 SSP-10

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.

표 4-6 SSP-10 라이센스 기능이 포함된 ASA 5585-X

라이센스	Base 및 Security Plus 라이센스									
Firewall 라이센스										
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*								
동시 방화벽 연결 수	1,000,000									
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*								
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*								
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 라이센스										
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(5,000개 세션)*								
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		선택적 기간별(VPN Flex) 라이센스:								*5000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:									
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*				
총 VPN(세션), 모든 유형 통합	5000									
기타 VPN(세션)	5000									
VPN 로드 밸런싱	지원									
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									
모든 유형의 인터페이스, 최대 개수	4612									
보안 컨텍스트	2	*옵션 라이센스:*		*5*	*10*	*20*	*50*	*100*		
클러스터링	비활성화됨	*선택적 라이센스: 16개 유닛에 제공*								
VLAN, 최대 개수	1024									

SSP-20이 포함된 ASA 5585-X

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.

표 4-7 SSP-20 라이센스 기능이 포함된 ASA 5585-X

라이센스	Base 및 Security Plus 라이센스										
Firewall 라이센스											
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*									
동시 방화벽 연결 수	2,000,000										
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*									
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*									
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 라이센스											
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(10,000개 세션)*									
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		선택적 기간별(VPN Flex) 라이센스:										*10,000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:											
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*						
총 VPN(세션), 모든 유형 통합	10,000											
기타 VPN(세션)	10,000											
VPN 로드 밸런싱	지원											
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											
모든 유형의 인터페이스, 최대 개수	4612											
보안 컨텍스트	2	*옵션 라이센스:*		*5*	*10*	*20*	*50*	*100*	*250*			
클러스터링	비활성화됨	*선택적 라이센스: 16개 유닛에 제공*										
VLAN, 최대 개수	1024											

1. 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

SSP-40 및 -60이 포함된 ASA 5585-X

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.

표 4-8 SSP-40 및 -60 라이센스 기능이 포함된 ASA 5585-X

라이센스	Base 라이센스										
Firewall 라이센스											
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*									
동시 방화벽 연결 수	**SSP-40이 포함된 5585-X**: 4,000,000					**SSP-60이 포함된 5585-X**: 10,000,000					
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*									
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*									
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 라이센스											
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(10,000개 세션)*									
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		선택적 기간별(VPN Flex) 라이센스:										*10,000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:											
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*						
총 VPN(세션), 모든 유형 통합	10,000											
기타 VPN(세션)	10,000											
VPN 로드 밸런싱	지원											
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											
모든 유형의 인터페이스, 최대 개수	4612											
보안 컨텍스트	2	*옵션 라이센스:*			*5*	*10*	*20*	*50*	*100*	*250*		
클러스터링	비활성화됨	*선택적 라이센스: 16개 유닛에 제공*										
VLAN, 최대 개수	1024											

1. 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

ASA Services Module

표 4-9 라이센스 기능ASASM

라이센스	Base 라이센스										
Firewall 라이센스											
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*									
동시 방화벽 연결 수	10,000,000										
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*									
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*									
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 라이센스											
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(10,000개 세션)*									
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		선택적 기간별(VPN Flex) 라이센스:										*10,000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:											
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*						
총 VPN(세션), 모든 유형 통합	10,000											
기타 VPN(세션)	10,000											
VPN 로드 밸런싱	지원											
일반 라이센스												
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*										
장애 조치	액티브/스탠바이 또는 액티브/액티브											
보안 컨텍스트	2	*옵션 라이센스:*										
		5	*10*	*20*	*50*	*100*	*250*					
클러스터링	지원 안 함											
VLAN, 최대 개수	1000											

1. 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

ASAv - 가상 CPU 1개 포함

표 4-10 ASAv - 1 vCPU 라이센스 기능 포함

라이센스	Standard 및 Premium 라이센스	
Firewall 라이센스		
봇넷 트래픽 필터	지원	
동시 방화벽 연결 수	100,000	
GTP/GPRS	지원	
Intercompany Media Eng.	지원	
UC 전화 프록시 세션, 총 UC 프록시 세션	250	
VPN 라이센스		
Adv. Endpoint Assessment	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Essentials	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원되지 않음
AnyConnect for Cisco VPN Phone	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect for Mobile	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Premium(세션)	**Standard 라이센스**: 2	**Premium 라이센스**: 250
	Shared 라이센스: 지원되지 않음	
총 VPN(세션), 모든 유형 통합	250	
기타 VPN(세션)	250	
VPN 로드 밸런싱	지원	
일반 라이센스		
암호화	Strong(3DES/AES)	
장애 조치	액티브/스탠바이	
모든 유형의 인터페이스, 최대 개수	716	
보안 컨텍스트	지원 안 함	
클러스터링	지원 안 함	
VLAN, 최대 개수	50	
RAM, vCPU 주파수 제한	2GB, 5000MHz	

ASAv - 가상 CPU 4개 포함

표 4-11 ASAv - 4 vCPU 라이센스 기능 포함

라이센스	Standard 및 Premium 라이센스	
Firewall 라이센스		
봇넷 트래픽 필터	지원	
동시 방화벽 연결 수	500,000	
GTP/GPRS	지원	
Intercompany Media Eng.	지원	
UC 전화 프록시 세션, 총 UC 프록시 세션	1000	
VPN 라이센스		
Adv. Endpoint Assessment	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Essentials	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원되지 않음
AnyConnect for Cisco VPN Phone	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect for Mobile	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Premium(세션)	**Standard 라이센스**: 2	**Premium 라이센스**: 750
	Shared 라이센스: 지원되지 않음	
총 VPN(세션), 모든 유형 통합	750	
기타 VPN(세션)	750	
VPN 로드 밸런싱	지원	
일반 라이센스		
암호화	Strong(3DES/AES)	
장애 조치	액티브/스탠바이	
모든 유형의 인터페이스, 최대 개수	1316	
보안 컨텍스트	지원 안 함	
클러스터링	지원 안 함	
VLAN, 최대 개수	200	
RAM, vCPU 주파수 제한	8GB, 20000MHz **참고** 4 vCPU 라이센스를 적용하였으나 2, 3개의 vCPU를 구축하도록 선택할 경우 다음과 같은 값이 표시됩니다. 가상 CPU 2개 — 4GB RAM, vCPU 주파수 제한 10000MHz, 동시 방화벽 연결 수 250,000개 가상 CPU 3개 — 4GB RAM, vCPU 주파수 제한 15000MHz, 동시 방화벽 연결 수 350,000개	

라이센스 참고 사항

표 4-12 에는 4-1 페이지의 모델당 라이센스의 여러 표에서 공유하고 있는 일반적인 각주가 포함되어 있습니다.

표 4-12 라이센스 참고 사항

라이센스	참고
AnyConnect Essentials	AnyConnect Essentials 세션에는 다음과 같은 VPN 유형이 포함됩니다. • SSL VPN • IKEv2를 사용하는 IPsec 원격 액세스 이 라이센스에서는 브라우저 기반(클라이언트리스) 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 라이센스는 제공된 ASA에서 AnyConnect Premium 라이센스(모든 유형) 또는 Advanced Endpoint Assessment 라이센스와 동시에 활성화될 수 없습니다. 그러나 같은 네트워크의 다른 ASA에서는 AnyConnect Essentials 라이센스와 AnyConnect Premium 라이센스를 실행할 수 있습니다. 기본적으로 ASA에서는 AnyConnect Essentials 라이센스를 사용하지만, **webvpn**을 입력한 후 **no anyconnect-essentials** 명령을 사용하거나, ASDM에서 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** 창을 사용하면 이 라이센스를 비활성화하여 다른 라이센스를 사용할 수 있습니다. 4-19 페이지의 VPN 라이센스 및 기능 호환성도 참조하십시오.
AnyConnect for Cisco VPN Phone	이 라이센스를 AnyConnect Premium 라이센스와 함께 사용하면 AnyConnect 호환성을 통해 구축된 하드웨어 IP 폰에서 액세스가 가능하도록 지원할 수 있습니다.

표 4-12 라이센스 참고 사항(계속)

라이센스	참고
AnyConnect for Mobile	이 라이센스에서는 Windows Mobile 5.0, 6.0, 6.1을 실행하는 터치스크린 모바일 디바이스용 AnyConnect Client에 대한 액세스를 제공합니다. AnyConnect 2.3 이상 버전에 모바일 액세스를 지원하려면 이 라이센스를 사용하는 것이 좋습니다. 이 라이센스를 사용하려면 AnyConnect Essentials 또는 AnyConnect Premium 라이센스 중 하나를 활성화하여 허용되는 총 SSL VPN 세션 수를 지정해야 합니다. **모바일 상태 지원** 원격 액세스 제어를 시행하고 모바일 디바이스에서 상태 데이터를 수집하려면 AnyConnect Mobile 라이센스나 AnyConnect Essentials 또는 AnyConnect Premium 라이센스를 ASA에 설치해야 합니다. 설치하는 라이센스를 기준으로 제공되는 기능은 다음과 같습니다. • AnyConnect Premium 라이센스 기능 – 지원되는 모바일 디바이스에서 DAP 정책을 시행하는 작업은 DAP 속성 및 기타 기존 엔드포인트 특성을 기준으로 이루어집니다. 여기에는 모바일 디바이스에서 원격 액세스를 허용하거나 거부하는 것도 포함됩니다. • AnyConnect Essentials 라이센스 기능 – 그룹 단위로 모바일 디바이스 액세스를 활성화 또는 비활성화하고 ASDM을 사용하여 이러한 기능을 구성합니다. – DAP 정책을 시행하거나 이러한 모바일 디바이스에 대한 원격 액세스를 거부 또는 허용할 수 있는 기능이 없어도 CLI 또는 ASDM을 통해 연결된 모바일 디바이스에 대한 정보를 표시합니다.
AnyConnect Premium	AnyConnect Premium 세션에는 다음과 같은 VPN 유형이 포함됩니다. • SSL VPN • 클라이언트리스 SSL VPN • IKEv2를 사용하는 IPsec 원격 액세스
AnyConnect Premium Shared	공유 라이센스를 사용하면 ASA에서는 여러 클라이언트ASA의 공유 라이센스 서버 역할을 수행할 수 있습니다. 공유 라이센스 풀은 용량이 크지만 각 ASA에서 사용되는 세션의 최대 수는 영구 라이센스에 나열된 최대 수를 초과할 수 없습니다.
봇넷 트래픽 필터	동적 데이터베이스를 다운로드하려면 Strong Encryption(3DES/AES) 라이센스가 필요합니다.
암호화	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.

표 4-12 라이센스 참고 사항(계속)

라이센스	참고
Intercompany Media Engine	IME(Intercompany Media Engine) 라이센스를 활성화할 경우, 구성된 TLS 프록시 한도의 최대치까지 TLS 프록시 세션을 사용할 수 있습니다. 기본 TLS 프록시 한도보다 높은 UC(Unified Communications) 라이센스가 설치된 경우, ASA에서는 이러한 제한을 UC 라이센스 제한으로 설정하며 여기에 해당하는 모델에 따라 추가 세션 수도 추가합니다. **tls-proxy maximum-sessions** 명령을 사용하거나 ASDM에서 **Configuration > Firewall > Unified Communications > TLS Proxy** 창을 사용하여 TLS 프록시 한도를 수동으로 구성할 수 있습니다. 모델의 한도를 보려면 **tls-proxy maximum-sessions ?** 명령을 입력합니다. 또한 UC 라이센스를 설치할 경우 UC에 제공되는 TLS 프록시 세션을 IME 세션에도 사용할 수 있습니다. 예를 들어, TLS 프록시 세션의 한도를 1000으로 구성하고 750-세션 UC 라이센스를 구매할 경우, 처음 250개의 IME 세션은 UC에 제공되는 세션에 영향을 미치지 않습니다. 250개 이상의 세션이 IME에 필요할 경우, UC 및 IME에서는 플랫폼 한도의 나머지 750개 세션을 선착순으로 사용합니다. • 라이센스 부품 번호가 "K8"로 끝나는 경우, TLS 프록시 세션이 1000으로 제한됩니다. • 라이센스 부품 번호가 "K9"로 끝나는 경우, TLS 프록시 한도는 해당하는 컨피그레이션 및 플랫폼 모델에 따라 달라집니다. **참고** K8 및 K9의 경우 해당 라이센스의 내보내기 제한 여부를 참조하며, K8은 제한되지 않고 K9는 제한됩니다. 연결에 SRTP 암호화 세션을 사용할 수도 있습니다. • K8 라이센스의 경우 SRTP 세션이 250개로 제한됩니다. • K9 라이센스의 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.
모든 유형의 인터페이스, 최대 개수	통합된 인터페이스(예: VLAN, 물리적, 이중화, 브릿지 그룹, EtherChannel 인터페이스)의 최대 개수입니다. 컨피그레이션에 정의된 모든 **interface** 명령은 이 한도의 대상이 됩니다. 예를 들어, GigabitEthernet 0/0 인터페이스가 port-channel 1의 일부로 정의된 경우 다음 인터페이스 둘 다 대상이 됩니다. **interface gigabitethernet 0/0** 및 **interface port-channel 1**
IPS 모듈	IPS 모듈 라이센스를 사용하면 IPS 소프트웨어 모듈을 ASA에서 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. • 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이센스가 아니므로 장애 조치에서 공유되지 않습니다. • 장애 조치를 수행하려면 IPS 서명 서브스크립션에 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 장애 조치 시 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.

표 4-12 라이센스 참고 사항(계속)

라이센스	참고
기타 VPN	기타 VPN 세션에는 다음과 같은 VPN 유형이 포함됩니다. • IKEv1을 사용하는 IPsec 원격 액세스 • IKEv1을 사용하는 IPsec 사이트 대 사이트 VPN • IKEv2를 사용하는 IPsec 사이트 대 사이트 VPN 이 라이센스는 Base 라이센스에 포함됩니다.
총 VPN(세션), 모든 유형 통합	• 최대 VPN AnyConnect 및 기타 VPN 세션 이상의 최대 VPN 세션이 추가될 경우에도, 통합된 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 시작(예: 독립형 클라이언트에서)한 후 클라이언트리스 SSL VPN 포털에 로그인할 경우 2개의 세션이 사용됩니다.

표 4-12 라이센스 참고 사항(계속)

라이센스	참고
UC 전화 프록시 세션, 총 UC 프록시 세션	다음 애플리케이션에서는 연결에 TLS 프록시 세션을 사용합니다. 이러한 애플리케이션에서 사용되는 각 TLS 프록시 세션의 수는 UC 라이센스 한도를 기준으로 계산됩니다. • 전화 프록시 • 프레즌스 페더레이션 프록시 • 암호화된 음성 감시 TLS 프록시 세션을 사용하는 기타 애플리케이션의 경우 UC 한도에 가산되지 않습니다. Mobility Advantage Proxy(라이센스가 필요하지 않음) 및 IME(별도의 IME 라이센스 필요)를 예로 들 수 있습니다. 일부 UC 애플리케이션에서는 연결에 다중 세션을 사용할 수 있습니다. 예를 들어, 전화를 기본으로 구성하고 Cisco Unified Communications Manager를 백업할 경우, 2개의 TLS 프록시 연결이 사용되므로 2개의 UC 프록시 세션이 사용됩니다. **tls-proxy maximum-sessions** 명령을 사용하거나 ASDM에서 **Configuration > Firewall > Unified Communications > TLS Proxy** 창을 사용하여 TLS 프록시 한도를 개별적으로 구성할 수 있습니다. 모델의 한도를 보려면 **tls-proxy maximum-sessions ?** 명령을 입력합니다. 기본 TLS 프록시 한도보다 높은 UC 라이센스를 적용할 경우, ASA에서는 TLS 프록시 한도를 UC 한도에 맞게 자동으로 설정합니다. TLS 프록시 한도는 UC 라이센스 한도보다 우선합니다. TLS 프록시 한도를 UC 라이센스보다 작게 설정하면 UC 라이센스에서 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 컨피그레이션을 지우면 TLS 프록시 한도가 모델의 기본값으로 설정됩니다. 이 기본값이 UC 라이센스 한도보다 낮을 경우, **tls-proxy maximum-sessions** 명령을 사용하여 한도를 다시 높이라는 오류 메시지가 표시됩니다(ASDM에서 **TLS Proxy** 창 사용). 장애 조치를 사용 중이고 **write standby** 명령을 입력하거나 ASDM에서 **File > Save Running Configuration to Standby Unit**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 라이센스의 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.
가상 CPU	ASAv에 Virtual CPU 라이센스를 설치해야 합니다. 라이센스를 설치하지 않으면 처리량은 100Kbps로 제한되므로 사전 연결 테스트를 수행할 수 있습니다. Virtual CPU 라이센스는 일반적인 작업에 필요합니다.

표 4-12 라이센스 참고 사항(계속)

라이센스	참고
VLAN, 최대 개수	어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예: `interface gigabitethernet 0/0.100` `  vlan 100`
VPN 로드 밸런싱	VPN 로드 밸런싱에는 Strong Encryption(3DES/AES) 라이센스가 필요합니다.

VPN 라이센스 및 기능 호환성

표 4-13 에는 VPN 라이센스와 기능을 조합하는 방법이 나와 있습니다.

AnyConnect Essentials 라이센스 및 AnyConnect Premium 라이센스에서 지원되는 자세한 기능 목록을 보려면 *AnyConnect Secure Mobility 클라이언트 기능, 라이센스, OS*를 참조하십시오.

- 버전 3.1:
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/feature/guide/anyconnect31features.html
- 버전 3.0:
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/feature/guide/anyconnect30features.html
- 버전 2.5:
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/feature/guide/anyconnect25features.html

표 4-13 VPN 라이센스 및 기능 호환성

	다음 라이센스 중 하나를 활성화[1]	
지원되는 항목	AnyConnect Essentials	AnyConnect Premium
AnyConnect for Cisco VPN Phone	아니요	예
AnyConnect for Mobile[2]	예	예
Advanced Endpoint Assessment	아니요	예
AnyConnect Premium Shared	아니요	예
클라이언트 기반 SSL VPN	예	예
브라우저 기반(클라이언트리스) SSL VPN	아니요	예
IPsec VPN	예	예
VPN 로드 밸런싱	예	예
Cisco Secure Desktop	아니요	예

1. AnyConnect Essentials 라이센스 또는 AnyConnect Premium 라이센스 중 하나의 유효한 라이센스 유형만 보유할 수 있습니다. 기본적으로 ASA에는 2개의 세션을 지원하는 AnyConnect Premium 라이센스가 포함됩니다. AnyConnect Essentials 라이센스를 설치하면 이 라이센스가 기본적으로 사용됩니다. Premium 라이센스를 대신 활성화하려면 **webvpn**을 표시한 다음 **no anyconnect-essentials** 명령 을 사용합니다.
2. Mobile Posture 지원은 AnyConnect Essentials 및 AnyConnect Premium 라이센스와 다릅니다. 자세한 내용은 4-14 페이지의 표 4-12를 참조하십시오.

기능 라이센스 정보

라이센스는 제공된 ASA에서 활성화되는 옵션을 지정합니다. 라이센스는 160비트(32비트 또는 20바이트 단어 5개) 값으로 된 활성화 키로 나타냅니다. 이 값은 일련 번호(11자 문자열) 및 활성화된 기능으로 인코딩됩니다.

사전 설치된 라이센스

기본적으로 ASA에는 라이센스가 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. 어떤 라이센스가 설치되어 있는지 확인하려면 4-37 페이지의 라이센스 모니터링 섹션을 참조하십시오.

영구 라이센스

단일한 영구 활성화 키를 설치할 수 있습니다. 영구 활성화 키에는 단일한 키로 모든 라이센스 기능이 포함됩니다. 기간별 라이센스를 설치할 경우, ASA에서는 영구 라이센스와 기간별 라이센스를 실행 중인 라이센스로 통합합니다. ASA에서 라이센스를 통합하는 방법에 대한 자세한 내용은 4-21 페이지의 영구 라이센스와 기간별 라이센스가 통합되는 원리를 참조하십시오.

기간별 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 라이센스를 구매하거나, 유효 기간이 1년인 Botnet Traffic Filter 기간별 라이센스를 주문할 수 있습니다.

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 *활성화*할 수 있습니다. 비활성 라이센스는 설치된 채로 유지되며 사용할 준비가 되어 있습니다. 예를 들어, 1000-세션 AnyConnect Premium 라이센스 및 2500-세션 AnyConnect Premium 라이센스를 설치할 경우, 이러한 라이센스 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 라이센스에 Botnet Traffic Filter 및 1000-세션 AnyConnect Premium 라이센스가 포함된 경우 독립형 기간별 2500-세션 AnyConnect Premium 라이센스를 활성화할 수 없습니다.

기간별 라이센스 타이머 작동 방식

- 기간별 라이센스의 타이머는 ASA에서 해당 라이센스를 활성화하면 카운트다운이 시작됩니다.
- 라이센스의 기간이 만료되기 전에 기간별 라이센스 사용을 중단할 경우 타이머가 중지됩니다. 타이머는 기간별 라이센스를 다시 활성화할 경우에만 다시 시작됩니다.
- 기간별 라이센스가 활성화되어 있고 ASA를 종료한 경우 타이머의 카운트다운은 계속 진행됩니다. 연장된 기간 동안 ASA를 종료 상태에 두려면 종료하기 전에 기간별 라이센스를 비활성화해야 합니다.

참고 기간별 라이센스를 설치한 후에는 시스템 클록을 변경하지 않는 것이 좋습니다. 시스템 클록을 이후 날짜로 설정하고 다시 로드할 경우, ASA에서는 시스템 클록을 원래 설치 시간과 비교하여 확인하며 실제로 사용한 시간보다 더 많은 시간이 지난 것으로 가정합니다. 클록을 앞으로 설정했고 실제 실행 시간이 원래 설치 시간과 시스템 클록 간의 시간보다 클 경우, 다시 로드하면 라이센스가 즉시 만료됩니다.

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. 표 4-14 에는 각 기능 라이센스의 통합 규칙이 나와 있습니다.

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

표 4-14 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 컨텍스트	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.
봇넷 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.

통합된 라이센스를 보려면 4-37 페이지의 라이센스 모니터링을 참조하십시오.

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 라이센스를 *스태킹*할 수 있도록 지원하므로, 새 라이센스를 조기에 설치하여 라이센스가 만료되거나 라이센스의 기간이 짧아지지 않을까 걱정하지 않아도 됩니다.

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

예:

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

라이센스가 동일하지 않을 경우(예: 1000-세션 AnyConnect Premium 라이센스와 2500-세션 라이센스) 라이센스가 통합되지 *않습니다*. 기능당 기간별 라이센스를 하나만 활성화할 수 있으므로 여러 라이센스 중 하나만 활성화할 수 있습니다. 라이센스 활성화에 대한 자세한 내용은 4-32 페이지의 키 활성화 또는 비활성화를 참조하십시오.

동일하지 않은 라이센스는 통합되지 않지만 현재 라이센스가 만료될 경우, 같은 기능 라이센스가 설치되어 있으면 ASA에서는 이를 자동으로 활성화합니다. 자세한 내용은 4-23 페이지의 기간별 라이센스 만료를 참조하십시오.

기간별 라이센스 만료

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

기능을 지원하는 추가 기간별 라이센스가 여러 개 있는 경우 ASA에서는 첫 번째 라이센스를 사용합니다. 이 라이센스는 사용자 구성 가능하지 않으며 내부 작업에 따라 달라집니다. ASA에서 활성화한 라이센스가 아닌 다른 기간별 라이센스를 사용하려면 원하는 라이센스를 수동으로 활성화해야 합니다. 4-32 페이지의 키 활성화 또는 비활성화를 참조하십시오.

기간별 2500-세션 AnyConnect Premium 라이센스(활성), 기간별 1000-세션 AnyConnect Premium 라이센스(비활성), 500-세션 AnyConnect Premium 라이센스가 있는 경우를 가정해 보겠습니다. 2500-세션 라이센스가 만료되면 ASA에서는 1000-세션 라이센스를 활성화합니다. 1000-세션 라이센스가 만료되면 ASA에서는 500-세션 영구 라이센스를 사용합니다.

Shared AnyConnect Premium 라이센스

공유 라이센스를 사용하면 AnyConnect Premium 세션을 대량으로 구매할 수 있으며, ASA 중 하나를 공유 라이센스 서버로 구성하고 나머지는 공유 라이센스 참가자로 구성하여 필요에 따라 ASA의 그룹 간에 세션을 공유할 수 있습니다. 이 섹션에서는 공유 라이센스가 어떤 방식으로 활용되는지 설명합니다.

공유 라이센스 서버 및 참가자 정보

다음 단계에서는 공유 라이센스가 어떤 방식으로 운영되는지 설명합니다.

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

참고 공유 라이센싱 백업 서버에는 참가자 라이센스만 필요합니다.

4. 공유 라이센스 서버에서 공유 비밀을 구성합니다. 공유 비밀을 보유한 모든 참가자는 공유 라이센스를 사용할 수 있습니다.
5. ASA를 참가자로 지정하면 ASA에서는 로컬 라이센스 및 모델 정보를 비롯한 자체 정보를 전송하여 공유 라이센스 서버에 등록됩니다.

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.

   a. 공유 라이센스 풀에 참가자가 사용할 세션이 충분히 남아 있지 않은 경우, 서버에서는 최대한 사용 가능한 세션 수에 응답합니다.
   b. 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 라이센스 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 있습니다. 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.

- 4-25 페이지의 장애 조치 및 공유 라이센스 서버
- 4-26 페이지의 장애 조치 및 공유 라이센스 참가자

장애 조치 및 공유 라이센스 서버

이 섹션에서는 기본 서버와 백업 서버가 장애 조치와 어떤 방식으로 상호 작용하는지 설명합니다. 공유 라이센스 서버에서는 ASA와 마찬가지로 일반적인 업무(예: VPN 게이트웨이 및 방화벽 역할 기능 수행)도 수행하므로, 안정성을 높이기 위해서는 기본 및 백업 공유 라이센스 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 계속 중단되어 있고 2번 쌍의 기본 유닛이 중단될 경우, 2번 쌍의 스탠바이 유닛이 공유 라이센스 서버로 사용됩니다.

스탠바이 백업 서버에서는 기본 백업 서버와 동일한 작동 한도를 공유합니다. 스탠바이 유닛이 액티브 상태가 되면, 기본 유닛이 중단된 곳에서 카운트다운을 계속 진행합니다. 자세한 내용은 4-25 페이지의 공유 라이센스 백업 서버 정보를 참조하십시오.

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

이전 버전의 ASA 소프트웨어에는 각 유닛과 일치하는 라이센스가 필요했습니다. 버전 8.3(1)부터는 더 이상 동일한 라이센스를 설치하지 않아도 됩니다. 일반적으로 기본 유닛에만 라이센스를 구매하며, 액티브/스탠바이 장애 조치가 이루어질 경우 보조 유닛이 액티브 유닛이 되면 보조 유닛에서 기본 라이센스를 상속합니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다.

이러한 규칙의 예외 사항은 다음과 같습니다.

- ASA 5512-X용 Security Plus — Base 라이센스에서는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 사용할 수 없습니다.
- 암호화 라이센스 — 두 유닛에는 모두 동일한 암호화 라이센스가 있어야 합니다.

- ASA 5555-X를 통한 ASA 5512-X용 IPS 모듈 — 두 유닛에는 모두 IPS 모듈 라이센스가 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 라이센스가 아니므로 장애 조치에서 공유되지 않습니다.
  - IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
- ASAv 가상 CPU — 장애 조치를 구축할 경우 기본 유닛과 동일한 수의 vCPU가 스탠바이 유닛에 할당되어 있는지 확인하십시오(vCPU 라이센스 일치 여부도 함께 확인).

참고 유효한 영구 키가 필요합니다. 드문 경우지만 인증 키가 제거될 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.

이러한 규칙의 예외 사항은 다음과 같습니다.

- 클러스터링 라이센스 — 각 유닛에 클러스터링 라이센스가 있어야 합니다.
- 암호화 라이센스 — 각 유닛에 동일한 암호화 라이센스가 있어야 합니다.

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 AnyConnect Premium 세션이 설치되어 있습니다. 이러한 라이센스는 총 20개의 AnyConnect Premium 세션으로 통합됩니다.
  - 2개의 ASA 5525-X에 각각 500개의 AnyConnect Premium 세션이 설치되어 있습니다. 플랫폼 한도는 750개이므로, 통합된 라이센스에서는 750개의 AnyConnect Premium 세션을 허용합니다.

  참고 위의 예에서 AnyConnect Premium 라이센스가 기간별 라이센스인 경우, 라이센스 중 하나를 비활성화하여 500개의 세션 라이센스가 "낭비"되지 않도록 할 수 있습니다. 플랫폼 한도로 인해 250개의 세션만 사용할 수 있기 때문입니다.

  - 2개의 ASA 5545-X ASA 중 하나에는 20개의 컨텍스트가 있고 나머지에는 10개의 컨텍스트가 있습니다. 통합된 라이센스에서는 30개의 컨텍스트를 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:

  - SSP-10이 포함된 4개의 ASA 5585-X ASA가 있고, 3개의 각 유닛에 50개의 컨텍스트가 있고 1개 유닛에는 기본 2개의 컨텍스트가 있습니다. 플랫폼 한도가 100이므로 통합된 라이센스에서는 최대 100개의 컨텍스트를 허용합니다. 따라서 마스터 유닛에서 최대 100개의 컨텍스트를 구성할 수 있습니다. 각 슬레이브 유닛에서도 컨피그레이션 복제를 통해 100개의 컨텍스트를 포함할 수 있습니다.
  - SSP-60이 포함된 4개의 ASA 5585-X ASA가 있고, 3개의 각 유닛에 50개의 컨텍스트가 있고 1개 유닛에는 기본 2개의 컨텍스트가 있습니다. 플랫폼 한도가 250이므로 라이센스가 통합되면 총 152개의 컨텍스트를 지원합니다. 따라서 마스터 유닛에서 최대 152개의 컨텍스트를 구성할 수 있습니다. 각 슬레이브 유닛에서도 컨피그레이션 복제를 통해 152개의 컨텍스트를 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.

통합된 라이센스를 보려면 4-37 페이지의 라이센스 모니터링을 참조하십시오.

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.

예:

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(4-32 페이지의 표 4-15 참조) 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.

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 커뮤니케이션
- 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(4-37 페이지의 라이센스 모니터링 참조), VPN 및 Unified Communications 라이센스가 나열되지 않습니다.

라이센스 FAQ

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

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

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

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

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

A. 예. 영구 라이센스를 활성화해도 기간별 라이센스에는 영향을 미치지 않습니다.

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

A. 번호 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.

Q. 장애 조치 쌍의 보조 유닛에 동일한 라이센스를 구매해야 합니까?

A. 번호 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 상속합니다. 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.

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

A. 예. 공유 라이센스는 로컬로 설치된 라이센스(기간별 또는 영구)가 모두 사용된 세션 이후에만 사용됩니다. **참고**: 공유 라이센스 서버에서는 영구 AnyConnect Premium 라이센스가 사용되지 않습니다. 그러나 기간별 라이센스는 공유 라이센스 서버 라이센스와 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.

지침 및 제한 사항

활성화 키에 대한 다음 지침을 참조하십시오.

컨텍스트 모드 지침

- 다중 컨텍스트 모드의 경우 시스템 실행 영역에서 활성화 키를 적용합니다.
- 공유 라이센스는 다중 컨텍스트 모드에서 지원되지 않습니다.

방화벽 모드 지침

라우팅 및 투명 모드에서는 모든 라이센스 유형을 사용할 수 있습니다.

장애 조치 지침

- 공유 라이센스는 액티브/액티브 모드에서 지원되지 않습니다. 자세한 내용은 4-25 페이지의 장애 조치 및 공유 라이센스를 참조하십시오.
- 4-26 페이지의 장애 조치 또는 ASA 클러스터 라이센스를 참조하십시오.

업그레이드 및 다운그레이드 지침

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 활성화 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 활성화 키가 이전 버전과 계속 호환됩니다. 그러나 *8.2 이상* 버전에 도입된 기능 라이센스를 활성화할 경우에는 활성화 키가 이전 버전과 호환되지 않습니다. 호환되지 않는 라이센스 키가 있을 경우 다음 지침을 참조하십시오.
  - 기존에 이전 버전에서 활성화 키를 입력한 경우 ASA에서 해당 키를 사용합니다(버전 8.2 이상에서 활성화된 새 라이센스 없음).
  - 새 시스템이 있으나 이전 활성화 키가 없는 경우, 이전 버전과 호환되는 새 활성화 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 활성화 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 및 제한

- 활성화 키는 컨피그레이션 파일에 저장되지 않으며, 플래시 메모리에 숨겨진 파일로 저장됩니다.
- 활성화 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.
- 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 라이센스가 사용됩니다. **webvpn**을 사용한 다음 **no anyconnect-essentials** 명령을 사용하거나 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 창을 사용하여 컨피그레이션에서 AnyConnect Essentials 라이센스를 비활성화하면 다른 라이센스의 사용을 복원할 수 있습니다.

라이센스 구성

활성화 키 얻기

활성화 키를 얻으려면 Cisco 어카운트 담당자를 통해 구매할 수 있는 제품 승인 키가 필요합니다. 각 기능 라이센스에 별도의 제품 승인 키를 구매해야 합니다. 예를 들어, Base 라이센스를 보유한 경우 Advanced Endpoint Assessment 및 추가 AnyConnect Premium 세션에 대한 별도의 키를 구매할 수 있습니다.

제품 승인 키를 얻은 후에는 다음 단계를 수행하여 Cisco.com에서 해당 키를 등록합니다.

세부 단계

1단계 다음 명령을 입력하여 ASA에 대한 일련 번호를 얻습니다.

```
ciscoasa# show version | grep Serial
```

2단계 Cisco.com에 등록되어 있지 않은 경우 어카운트를 생성합니다.

3단계 아래의 라이센스 웹 페이지로 이동합니다.

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

4단계 메시지가 표시되면 다음 정보를 입력합니다.

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

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

5단계 추가 제품 승인 키가 있는 경우 각 제품 승인 키에 4단계를 반복합니다. 제품 승인 키를 모두 입력하면, 등록한 모든 영구 기능이 포함된 최종 활성화 키가 제공됩니다.

키 활성화 또는 비활성화

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

전제 조건

- 다중 컨텍스트 모드인 경우, 시스템 실행 영역에 활성화 키를 입력합니다.
- 일부 영구 라이센스의 경우 활성화 후 ASA를 다시 로드해야 합니다. 표 4-15 에는 다시 로드해야 하는 라이센스가 나열되어 있습니다.

표 4-15 영구 라이센스 다시 로드 요구 사항

모델	다시 로드해야 하는 라이센스 작업
모든 모델	암호화 라이센스 다운그레이드
ASAv	vCPU 라이센스 다운그레이드

제한 사항

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 활성화 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 활성화 키가 이전 버전과 계속 호환됩니다. 그러나 *8.2 이상* 버전에 도입된 기능 라이센스를 활성화할 경우에는 활성화 키가 이전 버전과 호환되지 않습니다. 호환되지 않는 라이센스 키가 있을 경우 다음 지침을 참조하십시오.
  - 기존에 이전 버전에서 활성화 키를 입력한 경우 ASA에서 해당 키를 사용합니다(버전 8.2 이상에서 활성화된 새 라이센스 없음).
  - 새 시스템이 있으나 이전 활성화 키가 없는 경우, 이전 버전과 호환되는 새 활성화 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 활성화 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다.
  - 장애 조치 쌍에 일치하지 않는 라이센스가 있을 경우 다운그레이드를 수행하면 장애 조치가 비활성화됩니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.

세부 단계

	명령	목적
1단계	**activation-key** *key* [**activate** | **deactivate**] **예:** `ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	ASA에 활성화 키를 적용합니다. 이 *키*는 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 비활성화하려면 **deactivate** 키워드를 입력합니다. 키를 처음 입력하고 **deactivate**를 지정하면 ASA에 설치된 키가 비활성 상태가 됩니다. 자세한 내용은 4-20 페이지의 기간별 라이센스를 참조하십시오.
2단계	(필요할 수 있습니다.) **reload** **예:** `ciscoasa# reload`	ASAASA을(를) 다시 로드합니다. 일부 영구 라이센스의 경우 새 활성화 키를 입력한 후 ASAASA를 다시 로드해야 합니다. 다시 로드해야 하는 라이센스 목록은 4-32 페이지의 표 4-15를 참조하십시오. 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.`

공유 라이센스 구성

이 섹션에서는 공유 라이센스 서버 및 참가자를 구성하는 방법을 설명합니다. 공유 라이센스에 대한 자세한 내용은 4-23 페이지의 Shared AnyConnect Premium 라이센스를 참조하십시오.

공유 라이센스 서버 구성

이 섹션에서는 ASA를 공유 라이센스 서버로 구성하는 방법을 설명합니다.

전제 조건

서버에는 공유 라이센스 서버 키가 있어야 합니다.

세부 단계

	명령	목적
1단계	**license-server secret** *secret* **예:** `ciscoasa(config)# license-server secret farscape`	4~128자의 ASCII 문자열로 된 공유 비밀을 설정합니다. 이 공유 비밀을 보유한 모든 참가자는 라이센스 서버를 사용할 수 있습니다.
2단계	(선택 사항) **license-server refresh-interval** *seconds* **예:** `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.
3단계	(선택 사항) **license-server port** *port* **예:** `ciscoasa(config)# license-server port 40000`	참가자로부터 SSL 연결을 수신하는 서버에 대한 포트 값을 1~65535 사이로 설정합니다. 기본값은 TCP 포트 50554입니다.

	명령	목적
4단계	(선택 사항) **license-server backup** *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*] 예: `ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3`	백업 서버 IP 주소와 일련 번호를 식별합니다. 백업 서버가 장애 조치 쌍에 포함될 경우, 스탠바이 유닛 일련 번호도 식별합니다. 1개의 백업 서버 및 선택적 스탠바이 유닛만 식별할 수 있습니다.
5단계	**license-server enable** *interface_name* 예: `ciscoasa(config)# license-server enable inside`	이 유닛을 공유 라이센스 서버로 활성화합니다. 참가자가 서버에 접속하는 인터페이스를 지정합니다. 이 명령을 원하는 인터페이스 수에 반복할 수 있습니다.

예

다음 예에서는 공유 비밀을 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 dmz 인터페이스에서 이러한 유닛을 공유 라이센스 서버로 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
```

다음에 할 일

자세한 내용은 4-35 페이지의 공유 라이센스 백업 서버 구성(선택 사항) 또는 4-36 페이지의 공유 라이센스 참가자을 참조하십시오.

공유 라이센스 백업 서버 구성(선택 사항)

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

전제 조건

백업 서버에는 공유 라이센스 참가자 키가 있어야 합니다.

세부 단계

	명령	목적
1단계	**license-server address** *address* **secret** *secret* [**port** *port*] **예:** `ciscoasa(config)# license-server address 10.1.1.1 secret farscape`	공유 라이센스 서버 IP 주소와 공유 비밀을 식별합니다. 서버 컨피그레이션에서 기본 포트를 변경한 경우 백업 서버와 일치하도록 포트를 조정해야 합니다.
2단계	**license-server backup enable** *interface_name* **예:** `ciscoasa(config)# license-server backup enable inside`	이 유닛을 공유 라이센스 백업 서버로 활성화합니다. 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
```

다음에 할 일

4-36 페이지의 공유 라이센스 참가자을 참조하십시오.

공유 라이센스 참가자

이 섹션에서는 공유 라이센스 참가자가 공유 라이센스 서버와 통신을 수행하도록 구성합니다..

전제 조건

참가자는 공유 라이센스 참가자 키가 있어야 합니다.

세부 단계

	명령	목적
1단계	**license-server address** *address* **secret** *secret* [**port** *port*] 예: ciscoasa(config)# license-server address 10.1.1.1 secret farscape	공유 라이센스 서버 IP 주소와 공유 비밀을 식별합니다. 서버 컨피그레이션에서 기본 포트를 변경한 경우 참가자와 일치하도록 포트를 조정해야 합니다.
2단계	(선택 사항) **license-server backup address** *address* 예: ciscoasa(config)# license-server backup address 10.1.1.2	백업 서버를 구성한 경우, 백업 서버 주소를 입력합니다.

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
```

라이센스 모니터링

최신 라이센스 보기

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

지침

No Payload Encryption 모델을 보유한 상태에서 라이센스를 보려면 VPN 및 Unified Communications 라이센스가 나열되지 않습니다. 자세한 내용은 4-29 페이지의 No Payload Encryption 모델을 참조하십시오.

세부 단계

명령	목적
show activation-key [**detail**] 예: ciscoasa# show activation-key detail	이 명령을 사용하면 영구 라이센스, 기간별 라이센스, 실행 중인 라이센스가 표시되며 이 라이센스는 영구 라이센스와 활성화된 기간별 라이센스가 통합된 것입니다. **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 4-1 독립형 유닛에 대한 show activation-key 명령의 결과

다음은 독립형 유닛에 대한 **show activation-key** 명령의 샘플 결과로, 실행 중인 라이센스(영구 라이센스 및 기간별 라이센스 통합) 및 활성화된 각 기간별 라이센스가 표시되어 있습니다.

```
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 4-2 독립형 유닛에 대한 show activation-key 명령의 세부 정보

다음은 독립형 유닛에 대한 **show activation-key detail** 명령의 샘플 결과로, 실행 중인 라이센스(영구 라이센스 및 기간별 라이센스 통합)와 함께 영구 라이센스 및 설치된 각 기간별 라이센스(활성 및 비활성 상태)가 표시되어 있습니다.

```
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 4-3 장애 조치 쌍의 기본 유닛에 대한 show activation-key 명령의 출력 결과

다음은 기본 장애 조치 유닛에 대한 **show activation-key detail** 명령의 샘플 결과로, 아래와 같은 내용이 표시됩니다.

- 기본 유닛 라이센스(통합된 영구 라이센스 및 기간별 라이센스).
- 기본 및 보조 유닛의 통합된 라이센스인 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 및 보조 라이센스의 통합을 나타내는 이 라이센스의 값은 굵은 글꼴로 되어 있습니다.
- 기본 유닛 영구 라이센스.
- 기본 유닛에 설치된 기간별 라이센스(활성 및 비활성 상태).

```
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 4-4 장애 조치 쌍의 기본 유닛에 대한 show activation-key 명령 세부 정보

다음은 보조 장애 조치 유닛에 대한 **show activation-key detail** 명령의 샘플 결과로, 아래와 같은 내용이 표시됩니다.

- 보조 유닛 라이센스(통합된 영구 라이센스 및 기간별 라이센스).
- 기본 및 보조 유닛의 통합된 라이센스인 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 및 보조 라이센스의 통합을 나타내는 이 라이센스의 값은 굵은 글꼴로 되어 있습니다.
- 보조 유닛 영구 라이센스.

- 보조 유닛에 설치된 기간별 라이센스(활성 및 비활성 상태). 이 유닛에는 기간별 라이센스가 없으므로, 이 샘플 결과에 표시되는 내용이 없습니다.

```
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 4-5 라이센스가 없는 ASAv의 독립형 유닛에 대한 show activation-key 출력 결과

구축된 1 vCPU ASAv에 대한 다음 출력 결과에는 비어 있는 활성화 키, 라이센스가 없는 상태, 1 vCPU 라이센스를 설치하라는 메시지가 표시되어 있습니다.

참고 표시된 명령 출력 결과는 "This platform has an ASAv VPN Premium license"입니다. 이 메시지는 ASAv에서 페이로드 암호화를 수행할 수 있음을 지정하며, ASAv Standard 및 Premium 라이센스를 참조하지 않습니다.

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                      : 0              perpetual
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
```

```
This platform has an ASAv VPN Premium license.

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

예 4-6 4 vCPU Standard 라이센스가 있는 ASAv의 독립형 유닛에 대한 show activation-key 출력 결과

참고 표시된 명령 출력 결과는 "This platform has an ASAv VPN Premium license"입니다. 이 메시지는 ASAv에서 페이로드 암호화를 수행할 수 있음을 지정하며, ASAv Standard 및 Premium 라이센스를 참조하지 않습니다.

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              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           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

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

예 4-7 4 vCPU Premium 라이센스가 있는 ASAv의 독립형 유닛에 대한 show activation-key 출력 결과

참고 표시된 명령 출력 결과는 "This platform has an ASAv VPN Premium license"입니다. 이 메시지는 ASAv에서 페이로드 암호화를 수행할 수 있음을 지정하며, ASAv Standard 및 Premium 라이센스를 참조하지 않습니다.

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82
```

```
ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

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

예 4-8 장애 조치 쌍에 있는 ASA Services Module의 기본 유닛에 대한 show activation-key 출력 결과

다음은 기본 장애 조치 유닛에 대한 **show activation-key** 명령의 샘플 결과로, 아래와 같은 내용이 표시됩니다.

- 기본 유닛 라이센스(통합된 영구 라이센스 및 기간별 라이센스).
- 기본 및 보조 유닛의 통합된 라이센스인 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 및 보조 라이센스의 통합을 나타내는 이 라이센스의 값은 굵은 글꼴로 되어 있습니다.
- 기본 유닛에 설치된 기간별 라이센스(활성 및 비활성 상태).

```
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 4-9 장애 조치 쌍에 있는 ASA Services Module의 보조 유닛에 대한 show activation-key 출력 결과

다음은 보조 장애 조치 유닛에 대한 **show activation-key** 명령의 샘플 결과로, 아래와 같은 내용이 표시됩니다.

- 보조 유닛 라이센스(통합된 영구 라이센스 및 기간별 라이센스).
- 기본 및 보조 유닛의 통합된 라이센스인 "장애 조치 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 및 보조 라이센스의 통합을 나타내는 이 라이센스의 값은 굵은 글꼴로 되어 있습니다.
- 보조 유닛에 설치된 기간별 라이센스(활성 및 비활성 상태). 이 유닛에는 기간별 라이센스가 없으므로, 이 샘플 결과에 표시되는 내용이 없습니다.

```
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 4-10 클러스터에 대한 show activation-key 출력 결과

```
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 다음 명령 중 하나를 입력합니다.

명령	목적
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 라이센스 통계를 지우려면 **clear shared license** 명령을 입력합니다.
show activation-key	ASA에 설치된 라이센스를 표시합니다. **show version** 명령을 사용하면 라이센스 정보도 표시됩니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

예

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

```
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** 명령의 샘플 결과입니다.

```
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
...
```

라이센스의 기능 기록

표 4-16 에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 4-16 라이센스의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
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
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.

표 4-16 라이센스의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
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.
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.
Advanced Endpoint Assessment 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. 검사 결과는 ASA로 전송됩니다. ASA에서는 사용자 로그인 자격 증명과 컴퓨터 검사 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.
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 라이센스는 Windows 모바일 디바이스에서 AnyConnect 클라이언트를 사용하여 ASA에 연결할 수 있도록 지원합니다.
기간별 라이센스	8.0(4)/8.1(2)	기간별 라이센스에 대한 지원이 도입되었습니다.

표 4-16 라이센스의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
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.
AnyConnect Essentials 라이센스	8.2(1)	AnyConnect Essentials 라이센스가 도입되었습니다. 이 라이센스는 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 라이센스는 제공된 ASA에서 AnyConnect Premium 라이센스(모든 유형) 또는 Advanced Endpoint Assessment 라이센스와 동시에 활성화될 수 없습니다. 그러나 같은 네트워크의 다른 ASA에서는 AnyConnect Essentials 라이센스와 AnyConnect Premium 라이센스를 실행할 수 있습니다. 기본적으로 ASA에서는 AnyConnect Essentials 라이센스를 사용하지만 **webvpn**을 입력한 후 **no anyconnect-essentials** 명령을 사용하거나을 사용하면 이 라이센스를 비활성화하여 다른 라이센스를 사용할 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.
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.

표 4-16 라이센스의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
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**
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 그 전에 라이센스가 만료되지 않도록 하는 것이 특히 중요합니다. ASA에서는 기간별 라이센스를 *스태킹*할 수 있도록 지원하므로, 새 라이센스를 조기에 설치하여 라이센스가 만료되거나 라이센스의 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.

표 4-16 라이센스의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
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.
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 수가 50에서 250으로 증가했습니다.
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)	방화벽 연결 제한 증가: • 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.
IKEv2를 사용하는 IPsec 원격 액세스	8.4(1)	IKEv2를 사용하는 IPsec 원격 액세스 VPN이 AnyConnect Essentials 및 AnyConnect Premium 라이센스에 추가되었습니다. **참고** ASA에서 IKEv2를 지원할 경우 다음과 같은 제한 사항이 있습니다. 현재로써는 이중 보안 연결을 지원하지 않습니다. IKEv2 사이트 대 사이트 세션이 다른 VPN 라이센스에 추가되었습니다(이전의 IPsec VPN). 기타 VPN 라이센스는 Base 라이센스에 포함됩니다.

표 4-16 라이센스의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
수출용 No Payload Encryption 하드웨어	8.4(1)	No Payload Encryption이 제공되는 모델(예: ASA 5585-X)의 경우, ASA를 특정 국가에 수출하기 위해 ASA 소프트웨어에서는 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.
ASASM에서 VPN 지원	9.0(1)	이제 ASASM에서 모든 VPN 기능을 지원합니다.
ASASM에서 Unified Communications 지원	9.0(1)	이제 ASASM에서는 모든 Unified Communications 기능을 지원합니다.
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.
ASAv 1 vCPU 및 4 vCPU Standard 및 Premium 라이센스 도입	9.2(1)	ASAv에 간단한 라이센스 체계가 도입되었습니다. Standard 또는 Premium 수준에서 1 vCPU 또는 4 vCPU 영구 라이센스를 제공합니다. 추가 라이센스는 제공되지 않습니다.

5 장

투명 또는 라우팅 방화벽 모드

이 장에서는 방화벽 모드를 라우팅 또는 투명 모드로 설정하는 방법 및 각 방화벽 모드에서 방화벽이 어떻게 작동하는지에 대해 설명합니다. 또한 이 장에는 투명 방화벽 작업을 맞춤화하는 방법도 포함되어 있습니다.

다중 컨텍스트 모드의 각 컨텍스트에 방화벽 모드를 개별적으로 설정할 수 있습니다.

방화벽 모드 정보

라우팅 방화벽 모드 정보

라우팅 모드에서 Cisco ASA는 네트워크의 라우터 홉으로 간주합니다. 라우팅 모드에서는 많은 인터페이스를 지원합니다. 각 인터페이스는 다른 서브넷에 있습니다. 컨텍스트 간에 인터페이스를 공유할 수 있습니다.

ASA에서는 연결된 네트워크 간에 라우터로서의 역할을 수행하며, 각 인터페이스에는 다른 서브넷에 있는 IP 주소가 필요합니다. ASA에서는 여러 동적 라우팅 프로토콜을 지원합니다. 그러나 라우팅 수요가 높을 경우 ASA에 의존하는 대신 업스트림 및 다운스트림 라우터의 고급 라우팅 기능을 사용하는 것이 좋습니다.

투명 방화벽 모드 정보

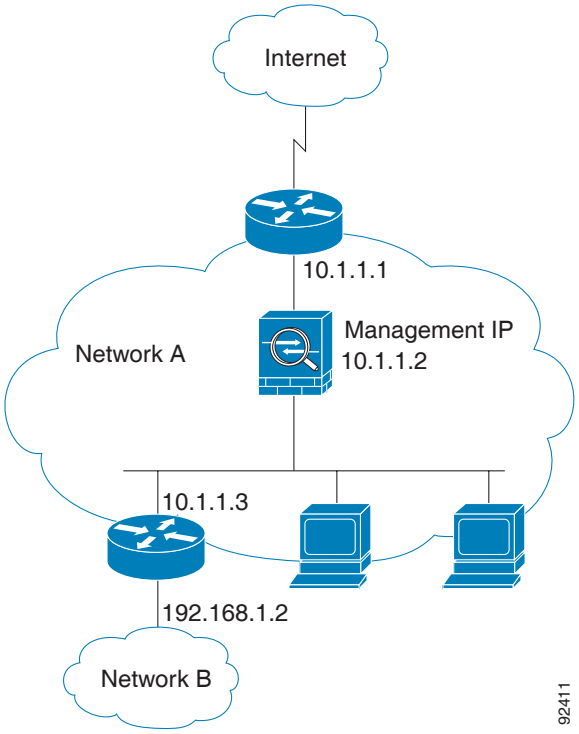
일반적으로 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

네트워크에서 투명 방화벽 사용

ASA에서는 인터페이스 간의 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로, 투명 모드를 기존 네트워크에서 쉽게 도입할 수 있습니다.

그림 5-1 에는 외부 디바이스가 내부 디바이스와 같은 서브넷에 존재하는 일반적인 투명 방화벽 네트워크가 나와 있습니다. 내부 라우터와 호스트는 외부 라우터에 직접 연결되어 있는 것으로 표시됩니다.

그림 5-1 투명 방어벽 네트워크

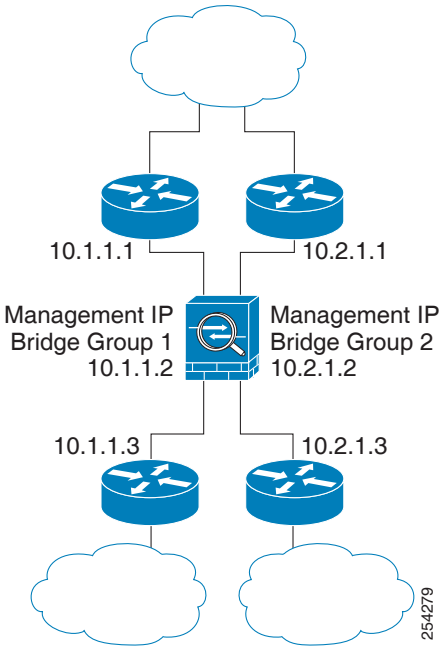


브릿지 그룹

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. 브릿지 그룹 트래픽은 다른 브릿지 그룹과 분리됩니다. 트래픽은 ASA 내의 다른 브릿지 그룹으로 라우팅되지 않으며, 트래픽은 외부 라우터에 의해 ASA의 다른 브릿지 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.

그림 5-2 에는 2개의 브릿지 그룹이 있는 ASA에 연결된 2개의 네트워크가 나와 있습니다.

그림 5-2 2개의 브릿지 그룹이 있는 투명 방화벽 네트워크



참고 각 브리지 그룹에는 관리 IP 주소가 필요합니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. 관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 다른 관리 방법에 대해서는 5-4 페이지의 관리 인터페이스(ASA 5512-X 이상)를 참조하십시오.

ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

관리 인터페이스(ASA 5512-X 이상)

각 브릿지 그룹 관리 IP 주소 이외에도 브릿지 그룹에 속하지 않은 별도의 관리 *슬롯/포트* 인터페이스를 추가할 수 있으며, 이렇게 하면 ASA에는 관리 트래픽만 허용됩니다. 자세한 내용은 9-2 페이지의 관리 인터페이스를 참조하십시오.

레이어 3 트래픽 허용

- ACL이 없어도 유니캐스트 IPv4 및 IPv6 트래픽이 상위 보안 인터페이스에서 하위 보안 인터페이스까지 투명 방화벽 모드를 자동으로 통과할 수 있습니다.

  참고 액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽을 전달할 수 있습니다. 자세한 내용은 방화벽 컨피그레이션 가이드 참조하십시오.

- ACL이 없어도 ARP가 투명 방화벽을 양방향으로 통과할 수 있습니다. ARP 트래픽은 ARP 감시로 제어할 수 있습니다.

- 하위 보안 인터페이스에서 상위 보안 인터페이스로 이동하는 레이어 3 트래픽의 경우, 하위 보안 인터페이스에 확장형 ACL이 필요합니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

허용되는 MAC 주소

아래의 목적지 MAC 주소는 투명 방화벽을 통과할 수 있습니다. 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

라우팅 모드에서 허용되지 않는 트래픽 전달

라우팅 모드에서는 일부 트래픽이 ASA를 통과하지 못할 수 있으며 ACL에서 허용한 경우에도 마찬가지입니다. 그러나 투명 방화벽 모드에서는 확장형 ACL(IP 트래픽용) 또는 EtherType ACL(비 IP 트래픽)을 사용하여 거의 모든 트래픽이 통과할 수 있습니다.

EtherType ACL을 사용하여 비 IP 트래픽(예: AppleTalk, IPX, BPDU, MPLS)이 통과되도록 구성할 수 있습니다.

참고 투명 모드 ASA에서는 CDP 패킷 또는 0x600 이상의 유효한 EtherType이 없는 패킷은 전달하지 않습니다. 예외적으로 BPDU 및 IS-IS는 지원됩니다.

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, 확장형 ACL을 사용하여 DHCP 트래픽(지원되지 않는 DHCP 릴레이 기능 대신) 또는 IP/TV에서 생성된 멀티캐스트 트래픽을 허용할 수 있습니다. 또한 투명 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수도 있습니다. 확장형 ACL을 기반으로 OSPF, RIP, EIGRP 또는 BGP 트래픽의 통과를 허용할 수 있습니다. 마찬가지로, HSRP 또는 VRRP 같은 프로토콜이 ASA를 통과할 수 있습니다.

BPDU 처리

Spanning Tree Protocol을 사용하여 루프를 방지하기 위해 기본적으로 BPDU가 전달됩니다. BPDU를 차단하려면 EtherType ACL에서 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 7-14 페이지의 투명 방화벽 모드 요구 사항을 참조하십시오.

MAC 주소 조회 및 경로 조회

투명 모드에서 ASA를 실행할 경우, 패킷의 발신 인터페이스는 경로 조회 대신 MAC 주소 조회를 수행하여 결정됩니다.

그러나 다음과 같은 트래픽 유형에는 경로 조회가 필요합니다.

- ASA에서 시작된 트래픽 — syslog 서버가 원격 네트워크에 있을 경우, 고정 경로를 사용하여 ASA가 해당 서브넷에 도달할 수 있도록 해야 합니다.
- NAT가 활성화되어 있고 ASA와 홉 간격이 최소 하나 이상 떨어진 트래픽 — ASA에서는 다음 홉 게이트웨이를 찾기 위해 경로 조회를 수행해야 합니다. 실제 호스트 주소를 위해서는 ASA에 고정 경로를 추가해야 합니다.
- 감시 기능이 활성화되어 있고, ASA와 홉 간격이 최소 하나 이상 떨어진 곳에 엔드포인트가 있는 VoIP(Voice over IP) 및 DNS 트래픽 — 예를 들어, CCM과 H.323 게이트웨이 간에 투명 방화벽을 사용하고 투명 방화벽과 H.323 게이트웨이 간에 라우터가 있을 경우 H.323 게이트웨이에서 호출을 완료하려면 ASA에 고정 경로를 추가해야 합니다. 감시된 트래픽에 NAT를 활성화할 경우, 패킷에 포함된 실제 호스트 주소의 이그레스(egress) 인터페이스를 결정하려면 고정 경로가 필요합니다. 영향을 받는 애플리케이션은 다음과 같습니다.
  - CTIQBE
  - DNS
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny(SCCP)

ARP 감시

기본적으로 모든 ARP 패킷은 ASA를 통과할 수 있습니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

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 인터페이스가 있다면 이 매개변수가 플러딩을 실행하도록 설정된 경우에도 패킷이 플러딩되지 않습니다.

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.

MAC 주소 테이블

ASA에서는 일반적인 브릿지 또는 스위치와 유사한 방식으로 MAC 주소 테이블을 학습하고 구축합니다. 디바이스에서 ASA를 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 브릿지에서는 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 — ASA의 경우 목적지 IP 주소에 대한 ARP 요청을 생성하므로, ASA에서는 어떤 인터페이스에서 ARP 응답을 수신하는지 알 수 있습니다.
- 원격 인터페이스에 대한 패킷 — ASA의 경우 목적지 IP 주소에 대한 Ping을 생성하므로 ASA에서는 어떤 인터페이스에서 Ping 응답을 수신하는지 알 수 있습니다.

원래 패킷은 손실됩니다.

방화벽 모드의 라이센스 요구 사항

다음 표에는 이 기능에 대한 라이센스 요구 사항이 나와 있습니다.

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

기본 설정

기본 모드는 라우팅 모드입니다.

투명 모드 기본값

- 기본적으로 모든 ARP 패킷은 ASA를 통과할 수 있습니다.
- ARP 감시를 활성화할 경우 기본 설정은 불일치 패킷을 플러딩하는 것입니다.
- 동적 MAC 주소 테이블 항목의 기본 시간 제한 값은 5분입니다.
- 기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다.

지침 및 제한 사항

컨텍스트 모드 지침

컨텍스트당 방화벽 모드를 설정합니다.

투명 방화벽 지침

- 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 두 가지 모두를 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않을 경우 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 *관리* 인터페이스를 사용하여 스위치에 액세스하도록 액세스 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.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- 브릿지 그룹 관리 IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 ASA의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 관리 트래픽의 반환 경로를 제공하는 데 필요한 투명 방화벽의 기본 경로는 단일한 브릿지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브릿지 그룹의 인터페이스 및 브릿지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브릿지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 고정 경로를 지정해야 합니다.

추가 지침은 12-4 페이지의 투명 모드 인터페이스의 가이드라인 및 제한 사항을 참조하십시오.

IPv6 지침

IPv6를 지원합니다.

추가 지침 및 제한

- 방화벽 모드를 변경할 경우, 다수의 명령이 양쪽 모드에서 모두 지원되지 않으므로 ASA에서는 실행 중인 컨피그레이션을 지웁니다. 시작 컨피그레이션은 변경되지 않고 유지됩니다. 저장하지 않고 다시 로드할 경우 시작 컨피그레이션이 로드되며 모드가 원래 설정으로 다시 전환됩니다. 컨피그레이션 파일에 대한 자세한 내용은 5-9 페이지의 방화벽 모드 설정을 참조하십시오.
- **firewall transparent** 명령으로 모드를 변경하는 텍스트 컨피그레이션을 ASA에 다운로드할 경우, 컨피그레이션의 맨 위에 해당 명령을 입력해야 합니다. ASA에서는 이 명령을 읽는 즉시 모드를 변경한 다음 다운로드된 컨피그레이션을 계속 읽습니다. 명령이 컨피그레이션의 뒤에 표시될 경우 ASA에서는 컨피그레이션의 앞에 있는 모든 줄을 지웁니다. 텍스트 파일 다운로드에 대한 자세한 내용은 36-20 페이지의 사용할 이미지 및 시작 컨피그레이션 설정을 참조하십시오.

투명 모드에서 지원되지 않는 기능

표 5-1 에는 투명 모드에서 지원되지 않는 기능이 나와 있습니다.

표 5-1 투명 모드에서 지원되지 않는 기능

기능	설명
동적 DNS	—
DHCP 릴레이	투명 방화벽은 DHCP 서버 역할을 수행할 수 있으나, DHCP 릴레이 명령을 지원하지는 않습니다. 2개의 확장형 ACL을 사용하여 DHCP 트래픽이 통과되도록 할 수 있으므로 DHCP 릴레이가 필요하지 않습니다. 이러한 확장형 ACL 중 하나는 DHCP 요청이 내부 인터페이스에서 외부 인터페이스로 전달되도록 하고, 나머지 하나는 서버의 응답을 다른 방향으로 전달할 수 있도록 합니다.

표 5-1 투명 모드에서 지원되지 않는 기능(계속)

기능	설명
동적 라우팅 프로토콜	ASA에서 시작된 트래픽에 대한 고정 경로를 추가할 수 있습니다. 또한 확장형 ACL을 사용하여 동적 라우팅 프로토콜이 ASA를 통과하도록 할 수 있습니다.
멀티캐스트 IP 라우팅	확장형 ACL에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 ASA를 통과하도록 할 수 있습니다.
QoS	—
통과 트래픽의 VPN 종료	투명 모드에서는 관리 연결에만 사이트 대 사이트 VPN 터널을 지원합니다. 그러나 이로 인해 ASA를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 확장형 ACL을 사용하여 VPN 트래픽이 ASA를 통과하도록 할 수 있으나, 비 관리 연결이 종료되지는 않습니다. 클라이언트리스 SSL VPN이 지원되지 않습니다.
통합 커뮤니케이션	—

방화벽 모드 설정

참고 이 섹션에서는 하여 방화벽 모드를 변경하는 방법에 대해 설명합니다.방화벽 모드를 변경하면 실행 중인 컨피그레이션이 지워지므로 다른 컨피그레이션을 수행하기 전에 방화벽 모드를 설정하는 것이 좋습니다.

전제 조건

모드를 변경하면 ASA에서는 실행 중인 컨피그레이션을 지웁니다(자세한 내용은 5-7 페이지의 지침 및 제한 사항 참조).

- 컨피그레이션이 이미 채워져 있는 경우 모드를 변경하기 전에 해당 컨피그레이션을 백업하십시오. 새 컨피그레이션을 생성할 때 이러한 백업을 참조할 수 있습니다. 36-24 페이지의 컨피그레이션 또는 기타 파일 백업 및 복원을 참조하십시오.
- 모드를 변경하려면 콘솔 포트에서 CLI를 사용합니다. ASDM Command Line Interface 툴이나 SSH를 비롯한 다른 유형의 세션을 사용할 경우, 컨피그레이션이 지워지면 연결이 끊어지며 콘솔 포트를 사용하여 ASA에 다시 연결해야 합니다.
- 컨텍스트 내에서 모드를 설정합니다.

세부 단계

참고 컨피그레이션이 지워진 후에 방화벽 모드를 투명 모드로 설정하고 ASDM 관리 액세스를 구성하려면 2-6 페이지의 ASDM 액세스 구성 또는 2-6 페이지의 ASDM 액세스 구성을 참조하십시오.

명령	목적
firewall transparent **예:** `ciscoasa(config)# firewall transparent`	방화벽 모드를 투명 모드로 설정합니다. 모드를 라우팅 모드로 변경하려면 **no firewall transparent** 명령을 입력합니다. **참고** 방화벽 모드 변경을 확인하는 메시지가 표시되지 않으며, 변경이 즉시 이루어집니다.

투명 방화벽의 ARP 감시 구성

이 섹션에서는 ARP 감시를 구성하는 방법에 대해 설명합니다.

ARP 감시 구성의 작업 흐름

ARP 감시를 구성하려면 다음 단계를 수행합니다.

1단계 5-10 페이지의 고정 ARP 항목 추가에 따라 고정 ARP 항목을 추가합니다. ARP 감시 기능은 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교하므로, 이 기능에는 고정 ARP 항목이 필요합니다.

2단계 5-11 페이지의 ARP 감시 활성화에 따라 ARP 감시를 활성화합니다.

고정 ARP 항목 추가

ARP 감시 기능은 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교합니다. 호스트에서 IP 주소로 패킷 목적지를 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 주소에 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 제한으로 만료됩니다. 항목이 잘못된 경우(예: 제공된 IP 주소의 MAC 주소가 변경된 경우), 해당 항목은 업데이트되기 전에 시간 제한으로 만료됩니다.

참고 투명 방화벽에서는 ASA로 들어오고 나가는 트래픽(예: 관리 트래픽)에 ARP 테이블의 동적 ARP 항목을 사용합니다.

세부 단계

명령	목적
arp *interface_name ip_address mac_address* 예: `ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100`	고정 ARP 항목을 추가합니다.

예

예를 들어, 외부 인터페이스의 MAC 주소가 0009.7cbe.2100인 10.1.1.1에서 라우터의 ARP 응답을 허용하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

다음에 할 일

5-11 페이지의 ARP 감시 활성화에 따라 ARP 감시를 활성화합니다.

ARP 감시 활성화

이 섹션에서는 ARP 감시를 활성화하는 방법에 대해 설명합니다.

세부 단계

명령	목적
arp-inspection *interface_name* **enable** [**flood** | **no-flood**] 예: `ciscoasa(config)# arp-inspection outside enable no-flood`	ARP 검사를 활성화합니다. **flood** 키워드는 불일치 ARP 패킷을 모든 인터페이스에 전달하며, **no-flood**는 불일치 패킷을 누락시킵니다. **참고** 기본 설정은 불일치 패킷을 플러딩하는 것입니다. ASA를 통과하는 ARP를 고정 항목으로만 제한하려면 이 명령을 **no-flood**로 설정합니다.

예

예를 들어, 외부 인터페이스에서 ARP 감시를 활성화하고 모든 불일치 ARP 패킷을 누락하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

투명 방화벽의 MAC 주소 테이블 맞춤화

이 섹션에서는 MAC 주소 테이블을 맞춤화하는 방법에 대해 설명합니다.

고정 MAC 주소 추가

일반적으로 MAC 주소는 특정 MAC 주소의 트래픽이 인터페이스에 들어올 때 MAC 주소 테이블에 동적으로 추가됩니다. 원하는 경우 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 누락하며 시스템 메시지가 생성됩니다. 고정 ARP 항목을 추가할 경우(5-10 페이지의 고정 ARP 항목 추가 참조), 고정 MAC 주소가 MAC 주소 테이블에 자동으로 추가됩니다.

MAC 주소 테이블에 고정 MAC 주소를 추가하려면 다음 명령어를 입력합니다.

명령	목적
mac-address-table static *interface_name mac_address* **예:** `ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100`	고정 MAC 항목을 추가합니다. *interface_name*은 소스 인터페이스입니다.

MAC Address 시간 제한 설정

동적 MAC 주소 테이블의 기본 시간 제한 값은 5분이지만, 시간 제한 값을 변경할 수 있습니다. 시간 제한을 변경하려면 다음 명령을 입력합니다.

명령	목적
mac-address-table aging-time *timeout_value* **예:** `ciscoasa(config)# mac-address-table aging-time 10`	MAC 주소 항목 시간 제한을 설정합니다. *timeout_value*(분 단위)의 범위는 5~720분(12시간)입니다. 5분이 기본값입니다.

MAC 주소 파악 비활성화

기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다. 원하는 경우 MAC 주소 파악을 비활성화할 수 있으나, 테이블에 MAC 주소를 고정으로 추가하지 않으면 트래픽이 ASA를 통과하여 전달될 수 없습니다.

MAC 주소 파악을 비활성화하려면 아래 명령을 입력하여 .

명령	목적
mac-learn *interface_name* **disable** 예: ciscoasa(config)# mac-learn inside disable	MAC 주소 파악을 비활성화합니다. 이 명령을 **no** 형식으로 사용하면 MAC 주소 파악을 다시 활성화할 수 있습니다. **clear configure mac-learn** 명령을 사용하면 모든 인터페이스에서 MAC 주소 파악을 다시 활성화할 수 있습니다.

투명 방화벽 모니터링

ARP 감시 모니터링

ARP 감시를 모니터링하려면 다음 작업을 수행합니다.

명령	목적
show arp-inspection	모든 인터페이스에서 ARP 감시에 대한 현재 설정을 표시합니다.

MAC 주소 테이블 모니터링

전체 MAC 주소 테이블(두 인터페이스의 고정 및 동적 항목 포함)을 보거나, 인터페이스의 MAC 주소 테이블을 볼 수 있습니다. MAC 주소 테이블을 보려면 다음 명령어를 입력합니다.

명령	목적
show mac-address-table [*interface_name*]	MAC 주소 테이블을 표시합니다.

예

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
```

방화벽 모드 예

이 섹션에는 트래픽이 어떻게 ASA를 통과하여 이동하는지에 대한 예가 포함되어 있습니다.

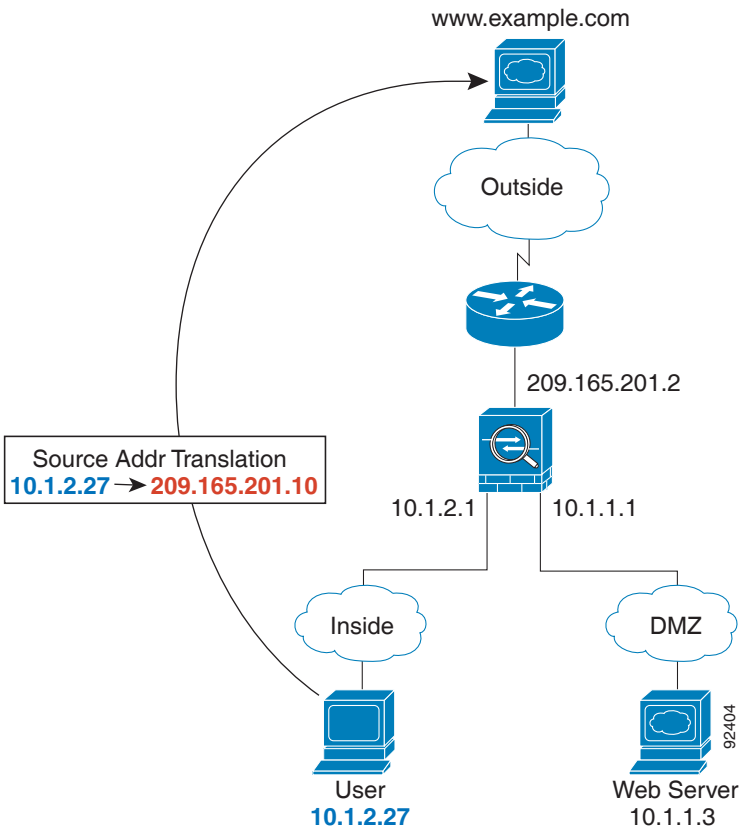
라우팅 방화벽 모드에서 데이터가 **ASA**를 통해 이동하는 방식

이 섹션에서는 라우팅 방화벽 모드에서 데이터가 ASA를 통과하여 이동하는 방식에 대해 설명합니다.

웹 서버를 방문하는 내부 사용자

그림 5-3에는 외부 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-3 내부 대 외부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-3 참조).

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

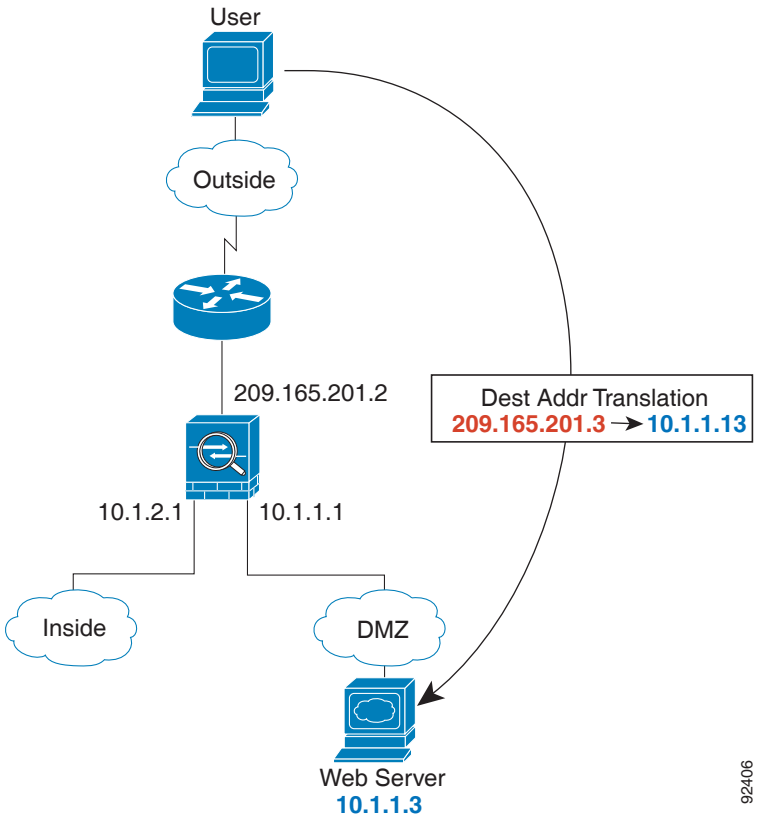
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 로컬 소스 주소(10.1.2.27)를 전역 주소(209.165.201.10)로 변환하며 이는 외부 인터페이스 서브넷에 있습니다.

   전역 주소는 모든 서브넷에 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

그림 5-4에는 DMZ 웹 서버에 액세스하는 외부 사용자의 경우가 나와 있습니다.

그림 5-4 외부 대 DMZ



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-4 참조).

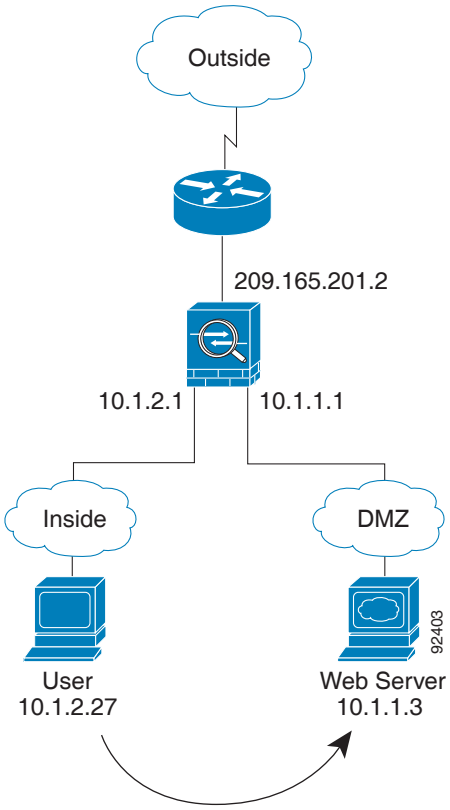
1. 외부 네트워크의 사용자가 외부 인터페이스 서브넷에 있는 전역 목적지 주소(209.165.201.3)를 사용하여 DMZ 웹 서버의 웹 페이지를 요청합니다.
2. ASA에 패킷이 수신되며 목적지 주소가 로컬 주소 10.1.1.3으로 변환되지 않습니다.
3. 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   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 로컬 소스 주소를 209.165.201.3으로 전환하여 NAT를 수행합니다.
6. ASA에서는 패킷을 외부 사용자에게 전달합니다.

DMZ의 웹 서버를 방문하는 내부 사용자

그림 5-5에는 DMZ 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-5 내부 대 DMZ



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-5 참조).

1. 내부 네트워크의 사용자가 목적지 주소(10.1.1.3)를 사용하여 DMZ 웹 서버의 웹 페이지를 요청합니다.

2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

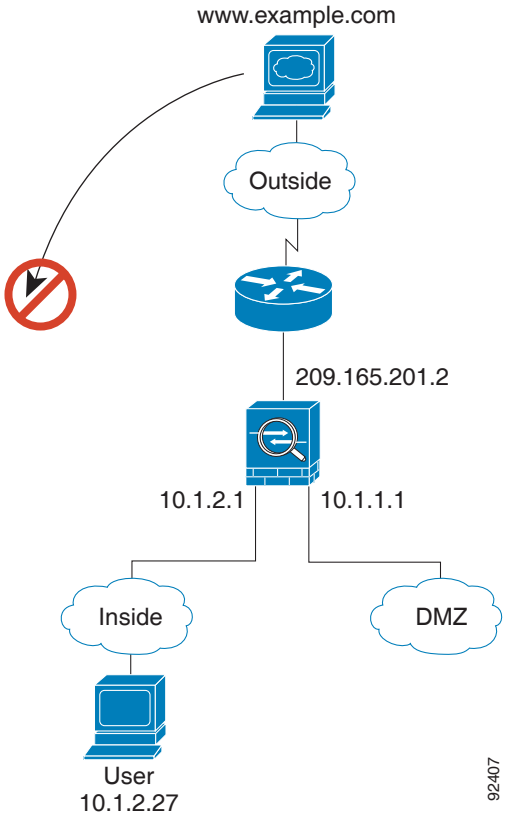
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.

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

그림 5-6에는 내부 네트워크에 액세스를 시도하는 외부 사용자의 경우가 나와 있습니다.

그림 5-6 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-6 참조).

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. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

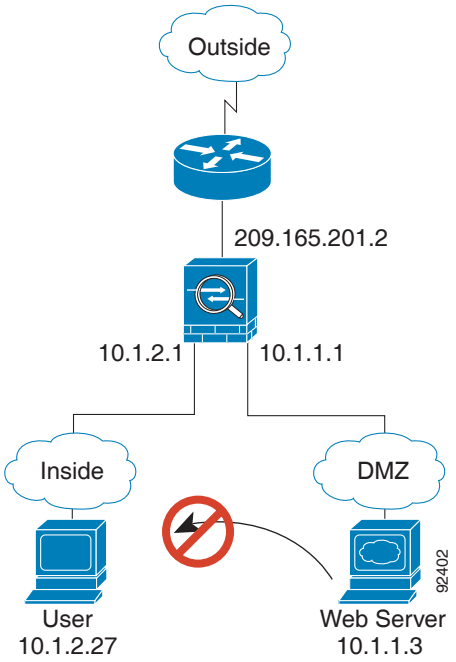
3. 패킷이 거부되며 ASA에서 해당 패킷을 누락시키고 연결 시도를 기록합니다.

   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

그림 5-7에는 DMZ 사용자가 내부 네트워크에 액세스를 시도하는 경우가 나와 있습니다.

그림 5-7 DMZ 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-7 참조).

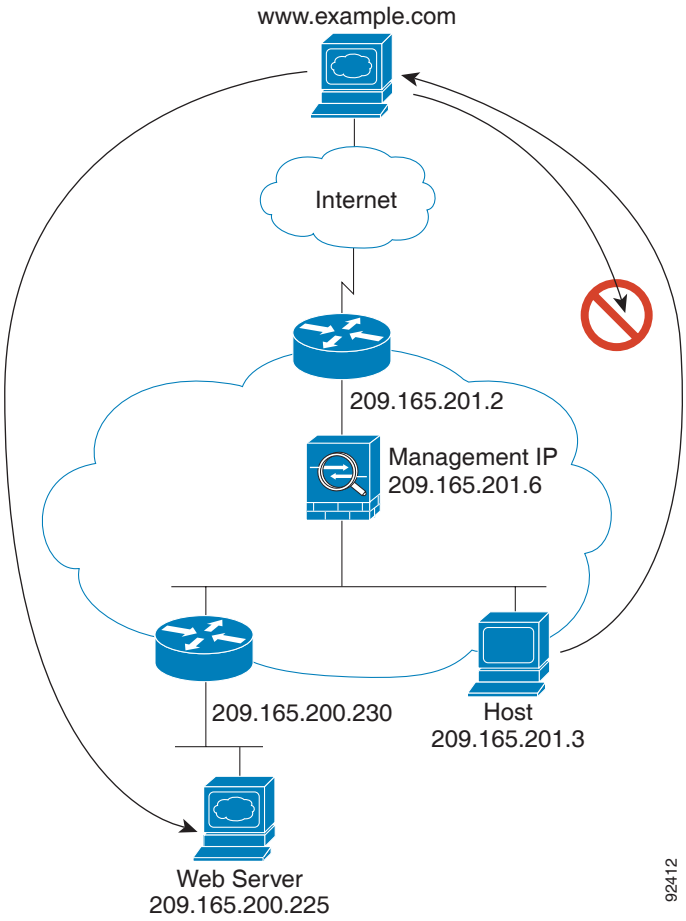
1. DMZ 네트워크 사용자가 내부 호스트에 연결하기 위해 시도합니다. DMZ에서는 인터넷의 트래픽을 라우팅해야 할 필요가 없으므로, 사설 주소 지정 체계로 라우팅을 방지할 수 없습니다.
2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   패킷이 거부되며 ASA에서 해당 패킷을 누락시키고 연결 시도를 기록합니다.

데이터가 투명 방화벽을 통해 이동하는 방식

그림 5-8에는 공용 웹 서버가 포함된 내부 네트워크에 투명 방화벽을 구현한 일반적인 예가 나와 있습니다. ASA에 액세스 목록이 있으므로 내부 사용자가 인터넷 리소스에 액세스할 수 있습니다. 다른 액세스 목록에서는 외부 사용자가 내부 네트워크의 웹 서버에만 액세스할 수 있도록 합니다.

그림 5-8 일반적인 투명 방화벽 데이터 경로



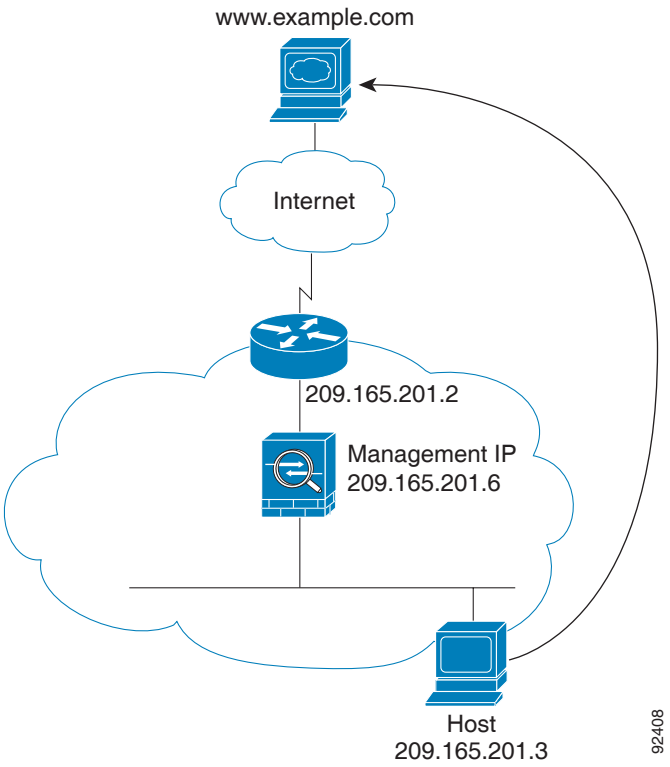
이 섹션에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

- 5-20 페이지의 웹 서버를 방문하는 내부 사용자
- 5-21 페이지의 NAT를 사용하여 웹 서버를 방문하는 내부 사용자
- 5-22 페이지의 내부 네트워크의 웹 서버를 방문하는 외부 사용자
- 5-23 페이지의 내부 호스트에 액세스를 시도하는 외부 사용자

웹 서버를 방문하는 내부 사용자

그림 5-9에는 외부 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-9 내부 대 외부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-9 참조).

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 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

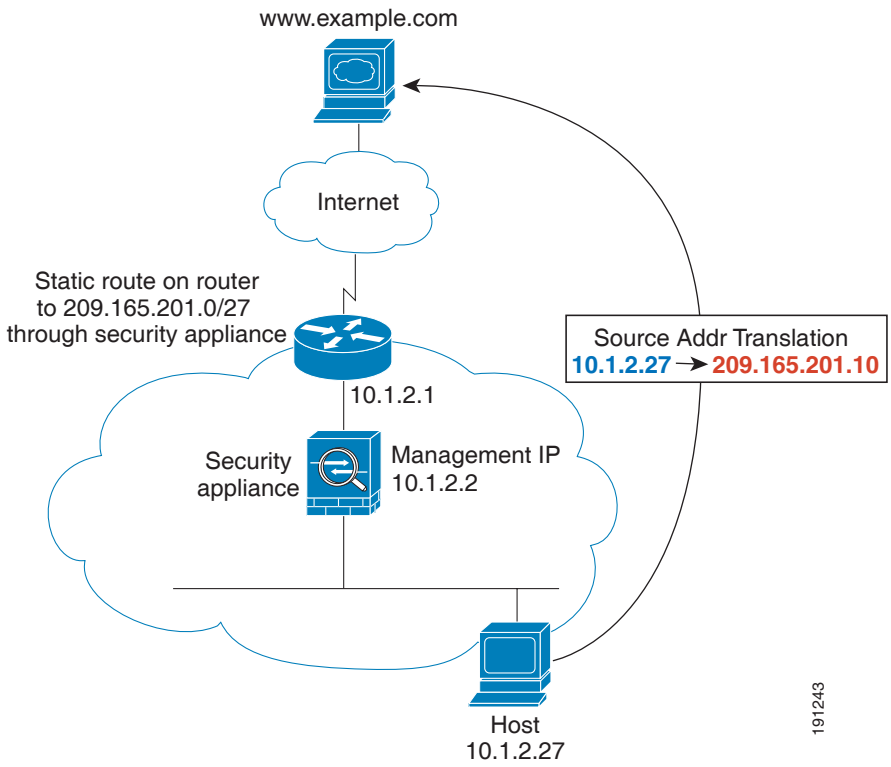
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 세션이 설정되었음을 기록합니다.
4. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 외부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 209.165.201.2입니다.

   목적지 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

그림 5-10에는 외부 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-10 내부 대 외부(NAT 사용)



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-10 참조).

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 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 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.

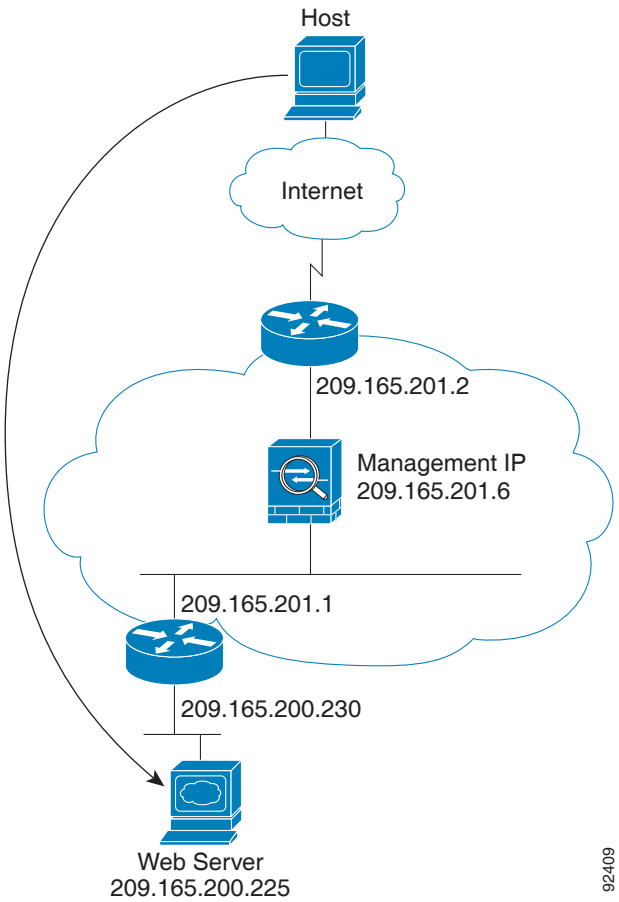
   매핑된 주소는 외부 인터페이스와 같은 네트워크에 있지 않으므로, ASA를 가리키는 매핑된 네트워크에 대한 고정 경로가 업스트림 라우터에 있어야 합니다.
4. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 외부 인터페이스에서 패킷을 전달합니다.
5. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 외부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 10.1.2.1입니다.

   목적지 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

그림 5-11에는 내부 웹 서버에 액세스하는 외부 사용자의 경우가 나와 있습니다.

그림 5-11 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-11 참조).

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 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

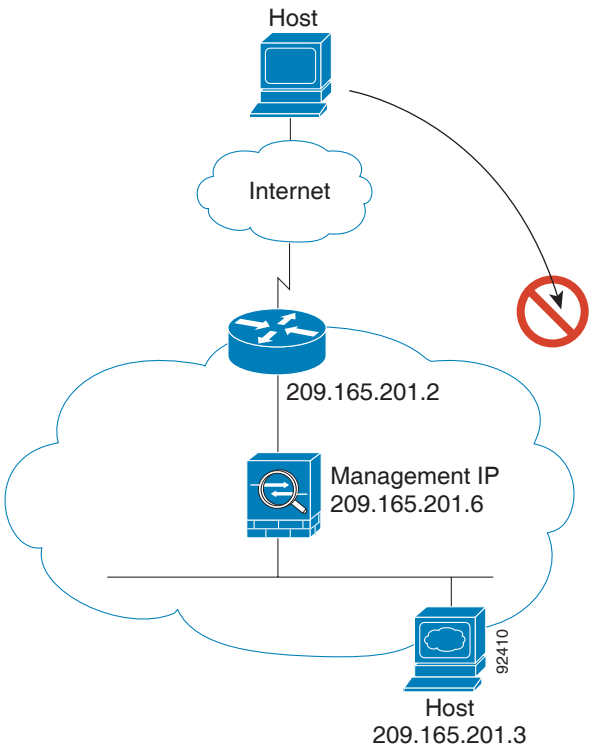
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 세션이 설정되었음을 기록합니다.
4. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 내부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 209.165.201.1입니다.

   목적지 MAC 주소가 ASA 테이블에 없는 경우, ASA에서는 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

그림 5-12에는 내부 네트워크의 호스트에 액세스를 시도하는 외부 사용자의 경우가 나와 있습니다.

그림 5-12 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-12 참조).

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 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. 외부 호스트를 허용하는 액세스 목록이 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 모드의 기능 기록

표 5-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 5-2 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. 도입된 명령: **firewall transparent**, **show firewall**
ARP 감시	7.0(1)	ARP 감시 기능은 모든 ARP 패킷의 MAC 주소, IP 주소, 소스 인터페이스를 ARP 테이블의 고정 항목과 비교합니다. 도입된 명령: **arp**, **arp-inspection**, **show arp-inspection**
MAC 주소 테이블	7.0(1)	투명 방화벽 모드에서는 MAC 주소 테이블을 사용합니다. 도입된 명령: **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable**, **show mac-address-table**
투명 방화벽 브릿지 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 브릿지 그룹을 구성할 수 있으며, 브릿지 그룹당 최대 4개의 인터페이스가 포함됩니다. **참고** ASA 5505에서 여러 개의 브릿지 그룹을 구성할 수는 있으나, ASA 5505의 투명 모드에서 데이터 인터페이스가 2개로 제한된다는 것은 실제로 사용 가능한 브릿지 그룹은 1개라는 의미입니다. 도입된 명령: **interface bvi**, **bridge-group**, **show bridge-group**

표 5-2 방화벽 모드의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
ARP cache additions for non-connected subnets	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 도입된 명령: **arp permit-nonconnected**
Mixed firewall mode support in multiple context mode	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. 수정된 명령: **firewall transparent**
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**

2 파 트

우수한 가용성 및 확장성

6 장

다중 컨텍스트 모드

이 장에서는 Cisco ASA에서 다중 보안 컨텍스트를 구성하는 방법을 설명합니다.

보안 컨텍스트에 대한 정보

단일 ASA를 보안 컨텍스트라고 부르는 여러 가상 디바이스로 분할할 수 있습니다. 각 컨텍스트는 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스의 역할을 합니다. 다중 컨텍스트는 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 다중 컨텍스트 모드에서 지원되지 않는 기능에 대해서는 6-14 페이지의 지침 및 제한 사항을 참조하십시오.

이 섹션에서는 보안 컨텍스트의 개요를 제공합니다.

보안 컨텍스트의 일반적인 용도

다음과 같은 상황에서 다중 보안 컨텍스트를 사용할 수 있습니다.

- 많은 고객에게 보안 서비스를 판매하려는 서비스 공급자라면 ASA에서 다중 보안 컨텍스트를 활성화함으로써 모든 고객의 트래픽을 분리하여 안전하게 지키는, 구성하기 용이한 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
- 둘 이상의 ASA가 필요한 네트워크

컨텍스트 컨피그레이션 파일

이 섹션에서는 ASA에서 다중 컨텍스트 모드 컨피그레이션을 구현하는 방법을 설명합니다.

- 6-2 페이지의 컨텍스트 컨피그레이션
- 6-2 페이지의 시스템 컨피그레이션
- 6-2 페이지의 관리 컨텍스트 컨피그레이션

컨텍스트 컨피그레이션

각 컨텍스트에서 ASA는 보안 정책, 인터페이스 그리고 독립형 디바이스에서 컨피그레이션 가능한 모든 옵션을 나타내는 컨피그레이션을 갖추고 있습니다. 컨텍스트 컨피그레이션을 플래시 메모리에 저장하거나 TFTP, FTP 또는 HTTP(S) 서버에서 다운로드할 수 있습니다.

시스템 컨피그레이션

시스템 관리자는 시스템 컨피그레이션에서 각 컨텍스트 컨피그레이션 위치, 할당된 인터페이스, 기타 컨텍스트 운영 매개 변수를 컨피그레이션함으로써 컨텍스트를 추가하고 관리합니다. 이는 단일 모드 컨피그레이션처럼 시작 컨피그레이션이 됩니다. 시스템 컨피그레이션은 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 컨텍스트*로 지정된 컨텍스트 중 하나를 사용합니다. 시스템 컨피그레이션은 장애 조치 트래픽만을 위한 전용 장애 조치 인터페이스를 포함합니다.

관리 컨텍스트 컨피그레이션

관리 컨텍스트는 여느 컨텍스트와 비슷하지만, 사용자가 관리 컨텍스트에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 컨텍스트에 액세스할 수 있다는 점이 다릅니다. 관리 컨텍스트는 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 컨텍스트에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 컨텍스트 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다. 관리 컨텍스트는 원격 위치가 아닌 플래시 메모리에 항상 있어야 합니다.

시스템이 이미 다중 컨텍스트 모드인 경우 또는 단일 모드에서 전환한 경우, 관리 컨텍스트가 내부 플래시 메모리에 admin.cfg라는 파일로 자동 생성됩니다. 이 컨텍스트의 이름은 "admin"입니다. admin.cfg를 관리 컨텍스트로 사용하고 싶지 않다면 관리 컨텍스트를 변경할 수 있습니다.

ASA의 패킷 분류

ASA에 들어오는 각 패킷은 분류되어야 합니다. 그러면 ASA에서 어떤 컨텍스트에 패킷을 보낼지 판단할 수 있습니다.

- 6-3 페이지의 유효한 분류자 기준
- 6-4 페이지의 분류의 예

참고 목적지 MAC 주소가 멀티캐스트 또는 브로드캐스트 MAC 주소인 경우 패킷이 복제되어 각 컨텍스트에 배포됩니다.

유효한 분류자 기준

이 섹션에서는 분류자에서 사용하는 기준에 대해 설명합니다.

- 6-3 페이지의 고유 인터페이스
- 6-3 페이지의 고유 MAC 주소
- 6-3 페이지의 NAT 컨피그레이션

참고 인터페이스로 갈 관리 트래픽에서는 인터페이스 IP 주소가 분류에 사용됩니다.

라우팅 테이블은 패킷 분류에 사용되지 않습니다.

고유 인터페이스

단 하나의 컨텍스트가 인그레스 인터페이스와 연결된 경우 ASA는 해당 패킷을 그 컨텍스트로 분류합니다. 투명 방화벽 모드에서는 컨텍스트에 대한 고유 인터페이스가 필요합니다. 따라서 항상 패킷 분류에 이 방법이 사용됩니다.

고유 MAC 주소

여러 컨텍스트에서 하나의 인터페이스를 공유할 경우, 분류자는 각 컨텍스트에서 인터페이스에 할당된 고유 MAC 주소를 사용합니다. 업스트림 라우터는 고유 MAC 주소가 없으면 컨텍스트에 곧바로 라우팅할 수 없습니다. 기본적으로 MAC 주소의 자동 생성이 활성화되어 있습니다. 또한 각 인터페이스를 구성할 때 직접 MAC 주소를 설정할 수도 있습니다.

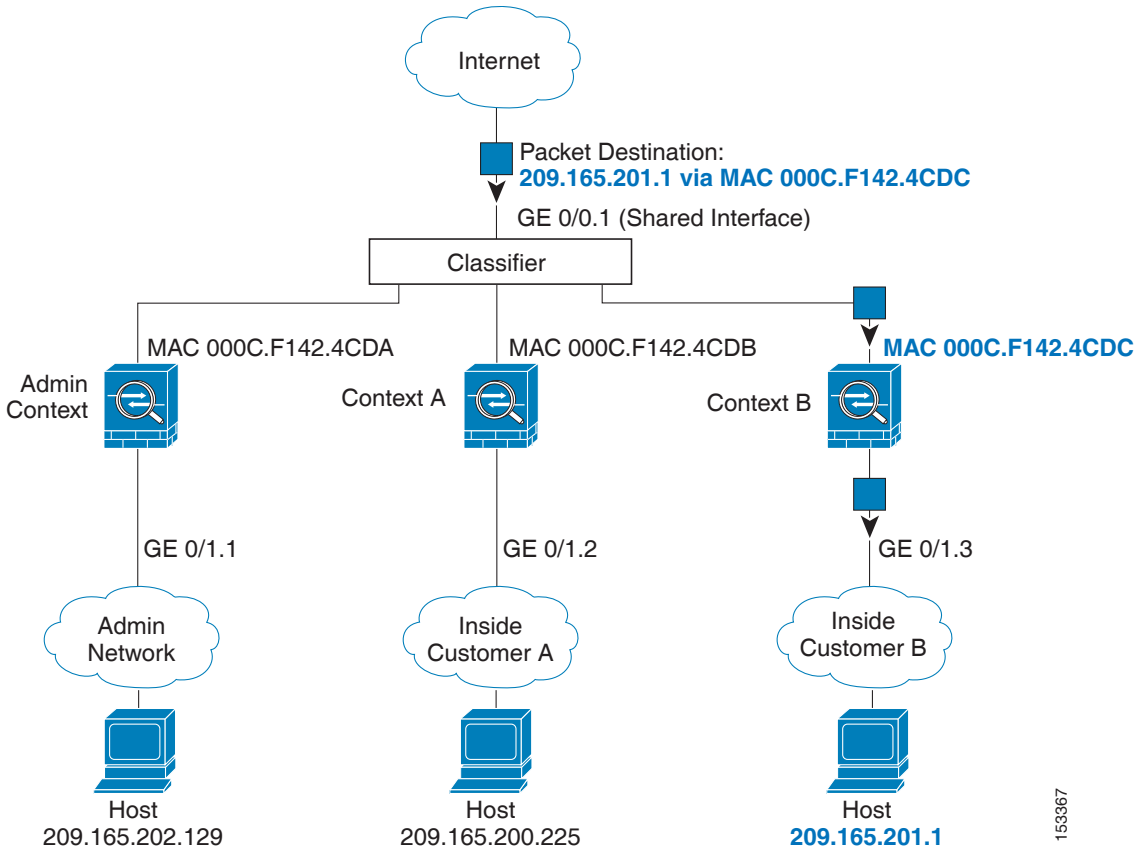
NAT 컨피그레이션

고유 MAC 주소의 사용을 비활성화한 경우 ASA에서는 NAT 컨피그레이션의 매핑된 주소를 사용하여 패킷을 분류합니다. NAT 대신 MAC 주소를 사용하는 것이 좋습니다. 그러면 NAT 컨피그레이션의 완전성과 상관없이 트래픽 분류가 가능해집니다.

분류의 예

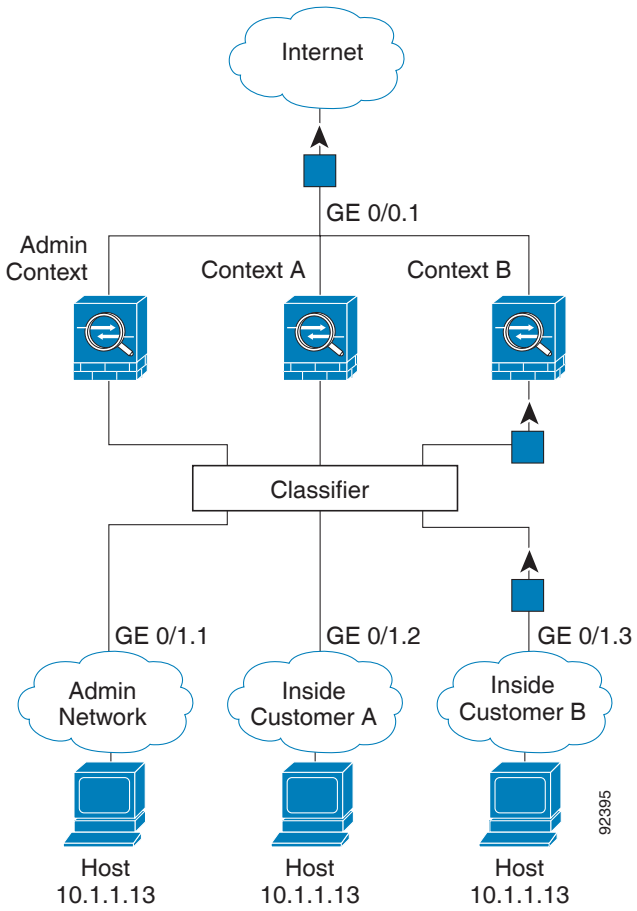
그림 6-1에서는 다중 컨텍스트가 외부 인터페이스는 공유하는 것을 보여줍니다. 분류자는 컨텍스트 B에 패킷을 지정합니다. 컨텍스트 B가 라우터에서 패킷을 보내는 패킷을 수신하는 MAC 주소를 포함하기 때문입니다.

그림 6-1 MAC 주소를 사용하는 공유 인터페이스를 통한 패킷 분류



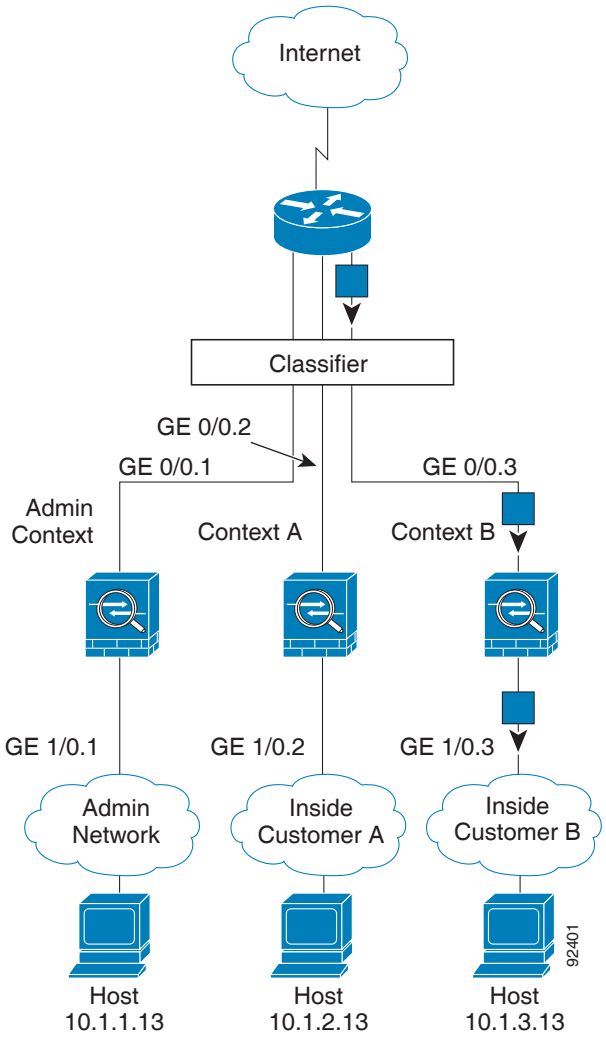
내부 네트워크에서 보낸 것을 비롯하여 모든 신규 수신 트래픽은 분류되어야 합니다. 그림 6-2에서는 인터넷에 액세스하는 컨텍스트 B 내부 네트워크의 호스트를 보여줍니다. 분류자는 컨텍스트 B에 패킷을 지정합니다. 인그레스 인터페이스가 컨텍스트 B에 지정되는 기가비트 이더넷 0/1.3이기 때문입니다.

그림 6-2 내부 네트워크에서 보내는 수신 트래픽



투명 방화벽의 경우 고유한 인터페이스를 사용해야 합니다. 그림 6-3에서는 인터넷에서 컨텍스트 B 내부 네트워크의 호스트로 갈 패킷을 보여줍니다. 분류자는 컨텍스트 B에 패킷을 지정합니다. 인그레스 인터페이스가 컨텍스트 B에 지정되는 기가비트 이더넷 1/0.3이기 때문입니다.

그림 6-3 투명 방화벽 컨텍스트



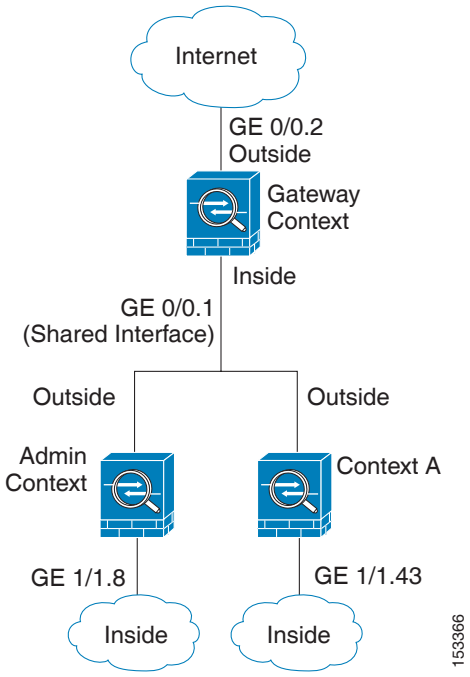
보안 컨텍스트 캐스케이딩

어떤 컨텍스트의 바로 앞에 다른 컨텍스트를 놓는 것을 *컨텍스트 캐스케이딩*이라고 합니다. 한 컨텍스트의 외부 인터페이스가 다른 컨텍스트의 내부 인터페이스가 됩니다. 최상위 컨텍스트에서 공유 매개 변수를 컨피그레이션함으로써 일부 컨텍스트의 컨피그레이션을 간소화하고 싶다면 컨텍스트 캐스케이딩이 유용할 수 있습니다.

참고 컨텍스트를 캐스케이딩하려면 컨텍스트 인터페이스별로 고유한 MAC 주소가 필요합니다(기본 설정). MAC 주소 없이 공유 인터페이스에서 패킷을 분류하면 여러 제약이 따라므로, 고유한 MAC 주소 없이 컨텍스트를 캐스케이딩하는 것은 권장되지 않습니다.

그림 6-4에서는 2개의 컨텍스트가 게이트웨이의 뒤에 있는 게이트웨이 컨텍스트를 보여줍니다.

그림 6-4 컨텍스트 캐스케이딩



보안 컨텍스트에 대한 관리 액세스

ASA에서는 다중 컨텍스트 모드에서 시스템 관리자 액세스를 제공할 뿐만 아니라 개별 컨텍스트 관리자를 위한 액세스도 제공합니다. 다음 섹션에서는 시스템 관리자나 컨텍스트 관리자로 로그인하는 것에 대해 설명합니다.

- 6-7 페이지의 시스템 관리자 액세스
- 6-8 페이지의 컨텍스트 관리자 액세스

시스템 관리자 액세스

2가지 방법으로 ASA에 시스템 관리자로 액세스할 수 있습니다.

- ASA 콘솔에 액세스합니다.

  콘솔에서 *시스템 실행 영역*에 액세스합니다. 여기서 입력하는 모든 명령은 시스템 컨피그레이션 또는 (런타임 명령의 경우) 시스템 실행에만 영향을 줍니다.

- 텔넷, SSH 또는 ASDM을 사용하여 관리 컨텍스트에 액세스합니다.

  텔넷, SSH, ASDM 액세스를 활성화하려면 35 장, "관리 액세스"를 참조하십시오.

시스템 관리자로서 모든 컨텍스트에 액세스할 수 있습니다.

관리 또는 시스템에서 어떤 컨텍스트로 전환하면 사용자 이름이 기본 이름인 "enable_15"로 바뀝니다. 그 컨텍스트에서 명령 권한 부여를 구성한 경우 "enable_15" 사용자에 대해 권한을 구성해야 합니다. 혹은 충분한 권한을 부여한 다른 이름으로 로그인할 수도 있습니다. 새 사용자 이름으로 로그인하려면 **login** 명령을 입력합니다. 예를 들어, 사용자 이름 "admin"으로 관리 컨텍스트에 로그

인합니다. 관리 컨텍스트는 어떤 명령 권한 부여 컨피그레이션도 없지만, 다른 모든 컨텍스트에 명령 권한 부여가 있습니다. 편의를 위해 각 컨텍스트 컨피그레이션에는 최대 권한을 가진 "admin" 사용자가 있습니다. 관리 컨텍스트에서 컨텍스트 A로 전환하면 사용자 이름이 enable_15로 바뀌므로, **login** 명령을 입력하여 다시 "admin"으로 로그인해야 합니다. 컨텍스트 B로 전환했으면 다시 **login** 명령을 입력하여 "admin"으로 로그인해야 합니다.

시스템 실행 영역은 AAA 명령을 지원하지 않으므로, 로컬 데이터베이스에 자체 enable 비밀번호와 사용자 이름을 구성하여 개별 로그인을 제공할 수 있습니다.

컨텍스트 관리자 액세스

텔넷, SSH 또는 ASDM을 사용하여 컨텍스트에 액세스할 수 있습니다. 비 admin 컨텍스트로 로그인한 경우 그 컨텍스트의 컨피그레이션만 액세스 가능합니다. 컨텍스트에 개별 로그인을 제공할 수 있습니다. 텔넷, SSH, ASDM 액세스를 활성화하고 관리 인증을 구성하려면 35 장, "관리 액세스"를 참조하십시오.

리소스 관리에 대한 정보

기본적으로 모든 보안 컨텍스트는 컨텍스트별 최대 제한이 적용되는 경우는 제외하고 ASA의 리소스에 무제한으로 액세스할 수 있습니다. 유일한 예외가 VPN 리소스인데, 이는 기본적으로 비활성화되어 있습니다. 하나 이상의 컨텍스트에서 너무 많은 리소스를 사용하고 있으며 그로 인해 다른 컨텍스트의 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 컨텍스트를 리소스 클래스에 지정하는 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 리소스는 ASA에서 클래스에 지정된 컨텍스트 각각에 리소스의 일부를 따로 배정하지 않습니다. 그보다는 ASA에서 컨텍스트의 최대 제한을 설정합니다. 리소스를 오버서브스크립션하거나 일부 리소스가 무제한이 되는 것을 허용할 경우, 몇몇 컨텍스트에서 이 리소스를 "소진"하여 다

른 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 ASA는 "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.

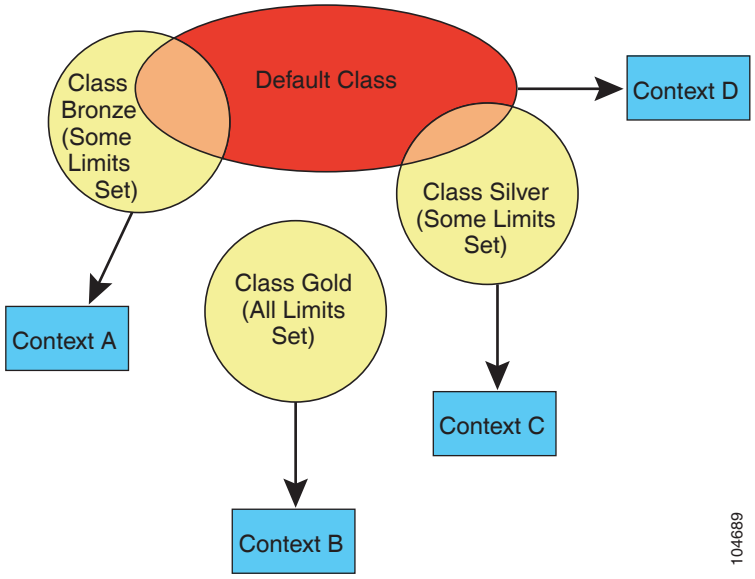
어떤 컨텍스트가 기본 클래스가 아닌 클래스에 속할 경우, 항상 이 클래스의 설정이 기본 클래스의 설정에 우선합니다. 그러나 그 클래스에서 어떤 설정이 정의되지 않았다면 멤버 컨텍스트는 기본 클래스의 해당 제한을 적용합니다. 예를 들어, 모든 동시 연결에 대한 2% 제한이 있지만 그 밖의 어떤 제한도 없는 클래스를 만든다면 그 밖의 제한은 기본 클래스로부터 상속됩니다. 이와 달리 모든 리소스에 대해 제한이 있는 클래스를 만들 경우 이 클래스는 기본 클래스의 어떤 설정도 사용하지 않습니다.

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(컨텍스트당 최대 제한)
- VPN 사이트 대 사이트 터널—0개 세션(VPN 세션을 허용하려면 직접 클래스를 구성해야 함)

그림 6-5에서는 기본 클래스와 다른 클래스의 관계를 보여줍니다. 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 Gold 클래스에 속해 있기 때문입니다. 컨텍스트 D는 클래스에 지정되지 않았으므로, 기본적으로 기본 클래스의 멤버입니다.

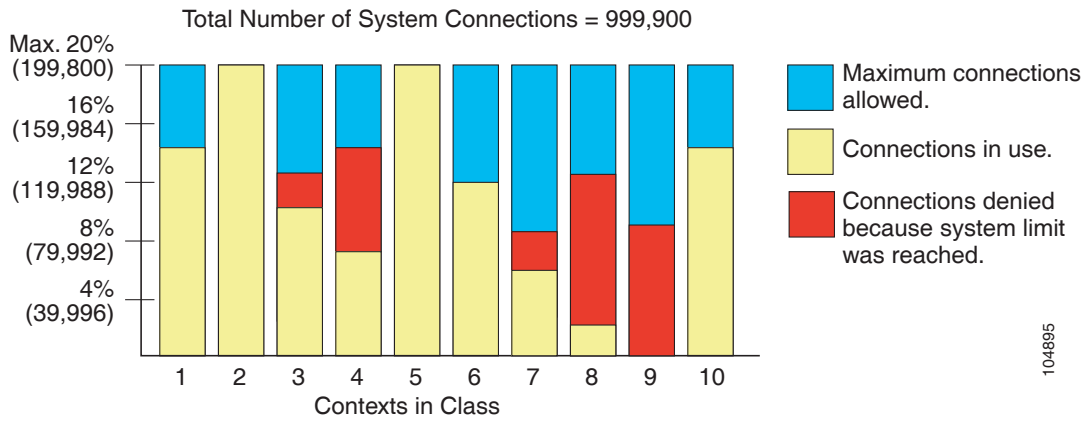
그림 6-5 리소스 클래스



오버서브스크립션된 리소스 사용

모든 컨텍스트를 통틀어 100%가 넘는 리소스를 할당함으로서 ASA를 오버서브스크립션할 수 있습니다(비 버스트 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 6-6를 참조하십시오.

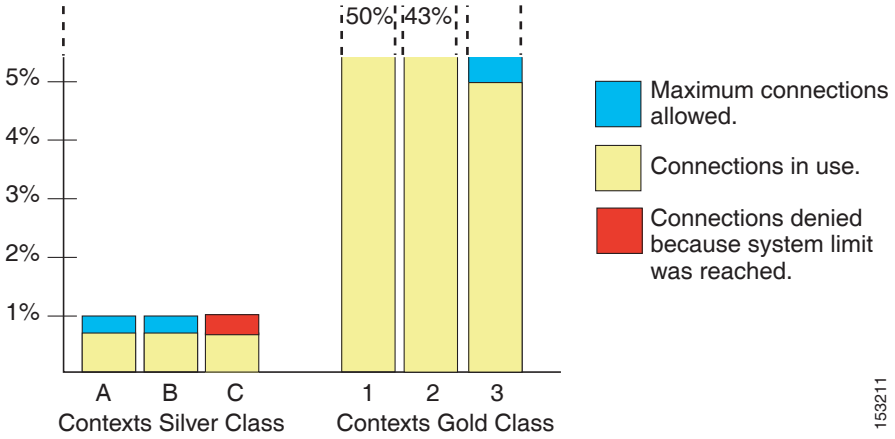
그림 6-6 리소스 오버서브스크립션



무제한 리소스 사용

ASA에서는 클래스의 하나 이상의 리소스에 대해 백분율이나 절대값이 아닌 무제한 액세스를 지정할 수 있습니다. 어떤 리소스가 무제한이 되면 컨텍스트는 시스템의 가용 제한에서 그 리소스를 최대한 많이 사용할 수 있습니다. 이를테면 컨텍스트 A, B, C는 Silver 클래스인데, 이 클래스는 각 멤버를 연결의 1%로 제한하므로 총 3%가 됩니다. 그러나 이 세 컨텍스트는 현재 모두 합쳐 2%만 사용하고 있습니다. Gold 클래스는 무제한으로 연결에 액세스합니다. Gold 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 (그림 6-7 참조). 무제한 액세스 설정은 ASA의 오버서브스크립션과 비슷하지만, 시스템의 오버서브스크립션 용량을 그만큼 제어하지는 않습니다.

그림 6-7 무제한 리소스



MAC 주소에 대한 정보

컨텍스트에서 인터페이스를 공유할 수 있도록 ASA에서는 기본적으로 각 공유 컨텍스트 인터페이스에 가상 MAC 주소를 부여합니다. 자동 생성을 사용자 지정하거나 비활성화하려면 6-24 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정을 참조하십시오.

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. 패킷 분류에 대한 자세한 내용은 6-3 페이지의 ASA의 패킷 분류를 참조하십시오.

드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 컨텍스트 내에서 그 인터페이스의 MAC 주소를 직접 설정할 수 있습니다. MAC 주소를 직접 설정하려면 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.

기본 MAC 주소

자동 MAC 주소 생성은 기본적으로 활성화되어 있습니다. ASA는 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동 생성합니다. 원한다면 접두사를 사용자 지정할 수 있습니다.

MAC 주소 생성을 비활성화한 경우 다음 기본 MAC 주소를 참조하십시오.

- ASA 5500-X 시리즈 어플라이언스—물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.
- ASASM—모든 VLAN 인터페이스가 백플레인 MAC 주소에서 파생된 동일한 MAC 주소를 사용합니다.

6-12 페이지의 MAC 주소 형식도 참조하십시오.

참고 (8.5(1.6) 이하) 장애 조치 쌍을 위한 히트리스(hitless) 업그레이드를 유지하고자 ASA는 장애 조치가 활성화된 경우 다시 로드할 때 기존 레거시 자동 생성 컨피그레이션을 변환하지 않습니다. 그러나 특히 ASASM에서는 장애 조치를 사용할 때 직접 접두사 생성 방법으로 바꾸는 것이 좋습니다. 접두사 방법을 사용하지 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. 레거시 방법에 대한 자세한 내용은 명령 참조에서 **mac-address auto** 명령을 참조하십시오.

수동 MAC 주소와의 상호 작용

직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우 직접 지정한 수동 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 삭제할 경우 자동 생성 주소가 사용됩니다.

자동 생성 주소는 (접두사 사용 시) A2로 시작하므로, 자동 생성도 사용하려는 경우 수동 MAC 주소가 A2로 시작해서는 안 됩니다.

장애 조치 MAC 주소

장애 조치에 사용할 수 있도록 ASA에서는 인터페이스마다 활성 MAC 주소와 대기 MAC 주소를 모두 생성합니다. 활성 유닛이 장애 조치하고 대기 유닛이 활성화되면 새 활성 유닛은 활성 MAC 주소를 사용하기 시작하므로 네트워크 중단이 최소화됩니다. 자세한 내용은 6-12 페이지의 MAC 주소 형식 섹션을 참조하십시오.

MAC 주소 형식

ASA에서는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx*.*yyzz*.*zzzz*

여기서 *xx*.*yy*는 사용자가 정의한 접두사이거나 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 자동 생성된 접두사이며, *zz*.*zzzz*는 ASA에 의해 생성된 내부 카운터입니다. 대기 MAC 주소는 동일하지만, 내부 카운터가 1만큼 큽니다.

접두사가 어떻게 사용되는지 예를 들어 설명하자면, 접두사를 77로 설정한 경우ASA는 77을 16진수 값인 004D(*yyxx*)로 변환합니다. 접두사가 MAC 주소에서 쓰일 때는 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 접두사 없는 MAC 주소 형식은 최신 ASA 버전에서 지원되지 않는 레거시 버전입니다. 레거시 형식에 대한 자세한 내용은 명령 참조에서 **mac-address auto** 명령을 참조하십시오.

다중 컨텍스트 모드를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASA 5512-X	• Base 라이센스: 지원 안 함 • Security Plus 라이센스: 2개 컨텍스트 *선택적 라이센스: 5개 컨텍스트*
ASA 5515-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5개 컨텍스트*
ASA 5525-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10 또는 20개 컨텍스트*
ASA 5545-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20 또는 50개 컨텍스트*
ASA 5555-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50 또는 100개 컨텍스트*
ASA 5585-X 및 SSP-10	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50 또는 100개 컨텍스트*
ASA 5585-X 및 SSP-20, -40, -60	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50, 100 또는 250개 컨텍스트*
ASASM	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50, 100 또는 250개 컨텍스트*
ASAv	지원 안 함

전제 조건

다중 컨텍스트 모드에 들어온 다음 시스템 또는 관리 컨텍스트에 연결하여 시스템 컨피그레이션에 액세스합니다. 비 관리 컨텍스트에서 시스템을 구성할 수 없습니다. 기본적으로 다중 컨텍스트 모드를 활성화한 다음에는 기본 관리 IP 주소를 사용하여 관리 컨텍스트에 연결할 수 있습니다. ASA에 연결하는 것에 대한 자세한 내용은 2 장, "시작하기"를 참조하십시오.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원됩니다. 컨텍스트별로 방화벽 모드를 설정합니다.

장애 조치 지침

활성/활성(Active/Active) 모드 장애 조치는 다중 컨텍스트 모드에서만 지원됩니다.

IPv6 지침

IPv6를 지원합니다.

참고 교차 컨텍스트 IPv6 라우팅은 지원되지 않습니다.

지원되지 않는 기능

다중 컨텍스트 모드는 다음 기능을 지원하지 않습니다.

- RIP
- OSPFv3. (OSPFv2는 지원)
- 멀티캐스트 라우팅
- 위협 감지
- 통합 커뮤니케이션
- QoS
- 원격 액세스 VPN (사이트 대 사이트 VPN은 지원)

추가 지침

- (단일 또는 다중) 컨텍스트 모드는 재부팅할 때 유지되더라도 컨피그레이션 파일에 저장되지 않습니다. 컨피그레이션을 다른 디바이스에 복사하려면 새 디바이스의 모드를 일치하게 설정합니다.
- 플래시 메모리의 루트 디렉토리에 컨텍스트 컨피그레이션을 저장할 경우, 일부 모델에서는 가용 메모리가 있더라도 이 디렉토리의 공간이 부족해질 수 있습니다. 그러한 경우 컨피그레이션 파일을 위한 하위 디렉토리를 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).

기본 설정

- 기본적으로 ASA는 단일 컨텍스트 모드입니다.
- 6-9 페이지의 기본 클래스를 참조하십시오.
- 6-12 페이지의 기본 MAC 주소를 참조하십시오.

다중 컨텍스트 모드 구성

이 섹션에서는 다중 컨텍스트 모드를 구성하는 방법을 설명합니다.

다중 컨텍스트 모드 구성의 작업 흐름

다중 컨텍스트 모드를 구성하려면 다음 단계를 수행합니다.

1단계 다중 컨텍스트 모드를 활성화합니다. 6-15 페이지의 다중 컨텍스트 모드 활성화 또는 비활성화를 참조하십시오.

2단계 (선택 사항) 리소스 관리를 위한 클래스를 구성합니다. 6-17 페이지의 리소스 관리를 위한 클래스 구성를 참조하십시오. **참고**: VPN을 지원하려면 리소스 클래스에 VPN 리소스를 구성해야 합니다. 기본 클래스는 VPN을 허용하지 않습니다.

3단계 시스템 실행 영역에서 인터페이스를 구성합니다.

- ASA 5500-X—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
- ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"

4단계 보안 컨텍스트를 구성합니다. 6-19 페이지의 보안 컨텍스트 구성을 참조하십시오.

5단계 (선택 사항) MAC 주소 할당을 사용자 지정합니다. 6-24 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정을 참조하십시오.

6단계 컨텍스트에서 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

다중 컨텍스트 모드 활성화 또는 비활성화

Cisco에 주문한 내용에 따라 ASA에서 이미 다중 보안 컨텍스트가 구성되었을 수도 있습니다. 단일 모드에서 다중 모드로 전환하려면 이 섹션의 절차를 따르십시오.

다중 컨텍스트 모드 활성화

단일 모드에서 다중 모드로 전환할 때 ASA는 실행 중 컨피그레이션을 (내부 플래시 메모리의 루트 디렉토리에서) 2개 파일로 변환합니다. 시스템 컨피그레이션인 새로운 시작 컨피그레이션과 관리 컨텍스트인 admin.cfg입니다. 원래의 실행 중 컨피그레이션은 old_running.cfg로 (내부 플래시 메모리의 루트 디렉토리에) 저장됩니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. ASA는 관리 컨텍스트 항목을 "admin"이라는 이름으로 시스템 컨피그레이션에 자동 추가합니다.

전제 조건

시작 컨피그레이션을 백업합니다. 단일 모드에서 다중 모드로 전환할 때 ASA는 실행 중 컨피그레이션을 2개 파일로 변환합니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. 36-24 페이지의 컨피그레이션 또는 기타 파일 백업 및 복원를 참조하십시오.

세부 단계

명령	목적
mode multiple **예:** `ciscoasa(config)# mode multiple`	다중 컨텍스트 모드로 바꿉니다. ASA를 재부팅하라는 메시지가 나타납니다.

단일 컨텍스트 모드 복원

기존의 실행 중 컨피그레이션을 시작 컨피그레이션에 복사하고 모드를 단일 모드로 변경하려면 다음 단계를 수행합니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

	명령	목적
1단계	**copy disk0:old_running.cfg startup-config** **예:** `ciscoasa(config)# copy disk0:old_running.cfg startup-config`	원래 실행 중 컨피그레이션의 백업 버전을 현재 시작 컨피그레이션에 복사합니다.
2단계	**mode single** **예:** `ciscoasa(config)# mode single`	모드를 단일 모드로 설정합니다. ASA를 재부팅하라는 메시지가 나타납니다.

리소스 관리를 위한 클래스 구성

시스템 컨피그레이션에서 클래스를 구성하려면 다음 단계를 수행합니다. 새 값으로 명령을 다시 입력하여 특정 리소스 제한의 값을 변경할 수 있습니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

지침

표 6-1에서는 리소스 유형과 그 제한을 보여줍니다. **show resource types** 명령도 참조하십시오.

표 6-1 리소스 이름 및 제한

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한[1]	설명
asdm	동시	최소 1 최대 5	32	ASDM 관리 세션. **참고** ASDM 세션은 2개의 HTTPS 연결을 사용합니다. 하나는 모니터링용으로 항상 실행되며, 다른 하나는 컨피그레이션 변경용으로 변경할 때만 실행됩니다. 예를 들어, 시스템 제한이 32개 ASDM 세션이라면 64개 HTTPS 세션을 의미합니다.
conns[2]	동시 또는 비율	N/A	동시 연결: 해당 모델의 연결 제한은 4-1 페이지의 모델당 지원되는 기능 라이센스를 참조하십시오. 비율: N/A	임의의 두 호스트 간의 TCP 또는 UDP 연결. 단일 호스트와 여러 다른 호스트 간의 연결 포함
hosts	동시	N/A	N/A	ASA를 통해 연결될 수 있는 호스트
inspects	비율	N/A	N/A	초당 애플리케이션 검사 수
mac-addresses	동시	N/A	65,535	투명 방화벽 모드의 경우 MAC 주소 테이블에서 허용되는 MAC 주소의 수
routes	동시	N/A	N/A	동적 경로
vpn burst other	동시	N/A	해당 모델의 기타 VPN 세션의 양에서 **vpn other**에 할당된 세션의 합계를 뺀 것.	**vpn other**로 컨텍스트에 할당된 양을 초과하는 허용된 사이트 대 사이트 VPN 세션 수 예를 들어, 모델에서 세션 5000개를 지원하는데 **vpn other**으로 컨텍스트 전체에 세션 4000개를 할당한 경우, 나머지 1000개 세션은 **vpn burst other**에서 사용 가능합니다. 컨텍스트에 대한 세션을 보장하는 **vpn other**와 달리, **vpn burst other**는 오버서브스크립션이 가능합니다. 버스트 풀은 모든 컨텍스트가 선착순으로 사용할 수 있습니다.

표 6-1 리소스 이름 및 제한(계속)

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한[1]	설명
vpn other	동시	N/A	해당 모델에서 사용 가능한 기타 VPN 세션은 4-1 페이지의 모델당 지원되는 기능 라이센스를 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.
ssh	동시	최소 1 최대 5	100	SSH 세션
syslogs	비율	N/A	N/A	초당 syslog 메시지 수
telnet	동시	최소 1 최대 5	100	텔넷 세션
xlates[2]	동시	N/A	N/A	네트워크 주소 변환

1. 이 열의 값이 N/A이면 해당 리소스에 대한 명시적 시스템 제한이 없으므로 리소스의 비율을 설정할 수 없습니다.
2. 어떤 제한이든 더 낮은 xlate 또는 conn일 때 syslog 메시지가 생성됩니다. 이를테면 xlate 제한을 7로, conn를 9로 설정한 경우 ASA는 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.

세부 단계

	명령	목적
1단계	**class** *name* **예:** `ciscoasa(config)# class gold`	클래스 이름을 지정하고 클래스 컨피그레이션 모드를 입력합니다. *name*은 최대 20자의 문자열입니다. 기본 클래스에 대해 이 제한을 설정하려면 **default**를 이름으로 입력합니다.
2단계	**limit-resource** [**rate**] *resource_name number*[**%**] **예:** `ciscoasa(config-class)# limit-resource rate inspects 10`	리소스 유형에 대한 리소스 제한을 설정합니다. 리소스 유형의 목록은 표 6-1 를 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
```

보안 컨텍스트 구성

시스템 컨피그레이션의 보안 컨텍스트 정의는 컨텍스트 이름, 컨피그레이션 파일 URL, 컨텍스트에서 사용할 수 있는 인터페이스 및 기타 설정을 나타냅니다.

전제 조건

- 시스템 실행 영역에서 이 절차를 수행합니다.
- ASASM에서는 3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"에 따라 스위치의 ASASM에 VLAN을 지정합니다.
- ASA 5500-X의 경우 9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"에 따라 물리적 인터페이스 매개 변수, VLAN 하위 인터페이스, EtherChannel, 이중 인터페이스를 구성합니다.
- 관리 컨텍스트가 없는 경우(예: 이 컨피그레이션을 지웠음) 먼저 다음 명령을 입력하여 관리 컨텍스트 이름을 지정해야 합니다.

  ```
  ciscoasa(config)# admin-context name
  ```

  이 컨텍스트는 아직 컨피그레이션에 없지만, 그 다음에 **context** *name* 명령을 입력하여 관리 컨텍스트 컨피그레이션을 계속할 수 있습니다.

세부 단계

	명령	목적
1단계	**context** *name* **예:** `ciscoasa(config)# context administrator`	컨텍스트를 추가하거나 수정합니다. *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. "System"과 "Null"(대문자 및 소문자 모두 해당)은 예약된 이름이므로 사용할 수 없습니다.
2단계	(선택 사항) **description** *text* **예:** `ciscoasa(config-ctx)# description Administrator Context`	이 컨텍스트에 대한 설명을 추가합니다.

명령	목적
3단계 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**] **예:** 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	컨텍스트에서 사용할 수 있는 인터페이스를 지정합니다. 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 컨텍스트 명령이 실행 중 컨피그레이션에서 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. ASASM를 위한 별도의 관리 인터페이스는 제공되지 않습니다. 라우티드 모드에서는 원한다면 여러 컨텍스트에 동일한 인터페이스를 지정할 수 있습니다. 투명 모드에서는 공유 인터페이스를 허용하지 않습니다. *mapped_name*은 인터페이스의 영숫자 별칭으로서 컨텍스트 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, 다음 이름을 사용할 수 있습니다. **int0**, **inta**, **int_0** 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, 다음과 같이 범위를 입력합니다. **int0-int10** 만약 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 100개 인터페이스를 포함합니다. **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100** 만약 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** 키워드는 매핑된 이름만 표시합니다.

	명령	목적
4단계	**config-url** *url* **예:** `ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg`	시스템이 컨텍스트 컨피그레이션을 다운로드할 URL을 나타냅니다. 컨텍스트 URL을 추가하면, 해당 컨피그레이션이 사용 가능한 경우 시스템에서 즉시 컨텍스트를 로드하므로 실행 중이 됩니다. **참고** **allocate-interface** 명령을 **config-url** 명령보다 먼저 입력합니다. **config-url** 명령을 먼저 입력하면 ASA는 즉시 컨텍스트 컨피그레이션을 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 컨텍스트에서 액세스할 수 있어야 합니다. 컨피그레이션 파일을 사용할 수 없는 경우 다음 메시지가 표시됩니다. `WARNING: Could not fetch the URL url` `INFO: Creating context with default config` 비 HTTP(S) URL 위치의 경우, URL을 지정한 다음 컨텍스트로 바꾸고 CLI에서 구성할 수 있습니다. 그리고 **write memory** 명령을 입력하여 URL 위치에 파일을 쓸 수 있습니다. HTTP(S)는 읽기 전용입니다. **참고** 관리 컨텍스트 파일은 내부 플래시 메모리에 저장해야 합니다. 사용 가능한 URL 유형은 **disk***number*(플래시 메모리), **ftp**, **http**, **https** 또는 **tftp** 등입니다. URL을 변경하려면 새 URL과 함께 **config-url** 명령을 다시 입력합니다. URL 변경에 대한 자세한 내용은 6-26 페이지의 보안 컨텍스트 URL 변경을 참조하십시오.
5단계	(선택 사항) **member** *class_name* **예:** `ciscoasa(config-ctx)# member gold`	리소스 클래스에 컨텍스트를 지정합니다. 클래스를 지정하지 않으면 컨텍스트는 기본 클래스에 속합니다. 하나의 컨텍스트는 하나의 리소스 클래스에만 지정할 수 있습니다.
6단계	(선택 사항) **allocate-ips** *sensor_name* [*mapped_name*] [**default**] **예:** `ciscoasa(config-ctx)# allocate-ips sensor1 highsec`	IPS 모듈이 설치된 경우 이 컨텍스트에 IPS 가상 센서를 지정합니다. 가상 센서에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

	명령	목적
7단계	(선택 사항) **join-failover-group** {**1** | **2**) 예: ciscoasa(config-ctx)# join-failover-group 2	활성/활성 장애 조치에서 장애 조치 그룹에 컨텍스트를 지정합니다. 기본적으로 컨텍스트는 그룹 1에 있습니다. 관리 컨텍스트는 항상 그룹 1에 있어야 합니다. 장애 조치 그룹에 대한 자세한 내용은 7-35 페이지의 선택적 장애 조치 매개변수 구성을 참조하십시오.
8단계	(선택 사항) **scansafe** [**license** *key*] 예: ciscoasa(config-ctx)# scansafe	이 컨텍스트에서 Cloud Web Security를 활성화합니다. **license**를 지정하지 않으면 컨텍스트는 시스템 컨피그레이션에 구성된 라이센스를 사용합니다. ASA는 Cloud Web Security 프록시 서버에 인증 키를 보내 어떤 조직에서 요청을 보냈는지 알립니다. 인증 키는 16바이트 16진수입니다. ScanSafe에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

예

다음 예에서는 관리 컨텍스트를 "administrator"가 되게 설정하고 내부 플래시 메모리에 "administrator"라는 컨텍스트를 만든 다음 FTP 서버에서 2개의 컨텍스트를 추가합니다.

```
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 silver
```

컨텍스트 인터페이스에 MAC 주소 자동 지정

이 섹션에서는 MAC 주소의 자동 생성을 구성하는 방법을 설명합니다.

이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다. 자세한 내용은, 특히 이전 AAA 버전에서 업그레이드하는 경우에는 6-11 페이지의 MAC 주소에 대한 정보를 참조하십시오. 6-36 페이지의 지정된 MAC 주소 보기도 참조하십시오.

지침

- 컨텍스트에서 인터페이스에 대해 **nameif** command을 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. MAC 주소를 직접 설정하려면 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.

세부 단계

명령	목적
mac-address auto [**prefix** *prefix*] **예:** `ciscoasa(config)# mac-address auto prefix 19`	각 컨텍스트 인터페이스에 사설 MAC 주소를 자동으로 지정합니다. 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. 접두사를 사용하는 방법에 대한 자세한 내용은 6-12 페이지의 MAC 주소 형식을 참조하십시오.

컨텍스트와 시스템 실행 영역 간 전환

시스템 실행 영역(또는 관리 컨텍스트)에 로그인한 경우 여러 컨텍스트로 전환하면서 각 컨텍스트에서 컨피그레이션 및 모니터링 작업을 수행할 수 있습니다. 컨피그레이션 모드에서 수정하거나 **copy** 또는 **write** 명령에서 사용되는 실행 중 컨피그레이션은 위치에 따라 달라집니다. 시스템 실행 영역이라면 실행 중 컨피그레이션은 시스템 컨피그레이션으로만 이루어집니다. 컨텍스트에 있을 경우 실행 중 컨피그레이션은 그 컨텍스트로만 이루어집니다. 예를 들어, **show running-config** 명령을 입력할 때 모든 실행 중 컨피그레이션(시스템 및 모든 컨텍스트)을 볼 수는 없습니다. 현재 컨피그레이션만 표시됩니다.

세부 단계

명령	목적
changeto context *name*	어떤 컨텍스트로 변경합니다. 프롬프트가 다음과 같이 바뀝니다. `ciscoasa/name#`
changeto system	시스템 실행 영역으로 변경합니다. 프롬프트가 다음과 같이 바뀝니다. `ciscoasa#`

보안 컨텍스트 관리

이 섹션에서는 보안 컨텍스트를 관리하는 방법을 설명합니다.

- 6-25 페이지의 보안 컨텍스트 삭제
- 6-26 페이지의 관리 컨텍스트 변경
- 6-26 페이지의 보안 컨텍스트 URL 변경
- 6-27 페이지의 보안 컨텍스트 다시 로드

보안 컨텍스트 삭제

현재 관리 컨텍스트를 삭제할 수 없습니다. **clear context** 명령을 사용하여 모든 컨텍스트를 삭제하는 것만 가능합니다.

참고 장애 조치를 사용하는 경우, 활성 유닛에서 컨텍스트를 삭제하는 시점과 대기 유닛에서 컨텍스트가 삭제되는 시점 간에 지연이 발생합니다. 활성 유닛과 대기 유닛의 인터페이스 수가 일치하지 않는다는 오류 메시지가 나타날 수 있으나, 이는 일시적인 것이므로 무시해도 됩니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

명령	목적
no context *name*	단일 컨텍스트를 삭제합니다. 모든 컨텍스트 명령도 삭제됩니다. 컨텍스트 컨피그레이션 파일은 config URL 위치에서 삭제되지 않습니다.
clear context	(관리 컨텍스트를 포함하여) 모든 컨텍스트를 삭제합니다. 컨텍스트 컨피그레이션 파일은 config URL 위치에서 삭제되지 않습니다.

관리 컨텍스트 변경

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.

관리 컨텍스트는 여느 컨텍스트와 비슷하지만, 사용자가 관리 컨텍스트에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 컨텍스트에 액세스할 수 있다는 점이 다릅니다. 관리 컨텍스트는 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 컨텍스트에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 컨텍스트 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다.

지침

어떤 컨텍스트도 관리 컨텍스트로 설정할 수 있습니다. 단, 컨피그레이션 파일이 내부 플래시 메모리에 저장되어 있어야 합니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

명령	목적
admin-context *context_name* **예:** `ciscoasa(config)# admin-context administrator`	관리 컨텍스트를 설정합니다. 텔넷, SSH, HTTPS와 같이 관리 컨텍스트에 연결되어 있는 원격 관리 세션은 모두 종료됩니다. 새 관리 컨텍스트에 다시 연결해야 합니다. **참고** **ntp server**와 같이 몇 가지 시스템 컨피그레이션 명령은 관리 컨텍스트에 속한 인터페이스 이름을 지정합니다. 관리 컨텍스트를 변경하는 경우, 그 인터페이스 이름이 새 관리 컨텍스트에 없다면 그 이름을 참조하는 모든 시스템 명령을 업데이트해야 합니다.

보안 컨텍스트 URL 변경

이 섹션에서는 컨텍스트 URL을 변경하는 방법을 설명합니다.

지침

- 새 URL에서 컨피그레이션을 다시 로드하지 않고는 보안 컨텍스트 URL을 변경할 수 없습니다. ASA에서는 새 컨피그레이션을 현재 실행 중인 컨피그레이션과 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 컨텍스트 실행에 영향을 줄 경 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.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

	명령	목적
1단계	(병합을 원치 않을 경우의 선택 사항) **changeto context** *name* **clear configure all** 예: `ciscoasa(config)# changeto context ctx1` `ciscoasa/ctx1(config)# clear configure all`	컨텍스트로 변경하고 그 컨피그레이션을 지웁니다. 병합을 하려면 2단계로 진행합니다.
2단계	**changeto system** 예: `ciscoasa/ctx1(config)# changeto system` `ciscoasa(config)#`	시스템 실행 영역으로 변경합니다.
3단계	**context** *name* 예: `ciscoasa(config)# context ctx1`	변경할 컨텍스트의 컨텍스트 컨피그레이션 모드로 들어갑니다.
4단계	**config-url** *new_url* 예: `ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg`	새 URL에 접속합니다. 시스템에서 즉시 컨텍스트를 로드하므로 실행 중이 됩니다.

보안 컨텍스트 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 컨피그레이션에서 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.

- 6-28 페이지의 컨피그레이션을 지워 다시 로드
- 6-28 페이지의 컨텍스트를 삭제하고 다시 추가하여 다시 로드

컨피그레이션을 지워 다시 로드

컨텍스트 컨피그레이션을 지우고 URL에서 컨피그레이션을 다시 로드하여 컨텍스트를 다시 로드하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**changeto context** *name* 예: `ciscoasa(config)# changeto context ctx1` `ciscoasa/ctx1(comfig)#`	다시 로드할 컨텍스트로 변경합니다.
2단계	**clear configure all** 예: `ciscoasa/ctx1(config)# clear configure all`	실행 중인 컨텍스트를 지웁니다. 이 명령은 모든 연결을 끊습니다.
3단계	**copy startup-config running-config** 예: `ciscoasa/ctx1(config)# copy startup-config running-config`	컨피그레이션을 다시 로드합니다. ASA에서는 시스템 컨피그레이션에 지정된 URL에서 컨피그레이션을 복사합니다. 컨텍스트 내에서 URL을 변경할 수 없습니다.

컨텍스트를 삭제하고 다시 추가하여 다시 로드

컨텍스트를 삭제한 다음 다시 추가하는 방법으로 컨텍스트를 다시 로드하려면 다음 섹션의 단계를 수행합니다.

1. 6-25 페이지의 보안 컨텍스트 삭제.
2. 6-19 페이지의 보안 컨텍스트 구성

보안 컨텍스트 모니터링

이 섹션에서는 컨텍스트 정보를 보고 모니터링하는 방법을 설명합니다.

- 6-29 페이지의 컨텍스트 정보 보기
- 6-30 페이지의 리소스 할당 보기
- 6-33 페이지의 리소스 사용량 보기
- 6-34 페이지의 컨텍스트의 SYN 공격 모니터링
- 6-36 페이지의 지정된 MAC 주소 보기

컨텍스트 정보 보기

시스템 실행 영역에서 이름, 할당된 인터페이스, 컨피그레이션 파일 URL이 포함된 컨텍스트 목록을 볼 수 있습니다.

시스템 실행 영역에서 다음 명령을 입력하여 모든 컨텍스트를 볼 수 있습니다.

명령	목적
show context [*name* | **detail**| **count**]	모든 컨텍스트를 표시합니다. 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.

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
```

표 6-2에서 각 필드에 대해 설명합니다.

표 6-2 컨텍스트 필드

필드	설명
Context Name	모든 컨텍스트 이름을 나열합니다. 별표(*)로 표시된 컨텍스트 이름이 관리 컨텍스트입니다.
Interfaces	컨텍스트에 지정된 인터페이스
URL	ASA에서 컨텍스트 컨피그레이션을 로드하는 URL

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.

리소스 할당을 보려면 다음 명령을 입력합니다.

명령	목적
show resource allocation [**detail**]	리소스 할당을 표시합니다. 이 명령은 리소스 할당을 보여주지만, 실제 리소스 사용량은 표시하지 않습니다. 실제 리소스 사용량에 대한 자세한 내용은 6-33 페이지의 리소스 사용량 보기를 참조하십시오. **detail** 인수는 추가 정보를 표시합니다. 자세한 내용은 다음 샘플 출력을 참조하십시오.

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
 Other VPN Sessions            20          2.66%
 Other VPN Burst               20          2.66%
 All                    unlimited
```

표 6-3에서 각 필드에 대해 설명합니다.

표 6-3 리소스 할당 필드

필드	설명
Resource	제한할 수 있는 리소스의 이름
Total	모든 컨텍스트에 할당된 리소스의 총량. 이는 동시 인스턴스 또는 초당 인스턴스의 절대값입니다. 클래스 정의에 백분율을 지정한 경우 ASA는 백분율을 절대값으로 환산하여 여기에 표시합니다.
% of Avail	리소스에 명시적 시스템 제한이 있을 경우, 모든 컨텍스트에 할당된 전체 시스템 리소스의 백분율. 리소스에 시스템 제한이 없을 경우 이 열에는 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%
```

표 6-4에서 각 필드에 대해 설명합니다.

표 6-4 리소스 할당 세부 필드

필드	설명
Resource	제한할 수 있는 리소스의 이름
Class	기본 클래스를 포함한 각 클래스의 이름 All contexts 필드는 모든 클래스를 포괄한 총계를 표시합니다.
Mmbrs	각 클래스에 지정된 컨텍스트의 수
Origin	이 리소스 제한의 출처 • A—개별 리소스가 아닌 **all** 옵션과 함께 이 제한을 설정합니다. • C—이 제한은 멤버 클래스에서 나온 것입니다. • D—이 제한은 멤버 클래스에 정의되지 않았지만, 기본 클래스에서 나온 것입니다. 기본 클래스에 지정된 컨텍스트의 경우 값은 "D"가 아니라 "C"가 됩니다. ASA에서는 "A"를 "C" 또는 "D"와 조합할 수 있습니다.
Limit	컨텍스트별 리소스 제한이며 절대값입니다. 클래스 정의에 백분율을 지정한 경우 ASA는 백분율을 절대값으로 환산하여 여기에 표시합니다.
Total	클래스의 모든 컨텍스트에 할당된 리소스의 총량. 이는 동시 인스턴스 또는 초당 인스턴스의 절대값입니다. 리소스가 무제한일 경우 이 필드는 비어 있습니다.
% of Avail	클래스의 모든 컨텍스트에 할당된 전체 시스템 리소스의 백분율. 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.

명령	목적
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 사용할 때는 **resource all**이 아닌 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 표 6-1를 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**—현재 동시 인스턴스 또는 현재 리소스 비율을 표시합니다. • **denied**—Limit 열에 표시된 리소스 제한을 초과하여 거부된 인스턴스의 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 **all**을 지정한 경우 *count_threshold*는 현재 사용량에 적용됩니다. **참고** 모든 리소스를 표시하려면 *count_threshold*를 **0**으로 설정합니다.

다음은 **show resource usage context** 명령의 샘플 출력입니다. 여기서는 관리 컨텍스트의 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
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
Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

컨텍스트의 SYN 공격 모니터링

ASA 에서는 TCP 인터셉트를 사용하여 SYN 공격을 차단합니다. TCP 인터셉트는 SYN 쿠키 알고리즘을 통해 TCP SYN 플러딩 공격을 막아냅니다. SYN 플러딩 공격은 일련의 SYN 패킷으로 구성되는데, 대개 스푸핑된 IP 주소에서 나온 것입니다. SYN 패킷이 지속적으로 유입되면서 서버 SYN 큐를 가득 채워 연결 요청을 서비스할 수 없게 만듭니다. 어떤 연결의 최초 연결 임계값을 초과하면 ASA는 서버의 프록시 역할을 하면서 클라이언트 SYN 요청에 대해 SYN-ACK 응답을 생성합니다. ASA에서 클라이언트로부터 다시 ACK를 받으면 클라이언트를 인증하고 서버와의 연결을 허용합니다.

다음 명령을 사용하여 SYN 공격을 모니터링합니다.

명령	목적
show perfmon	개별 컨텍스트의 공격 비율을 모니터링합니다.
show resource usage detail	개별 컨텍스트에서 TCP 인터셉트가 사용 중인 리소스의 양을 모니터링합니다.
show resource usage summary detail	전체 시스템에서 TCP 인터셉트가 사용 중인 리소스를 모니터링합니다.

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
```

지정된 MAC 주소 보기

시스템 컨피그레이션 내에서 또는 컨텍스트 내에서 자동 생성된 MAC 주소를 볼 수 있습니다.

- 6-37 페이지의 시스템 컨피그레이션에서 MAC 주소 보기
- 6-38 페이지의 컨텍스트 내 MAC 주소 보기

시스템 컨피그레이션에서 MAC 주소 보기

이 단원에서는 시스템 컨피그레이션에서 MAC 주소를 보는 방법을 설명합니다.

지침

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.

세부 단계

명령	목적
show running-config all context [*name*]	시스템 실행 영역에서 지정된 MAC 주소를 표시합니다. 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 대기 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 대기)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
!
```

컨텍스트 내 MAC 주소 보기

이 섹션에서는 컨텍스트 내에서 MAC 주소를 보는 방법을 설명합니다.

세부 단계

명령	목적
show interface | include (Interface)|(MAC)	컨텍스트 내에서 각 인터페이스가 사용 중인 MAC 주소를 표시합니다.

예

예:

```
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 컨피그레이션 내에서는 사용되지 않은 자동 생성 주소만 볼 수 있습니다.

다중 컨텍스트 모드 컨피그레이션의 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 컨텍스트를 "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 컨텍스트 모드의 기능 내역

표 6-5에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 6-5 다중 컨텍스트 모드의 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
다중 보안 컨텍스트	7.0(1)	다중 컨텍스트 모드를 도입했습니다. 도입된 명령: **context**, **mode**, **class**
자동 MAC 주소 지정	7.2(1)	컨텍스트 인터페이스에 MAC 주소를 자동으로 지정하는 기능을 도입했습니다. 도입된 명령: **mac-address auto**
리소스 관리	7.2(1)	리소스 관리를 도입했습니다. 도입된 명령: **class**, **limit-resource**, **member**
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 컨텍스트 또는 단일 모드 ASA를 하나 이상의 가상 센서에 지정하거나 여러 보안 컨텍스트를 동일한 가상 센서에 지정할 수 있습니다. 도입된 명령: **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. 수정된 명령: **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. 수정된 명령: **mac-address auto**

표 6-5 다중 컨텍스트 모드의 기능 내역(계속)

기능 이름	플랫폼 릴리스	기능 정보
MAC 주소 접두사 자동 생성	8.6(1)	다중 컨텍스트 모드에서 ASA의 자동 MAC 주소 생성 컨피그레이션은 기본 접두사를 사용하도록 변환됩니다. ASA는 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 볼 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 컨피그레이션의 MAC 주소 방식을 변환하지 *않습니다*. 그러나 특히 ASASM에서는 장애 조치를 사용할 때 직접 접두사 생성 방법으로 바꾸는 것이 좋습니다. 접두사 방법을 사용하지 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 생성에서 다시 기본 접두사를 사용할 수 있게 합니다. 수정된 명령: **mac-address auto**
보안 컨텍스트의 동적 라우팅	9.0(1)	EIGRP 및 OSPFv2 동적 라우팅 프로토콜이 다중 컨텍스트 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. 수정된 명령: **limit-resource, show resource types, show resource usage, show resource allocation**
다중 컨텍스트 모드의 사이트 대 사이트 VPN	9.0(1)	사이트 대 사이트 VPN 터널이 다중 컨텍스트 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. 수정된 명령: **limit-resource, show resource types, show resource usage, show resource allocation**

고가용성을 위한 장애 조치

이 장에서는 Cisco ASA의 고가용성을 실현하기 위해 액티브/스탠바이 또는 액티브/액티브 장애 조치를 구성하는 방법에 대해 설명합니다.

장애 조치 정보

장애 조치 개요

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.

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 컨텍스트 모드에서는 ASA에 액티브/스탠바이 장애 조치를 사용할 수 있습니다.
- 액티브/액티브 장애 조치 컨피그레이션에서는 두 ASA에서 모두 네트워크 트래픽을 전달할 수 있습니다. 액티브/액티브 장애 조치는 다중 컨텍스트 모드의 ASA에만 사용할 수 있습니다. 액티브/액티브 장애 조치에서 ASA의 보안 컨텍스트는 2개의 *장애 조치* 그룹으로 나뉩니다. 장애 조치 그룹은 단순히 하나 이상의 보안 컨텍스트로 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 가지 장애 조치 구성에서는 모두 스테이트풀 및 스테이트리스 장애 조치를 지원합니다.

장애 조치 시스템 요구 사항

이 절에서는 장애 조치 컨피그레이션에서 ASA의 하드웨어, 소프트웨어, 라이센스 요구 사항에 대해 설명합니다.

- 7-2 페이지의 하드웨어 요구 사항
- 7-2 페이지의 소프트웨어 요구 사항
- 7-3 페이지의 라이센스 요구 사항

하드웨어 요구 사항

장애 조치 컨피그레이션의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 모델이어야 합니다.
- 인터페이스 개수와 유형이 같아야 합니다.
- 같은 모듈을 설치해야 합니다(있을 경우).
- 같은 RAM을 설치해야 합니다.

장애 조치 컨피그레이션에서 플래시 메모리 크기가 다른 유닛을 사용 중인 경우, 용량이 플래시 메모리 용량이 작은 유닛에 소프트웨어 이미지 파일 및 컨피그레이션 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 컨피그레이션의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 방화벽 모드에 있어야 합니다(라우팅 또는 투명).
- 같은 컨텍스트 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 버전 8.3(2)으로 업그레이드하고 장애 조치를 활성 상태로 유지할 수 있습니다. 장기적으로 호환성을 보장하려면 두 유닛을 모두 같은 버전으로 업그레이드하는 것이 좋습니다.

  장애 조치 쌍에서 소프트웨어를 업그레이드하는 방법에 대한 자세한 내용은 36-4 페이지의 장애 조치 쌍 또는 ASA 클러스터 업그레이드를 참조하십시오.
- 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.

라이센스 요구 사항

장애 조치 컨피그레이션의 유닛 2개는 라이센스가 동일하지 않아도 됩니다. 이러한 라이센스는 통합되어 장애 조치 클러스터 라이센스를 생성합니다. 자세한 내용은 4-26 페이지의 장애 조치 또는 ASA 클러스터 라이센스를 참조하십시오.

장애 조치 및 스테이트풀 장애 조치 링크

장애 조치 링크 및 옵션으로 제공되는 스테이트풀 장애 조치 링크는 2개 유닛 간의 전용 연결입니다.

- 7-3 페이지의 장애 조치 링크
- 7-4 페이지의 스테이트풀 장애 조치 링크
- 7-5 페이지의 장애 조치 및 데이터 링크 중단 방지

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, PSH(Pre-Shared key)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.

장애 조치 링크

장애 조치 쌍의 유닛 2개에서는 장애 조치 링크를 통해 지속적으로 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.

- 7-3 페이지의 장애 조치 링크 데이터
- 7-4 페이지의 장애 조치 링크에 대한 인터페이스
- 7-4 페이지의 장애 조치 링크 연결

장애 조치 링크 데이터

다음 정보는 장애 조치 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 인터페이스(물리적, 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 선택에 따라 상태 링크용으로도 사용 가능).

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. Straight-through 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

스테이트풀 장애 조치 링크

스테이트풀 장애 조치를 사용하려면 연결 상태 정보를 전달할 스테이트풀 장애 조치 링크(상태 링크라고도 함)를 구성해야 합니다.

상태 링크에 사용 가능한 인터페이스 옵션은 3가지입니다.

- 7-4 페이지의 전용 인터페이스(권장)
- 7-5 페이지의 장애 조치 링크 공유
- 7-5 페이지의 일반 데이터 인터페이스 공유(권장하지 않음)

참고 상태 링크에는 관리 인터페이스를 사용하지 마십시오.

전용 인터페이스(권장)

상태 링크에 전용 인터페이스(물리적, 이중화 또는 EtherChannel)를 사용할 수 있습니다. 다음 두 가지 방법 중 하나를 사용하여 전용 상태 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 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. Straight-through 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

장거리 장애 조치를 사용할 경우 최적의 성능을 보장하려면 장애 조치 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 장애 조치 메시지의 재전송으로 인해 일부 성능이 저하됩니다.

장애 조치 링크 공유

충분한 인터페이스가 없는 경우 장애 조치 링크를 공유해야 할 수 있습니다. 장애 조치 링크를 상태 링크로 사용할 경우 제공되는 가장 빠른 이더넷 인터페이스를 사용해야 합니다. 해당 인터페이스에 성능 문제가 발생할 경우 상태 링크에 별도의 전용 인터페이스를 지정하는 방법을 고려하십시오.

일반 데이터 인터페이스 공유(권장하지 않음)

데이터 인터페이스를 상태 링크와 공유할 경우 재생 공격에 취약해질 수 있습니다. 또한 대량의 스테이트풀 장애 조치 트래픽이 인터페이스에서 전송되어 해당 네트워크 세그먼트에 성능 문제가 발생할 수 있습니다.

데이터 인터페이스를 상태 링크로 사용하는 방법은 단일 컨텍스트, 라우팅 모드에서만 지원됩니다.

장애 조치 및 데이터 링크 중단 방지

장애 조치 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 장애 조치 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 그림 7-1 및 그림 7-2에 나온 다음 2가지 연결 방법은 권장되지 않습니다.

그림 7-1 단일 스위치로 연결 — 권장하지 않음

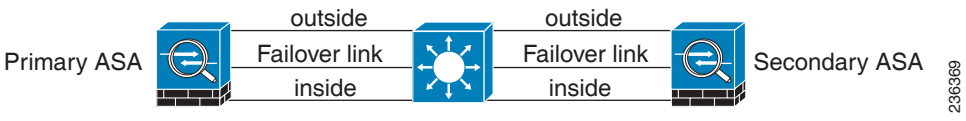
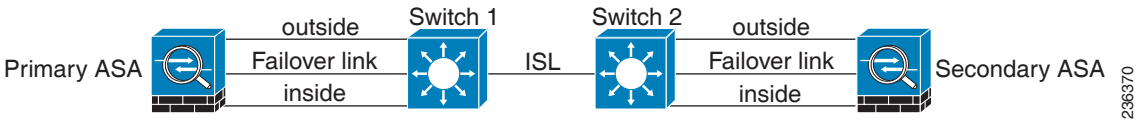


그림 7-2 이중 스위치로 연결 — 권장하지 않음



시나리오 2 — 권장

장애 조치 링크에서는 같은 스위치를 데이터 인터페이스로 사용하지 않는 것이 좋습니다. 대신 그림 7-3 및 그림 7-4에 나와 있는 것처럼 다른 스위치를 사용하거나 직접 케이블을 사용하여 장애 조치 링크에 연결합니다.

그림 7-3 다른 스위치로 연결

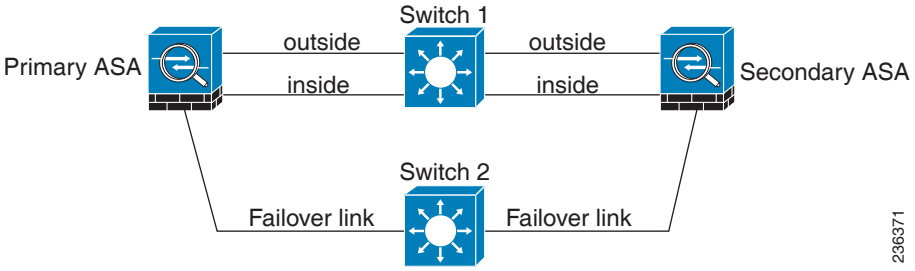
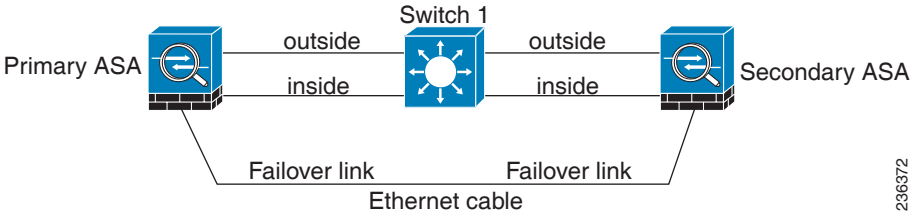


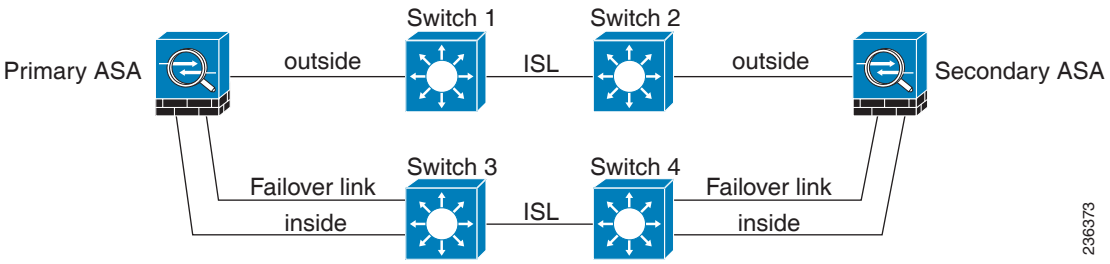
그림 7-4 케이블로 연결



시나리오 3 — 권장

ASA 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 장애 조치 링크는 이러한 스위치 중 하나에 연결될 수 있으며 그림 7-5에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 7-5 보안 스위치로 연결



시나리오 4 — 권장

가장 안정적인 장애 조치 컨피그레이션의 경우 그림 7-6 및 그림 7-7에 나와 있는 것처럼 장애 조치 링크에서 이중화 인터페이스를 사용합니다.

그림 7-6 이중화 인터페이스로 연결

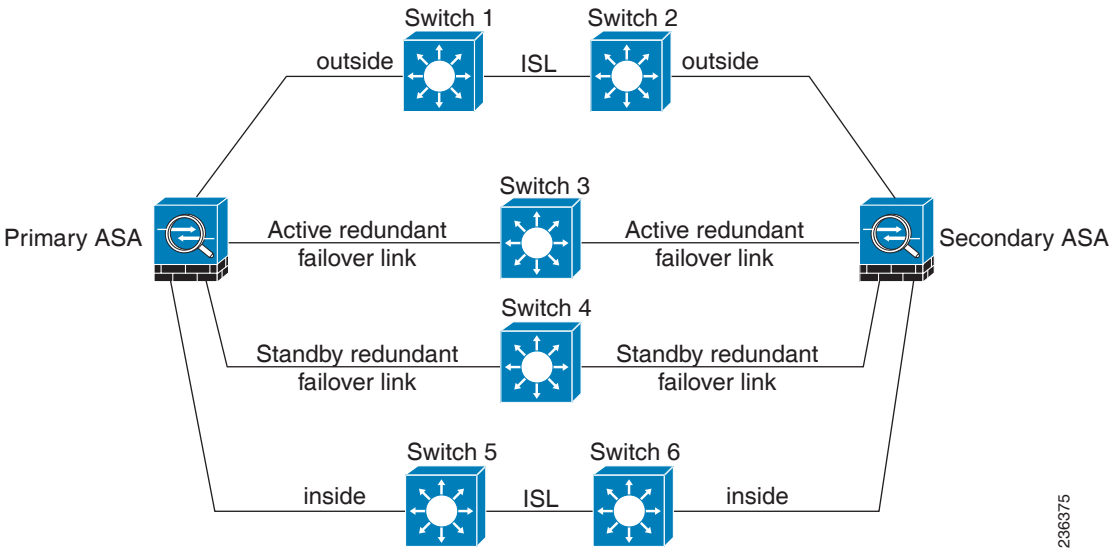
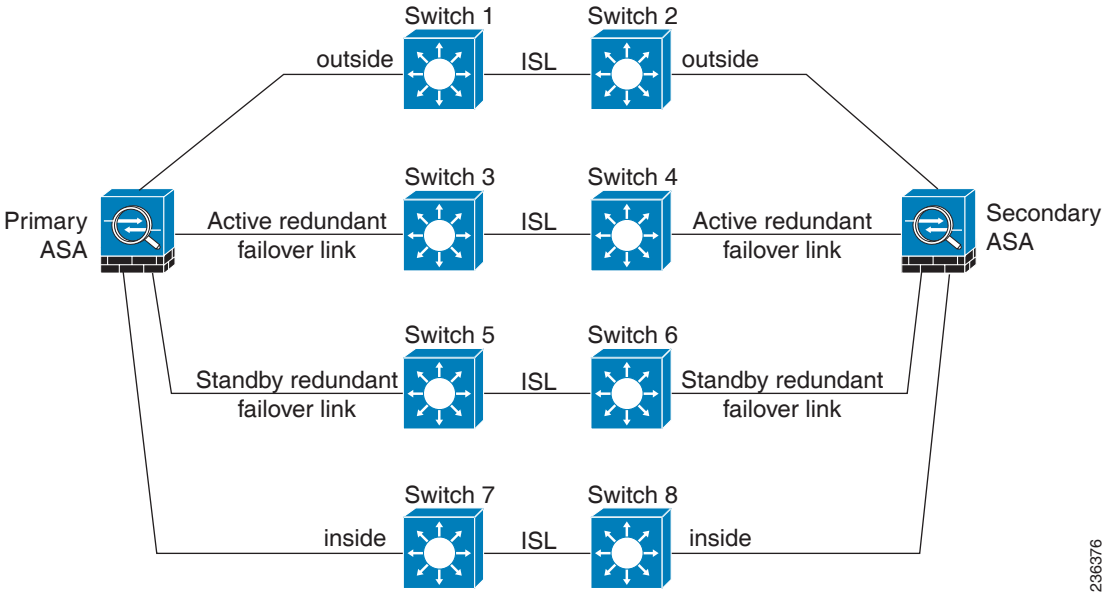


그림 7-7 스위치 간 링크로 연결



MAC 주소와 IP 주소

인터페이스를 구성할 경우, 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정해야 합니다.

1. 기본 유닛 또는 장애 조치 그룹에서 장애 조치를 시작할 경우, 보조 유닛에서는 기본 유닛의 IP 주소와 MAC 주소를 가정하고 트래픽 전달을 시작합니다.
2. 이제 스탠바이 상태가 된 유닛에서는 스탠바이 IP 주소와 MAC 주소를 인수합니다.

네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

참고 기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 그러나 기본 유닛이 사용 가능한 상태가 되면 보조(액티브) 유닛에서는 MAC 주소를 기본 유닛의 주소로 변경하므로 이 경우 네트워크 트래픽이 중단될 수 있습니다. 이와 마찬가지로 기본 유닛을 새 하드웨어로 교체할 경우에도 새로운 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. 다중 컨텍스트 모드의 경우 ASA에서는 기본적으로 가상 액티브 및 스탠바이 MAC 주소를 생성합니다. 자세한 내용은 6-11 페이지의 MAC 주소에 대한 정보를 참조하십시오. 단일 컨텍스트 모드에서는 가상 MAC 주소를 수동으로 구성할 수 있습니다. 자세한 내용은 7-30 페이지의 액티브/액티브 장애 조치 구성을 참조하십시오.

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.

참고 장애 조치 시 상태 링크의 IP 주소와 MAC 주소는 변경되지 않습니다. 유일한 예외는 상태 링크가 일반 데이터 인터페이스에서 구성된 경우입니다.

ASA Services Module을 위한 Intra-Chassis 및 Inter-Chassis 모듈 배치

기본 및 보조ASASM를 같은 스위치 또는 두 개의 개별 스위치 내에 배치할 수 있습니다. 다음 섹션에서는 각 옵션에 대해 설명합니다.

- 7-8 페이지의 Intra-Chassis 장애 조치
- 7-9 페이지의 Inter-Chassis 장애 조치

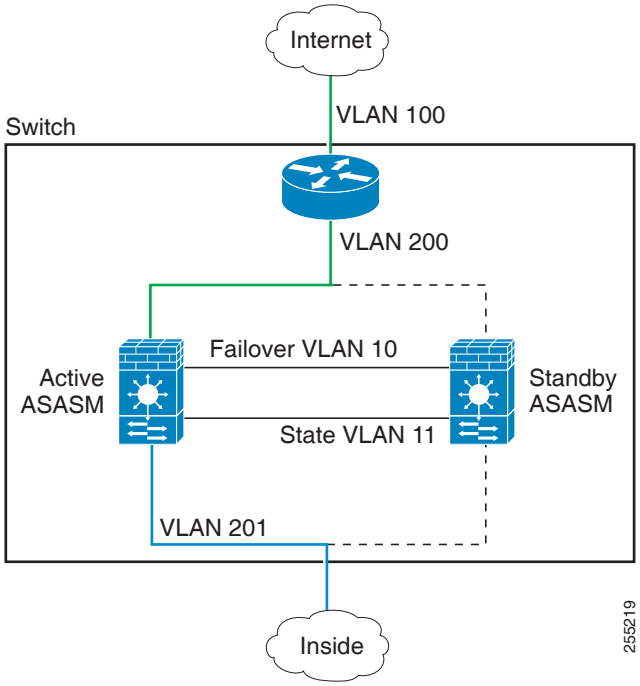
Intra-Chassis 장애 조치

기본 ASASM과 동일한 스위치에서 보조 ASASM을 설치할 경우 모듈 수준 오류를 방지할 수 있습니다. 모듈 수준 오류뿐만 아니라 스위치 수준 오류도 방지하려면 7-9 페이지의 Inter-Chassis 장애 조치를 참조하십시오.

두 ASASM이 모두 같은 VLAN에 할당된 경우에도 액티브 모듈만 네트워킹에 참여합니다. 스탠바이 모듈에서는 어떠한 트래픽도 전달하지 않습니다.

그림 7-8에는 Intra-Switch 컨피그레이션이 나와 있습니다.

그림 7-8 Intra-Switch 장애 조치



Inter-Chassis 장애 조치

스위치 수준 오류를 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.

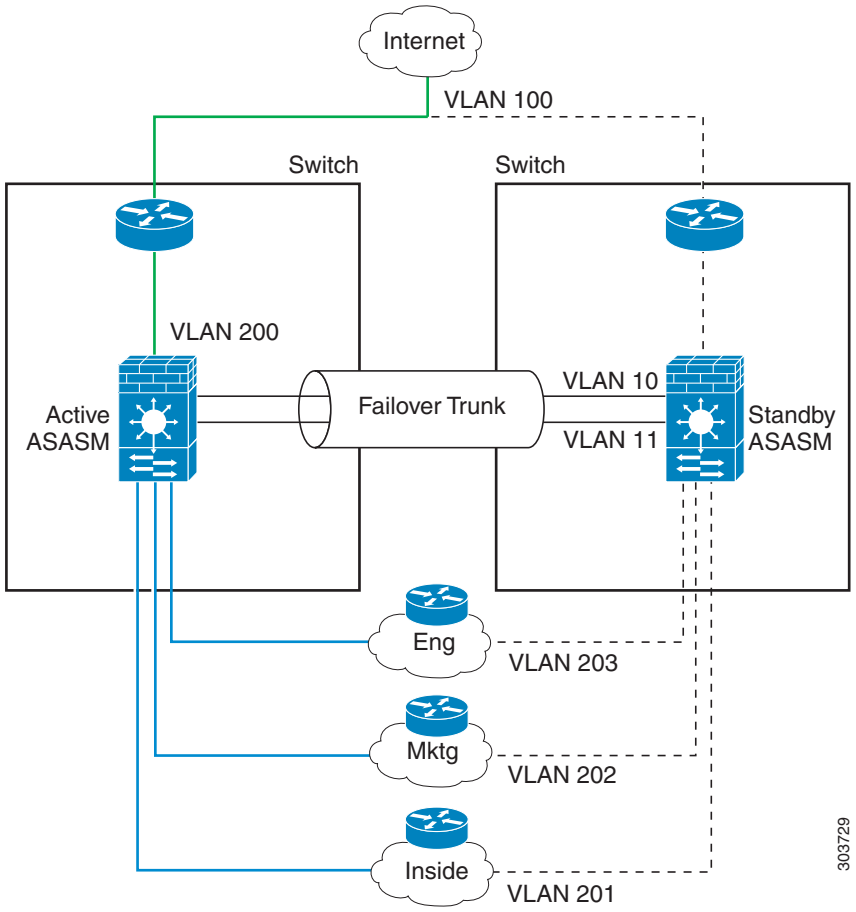
ASASM 간의 장애 조치 통신을 최대한 안정적으로 수행하려면 두 스위치 사이에 EtherChannel 트렁크 포트를 구성하여 장애 조치 및 상태 VLAN을 전송하는 것이 좋습니다.

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.

그림 7-9에는 일반적인 스위치 및 ASASM 이중화 컨피그레이션이 나와 있습니다. 두 스위치 간의 트렁크에서는 장애 조치 ASASM VLAN(VLAN 10 및 11)을 전송합니다.

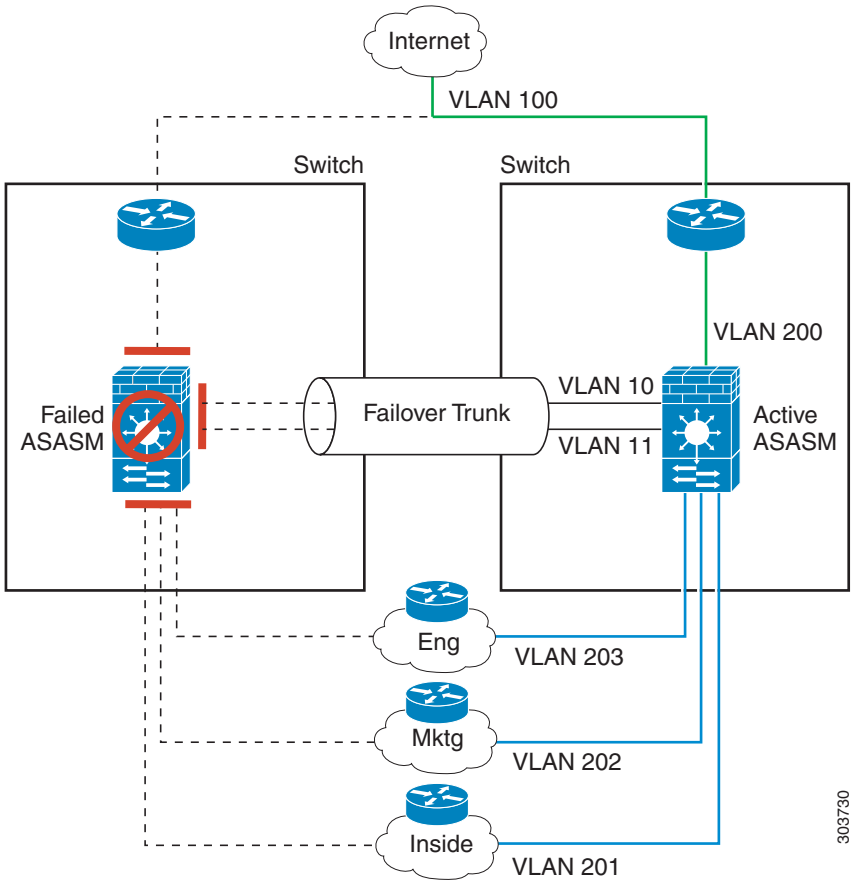
참고 ASASM 장애 조치는 스위치 장애 조치 작업과는 무관하지만, ASASM의 경우 모든 스위치 장애 조치 시나리오에서 작동합니다.

그림 7-9 정상 가동


Internet
VLAN 100
Switch
Switch
VLAN 200
Active
ASASM
Failover Trunk
VLAN 10
VLAN 11
Standby
ASASM
Eng
VLAN 203
Mktg
VLAN 202
Inside
VLAN 201
303729

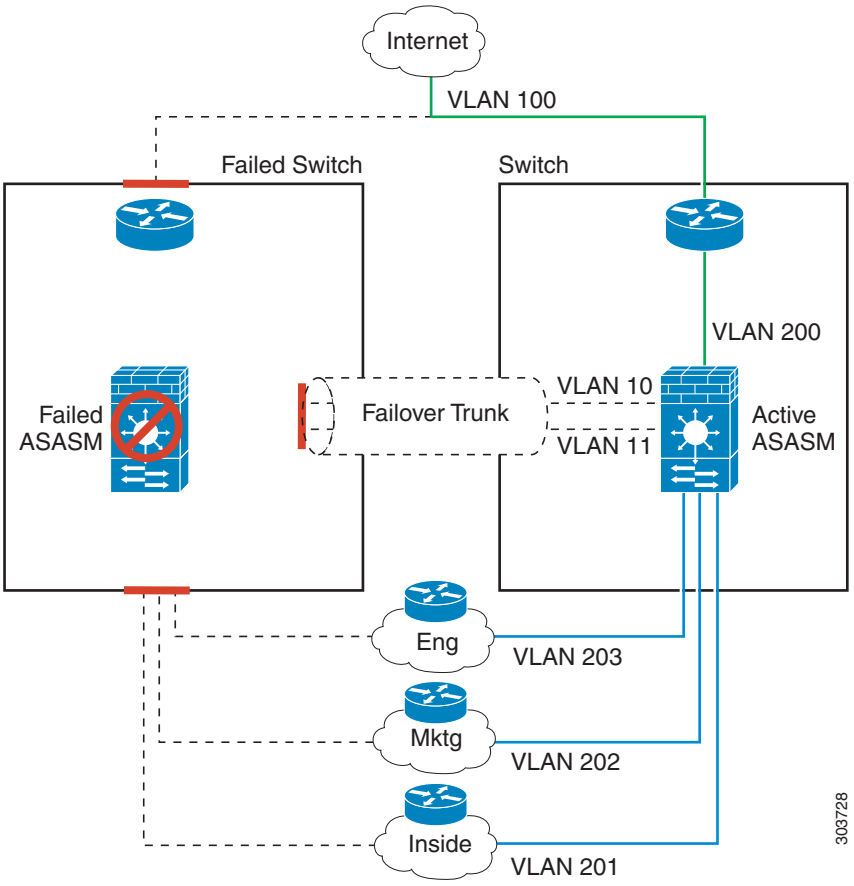
기본 ASASM에 오류가 발생하면 보조 ASASM이 액티브 상태가 되고 방화벽 VLAN을 올바르게 전달합니다(그림 7-10).

그림 7-10 ASASM 오류



ASASM을 비롯한 전체 스위치에 오류가 발생할 경우(예: 정전), 두 스위치 및 ASASM에서는 해당 보조 유닛으로 장애 조치를 시작합니다(그림 7-11).

그림 7-11 스위치 오류



스테이트리스 및 스테이트풀 장애 조치

ASA에서는 액티브/스탠바이 및 액티브/액티브 모드에 대해 두 가지 유형의 장애 조치(스테이트리스 및 스테이트풀)를 지원합니다.

- 7-13 페이지의 스테이트리스 장애 조치
- 7-13 페이지의 스테이트풀 장애 조치

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 장애 조치

스테이트풀 장애 조치를 활성화한 경우 액티브 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.

- 7-13 페이지의 지원 기능
- 7-14 페이지의 지원되지 않는 기능

지원 기능

스테이트풀 장애 조치가 활성화될 경우 다음 상태 정보가 스탠바이 ASA에 전달됩니다.

- NAT 변환 테이블
- TCP 연결 상태
- UDP 연결 상태
- ARP 테이블
- 레이어 2 브릿지 테이블(투명 방화벽 모드에서 실행 중일 경우)
- HTTP 연결 상태(HTTP 복제가 활성화된 경우) — 기본적으로 ASA에서는 스테이트풀 장애 조치가 활성화된 경우 HTTP 세션을 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.
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 신호 세션
- ICMP 연결 상태 — ICMP 연결 복제는 해당 인터페이스가 비대칭 라우팅 그룹에 할당된 경우에만 활성화됩니다.
- 동적 라우팅 프로토콜 — 스테이트풀 장애 조치는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 얻은 경로는 스탠바이 유닛의 RIB(라우팅 정보 베이스) 테이블에 유지됩니다. 장애 조치 이벤트 발생 시, 액티브 보조 ASA에서는 초기 규칙에 따라 기본 ASA를 미러링하므로 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 장애 조치가 끝난 직후에는 새로운 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.

- Cisco IP SoftPhone 세션 — 액티브 Cisco IP SoftPhone 세션 도중 장애 조치가 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.
- VPN — VPN 최종 사용자는 장애 조치 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 장애 조치 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.

지원되지 않는 기능

스테이트풀 장애 조치가 활성화될 경우 다음 상태 정보가 스탠바이 ASA에 전달되지 *않습니다*.

- HTTP 연결 케이블(HTTP 복제를 활성화지 않은 경우)
- 사용자 인증(uauth) 테이블
- 고급 TCP 상태 추적이 적용되는 애플리케이션 감시 — 이러한 연결의 TCP 상태는 자동으로 복제되지 않습니다. 이러한 연결이 스탠바이 유닛에 복제되는 동안 TCP 상태를 다시 설정하기 위한 최상의 시도가 이루어집니다.
- DHCP 서버 주소 리스
- ASA IPS SSP 또는 ASA CX SSP 같은 모듈의 상태 정보
- 전화 프록시 연결 — 액티브 유닛이 중단될 경우, 통화가 되지 않으며 미디어의 흐름이 중단됩니다. 오류가 발생한 유닛에서 해당 전화의 등록을 해제하고 액티브 유닛에 대한 등록도 취소해야 합니다. 통화를 다시 설정해야 합니다.
- 선택한 클라이언트 리스 SSL VPN 기능:
  - 스마트 터널
  - 포트 전달
  - 플러그인
  - Java 애플릿
  - IPv6 클라이언트리스 또는 AnyConnect 세션
  - Citrix 인증(Citrix 사용자는 장애 조치 후 다시 인증을 수행해야 함)

투명 방화벽 모드 요구 사항

- 7-15 페이지의 어플라이언스에 대한 투명 모드 요구 사항
- 7-15 페이지의 모듈의 투명 모드 요구 사항

어플라이언스에 대한 투명 모드 요구 사항

액티브 유닛에서 스탠바이 유닛으로 장애 조치를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30~50초 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 — EtherType 규칙이 있는 내부 및 외부 인터페이스에서 ASA의 BPDU를 차단합니다.

  ```
  access-list id ethertype deny bpdu
  access-group id in interface inside_name
  access-group id in interface outside_name
  ```

  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.

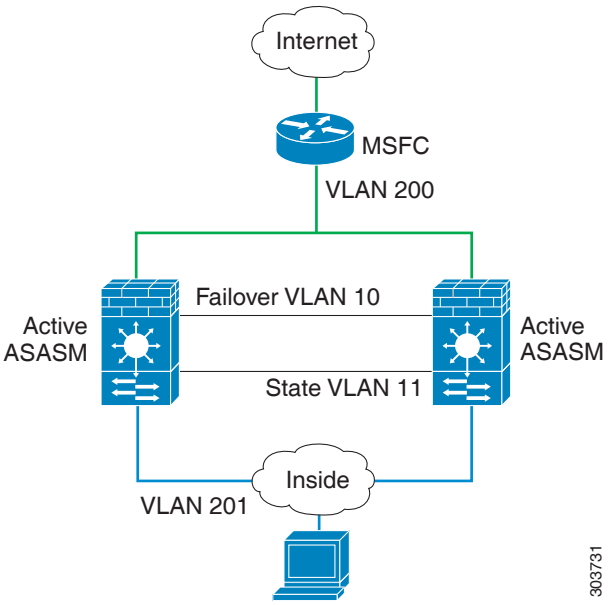
- 인터페이스 모니터링을 비활성화합니다.
- 인터페이스 대기 시간을 큰 값으로 늘려 ASA에서 장애 조치를 수행하기 전에 STP가 통합될 수 있도록 합니다.
- STP 타이머를 줄여 STP가 인터페이스 대기 시간보다 빨리 통합될 수 있도록 합니다.

모듈의 투명 모드 요구 사항

투명 모드에서 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 개의 VLAN 간의 패킷을 연결하므로, 외부로 전달되어야 할 내부 패킷이 ASASM에 의해 끊임없이 복제될 경우 루프가 발생할 수 있습니다(그림 7-12 참조). BPDU가 적시에 교환되는 경우 Spanning Tree Protocol에서는 이러한 루프를 끊을 수 있습니다. 루프를 끊으려면 VLAN 200과 VLAN 201 간에 전송된 BPDU를 연결해야 합니다.

그림 7-12 투명 모드 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.

- 7-16 페이지의 유닛 상태 모니터링
- 7-17 페이지의 인터페이스 모니터링

유닛 상태 모니터링

ASA에서는 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 인터페이스 hello 메시지를 전송하여 피어의 응답 여부를 확인합니다. 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. 장애 조치 링크가 실패한 것으로 표시됩니다. 장애 조치 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치할 수 없으므로 최대한 빨리 장애 조치 링크를 복원해야 합니다.
- ASA에서 인터페이스에 대한 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 실패한 것으로 분류합니다.

인터페이스 모니터링

최대 250개의 인터페이스를 모니터링할 수 있습니다(다중 모드에서 해당되며 모든 컨텍스트 간에 분할됨). 중요한 인터페이스를 모니터링해야 합니다. 예를 들어, 다중 모드에서는 하나의 컨텍스트를 구성하여 공유 인터페이스를 공유할 수 있습니다 (인터페이스가 공유되므로 모든 컨텍스트에서는 모니터링으로 인한 이점을 누릴 수 있습니다.).

구성된 대기 시간의 절반 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 다음과 같은 테스트가 실행됩니다.

1. 링크 작동/중단 테스트 — 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 작동 중인지 여부를 나타내며 ASA에서는 네트워크 테스트를 수행합니다. 이 테스트의 목적은 네트워크 트래픽을 생성하여 어떤 유닛에서 오류가 발생했는지 확인하는 것입니다. 각 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 각 테스트를 종료할 때마다 각 유닛에서는 수신된 트래픽이 있는지 확인합니다. 수신된 트래픽이 있는 경우 인터페이스가 제대로 작동 중인 것으로 간주합니다. 한 유닛에는 테스트용 트래픽이 수신되고 다른 유닛에는 수신되지 않을 경우, 트래픽이 수신되지 않은 유닛은 오류가 발생한 것으로 간주합니다. 모든 유닛에 트래픽이 수신되지 않을 경우 다음 테스트가 사용됩니다.
2. 네트워크 활동 테스트 — 수신된 네트워크 활동 테스트입니다. 유닛에서는 최대 5초 동안 수신된 모든 패킷의 수를 셉니다. 이 간격 동안 언제라도 수신된 패킷이 있을 경우 인터페이스가 작동 중인 것으로 간주되며 테스트가 중지됩니다. 트래픽이 수신되지 않으면 ARP 테스트가 시작됩니다.
3. ARP 테스트 — 가장 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 Ping 테스트가 시작됩니다.
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.

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown — 초기 상태입니다. 이 상태는 상태를 확인할 수 없다는 의미이기도 합니다.
- Normal — 인터페이스에서 트래픽을 수신 중입니다.
- Testing — 5번의 폴링 시간 동안 Hello 메시지가 인터페이스에서 수신되지 않습니다.
- Link Down — 인터페이스 또는 VLAN의 관리 상태가 중단되었습니다.
- No Link — 인터페이스의 물리적 링크가 중단되었습니다.
- Failed — 인터페이스에 트래픽이 수신되지 않았으나, 피어 인터페이스에는 트래픽이 수신되었습니다.

인터페이스에 구성된 IPv4 및 IPv6 주소가 없는 경우 ASA에서는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다.

인터페이스에 IPv6 주소만 구성된 경우 ASA에서는 ARP 대신 IPv6 인접 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 Ping 테스트의 경우 ASA에서는 IPv6의 모든 노드 주소를 사용합니다(FE02::1).

인터페이스에 대한 모든 네트워크 테스트가 실패하였으나 다른 유닛에 있는 이 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 제한에 대한 계산을 수행하지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 오류 임계값이 더 이상 충족되지 않을 경우 오류가 발생한 ASA는 스탠바이 모드로 돌아갑니다.

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.

장애 조치 시간

표 7-1에 최소, 기본 및 최대 장애 조치 시간이 나와 있습니다.

표 7-1 ASA 장애 조치 시간

장애 조치 상태	최소	기본	최대
액티브 유닛의 전원이 중단되거나 정상적인 작동이 중지됩니다.	800밀리초	15초	45초
액티브 유닛 메인 보드 인터페이스 링크가 중단됩니다.	500밀리초	5초	15초
액티브 유닛 4GE 모듈 인터페이스 링크가 중단됩니다.	2초	5초	15초
액티브 유닛 IPS 또는 CSC 모듈에 오류가 발생합니다.	2초	2초	2초
액티브 유닛 인터페이스가 작동되지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

컨피그레이션 동기화

장애 조치에는 2가지 유형의 컨피그레이션 동기화가 포함됩니다.

- 7-18 페이지의 실행 중인 컨피그레이션 복제
- 7-19 페이지의 명령 복제

실행 중인 컨피그레이션 복제

하나 또는 두 디바이스가 모두 장애 조치 쌍 부팅 중일 경우 실행 중인 컨피그레이션이 복제됩니다. 컨피그레이션은 액티브 유닛에서 스탠바이 유닛으로 항상 동기화됩니다. 스탠바이 유닛에서 초기 시작을 완료하면 실행 중인 컨피그레이션이 지워지며(장애 조치 명령과 액티브 유닛이 통신을 수행해야 하는 경우는 예외), 액티브 유닛에서는 전체 컨피그레이션을 스탠바이 유닛으로 보냅니다.

복제가 시작되면 액티브 유닛의 ASA 콘솔에는 "Beginning configuration replication: Sending to mate"는 메시지가 표시되며, 이 작업이 완료되면 ASA에서는 "End Configuration Replication to mate"라는 메시지를 표시합니다. 컨피그레이션의 크기에 따라 복제가 완료되기까지 몇 초에서 몇 분이 걸릴 수 있습니다.

스탠바이 유닛에서 컨피그레이션은 실행 중인 메모리에만 존재합니다. 2-16 페이지의 컨피그레이션 변경 사항 저장에 따라 컨피그레이션을 플래시 메모리에 저장해야 합니다.

참고 복제가 실행되는 동안 액티브 유닛에 입력된 명령은 스탠바이 유닛에 제대로 복제되지 않을 수 있으며, 스탠바이 유닛에 입력된 명령은 액티브 유닛에서 복제한 컨피그레이션으로 덮어쓰기 될 수 있습니다. 컨피그레이션 복제 프로세스가 진행되는 동안에는 유닛에 명령을 입력하지 마십시오.

참고 **crypto ca server** 명령 및 관련 하위 명령은 장애 조치 피어에 동기화되지 않습니다.

참고 컨피그레이션 동기화 시 다음 파일 및 컨피그레이션 요소는 복제되지 않으므로, 이러한 파일을 수동으로 복사하여 일치시켜야 합니다.

- AnyConnect 이미지
- CSD 이미지
- AnyConnect 프로파일
- 로컬 CA(Certificate Authority)
- ASA 이미지
- ASDM 이미지

명령 복제

시작 후 액티브 유닛에 입력하는 메시지는 스탠바이 유닛에 즉시 복제됩니다. 액티브 컨피그레이션을 플래시 메모리에 저장하여 명령을 복제하지 않아도 됩니다.

액티브/액티브 장애 조치의 경우, 시스템 에 입력된 명령 변경 사항은 유닛에서 활성 상태인 장애 조치 그룹 1로 복제됩니다.

명령 복제를 실행할 해당 유닛에 명령 을 입력하지 못할 경우 컨피그레이션이 동기화되지 않습니다. 이러한 변경 사항은 다음번에 초기 컨피그레이션 동기화가 실행될 때 손실될 수 있습니다.

다음 명령어는 스탠바이 ASA에 복제됩니다.

- **mode**, **firewall**, **failover lan unit**을 제외한 모든 컨피그레이션 명령
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

다음 명령어는 스탠바이 ASA에 복제되지 *않습니다*.

- **copy running-config startup-config**을 제외한 모든 형태의 **copy** 명령
- **write memory**를 제외한 모든 형태의 **write** 명령
- **debug**

- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** and **pager**

액티브/스탠바이 장애 조치

액티브/스탠바이 장애 조치에서는 스탠바이 ASA를 사용해 실패한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛이 실패하면 스탠바이 상태로 변경되며, 스탠바이 유닛은 액티브 상태로 변경됩니다.

참고 다중 컨텍스트 모드의 경우 ASA에서는 전체 유닛(모든 컨텍스트 포함)으로 장애 조치를 실행할 수 있으나 개별 컨텍스트를 대상으로 별도로 장애 조치를 수행할 수는 없습니다.

- 7-20 페이지의 기본/보조 역할 및 액티브/스탠바이 상태
- 7-20 페이지의 시작 시 액티브 유닛 결정
- 7-20 페이지의 장애 조치 이벤트

기본/보조 역할 및 액티브/스탠바이 상태

장애 조치 쌍에서 두 유닛 간의 주요 차이점은 어느 유닛이 액티브 유닛에 연결되어 있고 어느 유닛이 스탠바이 유닛에 연결되어 있는지와 관련이 있으며 즉, 다시 말해 어떤 IP 주소를 사용하고 어떤 유닛에서 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 장애 조치 링크를 통해 기본 유닛의 MAC 주소를 수신할 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.

장애 조치 이벤트

액티브/스탠바이 장애 조치 시 장애 조치는 유닛을 기준으로 실행됩니다. 다중 컨텍스트 모드에서 실행 중인 시스템에서도 개별 또는 컨텍스트 그룹으로는 장애 조치를 수행할 수 없습니다.

표 7-2에는 각 장애 조치 이벤트에 대한 장애 조치가 나와 있습니다. 이 표에는 각 장애 조치 이벤트에 적용되는 장애 조치 정책(장애 조치 실행 또는 장애 조치 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 장애 조치 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 7-2 장애 조치 동작

오류 이벤트	정책	액티브 조치	스탠바이 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	장애 조치	N/A	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 장애 조치 링크에 대한 hello 메시지가 수신되지 않음
이전 액티브 유닛 복구	장애 조치 없음	스탠바이 상태가 됨	조치 없음	없음
스탠바이 유닛 오류(전력 또는 하드웨어)	장애 조치 없음	스탠바이가 실패한 것으로 표시됨	N/A	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 장애 조치를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 장애 조치 링크에 오류 발생	장애 조치 없음	장애 조치 링크가 실패한 것으로 표시됨	장애 조치 링크가 실패한 것으로 표시됨	장애 조치가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치를 시작하지 못하므로 최대한 빨리 장애 조치 링크를 복구해야 합니다.
시작 시 장애 조치 링크에 오류 발생	장애 조치 없음	장애 조치 링크가 실패한 것으로 표시됨	액티브 상태가 됨	시작 시 장애 조치 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	장애 조치 없음	조치 없음	조치 없음	장애 조치가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	장애 조치	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	장애 조치 없음	조치 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 장애 조치를 시도하지 않으며 인터페이스 장애 조치 임계값을 넘은 경우에도 마찬가지입니다.

액티브/액티브 장애 조치 정보

이 섹션에서는 액티브/액티브 장애 조치에 대해 설명합니다.

액티브/액티브 장애 조치 개요

액티브/액티브 장애 조치 컨피그레이션에서는 두 ASA에서 모두 네트워크 트래픽을 전달할 수 있습니다. 액티브/액티브 장애 조치는 다중 컨텍스트 모드의 ASA에만 사용할 수 있습니다. 액티브/액티브 장애 조치에서 ASA의 보안 컨텍스트는 최대 2개의 장애 조치 그룹으로 나뉩니다.

장애 조치 그룹은 단순히 하나 이상의 보안 컨텍스트로 구성된 논리적 그룹입니다. 기본 ASA에서 액티브 상태가 되는 장애 조치 그룹 1을 할당하고 보조 ASA에서 액티브 상태가 되는 장애 조치 그룹 2를 할당할 수 있습니다. 장애 조치는 장애 조치 그룹 수준에서 수행됩니다. 예를 들어, 인터페이스 오류 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 컨텍스트는 항상 장애 조치 그룹 1의 멤버입니다. 또한 할당되지 않은 모든 보안 컨텍스트도 기본적으로 장애 조치 그룹 1의 멤버입니다. 액티브/액티브 장애 조치만 수행하고 다중 컨텍스트는 사용하지 않으려는 경우, 가장 간단한 컨피그레이션 방법은 추가 컨텍스트 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 액티브/스탠바이 상태

액티브/스탠바이 장애 조치와 마찬가지로, 액티브/액티브 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 구성됩니다.

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

- 두 유닛이 동시에 부팅될 때, 컨피그레이션 동기화 후 각 장애 조치 그룹이 기본 유닛에서 액티브 상태가 된 경우

장애 조치 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 컨텍스트를 포함할 수 있고 각 컨텍스트에는 여러 인터페이스가 포함될 수 있으므로, 관련된 장애 조치 그룹에 오류가 발생하는 대신 단일 컨텍스트 내의 모든 인터페이스에 오류가 발생할 수 있습니다.

표 7-3에는 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 7-3 액티브/액티브 장애 조치에 대한 장애 조치 동작

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	조치 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.
이전 액티브 장애 조치 그룹 복구	장애 조치 없음	조치 없음	조치 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	장애 조치 없음	조치 없음	조치 없음	장애 조치가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
작동 중 장애 조치 링크에 오류 발생	장애 조치 없음	N/A	N/A	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

액티브/스탠바이 장애 조치

모델	라이센싱 요구 사항
ASA 5512-X	Security Plus 라이센스
ASAv	Standard 및 Premium 라이센스
기타 모델	Base 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. 이러한 규칙의 예외 사항은 다음과 같습니다.

- 5512-X용 Security Plus 라이센스 — Base 라이센스에서는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 사용할 수 없습니다.
- 암호화 라이센스 — 두 유닛에는 모두 동일한 암호화 라이센스가 있어야 합니다.
- ASA 5555-X를 통한 ASA 5512-X용 IPS 모듈 — 두 유닛에는 모두 IPS 모듈 라이센스가 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 라이센스가 아니므로 장애 조치에서 공유되지 않습니다.
  - IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
- ASAv 가상 CPU — 장애 조치를 구축할 경우 기본 유닛과 동일한 수의 vCPU가 스탠바이 유닛에 할당되어 있는지 확인하십시오(vCPU 라이센스 일치 여부도 함께 확인).

액티브/액티브 장애 조치

모델	라이센싱 요구 사항
ASA 5512-X	Security Plus 라이센스
ASAv	지원 안 함
기타 모델	Base 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. 이러한 규칙의 예외 사항은 다음과 같습니다.

- 5512-X용 Security Plus 라이센스 — Base 라이센스에서는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 사용할 수 없습니다.
- 암호화 라이센스 — 두 유닛에는 모두 동일한 암호화 라이센스가 있어야 합니다.

- ASA 5555-X를 통한 ASA 5512-X용 IPS 모듈 — 두 유닛에는 모두 IPS 모듈 라이센스가 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 라이센스가 아니므로 장애 조치에서 공유되지 않습니다.
  - IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
- ASAv 가상 CPU — 장애 조치를 구축할 경우 기본 유닛과 동일한 수의 vCPU가 스탠바이 유닛에 할당되어 있는지 확인하십시오(vCPU 라이센스 일치 여부도 함께 확인).

장애 조치 사전 요구 사항

7-2 페이지의 장애 조치 시스템 요구 사항을 참조하십시오.

장애 조치 지침

컨텍스트 모드 지침

- 액티브/스탠바이 모드는 단일 및 다중 컨텍스트 모드에서 지원됩니다.
- 액티브/액티브 모드는 다중 컨텍스트 모드에서만 지원됩니다.
- 다중 컨텍스트 모드의 경우, 달리 명시되지 않는 한 모든 단계가 시스템 실행 영역에서 수행됩니다.
- 둘 이상의 컨텍스트에서 컨피그레이션을 동시에 변경하려고 할 경우 ASA 장애 조치 복제가 실패합니다. 해결 방법은 각 컨텍스트에서 순차적으로 컨피그레이션을 변경하는 것입니다.

추가 지침 및 제한

- 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 컨텍스트 전반에 걸쳐 최대 250개의 인터페이스를 모니터링할 수 있습니다.
- 액티브/액티브 장애 조치의 경우 같은 ASR 그룹의 같은 컨텍스트에서 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 컨텍스트가 항상 포함됩니다. 장애 조치 그룹에 할당되지 않은 모든 컨텍스트는 장애 조치 그룹 1에 기본 설정됩니다. 컨텍스트가 명시적으로 할당된 장애 조치 그룹은 제거할 수 없습니다.

관련 주제

- 36-35 페이지의 장애 조치 컨피그레이션에서 자동 업데이트 서버 지원

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 다중 컨텍스트 모드에서 활성화됨. 단일 컨텍스트 모드에서는 가상 MAC 주소가 비활성화됨
- 모든 물리적 인터페이스 또는 ASASM, 모든 VLAN 인터페이스에 대한 모니터링

액티브/스탠바이 장애 조치 구성

- 7-26 페이지의 액티브/스탠바이 장애 조치를 위한 기본 유닛 구성
- 7-29 페이지의 액티브/스탠바이 장애 조치를 위한 보조 유닛 구성

액티브/스탠바이 장애 조치를 위한 기본 유닛 구성

이 섹션의 단계에 따라 액티브/스탠바이 장애 조치 컨피그레이션에서 기본 유닛을 구성하십시오. 이러한 단계에서는 기본 유닛에서 장애 조치를 사용하는 데 필요한 최소 컨피그레이션을 제공합니다.

시작하기 전에

- 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 장애 조치 및 상태 링크를 제외한 모든 인터페이스에 사용할 스탠바이 IP 주소를 구성합니다.
- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

절차

1단계 이 유닛을 기본 유닛으로 지정합니다.

```
failover lan unit primary
```

2단계 장애 조치 링크로 사용할 인터페이스를 지정합니다.

```
failover lan interface if_name interface_id
```

예:

```
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, 이중화 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

패킷의 오류를 방지하기 위해 EtherChannel를 장애 조치 또는 상태 링크로 사용할 수는 있지만, EtherChannel에는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

3단계 액티브 및 스탠바이 IP 주소를 장애 조치 링크에 할당합니다.

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

예:

```
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.

스탠바이 IP 주소는 액티브 IP 주소와 동일한 서브넷에 있어야 합니다.

4단계 장애 조치 링크를 활성화합니다.

interface *failover_interface_id*
  no shutdown

예:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

5단계 (선택 사항) 상태 링크로 사용하려는 인터페이스를 지정합니다.

failover link *if_name interface_id*

예:

```
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, 이중화 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

패킷의 오류를 방지하기 위해 EtherChannel를 장애 조치 또는 상태 링크로 사용할 수는 있지만, EtherChannel에는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

6단계 별도의 상태 링크를 지정한 경우 상태 링크에 액티브 및 스탠바이 IP 주소를 할당합니다.

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address/prefix*} **standby** *ip_address*

예:

```
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.

스탠바이 IP 주소는 액티브 IP 주소와 동일한 서브넷에 있어야 합니다.

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

7단계 별도의 상태 링크를 지정한 경우 해당 상태 링크를 사용합니다.

interface *state_interface_id*
no shutdown

예:

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

8단계 (선택 사항) 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
  ```

  *키*의 최대 길이는 128자입니다. 두 유닛의 동일한 키를 식별합니다. IKEv2에서는 이 키를 사용하여 터널을 설정합니다.

  마스터 암호(13-10 페이지의 마스터 패스프레이즈 구성 참조)를 사용할 경우 컨피그레이션에서 키가 암호화됩니다. 컨피그레이션에서(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(컨피그레이션의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

  IPsec 암호화 및 레거시 **failover key** 암호화를 함께 사용할 수 없습니다. 두 방법을 모두 구성할 경우 IPsec가 사용됩니다. 그러나 마스터 암호(13-10 페이지의 마스터 패스프레이즈 구성 참조)를 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.

- (선택 사항) 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 암호(13-10 페이지의 마스터 패스프레이즈 구성 참조)를 사용할 경우 컨피그레이션에서 공유 비밀 또는 16진수 키가 암호화됩니다. 컨피그레이션에서(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(컨피그레이션의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

9단계 장애 조치를 사용하도록 설정합니다.

failover

10단계 플래시 메모리에 시스템 컨피그레이션을 저장합니다.

write memory

예

다음 예에서는 기본 유닛의 장애 조치 매개변수를 구성합니다.

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover ipsec pre-shared-key a3rynsun
failover
```

액티브/스탠바이 장애 조치를 위한 보조 유닛 구성

보조 유닛에 필요한 유일한 컨피그레이션은 장애 조치 링크에 대한 컨피그레이션입니다. 보조 유닛에서 기본 유닛과 처음 통신을 수행하려면 이러한 명령이 필요합니다. 기본 유닛에서 해당 컨피그레이션을 보조 유닛으로 전송하면, 두 컨피그레이션 간의 유일한 영구적인 차이점은 **failover lan unit** 명령이며 이 명령은 각 유닛을 기본 또는 보조 유닛으로 식별합니다.

시작하기 전에

- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

절차

1단계 **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. 7-26 페이지의 액티브/스탠바이 장애 조치를 위한 기본 유닛 구성을 참조하십시오.

예:

```
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
```

2단계 장애 조치 컨피그레이션을 동기화한 후 컨피그레이션을 플래시 메모리에 저장합니다.

```
ciscoasa(config)# write memory
```

액티브/액티브 장애 조치 구성

액티브/액티브 장애 조치를 위한 기본 유닛 구성

이 섹션의 단계에 따라 액티브/액티브 장애 조치 컨피그레이션에서 기본 유닛을 구성하십시오. 이러한 단계에서는 기본 유닛에서 장애 조치를 사용하는 데 필요한 최소 컨피그레이션을 제공합니다.

시작하기 전에

- 6-15 페이지의 다중 컨텍스트 모드 활성화 또는 비활성화에 따라 다중 컨텍스트 모드를 활성화합니다.
- 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 장애 조치 및 상태 링크를 제외한 모든 인터페이스에 사용할 스탠바이 IP 주소를 구성합니다.
- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 시스템 실행 영역에서 이 절차를 완료합니다. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

절차

1단계 이 유닛을 기본 유닛으로 지정합니다.

```
failover lan unit primary
```

2단계 장애 조치 링크로 사용할 인터페이스를 지정합니다.

```
failover lan interface if_name interface_id
```

예:

```
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, 이중화 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

패킷의 오류를 방지하기 위해 EtherChannel를 장애 조치 또는 상태 링크로 사용할 수는 있지만, EtherChannel에는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

3단계 액티브 및 스탠바이 IP 주소를 장애 조치 링크에 할당합니다.

```
failover interface ip if_name {ip_address mask | ipv6_address/prefix} standby ip_address
```

예:

```
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.

스탠바이 IP 주소는 액티브 IP 주소와 동일한 서브넷에 있어야 합니다.

4단계 장애 조치 링크를 활성화합니다.

```
interface failover_interface_id
  no shutdown
```

예:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

5단계 (선택 사항) 상태 링크로 사용하려는 인터페이스를 지정합니다.

```
failover link if_name interface_id
```

예:

```
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, 이중화 인터페이스 또는 EtherChannel 인터페이스 ID가 될 수 있습니다. ASASM에서 *interface_id*는 VLAN ID를 지정합니다.

패킷의 오류를 방지하기 위해 EtherChannel를 장애 조치 또는 상태 링크로 사용할 수는 있지만, EtherChannel에는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

6단계 별도의 상태 링크를 지정한 경우 상태 링크에 액티브 및 스탠바이 IP 주소를 할당합니다.

이 주소는 장애 조치 링크와 다른 사용되지 않는 서브넷에 있어야 합니다.

스탠바이 IP 주소는 액티브 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*

예:

```
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
```

7단계 별도의 상태 링크를 지정한 경우 해당 상태 링크를 사용합니다.

interface *state_interface_id*
  no shutdown

예:

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

상태 링크를 공유 중인 경우 이 단계를 건너뜁니다.

8단계 (선택 사항) 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
  ```

  *키*의 최대 길이는 128자입니다. 두 유닛의 동일한 키를 식별합니다. IKEv2에서는 이 키를 사용하여 터널을 설정합니다.

  마스터 암호(13-10 페이지의 마스터 패스프레이즈 구성 참조)를 사용할 경우 컨피그레이션에서 키가 암호화됩니다. 컨피그레이션에서(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(컨피그레이션의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

  IPsec 암호화 및 레거시 **failover key** 암호화를 함께 사용할 수 없습니다. 두 방법을 모두 구성할 경우 IPsec가 사용됩니다. 그러나 마스터 암호(13-10 페이지의 마스터 패스프레이즈 구성 참조)를 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.

- (선택 사항) 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 암호(13-10 페이지의 마스터 패스프레이즈 구성 참조)를 사용할 경우 컨피그레이션에서 공유 비밀 또는 16진수 키가 암호화됩니다. 컨피그레이션에서(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(컨피그레이션의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

9단계 장애 조치 그룹 1을 생성합니다.

failover group 1

기본적으로 이 그룹은 기본 유닛에 할당됩니다. 일반적으로 그룹 1은 기본 유닛에 할당하고 그룹 2는 보조 유닛에 할당합니다. 비표준 컨피그레이션을 사용하려면 필요한 경우 **primary** 또는 **secondary** 하위 명령을 사용하여 다른 유닛 기본 설정을 지정할 수 있습니다.

10단계 장애 조치 그룹 2를 생성하고 이를 보조 유닛에 할당합니다.

```
failover group 2
  secondary
```

11단계 제공된 컨텍스트에 대한 컨텍스트 컨피그레이션 모드로 들어간 다음 장애 조치 그룹에 컨텍스트를 할당합니다.

context *name*
  join-failover-group {**1** | **2**}

예:

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

각 컨텍스트에 이 명령을 반복합니다.

할당되지 않은 모든 컨텍스트는 장애 조치 그룹 1에 자동으로 할당됩니다. 관리자 컨텍스트는 항상 장애 조치 그룹 1의 멤버이며 이를 그룹 2에 할당할 수 없습니다.

12단계 장애 조치를 사용하도록 설정합니다.

failover

13단계 플래시 메모리에 시스템 컨피그레이션을 저장합니다.

write memory

예

다음 예에서는 기본 유닛의 장애 조치 매개변수를 구성합니다.

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover group 1
failover group 2
  secondary
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

액티브/액티브 장애 조치를 위한 보조 유닛 구성

보조 유닛에 필요한 유일한 컨피그레이션은 장애 조치 링크에 대한 컨피그레이션입니다. 보조 유닛에서 기본 유닛과 처음 통신을 수행하려면 이러한 명령이 필요합니다. 기본 유닛에서 해당 컨피그레이션을 보조 유닛으로 전송하면, 두 컨피그레이션 간의 유일한 영구적인 차이점은 **failover lan unit** 명령이며 이 명령은 각 유닛을 기본 또는 보조 유닛으로 식별합니다.

시작하기 전에

- 6-15 페이지의 다중 컨텍스트 모드 활성화 또는 비활성화에 따라 다중 컨텍스트 모드를 활성화합니다.
- 장애 조치 및 상태 링크에 **nameif**를 구성하지 마십시오.
- 시스템 실행 영역에서 이 절차를 완료합니다. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

절차

1단계 **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. 7-30 페이지의 액티브/액티브 장애 조치를 위한 기본 유닛 구성을 참조하십시오.

예:

```
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
```

2단계 기본 유닛에서 장애 조치 컨피그레이션을 동기화한 후 컨피그레이션을 플래시 메모리에 저장합니다.

```
ciscoasa(config)# write memory
```

3단계 필요한 경우, 장애 조치 그룹 2가 보조 유닛에서 액티브 상태가 되도록 강제 설정합니다.

```
failover active group 2
```

선택적 장애 조치 매개변수 구성

원하는 경우 장애 조치 설정을 맞춤화할 수 있습니다.

- 7-35 페이지의 장애 조치 기준 구성, HTTP 복제, 그룹 사전 대응 방식, MAC 주소
- 7-38 페이지의 인터페이스 모니터링 및
- 7-38 페이지의 비대칭 라우팅 패킷을 위한 지원 구성(액티브/액티브 모드)

장애 조치 기준 구성, HTTP 복제, 그룹 사전 대응 방식, MAC 주소

이 섹션에서 변경할 수 있는 다양한 매개변수에 대한 기본 설정은 7-26 페이지의 장애 조치 기본값을 참조하십시오. 액티브/액티브 모드에서는 장애 조치 그룹당 가장 많은 기준을 설정합니다.

시작하기 전에

다중 컨텍스트 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

절차

1단계 유닛 폴링 및 대기 시간을 변경합니다.

액티브/액티브 모드에서 시스템에 대한 이러한 속도를 설정합니다. 이러한 속도는 장애 조치 그룹당 설정할 수 없습니다.

대기 시간은 유닛 폴링 시간보다 3배 적게 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.

한 차례의 폴링 기간 동안 장애 조치 통신 인터페이스에 대한 hello 패킷이 유닛에 수신되지 않을 경우, 나머지 인터페이스 전체에 추가 테스트가 이루어집니다. 대기 시간 동안에도 피어 유닛에서 여전히 응답이 없을 경우 해당 유닛에 오류가 발생한 것으로 간주하며, 오류가 발생한 유닛이 액티브 유닛인 경우 스탠바이 유닛이 액티브 유닛으로 인계됩니다.

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

예:

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

2단계 초당 연결의 HTTP 복제 속도를 설정합니다.

속도의 범위는 8341~50000 내에서 설정합니다. 기본값은 50000입니다. 액티브/액티브 모드에서 시스템에 대한 이러한 속도를 설정합니다. 이러한 속도는 장애 조치 그룹당 설정할 수 없습니다.

failover replication rate *conns*

예:

```
ciscoasa(config)# failover replication rate 20000
```

3단계 (액티브/액티브 모드에만 해당) 맞춤화하려는 장애 조치 그룹을 지정합니다.

failover group {**1** | **2**}

예:

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

4단계 (액티브/액티브 모드에만 해당) 장애 조치 그룹 1에 대한 장애 조치 사전 대응 방식을 구성합니다.

preempt [*delay*]

예:

```
ciscoasa(config-fover-group)# preempt 1200
```

한 유닛이 다른 유닛보다 먼저 부팅될 경우, 기본 또는 보조 설정에 관계없이 두 장애 조치 그룹 모두 해당 유닛에서 액티브 상태가 됩니다. 이 명령을 사용하면 유닛이 사용 가능한 상태가 되었을 때 지정된 유닛에서 장애 조치 그룹이 자동으로 액티브 상태가 됩니다.

선택적인 *지연* 값을 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. 올바른 값의 범위는 1부터 1200까지입니다.

스테이트풀 장애 조치를 사용할 경우, 장애 조치 그룹이 현재 액티브 상태로 있는 유닛에서 연결이 복제될 때까지 사전 대응이 지연됩니다.

5단계 HTTP 상태 복제를 사용하도록 설정합니다.

- 액티브/스탠바이 모드의 경우:

  failover replication http

- 액티브/액티브 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.

6단계 인터페이스에 오류가 발생할 경우에 대한 장애 조치의 임계값을 설정합니다.

- 액티브/스탠바이 모드의 경우:

  failover interface-policy *num*[%]

  예:

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- 액티브/액티브 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 250까지입니다.

인터페이스의 백분율을 지정할 경우, *num* 인수의 지원되는 범위는 1에서 100까지입니다.

7단계 인터페이스 폴링 및 대기 시간을 변경합니다.

- 액티브/스탠바이 모드의 경우:

  failover polltime interface [**msec**] *time* [**holdtime** *time*]

  예:

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- 액티브/액티브 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. 선택적 **msec** 키워드가 사용될 경우, 범위는 500~999밀리초입니다. 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 스탠바이 유닛이 액티브 상태가 됩니다.

8단계 인터페이스에 가상 MAC 주소를 구성합니다.

- 액티브/스탠바이 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
  ```

- 액티브/액티브 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 gigabitethernet0/1 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.

9단계 (액티브/액티브 모드에만 해당) 필요한 경우 다른 장애 조치 그룹에 이 절차를 반복합니다.

인터페이스 모니터링 및

기본적으로 모니터링은 모든 물리적 인터페이스 또는 ASASM, 모든 VLAN 인터페이스, ASA에 설치된 모든 하드웨어 모듈에서 사용됩니다. 중요도가 낮은 네트워크에 연결된 인터페이스를 제외하여 장애 조치 정책에 영향을 미치지 않도록 하고자 할 수 있습니다.

시작하기 전에

- 한 유닛에서 최대 250개의 인터페이스를 모니터링할 수 있습니다(다중 컨텍스트 모드의 전체 컨텍스트 전반에 걸쳐).
- 다중 컨텍스트 모드에서 각 컨텍스트 내에 인터페이스를 구성합니다.

절차

1단계 인터페이스에 대한 상태 모니터링을 활성화하거나 비활성화합니다.

[**no**] **monitor-interface** {*if_name* | **service-module**}

예:

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

ASA FirePOWER 모듈 같은 하드웨어 모듈 오류로 인해 장애 조치가 일어나지 않도록 하려는 경우 **no monitor-interface service-module** 명령을 사용하여 모듈 모니터링을 비활성화할 수 있습니다.

비대칭 라우팅 패킷을 위한 지원 구성(액티브/액티브 모드)

액티브/액티브 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 액티브 컨텍스트 외부 인터페이스를 할당하고, 보조 유닛에서는 동일한 ASR 그룹 1에 액티브 컨텍스트 외부 인터페이스를 할당합니다. 기본 유닛의 외부 인터페이스에 세션 정보가 없는 패킷이 수신될 경우, 동일한 그룹(이 경우에는 ASR 그룹 1)에 있는 스탠바이 컨텍스트의 다른 인터페이스에 대한 세션 정보를 검사합니다. 일치하는 정보가 없을 경우 해당 패킷은 손실됩니다. 일치하는 정보가 있을 경우 다음 작업 중 하나가 실행됩니다.

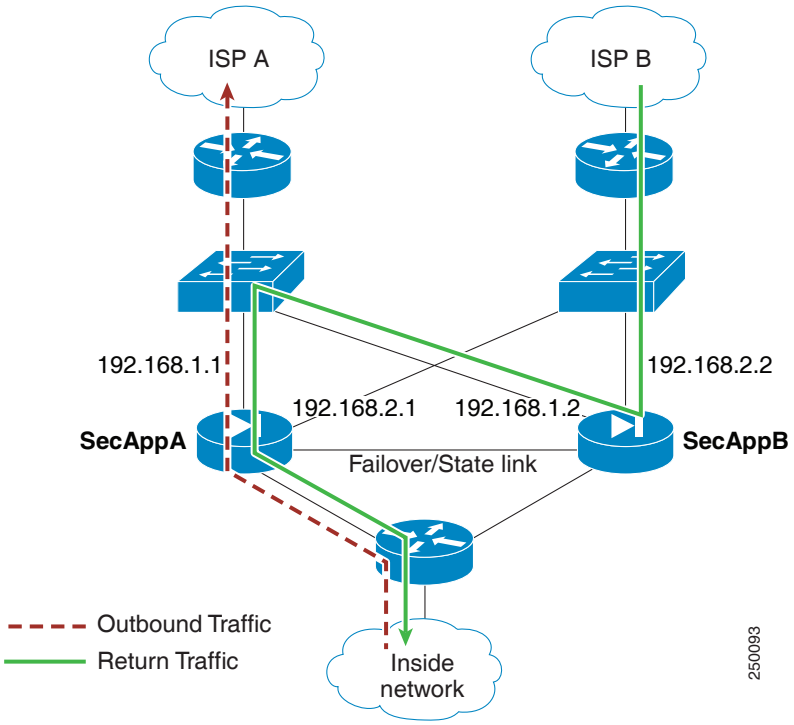
- 수신 트래픽이 피어 유닛에서 시작된 경우, 레이어 2 헤더의 일부 또는 전체가 다시 작성되고 패킷이 다른 유닛에 리디렉션됩니다. 이러한 리디렉션은 세션이 활성화되어 있는 동안 지속합니다.

- 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.

그림 7-13에는 비대칭 라우팅 패킷의 예가 나와 있습니다.

그림 7-13 ASR 예



1. 아웃바운드 세션이 액티브 SecAppA 컨텍스트가 포함된 ASA를 통해 전달됩니다. 이 컨텍스트는 outsideISP-A(192.168.1.1)에 있습니다.
2. 비대칭 라우팅이 업스트림에서 구성되었으므로, 액티브 SecAppB 컨텍스트가 포함된 ASA를 통해 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.

전제 조건

- 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 액티브 컨텍스트에서 이 절차를 수행합니다.

세부 단계

	명령	목적
1단계	기본 유닛의 경우: **interface** *phy_if* **예:** `primary/admin(config)# interface gigabitethernet 0/0`	비대칭 라우팅 패킷을 사용하려는 기본 유닛에서 인터페이스를 지정합니다.
2단계	**asr-group** *num* **예:** `primary/admin(config-ifc)# asr-group 1`	인터페이스에 대한 ASR 그룹 번호를 설정합니다. *num* 범위의 올바른 값은 1~32입니다.
3단계	보조 유닛의 경우: **interface** *phy_if* **예:** `secondary/ctx1(config)# interface gigabitethernet 0/1`	비대칭 라우팅 패킷을 사용하려는 보조 유닛에서 유사한 인터페이스를 지정합니다.
4단계	**asr-group** *num* **예:** `secondary/ctx1(config-ifc)# asr-group 1`	인터페이스의 ASR 그룹 번호를 기본 유닛 인터페이스와 일치하도록 설정합니다.

예

두 개의 유닛에 다음과 같은 컨피그레이션이 포함됩니다(컨피그레이션에는 관련 명령만 표시됨). 다이어그램에 SecAppA로 표시된 디바이스는 장애 조치 쌍의 기본 유닛입니다.

예 7-1 기본 유닛 시스템 컨피그레이션

```
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
```

예 7-2 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
```

예 7-3 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

장애 조치 강제 실행

스탠바이 유닛을 강제로 액티브 유닛으로 만들려면 다음 절차를 수행합니다.

전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

명령	목적
스탠바이 유닛에서 액티브/스탠바이 모드의 경우: **failover active** 스탠바이 유닛에서 액티브/액티브 모드의 경우: **failover active** [**group** *group_id*] **예:** `standby# failover active` 또는: `standby# failover active group 1`	*standby* 유닛이 되면 장애 조치를 강제로 실행합니다. 스탠바이 유닛이 액티브 유닛이 됩니다. **group** *group_id*를 지정하면 이 명령에서는 지정된 액티브/액티브 장애 조치 그룹이 *standby* 유닛이 될 때 장애 조치를 강제로 실행합니다. 스탠바이 유닛은 장애 조치 그룹의 액티브 유닛이 됩니다.
액티브 유닛에서 액티브/스탠바이 모드의 경우: **no failover active** 액티브 유닛에서 액티브/액티브 모드의 경우: **no failover active** [**group** *group_id*] **예:** `active# no failover active` 또는: `active# no failover active group 1`	*액티브* 유닛이 되면 장애 조치를 강제로 실행합니다. 액티브 유닛은 스탠바이 유닛이 됩니다. **group** *group_id*를 지정하면 이 명령에서는 지정된 장애 조치 그룹이 *active* 유닛이 될 때 장애 조치를 강제로 실행합니다. 액티브 유닛은 장애 조치 그룹의 스탠바이 유닛이 됩니다.

장애 조치 비활성화

장애 조치를 비활성화하려면 다음 절차를 수행 합니다.

전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

명령	목적
no failover **예:** `ciscoasa(config)# no failover`	장애 조치를 비활성화합니다. 액티브/스탠바이 쌍의 장애 조치를 비활성화하면 사용자가 다시 로드하기 전까지는 각 유닛의 액티브 및 스탠바이 상태가 유지됩니다. 예를 들어, 스탠바이 유닛은 스탠바이 모드에서 유지되므로 두 유닛에서는 모두 트래픽 전달을 시작할 수 없습니다. 스탠바이 유닛을 액티브 상태로 만들려면(비활성화된 장애 조치 포함) 7-42 페이지의 장애 조치 강제 실행을 참조하십시오. 액티브/액티브 장애 조치 쌍에서 장애 조치를 비활성화할 경우 장애 조치 그룹은 액티브 상태에 있는 어느 유닛에서든, 그리고 기본으로 구성하는 어떤 유닛에서든 액티브 상태를 유지합니다.

오류가 발생한 유닛 복원

오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원하려면 다음 절차를 수행합니다.

전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

명령	목적
액티브/스탠바이 모드의 경우: **failover reset** 액티브/액티브 모드의 경우: **failover reset** [**group** *group_id*] **예:** `ciscoasa(config)# failover reset` 또는: `ciscoasa(config)# failover reset group 1`	오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원합니다. 오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원한다고 해서 자동으로 액티브 유닛이 되지는 않습니다. 복원된 유닛은 장애 조치를 통해(강제로 또는 자연적으로) 액티브 유닛이 되기 전까지는 스탠바이 상태로 유지됩니다. 한 가지 예외는 장애 조치 사전 대응 방식으로 구성된 장애 조치 그룹(액티브/액티브 모드에만 해당)입니다. 이전의 액티브 장애 조치 그룹이 액티브 상태가 되고, 사전 대응 방식으로 구성되었으며, 유닛에 오류가 발생한 경우 해당 유닛이 기본 유닛입니다. **group** *group_id*를 지정할 경우, 이 명령을 사용하면 오류가 발생한 액티브/액티브 장애 조치 그룹이 오류가 발생하지 않은 상태로 복원됩니다.

컨피그레이션 다시 동기화

액티브 유닛에 **write standby** 명령을 입력할 경우, 스탠바이 유닛의 실행 중인 컨피그레이션(액티브 유닛과의 통신에 사용되는 장애 조치 명령은 제외)이 지워지며, 액티브 유닛에서는 전체 컨피그레이션을 스탠바이 유닛으로 전송합니다.

다중 컨텍스트 모드에서 시스템 실행 영역에 **write standby** 명령을 입력하면 모든 컨텍스트가 복제됩니다. 컨텍스트 내에서 **write standby** 명령을 입력하면 해당 명령에서는 컨텍스트 컨피그레이션만 복제합니다.

복제된 명령어는 실행 중인 컨피그레이션에 저장됩니다.

장애 조치 기능 테스트

장애 조치 기능을 테스트하려면 다음 절차를 수행합니다.

세부 단계

1단계 액티브 유닛에서 FTP(예)를 사용하여 정상적으로 트래픽을 전달하여 다른 인터페이스의 호스트 간에 파일을 전송하는지 테스트합니다.

2단계 액티브 유닛에 다음 명령을 입력하여 장애 조치를 강제로 실행합니다.

액티브/스탠바이 모드:

```
ciscoasa(config)# no failover active
```

액티브/액티브 모드:

```
ciscoasa(config)# no failover active group group_id
```

3단계 FTP를 사용하여 동일한 두 호스트 간에 다른 파일을 전송합니다.

4단계 테스트에 성공하지 못할 경우, **show failover** 명령을 입력하여 장애 조치 상태를 확인합니다.

5단계 완료되면 다음 명령을 새 액티브 유닛에 입력하여 유닛을 액티브 상태로 복원할 수 있습니다.

액티브/스탠바이 모드:

```
ciscoasa(config)# no failover active
```

액티브/액티브 모드:

```
ciscoasa(config)# failover active group group_id
```

참고 ASA 인터페이스가 중단될 경우 장애 조치를 위해 이는 계속 유닛 문제로 간주합니다. ASA에서 인터페이스 중단이 감지될 경우, 인터페이스 대기 시간을 기다리지 않고 장애 조치가 즉시 이루어집니다. 인터페이스 대기 시간은 피어에서 hello 패킷이 수신되지 않는 경우에도 상태가 괜찮은 것으로 ASA에서 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

컨피그레이션 명령은 액티브 유닛 또는 컨텍스트에서 스탠바이 유닛이나 컨텍스트로 복제되므로, 어떤 유닛에 로그인해도 **failover exec** 명령을 사용하여 올바른 유닛에 컨피그레이션 명령을 입력할 수 있습니다. 예를 들어, 스탠바이 유닛에 로그인한 경우 **failover exec active** 명령을 사용하여 컨피그레이션 변경 사항을 액티브 유닛에 보낼 수 있습니다. 그런 다음 이러한 변경 사항은 스탠바이 유닛에 복제됩니다. **failover exec** 명령을 사용하여 컨피그레이션 명령을 스탠바이 유닛이나 컨텍스트에 보내지 마십시오. 이러한 컨피그레이션 명령은 액티브 유닛에 복제되지 않으며 두 개의 컨피그레이션이 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 실행하여 로컬 유닛에 명령을 실행하려면 충분한 권한이 있어야 합니다.

세부 단계

1단계 다중 컨텍스트 모드에 있을 경우, **changeto context** *name* 명령을 사용하여 구성하려는 컨텍스트를 변경합니다. **failover exec** 명령으로는 장애 조치 피어에서 컨텍스트를 변경할 수 없습니다.

2단계 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 7-45 페이지의 명령 모드 변경을 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 컨피그레이션 모드에서 시작됩니다. **failover exec** 명령을 사용하면 적절한 명령(예: **interface** 명령)을 전송하여 명령 모드를 변경할 수 있습니다. **failover exec**을 사용하여 모드를 변경할 경우 세션 프롬프트가 변경되지 않습니다.

예를 들어, 장애 조치 쌍에 있는 액티브 유닛의 전역 컨피그레이션 모드에 로그인되어 있고 **failover exec active** 명령을 사용하여 인터페이스 컨피그레이션 모드를 변경할 경우, 터미널 프롬프트는 전역 컨피그레이션 모드로 유지되지만 **failover exec**을 사용하여 입력한 명령은 인터페이스 컨피그레이션 모드에 입력됩니다.

다음 예에는 터미널 세션 모드와 **failover exec** 명령 모드의 차이점이 나와 있습니다. 이 예에서 관리자는 액티브 유닛의 **failover exec** 모드를 인터페이스 GigabitEthernet0/1를 위한 인터페이스 컨피그레이션 모드로 변경합니다. 그런 다음 **failover exec active**를 사용하여 입력된 모든 명령은 인터페이스 GigabitEthernet0/1를 위한 인터페이스 컨피그레이션 모드로 전송됩니다. 관리자는 장애 조치 exec 액티브를 사용하여 해당 인터페이스에 IP 주소를 할당할 수 있습니다. 프롬프트는 전역 컨피그레이션 모드를 나타내지만, 인터페이스 컨피그레이션 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)#
```

디바이스에 대한 현재 세션의 명령 모드를 변경할 경우 **failover exec** 명령에서 사용되는 명령 모드에 영향을 미치지 않습니다. 예를 들어, 액티브 유닛에서 인터페이스 컨피그레이션 모드를 사용 중이고 **failover exec** 명령 모드를 변경한 경우, 다음 명령이 전역 컨피그레이션 모드에서 실행됩니다. 그 결과 디바이스에 대한 세션은 인터페이스 컨피그레이션 모드에서 유지되는 반면, **failover exec active**를 사용하여 입력한 명령은 지정된 라우팅 프로세스의 라우터 컨피그레이션 모드로 전송됩니다.

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

failover exec 명령을 실행하여 명령이 전송되는 지정된 디바이스에 명령 모드를 표시하려면 **show failover exec** 명령을 사용합니다. **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 결과입니다.

```
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 제한 사항

원격 명령을 사용할 경우 다음과 같은 제한 사항이 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 컨텍스트 도움말이 제공되지 않습니다.
- 다중 컨텍스트 모드의 경우, 피어 유닛에 있는 피어 컨텍스트에 명령을 전송하는 것만 가능합니다. 다른 컨텍스트에 명령을 전송하려면 우선 유닛의 해당 컨텍스트를 로그인한 컨텍스트로 변경해야 합니다.

- 다음 명령은 **failover exec** 명령과 함께 사용할 수 없습니다.
  - **changeto**
  - **debug** (**undebug**)
- 스탠바이 유닛에 오류가 발생한 상태이고 오류의 원인이 서비스 카드 오류인 경우 **failover exec** 명령을 계속 수신할 수 있습니다. 그렇지 않을 경우에는 원격 명령을 실행할 수 없습니다.
- **failover exec** 명령을 사용하여 장애 조치 피어의 특권 EXEC 모드를 전역 컨피그레이션 모드로 전환할 수 없습니다. 예를 들어, 현재 유닛이 EXEC 모드에 있고 **failover exec mate configure terminal**을 입력할 경우 **show failover exec mate** 결과에는 장애 조치 exec 세션이 전역 컨피그레이션 모드에 있는 것으로 표시됩니다. 그러나 현재 유닛이 전역 컨피그레이션 모드가 되지 않는 한 **failover exec**을 사용하여 피어 유닛에 컨피그레이션 명령을 입력할 경우 오류가 발생합니다.
- **failover exec mate failover exec mate** 명령 같은 재귀적 장애 조치 exec 명령은 입력할 수 없습니다.
- 사용자 입력 또는 확인이 필요한 명령에는 **/nonconfirm** 옵션을 사용해야 합니다.

모니터링 장애 조치

장애 조치 메시지

장애 조치가 일어날 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. 로깅을 사용하려면 39 장, "로깅"을 참조하십시오.

참고 장애 조치가 실행되는 동안에는 장애 조치가 논리적으로 종료되고 인터페이스가 호출되어 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 문제 해결 또는 Cisco TAC와의 문제 해결 세션 동안에만 사용하십시오.

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. 자세한 내용은 40 장, "SNMP"를 참조하십시오.

모니터링 장애 조치

장애 조치를 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
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 컨피그레이션의 장애 조치 명령을 표시합니다.

모니터링 명령의 출력에 대한 자세한 내용은 명령 참조를 참조하십시오.

장애 조치에 대한 기능 기록

표 7-4에서는 이 기능의 출시 내역을 정리합니다.

표 7-4 선택적 액티브/스탠바이 장애 조치 설정에 대한 기능 기록

기능 이름	릴리스	기능 정보
액티브/스탠바이 장애 조치	7.0(1)	이 기능은 도입되었습니다.
액티브/액티브 장애 조치	7.0(1)	이 기능은 도입되었습니다.
장애 조치 키에 16진수 값 지원	7.0(4)	이제 장애 조치 링크 암호화에 16진수 값을 지정할 수 있습니다. 변경된 명령: **failover key hex**

표 7-4 선택적 액티브/스탠바이 장애 조치 설정에 대한 기능 기록(계속)

기능 이름	릴리스	기능 정보
장애 조치 키에 마스터 암호 지원	8.3(1)	이제 장애 조치 키에서 마스터 암호를 지원하며, 이 기능은 실행 중인 컨피그레이션과 시작 컨피그레이션의 공유 키를 암호화합니다. ASA에서 다른 ASA로 공유 비밀을 복사할 경우(예: **more system:running-config** 명령에서), PSK(Pre-Shared Key)를 복사하여 붙여넣을 수 있습니다. **참고** **failover key** shared secret은 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다. 변경된 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**
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 터널의 경우 IPsec(기타 VPN) 라이센스는 계산에 포함하지 않습니다. 도입되거나 수정된 명령: **failover ipsec pre-shared-key**, **show vpn-sessiondb**
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. 수정된 명령: **monitor-interface service-module**

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. 8-24 페이지의 클러스터링으로 지원되지 않는 기능을 참조하십시오.

ASA 클러스터링 정보

이 섹션에서는 클러스터링 아키텍처 및 이러한 아키텍처의 작동 방식에 대해 설명합니다.

- 8-12 페이지의 로드 밸런싱 방법
- 8-18 페이지의 사이트 간 클러스터링
- 8-21 페이지의 ASA 클러스터의 연결 관리 방법
- 8-24 페이지의 ASA 기능 및 클러스터링

ASA 클러스터를 네트워크에 맞게 활용하는 방법

클러스터는 하나의 유닛으로 작동하는 여러 개의 ASA로 구성됩니다. 클러스터로 작동하려면 ASA에는 다음과 같은 인프라가 필요합니다.

- 클러스터 내 커뮤니케이션을 위한 분리된 고속 백플레인 네트워크(또는 *클러스터 제어 링크*라고 함)
- 컨피그레이션 및 모니터링을 지원하는 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.

- Spanned 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.

관련 주제

- 8-31 페이지의 ASA 클러스터링 라이센스
- 8-5 페이지의 클러스터 제어 링크
- 8-11 페이지의 ASA 클러스터 관리
- 8-13 페이지의 Spanned EtherChannel(권장)
- 8-17 페이지의 정책 기반 라우팅(라우팅 방화벽 모드 전용)
- 8-18 페이지의 Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용)

성능 확장 팩터

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 구성원

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다. 이 섹션에서는 각 멤버 역할의 특성을 설명합니다.

- 8-3 페이지의 부트스트랩 컨피그레이션
- 8-3 페이지의 마스터 및 슬레이브 유닛 역할
- 8-3 페이지의 마스터 유닛 선택

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 *슬레이브*로 참가합니다.

마스터 및 슬레이브 유닛 역할

클러스터의 멤버 1개는 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 인터페이스로 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.

관련 주제

- 8-25 페이지의 클러스터링을 위한 중앙 집중식 기능

마스터 유닛 선택

클러스터의 구성원은 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.

관련 주제

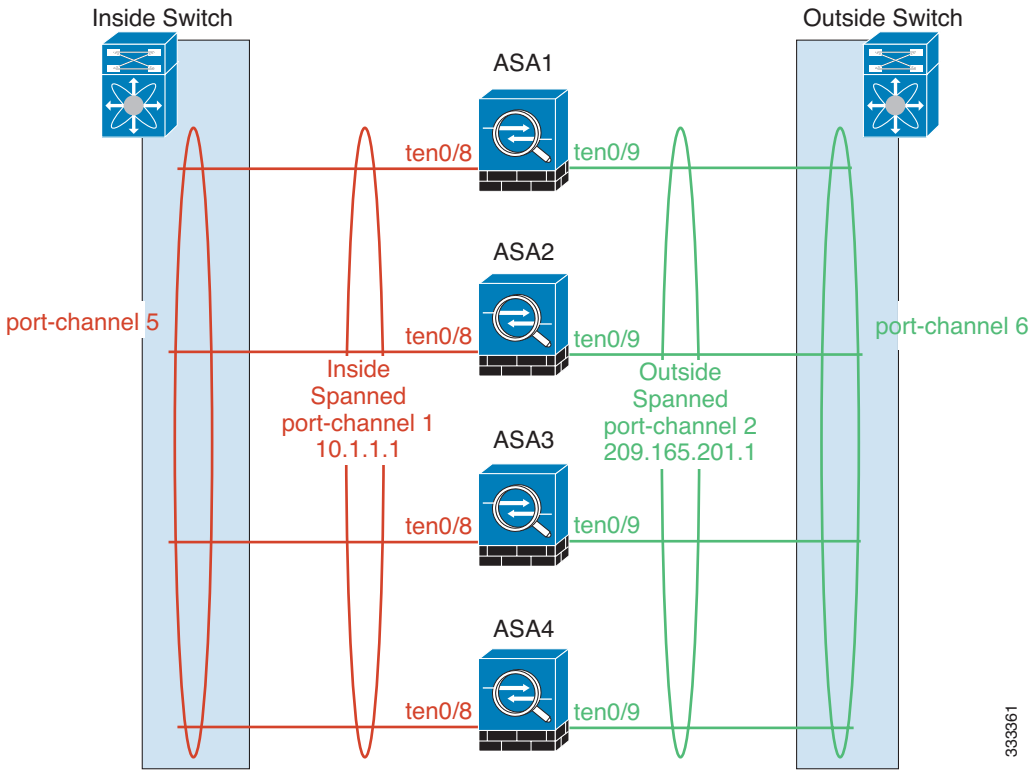
- 8-25 페이지의 클러스터링을 위한 중앙 집중식 기능

클러스터 인터페이스

데이터 인터페이스를 Spanned EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 클러스터의 모든 데이터 인터페이스는 1가지 유형만 가능합니다.

Spanned EtherChannel(권장)

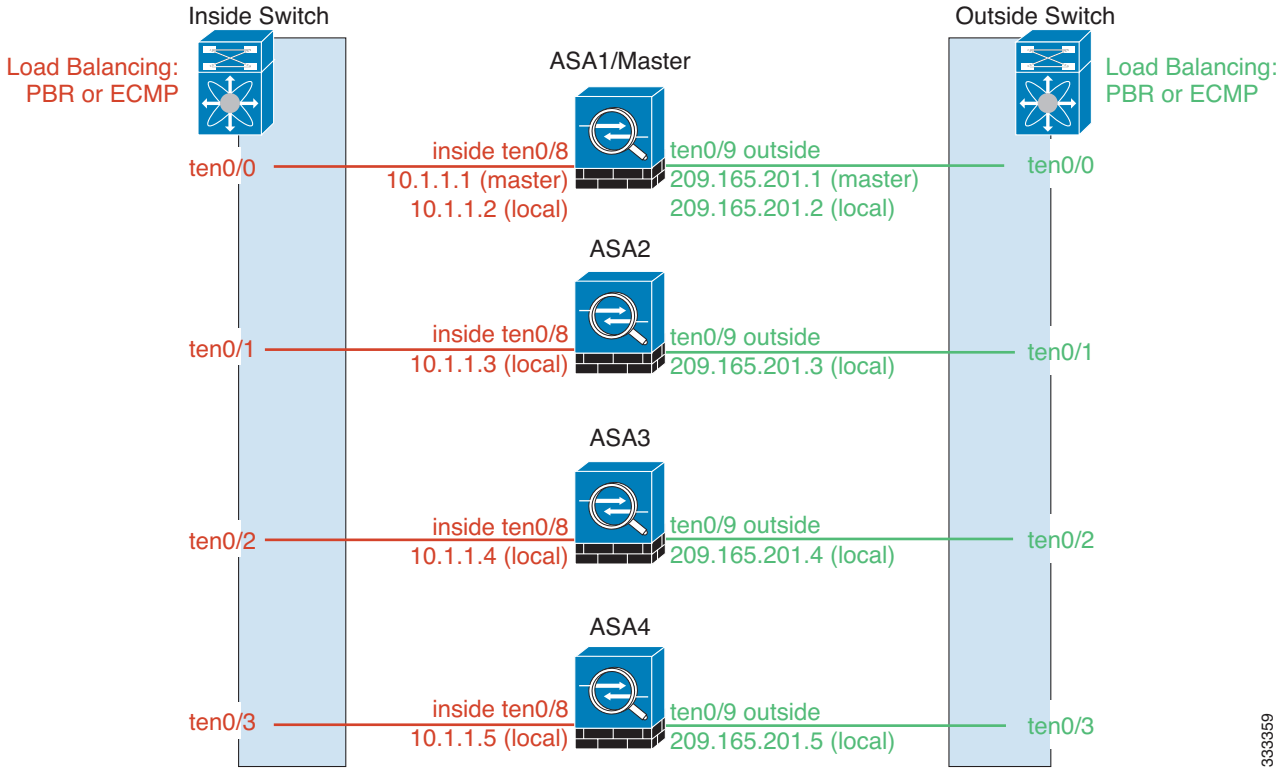
유닛당 하나 이상의 인터페이스를 클러스터 내의 모든 유닛을 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. Spanned EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 IP 주소가 인터페이스가 아닌 브릿지 그룹에 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.



개별 인터페이스(라우팅 방화벽 모드 전용)

개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 *로컬 IP 주소*가 있습니다. 인터페이스 컨피그레이션은 마스터 유닛에서만 구성해야 하므로, 인터페이스 컨피그레이션을 사용하면 클러스터 컨피그레이션원에 대해 지정된 인터페이스에 사용할 IP 주소 풀을 설정할 수 있습니다. *기본 클러스터 IP 주소*는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 기본 클러스터 IP 주소는 마스터 유닛의 보조 IP 주소이며, 로컬 IP 주소는 항상 라우팅의 기본 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 Spanned 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.



관련 주제

- 8-12 페이지의 로드 밸런싱 방법

클러스터 제어 링크

각 유닛에서는 최소 1개의 하드웨어 인터페이스를 클러스터 제어 링크로 지정해야 합니다.

- 8-6 페이지의 클러스터 제어 링크 트래픽 개요
- 8-6 페이지의 클러스터 제어 링크 인터페이스 및 네트워크

- 8-7 페이지의 클러스터 제어 링크 크기 조정
- 8-7 페이지의 클러스터 제어 링크 이중화
- 8-8 페이지의 클러스터 제어 링크 안정성
- 8-8 페이지의 클러스터 제어 링크 오류

클러스터 제어 링크 트래픽 개요

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 마스터 선택
- 컨피그레이션 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

관련 주제

- 8-3 페이지의 클러스터 구성원
- 8-11 페이지의 컨피그레이션 복제
- 8-9 페이지의 유닛 상태 모니터링
- 8-10 페이지의 데이터 경로 연결 상태 복제
- 8-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

클러스터 제어 링크 인터페이스 및 네트워크

클러스터 제어 링크에는 모든 데이터 인터페이스를 사용할 수 있으나 다음 경우는 제외입니다.

- VLAN Subinterface는 클러스터 제어 링크로 사용할 수 없습니다.
- 관리 *x/x* 인터페이스는 단독으로든 EtherChannel로든 클러스터 제어 링크로 사용할 수 없습니다.
- ASA IPS 모듈이 포함된 ASA 5585-X의 경우 클러스터 제어 링크에 모듈 인터페이스를 사용할 수 없습니다. 그러나 ASA 5585-X 네트워크 모듈에서는 인터페이스를 사용할 수 있습니다.

EtherChannel 또는 이중화 인터페이스를 사용할 수 있습니다.

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.

각 클러스터 제어 링크는 동일한 서브넷에 IP 주소가 있습니다. 이 서브넷은 모든 다른 트래픽과 분리되어 있어야 하며, 클러스터 제어 링크 ASA 인터페이스만 포함해야 합니다.

2-멤버 클러스터의 경우 클러스터 제어 링크를 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.

관련 주제

- 8-7 페이지의 클러스터 제어 링크 이중화
- 8-7 페이지의 클러스터 제어 링크 크기 조정

클러스터 제어 링크 크기 조정

클러스터 제어 링크의 크기를 각 멤버의 예상 처리량에 맞게 조정해야 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. 예를 들어, 상태 업데이트의 경우 통과 트래픽이 짧은 TCP 연결을 제외한 트래픽으로 구성되어 있다면 통과 트래픽의 최대 10%를 사용하게 될 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예:

- 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.

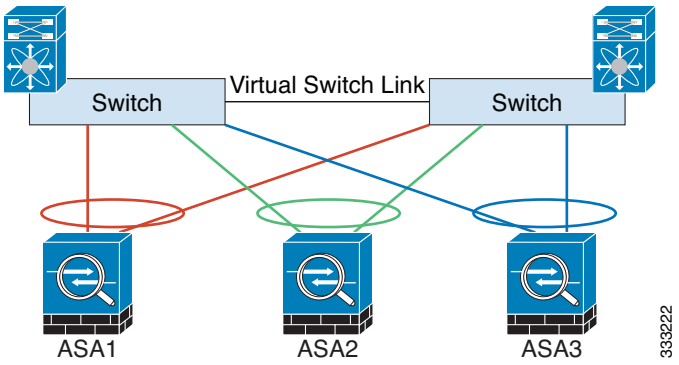
관련 주제

- 8-18 페이지의 사이트 간 클러스터링

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 ASA 인터페이스를 동일한 EtherChannel 내에서 연결하여 VSS 또는 vPC의 스위치와 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 수행하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 Spanned EtherChannel입니다.



클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(왕복 시간)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.

관련 주제

8-10 페이지의 클러스터 다시 참가

ASA 클러스터 내의 고가용성

ASA 클러스터링에서는 유닛과 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

- 8-9 페이지의 유닛 상태 모니터링
- 8-9 페이지의 인터페이스 모니터링
- 8-9 페이지의 유닛 또는 인터페이스 오류
- 8-10 페이지의 데이터 경로 연결 상태 복제

유닛 상태 모니터링

마스터 유닛에서는 클러스터 제어 링크를 통해 keepalive 메시지를 주기적으로 전송하여 모든 슬레이브 유닛을 모니터링합니다(기간은 구성 가능함). 각 슬레이브 유닛에서는 동일한 메커니즘을 사용하여 마스터 유닛을 모니터링합니다.

인터페이스 모니터링

각 유닛에서는 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 마스터 유닛에 보고합니다.

- Spanned 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.

유닛 또는 인터페이스 오류

상태 모니터링 기능이 사용 설정된 경우, 유닛에 오류가 발생하거나 유닛의 인터페이스에 오류가 발생하면 클러스터에서 해당 유닛이 제거됩니다. 특정 유닛의 인터페이스에 오류가 발생하였으나 다른 유닛의 동일한 인터페이스는 활성 상태인 경우, 클러스터에서 해당 특정 유닛이 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다. EtherChannel(Spanned 또는 일반)의 경우, 설정된 멤버에 대한 인터페이스가 중지될 경우 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.

클러스터의 유닛에 오류가 발생할 경우, 해당 유닛에서 호스팅하는 연결이 다른 유닛으로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 클러스터 링크를 통해 공유됩니다.

마스터 유닛에 오류가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 마스터 유닛이 됩니다.

ASA에서는 클러스터에 자동으로 다시 참가하려고 합니다.

참고 ASA가 비활성화되고 클러스터에 자동으로 다시 참가하지 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 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.

관련 주제

8-10 페이지의 클러스터 다시 참가

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 클러스터 제어 링크 오류 — 클러스터 제어 링크의 문제를 해결한 후에는 **클러스터** *이름*을 입력한 다음 **활성화하여** 콘솔 포트에서 클러스터링을 다시 사용 설정함으로써 클러스터에 수동으로 다시 참가해야 합니다.
- 데이터 인터페이스 오류 — ASA에서는 5분에 다시 참가를 시도하며 그 다음에는 10분, 마지막으로 20분에 참가를 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 ASA에서는 클러스터링을 비활성화합니다. 데이터 인터페이스 문제를 해결한 후에는 **클러스터** *이름*을 입력한 다음 **활성화하여 콘솔 포트에서 클러스터링을 수동으로 사용 설정해야 합니다**.
- 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 활성 상태이고 클러스터링의 **사용** 명령이 계속 활성화되어 있으면 전원을 다시 가동할 때 유닛이 클러스터에 다시 참가할 수 있습니다.

관련 주제

- 8-46 페이지의 마스터 유닛 부트스트랩 설정 구성

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 오류 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 오류가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다.

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.

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 8-1 클러스터 전반에 걸쳐 복제된 ASA 기능

트래픽	상태 지원	참고
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	투명 모드 전용입니다.
MAC 주소 테이블	예	투명 모드 전용입니다.
사용자 ID	예	AAA 규칙(uauth)을 포함하고 방화벽을 식별합니다.
IPv6 인접 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—
VPN(사이트 대 사이트)	아니요	마스터 유닛에 오류가 발생할 경우 VPN 세션의 연결이 끊어집니다.

컨피그레이션 복제

클러스터의 모든 유닛에서는 단일 컨피그레이션을 공유합니다. 초기 부트스트랩 컨피그레이션을 제외하고, 마스터 유닛에서는 컨피그레이션만 변경할 수 있으며 변경 사항은 클러스터의 모든 다른 유닛에 자동으로 복제됩니다.

ASA 클러스터 관리

ASA 클러스터링을 사용하는 데 따른 여러 장점 중 하나는 관리하기가 쉽다는 점입니다. 이 섹션에서는 클러스터를 관리하는 방법에 대해 설명합니다.

- 8-11 페이지의 관리 네트워크
- 8-11 페이지의 관리 인터페이스
- 8-12 페이지의 마스터 유닛 관리 및 슬레이브 유닛 관리 비교
- 8-12 페이지의 RSA 키 복제
- 8-12 페이지의 ASDM 연결 인증서 IP 주소 불일치

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결하는 것이 좋습니다. 이러한 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 Spanned EtherChannel 인터페이스로 구성할 수 있습니다.

데이터 인터페이스에 Spanned EtherChannel을 사용 중인 경우에도, 관리용으로는 개별 인터페이스를 사용하는 것이 좋습니다. 개별 인터페이스를 사용하면 필요한 경우 각 유닛에 직접 연결할 수 있는 반면, Spanned EtherChannel 인터페이스의 경우에는 현재 마스터 유닛에 원격 연결만 가능합니다.

참고 Spanned EtherChannel 인터페이스 모드를 사용 중이고 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 라우팅을 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.

Spanned 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 관리 및 슬레이브 유닛 관리 비교

부트스트랩 컨피그레이션을 제외하고, 모든 관리 및 모니터링 작업은 마스터 유닛에서 이루어질 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(컨피그레이션 백업 및 이미지 업데이트 포함). 다음 기능은 마스터 유닛에서 사용할 수 없습니다.

- 유닛당 클러스터별 통계 모니터링
- 유닛당 Syslog 모니터링
- 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.

관련 주제

- 34 장, "디지털 인증서"

로드 밸런싱 방법

사용 가능한 로드 밸런싱 방법은 방화벽 모드 및 인터페이스 유형에 따라 다릅니다.

- 8-13 페이지의 Spanned EtherChannel(권장)
- 8-17 페이지의 정책 기반 라우팅(라우팅 방화벽 모드 전용)
- 8-18 페이지의 Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용)

Spanned EtherChannel(권장)

유닛당 하나 이상의 인터페이스를 클러스터 내의 모든 유닛을 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다.

Spanned EtherChannel 이점

EtherChannel 로드 밸런싱 방식을 다른 방법보다 우선하여 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

관련 주제

9-4 페이지의 EtherChannel

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.

로드 밸런싱

소스 또는 목적지 IP 주소 및 TCP, UDP 포트 번호를 기준으로 전용 해시 알고리즘을 사용하여 EtherChannel 링크를 선택합니다.

참고 ASA에서는 로드 밸런싱 알고리즘 기본값을 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 있기 때문입니다.

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.

관련 주제

- 9-21 페이지의 EtherChannel 맞춤화
- 9-6 페이지의 로드 밸런싱
- 8-29 페이지의 NAT 및 클러스터링

EtherChannel 이중화

EtherChannel에는 이중화 기능이 내장되어 있으며, 모든 링크의 라인 프로토콜 상태를 모니터링합니다. 링크 하나에 오류가 발생하면 나머지 링크 간의 트래픽이 재밸런싱됩니다. 특정 유닛에서 EtherChannel의 모든 링크에 오류가 발생했으나 다른 유닛은 아직 가동 중인 경우, 클러스터에서 특정 유닛이 제거됩니다.

VSS 또는 vPC에 연결

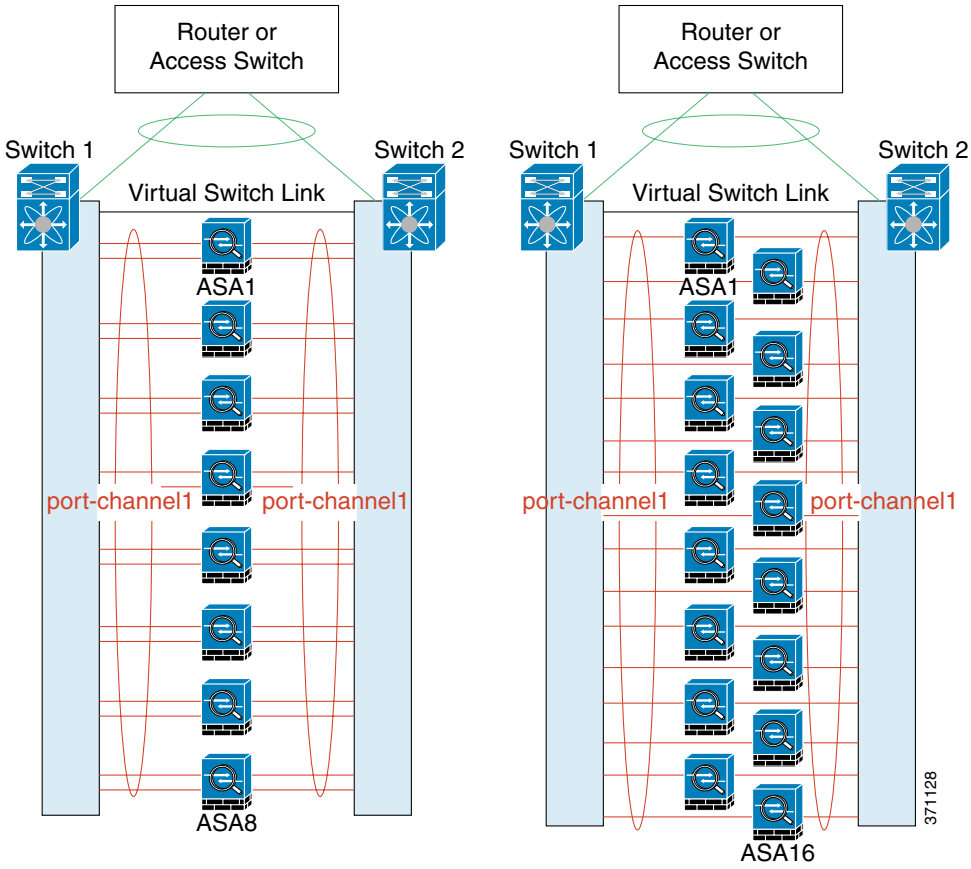
Spanned EtherChannel에서 ASA당 여러 인터페이스를 포함할 수 있습니다. ASA당 여러 인터페이스는 VSS 또는 vPC에서 두 스위치에 모두 연결하는 경우에 특히 유용합니다.

스위치에 따라 Spanned 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.

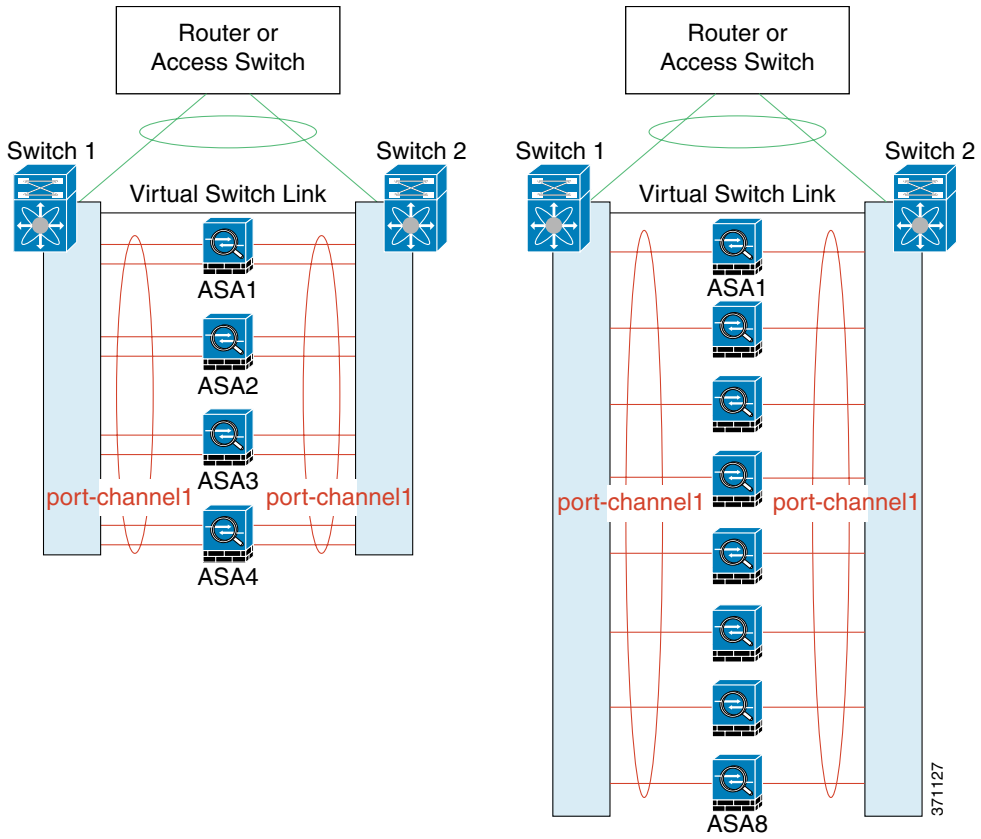
EtherChannel에서 8개의 활성 링크를 지원하는 스위치를 사용하려면, VSS/vPC에서 2개의 스위치에 연결할 때 Spanned EtherChannel에 최대 16개의 활성 링크를 구성하면 됩니다.

Spanned 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.

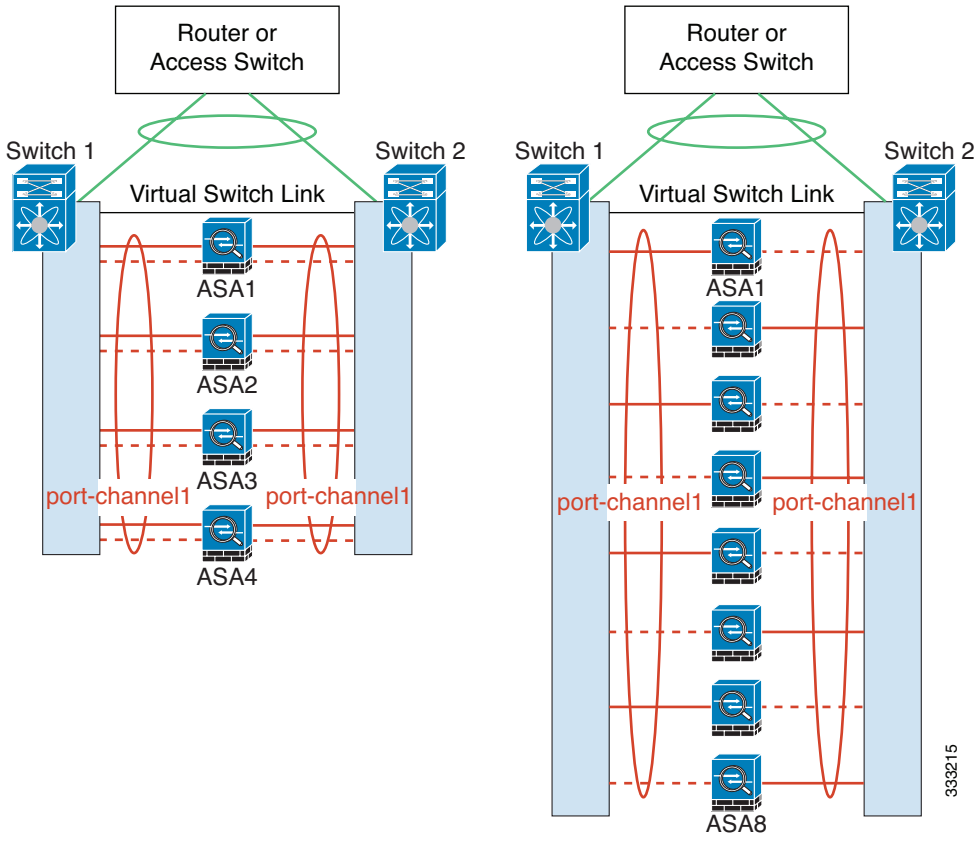
다음 그림에는 8-ASA 클러스터 및 16-ASA 클러스터의 32개 활성 링크 Spanned EtherChannel이 나와 있습니다.



다음 그림에는 4-ASA 클러스터 및 8-ASA 클러스터의 16개 활성 링크 Spanned EtherChannel이 나와 있습니다.



다음 그림에는 4-ASA 클러스터 및 8-ASA 클러스터의 8개 활성/8개 스탠바이 링크 Spanned EtherChannel이 나와 있습니다. 활성 링크는 실선으로 표시되어 있고 비활성 링크는 점선으로 표시되어 있습니다. cLACP 로드 밸런싱의 경우 EtherChannel에서 활성화할 최상의 링크 8개를 자동으로 선택합니다. 그림과 같이, cLACP를 사용하면 링크 수준에서 로드 밸런싱을 실현하는 데 도움이 됩니다.



정책 기반 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 PBR(정책 기반 라우팅)입니다.

이미 PBR을 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다. 이 방법에서는 추가적인 튜닝 옵션 및 Spanned EtherChannel을 제공할 수 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 각각의 ASA를 모니터링합니다. 그런 다음 특정 ASA의 도달 범위를 기준으로 경로 맵을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 다음 URL을 참조하십시오.

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 방법에서는 추가적인 튜닝 옵션 및 Spanned EtherChannel을 제공할 수 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 오류가 발생하면 문제를 초래할 수 있습니다. 경로는 계속 사용할 수 있으며 오류가 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.

사이트 간 클러스터링

사이트 간 설치의 경우 다음 지침을 준수하여 ASA 클러스터링을 활용할 수 있습니다.

- 8-18 페이지의 사이트 간 클러스터링 지침
- 8-19 페이지의 데이터 센터 인터커넥트 크기 조정
- 8-20 페이지의 사이트 간 예

사이트 간 클러스터링 지침

사이트 간 클러스터링에 대한 다음 지침을 참조하십시오.

- 다음과 같은 인터페이스 및 방화벽 모드에서는 사이트 간 클러스터링을 지원합니다.

	방화벽 모드	
인터페이스 모드	라우팅	투명
개별 인터페이스	예	N/A
Spanned EtherChannel	아니요	예

- 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 재밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 연결이 재밸런싱됩니다.
- 클러스터를 구현할 경우 여러 사이트에 있는 멤버가 구분되지 않습니다. 따라서 하나의 특정한 연결의 연결 역할은 사이트 전체를 포괄하게 될 수 있습니다. 이는 정상적인 동작입니다.

- 투명 모드의 경우 내부 라우터에서 모두 동일한 MAC 주소를 공유하는지 확인하고, 외부 라우터에서도 모두 동일한 MAC 주소를 공유하는지 확인해야 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.
- Spanned EtherChannel 모드의 경우 데이터 사이트 간의 ASA 클러스터에 직접 연결된 데이터 VLAN을 확장하지 않습니다. 이렇게 할 경우 루프가 발생합니다. 확장된 데이터 VLAN은 라우터를 통해 클러스터와 분리해야 합니다.

관련 주제

- 8-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱
- 8-22 페이지의 연결 역할

데이터 센터 인터커넥트 크기 조정

클러스터 제어 링크 트래픽을 처리하기 위한 DCI(데이터 센터 인터커넥트) 대역폭을 다음 계산과 같이 예약해야 합니다.

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

각 사이트의 멤버 수가 다를 경우, 더 큰 숫자를 계산에 사용합니다. DCI의 최소 대역폭은 한 멤버에 대한 클러스터 제어 링크의 크기보다 작으면 안 됩니다.

예:

- 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)
- 2개 사이트에 멤버가 8개인 경우 크기가 다음과 같이 증가함
  - 총 클러스터 멤버 8개
  - 사이트당 멤버 4개
  - 멤버당 5Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 10Gbps(4/2 x 5Gbps)
- 3개 사이트에 멤버가 6개인 경우
  - 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
  - 각 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.

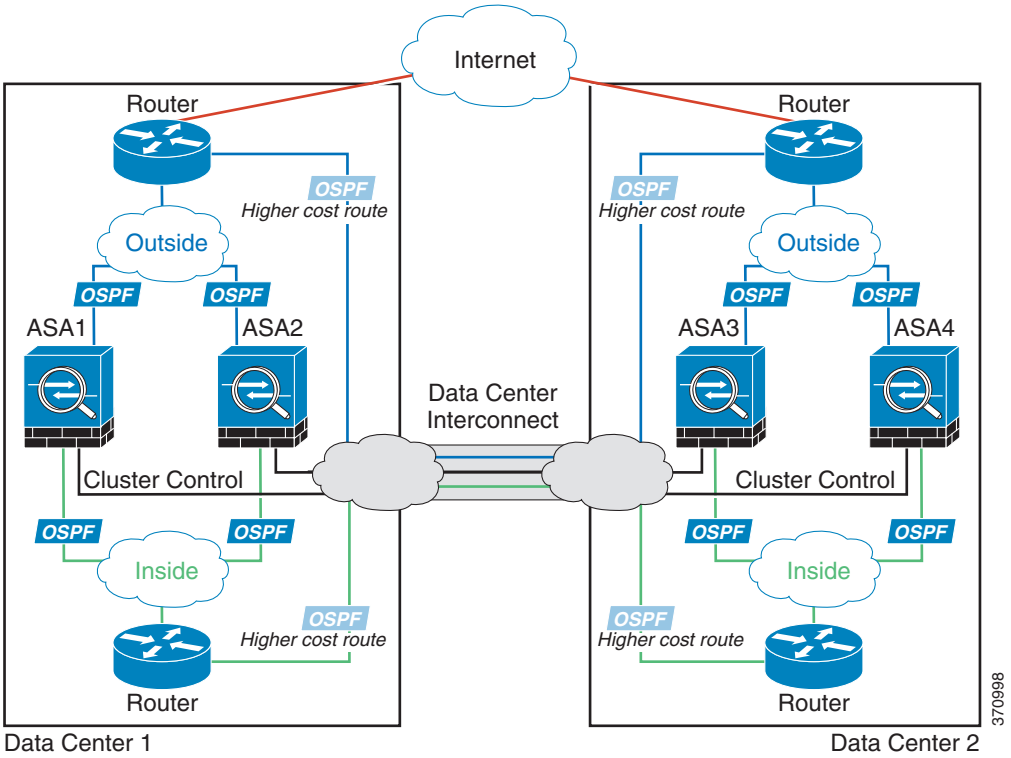
사이트 간 예

다음 예에는 지원되는 클러스터 구축에 대한 내용이 나와 있습니다.

- 8-20 페이지의 개별 인터페이스 사이트 간 예
- 8-20 페이지의 Spanned EtherChannel 투명 모드 사이트 간 예

개별 인터페이스 사이트 간 예

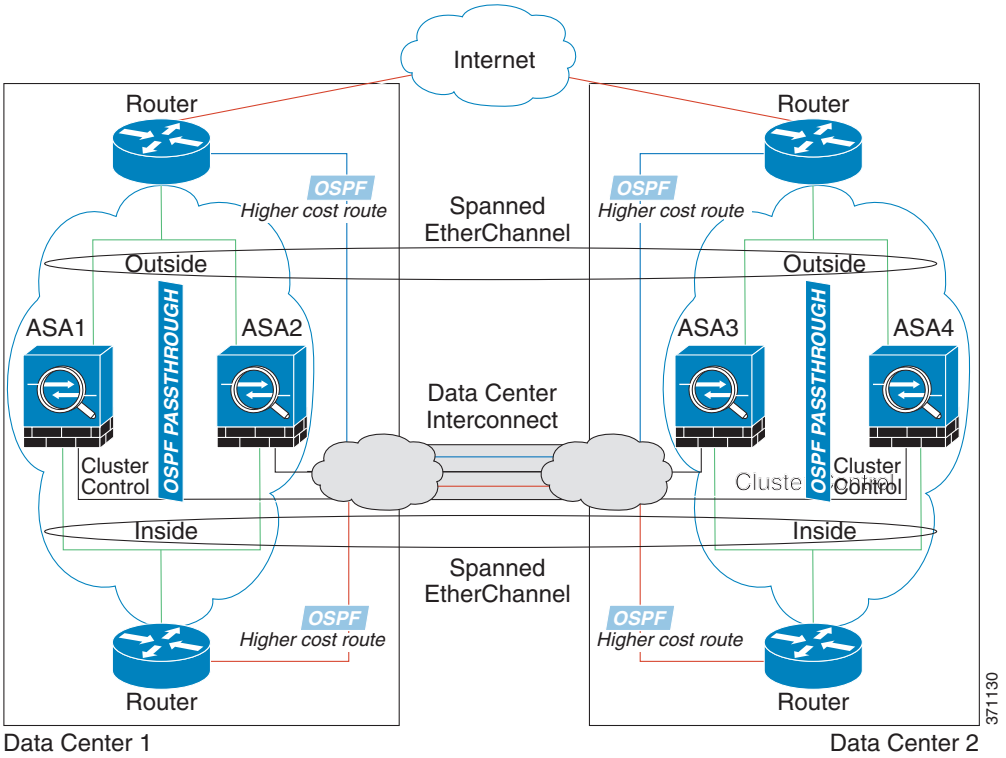
다음 예에는 각 데이터 센터 2개의 ASA 클러스터 멤버 2개가 나와 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 데이터 센터의 내부 및 외부 라우터에서는 OSPF와 PBR 또는 ECMP를 사용하여 클러스터 멤버 간의 트래픽을 로드 밸런싱합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 ASA 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 ASA 클러스터 멤버로 이동합니다.



Spanned EtherChannel 투명 모드 사이트 간 예

다음 예에는 각 데이터 센터 2개의 ASA 클러스터 멤버 2개가 나와 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부용 Spanned EtherChannel을 사용하여 로컬 스위치에 연결됩니다. ASA EtherChannel은 클러스터의 모든 ASA 전반에 걸쳐 있습니다. 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 ASA 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트

래픽이 유지됩니다. ASA를 통과하는 비용이 낮은 경로의 경우, 클러스터의 각 사이트에 있는 같은 브릿지 그룹을 거쳐 비대칭 연결을 유지해야 합니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 ASA 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 ASA 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 ASA 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 ASA의 Spanned EtherChannel은 로컬 스위치에만 연결된 데이터 센터 1 ASA, 그리고 이러한 로컬 스위치에 연결된 데이터 센터 2 ASA로 이루어져 있으나, 근본적으로 Spanned EtherChannel은 "분리"되어 있습니다. 각 로컬 VSS/vPC에서는 Spanned EtherChannel을 사이트-로컬 EtherChannel로 간주합니다.

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.

- 8-22 페이지의 연결 역할
- 8-22 페이지의 새 연결 소유권
- 8-23 페이지의 샘플 데이터 흐름
- 8-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

연결 역할

각 연결에는 3가지 종류의 다른 ASA 역할이 정의됩니다.

- 소유자 — 연결을 가장 처음 수신하는 유닛입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다.
- 관리자 — 전달자의 소유자 조회 요청을 처리하고 연결 상태를 유지하여 소유자 유닛에 오류가 발생한 경우 백업 역할을 수행하는 유닛입니다. 소유자가 새 연결을 수신할 경우, 소유자 유닛에서는 소스/목적지 IP 주소와 TCP 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.
- 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. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 순서 임의 설정을 사용하지 않을 경우, SYN 쿠키가 사용되지 않으며 관리자 유닛에 조회해야 합니다.) DNS 및 ICMP 같은 짧은 흐름의 경우, 조회 대신 전달자 유닛에서 패킷을 관리자 유닛에 직접 전송하며, 관리자 유닛에서는 이 패킷을 소유자 유닛에 보냅니다. 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.

새 연결 소유권

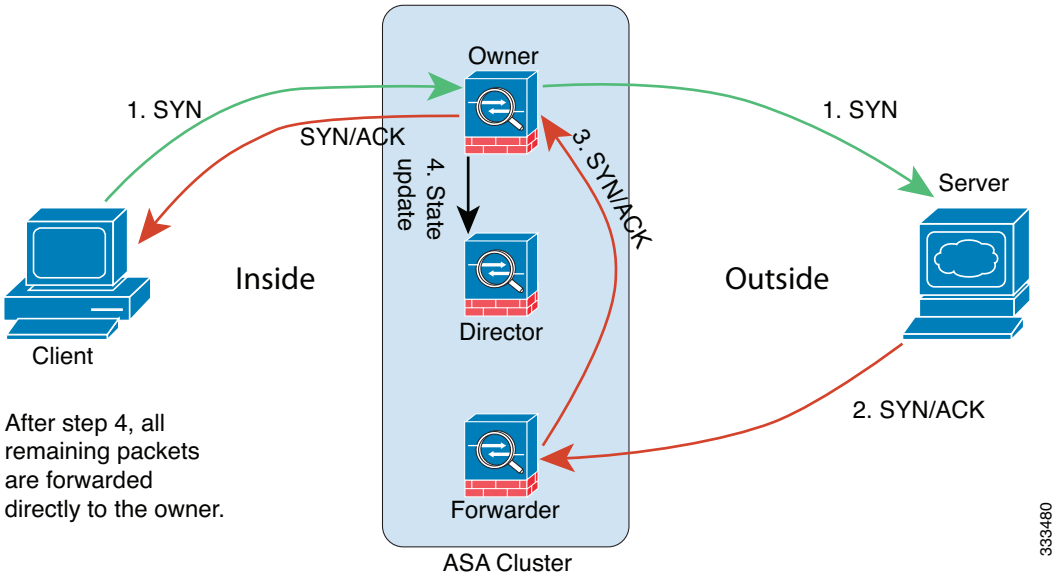
로드 밸런싱을 통해 클러스터의 멤버에 새 연결이 전송될 경우, 해당 유닛에서는 연결의 양방향을 모두 소유합니다. 다른 유닛에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 유닛에 전달됩니다. 최상의 성능을 실현하려면, 같은 유닛에 전송될 수 있도록 흐름의 양방향에 적절한 외부 로드 밸런싱이 필요합니다. 또한 흐름은 유닛 간에 균일하게 분산되어야 합니다. 다른 유닛에 반대 방향의 흐름이 전송될 경우, 이는 원래 유닛으로 다시 리디렉션됩니다.

관련 주제

- 8-12 페이지의 로드 밸런싱 방법

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 재밸런싱

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.

- 통합 커뮤니케이션
- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- 다음과 같은 애플리케이션 감시:
  - CTIQBE
  - GTP
  - H323, H225, RAS
  - IPsec 통과
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP(Skinny)
  - WAAS
  - WCCP
- 봇넷 트래픽 필터
- 자동 업데이트 서버
- DHCP 클라이언트, 서버, 릴레이, 프록시
- VPN 로드 밸런싱
- 장애 조치
- ASA CX 모듈

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 허용합니다. 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.

재밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 마스터 유닛으로 재밸런싱될 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.

- 사이트 대 사이트 VPN
- 다음과 같은 애플리케이션 감시:
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- 동적 라우팅(Spanned EtherChannel 모드 전용)
- 멀티캐스트 라우팅(개별 인터페이스 모드 전용)
- 고정 경로 모니터링
- IGMP 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 평면 전달은 클러스터 전체에 분산됨)
- PIM 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 평면 전달은 클러스터 전체에 분산됨)
- 네트워크 액세스에 대한 인증 및 권한 부여. 어카운팅이 분산됨
- 필터링 서비스

관련 주제

- 8-7 페이지의 클러스터 제어 링크 크기 조정
- 8-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

개별 유닛에 적용되는 기능

이러한 기능은 전체 클러스터 또는 마스터 유닛이 아닌 각ASA 유닛에 적용됩니다.

- QoS — QoS 정책은 컨피그레이션 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. 8개 유닛으로 구성되고 트래픽이 균일하게 분산된 클러스터의 경우, 적응 속도는 클러스터 *속도*의 8배가 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 컨텍스트 모드에서 리소스 관리는 로컬 사용량을 기준으로 각 유닛에 개별적으로 시행됩니다.
- ASA FirePOWER 모듈 — ASA FirePOWER 모듈 간에는 컨피그레이션 동기화 또는 상태 공유 기능이 없습니다. 클러스터의 ASA FirePOWER 모듈에 일관된 정책을 유지하려면 FireSIGHT Management Center를 사용해야 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. 클러스터링의 이러한 연결은 여러 ASA 디바이스 간에 균형 조정이 이루어지며, 각각에는 고유한 IPS 모듈이 있습니다. 이러한 IPS 모듈에서는 상태 정보를 공유하지 않으므로, 클러스터에서 포트 검사를 결과로 감지하지 못할 수 있습니다.

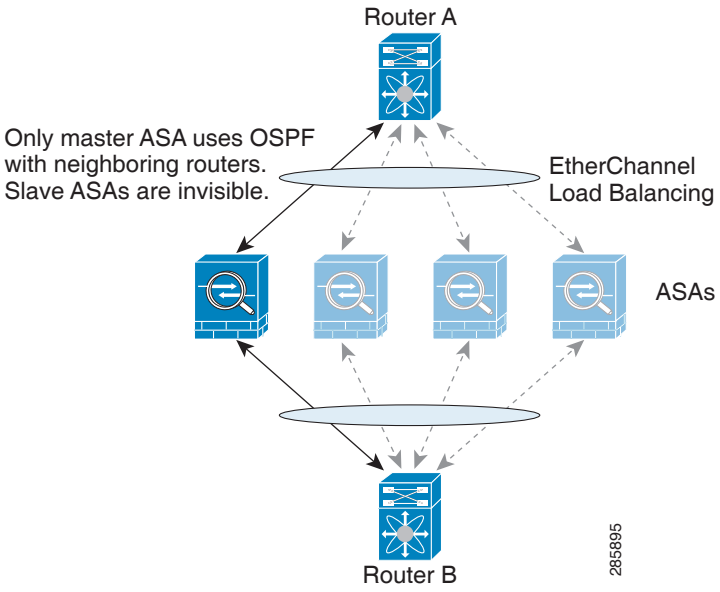
동적 라우팅 및 클러스터링

- 8-27 페이지의 Spanned EtherChannel 모드의 동적 라우팅
- 8-28 페이지의 개별 인터페이스 모드의 동적 라우팅

Spanned EtherChannel 모드의 동적 라우팅

Spanned 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 8-1 Spanned EtherChannel 모드의 동적 라우팅



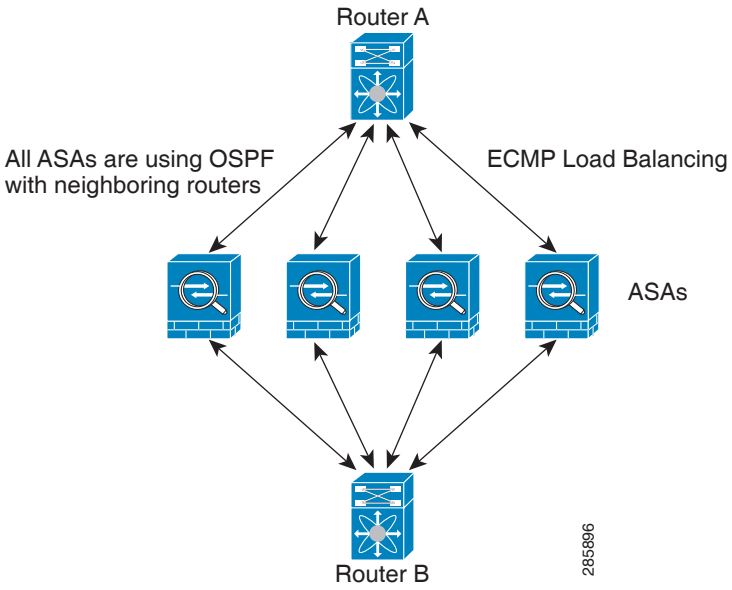
슬레이브 멤버가 마스터 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 마스터 유닛에서 슬레이브 유닛으로 동기화되지 않습니다. 마스터 유닛 전환이 있을 경우, 인접한 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.

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 8-2 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.

멀티캐스트 라우팅 및 클러스터링

멀티캐스트 라우팅은 인터페이스 모드에 따라 다르게 작동합니다.

- 8-28 페이지의 Spanned EtherChannel 모드의 멀티캐스트 라우팅
- 8-28 페이지의 개별 인터페이스 모드의 멀티캐스트 라우팅

Spanned EtherChannel 모드의 멀티캐스트 라우팅

Spanned 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 연결 소유자가 아닌 ASA에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다.

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 않는 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. Spanned EtherChannel의 경우에는 하나의 IP 주소만 클러스터 인터페이스에 연결되므로 이것이 문제가 되지 않습니다.
- 개별 인터페이스에 인터페이스 PAT 없음 — 개별 인터페이스에는 인터페이스 PAT가 지원되지 않습니다.
- 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. 주소 할당을 보려면 **show nat pool cluster** 명령을 사용합니다.
- 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 트래픽에서는 세션당 PAT xlate를 사용합니다. 다중 세션 PAT가 필요한 트래픽(예: H.323, SIP 또는 Skinny)의 경우 세션당 PAT를 사용하지 않도록 설정할 수 있습니다. 세션당 PAT에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.
- 다음을 검사할 수 있는 고정 PAT 없음
  - FTP
  - PPTP
  - RSH
  - SQLNet
  - TFTP
  - XDMCP
  - 모든 VoIP(voice-over-IP) 제품

네트워크 액세스 및 클러스터링용 AAA

네트워크 액세스용 AAA는 인증, 권한 부여, 어카운팅이라는 세 가지 구성 요소로 이루어져 있습니다. 인증 및 어카운팅은 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.

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 컨피그레이션은 클러스터의 모든 유닛에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 유닛에서는 단일한 유닛에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 컨피그레이션에 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.

관련 주제

- 39-15 페이지의 디바이스 ID를 Non-EMBLEM 형식 Syslog 메시지에 포함

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.

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 Spanned 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.

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.

Cisco TrustSec 및 클러스터링

마스터 유닛에서만 SGT(보안 그룹 태그) 정보를 파악합니다. 그런 다음 마스터 유닛에서는 SGT를 슬레이브에 제공하며, 슬레이브에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

ASA 클러스터링 라이센스

모델	라이센싱 요구 사항
ASA 5585-X	클러스터 라이센스, 최대 16개까지 지원. 클러스터 라이센스는 각 유닛에 필요합니다. 기타 기능 라이센스의 경우, 클러스터 유닛에서는 각 유닛에 동일한 라이센스를 필요로 하지 않습니다. 여러 유닛에 기능 라이센스를 보유한 경우, 해당 라이센스는 단일하게 실행되는 ASA 클러스터 라이센스로 통합됩니다. **참고** 각 유닛에는 동일한 암호화 라이센스 및 동일한 10 GE I/O 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.
기타 모델	지원 안 함

ASA 클러스터링의 사전 요구 사항

ASA 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 유닛은 다음과 같아야 합니다.

- 동일한 DRAM과 같은 모델이어야 합니다. 플래시 메모리는 동일하지 않아도 됩니다.
- 이미지 업그레이드 시 동일한 소프트웨어 예외를 실행해야 합니다. 무중단 업그레이드가 지원됩니다.
- 개별 인터페이스 모드를 사용할 경우 지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버를 보유할 수 있습니다.
- 동일한 보안 컨텍스트 모드(단일 또는 다중)에 있어야 합니다.

- (단일 컨텍스트 모드) 동일한 방화벽 모드(라우팅 또는 투명 모드)여야 합니다.
- 새 클러스터 컨피그레이션원은 컨피그레이션을 복제하기 전에 맨 처음 클러스터 제어 링크 통신을 수행할 경우 동일한 SSL 암호화 설정(**ssl 암호화** 명령)을 마스터 유닛으로 사용해야 합니다.
- ASA 5585-X, 10 GE I/O 라이센스의 클러스터, 암호화는 동일해야 합니다.

스위치 사전 요구 사항

- ASA에서 클러스터링을 구성하기 전에 스위치 컨피그레이션을 완료해야 합니다.
- 다음 표에는 ASA 클러스터링과의 상호 운용을 지원하는 외부 하드웨어 및 소프트웨어 목록이 나와 있습니다.

표 8-2 ASA 클러스터링을 위한 외부 하드웨어 및 소프트웨어 지원

외부 하드웨어	외부 소프트웨어	ASA 버전
Cisco Nexus 9300	Cisco NX-OS 6.1(2)I2(1) 이상	9.2(1) 이상
Cisco Nexus 7000	Cisco NX-OS 5.2(5) 이상	9.0(1) 이상
Cisco Nexus 5000	Cisco NX-OS 7.0(1) 이상	9.1(4) 이상
Catalyst 6500(Supervisor 32, 720, 720-10GE 포함)	Cisco IOS 12.2(33)SXI7, SXI8, SXI9 이상	9.0(1) 이상
Catalyst 3750-X	Cisco IOS 15.0(2) 이상	9.1(4) 이상

ASA 사전 요구 사항

- 각 유닛이 관리 네트워크에 참가하기 전에 각 유닛에 고유한 IP 주소를 제공해야 합니다.
  - ASA 에 연결하고 관리 IP 주소를 설정하는 방법에 대한 자세한 내용은 시작 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.

기타 사전 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.

관련 주제

- 8-33 페이지의 ASA 클러스터링 지침
- 9-24 페이지의 점보 프레임 지원 활성화
- 8-3 페이지의 부트스트랩 컨피그레이션

ASA 클러스터링 지침

컨텍스트 모드

모드는 각 멤버 유닛과 일치해야 합니다.

방화벽 모드

단일 모드의 경우 방화벽 모드는 모든 유닛과 일치해야 합니다.

장애 조치

클러스터링에서는 장애 조치가 지원되지 않습니다.

IPv6

클러스터 제어 링크는 IPv4를 사용하는 경우에만 지원됩니다.

모델

지원되는 모델:

- ASA 5585-X

  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.

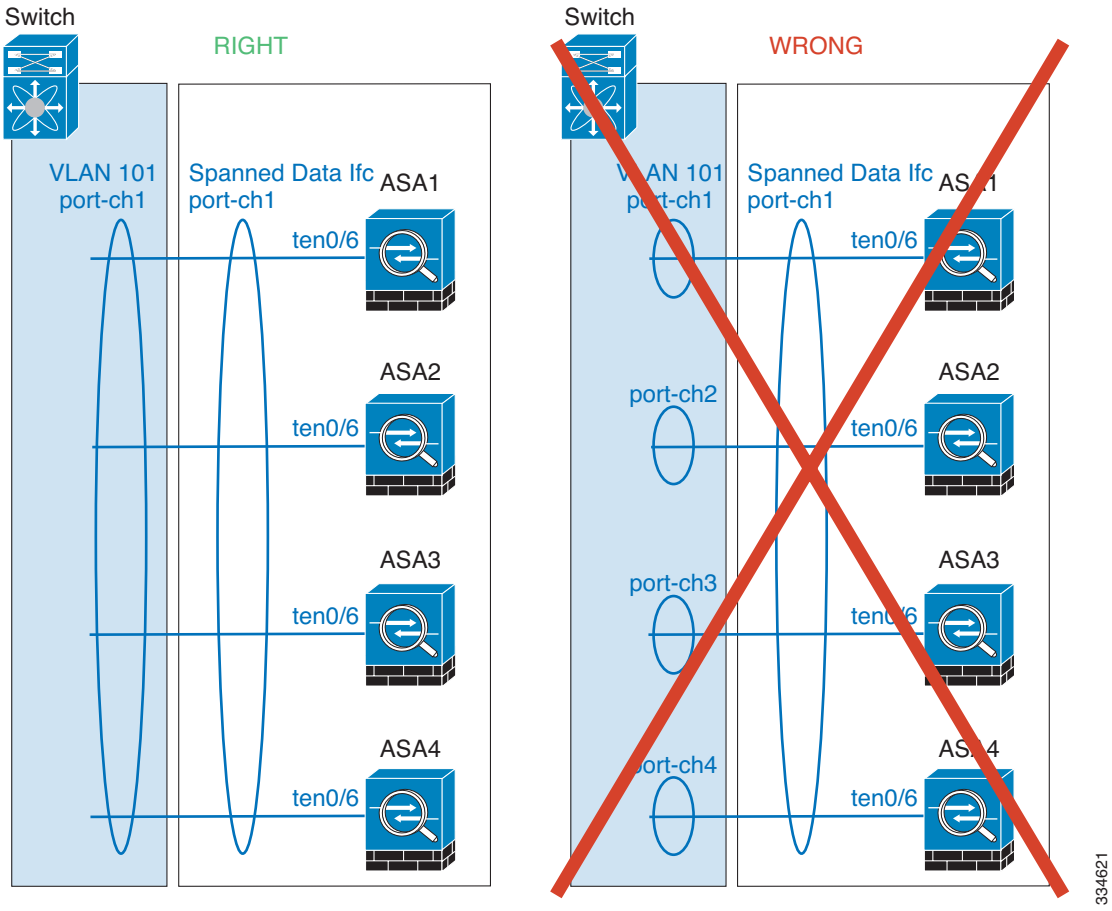
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X

스위치

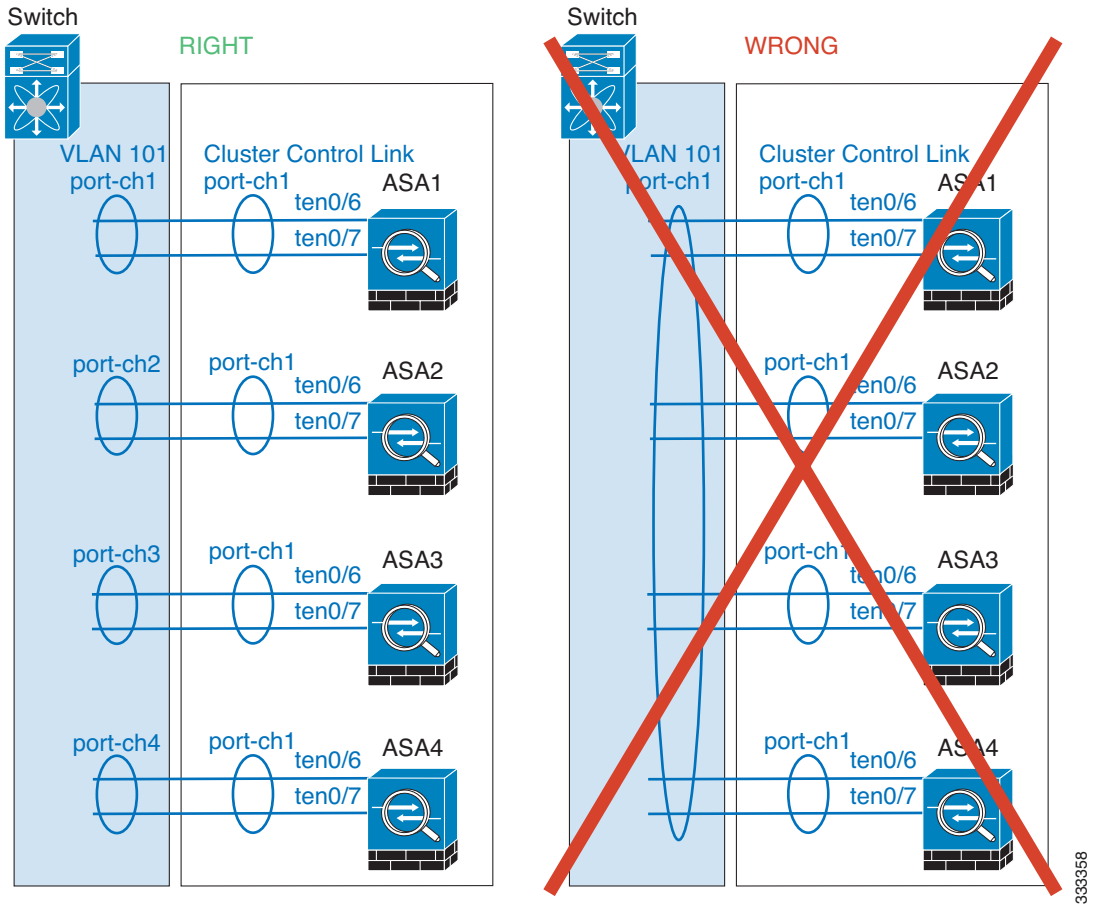
- 클러스터 제어 링크 인터페이스용 스위치의 경우, ASA에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 ASA에 트래픽이 균일하지 않게 분산될 수 있기 때문입니다. ASA에서 로드 밸런싱 알고리즘의 기본값을 변경하지 *마십시오*(**port-channel load-balance** 명령의 경우).
- 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.
- Cisco Nexus 스위치의 경우 모든 클러스터용 EtherChannel 인터페이스에서 LACP Graceful Convergence 기능을 사용하지 않도록 설정해야 합니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 사용하지 않도록 설정하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 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.

EtherChannel

- ASA에서는 EtherChannel을 스위치 스택에 연결하도록 지원하지 않습니다. ASA EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다.
- Spanned 및 디바이스-로컬 EtherChannel 컨피그레이션 비교 — Spanned EtherChannel와 디바이스-로컬 EtherChannel에 대한 스위치를 올바르게 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 ASA *Spanned* EtherChannel의 경우, 인터페이스가 스위치의 단일한 EtherChannel로 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



  - 디바이스-로컬 EtherChannel — 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 ASA *디바이스-로컬* EtherChannel*의* 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 ASA EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



추가 지침

- 중요한 토폴로지 변경 사항이 발생할 경우(예: EtherChannel 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 생성) 상태 검사 기능을 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 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 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.

관련 주제

- 8-7 페이지의 클러스터 제어 링크 크기 조정
- 8-3 페이지의 부트스트랩 컨피그레이션
- 8-24 페이지의 클러스터링으로 지원되지 않는 기능

- 9-19 페이지의 EtherChannel 구성
- 9-12 페이지의 EtherChannel 지침

ASA 클러스터의 기본값

- Spanned EtherChannel을 사용할 경우, cLACP 시스템 ID가 자동 생성되며 시스템 우선순위는 기본적으로 1입니다.
- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다.
- 연결 재밸런싱은 기본적으로 비활성화되어 있습니다. 연결 재밸런싱을 활성화할 경우 로드 정보를 교환하는 데 걸리는 기본 시간은 5초입니다.

ASA 클러스터링 구성

참고 클러스터링을 활성화하거나 비활성화하려면 콘솔 연결(CLI용) 또는 ASDM 연결을 사용해야 합니다.

클러스터링을 구성하려면 다음 작업을 수행합니다.

1단계 8-31 페이지의 ASA 클러스터링의 사전 요구 사항 및 8-33 페이지의 ASA 클러스터링 지침에 따라 스위치와 ASA에 대한 사전 컨피그레이션을 모두 완료합니다.

2단계 8-36 페이지의 클러스터 유닛 케이블 연결 및 업스트림/다운스트림 장비 구성

3단계 8-38 페이지의 각 유닛의 마스터 유닛에서 구성. 클러스터링의 인터페이스 유형은 Spanned EtherChannel 또는 개별 인터페이스 중 한 가지로만 구성할 수 있습니다.

4단계 8-39 페이지의 마스터 유닛의 인터페이스 구성. 인터페이스가 클러스터링을 수행할 준비가 되어 있지 않은 경우 클러스터링을 사용할 수 없습니다.

5단계 8-46 페이지의 마스터 유닛 부트스트랩 설정 구성

6단계 8-51 페이지의 슬레이브 유닛 부트스트랩 설정 구성

7단계 마스터 유닛에 대한 보안 정책을 구성합니다. 마스터 유닛에서 지원되는 기능을 구성하려면 이 가이드의 해당 장을 참조하십시오. 컨피그레이션은 슬레이브 유닛에 복제됩니다.

클러스터 유닛 케이블 연결 및 업스트림/다운스트림 장비 구성

클러스터링을 구성하기 전에 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.

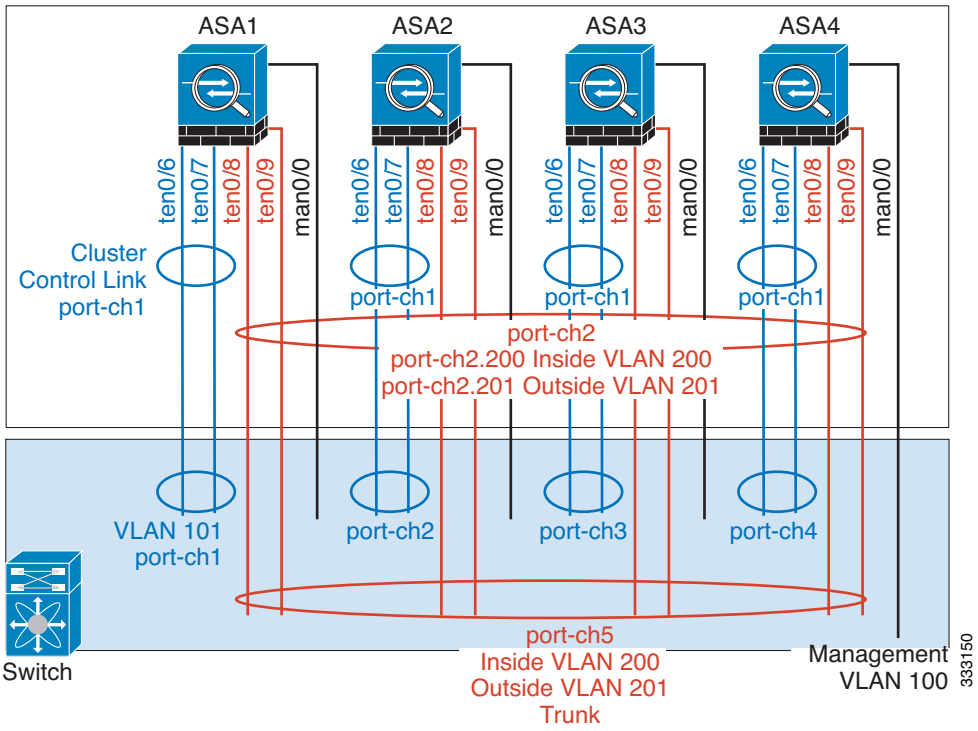
예

참고 이 예에서는 로드 밸런싱에 EtherChannel을 사용합니다. PBR 또는 ECMP를 사용할 경우 스위치 컨피그레이션이 달라집니다.

각각 4개의 ASA 5585-X에서 다음과 같은 기능을 사용하는 것으로 가정해 보겠습니다.

- 클러스터 제어 링크에 대한 디바이스-로컬 EtherChannel에서 10기가비트 이더넷 인터페이스 2개
- 내부 및 외부 네트워크에 대한 Spanned 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 각각의 TenGigabitEthernet 0/6 및 TenGigabitEthernet 0/7 쌍은 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 ASA 전반에 걸쳐). 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 유닛의 마스터 유닛에서 구성

클러스터링의 인터페이스 유형은 Spanned EtherChannel 또는 개별 인터페이스 중 한 가지로만 구성할 수 있으며, 클러스터에서 여러 인터페이스 유형을 함께 사용할 수 없습니다.

시작하기 전에

- 클러스터에 추가할 각각의 ASA에 모드를 별도로 설정해야 합니다.
- 관리 전용 인터페이스는 항상 개별 인터페이스로 구성할 수 있으며(권장), Spanned EtherChannel 모드에서도 마찬가지입니다. 투명 방화벽 모드에서도 관리 인터페이스는 개별 인터페이스가 될 수 있습니다.
- Spanned EtherChannel 모드에서 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 라우팅을 사용해야 합니다.
- 다중 컨텍스트 모드에서는 모든 컨텍스트에 한 가지 인터페이스 유형을 선택해야 합니다. 예를 들어, 투명 및 라우팅 모드 컨텍스트를 함께 선택한 경우 투명 모드에는 한 가지 인터페이스 유형만 허용되므로 모든 컨텍스트에 Spanned EtherChannel 모드를 사용해야 합니다.

절차

1단계 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**

예:

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

2단계 클러스터링에 대한 인터페이스 모드를 설정합니다.

```
cluster interface-mode {individual | spanned} force
```

예:

```
ciscoasa(config)# cluster interface-mode spanned force
```

기본 설정은 없으며, 모드를 명시적으로 선택해야 합니다. 모드를 설정하지 않을 경우 클러스터링을 사용할 수 없습니다.

강제 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, **강제** 옵션을 사용하여 최소한 기존 컨피그레이션에서 시작하는 방법을 권장합니다. 자세한 지침을 보려면 모드를 설정한 후 **세부 정보 확인** 옵션을 다시 실행합니다.

강제 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 컨피그레이션원과 동기화하는 것이 좋습니다.

이 섹션에서는 클러스터링과 호환되는 인터페이스를 구성하는 방법에 대해 설명합니다. 데이터 인터페이스를 Spanned EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 각 방법에서는 다양한 로드 밸런싱 메커니즘을 사용합니다. Spanned EtherChannel 모드에서도 개별 인터페이스가 될 수 있는 관리 인터페이스를 제외하고는 같은 컨피그레이션에 두 가지 유형을 모두 구성할 수 없습니다.

- 8-39 페이지의 개별 인터페이스 구성(관리 인터페이스 권장 사항)
- 8-42 페이지의 Spanned EtherChannel 구성

관련 주제

- 8-4 페이지의 클러스터 인터페이스

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 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다.

Spanned EtherChannel 모드의 경우 관리 인터페이스를 개별 인터페이스로 구성하는 방법을 권장합니다. 개별 인터페이스를 사용하면 필요한 경우 각 유닛에 직접 연결할 수 있는 반면, Spanned EtherChannel 인터페이스의 경우에는 현재 마스터 유닛에 대한 연결만 가능합니다.

시작하기 전에

- 관리 전용 인터페이스를 제외하고, 개별 인터페이스 모드를 사용해야 합니다.
- 다중 컨텍스트 모드의 경우, 각 컨텍스트에서 이러한 절차를 수행합니다. 현재 컨텍스트 컨피그레이션 모드에 있지 않은 경우, Configuration > *Device List* 창 changeto context name 명령을 입력합니다.
- 개별 인터페이스는 인접 디바이스의 로드 밸런싱을 구성해야 합니다. 관리 인터페이스에는 외부 로드 밸런싱이 필요하지 않습니다.
- (선택 사항) 인터페이스를 디바이스-로컬 EtherChannel, 이중화 인터페이스로 구성하거나 하위 인터페이스로 구성합니다.
  - EtherChannel의 경우 이러한 EtherChannel은 유닛에 대해 로컬이며 Spanned EtherChannel이 아닙니다.
  - 관리 전용 인터페이스는 이중화 인터페이스가 될 수 없습니다.

절차

1단계 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*

예:

```
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 마스터 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.

2단계 인터페이스 컨피그레이션 모드로 들어갑니다.

interface *interface_id*

예:

```
ciscoasa(config)# interface tengigabitethernet 0/8
```

3단계 (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 Spanned인 경우 이 설정이 필요합니다.

4단계 인터페이스 이름을 지정합니다.

nameif *name*

예:

```
ciscoasa(config-if)# nameif inside
```

*name*은 최대 48자의 텍스트이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다.

5단계 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*

예:

```
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 컨피그레이션은 지원되지 않습니다. 수동으로 IP 주소를 구성해야 합니다.

6단계 보안 수준을 설정합니다. 입력할 *숫자*는 0(가장 낮음)에서 100(가장 높음) 사이의 정수입니다.

security-level *number*

예:

```
ciscoasa(config-if)# security-level 100
```

7단계 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
```

관련 주제

- 8-11 페이지의 관리 인터페이스
- 8-38 페이지의 각 유닛의 마스터 유닛에서 구성
- 8-12 페이지의 로드 밸런싱 방법
- 9-19 페이지의 EtherChannel 구성
- 9-17 페이지의 이중화 인터페이스 구성
- 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹
- 11-1 페이지의 보안 레벨

Spanned EtherChannel 구성

Spanned EtherChannel은 클러스터의 모든 ASA를 포괄하며, EtherChannel이 실행되는 과정의 일환으로 로드 밸런싱을 제공합니다.

시작하기 전에

- Spanned EtherChannel 인터페이스 모드에 있어야 합니다.
- 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 시작합니다. 현재 시스템 컨피그레이션 모드에 있지 않은 경우.
- 투명 모드의 경우 브릿지 그룹을 구성합니다.
- EtherChannel에서는 최대 및 최소 링크를 지정하지 *마십시오*. EtherChannel에서는 ASA 또는 스위치에 최대 및 최소 링크를 지정하지 않는 것이 좋습니다(**lacp max-bundle** 및 **port-channel min-bundle** 명령). 사용해야 하는 경우 다음 사항을 주의하십시오.
  - ASA에 설정되는 최대 링크는 전체 클러스터의 총 활성 포트 개수입니다. 스위치에 구성된 최대 링크 값이 ASA 값보다 크지 않은지 확인하십시오.
  - ASA에 설정된 최소 링크는 *유닛당* 포트 채널 인터페이스를 가져오는 최소 활성 포트입니다. 스위치의 최소 링크는 클러스터 전체의 최소 링크이므로 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 있기 때문입니다.
- **lacp port-priority** 및 **lacp system-priority** 명령은 Spanned EtherChannel에 사용되지 않습니다.
- Spanned EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 작동하지 않습니다. 이러한 요구 사항으로 인해 클러스터의 활성 유닛이 아닌 유닛에는 트래픽이 전달되지 않습니다.

절차

1단계 채널 그룹에 추가할 인터페이스를 지정합니다.

interface *physical_interface*

예:

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID에는 유형, 슬롯, 포트 번호가 *유형 슬롯/포트*로 포함됩니다. 채널 그룹의 첫 번째 인터페이스는 그룹에 있는 모든 기타 인터페이스의 유형과 속도를 결정합니다.

2단계 이 인터페이스를 EtherChannel에 할당합니다.

channel-group *channel_id* **mode active** [**vss-id** {**1** | **2**}]

예:

```
ciscoasa(config-if)# channel-group 1 mode active
```

*channel_id*는 1에서 48까지의 숫자입니다. 이 채널 ID의 포트 채널 인터페이스가 아직 컨피그레이션에 없는 경우, 자동으로 추가됩니다.

interface port-channel *channel_id*

Spanned 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 인터페이스에는 **port-channel span-cluster vss-load-balance** 명령을 사용해야 합니다.

3단계 인터페이스를 활성화합니다.

no shutdown

4단계 (선택 사항) 1단계~3단계단계를 반복하여 EtherChannel에 추가 인터페이스를 추가합니다.

예:

```
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 Spanned 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. 스탠바이 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 Spanned EtherChannel의 인터페이스는 총 32개입니다.

5단계 포트 채널 인터페이스를 지정합니다.

interface port-channel *channel_id*

예:

```
ciscoasa(config)# interface port-channel 1
```

이 인터페이스는 채널 그룹에 인터페이스를 추가할 경우 자동으로 생성된 것입니다.

6단계 이 EtherChannel을 Spanned EtherChannel로 설정합니다.

port-channel span-cluster [**vss-load-balance**]

예:

```
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 보장합니다. 로드 밸런싱을 활성화하기 전에 **channel-group** 명령에서 **vss-id** 키워드를 각 멤버 인터페이스에 대해 구성해야 합니다(2단계 참조).

7단계 (선택 사항) 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.

8단계 (선택 사항) 이러한 EtherChannel에 VLAN 하위 인터페이스를 생성하려면 지금 수행하십시오.

예:

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

이 절차의 나머지는 하위 인터페이스에 적용됩니다.

9단계 (다중 컨텍스트 모드) 컨텍스트에 인터페이스를 할당합니다. 그리고 다음과 같이 입력합니다.

changeto context *name*
interface port-channel *channel_id*

예:

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

다중 컨텍스트 모드의 경우, 각 컨텍스트에서 인터페이스 컨피그레이션의 나머지 부분이 이루어집니다.

10단계 인터페이스 이름을 지정합니다.

nameif *name*

예:

```
ciscoasa(config-if)# nameif inside
```

*name*은 최대 48자의 텍스트이며 대/소문자를 구분하지 않습니다. 이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다.

11단계 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.

- 투명 모드 — 브릿지 그룹에 인터페이스를 할당합니다.

  bridge-group *number*

  예:

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

*숫자*는 1에서 100까지의 정수입니다. 최대 4개의 인터페이스를 하나의 브리지 그룹에 지정할 수 있습니다. 동일한 인터페이스를 둘 이상의 브리지 그룹에 지정할 수 없습니다. BVI 컨피그레이션에는 IP 주소가 포함되어 있습니다.

12단계 보안 수준을 설정합니다.

security-level *number*

예:

```
ciscoasa(config-if)# security-level 50
```

*숫자*는 0(가장 낮음)에서 100(가장 높음)까지의 정수입니다.

13단계 Spanned EtherChannel의 MAC 주소를 구성하여 현재 마스터 유닛이 클러스터를 벗어날 경우 MAC 주소가 변경되지 않도록 합니다.

mac-address *mac_address*

예:

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

수동 구성된 MAC 주소를 사용할 경우, 해당 MAC 주소가 현재 마스터 유닛에 유지됩니다. 다중 컨텍스트 모드에서 컨텍스트 간에 인터페이스를 공유할 경우, 기본적으로 MAC 자동 생성이 활성화됩니다. 따라서 자동 생성을 비활성화한 경우 공유 인터페이스의 MAC 주소를 수동으로 설정하기만 하면 됩니다. 공유되지 않는 인터페이스의 MAC 주소는 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.

관련 주제

- 8-38 페이지의 각 유닛의 마스터 유닛에서 구성
- 12-6 페이지의 브리지 그룹 구성
- 8-46 페이지의 마스터 유닛 부트스트랩 설정 구성
- 9-19 페이지의 EtherChannel 구성
- 9-12 페이지의 EtherChannel 지침
- 8-14 페이지의 VSS 또는 vPC에 연결
- 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성
- 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹
- 6-19 페이지의 보안 컨텍스트 구성
- 11-1 페이지의 보안 레벨
- 8-33 페이지의 ASA 클러스터링 지침

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

- 클러스터링을 활성화하거나 비활성화하려면 콘솔 포트를 사용해야 합니다. 텔넷이나 SSH는 사용할 수 없습니다.
- 향후 클러스터에서 벗어나려는 경우 컨피그레이션을 백업한 후 해당 컨피그레이션을 복원해야 합니다.
- 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 완료하십시오. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.
- 클러스터 제어 링크에 사용하려면 점보 프레임 예약을 활성화하는 것이 좋습니다.
- 클러스터 제어 링크를 제외하고, 컨피그레이션의 모든 인터페이스는 클러스터링을 활성화하기 전에 인터페이스 모드에 따라 클러스터 IP 풀 또는 Spanned EtherChannel로 구성해야 합니다. 기존의 인터페이스 컨피그레이션이 있는 경우, 클러스터링을 활성화하기 전에 해당 인터페이스 컨피그레이션을 지우거나(**clear configure interface**) 인터페이스를 클러스터 인터페이스로 변환할 수 있습니다.
- 실행 중인 클러스터에 유닛을 추가할 경우, 일시적이고 제한적으로 패킷/연결이 감소할 수 있으며 이는 정상적인 동작입니다.
- 클러스터 제어 링크의 크기를 결정합니다.

절차

1단계 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 컨피그레이션은 마스터 유닛에서 슬레이브 유닛으로 복제되지 않지만, 각 유닛에는 동일한 컨피그레이션을 사용해야 합니다. 이 컨피그레이션은 복제되지 않으므로, 각 유닛에 클러스터 제어 링크 인터페이스를 별도로 구성해야 합니다.

- VLAN Subinterface는 클러스터 제어 링크로 사용할 수 없습니다.
- 관리 *x/x* 인터페이스는 단독으로든 EtherChannel로든 클러스터 제어 링크로 사용할 수 없습니다.
- ASA IPS 모듈이 포함된 ASA 5585-X의 경우, 클러스터 제어 링크에 모듈 인터페이스를 사용할 수 없습니다.

a. 인터페이스 컨피그레이션 모드로 들어갑니다.

interface *interface_id*

예:

```
ciscoasa(config)# interface tengigabitethernet 0/6
```

b. (EtherChannel의 선택 사항) 이 물리적 인터페이스를 EtherChannel에 할당합니다.

channel-group *channel_id* **mode on**

예:

```
ciscoasa(config-if)# channel-group 1 mode on
```

*channel_id*는 1에서 48까지의 숫자입니다. 이 채널 ID의 포트 채널 인터페이스가 아직 컨피그레이션에 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 필요 없습니다. **참고:** 액티브 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.

예:

```
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

2단계 (선택 사항) 클러스터 제어 링크 인터페이스의 최대 전송 유닛을 지정합니다.

mtu cluster *bytes*

예:

```
ciscoasa(config)# mtu cluster 9000
```

MTU를 64에서 65,535바이트 사이로 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 컨피그레이션 명령일 뿐만 아니라 유닛 간에 복제되지 않은 부트스트랩 컨피그레이션의 일부입니다.

3단계 클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드로 들어갑니다.

cluster group *name*

예:

```
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.

4단계 이 클러스터 멤버의 이름을 지정하십시오.

local-unit *unit_name*

```
ciscoasa(cfg-cluster)# local-unit unit1
```

1~38자로 된 고유한 ASCII 문자열을 사용합니다. 각 유닛에는 고유한 이름이 있어야 합니다. 이름이 중복된 유닛은 클러스터에서 사용할 수 없습니다.

5단계 클러스터 제어 링크 인터페이스를 지정하며, EtherChannel이 권장됩니다.

cluster-interface *interface_id* **ip** *ip_address mask*

예:

```
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.

6단계 마스터 유닛 선택을 위해 이 유닛의 우선순위를 설정합니다.

priority *priority_number*

예:

```
ciscoasa(cfg-cluster)# priority 1
```

우선순위는 1에서 100까지이며 1의 우선순위가 가장 높습니다.

7단계 (선택 사항) 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 설정합니다.

key *shared_secret*

예:

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

공유 비밀은 1~63자로 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.

8단계 (선택 사항) 유닛 검사 모니터링 및 인터페이스 상태 모니터링이 포함된 클러스터 상태 검사 기능을 맞춤화합니다.

health-check [**holdtime** *timeout*] [**vss-enabled**]

예:

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

대기 시간은 유닛 간의 keepalive 상태 메시지 시간 간격을 0.8초에서 45초 사이로 지정하며, 기본값은 3초입니다. 대기 시간 값은 *유닛* 상태 검사에만 영향을 미칩니다. 인터페이스 상태의 경우 ASA에서는 인터페이스 상태(가동 또는 중지)를 사용합니다.

유닛 상태를 확인하기 위해 ASA 클러스터 유닛에서는 다른 유닛에 대한 클러스터 제어 링크에 keepalive 메시지를 보냅니다. 피어 유닛의 keepalive 메시지가 대기 시간 내에 유닛에 전송되지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주합니다. 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 대기 시간 제한을 낮은 값으로 설정한 경우(0.8초) 클러스터에서 ASA가 잘못 제거될 수 있으며 ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다. **vss-enabled**를 활성화할 경우, ASA에서는 하나 이상의 스위치에 keepalive 메시지가 전송되도록 하기 위해 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 대량의 keepalive 메시지를 보냅니다.

인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 특정 유닛의 인터페이스에 오류가 발생하였으나 다른 유닛의 동일한 인터페이스는 활성 상태인 경우, 클러스터에서 해당 특정 유닛이 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다.

상태 검사는 기본적으로 활성화되어 있습니다. 이 명령의 **no** 형식을 사용하여 이 기능을 비활성화할 수 있습니다.

토폴로지에 변경 사항이 발생할 경우(예: 데이터 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 생성) 상태 검사 기능을 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.

9단계 (선택 사항) TCP 트래픽을 위해 연결 재밸런싱을 활성화합니다.

conn-rebalance [**frequency** *seconds*]

예:

```
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 5초입니다.

사이트 간 토폴로지에 대한 연결 재밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 대한 연결이 재밸런싱됩니다.

10단계 (선택 사항) 슬레이브 유닛에서 마스터 유닛으로 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.

11단계 (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 Spanned EtherChannel 멤버를 지원하는 것이 허용되므로 최대 32개의 멤버를 지원할 수 있습니다. 이 명령을 사용하지 않을 경우 8개의 활성 멤버 및 8개의 스탠바이 멤버만 지원됩니다. 이 명령을 활성화할 경우 스탠바이 멤버를 사용할 수 없으며 모든 멤버가 활성 상태로 됩니다.

12단계 (선택 사항) cLACP 시스템 ID 및 시스템 우선순위를 수동으로 지정합니다.

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

예:

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

Spanned EtherChannel을 사용할 경우 ASA에서는 cLACP를 사용하여 EtherChannel과 인접 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 슬레이브에 복제됩니다. 또는 *H.H.H* 형식으로 이러한 명령을 통해 수동으로 지정됩니다. 여기서 H는 16비트로 된 16진수를 의미합니다. (예를 들어 MAC 주소 00-0A-00-00-AA-AA는 000A.0000.AAAA로 입력됩니다.) 예를 들어, 문제 해결을 위해 MAC 주소를 수동으로 구성하려는 경우 식별하기 쉬운 MAC 주소를 사용할 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 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다. 그러나 클러스터링을 활성화한 후에는 이 값을 변경할 수 없습니다.

13단계 클러스터링을 활성화합니다.

enable [**noconfirm**]

예:

```
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 컨피그레이션을 검사하여 클러스터링에서 지원되지 않는 기능에 대한 호환되지 않는 명령을 확인하며, 여기에는 기본 컨피그레이션에 없을 수 있는 명령이 포함됩니다. 호환되지 않는 명령을 삭제하라는 메시지가 표시됩니다. **No**를 선택하면 클러스터링이 활성화되지 않습니다. 확인을 우회하고 호환되지 않는 명령을 자동으로 삭제하려면 **noconfirm** 키워드를 사용합니다.

활성화된 첫 번째 유닛을 대상으로 마스터 유닛 선택이 이루어집니다. 첫 번째 유닛은 현재로서 클러스터의 유일한 멤버이므로, 마스터 유닛이 됩니다. 이 기간에는 어떠한 컨피그레이션도 변경하지 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. 이 유닛은 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
```

관련 주제

- 9-24 페이지의 점보 프레임 지원 활성화
- 8-39 페이지의 마스터 유닛의 인터페이스 구성
- 8-7 페이지의 클러스터 제어 링크 크기 조정
- 8-3 페이지의 마스터 유닛 선택
- 8-9 페이지의 인터페이스 모니터링
- 8-55 페이지의 클러스터 벗어나기

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 컨피그레이션을 백업한 후 해당 컨피그레이션을 복원해야 합니다.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.
- 클러스터 제어 링크에 사용하려면 점보 프레임 예약을 활성화하는 것이 좋습니다.
- 컨피그레이션에 클러스터링이 구성되지 않은 인터페이스가 있는 경우(예: 기본 컨피그레이션 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 감소할 수 있으며 이는 정상적인 동작입니다.

절차

1단계 마스터 유닛에 설정한 것과 동일한 클러스터 제어 링크 인터페이스를 구성합니다.

예:

```
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
```

2단계 마스터 유닛에 구성한 것과 동일한 MTU를 지정합니다.

예:

```
ciscoasa(config)# mtu cluster 9000
```

3단계 마스터 유닛에 구성한 것과 동일한 클러스터 이름을 식별합니다.

예:

```
ciscoasa(config)# cluster group pod1
```

4단계 고유한 문자열로 이 클러스터 멤버의 이름을 지정합니다.

local-unit *unit_name*

예:

```
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.

5단계 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*

예:

```
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.

6단계 마스터 유닛 선택을 위해 이 유닛의 우선순위를 지정합니다. 일반적으로 마스터 유닛보다 숫자가 커야 합니다.

priority *priority_number*

예:

```
ciscoasa(cfg-cluster)# priority 2
```

우선순위를 1에서 100까지 설정하며, 1의 우선순위가 가장 높습니다.

7단계 마스터 유닛에 설정한 동일한 인증 키를 설정합니다.

예:

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

8단계 클러스터링을 활성화합니다.

enable as-slave

enable as-slave 명령을 사용하여 컨피그레이션 비호환성(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. 슬레이브의 컨피그레이션은 마스터 유닛에서 동기화된 컨피그레이션으로 덮어쓰기 됩니다.

클러스터링을 비활성화하려면 **no enable** 명령을 입력합니다.

참고 클러스터링을 비활성화할 경우, 모든 데이터 인터페이스가 종료되며 관리 인터페이스만 활성 상태가 됩니다.

예

다음 예에는 슬레이브 유닛인 unit2에 대한 컨피그레이션이 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
```

관련 주제

- 9-24 페이지의 점보 프레임 지원 활성화
- 8-3 페이지의 마스터 유닛 선택
- 8-55 페이지의 클러스터 벗어나기

ASA 클러스터 구성원 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 컨피그레이션원을 관리할 수 있습니다.

- 8-53 페이지의 구성원 비활성화
- 8-54 페이지의 마스터 유닛의 구성원
- 8-55 페이지의 클러스터 벗어나기
- 8-56 페이지의 마스터 유닛 변경
- 8-57 페이지의 클러스터 전체에 명령 실행

구성원 비활성화

클러스터의 컨피그레이션원을 비활성화하려면, 클러스터링 컨피그레이션은 그대로 유지한 상태로 유닛의 클러스터링을 비활성화합니다.

참고 ASA가 비활성화되면(수동으로 또는 상태 검사 오류를 통해) 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 인터페이스에

서는 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.

시작하기 전에

- 콘솔 포트를 사용해야 합니다. 원격 CLI 연결에서는 클러스터링을 활성화하거나 비활성화할 수 없습니다.
- 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 현재 시스템 컨피그레이션 모드에 있지 않은 경우, .

절차

1단계 클러스터 컨피그레이션 모드로 들어갑니다.

cluster group *name*

예:

```
ciscoasa(config)# cluster group pod1
```

2단계 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.

관련 주제

- 8-55 페이지의 클러스터 벗어나기

마스터 유닛의 구성원

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 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.

시작하기 전에

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 현재 시스템 컨피그레이션 모드에 있지 않은 경우, .

절차

1단계 클러스터에서 유닛을 제거합니다.

cluster remove unit *unit_name*

예:

```
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 컨피그레이션뿐만 아니라 마스터 유닛에서 동기화된 최종 컨피그레이션도 그대로 유지되므로, 컨피그레이션이 손실되는 일 없이 유닛을 나중에 다시 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.

관련 주제

- 8-55 페이지의 클러스터 벗어나기

클러스터 벗어나기

클러스터를 모두 벗어나려는 경우, 전체 클러스터 부트스트랩 컨피그레이션을 제거해야 합니다. 각 컨피그레이션원에 대한 현재 컨피그레이션이 동일하므로(마스터 유닛에서 동기화됨), 클러스터를 벗어날 경우 백업에서 사전 클러스터링 컨피그레이션을 복원하거나, IP 주소 충돌을 피하려면 컨피그레이션을 지우고 처음부터 다시 시작하게 됩니다.

시작하기 전에

콘솔 포트를 사용해야 합니다. 클러스터 컨피그레이션을 제거하면 관리 인터페이스 및 클러스터 제어 링크를 비롯한 모든 인터페이스가 종료됩니다. 또한 원격 CLI 연결에서는 클러스터링을 활성화하거나 비활성화할 수 없습니다.

절차

1단계 슬레이브 유닛의 클러스터링을 비활성화합니다.

cluster group *cluster_name*
no enable

예:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

슬레이브 유닛에 클러스터링이 활성화되어 있는 동안에는 컨피그레이션을 변경할 수 없습니다.

2단계 클러스터 컨피그레이션을 지웁니다.

clear configure cluster

ASA에서는 관리 인터페이스 및 클러스터 제어 링크를 비롯한 모든 인터페이스를 종료합니다.

3단계 클러스터 인터페이스 모드를 비활성화합니다.

no cluster interface-mode

모드는 컨피그레이션에 저장되지 않으며 수동으로 재설정해야 합니다.

4단계 백업 컨피그레이션이 있을 경우, 실행 중인 컨피그레이션에 백업 컨피그레이션을 복사합니다.

copy *backup_cfg* **running-config**

예:

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

5단계 시작에 컨피그레이션을 저장합니다.

write memory

6단계 백업 컨피그레이션이 없는 경우 관리 액세스를 다시 구성합니다. 인터페이스 IP 주소를 변경하고 이를테면 올바른 호스트 이름을 복원해야 합니다.

관련 주제

- 2 장, "시작하기"

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 수행하십시오.

시작하기 전에

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 현재 시스템 컨피그레이션 모드에 있지 않은 경우, .

절차

1단계 새 유닛을 마스터 유닛으로 설정합니다.

cluster master unit *unit_name*

예:

```
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 정보** 명령을 입력합니다.

관련 주제

- 8-53 페이지의 구성원 비활성화
- 8-25 페이지의 클러스터링을 위한 중앙 집중식 기능

클러스터 전체에 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.

절차

1단계 모든 멤버 또는 유닛 이름을 지정한 경우 특정 멤버에 명령을 전송합니다.

cluster exec [**unit** *unit_name*] *command*

예:

```
ciscoasa# cluster exec show xlate
```

멤버 이름을 보려면 **cluster exec unit ?** 을 입력하거나(현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info 정보** 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. 대상 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
primary(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)
 secondary:*********************************************************************
 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 commands를 참조하십시오.

- **show cluster info [health]**

  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 내용은 다음 출력을 참조하십시오.

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Version   : 100.8(0.52)
      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
      Version   : 100.8(0.52)
      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
      Version   : 100.8(0.52)
      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
      Version   : 100.8(0.52)
      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 history**

  클러스터 내역을 보여줍니다.

클러스터 전체 패킷 캡처

클러스터의 패킷을 캡처하는 방법에 대한 내용은 다음 commands를 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.

관련 주제

- 38-1 페이지의 패킷 캡처

클러스터 리소스 모니터링

클러스터 리소스 모니터링에 대한 내용은 다음 commands를 참조하십시오.

show cluster {**cpu** | **memory** | **resource**} [*options*]

전체 클러스터의 취합된 데이터를 표시합니다. 사용 가능한 *옵션*은 데이터 유형에 따라 달라집니다.

클러스터 트래픽 모니터링

클러스터 트래픽 모니터링에 대한 내용은 다음 commands를 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 흐름이 어떤 방식으로 전송되는지 볼 수 있습니다. 클러스터의 처리량은 로드 밸런싱의 효율성과 컨피그레이션에 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** 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, 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, M - SMTP data, m - SIP media, n - GUP
            O - outbound data, P - inside back connection, p - Phone-proxy TFTP
            connection,
```

```
            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,
            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. 흐름에 관리자(Y), 백업(y), 전달자(z) 플래그가 있는지 살펴보십시오. 다음 예에는 3가지 전체 ASA의 SSH 연결이 172.18.124.187:22부터 192.168.103.131:44727까지 표시되어 있습니다. ASA 1에는 연결의 전달자 유닛을 의미하는 z 플래그가 있고, ASA3에는 연결의 관리자 유닛을 의미하는 Y 플래그가 있으며, ASA2에는 특별한 플래그가 없어 소유자 유닛임을 나타냅니다. 아웃바운드 방향의 경우, 이 연결에 대한 패킷은 ASA2의 내부 인터페이스로 들어오고 외부 인터페이스로 나갑니다. 인바운드 방향의 경우, 이 연결에 대한 패킷은 ASA 1 및 ASA3의 외부 인터페이스로 들어온 후 클러스터 제어 링크를 통해 ASA2로 전달된 다음 ASA2의 내부 인터페이스로 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**]

  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 재밸런싱 통계가 표시됩니다.

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  전체 클러스터의 취합된 데이터를 표시합니다. 사용 가능한 *옵션*은 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 유닛에 대해 사용 중인 연결의 개수를 취합하여 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.

관련 주제

- 연결 역할, 11~22페이지

클러스터 라우팅 모니터링

클러스터 라우팅 모니터링에 대한 내용은 다음 명령을 참조하십시오.

show route cluster

debug route cluster

라우팅에 대한 클러스터 정보를 표시합니다.

클러스터링의 로깅 구성

클러스터링의 로깅 구성에 대한 내용은 다음 commands를 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.

관련 주제

- 39-15 페이지의 디바이스 ID를 Non-EMBLEM 형식 Syslog 메시지에 포함

클러스터 인터페이스 모니터링

클러스터 인터페이스 모니터링에 대한 내용은 다음 명령을 참조하십시오.

- **show cluster interface-mode**

  클러스터 인터페이스 모드를 표시합니다.
- **show port-channel**

  포트 채널이 Spanned인지 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.

클러스터링 디버깅

클러스터링 디버깅에 대한 내용은 다음 명령을 참조하십시오.

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  클러스터링에 대한 디버그 메시지가 표시됩니다.
- **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 컨피그레이션이 포함되어 있습니다.

샘플 ASA 및 스위치 컨피그레이션

다음 샘플 컨피그레이션에서는 ASA와 스위치 간에 다음과 같은 인터페이스를 연결합니다.

ASA Interface	Switch Interface
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
```

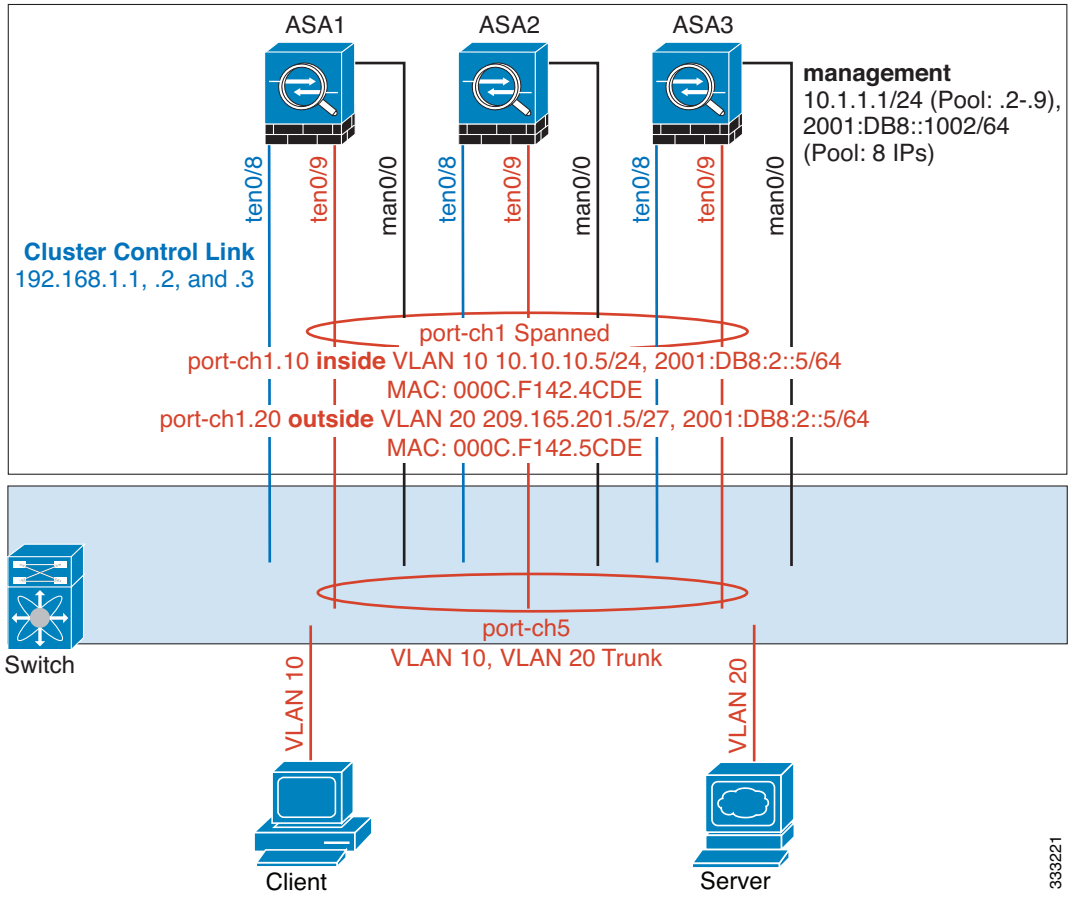
마스터 인터페이스 컨피그레이션

```
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 컨피그레이션

```
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.

Spanned EtherChannel을 사용할 경우, 모든 데이터 링크가 스위치 측의 단일한 EtherChannel로 그룹화됩니다. ASA를 사용할 수 없게 될 경우, 스위치에서 나머지 유닛 간의 트래픽을 재밸런싱합니다.

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
```

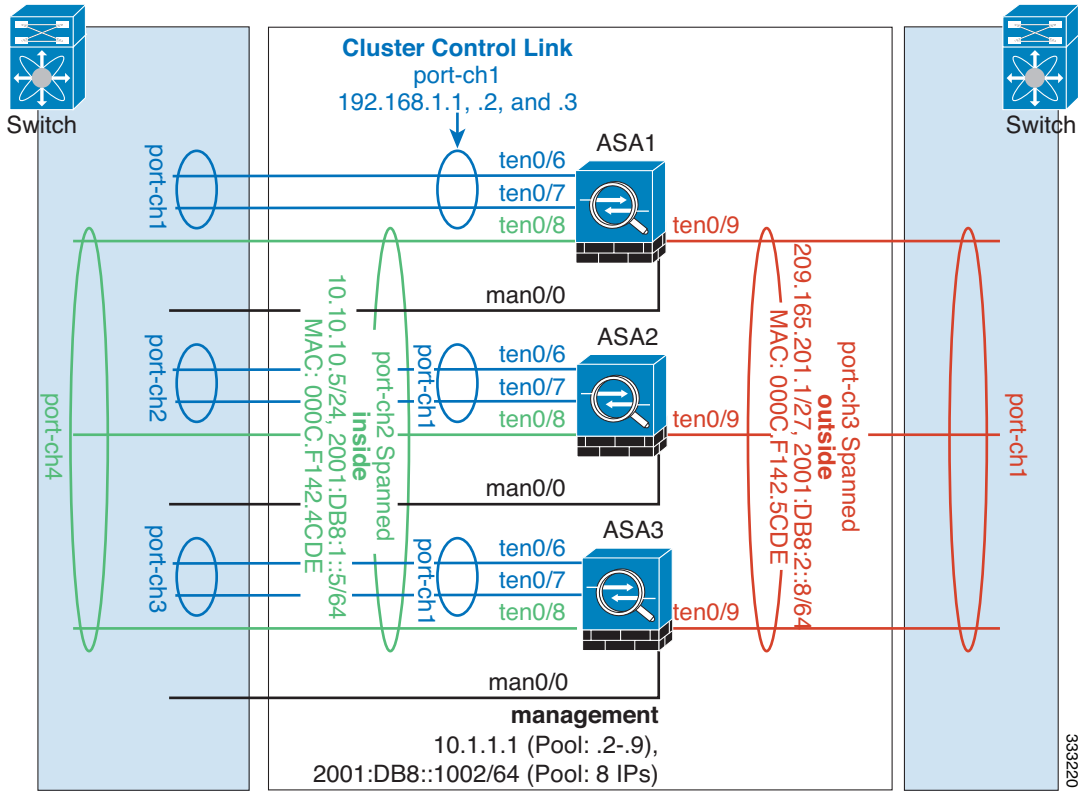
ASA3 슬레이브 부트스트랩 컨피그레이션

```
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 분리하고자 할 수 있습니다.

위의 다이어그램에 표시된 것과 같이, 왼쪽에는 내부 스위치에 연결되는 Spanned EtherChannel이 하나 있고 오른쪽에는 외부 스위치에 연결되는 Spanned 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
```

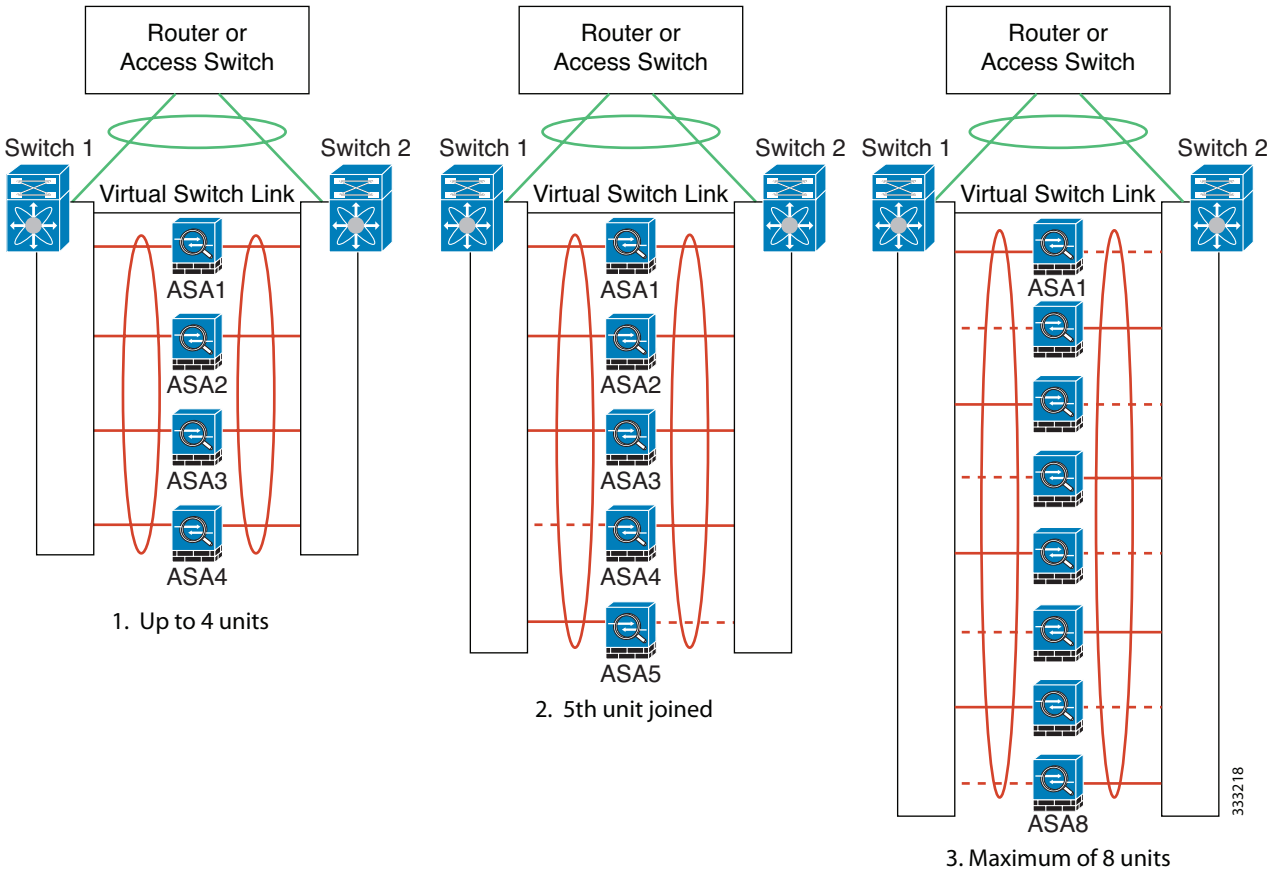
마스터 인터페이스 컨피그레이션

```
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
```

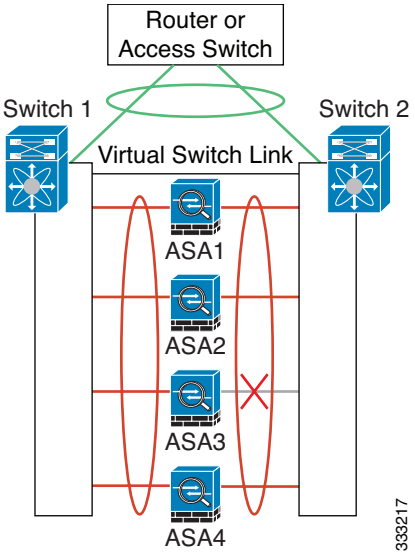
백업 링크가 포함된 Spanned EtherChannel(기존 8 액티브 포트/8 스탠바이)

기존 EtherChannel에서 활성 포트의 최대 개수는 스위치 측에서 8개로 제한됩니다. 8-ASA 클러스터가 있을 경우 유닛당 2개의 포트를 EtherChannel에 할당하며, 이렇게 하면 총 16개의 전체 포트 중 8개는 스탠바이 모드가 되어야 합니다. ASA에서는 LACP를 사용하여 어떤 링크를 활성화하거나 스탠바이 상태로 설정해야 하는지 협상을 수행합니다. VSS 또는 vPC를 사용하여 다중 스위치 EtherChannel을 활성화할 경우 스위치 간 이중화를 실현할 수 있습니다. ASA의 모든 물리적 포트는 우선 슬롯 번호를 기준으로, 그 다음에는 포트 번호를 기준으로 순서가 지정됩니다. 다음 그림에서 순서가 낮은 포트가 "기본" 포트(예: GigabitEthernet 0/0)이고, 다른 포트가 "보조" 포트(예: GigabitEthernet 0/1)입니다. 하드웨어 연결은 대칭을 이루어야 합니다. 모든 기본 링크는 하나의 스위치에서 종료되어야 하며, 모든 보조 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.

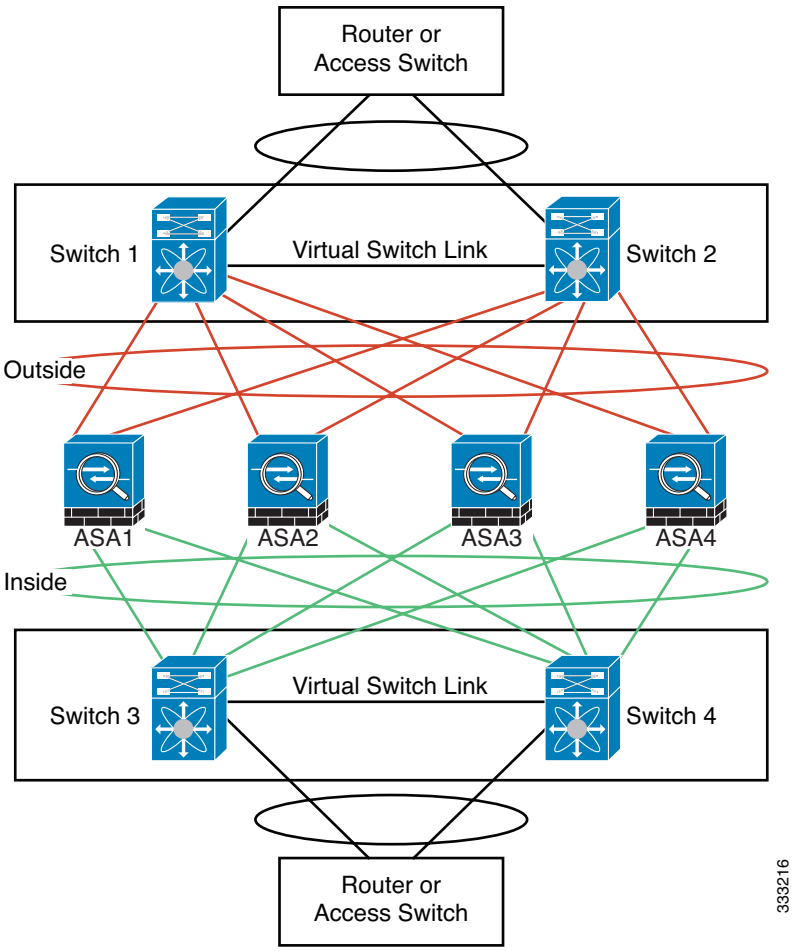


원칙적으로는 우선 채널에 있는 활성 포트의 수를 최대화하고, 그 다음에는 활성 기본 포트의 수와 활성 보조 포트의 수가 균형을 이루도록 유지하는 것입니다. 클러스터에 5번째 유닛이 참가할 경우 모든 유닛 간의 트래픽이 균일하게 조정되지 않습니다.

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 기본 및 보조 링크에 모두 오류가 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
```

ASA 클러스터링에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
ASA 5580 및 5585-X를 위한 ASA 클러스터링	9.0(1)	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. 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. 도입되거나 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**
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. 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 표시되지만, 스위치 측의 트래픽을 통과하지 않습니다. ASA 대기 시간 제한을 낮은 값으로 설정한 경우(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 하나 이상의 스위치에 keepalive 메시지가 전송되도록 하기 위해 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 대량의 keepalive 메시지를 보냅니다. 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
투명 모드의 경우 지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버 지원	9.2(1)	이제 투명 방화벽 모드에서 Spanned EtherChannel 모드를 사용할 경우 지리적으로 다른 위치에 클러스터 멤버를 배치할 수 있습니다. 라우팅 방화벽 모드에서 Spanned EtherChannel을 사용한 사이트 간 클러스터링은 지원되지 않습니다. 어떤 명령도 수정하지 않았습니다.
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 Spanned 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. 도입된 명령: **clacp static-port-priority**
Spanned EtherChannel에서 32개의 활성 링크 지원	9.2(1)	이제 ASA EtherChannel에서는 최대 16개의 활성 링크를 지원합니다. *Spanned* 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 Spanned EtherChannel에 16개의 활성 링크를 구성하면 됩니다(각 스위치에 8개씩 연결됨). 이전에는 VSS/vPC와 함께 사용해도 Spanned EtherChannel에서 8개의 활성 링크, 8개의 스탠바이 링크만 지원되었습니다. **참고** Spanned 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. 도입된 명령: **clacp static-port-priority**
ASA 5585-X에 클러스터 멤버 16개 지원	9.2(1)	이제 ASA 5585-X에서는 16-유닛 클러스터를 지원합니다. 어떤 명령도 수정하지 않았습니다.
ASA 클러스터링을 위한 BGP 지원	9.3(1)	ASA 클러스터링에서 BGP 지원을 추가했습니다. 도입된 명령: **bgp router-id clusterpool**

3 파 트

인터페이스스

9 장

기본 인터페이스 컨피그레이션 (ASA 5512-X 이상)

이 장에는 이더넷 설정, 이중화 인터페이스, EtherChannel을 비롯한 Cisco ASA 5512-X 이상 버전의 인터페이스 컨피그레이션을 시작하는 작업에 대한 내용이 포함되어 있습니다.

참고 다중 상황 모드의 경우, 시스템 실행 영역에서 모든 작업을 완료합니다. 상황 정보에서 시스템 실행 영역으로 변경하려면, **changeto system** 명령을 사용합니다..

특수한 요구 사항을 충족해야 하는 ASA 클러스터 인터페이스에 대한 내용은 8 장, "ASA 클러스터"를 참조하십시오.

ASA 5512-X 이상 버전의 인터페이스 컨피그레이션 시작에 대한 정보

자동 MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 자동 MDI/MDIX 기능도 포함됩니다. 자동 MDI/MDIX 기능을 사용하면 자동 협상 단계에서 직선형 케이블이 감지될 경우 내부 crossover를 수행하게 되므로 crossover 케이블을 연결할 필요가 없습니다. 자동 협상을 실행하여 인터페이스에 자동 MDI/MDIX 기능을 활성화하려면 속도 또는 양방향을 설정해야 합니다. 속도 및 양방향을 모두 명시적인 고정 값으로 설정할 경우, 두 설정에 대한 자동 협상이 비활성화되며 자동 MDI/MDIX 기능도 비활성화됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정할 경우, 인터페이스에서 항상 자동 협상이 실행되므로 자동 MDI/MDIX 기능도 활성화되며 이를 비활성화할 수 없습니다.

투명 모드의 인터페이스

투명 모드의 인터페이스는 "브릿지 그룹"에 속하며, 각 네트워크에 하나의 브릿지 그룹이 있습니다. 각 상황당 또는 단일 모드에서 인터페이스 4개당 최대 8개의 브릿지가 포함될 수 있습니다. 브릿지 그룹에 대한 자세한 내용은 12-1 페이지의 투명 모드의 브리지 그룹을 참조하십시오.

관리 인터페이스

관리 인터페이스 개요

다음에 연결하여 ASA를 관리할 수 있습니다.

- 통과 트래픽 인터페이스
- 전용 관리 *슬롯/포트* 인터페이스(모델에 제공되는 경우)

35 장, "관리 액세스"에 따라 인터페이스에 대한 관리 액세스를 구성해야 할 수 있습니다.

관리 *슬롯/포트* 인터페이스

표 9-1에는 모델당 관리 인터페이스가 나와 있습니다.

표 9-1 모델당 관리 인터페이스

모델	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	통과 트래픽의 구성 가능 요소[2]	하위 인터페이스 허용 여부
ASA 5512-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5515-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5525-X	예	아니요	아니요	아니요	아니요	아니요

표 9-1 모델당 관리 인터페이스

모델	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	통과 트래픽의 구성 가능 요소[2]	하위 인터페이스 허용 여부
ASA 5545-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5555-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5585-X	예	예	예[3]	예[3]	예	예
ASASM	아니요	아니요	아니요	아니요	N/A	N/A
ASAv	예	아니요	아니요	아니요	아니요	아니요

1. Management 0/0 인터페이스는 기본 공장 컨피그레이션에 포함되어 ASDM 액세스를 위해 구성됩니다. 자세한 내용은 2-12 페이지의 공장 기본 컨피그레이션을 참조하십시오.
2. 기본적으로 Management 0/0 인터페이스는 관리 전용 트래픽(**management-only** 명령)을 위해 구성됩니다. 라우팅 모드에서 지원되는 모델의 경우, 제한 사항을 제거하고 통과 트래픽을 전달할 수 있습니다. 모델이 추가 관리 인터페이스가 포함될 경우 이를 통과 트래픽에도 사용할 수 있습니다. 단, 관리 인터페이스가 통과 트래픽에 최적화되어 있지 않을 수 있습니다.
3. 슬롯 1에 SSP가 설치된 경우 Management 1/0 및 1/1에서는 슬롯 1의 SSP에만 관리 액세스를 제공합니다.

참고 모듈을 설치한 경우, 모듈 관리 인터페이스에서는 해당 모듈에만 관리 액세스를 제공합니다. ASA 5512-X부터 ASA 5555-X 버전까지 소프트웨어 모듈에서 사용하는 물리적 Management 0/0 인터페이스는 ASA와 동일합니다.

관리 전용 트래픽에 모든 인터페이스 사용

모든 인터페이스를 관리 트래픽용으로 구성하여 이를 관리 전용 인터페이스로 사용할 수 있으며 여기에는 EtherChannel 인터페이스가 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. 다른 기타 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다.

다중 상황 모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 상황에서 공유할 수 없습니다. 상황별 관리를 위해 관리 인터페이스의 하위 인터페이스를 만들고 각 상황에 관리 하위 인터페이스를 할당할 수 있습니다. ASA 5512-X부터 ASA 5555-X까지는 관리 인터페이스에서 하위 인터페이스를 지원하지 않습니다. 따라서 상황별 관리를 위해서는 데이터 인터페이스에 연결해야 합니다.

관리 인터페이스는 일반적인 브릿지 그룹에 포함되지 않습니다. 운영상의 용도로 인해 관리 인터페이스는 구성 불가능한 브릿지 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 두 가지 모두를 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않을 경우 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 *관리* 인터페이스를 사용하여 스위치에 액세스하도록 액세스 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.

이중화 관리 인터페이스 미지원

이중 인터페이스는 관리 *슬롯/포트* 인스턴스를 멤버로 지원하지 않습니다. 또한 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 없습니다.

ASA 5512-X~ASA 5555-X의 Management 0/0 인터페이스

ASA 5512-X부터 ASA 5555-X 버전까지 Management 0/0 인터페이스의 특징은 다음과 같습니다.

- 통과 트래픽을 지원하지 않음
- 하위 인터페이스를 지원하지 않음
- 우선순위 대기열을 지원하지 않음
- 멀티캐스트 MAC을 지원하지 않음
- 소프트웨어 모듈에서는 Management 0/0 인터페이스를 공유합니다. ASA 및 모듈에서는 별도의 MAC 주소와 IP 주소가 지원됩니다. 모듈 운영 체제 내에서 모듈 IP 주소의 컨피그레이션을 수행해야 합니다. 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다.

이중화 인터페이스

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 디바이스 수준 장애 조치를 구성할 수 있습니다.

이중화 인터페이스 MAC 주소

이중화 인터페이스에서는 맨 처음 추가되는 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 또는 멤버 인터페이스 MAC 주소에 관계없이 사용되는 이중화 인터페이스에 MAC 주소를 할당할 수 있습니다(11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성 또는 6-15 페이지의 다중 컨텍스트 모드 구성 참조). 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작하면 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

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.

- 9-5 페이지의 채널 그룹 인터페이스
- 9-5 페이지의 다른 디바이스에서 EtherChannel에 연결
- 9-6 페이지의 Link Aggregation Control Protocol
- 9-6 페이지의 로드 밸런싱
- 9-7 페이지의 EtherChannel MAC 주소

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.

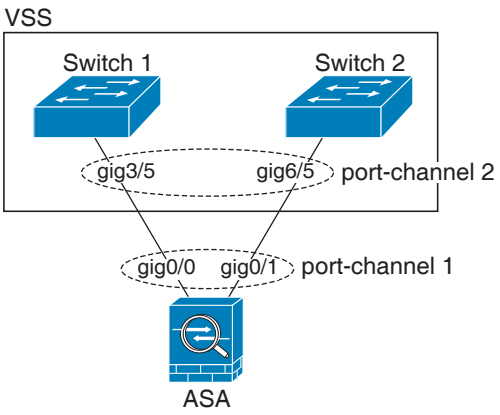
EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

다른 디바이스에서 EtherChannel에 연결

ASA EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어, Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.

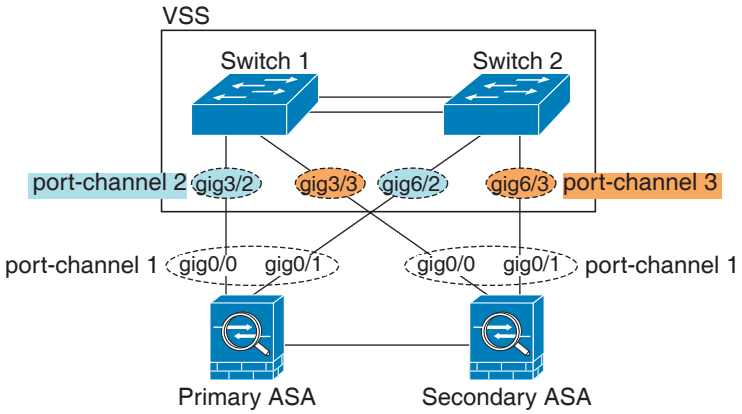
스위치가 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel)의 일부인 경우, 동일한 EtherChannel 내에서 ASA 인터페이스를 연결하여 VSS/vPC에서 스위치를 분리할 수 있습니다. 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버이므로 별도의 스위치는 단일 스위치 역할을 합니다(그림 9-1 참조).

그림 9-1 VSS/vPC에 연결



액티브/스탠바이 장애 조치 구축 시 ASA를 사용할 경우 VSS/vPC의 스위치에 각 ASA에 별도의 EtherChannel을 생성해야 합니다.(그림 9-1 참조). 각 ASA에서 단일한 EtherChannel은 두 스위치에 모두 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 9-2 액티브/스탠바이 장애 조치 및 VSS/vPC



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.

- Active — 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. 액티브 EtherChannel에서는 액티브 EtherChannel과의 연결만 설정할 수 있습니다.
- On — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 또 다른 "on" 상태의 EtherChannel과의 연결만 설정할 수 있습니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 컨피그레이션 오류를 처리하고 컨피그레이션원 인터페이스의 끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

로드 밸런싱

ASA에서는 패킷의 소스 및 목적지 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(이 조건은 구성 가능하며 9-21 페이지의 EtherChannel 맞춤화를 참조하십시오). 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 인터페이스가 되고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스 등으로 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.

클러스터링에서 Spanned EtherChannel의 경우 ASA 단위로 로드 밸런싱이 이루어집니다. 예를 들어, 8개의 ASA 전체에서 Spanned EtherChannel에 32개의 액티브 인터페이스가 있는 경우 EtherChannel의 ASA 하나당 인터페이스는 4개이며 ASA의 4개 인터페이스에만 로드 밸런싱이 실행됩니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 레이어 2의 스패닝 트리와 레이어 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

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 인터페이스에 고유한 MAC 주소를 자동으로 지정할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 다중 상황 모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그 다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

MTU 및 TCP 최대 세그먼트 크기로 조각화 제어

MTU 개요

MTU에서는 ASA가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, FCS 또는 VLAN 태깅이 *없는* 프레임 크기입니다. 이더넷 헤더는 14바이트이고 FCS는 4바이트입니다. MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더를 포함하여 1518바이트입니다. VLAN 태깅(4바이트가 더 추가됨)을 사용 중인 상태에서 MTU를 1500으로 설정할 경우 예상 프레임 크기는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오. MTU 설정을 변경하는 대신 MTU 최대 세그먼트 크기를 변경하여 캡슐화를 위한 TCP 헤더를 수용하는 방법에 대한 자세한 내용은 9-8 페이지의 TCP 최대 세그먼트 크기 개요를 참조하십시오.

발신 IP 패킷이 지정된 MTU보다 큰 경우 해당 패킷은 2개 이상의 프레임으로 분할됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

참고 ASA에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다. 큰 프레임을 지원하기 위해 메모리를 늘리는 방법은 9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오.

기본 MTU

ASA의 기본 MTU는 1500바이트입니다. 이 값에는 18바이트 이상의 이더넷 헤더, CRC, VLAN 태깅 등이 포함되지 않습니다.

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.

MTU 및 점보 프레임 설정

11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오. 다중 상황 모드의 경우, 각 상황 내에서 MTU를 설정합니다.

9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오. 다중 상황 모드의 경우 시스템 실행 영역에서 점보 프레임 지원을 설정합니다.

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 경우, MTU를 최대 9198바이트까지 설정할 수 있습니다.

TCP 최대 세그먼트 크기 개요

TCP MSS(TCP 최대 세그먼트 크기)는 TCP 헤더가 추가되기 *전의* TCP 페이로드의 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

ASA에서 TCP MSS를 설정할 수 있습니다. 연결의 엔드포인트에서 ASA에 설정된 값보다 큰 TCP MSS를 요청할 경우, ASA에서는 요청 패킷의 TCP MSS를 ASA 최대값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우 ASA에서는 RFC 793 기본값을 536바이트로 추정하며 패킷을 수정하지 않습니다. 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.

기본값이 1500바이트인 MTU를 구성하는 경우를 예로 들어보겠습니다. 호스트에서는 값이 1700인 MSS를 요청합니다. ASA 최대 TCP MSS가 1380이면 ASA에서는 TCP 요청 패킷의 MSS 값을 1380으로 변경합니다. 그러면 서버에서는 1380바이트 패킷을 전송합니다.

기본 TCP MSS

기본적으로 ASA의 최대 TCP MSS는 1380바이트 입니다. 이러한 기본값을 사용하면 헤더에 120바이트를 추가할 수 있는 경우 VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

VPN 및 비 VPN 트래픽의 TCP MSS 설정

11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오. 다중 상황 모드의 경우, 각 상황 내에서 TCP MSS를 설정합니다.

다음 지침을 참조하십시오.

- 비 VPN 트래픽 — VPN을 사용하지 않고 헤더에 추가 공간이 필요하지 않은 경우, TCP MSS 제한을 비활성화하고 연결과 엔드포인트 간에 설정된 값을 승인해야 합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 VPN 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- VPN 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 더 높은 값으로 설정할 경우 새로운 MTU를 수용할 수 있는 TCP MSS를 설정해야 합니다.

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
```

ASA 5512-X 이상 버전의 인터페이스 라이센스 요구 사항

모델	라이센스 요건
ASA 5512-X	VLAN: Base License: 50 Security Plus License: 100 모든 유형의 인터페이스: Base License: 716 Security Plus License: 916
ASA 5515-X	VLAN: Base License: 100 모든 유형의 인터페이스: Base License: 916

모델	라이센스 요건
ASA 5525-X	VLAN: Base License: 200 모든 유형의 인터페이스: Base License: 1316
ASA 5545-X	VLAN: Base License: 300 모든 유형의 인터페이스: Base License: 1716
ASA 5555-X	VLAN: Base License: 500 모든 유형의 인터페이스: Base License: 2516
ASA 5585-X	VLAN: Base 및 Security Plus License: 1024 SSP-10 및 SSP-20을 위한 인터페이스 속도: Base License—파이버 인터페이스용 1기가비트 이더넷 10GE I/O 라이센스(Security Plus)—파이버 인터페이스용 10기가비트 이더넷 (SSP-40 및 SSP-60은 10기가비트 이더넷을 기본적으로 지원) 모든 유형의 인터페이스: Base 및 Security Plus License: 4612

참고 어떤 인터페이스가 VLAN 한도에 포함되려면 인터페이스에 VLAN을 지정해야 합니다. 예:
interface gigabitethernet 0/0.100
vlan 100

모든 유형의 인터페이스는 통합된 인터페이스의 최대 개수로 구성되며 여기에는 VLAN, 물리적, 이중화, 브릿지 그룹, EtherChannel 인터페이스가 해당됩니다. 컨피그레이션에 정의된 모든 **interface** 명령은 이 한도에 포함 됩니다. 예를 들어, GigabitEthernet 0/0 인터페이스가 port-channel 1의 일부로 정의된 경우 다음 인터페이스 둘 다 대상이 됩니다.
interface gigabitethernet 0/0
및
interface port-channel 1

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

상황 모드 지침

상황 모드의 경우 9-13 페이지의 인터페이스 컨피그레이션 시작(ASA 5512-X 이상)에 따라 시스템 실행 영역에서 물리적 인터페이스를 구성합니다. 그런 다음 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 상황 실행 영역에서 논리적 인터페이스 파라미터를 구성합니다.

방화벽 모드 지침

- 투명 모드의 경우 상황당 또는 단일 모드 디바이스에 최대 8개의 브릿지 그룹을 구성할 수 있습니다.
- 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다.
- 다중 상황, 투명 모드의 경우 각 상황에서는 다른 인터페이스를 사용해야 하며 상황 간에 인터페이스를 공유할 수 없습니다.

장애 조치 지침

- 이중화 또는 EtherChannel 인터페이스를 장애 조치 링크로 사용할 경우, 장애 조치 쌍의 두 유닛에 모두 이를 사전 구성해야 합니다. *복제를 위해서는 장애 조치 링크 자체가 필요하므로* 이러한 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 이중화 또는 EtherChannel 인터페이스를 사용할 경우, 특별한 컨피그레이션이 필요하지 않으며 컨피그레이션을 기본 유닛에서 정상적으로 복제할 수 있습니다.
- **monitor-interface** 명령을 사용하여 장애 조치를 위한 이중화 또는 EtherChannel 인터페이스를 모니터링할 수 있습니다. 이때 논리적 이중화 인터페이스 이름을 참조해야 합니다. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준 장애 조치가 모니터링되고 있으면 이 작업을 수행해도 이중화 또는 EtherChannel 인터페이스에 오류가 발생하는 것으로 나타나지 않습니다. 모든 물리적 인터페이스에 오류가 발생한 경우에만 이중화 또는 EtherChannel 인터페이스에 오류가 발생하는 것으로 나타납니다(EtherChannel 인터페이스의 경우 오류 발생이 허용되는 인터페이스 수를 구성할 수 있음).
- 장애 조치 또는 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 패킷의 오류를 방지하기 위해 EtherChannel에서 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다. 컨피그레이션을 변경하려면 변경 사항을 적용하는 동안에는 EtherChannel을 종료하거나 장애 조치를 일시적으로 비활성화해야 합니다. 이렇게 하면 해당 기간에는 장애 조치가 발생하지 않습니다.
- 장애 조치 또는 상태 인터페이스는 데이터 인터페이스와 공유할 수 없습니다.

클러스터링 지침

- 이중화 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.
- Spanned EtherChannel을 구성하려면 8-42 페이지의 Spanned EtherChannel 구성을 참조하십시오.
- 개별 클러스터 인터페이스를 구성하려면 8-39 페이지의 개별 인터페이스 구성(관리 인터페이스 권장 사항)을 참조하십시오.

이중화 인터페이스 지침

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 이중화 인터페이스를 참조합니다.
- 이중화 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중화 인터페이스 일부로 사용할 수 없습니다. 이중화 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. 또한 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 없습니다.
- 장애 조치 지침에 대한 내용은 9-11 페이지의 장애 조치 지침을 참조하십시오.
- 클러스터링 지침에 대한 내용은 9-11 페이지의 클러스터링 지침을 참조하십시오.

EtherChannel 지침

- 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.
- ASA EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어, Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.
- 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 합니다. 다중 상황 모드의 경우 이러한 메시지가 패킷 캡처에 포함되지 않으므로 문제를 쉽게 진단할 수 없습니다.
- ASA에서는 EtherChannel을 스위치 스택에 연결하도록 지원하지 않습니다. ASA EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.
- 이중화 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중화 인터페이스 일부로 사용할 수 없습니다. 이중화 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.
- 장애 조치 지침에 대한 내용은 9-11 페이지의 장애 조치 지침을 참조하십시오.
- 클러스터링 지침에 대한 내용은 9-11 페이지의 클러스터링 지침을 참조하십시오.

기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-12 페이지의 공장 기본 컨피그레이션을 참조하십시오.

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 인터페이스가 시스템 실행 영역에서도 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 — 비활성화되어 있습니다.
- 이중화 인터페이스 — 활성화되어 있습니다. 그러나 이중화 인터페이스를 통해 트래픽을 전달하려면 멤버 물리적 인터페이스도 활성화되어야 합니다.
- 하위 인터페이스 — 활성화되어 있습니다. 그러나 하위 인터페이스를 통해 트래픽을 전달하려면 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 채널 인터페이스 — 활성화되어 있습니다. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.

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 모델에 포함되는 커넥터 유형은 구리 RJ-45와 파이버 SFP로 된 두 가지 종류입니다. RJ-45가 기본값입니다. 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.

인터페이스 컨피그레이션 시작(ASA 5512-X 이상)

인터페이스 컨피그레이션 시작을 위한 작업 흐름

참고 기존 컨피그레이션을 보유하고 있고 사용 중인 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환하려면 를 사용해 컨피그레이션을 오프라인으로 수행하여 작업 중단을 최소화하십시오. 9-25 페이지의 사용 중인 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환을 참조하십시오.

인터페이스 구성을 시작하려면 다음 단계를 수행합니다.

1단계 (다중 상황 모드) 시스템 실행 영역에서 모든 작업을 완료합니다. 상황 정보에서 시스템 실행 영역으로 변경하려면, **changeto system** 명령을 사용합니다..

2단계 물리적 인터페이스를 활성화하고 선택에 따라 이더넷 파라미터를 변경합니다. 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성을 참조하십시오.

물리적 인터페이스는 기본적으로 비활성화되어 있습니다.

3단계 (선택 사항) 이중화 인터페이스 쌍을 구성합니다. 9-17 페이지의 이중화 인터페이스 구성을 참조하십시오.

논리적 이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다.

4단계 (선택 사항) EtherChannel을 구성합니다. 9-19 페이지의 EtherChannel 구성을 참조하십시오.

EtherChannel은 여러 이더넷 인터페이스를 단일한 논리적 인터페이스로 그룹화합니다.

5단계 (선택 사항) VLAN 하위 인터페이스를 구성합니다. 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.

6단계 (선택 사항) 9-24 페이지의 점보 프레임 지원 활성화에 따라 점보 프레임 지원을 활성화합니다.

7단계 (다중 상황 모드만 해당) 시스템 실행 영역에서 인터페이스의 컨피그레이션을 완료하려면 6 장, “다중 컨텍스트 모드”에 설명된 다음 작업을 수행하십시오.

- 상황에 인터페이스를 할당하려면 6-19 페이지의 보안 컨텍스트 구성을 참조하십시오.
- (선택 사항) 고유한 MAC 주소를 상황 인터페이스에 자동으로 할당하려면 6-24 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정을 참조하십시오.

이 MAC 주소는 상황 내에서 패킷을 분류하는 데 사용됩니다. 인터페이스를 공유하고 있지만 각 상황의 인터페이스에 고유한 MAC 주소가 없는 경우, 패킷을 분류하는 데 목적지 IP 주소가 사용됩니다. 또는 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 상황 내에서 MAC 주소를 수동으로 할당할 수 있습니다.

8단계 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 인터페이스 컨피그레이션을 완료합니다.

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

전제 조건

다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황 정보에서 시스템 실행 영역으로 변경하려면, **changeto system** 명령을 사용합니다..

세부 단계

	명령	목적
1단계	**interface** *physical_interface* 예: `ciscoasa(config)# interface gigabitethernet 0/0`	구성할 인터페이스를 지정합니다. *physical_interface* ID에는 유형, 슬롯, 포트 번호가 *type*[*slot*/]*port*로 포함됩니다. 물리적 인터페이스 유형은 다음과 같습니다. • **gigabitethernet** • **tengigabitethernet** • **management** 유형 뒤에는 *slot*/*port*를 입력합니다(예: **gigabitethernet0/1**). 공간은 유형과 슬롯/포트 간의 선택 사항입니다.
2단계	(선택 사항) **media-type sfp** 예: `ciscoasa(config-if)# media-type sfp`	모델에 제공되는 경우 미디어 유형을 SFP로 설정합니다. 기본값 RJ-45를 복원하려면 **media-type rj45** 명령을 입력합니다.
3단계	(선택 사항) **speed** {**auto** | **10** | **100** | **1000** | **nonegotiate**} 예: `ciscoasa(config-if)# speed 100`	속도를 설정합니다. RJ-45 인터페이스의 기본 설정은 **auto**입니다. SFP 인터페이스의 기본 설정은 **no speed nonegotiate**이며, 이 경우 속도가 최대 속도로 설정되고 흐름 제어 파라미터 및 원격 오류 정보에 대한 링크 협상이 활성화됩니다. **nonegotiate** 키워드는 SFP에 사용할 수 있는 유일한 키워드입니다. **speed nonegotiate** 명령어를 사용하면 링크 협상이 비활성화됩니다.
4단계	(선택 사항) **duplex** {**auto** | **full** | **half**} 예: `ciscoasa(config-if)# duplex full`	RJ-45 인터페이스에 양방향을 설정합니다. **auto** 설정이 기본값입니다. **참고** EtherChannel 인터페이스의 양방향 설정은 Full 또는 Auto여야 합니다.

	명령	목적
5단계	(선택 사항) **flowcontrol send on** [*low_water high_water pause_time*] [**noconfirm**] 예: `ciscoasa(config-if)# flowcontrol send on 95 200 10000`	GigabitEthernet 및 TenGigabitEthernet 인터페이스에서 흐름 제어를 위한 일시 중지(XOFF) 프레임을 활성화합니다. 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. 기본 *high_water* 값은 128KB(10 GigabitEthernet) 및 24KB(1 GigabitEthernet)이며 이 범위를 0~511(10 GigabitEthernet) 또는 0~47KB(1 GigabitEthernet) 사이로 설정할 수 있습니다. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. 기본 *low_water* 값은 64KB(10 GigabitEthernet) 및 16KB(1 GigabitEthernet)이며 이 범위를 0~511(10 GigabitEthernet) 또는 0~47KB(1 GigabitEthernet) 사이로 설정할 수 있습니다. XON이 수신된 후 또는 XOFF가 만료된 후, 일시 중지 프레임의 타이머 값에서 제어하는 대로 링크 파트너를 다시 시작할 수 있습니다. 기본 *pause_time* 값은 26624이며 이를 0~65535 사이로 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?` 메시지가 표시되지 않고 파라미터를 변경하려면 **noconfirm** 키워드를 사용합니다. **참고** 802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.
6단계	**no shutdown** 예: `ciscoasa(config-if)# no shutdown`	인터페이스를 활성화합니다. 인터페이스를 비활성화하려면 **shutdown** 명령을 입력합니다. **shutdown** 명령을 입력할 경우 모든 하위 인터페이스도 종료됩니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.

다음에 할 일

선택적 작업:

- 이중화 인터페이스 쌍을 구성합니다. 9-17 페이지의 이중화 인터페이스 구성을 참조하십시오.
- EtherChannel을 구성합니다. 9-19 페이지의 EtherChannel 구성을 참조하십시오.
- VLAN 하위 인터페이스를 구성합니다. 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.
- 점보 프레임 지원을 구성합니다. 9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 상황 모드의 경우, 상황에 인터페이스를 할당하고 상황 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 6-15 페이지의 다중 컨텍스트 모드 구성을 참조하십시오.
- 단일 상황 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

이중화 인터페이스 구성

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 장애 조치를 구성할 수 있습니다.

이 섹션에서는 이중화 인터페이스를 구성하는 방법에 대해 설명합니다.

이중화 인터페이스 구성

이 섹션에서는 이중화 인터페이스를 생성하는 방법에 대해 설명합니다. 기본적으로 이중화 인터페이스는 활성화되어 있습니다.

지침 및 제한 사항

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 이중화 인터페이스 지연 값은 구성 가능하나, 기본적으로 ASA에서는 멤버 인터페이스의 물리적 유형을 기준으로 기본 지연 값을 상속합니다.
- 9-12 페이지의 이중화 인터페이스 지침도 참조하십시오.

전제 조건

- 두 인터페이스 모두 물리적 유형이 같아야 합니다. 예를 들어, 모두 GigabitEthernet이어야 합니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중화 인터페이스에 추가할 수 없습니다. **no nameif** 명령을 사용하여 우선 이름을 제거해야 합니다.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황 정보에서 시스템 실행 영역으로 변경하려면, **changeto system** 명령을 사용합니다..

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

세부 단계

	명령	목적
1단계	**interface redundant** *number* 예: `ciscoasa(config)# interface redundant 1`	논리적 이중화 인터페이스를 추가하며, *number* 인수는 1~8 사이의 정수입니다. **참고** 논리적 파라미터(예: 이름)를 구성하기 전에 하나 이상의 멤버 인터페이스를 이중화 인터페이스에 추가해야 합니다.
2단계	**member-interface** *physical_interface* 예: `ciscoasa(config-if)# member-interface gigabitethernet 0/0`	첫 번째 멤버 인터페이스를 이중화 인터페이스에 추가합니다. 물리적 인터페이스 ID의 설명에 대한 내용은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성을 참조하십시오. 이중 인터페이스는 관리 *슬롯/포트* 인스턴스를 멤버로 지원하지 않습니다. 인터페이스를 추가하면 해당 인터페이스의 모든 컨피그레이션(예: IP 주소)이 제거됩니다.
3단계	**member-interface** *physical_interface* 예: `ciscoasa(config-if)# member-interface gigabitethernet 0/1`	두 번째 멤버 인터페이스를 이중화 인터페이스에 추가합니다. 두 번째 인터페이스는 첫 번째 인터페이스와 물리적 유형이 동일해야 합니다. 멤버 인터페이스를 제거하려면 **no member-interface** *physical_interface* 명령을 입력합니다. 이중화 인터페이스에서 두 멤버 인터페이스를 모두 제거할 수 없습니다. 이중화 인터페이스에는 최소 하나의 멤버 인터페이스가 필요합니다.

예

다음 예에서는 2개의 이중화 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
```

다음에 할 일

선택적 작업:

- VLAN 하위 인터페이스를 구성합니다. 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.
- 점보 프레임 지원을 구성합니다. 9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 상황 모드의 경우, 상황에 인터페이스를 할당하고 상황 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 6-15 페이지의 다중 컨텍스트 모드 구성을 참조하십시오.
- 단일 상황 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

액티브 인터페이스 변경

기본적으로, 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 인터페이스입니다. 어떤 인터페이스가 액티브인지 보려면에 다음 명령을 입력합니다.

```
ciscoasa# show interface redundantnumber detail | grep Member
```

예:

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

액티브 인터페이스를 변경하려면 다음 명령을 입력합니다.

```
ciscoasa# redundant-interface redundantnumber active-member physical_interface
```

redundant*number* 인수는 이중화 인터페이스 ID(예: **redundant1**)입니다.

*physical_interface*는 액티브 인터페이스로 변경하려는 멤버 인터페이스 ID입니다.

EtherChannel 구성

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하며, EtherChannel을 맞춤화하는 방법에 대해 알아봅니다.

- 9-19 페이지의 EtherChannel에 인터페이스 추가
- 9-21 페이지의 EtherChannel 맞춤화

EtherChannel에 인터페이스 추가

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하는 방법에 대해 알아봅니다. 기본적으로 포트 채널 인터페이스는 활성화되어 있습니다.

지침 및 제한 사항

- 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 Spanned EtherChannel을 구성하려면 이 절차 대신 8-42 페이지의 Spanned EtherChannel 구성을 참조하십시오.
- 9-12 페이지의 EtherChannel 지침도 참조하십시오.

전제 조건

- 채널 그룹의 모든 인터페이스는 동일한 유형과 속도, 양방향이어야 합니다. 반이중은 지원되지 않습니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 채널 그룹에 추가할 수 없습니다. **no nameif** 명령을 사용하여 우선 이름을 제거해야 합니다.
- 다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황 정보에서 시스템 실행 영역으로 변경하려면, **changeto system** 명령을 사용합니다..

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

세부 단계

	명령	목적
1단계	**interface** *physical_interface* **예:** `ciscoasa(config)# interface gigabitethernet 0/0`	채널 그룹에 추가할 인터페이스를 지정합니다. *physical_interface* ID에는 유형, 슬롯, 포트 번호가 *type*[*slot*/]*port*로 포함됩니다. 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.
2단계	**channel-group** *channel_id* **mode** {**active** | **passive** | **on**} **예:** `ciscoasa(config-if)# channel-group 1 mode active`	이 물리적 인터페이스를 *channel_id*가 1~48 사이의 범위로 된 EtherChannel에 할당합니다. 이러한 채널 ID의 채널 포트 인터페이스가 컨피그레이션에 아직 없을 경우, 다음이 추가됩니다. **interface port-channel** *channel_id* **active** 모드를 사용하는 것이 좋습니다. 액티브, 패시브 및 on 모드에 대한 자세한 내용은 9-6 페이지의 Link Aggregation Control Protocol을 참조하십시오.
3단계	(선택 사항) **lacp port-priority** *number* **예:** `ciscoasa(config-if)# lacp port-priority 12345`	채널 그룹에서 물리적 인터페이스의 우선순위를 1~65535 사이로 설정합니다. 기본값은 32768입니다. 숫자가 높을수록 우선순위는 낮아집니다. 사용할 수 있는 인터페이스보다 더 많은 인터페이스가 할당된 경우, ASA에서는 이 설정을 사용하여 어떤 인터페이스가 액티브이고 스탠바이인지 확인합니다. 포트 우선순위 설정이 모든 인터페이스에 대해 동일한 경우, 인터페이스 ID(슬롯/포트)로 우선순위가 결정됩니다. 가장 낮은 인터페이스 ID의 우선순위가 가장 높습니다. 예를 들어, GigabitEthernet 0/0은 GigabitEthernet 0/1보다 우선순위가 더 높습니다. 인터페이스 ID가 더 큰 인터페이스에 우선순위를 부여하여 액티브 상태로 만들려면 이 명령을 더 낮은 값으로 설정합니다. 예를 들어, GigabitEthernet 1/3을 GigabitEthernet 0/7보다 우선순위가 높은 액티브 상태로 만들려면 0/7 인터페이스의 기본값인 32768과 대조적으로, 1/3 인터페이스의 **lacp port-priority** 값을 12345로 설정합니다. EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선순위가 충돌할 경우, 시스템 우선순위를 통해 어느 포트 우선순위를 사용해야 할지 결정됩니다. 9-21 페이지의 EtherChannel 맞춤화에서 **lacp system-priority** 명령을 참조하십시오.
4단계	채널 그룹에 추가할 각 인터페이스에 1~3단계를 반복합니다.	채널 그룹의 각 인터페이스는 유형과 속도가 같아야 합니다. 반이중은 지원되지 않습니다. 일치하지 않는 인터페이스를 추가할 경우 보류 상태가 됩니다.

다음에 할 일

선택적 작업:

- EtherChannel 인터페이스를 맞춤화합니다. 9-21 페이지의 EtherChannel 맞춤화를 참조하십시오.
- VLAN 하위 인터페이스를 구성합니다. 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.

필수 작업:

- 다중 상황 모드의 경우, 상황에 인터페이스를 할당하고 상황 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 6-15 페이지의 다중 컨텍스트 모드 구성을 참조하십시오.
- 단일 상황 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

EtherChannel 맞춤화

이 섹션에서는 EtherChannel의 인터페이스 최대 개수, 활성 상태가 되어야 할 EtherChannel의 최소 운영 인터페이스 개수, 로드 밸런싱 알고리즘, 기타 선택적 파라미터를 설정하는 방법에 대해 설명합니다.

세부 단계

	명령	목적
1단계	**interface port-channel** *channel_id* 예: `ciscoasa(config)# interface port-channel 1`	포트 채널 인터페이스를 지정합니다. 이 인터페이스는 채널 그룹에 인터페이스를 추가할 경우 자동으로 생성된 것입니다. 인터페이스를 아직 추가하지 않은 경우 이 명령을 사용하면 포트 채널 인터페이스가 생성됩니다. **참고** 논리적 파라미터(예: 이름)를 구성하기 전에 하나 이상의 멤버 인터페이스를 포트-채널 인터페이스에 추가해야 합니다.
2단계	**lacp max-bundle** *number* 예: `ciscoasa(config-if)# lacp max-bundle 6`	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 1~16 사이로 지정합니다. 기본값은 16입니다. 스위치에서 16개의 액티브 인터페이스를 지원하지 않을 경우, 이 명령을 8 이하로 설정합니다.
3단계	**port-channel min-bundle** *number* 예: `ciscoasa(config-if)# port-channel min-bundle 2`	포트 채널 인터페이스를 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 1~16 사이로 지정합니다. 기본값은 1입니다. 채널 그룹의 액티브 인터페이스가 이 값의 범위에 속할 경우, 포트 채널 인터페이스가 종료되며 디바이스 수준 장애 조치가 일어납니다.

	명령	목적
4단계	**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**} 예: `ciscoasa(config-if)# port-channel load-balance src-dst-mac`	로드 밸런싱 알고리즘을 구성합니다. 기본적으로 ASA에서는 패킷의 소스 및 목적지 IP 주소(**src-dst-ip**)에 따라 인터페이스의 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. 로드 밸런싱에 대한 자세한 내용은 9-6 페이지의 로드 밸런싱을 참조하십시오.
5단계	**lacp system-priority** *number* 예: `ciscoasa(config)# lacp system-priority 12345`	LACP 시스템 우선순위를 1~65535까지 설정합니다. 기본값은 32768입니다. 숫자가 높을수록 우선순위는 낮아집니다. 이 명령어는 ASA에 전체적으로 적용됩니다. EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선순위가 충돌할 경우, 시스템 우선순위를 통해 어느 포트 우선순위를 사용해야 할지 결정됩니다. EtherChannel 내의 인터페이스 우선순위에 대한 내용은 9-19 페이지의 EtherChannel에 인터페이스 추가에서 **lacp port-priority** 명령을 참조하십시오.
6단계	(선택 사항) 포트 채널 인터페이스에 대한 이더넷 속성을 설정하여 개별 인터페이스의 속성 설정을 재정의할 수 있습니다.	이더넷 명령에 대한 내용은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성을 참조하십시오. 이러한 파라미터는 채널 그룹의 모든 인터페이스와 일치해야 하므로, 이 방법을 사용하면 이러한 파라미터를 빠르게 설정할 수 있습니다.

다음에 할 일

선택적 작업:

- VLAN 하위 인터페이스를 구성합니다. 9-22 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.
- 점보 프레임 지원을 구성합니다. 9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 상황 모드의 경우, 상황에 인터페이스를 할당하고 상황 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 6-15 페이지의 다중 컨텍스트 모드 구성을 참조하십시오.
- 단일 상황 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹

하위 인터페이스를 사용하면 물리적, 이중화 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 물리적 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 추가적인 물리적 인터페이스 또는 를 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 ASA있습니다. 이 기능은 다중 상황 모드에서 특히 유용하며 각 상황에 고유한 인터페이스를 할당할 수 있습니다.

지침 및 제한 사항

- 최대 하위 인터페이스 — 모델에 사용 가능한 최대 VLAN 하위 인터페이스 수를 확인하려면 9-9 페이지의 ASA 5512-X 이상 버전의 인터페이스 라이센스 요구 사항을 참조하십시오.
- 물리적 인터페이스의 태그 처리되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 처리되지 않은 패킷을 전달하기 때문입니다. 이러한 속성은 이중화 인터페이스 쌍의 물리적 인터페이스 및 EtherChannel 링크에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적, 이중화 또는 EtherChannel 인터페이스를 활성화해야 하므로, **nameif** 명령을 제외하는 방법을 통해 물리적, 이중화 또는 EtherChannel 인터페이스에서 트래픽을 전달하지 않도록 합니다. 물리적, 이중화 또는 EtherChannel 인터페이스에서 태그 처리되지 않은 패킷을 전달하는 것을 허용하려면 **nameif** 명령을 정상적으로 구성합니다. 인터페이스 컨피그레이션 완료에 대한 자세한 내용은 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.
- (ASA 5512-X부터 ASA 5555-X 버전까지) Management 0/0 인터페이스에 하위 인터페이스를 구성할 수 없습니다.
- ASA에서는 DTP(Dynamic Trunking Protocol)를 지원하지 않으므로 조건 없이 트렁킹을 수행할 연결된 스위치 포트를 구성해야 합니다.

전제 조건

다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 상황 정보에서 시스템 실행 영역으로 변경하려면, **changeto system** 명령을 사용합니다..

세부 단계

	명령	목적
1단계	**interface** {*physical_interface* | **redundant** *number* | **port-channel** *number*}.*subinterface* 예: `ciscoasa(config)# interface gigabitethernet 0/1.100`	새 하위 인터페이스를 지정합니다. 물리적 인터페이스 ID에 대한 설명은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성 섹션을 참조하십시오. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. **port-channel** *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. *subinterface* ID는 1~4294967293 사이의 정수입니다.
2단계	**vlan** *vlan_id* 예: `ciscoasa(config-subif)# vlan 101`	하위 인터페이스에 대한 VLAN을 지정합니다. *vlan_id*는 1~4094 사이의 정수입니다. 일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로, 자세한 내용을 보려면 스위치 설명서를 선택하십시오. 하나의 하위 인터페이스에 단일한 VLAN만 할당할 수 있으며, 같은 VLAN을 여러 하위 인터페이스에 할당할 수 없습니다. 물리적 인터페이스에는 VLAN을 할당할 수 없습니다. 트래픽을 전달하려면 각 하위 인터페이스에 VLAN ID가 있어야 합니다. VLAN ID를 변경하려는 경우 **no** 옵션으로 기존 VLAN ID를 제거할 필요가 없습니다. **vlan** 명령을 다른 VLAN ID와 함께 입력하면 ASA에서는 기존 ID를 변경합니다.

다음에 할 일

선택적 작업:

- 점보 프레임 지원을 구성합니다. 9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 상황 모드의 경우, 상황에 인터페이스를 할당하고 상황 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 6-15 페이지의 다중 컨텍스트 모드 구성을 참조하십시오.
- 단일 상황 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

점보 프레임 지원 활성화

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. 자세한 내용은 9-7 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 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. 를 참조하십시오. 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성 다중 상황 모드의 경우, 각 상황 내에서 MTU를 설정합니다.
- 비 VPN 트래픽에는 TCP MSS를 비활성화(**sysopt connection tcpmss 0** 명령 사용)하거나, 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 MTU에 맞춰 TCP MSS를 늘리는 방식으로 TCP MSS를 조정해야 합니다.

세부 단계

명령	목적
jumbo-frame reservation **예:** `ciscoasa(config)# jumbo-frame reservation`	점보 프레임을 지원을 활성화합니다. 점보 프레임을 비활성화하려면 이 명령을 **no** 형식으로 사용합니다.

예

다음 예에서는 점보 프레임 예약을 활성화하고, 컨피그레이션을 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
```

다음에 할 일

- 다중 상황 모드의 경우, 상황에 인터페이스를 할당하고 상황 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 6-15 페이지의 다중 컨텍스트 모드 구성을 참조하십시오.
- 단일 상황 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

사용 중인 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환

기존 컨피그레이션을 사용 중이고 현재 사용 중인 인터페이스에 이중화 또는 EtherChannel 인터페이스 기능의 장점을 활용하려면, 논리적 인터페이스를 변환할 경우 약간의 다운타임이 발생하게 됩니다.

이 섹션에서는 다운타임을 최소화하여 기존 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환하는 방법의 개요를 제공합니다. 자세한 내용은 9-17 페이지의 이중화 인터페이스 구성 및 9-19 페이지의 EtherChannel 구성에서 참조하십시오.

- 9-25 페이지의 자세한 단계(단일 모드)
- 9-30 페이지의 자세한 단계(다중 모드)

자세한 단계(단일 모드)

다음과 같은 이유에 따라 컨피그레이션을 오프라인에서 텍스트 파일로 업데이트한 후, 전체 컨피그레이션을 다시 가져오는 것이 좋습니다.

- 이름이 지정된 인터페이스는 이중화 또는 EtherChannel 인터페이스의 멤버로 추가할 수 없으므로, 인터페이스에서 이름을 제거해야 합니다. 인터페이스에서 이름을 제거하면 해당 이름을 참조하던 모든 명령이 삭제됩니다. 인터페이스 이름을 참조하는 명령은 컨피그레이션 전반에 걸쳐 광범위하게 존재하고 여러 기능에 영향을 미치므로, CLI 또는 ASDM에서 사용 중인 인터페이스에서 이름을 제거하면 새 인터페이스 이름과 관련된 모든 기능이 다시 구성되는 동시에 심각한 다운타임이 발생하는 것은 물론, 컨피그레이션에 큰 손상이 발생할 수 있습니다.
- 컨피그레이션을 오프라인으로 변경하면 새 논리적 인터페이스에 동일한 인터페이스 이름을 사용할 수 있으므로, 인터페이스 이름을 참조하는 기능 컨피그레이션에 손을 댈 필요가 없습니다. 인터페이스 컨피그레이션만 변경하면 됩니다.
- 실행 중인 컨피그레이션을 지운 뒤 바로 새 컨피그레이션을 적용하면 인터페이스의 다운타임을 최소화할 수 있습니다. 인터페이스를 실시간으로 구성하기 위해 기다리지 않아도 됩니다.

1단계 ASA에 연결합니다. 장애 조치를 사용 중인 경우 액티브 ASA에 연결합니다.

2단계 장애 조치를 사용 중인 경우 **no failover** 명령을 입력해경고 메시지가 표시되어도 계속 진행합니다.

3단계 **more system:running-config** 명령을 입력하고 표시되는 출력을 텍스트 편집기에 복사해

편집할 때 오류가 발생할 경우에 대비하여 기존 컨피그레이션의 추가 복사본을 저장해야 합니다.

4단계 이중화 또는 EtherChannel 인터페이스에 추가할 사용 중인 각 인터페이스의 경우, 새 논리적 인터페이스를 생성하는 데 사용할 수 있도록 **interface** 명령 아래의 모든 명령을 잘라서 인터페이스 컨피그레이션 섹션의 끝에 붙여넣습니다. 유일한 예외 사항은 다음 명령이며, 이는 물리적 인터페이스 컨피그레이션에 그대로 유지됩니다.

- **media-type**
- **speed**
- **duplex**
- **flowcontrol**

참고 EtherChannel 또는 이중화 인터페이스에는 *물리적* 인터페이스만 추가할 수 있으며, 물리적 인터페이스에는 VLAN을 구성할 수 없습니다.

정해진 EtherChannel 또는 이중화 인터페이스에서 모든 인터페이스에 대해 위의 값이 일치해야 합니다. EtherChannel 인터페이스의 양방향 설정은 Full 또는 Auto여야 합니다.

예를 들어, 다음과 같은 인터페이스 컨피그레이션이 있을 수 있습니다. 굵게 표시된 명령은 3개의 새 EtherChannel 인터페이스와 함께 사용할 명령이며, 이를 잘라서 인터페이스 섹션의 끝에 붙여넣어야 합니다.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif mgmt
```

```
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
```

5단계 붙여넣은 각 명령 섹션의 위에 다음 명령 중 하나를 입력하여 새 논리적 인터페이스를 생성합니다.

- **interface redundant** *number* [1-8]
- **interface port-channel** *channel_id* [1-48]

예:

```
...

interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
```

6단계 새 논리적 인터페이스에 물리적 인터페이스를 할당합니다.

- 이중화 인터페이스 — 새 **interface redundant** 명령 아래에 다음 명령을 입력합니다.

  member-interface *physical_interface1*
  member-interface *physical_interface2*

  물리적 인터페이스가 두 인터페이스와 동일한 유형입니다(이전에 사용 중 또는 미사용). 관리 인터페이스는 이중화 인터페이스에 할당할 수 없습니다.

  예를 들어, 기존 케이블 연결을 활용하려는 경우 기존 역할에서 이전에 사용 중인 인터페이스를 내부 및 외부 이중화 인터페이스의 일부로 계속 사용할 수 있습니다.

```
interface redundant 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 member-interface GigabitEthernet0/0
 member-interface GigabitEthernet0/2

interface redundant 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 member-interface GigabitEthernet0/1
 member-interface GigabitEthernet0/3
```

- EtherChannel 인터페이스 — EtherChannel에 추가할 각 인터페이스(이전에 사용 중 또는 미사용)의 아래에 다음 명령을 입력합니다. EtherChannel당 최대 16개의 인터페이스를 할당할 수 있습니다. 단, 8개만 액티브 상태로 설정할 수 있으며 나머지는 오류에 대비하여 스탠바이 상태로 유지됩니다.

  channel-group *channel_id* **mode active**

  예를 들어, 기존 케이블 연결을 활용하려는 경우 기존 역할에서 이전에 사용 중인 인터페이스를 내부 및 외부 EtherChannel 인터페이스의 일부로 계속 사용할 수 있습니다.

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 shutdown
 no nameif
 no security-level
 no ip address

...
```

7단계 **shutdown** 명령 앞에 **no**를 추가하여 현재 논리적 인터페이스의 일부인 이전에 사용되지 않은 각 인터페이스를 활성화합니다.

예를 들어, 최종 EtherChannel 컨피그레이션은 다음과 같습니다.

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
```

참고 새 컨피그레이션을 가져온 후 기타 선택적인 EtherChannel 파라미터를 구성할 수 있습니다. 9-19 페이지의 EtherChannel 구성을 참조하십시오.

8단계 ASA CLI 프롬프트에서 연결(콘솔 또는 원격)에 따라 다음 단계를 수행합니다.

- 콘솔 연결:
  a. 변경된 인터페이스 섹션을 포함하여 전체 새 컨피그레이션을 클립보드에 복사합니다.
  b. 다음을 입력하여 실행 중인 컨피그레이션을 지웁니다.

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

  이 경우 ASA를 통한 트래픽이 중단됩니다.
  c. 프롬프트에서 새 컨피그레이션에 붙여넣습니다.

  ASA를 통한 트래픽이 다시 시작됩니다.
- 원격 연결:
  a. 새 컨피그레이션을 TFTP 또는 FTP 서버에 저장하여 이를 ASA의 시작 컨피그레이션에 복사할 수 있도록 합니다. 예를 들어, PC에서 TFTP 또는 FTP 서버를 실행할 수 있습니다.
  b. 다음을 입력하여 시작 컨피그레이션을 지웁니다.

```
ciscoasa(config)# write erase
```

  c. 다음을 입력하여 새 컨피그레이션을 시작 컨피그레이션에 복사합니다.

```
ciscoasa(config)# copy url startup-config
```

  36-16 페이지의 ASA에 파일 복사를 참조하십시오.
  d. **reload** 명령을 사용하여 ASA를 다시 로드합니다. 실행 중인 컨피그레이션을 저장하지 마십시오.

9단계 **failover** 명령을 입력해.

자세한 단계(다중 모드)

다음과 같은 이유에 따라 시스템 및 상황 컨피그레이션을 오프라인에서 텍스트 파일로 업데이트한 후 이를 다시 가져오는 것이 좋습니다.

- 할당된 인터페이스는 이중화 또는 EtherChannel 인터페이스의 멤버로 추가할 수 없으므로, 상황에서 인터페이스의 할당을 취소해야 합니다. 인터페이스 할당을 취소할 경우 해당 인터페이스를 참조하던 모든 상황 명령이 삭제됩니다. 인터페이스를 참조하는 명령은 컨피그레이션 전반에 걸쳐 광범위하게 존재하고 여러 기능에 영향을 미치므로, CLI 또는 ASDM에서 사용 중인 인터페이스에서 할당을 제거하면 새 인터페이스와 관련된 모든 기능이 다시 구성되는 동시에 심각한 다운타임이 발생하는 것은 물론, 컨피그레이션에 큰 손상이 발생할 수 있습니다.
- 컨피그레이션을 오프라인으로 변경하면 새 논리적 인터페이스에 동일한 인터페이스 이름을 사용할 수 있으므로, 인터페이스 이름을 참조하는 기능 컨피그레이션에 손을 댈 필요가 없습니다. 인터페이스 컨피그레이션만 변경하면 됩니다.
- 실행 중인 시스템 컨피그레이션을 지운 뒤 바로 새 컨피그레이션을 적용하면 인터페이스의 다운타임을 최소화할 수 있습니다. 인터페이스를 실시간으로 구성하기 위해 기다리지 않아도 됩니다.

1단계 ASA에 연결하고 시스템으로 변경합니다. 장애 조치를 사용 중인 경우 액티브 ASA에 연결합니다.

2단계 장애 조치를 사용 중인 경우 **no failover** 명령을 입력해경고 메시지가 표시되어도 계속 진행합니다.

3단계 시스템에서 **more system:running-config** 명령을 입력해를 선택하고 표시되는 출력을 텍스트 편집기에 복사하여 실행 중인 컨피그레이션을 복사합니다.

편집할 때 오류가 발생할 경우에 대비하여 기존 컨피그레이션의 추가 복사본을 저장해야 합니다.

예를 들어, 시스템 컨피그레이션에서 인터페이스를 다음과 같이 컨피그레이션 및 할당하고 두 상황 간에 인터페이스를 공유할 수 있습니다.

시스템

```
interface GigabitEthernet0/0
    no shutdown
interface GigabitEthernet0/1
    no shutdown
interface GigabitEthernet0/2
    shutdown
interface GigabitEthernet0/3
    shutdown
interface GigabitEthernet0/4
    shutdown
interface GigabitEthernet0/5
    shutdown
interface Management0/0
    no shutdown
interface Management1/0
    shutdown
!
context customerA
    allocate-interface gigabitethernet0/0 int1
    allocate-interface gigabitethernet0/1 int2
    allocate-interface management0/0 mgmt
context customerB
    allocate-interface gigabitethernet0/0
    allocate-interface gigabitethernet0/1
    allocate-interface management0/0
```

4단계 새 EtherChannel 또는 이중화 인터페이스를 사용할 *모든* 상황 컨피그레이션의 복사본을 가져옵니다. 36-24 페이지의 컨피그레이션 또는 기타 파일 백업 및 복원을 참조하십시오.

예를 들어, 다음과 같은 상황 컨피그레이션(표시되는 인터페이스 컨피그레이션)을 다운로드합니다.

CustomerA Context

```
interface int1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface int2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface mgmt
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 management-only
```

CustomerB Context

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

5단계 시스템 컨피그레이션에서 9-17 페이지의 이중화 인터페이스 구성 또는 9-19 페이지의 EtherChannel 구성에 따라 새 논리적 인터페이스를 생성합니다. 논리적 인터페이스의 일부로 사용하려는 추가적인 물리적 인터페이스에 **no shutdown** 명령을 입력해야 합니다.

참고 EtherChannel 또는 이중화 인터페이스에는 *물리적* 인터페이스만 추가할 수 있으며, 물리적 인터페이스에는 VLAN을 구성할 수 없습니다.

정해진 EtherChannel 또는 이중화 인터페이스에서 모든 인터페이스의 물리적 인터페이스 파라미터(예: 속도 및 양방향)가 일치해야 합니다. EtherChannel 인터페이스의 양방향 설정은 Full 또는 Auto여야 합니다.

예를 들어, 새 컨피그레이션은 다음과 같습니다.

시스템

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
```

```
interface Management0/1
 channel-group 3 mode active
 no shutdown
!
interface port-channel 1
interface port-channel 2
interface port-channel 3
```

6단계 상황당 인터페이스 할당을 변경하여 새 EtherChannel 또는 이중화 인터페이스를 사용합니다. 6-19 페이지의 보안 컨텍스트 구성을 참조하십시오.

예를 들어, 기존 케이블 연결을 활용하려는 경우 기존 역할에서 이전에 사용 중인 인터페이스를 내부 및 외부 이중화 인터페이스의 일부로 계속 사용할 수 있습니다.

```
context customerA
    allocate-interface port-channel1 int1
    allocate-interface port-channel2 int2
    allocate-interface port-channel3 mgmt
context customerB
    allocate-interface port-channel1
    allocate-interface port-channel2
    allocate-interface port-channel3
```

참고 매핑된 이름을 인터페이스에 아직 할당하지 않은 경우, 이 기회를 통해 이를 수행하고자 할 수 있습니다. 예를 들어, customerA의 컨피그레이션은 변경할 필요가 전혀 없으며 ASA에서 다시 적용하기만 하면 됩니다. 그러나 customerB 컨피그레이션의 경우에는 모든 인터페이스 ID를 변경해야 합니다. customerB에 매핑된 이름을 할당할 경우, 상황 컨피그레이션에서 인터페이스 ID를 변경해야 하는 것은 마찬가지이지만 매핑된 이름을 사용하면 나중에 인터페이스를 변경할 때 유용할 수 있습니다.

7단계 매핑된 이름을 사용하지 않는 상황의 경우 새 EtherChannel 또는 이중화 인터페이스 ID를 사용하도록 상황 컨피그레이션을 변경합니다. (매핑된 인터페이스 이름을 사용하는 상황는 변경할 필요가 없습니다.)

예:

CustomerB Context

```
interface port-channel1
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface port-channel2
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface port-channel3
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

8단계 새 상황 컨피그레이션 파일을 기존 파일에 복사합니다. 예를 들어, 상황가 FTP 서버에 있을 경우 FTP를 사용하여 기존 파일에 복사합니다(원하는 경우 백업 생성). 상황가 플래시 메모리에 있을 경우 **copy** 명령을 사용하여 PC에서 TFTP 또는 FTP 서버를 실행하거나 안전한 복사본을 사용합니다. 36-16 페이지의 ASA에 파일 복사를 참조하십시오. 이러한 변경은 시작 컨피그레이션에만 영향을 미치며, 실행 중인 컨피그레이션에서는 기존 상황 컨피그레이션을 계속 사용합니다.

9단계 ASA 시스템 CLI 프롬프트에서 연결(콘솔 또는 원격)에 따라 다음 단계를 수행합니다.

- 콘솔 연결:
  a. 변경된 인터페이스 섹션을 포함하여 전체 새 시스템 컨피그레이션을 클립보드에 복사합니다.
  b. 다음 명령을 입력하여 실행 중인 컨피그레이션(시스템 및 상황 모두)을 지웁니다.

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

     이 경우 ASA를 통한 트래픽이 중단됩니다.
  c. 프롬프트에서 새 시스템 컨피그레이션에 붙여넣습니다.

     모든 새 상황 컨피그레이션이 다시 로드됩니다. 다시 로드하는 작업이 완료되면 ASA를 통한 트래픽이 다시 시작됩니다.
- 원격 연결:
  a. 새 시스템 컨피그레이션을 TFTP 또는 FTP 서버에 저장하여 이를 ASA의 시작 컨피그레이션에 복사할 수 있도록 합니다. 예를 들어, PC에서 TFTP 또는 FTP 서버를 실행할 수 있습니다.
  b. 다음을 입력하여 시작 컨피그레이션을 지웁니다.

     ```
     ciscoasa(config)# write erase
     ```
  c. 다음을 입력하여 새 시스템 컨피그레이션을 시작 컨피그레이션에 복사합니다.

     ```
     ciscoasa(config)# copy url startup-config
     ```

     36-16 페이지의 ASA에 파일 복사를 참조하십시오.
  d. **reload** 명령을 사용하여 ASA를 다시 로드합니다. 실행 중인 컨피그레이션을 저장하지 마십시오.

10단계 **failover** 명령을 입력해.

인터페이스 모니터링

명령	목적
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 명령어를 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]	EtherChannel의 경우 정해진 파라미터에 선택된 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보가 표시됩니다.

ASA 5512-X 이상 버전의 인터페이스 컨피그레이션 예

물리적 인터페이스 파라미터의 예

다음 예에서는 단일 모드에서 물리적 인터페이스의 파라미터를 구성합니다.

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

하위 인터페이스 파라미터의 예

다음 예에서는 단일 모드에서 하위 인터페이스의 파라미터를 구성합니다.

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

다중 상황 모드의 예

다음 예에서는 다중 상황 모드에서 시스템 컨피그레이션에 대한 인터페이스 파라미터를 구성하고, 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
```

EtherChannel의 예

다음 예에서는 세 가지 인터페이스를 EtherChannel의 일부로 구성합니다. 또한 시스템 우선순위를 더 높은 우선순위로 설정하고, EtherChannel에 8개 이상의 인터페이스가 할당된 경우 GigabitEthernet 0/2의 우선순위를 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
```

다음으로 살펴볼 내용

- 다중 상황 모드의 경우:
  a. 인터페이스를 상황에 할당하고 고유한 MAC 주소를 상황 인터페이스에 자동으로 할당합니다. 6 장, "다중 컨텍스트 모드"를 참조하십시오.
  b. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 인터페이스 컨피그레이션을 완료합니다.
- 단일 상황 모드의 경우, 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 인터페이스 컨피그레이션을 완료합니다.

ASA 5512-X 이상 버전의 인터페이스 기능 기록

표 9-2에서는 이 기능의 출시 내역을 정리합니다.

표 9-2 인터페이스의 기능 기록

기능 이름	릴리스	기능 정보
VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base License의 VLAN은 0개에서 10개. • ASA5510 Security Plus License의 VLAN은 10개에서 25개. • ASA5520 VLAN은 25개에서 100개. • ASA5540 VLAN은 100개에서 200개.
ASA 5510의 Base License 인터페이스 증가	7.2(2)	ASA 5510의 Base License의 경우, 인터페이스의 최대 수가 3개에서 관리 인터페이스까지 추가하여 무제한 인터페이스로 증가했습니다.
VLAN 증가	7.2(2)	ASA 5510(Base License는 10에서 50으로, Security Plus License는 25에서 100으로), ASA 5520(100에서 150으로), ASA 5550(200에서 250으로)의 VLAN 제한이 증가했습니다.

표 9-2 인터페이스의 기능 기록(계속)

기능 이름	릴리스	기능 정보
ASA 5510 Security Plus License의 기가비트 이더넷 지원	7.2(3)	이제 ASA 5510 ASA에서는 Security Plus License와 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.
이중 인터페이스	8.0(2)	논리적 이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 장애 조치를 구성할 수 있습니다. 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 표준 최대 크기인 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 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. 도입된 명령: **jumbo-frame reservation**
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
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. 도입된 명령: **flowcontrol**
기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(5)/8.4(2)	이제 모든 모델에서 기가비트 이더넷 인터페이스에 흐름 제어를 위한 일시 중지(XOFF) 프레임을 사용할 수 있습니다. 수정된 명령: **flowcontrol**.

표 9-2 인터페이스의 기능 기록(계속)

기능 이름	릴리스	기능 정보
EtherChannel 지원	8.4(1)	8개의 액티브 인터페이스마다 최대 48개의 802.3ad EtherChannel을 구성할 수 있습니다. 도입된 명령: **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.
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 10 기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000). **참고** 이전 ASA 버전에서 업그레이드할 경우 호환성을 위해 액티브 인터페이스의 최대 수는 8개로 설정됩니다(**lacp max-bundle** 명령). 수정된 명령: **lacp max-bundle** 및 **port-channel min-bundle**

10 장

기본 인터페이스 컨피그레이션(ASAv)

이 장에서는 이더넷 설정, 이중화 인터페이스, VLAN 하위 인터페이스를 비롯한 Cisco ASAv의 인터페이스 컨피그레이션을 시작하는 작업에 대한 내용이 포함되어 있습니다.

ASAv 인터페이스 컨피그레이션 시작 정보

ASAv 인터페이스 및 가상 NIC

가상화 플랫폼의 게스트인 ASAv에서는 기본 물리적 플랫폼의 네트워크 인터페이스를 활용합니다. 각 ASAv 인터페이스는 가상 NIC(vNIC)에 매핑됩니다.

ASAv 인터페이스

ASAv에는 다음과 같은 기가비트 이더넷 인터페이스가 포함되어 있습니다.

- Management 0/0
- GigabitEthernet 0/0에서 0/8까지 포함. GigabitEthernet 0/8은 ASAv를 장애 조치 페어의 일부분으로 구축할 경우 장애 조치 링크에 사용됩니다.

지원되는 vNIC

ASAv에서는 다음 vNIC를 지원합니다.

vNIC 유형	하이퍼바이저 지원		ASAv 버전	참고
	VMWare	KVM		
VMXNET3	예	아니요	9.2(1) 이상	VMXNET3을 사용할 경우 LRO(Large Receive Offload)을 비활성화하여 TCP 성능 저하를 방지해야 합니다. 다음 VMware 지원 문서를 참조하십시오. http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	예	예	9.2(1) 이상	9.3(1) 이하 버전의 .

VMware에서 vNIC와 ASAv의 인터페이스 일치

vSphere Client Virtual Machine Properties 화면(ASAv 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings** 선택)에는 각 네트워크 어댑터 및 할당된 네트워크가 표시됩니다. 그러나 이 화면에 ASAv 인터페이스 ID는 표시되지 않습니다(네트워크 어댑터 ID만 표시). 네트워크 어댑터 ID와 ASAv ID는 다음과 같이 상호 일치된다는 점을 참조하십시오.

네트워크 어댑터 ID	ASAv 인터페이스 ID
네트워크 어댑터 1	Management 0/0
네트워크 어댑터 2	GigabitEthernet0/0
네트워크 어댑터 3	GigabitEthernet0/1
네트워크 어댑터 4	GigabitEthernet0/2
네트워크 어댑터 5	GigabitEthernet0/3
네트워크 어댑터 6	GigabitEthernet0/4
네트워크 어댑터 7	GigabitEthernet0/5
네트워크 어댑터 8	GigabitEthernet0/6
네트워크 어댑터 9	GigabitEthernet0/7
네트워크 어댑터 10	GigabitEthernet0/8

투명 모드의 인터페이스

투명 모드의 인터페이스는 "브릿지 그룹"에 속하며, 각 네트워크에 하나의 브릿지 그룹이 있습니다. 인터페이스 4개당 최대 8개의 브릿지가 포함될 수 있습니다. 브릿지 그룹에 대한 자세한 내용은 12-1 페이지의 투명 모드의 브리지 그룹을 참조하십시오.

관리 인터페이스

관리 인터페이스 개요

다음에 연결하여 ASA를 관리할 수 있습니다.

- 통과 트래픽 인터페이스
- 전용 Management 0/0 인터페이스

35 장, "관리 액세스"에 따라 인터페이스에 대한 관리 액세스를 구성해야 할 수 있습니다.

관리 전용 트래픽에 모든 인터페이스 사용

모든 인터페이스를 관리 트래픽용으로 구성하여 이를 관리 전용 인터페이스로 사용할 수 있습니다(**management-only** 명령 참조).

투명 모드의 관리 인터페이스

투명 방화벽 모드에서는 최대 허용되는 통과 트래픽 인터페이스 외에도, Management 0/0 인터페이스(물리적 인터페이스 또는 하위 인터페이스)를 별도의 관리 인터페이스로 사용할 수도 있습니다. 다른 기타 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다. 관리 인터페이스는 일반적인 브릿지 그룹에 포함되지 않습니다. 운영상의 용도로 인해 관리 인터페이스는 구성 불가능한 브릿지 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 두 가지 모두를 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않을 경우 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 *관리* 인터페이스를 사용하여 스위치에 액세스하도록 액세스 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.

통과 트래픽 지원되지 않음

Management 0/0 인터페이스는 항상 관리 전용으로 설정되며, 이 인터페이스는 통과 트래픽을 지원하는 용도로 사용할 수 없습니다.

이중화 인터페이스

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 디바이스 수준 장애 조치를 구성할 수 있습니다.

이중화 인터페이스 MAC 주소

이중화 인터페이스에서는 맨 처음 추가되는 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 또는 멤버 인터페이스 MAC 주소에 관계없이 사용되는 이중화 인터페이스에 MAC 주소를 할당할 수 있습니다(11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성 또는 6-15 페이지의 다중 컨텍스트 모드 구성 참조). 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작하면 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

MTU 및 TCP 최대 세그먼트 크기로 조각화 제어

MTU 개요

MTU에서는 ASA가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, FCS 또는 VLAN 태깅이 *없는* 프레임 크기입니다. 이더넷 헤더는 14바이트이고 FCS는 4바이트입니다. MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더를 포함하여 1518바이트입니다. VLAN 태깅(4바이트가 더 추가됨)을 사용 중인 상태에서 MTU를 1500으로 설정할 경우 예상 프레임 크기는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오. MTU 설정을 변경하는 대신 MTU 최대 세그먼트 크기를 변경하여 캡슐화를 위한 TCP 헤더를 수용하는 방법에 대한 자세한 내용은 10-5 페이지의 TCP 최대 세그먼트 크기 개요를 참조하십시오.

참고 ASA에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다. 큰 프레임을 지원하기 위해 메모리를 늘리는 방법은 10-14 페이지의 점보 프레임 지원 활성화를 참조하십시오.

기본 MTU

ASA의 기본 MTU는 1500바이트입니다. 이 값에는 18바이트 이상의 이더넷 헤더, CRC, VLAN 태깅 등이 포함되지 않습니다.

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.

MTU 및 점보 프레임 설정

11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.

10-14 페이지의 점보 프레임 지원 활성화를 참조하십시오.

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 경우, MTU를 최대 9000바이트까지 설정할 수 있습니다.

TCP 최대 세그먼트 크기 개요

TCP MSS(TCP 최대 세그먼트 크기)는 TCP 헤더가 추가되기 *전의* TCP 페이로드의 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

ASA에서 TCP MSS를 설정할 수 있습니다. 연결의 엔드포인트에서 ASA에 설정된 값보다 큰 TCP MSS를 요청할 경우, ASA에서는 요청 패킷의 TCP MSS를 ASA 최대값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우 ASA에서는 RFC 793 기본값을 536바이트로 추정하며 패킷을 수정하지 않습니다. 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.

기본값이 1500바이트인 MTU를 구성하는 경우를 예로 들어보겠습니다. 호스트에서는 값이 1700인 MSS를 요청합니다. ASA 최대 TCP MSS가 1380이면 ASA에서는 TCP 요청 패킷의 MSS 값을 1380으로 변경합니다. 그러면 서버에서는 1380바이트 패킷을 전송합니다.

기본 TCP MSS

기본적으로 ASA의 최대 TCP MSS는 1380바이트 입니다. 이러한 기본값을 사용하면 헤더에 120바이트를 추가할 수 있는 경우 VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

VPN 및 비 VPN 트래픽의 TCP MSS 설정

11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.

다음 지침을 참조하십시오.

- 비 VPN 트래픽 — VPN을 사용하지 않고 헤더에 추가 공간이 필요하지 않은 경우, TCP MSS 제한을 비활성화하고 연결과 엔드포인트 간에 설정된 값을 승인해야 합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 VPN 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- VPN 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 더 높은 값으로 설정할 경우 새로운 MTU를 수용할 수 있는 TCP MSS를 설정해야 합니다.

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 9000
mtu outside 9000
sysopt connection tcpmss 0
```

다음 예에서는 점보 프레임을 활성화하고, 모든 인터페이스의 MTU를 높이며, VPN 트래픽의 TCP MSS를 8880으로 변경합니다(MTU 빼기 120).

```
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 8880
```

ASAv 인터페이스의 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv - 가상 CPU 1개 포함	VLAN: Standard 및 Premium 라이센스: 50 모든 유형의 인터페이스: Standard 및 Premium 라이센스: 716
ASAv - 가상 CPU 4개 포함	VLAN: Standard 및 Premium 라이센스: 200 모든 유형의 인터페이스: Standard 및 Premium 라이센스: 1316

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예:
interface gigabitethernet 0/0.100
vlan 100

모든 유형의 인터페이스는 통합된 인터페이스의 최대 개수로 구성되며 여기에는 VLAN, 물리적, 이중화, 브릿지 그룹 인터페이스가 해당됩니다. 컨피그레이션에 정의된 모든 **interface** 명령은 이 한도의 대상이 됩니다.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

방화벽 모드 지침

- 투명 모드의 경우 최대 8개의 브릿지 그룹을 구성할 수 있습니다.
- 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다.

장애 조치 지침

- 이중화 인터페이스를 장애 조치 링크로 사용할 경우, 장애 조치 쌍의 두 유닛에 모두 이를 구성해야 합니다. *복제를 위해서는 장애 조치 링크 자체가 필요하므로* 이중화 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 이중화 인터페이스를 사용할 경우, 특별한 컨피그레이션이 필요하지 않으며 컨피그레이션을 기본 유닛에서 정상적으로 복제할 수 있습니다.
- **monitor-interface** 명령을 사용하여 장애 조치를 위한 이중화 인터페이스를 모니터링할 수 있습니다. 이때 논리적 이중화 인터페이스 이름을 참조해야 합니다. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준 장애 조치가 모니터링되고 있으면 이 작업을 수행해도 이중화 인터페이스에 오류가 발생하는 것으로 나타나지 않습니다. 모든 물리적 인터페이스에 오류가 발생한 경우에만 이중화 인터페이스에 오류가 발생하는 것으로 나타납니다.
- 장애 조치 또는 상태 인터페이스는 데이터 인터페이스와 공유할 수 없습니다.

이중화 인터페이스 지침

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 이중화 인터페이스를 참조합니다.
- 액티브 인터페이스를 종료할 경우 스탠바이 인터페이스가 액티브 상태로 됩니다.
- 이중화 인터페이스는 관리 전용으로 설정할 수 없습니다.
- 장애 조치 지침에 대한 내용은 10-7 페이지의 장애 조치 지침을 참조하십시오.

기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-12 페이지의 공장 기본 컨피그레이션을 참조하십시오.

인터페이스의 기본 상태

- 물리적 인터페이스 — 비활성화되어 있습니다.
- 이중화 인터페이스 — 활성화되어 있습니다. 그러나 이중화 인터페이스를 통해 트래픽을 전달하려면 멤버 물리적 인터페이스도 활성화되어야 합니다.

- 하위 인터페이스 — 활성화되어 있습니다. 그러나 하위 인터페이스를 통해 트래픽을 전달하려면 물리적 인터페이스도 활성화되어야 합니다.

기본 속도와 양방향

- 기본적으로 인터페이스의 속도와 양방향은 자동 협상이 이루어지도록 설정됩니다.

기본 MAC 주소

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

기본 vNIC

모든 인터페이스에서는 E1000 에뮬레이션을 사용합니다.

인터페이스 컨피그레이션 시작(ASAv)

인터페이스 컨피그레이션 시작을 위한 작업 흐름

인터페이스 구성을 시작하려면 다음 단계를 수행합니다.

1단계 물리적 인터페이스를 활성화하고 선택에 따라 이더넷 매개변수를 변경합니다. 10-9 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성을 참조하십시오.

물리적 인터페이스는 기본적으로 비활성화되어 있습니다.

2단계 (선택 사항) 이중화 인터페이스 쌍을 구성합니다. 10-11 페이지의 이중화 인터페이스 구성을 참조하십시오.

논리적 이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다.

3단계 (선택 사항) VLAN 하위 인터페이스를 구성합니다. 10-13 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.

4단계 (선택 사항) 10-14 페이지의 점보 프레임 지원 활성화에 따라 점보 프레임 지원을 활성화합니다.

물리적 인터페이스 활성화 및 이더넷 매개변수 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화
- 특정 속도 및 양방향 설정
- 흐름 제어를 위한 일시 중지 프레임 활성화

세부 단계

	명령	목적
1단계	**interface** *physical_interface* 예: `ciscoasa(config)# interface gigabitethernet 0/0`	구성할 인터페이스를 지정합니다. *physical_interface* ID에는 유형, 슬롯, 포트 번호가 *type*[*slot*/]*port*로 포함됩니다. 물리적 인터페이스 유형은 다음과 같습니다. • **gigabitethernet** • **management** 유형 뒤에는 *slot*/*port*를 입력합니다(예: **gigabitethernet0/1**). 공간은 유형과 슬롯/포트 간의 선택 사항입니다.
2단계	(선택 사항) **speed** {**auto** | **10** | **100** | **1000**} 예: `ciscoasa(config-if)# speed 100`	속도를 설정합니다. 기본 설정은 **auto**입니다.
3단계	(선택 사항) **duplex** {**auto** | **full** | **half**} 예: `ciscoasa(config-if)# duplex full`	양방향을 설정합니다. **auto** 설정이 기본값입니다.

	명령	목적
4단계	(선택 사항) **flowcontrol send on** [*low_water high_water pause_time*] [**noconfirm**] **예:** `ciscoasa(config-if)# flowcontrol send on 95 200 10000`	흐름 제어를 위해 일시 중지(XOFF) 프레임을 활성화합니다. 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. 기본 *high_water* 값은 24KB이며 이를 0~47KB 사이로 설정할 수 있습니다. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. 기본적으로 *low_water* 값은 16KB이며 이를 0~47KB 사이로 설정할 수 있습니다. XON이 수신된 후 또는 XOFF가 만료된 후, 일시 중지 프레임의 타이머 값에서 제어하는 대로 링크 파트너를 다시 시작할 수 있습니다. 기본 *pause_time* 값은 26624이며 이를 0~65535 사이로 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?` 메시지가 표시되지 않고 매개변수를 변경하려면 **noconfirm** 키워드를 사용합니다. **참고** 802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.
5단계	**no shutdown** **예:** `ciscoasa(config-if)# no shutdown`	인터페이스를 활성화합니다. 인터페이스를 비활성화하려면 **shutdown** 명령을 입력합니다. **shutdown** 명령을 입력할 경우 모든 하위 인터페이스도 종료됩니다. 시스템 실행 영역에서 인터페이스를 종료할 경우, 이를 공유하는 모든 컨텍스트에서 해당 인터페이스가 종료됩니다.

다음에 할 일

선택적 작업:

- 이중화 인터페이스 쌍을 구성합니다. 10-11 페이지의 이중화 인터페이스 구성을 참조하십시오.
- VLAN 하위 인터페이스를 구성합니다. 10-13 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.
- 점보 프레임 지원을 구성합니다. 10-14 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

이중화 인터페이스 구성

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 장애 조치를 구성할 수 있습니다.

이 섹션에서는 이중화 인터페이스를 구성하는 방법에 대해 설명합니다.

- 10-11 페이지의 이중화 인터페이스 구성
- 10-12 페이지의 액티브 인터페이스 변경

이중화 인터페이스 구성

이 섹션에서는 이중화 인터페이스를 생성하는 방법에 대해 설명합니다. 기본적으로 이중화 인터페이스는 활성화되어 있습니다.

지침 및 제한 사항

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 이중화 인터페이스 지연 값은 구성 가능하나, 기본적으로 ASA에서는 멤버 인터페이스의 물리적 유형을 기준으로 기본 지연 값을 상속합니다.
- 10-7 페이지의 이중화 인터페이스 지침도 참조하십시오.

전제 조건

- 두 인터페이스 모두 물리적 유형이 같아야 합니다. 예를 들어, 모두 GigabitEthernet이어야 합니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중화 인터페이스에 추가할 수 없습니다. **no nameif** 명령을 사용하여 우선 이름을 제거해야 합니다.

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

세부 단계

	명령	목적
1단계	**interface redundant** *number* 예: `ciscoasa(config)# interface redundant 1`	논리적 이중화 인터페이스를 추가하며, *number* 인수는 1~8 사이의 정수입니다. **참고** 논리적 매개변수(예: 이름)를 구성하기 전에 하나 이상의 멤버 인터페이스를 이중화 인터페이스에 추가해야 합니다.
2단계	**member-interface** *physical_interface* 예: `ciscoasa(config-if)# member-interface gigabitethernet 0/0`	첫 번째 멤버 인터페이스를 이중화 인터페이스에 추가합니다. 인터페이스를 추가하면 해당 인터페이스의 모든 컨피그레이션(예: IP 주소)이 제거됩니다.

	명령	목적
3단계	**member-interface** *physical_interface* 예: ciscoasa(config-if)# member-interface gigabitethernet 0/1	두 번째 멤버 인터페이스를 이중화 인터페이스에 추가합니다. 두 번째 인터페이스는 첫 번째 인터페이스와 물리적 유형이 동일해야 합니다. 멤버 인터페이스를 제거하려면 **no member-interface** *physical_interface* 명령을 입력합니다. 이중화 인터페이스에서 두 멤버 인터페이스를 모두 제거할 수 없습니다. 이중화 인터페이스에는 최소 하나의 멤버 인터페이스가 필요합니다.

예

다음 예에서는 2개의 이중화 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
```

다음에 할 일

선택적 작업:

- VLAN 하위 인터페이스를 구성합니다. 10-13 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹을 참조하십시오.
- 점보 프레임 지원을 구성합니다. 10-14 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

액티브 인터페이스 변경

기본적으로, 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 인터페이스입니다. 어떤 인터페이스가 액티브인지 보려면에 다음 명령을 입력합니다.

```
ciscoasa# show interface redundantnumber detail | grep Member
```

예:

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

액티브 인터페이스를 변경하려면 다음 명령을 입력합니다.

```
ciscoasa# redundant-interface redundantnumber active-member physical_interface
```

redundant*number* 인수는 이중화 인터페이스 ID(예: **redundant1**)입니다.

*physical_interface*는 액티브 인터페이스로 변경하려는 멤버 인터페이스 ID입니다.

VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹

하위 인터페이스를 사용하면 물리적 또는 이중화 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 물리적 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 추가적인 물리적 인터페이스 또는 ASA를 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

지침 및 제한 사항

- 최대 하위 인터페이스 — 모델에 사용 가능한 최대 VLAN 하위 인터페이스 수를 확인하려면 10-6 페이지의 ASAv 인터페이스의 라이센스 요구 사항을 참조하십시오.
- 물리적 인터페이스의 태그 처리되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 처리되지 않은 패킷을 전달하기 때문입니다. 이러한 속성은 이중화 인터페이스 쌍의 액티브 물리적 인터페이스에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적 또는 이중화 인터페이스를 활성화해야 하므로, **nameif** 명령을 제외하는 방법을 통해 물리적 또는 이중화 인터페이스에서 트래픽을 전달하지 않도록 합니다. 물리적 또는 이중화 인터페이스에서 태그 처리되지 않은 패킷을 전달하는 것을 허용하려면 **nameif** 명령을 정상적으로 구성합니다. 인터페이스 컨피그레이션 완료에 대한 자세한 내용은 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

세부 단계

	명령	목적
1단계	**interface** {*physical_interface* | **redundant** *number*}.*subinterface* 예: `ciscoasa(config)# interface gigabitethernet 0/1.100`	새 하위 인터페이스를 지정합니다. 물리적 인터페이스 ID의 설명에 대한 내용은 10-9 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성을 참조하십시오. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. *subinterface* ID는 1~4294967293 사이의 정수입니다.
2단계	**vlan** *vlan_id* 예: `ciscoasa(config-subif)# vlan 101`	하위 인터페이스에 대한 VLAN을 지정합니다. *vlan_id*는 1~4094 사이의 정수입니다. 일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로, 자세한 내용을 보려면 스위치 설명서를 선택하십시오. 하나의 하위 인터페이스에 단일한 VLAN만 할당할 수 있으며, 같은 VLAN을 여러 하위 인터페이스에 할당할 수 없습니다. 물리적 인터페이스에는 VLAN을 할당할 수 없습니다. 트래픽을 전달하려면 각 하위 인터페이스에 VLAN ID가 있어야 합니다. VLAN ID를 변경하려는 경우 **no** 옵션으로 기존 VLAN ID를 제거할 필요가 없습니다. **vlan** 명령을 다른 VLAN ID와 함께 입력하면 ASA에서는 기존 ID를 변경합니다.

다음에 할 일

선택적 작업:

- 점보 프레임 지원을 구성합니다. 10-14 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

점보 프레임 지원 활성화

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. 자세한 내용은 10-4 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 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 9000으로 설정합니다. 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.
- 비 VPN 트래픽에는 TCP MSS를 비활성화(**sysopt connection tcpmss 0** 명령 사용)하거나, 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 MTU에 맞춰 TCP MSS를 늘리는 방식으로 TCP MSS를 조정해야 합니다.

세부 단계

명령	목적
jumbo-frame reservation 예: `ciscoasa(config)# jumbo-frame reservation`	점보 프레임을 지원을 활성화합니다. 점보 프레임을 비활성화하려면 이 명령을 **no** 형식으로 사용합니다.

예

다음 예에서는 점보 프레임 예약을 활성화하고, 컨피그레이션을 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
```

다음에 할 일

인터페이스 컨피그레이션을 완료합니다. 11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"를 참조하십시오.

인터페이스 모니터링

인터페이스를 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
show interface	인터페이스 통계를 표시합니다.
show interface ip brief	인터페이스 IP 주소와 상태를 표시합니다.

ASAv 인터페이스 컨피그레이션 예

- 10-15 페이지의 물리적 인터페이스 매개변수의 예
- 10-15 페이지의 하위 인터페이스 매개변수의 예

물리적 인터페이스 매개변수의 예

다음 예에서는 물리적 인터페이스의 매개변수를 구성합니다.

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

하위 인터페이스 매개변수의 예

다음 예에서는 하위 인터페이스의 매개변수를 구성합니다.

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

다음으로 살펴볼 내용

11 장, "라우팅 모드 인터페이스" 또는 12 장, "투명 모드 인터페이스"에 따라 인터페이스 컨피그레이션을 완료합니다.

ASAv 인터페이스의 기능 기록

표 10-1 인터페이스의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
ASAv 지원	9.2(1)	ASAv는 도입되었습니다.

라우팅 모드 인터페이스

이 장에는 라우팅 방화벽 모드에서 모든 모델의 인터페이스 컨피그레이션을 완료하는 작업에 대한 내용이 포함되어 있습니다.

참고 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 섹션의 작업을 수행합니다. 구성할 컨텍스트로 변경하려면 **changeto context** *name* 명령을 입력합니다.

라우팅 모드에서 인터페이스 컨피그레이션 완료 정보

보안 레벨

각 인터페이스는 0(가장 낮음)~100(가장 높음)의 보안 레벨이 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. 자세한 내용은 11-13 페이지의 동일한 보안 레벨 통신 허용을 참조하십시오.

이 레벨은 다음 동작을 제어합니다.

- 네트워크 액세스—기본적으로 상위 보안 인터페이스에서 하위 보안 인터페이스로 암시적 허용이 이루어집니다(아웃바운드). 상위 보안 인터페이스의 호스트는 하위 보안 인터페이스의 어떤 호스트에도 액세스할 수 있습니다. 인터페이스에 ACL을 적용하여 액세스를 제한할 수 있습니다.

  동일한 보안 인터페이스에 대한 통신을 활성화할 경우(11-13 페이지의 동일한 보안 레벨 통신 허용 참조), 해당 인터페이스에서 보안 레벨이 같거나 더 낮은 다른 인터페이스에 액세스하는 것이 암시적으로 허용됩니다.

- 검사 엔진—일부 애플리케이션 검사 엔진은 보안 레벨에 좌우됩니다. 동일한 보안 인터페이스에서는 검사 엔진이 어느 방향의 트래픽에도 적용됩니다.
  - NetBIOS 검사 엔진—아웃바운드 연결에만 적용됩니다.
  - SQL*Net 검사 엔진—어떤 호스트 쌍에 SQL*Net(이전의 OraServ) 포트에 대한 제어 연결이 있을 경우 인바운드 데이터 연결만 ASA에서 허용됩니다.
- 필터링—HTTP(S) 및 FTP 필터링은 아웃바운드 연결(상위에서 하위로)에만 적용됩니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 어느 방향의 트래픽도 필터링할 수 있습니다.

- **established** 명령—이 명령은 상위 보안 호스트에서 하위 보안 호스트로의 연결이 이미 설정된 경우 하위 호스트에서 상위 호스트로 돌아가는 연결을 허용합니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 양방향 모두에 **established** 명령을 구성할 수 있습니다.

이중 IP Stack(IPv4 및 IPv6)

Cisco ASA에서는 인터페이스에서 IPv6 및 IPv4 컨피그레이션을 모두 지원합니다. 이를 위해 특수한 명령을 입력할 필요가 없으며, 일반적으로 하는 것처럼 IPv4 컨피그레이션 명령 및 IPv6 컨피그레이션 명령을 입력하기만 하면 됩니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다.

라우팅 모드에서 인터페이스 컨피그레이션을 완료하는 데 필요한 라이센스 요구 사항

모델	라이센싱 요구 사항
ASA 5512-X	VLAN: Base 라이센스: 50 Security Plus 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 716 Security Plus 라이센스: 916
ASA 5515-X	VLAN: Base 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 916
ASA 5525-X	VLAN: Base 라이센스: 200 모든 유형의 인터페이스: Base 라이센스: 1316
ASA 5545-X	VLAN: Base 라이센스: 300 모든 유형의 인터페이스: Base 라이센스: 1716
ASA 5555-X	VLAN: Base 라이센스: 500 모든 유형의 인터페이스: Base 라이센스: 2516
ASA 5585-X	VLAN: Base 및 Security Plus 라이센스: 1024 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) 모든 유형의 인터페이스: Base 및 Security Plus 라이센스: 4612

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예:
interface gigabitethernet 0/0.100
vlan 100

모든 유형의 인터페이스는 통합된 인터페이스의 최대 개수로 구성되며 여기에는 VLAN, 물리적, 이중화, 브릿지 그룹, EtherChannel 인터페이스가 해당됩니다. 컨피그레이션에 정의된 모든 **interface** 명령은 이 한도의 대상이 됩니다. 예를 들어, GigabitEthernet 0/0 인터페이스가 port-channel 1의 일부로 정의된 경우 다음 인터페이스 둘 다 대상이 됩니다.
interface gigabitethernet 0/0
및
interface port-channel 1

모델	라이센싱 요구 사항
ASASM	VLAN: Base 라이센스: 1000

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

- 다중 컨텍스트 모드의 ASA 5512-X 이상에서는 시스템 실행 영역에서 9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"에 따라 물리적 인터페이스를 구성합니다. 그런 다음 컨텍스트 실행 영역에서 이 장의 내용에 따라 논리적 인터페이스 매개 변수를 구성합니다. 다중 컨텍스트 모드의 ASASM에서는 스위치에서 스위치 포트와 VLAN을 구성하고 3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"에 따라 ASASM에 VLAN을 지정합니다.

  ASAv는 다중 컨텍스트 모드를 지원하지 않습니다.
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 구성할 수 있습니다.
- PPPoE는 다중 컨텍스트 모드에서 지원되지 않습니다.

방화벽 모드 지침

라우팅 방화벽 모드에서 지원됩니다. 투명 모드에 대한 내용은 12 장, "투명 모드 인터페이스"를 참조하십시오.

장애 조치 지침

이 장의 절차를 사용하여 장애 조치 인터페이스 구성을 마쳐서는 안 됩니다. 장애 조치 및 상태 링크 구성에 대해서는 7 장, "고가용성을 위한 장애 조치"를 참조하십시오. 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 장애 조치 인터페이스가 구성됩니다.

IPv6 지침

IPv6를 지원합니다.

ASASM를 위한 VLAN ID 지침

어떤 VLAN ID도 컨피그레이션에 추가할 수 있으나, 스위치에 의해 ASA에 지정된 VLAN만 트래픽을 전달할 수 있습니다. ASA에 지정된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다.

아직 스위치에 의해 ASA에 지정되지 않은 VLAN을 위해 인터페이스를 추가할 경우 그 인터페이스는 중지(down) 상태가 됩니다. VLAN을 ASA에 지정하면 인터페이스는 작동(up) 상태로 바뀝니다. 인터페이스 상태에 대한 자세한 내용은 **show interface** 명령을 참조하십시오.

기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-12 페이지의 공장 기본 컨피그레이션을 참조하십시오.

기본 보안 레벨

기본 보안 레벨은 0입니다. 인터페이스의 이름을 "inside"로 지정한 다음 보안 레벨을 명시적으로 설정하지 않으면 ASA는 보안 레벨을 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.

ASASM의 인터페이스 기본 상태

- 단일 모드 또는 시스템 시행 영역에서는 VLAN 인터페이스가 기본적으로 활성화되어 있습니다.
- 다중 컨텍스트 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 인터페이스가 시스템 실행 영역에서도 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 컨텍스트에서 중지됩니다.

점보 프레임 지원

기본적으로 ASASM는 점보 프레임을 지원합니다. 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 원하는 패킷 크기의 MTU를 구성합니다.

라우팅 모드에서 인터페이스 컨피그레이션 완료

인터페이스 컨피그레이션 완료의 작업 흐름

1단계 모델에 따라 인터페이스를 설정합니다.

- ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"

- ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
- ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"

2단계 (다중 컨텍스트 모드) 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 컨텍스트에 인터페이스를 배정합니다.

3단계 (다중 컨텍스트 모드) 구성하려는 컨텍스트를 변경하려면 **changeto context** *name* 명령을 입력합니다. 인터페이스 이름, 보안 수준, IPv4 주소를 비롯한 일반적인 인터페이스 매개변수를 구성합니다. 11-6 페이지의 일반 인터페이스 매개 변수 구성을 참조하십시오.

4단계 (선택 사항) MAC 주소 및 MTU를 구성합니다. 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.

5단계 (선택 사항) IPv6 주소 지정을 구성합니다. 11-11 페이지의 IPv6 주소 지정 구성을 참조하십시오.

6단계 (선택 사항) 두 인터페이스 간 통신을 허용하거나 트래픽이 동일한 인터페이스에 들어오고 나가는 것을 허용하는 방법 중 하나로 동일한 보안 레벨 통신을 허용합니다. 11-13 페이지의 동일한 보안 레벨 통신 허용을 참조하십시오.

일반 인터페이스 매개 변수 구성

이 절차에서는 이름, 보안 수준, IPv4 주소 및 기타 옵션을 설정하는 방법에 대해 설명합니다.

ASA 5512-X 이상과 ASAv의 경우 다음 인터페이스 유형에 대한 인터페이스 매개 변수를 구성해야 합니다.

- 물리적 인터페이스
- VLAN 하위 인터페이스
- 이중 인터페이스
- EtherChannel 인터페이스

ASASM에서는 다음 인터페이스 유형에 대해 인터페이스 매개 변수를 구성해야 합니다.

- VLAN 인터페이스

지침 및 제한 사항

장애 조치를 사용하는 경우 장애 조치 및 상태 기반 시스템 대체 작동 통신 전용 인터페이스의 이름을 지정하는 데 이 절차를 사용하지 마십시오. 장애 조치 및 상태 링크 구성에 대해서는 7 장, "고가용성을 위한 장애 조치"를 참조하십시오.

제한 사항

- PPPoE는 다중 컨텍스트 모드에서 지원되지 않습니다.
- PPPoE 및 DHCP는 ASASM에서 지원되지 않습니다.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
  - ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
  - ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"

- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 구성할 수 있습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

세부 단계

	명령	목적
1단계	ASA 5512-X 이상 버전 및 ASAv의 경우: **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} ASASM: ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **예:** ciscoasa(config)# interface gigabithethernet 0/0	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. **port-channel** *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. 물리적 인터페이스 ID에 대한 설명은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성 섹션을 참조하십시오. 물리적 인터페이스 ID 또는 이중 인터페이스 ID의 끝에 *하위 인터페이스* ID를 추가하고 마침표(.)로 구분합니다. 다중 컨텍스트 모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**nameif** *name* **예:** ciscoasa(config-if)# nameif inside	인터페이스의 이름을 지정합니다. *name*은 최대 48자의 텍스트이며 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.
3단계	다음 중 하나를 수행합니다.	
	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	직접 IP 주소를 설정합니다. **참고** 장애 조치와 함께 사용할 경우 IP 주소 및 스탠바이 주소를 수동으로 설정해야 하며, DHCP 및 PPPoE는 지원되지 않습니다. *ip_address* 및 *mask* 인수는 인터페이스 IP 주소와 서브넷 마스크를 설정합니다. **standby** *ip_address* 인수는 장애 조치에 사용됩니다. 자세한 내용은 7-26 페이지의 액티브/스탠바이 장애 조치 구성 또는 7-30 페이지의 액티브/액티브 장애 조치 구성을 참조하십시오.
	ip address dhcp [**setroute**] **예:** ciscoasa(config-if)# ip address dhcp	DHCP 서버에서 IP 주소를 얻습니다. **setroute** 키워드는 ASA에서 DHCP 서버가 제공한 기본 경로를 사용할 수 있게 합니다. DHCP 임대를 재설정하고 새 임대를 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.

	명령	목적
	PPPoE 서버에서 IP 주소를 얻으려면 VPN 컨피그레이션 가이드을(를) 참조하십시오.	PPPoE는 다중 컨텍스트 모드에서 지원되지 않습니다.
4단계	**security-level** *number* 예: `ciscoasa(config-if)# security-level 50`	보안 레벨을 설정합니다. *number*는 0(가장 낮음)~100(가장 높음) 범위의 정수입니다. 11-1 페이지의 보안 레벨을 참조하십시오.
5단계	(선택 사항) **management-only** 예: `ciscoasa(config-if)# management-only`	인터페이스를 관리 전용 모드로 설정하여 통과 트래픽을 전달하지 않도록 합니다. 기본적으로 관리 인터페이스는 관리 전용으로 구성됩니다. 이 설정을 비활성화하려면 **no management-only** 명령을 입력합니다. (ASA 5512-X부터 ASA 5555-X까지) Management 0/0 인터페이스에서 **management-only**를 비활성화할 수 없습니다. 이중화 인터페이스에는 **management-only** 명령이 지원되지 않습니다.

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 컨텍스트 모드에서 컨텍스트 컨피그레이션을 위한 매개변수를 구성합니다. 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
```

다음에 할 일

- (선택 사항) MAC 주소 및 MTU를 구성합니다. 11-8 페이지의 MAC Address, MTU 및 TCP MSS 구성을 참조하십시오.
- (선택 사항) IPv6 주소 지정을 구성합니다. 11-11 페이지의 IPv6 주소 지정 구성을 참조하십시오.

MAC Address, MTU 및 TCP MSS 구성

이 섹션에서는 인터페이스의 MAC 주소를 구성하는 방법 및 MTU와 TCP MSS를 설정하는 방법을 설명합니다.

MAC 주소에 대한 정보

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

ASASM에서는 모든 VLAN이 백플레인에서 제공한 동일한 MAC 주소를 사용합니다.

이중 인터페이스는 사용자가 추가한 첫 번째 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 이 명령을 사용하여 이중 인터페이스에 MAC 주소를 지정하면 멤버 인터페이스 MAC 주소와 상관없이 이 주소가 사용됩니다.

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 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 다중 컨텍스트 모드에서는 EtherChannel 포트 인터페이스를 비롯한 인터페이스에 고유한 MAC 주소를 자동으로 지정할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 다중 컨텍스트 모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그 다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

다중 컨텍스트 모드에서는 여러 컨텍스트가 하나의 인터페이스를 공유할 경우 각 컨텍스트에서 인터페이스에 고유한 MAC 주소를 지정할 수 있습니다. 이 기능 덕분에 ASA에서 손쉽게 알맞은 컨텍스트로 패킷을 분류할 수 있습니다. 고유한 MAC 주소 없이 공유 인터페이스를 사용할 수 있으나, 몇 가지 제한이 있습니다. 자세한 내용은 6-3 페이지의 ASA의 패킷 분류를 참조하십시오. 각 MAC 주소를 직접 지정하거나 컨텍스트에서 공유 인터페이스의 MAC 주소를 자동으로 생성할 수 있습니다. MAC 주소를 자동으로 생성하려면 6-24 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정을 참조하십시오. MAC 주소를 자동으로 생성한 경우 생성된 주소를 재정의하는 데 이 절차를 사용할 수 있습니다.

단일 컨텍스트 모드에서는 또는 다중 컨텍스트 모드에서 공유되지 않는 인터페이스에 대해서는 하위 인터페이스에 고유 MAC 주소를 지정해야 하는 경우가 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다.

MTU 및 TCP MSS에 대한 정보

9-7 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
  - ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
  - ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 구성할 수 있습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.
- MTU를 1500 이상으로 높이려면 9-24 페이지의 점보 프레임 지원 활성화에 따라 점보 프레임을 활성화합니다. ASASM에서는 기본적으로 점보 프레임을 지원하므로, 활성화할 필요 없습니다.

세부 단계

	명령	목적
1단계	ASA 5512-X 이상 및 ASAv: **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} ASASM: ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **예:** ciscoasa(config)# interface vlan 100	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. **port-channel** *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. 물리적 인터페이스 ID에 대한 설명은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성 섹션을 참조하십시오. 물리적 인터페이스 ID 또는 이중 인터페이스 ID의 끝에 *하위 인터페이스* ID를 추가하고 마침표(.)로 구분합니다. 다중 컨텍스트 모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**mac-address** *mac_address* [**standby** *mac_address*] **예:** ciscoasa(config-if)# mac-address 000C.F142.4CDE	이 인터페이스에 사설 MAC 주소를 지정합니다. *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. 장애 조치와 함께 사용하려면 **standby** MAC 주소를 설정합니다. 활성 유닛이 장애 조치되고 대기 유닛이 활성 상태가 되면, 네트워크 중단을 최소화하기 위해 새 활성 유닛에서 활성 MAC 주소를 사용하기 시작하고 기존 활성 유닛은 대기 주소를 사용합니다.
3단계	**mtu** *interface_name bytes* **예:** ciscoasa(config)# mtu inside 9200	MTU를 300바이트~9198(ASAv는 9000)바이트 범위에서 설정합니다. 기본값은 1500바이트입니다. **참고** 이중 또는 포트 채널 인터페이스를 위해 MTU를 설정하면 ASA는 모든 멤버 인터페이스에 이 설정을 적용합니다. 점보 프레임을 지원하는 모델에서 어떤 인터페이스에 1500보다 큰 값을 입력한 경우 점보 프레임 지원을 활성화해야 합니다. 9-24 페이지의 점보 프레임 지원 활성화를 참조합니다.
4단계	**sysopt connection tcpmss** [**minimum**] *bytes* **예:** ciscoasa(config)# sysopt connection tcpmss 8500 ciscoasa(config)# sysopt connection tcpmss minimum 1290	최대 TCP 세그먼트 크기(바이트)를 48~임의의 최대값 범위에서 설정합니다. 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. minimum 기능은 기본적으로 비활성화되어 있습니다(0으로 설정됨).

다음에 할 일

(선택 사항) IPv6 주소 지정을 구성합니다. 11-11 페이지의 IPv6 주소 지정 구성을 참조하십시오.

IPv6 주소 지정 구성

이 섹션에서는 IPv6 주소 지정의 구성 방법을 설명합니다.

IPv6에 대한 정보

이 섹션에서는 IPv6를 구성하는 방법을 다룹니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- Global—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다.
- Link-local—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 컨피그레이션에 또는 주소 확인, Neighbor Discovery와 같은 ND 기능에 사용할 수 있습니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 Link-Local 주소가 인터페이스에서 자동으로 구성되므로, Link-Local 주소를 특별히 구성하지 않아도 됩니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

참고 링크-로컬 주소만 구성하려면 명령 참조에서 **ipv6 enable**(자동 구성) 또는 **ipv6 address link-local**(수동 구성) 명령을 참조하십시오.

Modified 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.

```
%ASA-3-325003: 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. 라우터 뒤에 있는 호스트로부터 받은 패킷은 주소 형식 검증을 통과하지 못해 폐기됩니다. 그 소스 MAC 주소가 호스트 MAC 주소가 아닌 라우터 MAC 주소이기 때문입니다.

전역 IPv6 주소 구성

전역 IPv6 주소를 구성하려면 다음 단계를 수행합니다.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다.

제한 사항

ASA는 IPv6 애니캐스트 주소를 지원하지 않습니다.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
  - ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
  - ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 구성할 수 있습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

세부 단계

	명령	목적
1단계	ASA 5512-X 이상 및 ASAv: **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} ASASM: ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **예:** ciscoasa(config)# interface gigabithethernet 0/0	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. **port-channel** *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. 물리적 인터페이스 ID의 설명에 대한 내용은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성을 참조하십시오. 물리적 인터페이스 ID 또는 이중 인터페이스 ID의 끝에 *하위 인터페이스* ID를 추가하고 마침표(.)로 구분합니다. 다중 컨텍스트 모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.

	명령	목적
2단계	다음 중 하나를 수행합니다.	
	ipv6 address autoconfig 예: `ciscoasa(config-if)# ipv6 address autoconfig`	인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화합니다. 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 컨피그레이션에 구성된 호스트에서 라우터 광고 메시지를 보내지 않도록 지정하지만, 이 경우에는 ASA에서 라우터 광고 메시지를 전송합니다. 메시지를 보내지 않도록 하려면 **ipv6 nd suppress-ra** 명령을 참조하십시오.
	ipv6 address *ipv6-address/prefix-length* [**standby** *ipv6-address*] 예: `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48`	인터페이스에 전역 주소를 지정합니다. 전역 주소를 할당하면 인터페이스에 대한 Link-Local 주소가 자동으로 생성됩니다. **standby**는 장애 조치 쌍에서 보조 유닛 또는 장애 조치 그룹에서 사용하는 인터페이스 주소를 지정합니다.
	ipv6 address *ipv6-prefix/prefix-length* **eui-64** 예: `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98::/48 eui-64`	Modified EUI-64 형식을 사용하여 인터페이스 MAC 주소에서 생성된 인터페이스 ID와 지정된 접두사를 결합하여 인터페이스에 전역 주소를 할당합니다. 전역 주소를 할당하면 인터페이스에 대한 Link-Local 주소가 자동으로 생성됩니다. 스탠바이 주소를 지정하지 않아도 되며, 인터페이스 ID가 자동으로 생성됩니다.
3단계	(선택 사항) **ipv6 enforce-eui64** *if_name* 예: `ciscoasa(config)# ipv6 enforce-eui64 inside`	로컬 링크의 IPv6 주소에서 반드시 Modified EUI-64 형식 인터페이스 식별자를 사용하게 합니다. *if_name* 인수는 **nameif** 명령으로 지정된, 주소 형식 강제 적용을 활성화하고 있는 인터페이스의 이름입니다. 자세한 내용은 11-11 페이지의 Modified EUI-64 인터페이스 ID를 참조하십시오.

IPv6 Neighbor Discovery 구성

IPv6 Neighbor Discovery를 구성하려면 25 장, "IPv6 인접 디바이스 검색"을 참조하십시오.

동일한 보안 레벨 통신 허용

기본적으로 동일한 보안 레벨의 인터페이스는 서로 통신할 수 없고 패킷이 동일한 인터페이스에 들어오고 나갈 수 없습니다. 이 섹션에서는 인터페이스의 보안 수준이 동일할 때 인터페이스 간 통신을 수행하는 방법, 그리고 인터페이스 내 통신을 수행하는 방법에 대해 설명합니다.

인터페이스 간 통신에 대한 정보

동일한 보안 수준에서 각 인터페이스끼리 서로 통신을 수행할 수 있도록 허용할 경우 다음과 같은 이점이 제공됩니다.

- 101개 이상의 통신 인터페이스를 구성할 수 있습니다.

인터페이스마다 다른 수준을 사용하고 인터페이스에 동일한 보안 수준을 할당하지 않을 경우, 수준(0~100) 하나당 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.

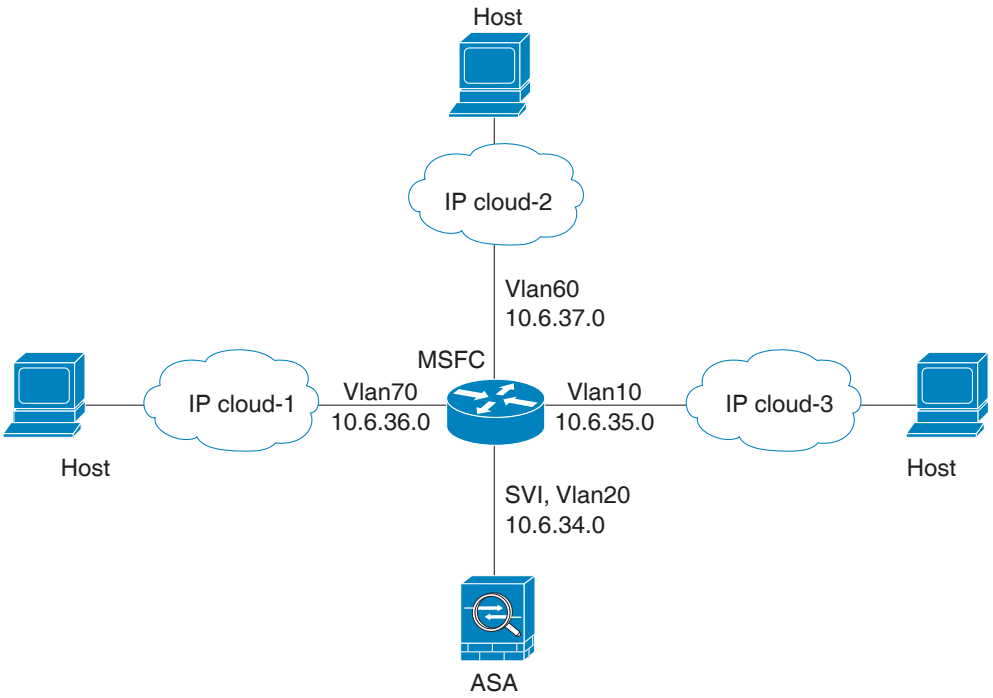
인터페이스 내 통신 정보

인터페이스 내 통신은 인터페이스에 들어오지만 동일한 인터페이스 밖으로 라우팅되는 VPN 트래픽에 유용할 수 있습니다. 이 경우 VPN 트래픽이 암호화되지 않거나 다른 VPN 연결을 위해 다시 암호화될 수 있습니다. 예를 들어, 허브 및 스포크 VPN 네트워크가 있다고 가정했을 때 ASA가 허브이고 원격 VPN 네트워크가 스포크라면, 한 스포크가 다른 스포크와 통신을 수행할 경우 트래픽은 ASA로 들어갔다 나온 후 다시 다른 스포크로 들어가야 합니다.

참고 이 기능을 통해 허용되는 모든 트래픽은 여전히 방화벽 규칙의 적용을 받습니다. 비대칭 라우팅 현상을 초래하지 않도록 주의하십시오. 이 경우 반환 트래픽이 ASA로 이동하지 않는 결과가 발생할 수 있습니다.

ASASM의 경우 이 기능을 활성화하기 전에, MSFC를 먼저 올바르게 구성하여 패킷이 스위치를 직접 통해 목적지 호스트에서 전송되는 대신 ASA MAC 주소로 전송되도록 해야 합니다. 그림 11-1에는 동일한 인터페이스의 호스트 간에 통신을 수행해야 하는 네트워크가 나와 있습니다.

그림 11-1 동일한 인터페이스에 있는 호스트 간의 통신



다음 샘플 컨피그레이션에는 Cisco IOS **route-map** 명령을 사용하여 그림 11-1에 표시된 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
```

세부 단계

명령	목적
same-security-traffic permit inter-interface	동일한 보안 레벨에서 인터페이스를 활성화하여 서로 통신할 수 있게 합니다.
same-security-traffic permit intra-interface	동일한 인터페이스에 연결된 호스트 간의 통신을 활성화합니다.

인터페이스 끄기 및 켜기

이 섹션에서는 인터페이스를 끄고 켜는 방법을 설명합니다.

모은 인터페이스는 기본적으로 활성화되어 있습니다. 다중 컨텍스트 모드에서는 어떤 컨텍스트 내에서 인터페이스를 비활성화하거나 다시 활성화할 경우 그 컨텍스트 인터페이스에만 적용됩니다. 그러나 시스템 실행 영역에서 인터페이스를 비활성화하거나 다시 활성화하면 모든 컨텍스트의 해당 인터페이스에 적용됩니다.

세부 단계

	명령	목적
1단계	ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} 예: ciscoasa(config)# interface vlan 100	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. 다중 컨텍스트 모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**shutdown** 예: ciscoasa(config-if)# shutdown	인터페이스를 비활성화합니다.
3단계	**no shutdown** 예: ciscoasa(config-if)# no shutdown	인터페이스를 다시 활성화합니다.

인터페이스 모니터링

인터페이스를 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
show interface	인터페이스 통계를 표시합니다.
show interface ip brief	인터페이스 IP 주소와 상태를 표시합니다.

라우팅 모드의 인터페이스 기능 기록

표 11-1에서는 이 기능의 출시 내역을 정리합니다.

표 11-1 인터페이스의 기능 기록

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 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. 이제 20개의 전 기능 인터페이스를 지원하므로, 백업 ISP 인터페이스를 무력화하기 위해 백업 인터페이스 명령을 사용할 필요 없습니다. 이 목적으로 전 기능 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.
ASA 5510 Security Plus 라이센스의 기가비트 이더넷 지원	7.2(3)	ASA 5510 Security Plus 라이센스는 포트 0과 포트 1에서 GE(기가비트 이더넷)를 지원합니다. Base 라이센스를 Security Plus 라이센스로 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.

표 11-1 인터페이스의 기능 기록(계속)

기능 이름	릴리스	기능 정보
ASA 5505의 VLAN 기본 지원	7.2(4)/8.0(4)	ASA 5505 트렁크 포트에 기본 VLAN을 포함할 수 있습니다. 다음 명령을 도입했습니다. **switchport trunk native vlan**
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 표준 최대 크기인 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 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. 도입된 명령: **jumbo-frame reservation**
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
투명 모드의 IPv6 지원	8.2(1)	투명 방화벽 모드를 위한 IPv6 지원을 도입했습니다.
ASA 5580 10기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(2)	흐름 제어를 위해 Pause(XOFF) 프레임을 활성화할 수 있습니다. 도입된 명령: **flowcontrol**

12 장

투명 모드 인터페이스

이 장에서는 투명 방화벽 모드의 모든 모델에서 인터페이스 컨피그레이션을 완료하는 작업을 다룹니다.

참고 다중 상황모드에서는 상황실행 영역에서 이 섹션의 작업을 수행합니다. 구성할 상황으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

투명 모드 인터페이스에 대한 정보

투명 모드의 브리지 그룹

보안 상황의 오버헤드를 원치 않을 경우 또는 보안 상황 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 트래픽이 Cisco ASA 내의 다른 브리지 그룹으로 라우팅되지 않으며, 반드시 ASA를 나와야 외부 라우터에 의해 ASA의 다른 브리지 그룹으로 라우팅될 수 있습니다. 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 상황에서 한 브리지 그룹의 보안 상황를 사용합니다. 상황마다 또는 단일 모드에서 하나 이상의 브리지 그룹이 필요합니다.

각 브리지 그룹에는 관리 IP 주소가 필요합니다. 다른 관리 방법에 대해서는 9-2 페이지의 관리 인터페이스를 참조하십시오.

참고 ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

보안 레벨

각 인터페이스는 0(가장 낮음)~100(가장 높음)의 보안 레벨이 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. 자세한 내용은 12-16 페이지의 동일한 보안 레벨 통신 허용을 참조하십시오.

이 레벨은 다음 동작을 제어합니다.

- 네트워크 액세스—기본적으로 상위 보안 인터페이스에서 하위 보안 인터페이스로 암시적 허용이 이루어집니다(아웃바운드). 상위 보안 인터페이스의 호스트는 하위 보안 인터페이스의 어떤 호스트에도 액세스할 수 있습니다. 인터페이스에 ACL을 적용하여 액세스를 제한할 수 있습니다.

  동일한 보안 인터페이스에 대한 통신을 활성화할 경우(12-16 페이지의 동일한 보안 레벨 통신 허용 참조), 해당 인터페이스에서 보안 레벨이 같거나 더 낮은 다른 인터페이스에 액세스하는 것이 암시적으로 허용됩니다.

- 검사 엔진—일부 애플리케이션 검사 엔진은 보안 레벨에 좌우됩니다. 동일한 보안 인터페이스에서는 검사 엔진이 어느 방향의 트래픽에도 적용됩니다.
  - NetBIOS 검사 엔진—아웃바운드 연결에만 적용됩니다.
  - SQL*Net 검사 엔진—어떤 호스트 쌍에 SQL*Net(이전의 OraServ) 포트에 대한 제어 연결이 있을 경우 인바운드 데이터 연결만 ASA에서 허용됩니다.

- 필터링—HTTP(S) 및 FTP 필터링은 아웃바운드 연결(상위에서 하위로)에만 적용됩니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 어느 방향의 트래픽도 필터링할 수 있습니다.

- **established** 명령—이 명령은 상위 보안 호스트에서 하위 보안 호스트로의 연결이 이미 설정된 경우 하위 호스트에서 상위 호스트로 돌아가는 연결을 허용합니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 양방향 모두에 **established** 명령을 구성할 수 있습니다.

투명 모드 인터페이스를 위한 라이센스 요건

모델	라이센스 요건
ASA 5512-X	VLAN: Base License: 50 Security Plus License: 100 모든 유형의 인터페이스: Base License: 716 Security Plus License: 916
ASA 5515-X	VLAN: Base License: 100 모든 유형의 인터페이스: Base License: 916
ASA 5525-X	VLAN: Base License: 200 모든 유형의 인터페이스: Base License: 1316
ASA 5545-X	VLAN: Base License: 300 모든 유형의 인터페이스: Base License: 1716
ASA 5555-X	VLAN: Base License: 500 모든 유형의 인터페이스: Base License: 2516
ASA 5585-X	VLAN: Base 및 Security Plus License: 1024 SSP-10 및 SSP-20을 위한 인터페이스 속도: Base License—파이버 인터페이스용 1기가비트 이더넷 10GE I/O 라이센스(Security Plus)—파이버 인터페이스용 10기가비트 이더넷 (SSP-40 및 SSP-60은 10기가비트 이더넷을 기본적으로 지원) 모든 유형의 인터페이스: Base 및 Security Plus License: 4612

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다. 예:

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

모든 유형의 인터페이스는 통합된 인터페이스의 최대 개수로 구성되며 여기에는 VLAN, 물리적, 이중화, 브릿지 그룹, EtherChannel 인터페이스가 해당됩니다. 컨피그레이션에 정의된 모든 **interface** 명령은 이 한도의 대상이 됩니다. 예를 들어, GigabitEthernet 0/0 인터페이스가 port-channel 1의 일부로 정의된 경우 다음 인터페이스 둘 다 대상이 됩니다.
interface gigabitethernet 0/0
및
interface port-channel 1

모델	라이센스 요건
ASASM	VLAN: Base License: 1000

투명 모드 인터페이스의 가이드라인 및 제한 사항

이 섹션에서는 이 기능에 대한 가이드라인과 제한 사항을 소개합니다.

상황모드 가이드라인

- 다중 상황모드의 ASA 5512-X 이상에서는 시스템 실행 영역에서 9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"에 따라 물리적 인터페이스를 구성합니다. 그런 다음 상황실행 영역에서 이 장의 내용에 따라 논리적 인터페이스 매개 변수를 구성합니다. 다중 상황모드의 ASASM에서는 스위치에서 스위치 포트와 VLAN을 구성하고 3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"에 따라 ASASM에 VLAN을 지정합니다.

  ASAv는 다중 상황모드를 지원하지 않습니다.
- 시스템 컨피그레이션에서 **allocate-interface** 명령을 사용하여 이미 상황에 지정한 상황인터페이스만 구성할 수 있습니다.

방화벽 모드 가이드라인

- 단일 모드에서 또는 다중 모드는 상황마다 최대 250개의 브리지 그룹을 구성할 수 있습니다. 하나 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다.
- IPv4에서는 관리 트래픽과 ASA를 거칠 트래픽 모두 브리지 그룹마다 관리 IP 주소가 필요합니다.

  인터페이스마다 IP 주소가 필요한 라우티드 모드와 달리, 투명 방화벽은 브리지 그룹 전체에 IP 주소가 지정됩니다. ASA에서는 ASA에서 시작하는 패킷(예: 시스템 메시지 또는 AAA 통신)의 소스 주소로 이 IP 주소를 사용합니다. 브리지 그룹 관리 주소 외에도 일부 모델에서는 관리 인터페이스를 구성할 수도 있습니다. 자세한 내용은 9-2 페이지의 관리 인터페이스를 참조하십시오.

  관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다. ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다. 관리 IP 서브넷에 대한 자세한 내용은 12-6 페이지의 브리지 그룹 구성을 참조하십시오.
- IPv6에서는 적어도 전달할 트래픽에 대해서는 인터페이스마다 링크-로컬 주소를 구성해야 합니다. ASA 관리 기능을 포함하여 모든 기능을 제공하려면 브리지 그룹마다 전역 IPv6 주소를 구성해야 합니다.

- 다중 상황모드에서는 상황마다 다른 인터페이스를 사용해야 합니다. 여러 상황에서 한 인터페이스를 공유할 수 없습니다.
- 다중 상황모드에서는 일반적으로 상황마다 다른 서브넷을 사용합니다. 겹치는 서브넷을 사용할 수도 있으나, 네트워크 토폴로지상 라우터 및 NAT 컨피그레이션에서 라우팅과 관련하여 이를 허용해야 합니다.

장애 조치 가이드라인

이 장의 절차를 사용하여 장애 조치 인터페이스 구성을 마쳐서는 안 됩니다. 장애 조치 및 상태 링크 구성에 대해서는 7 장, "고가용성을 위한 장애 조치"를 참조하십시오. 다중 상황모드에서는 시스템 컨피그레이션에서 장애 조치 인터페이스가 구성됩니다.

IPv6 가이드라인

투명 모드에서는 IPv6 애니캐스트 주소를 지원하지 않습니다.

ASASM를 위한 VLAN ID 가이드라인

어떤 VLAN ID도 컨피그레이션에 추가할 수 있으나, 스위치에 의해 ASA에 지정된 VLAN만 트래픽을 전달할 수 있습니다. ASA에 지정된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다.

아직 스위치에 의해 ASA에 지정되지 않은 VLAN을 위해 인터페이스를 추가할 경우 그 인터페이스는 중지(down) 상태가 됩니다. VLAN을 ASA에 지정하면 인터페이스는 작동(up) 상태로 바뀝니다. 인터페이스 상태에 대한 자세한 내용은 **show interface** 명령을 참조하십시오.

투명 모드 인터페이스의 기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-12 페이지의 공장 기본 컨피그레이션을 참조하십시오.

기본 보안 레벨

기본 보안 레벨은 0입니다. 인터페이스의 이름을 "inside"로 지정한 다음 보안 레벨을 명시적으로 설정하지 않으면 ASA는 보안 레벨을 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.

ASASM의 인터페이스 기본 상태

- 단일 모드 또는 시스템 시행 영역에서는 VLAN 인터페이스가 기본적으로 활성화되어 있습니다.
- 다중 상황모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 인터페이스가 시스템 실행 영역에서도 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.

점보 프레임 지원

기본적으로 ASASM는 점보 프레임을 지원합니다. 12-11 페이지의 MAC 주소, MTU, TCP MSS 구성에 따라 원하는 패킷 크기의 MTU를 구성합니다.

투명 모드에서 인터페이스 컨피그레이션 완료

인터페이스 컨피그레이션 완료의 작업 흐름

1단계 모델에 따라 인터페이스를 설정합니다.

- ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
- ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
- ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"

2단계 (다중 상황모드) 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 상황에 인터페이스를 배정합니다.

3단계 (다중 상황모드) 구성할 상황로 변경하기 위해 **changeto context** *name* 명령을 입력합니다.

4단계 IPv4 주소를 포함하여 하나 이상의 브리지 그룹을 구성합니다. 12-6 페이지의 브리지 그룹 구성을 참조하십시오.

5단계 인터페이스가 속한 브리지 그룹, 인터페이스 이름, 보안 레벨 등 일반 인터페이스 매개 변수를 구성합니다. 12-7 페이지의 일반 인터페이스 매개 변수 구성을 참조하십시오.

6단계 (선택 사항) 관리 인터페이스를 구성합니다. 12-9 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)을 참조하십시오.

7단계 (선택 사항) MAC 주소 및 MTU를 구성합니다. 12-11 페이지의 MAC 주소, MTU, TCP MSS 구성을 참조하십시오.

8단계 (선택 사항) IPv6 주소 지정을 구성합니다. 12-14 페이지의 IPv6 주소 지정 구성을 참조하십시오.

9단계 (선택 사항) 두 인터페이스 간 통신을 허용하거나 트래픽이 동일한 인터페이스에 들어오고 나가는 것을 허용하는 방법 중 하나로 동일한 보안 레벨 통신을 허용합니다. 12-16 페이지의 동일한 보안 레벨 통신 허용을 참조하십시오.

브리지 그룹 구성

각 브리지 그룹에는 관리 IP 주소가 필요합니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. 관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. IPv4 트래픽의 경우 트래픽을 전달하려면 관리 IP 인터페이스가 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.

가이드라인 및 제한 사항

단일 모드에서 또는 다중 모드는 상황마다 최대 250개의 브리지 그룹을 구성할 수 있습니다. 하나 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.

참고 별도의 관리 인터페이스(지원되는 모델)에서는 컨피그레이션 불가한 브리지 그룹(ID 301)이 자동으로 컨피그레이션에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

세부 단계

	명령	목적
1단계	**interface bvi** *bridge_group_number* 예: `ciscoasa(config)# interface bvi 1`	브리지 그룹을 만듭니다. *bridge_group_number*는 1~250 범위의 정수입니다.
2단계	**ip address** *ip_address* [*mask*] [**standby** *ip_address*] 예: `ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2`	브리지 그룹의 관리 IP 주소를 지정합니다. 브리지 그룹에 호스트 주소(/32 또는 255.255.255.255)를 지정하지 마십시오. 또한 /30 서브넷(255.255.255.252)과 같이 3개 미만의 호스트 주소(업스트림 라우터, 다운스트림 라우터, 투명 방화벽 각각 하나씩)를 포함한 다른 서브넷은 사용하지 마십시오. ASA에서는 서브넷의 첫 주소 및 마지막 주소에 또는 이 주소로부터 모든 ARP 패킷을 폐기합니다. 따라서 /30 서브넷을 사용하고 그 서브넷에서 업스트림 라우터에 예약된 주소를 지정할 경우 ASA는 다운스트림 라우터에서 업스트림 라우터로 ARP 요청을 폐기합니다. ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다. **standby** 키워드와 주소는 장애 조치에 사용됩니다.

예

다음 예에서는 브리지 그룹 1의 관리 주소와 대기 주소를 설정합니다.

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

다음에 할 일

일반 인터페이스 매개 변수를 구성합니다. 12-7 페이지의 일반 인터페이스 매개 변수 구성을 참조하십시오.

일반 인터페이스 매개 변수 구성

이 절차에서는 각 투명 인터페이스의 이름, 보안 레벨, 브리지 그룹을 설정하는 방법에 대해 설명합니다.

별도의 관리 인터페이스를 구성하려면 12-9 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)을 참조하십시오.

ASA 5512-X 이상과 ASAv의 경우 다음 인터페이스 유형에 대한 인터페이스 매개 변수를 구성해야 합니다.

- 물리적 인터페이스
- VLAN 하위 인터페이스
- 이중 인터페이스
- EtherChannel 인터페이스

ASASM에서는 다음 인터페이스 유형에 대해 인터페이스 매개 변수를 구성해야 합니다.

- VLAN 인터페이스

가이드라인 및 제한 사항

- 브리지 그룹당 최대 4개의 인터페이스를 구성할 수 있습니다.
- 보안 레벨에 대한 자세한 내용은 12-2 페이지의 보안 레벨을 참조하십시오.
- 장애 조치를 사용하는 경우 장애 조치 및 상태 기반 시스템 대체 작동 통신 전용 인터페이스의 이름을 지정하는 데 이 절차를 사용하지 마십시오. 장애 조치 및 상태 링크 구성에 대해서는 7 장, "고가용성을 위한 장애 조치"를 참조하십시오.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
  - ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
  - ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"
- 다중 상황모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황인터페이스만 구성할 수 있습니다.
- 다중 상황모드에서는 상황실행 영역에서 이 절차를 완료합니다. 시스템에서 상황컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

세부 단계

	명령	목적
1단계	ASA 5512-X 이상 및 ASAv: **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} **예:** `ciscoasa(config)# interface gigabitethernet 0/0`	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. **port-channel** *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. 물리적 인터페이스 ID에 대한 설명은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성 섹션을 참조하십시오. 관리 인터페이스에는 이 절차를 사용하지 마십시오. 관리 인터페이스 구성에 대해서는 12-9 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)을 참조하십시오. 물리적 인터페이스 ID 또는 이중 인터페이스 ID의 끝에 *하위 인터페이스* ID를 추가하고 마침표(.)로 구분합니다. 다중 상황모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**bridge-group** *number* **예:** `ciscoasa(config-if)# bridge-group 1`	인터페이스를 브리지 그룹에 지정합니다. *number*는 1~100의 정수입니다. 최대 4개의 인터페이스를 하나의 브리지 그룹에 지정할 수 있습니다. 동일한 인터페이스를 둘 이상의 브리지 그룹에 지정할 수 없습니다.
3단계	**nameif** *name* **예:** `ciscoasa(config-if)# nameif inside`	인터페이스의 이름을 지정합니다. *name*은 최대 48자의 텍스트이며 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.
4단계	**security-level** *number* **예:** `ciscoasa(config-if)# security-level 50`	보안 레벨을 설정합니다. *number*는 0(가장 낮음)~100(가장 높음) 범위의 정수입니다.

다음에 할 일

- (선택 사항) 관리 인터페이스를 구성합니다. 12-9 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)을 참조하십시오.
- (선택 사항) MAC 주소 및 MTU를 구성합니다. 12-11 페이지의 MAC 주소, MTU, TCP MSS 구성을 참조하십시오.
- (선택 사항) IPv6 주소 지정을 구성합니다. 12-14 페이지의 IPv6 주소 지정 구성을 참조하십시오.

관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)

단일 모드에서 또는 상황별로 브리지 그룹 인터페이스와는 별개인 관리 인터페이스를 구성할 수 있습니다. 자세한 내용은 9-2 페이지의 관리 인터페이스를 참조하십시오.

제한 사항

- 9-2 페이지의 관리 인터페이스를 참조하십시오.
- 이 인터페이스는 브리지 그룹에 지정하지 마십시오. 컨피그레이션 불가한 브리지 그룹(ID 101)이 자동으로 컨피그레이션에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.
- 사용하는 모델에 관리 인터페이스가 없을 경우 데이터 인터페이스에서 투명 방화벽 모드를 관리해야 합니다. 이 절차를 건너뛰십시오(예: ASASM에서).
- 다중 상황모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 상황에서 공유할 수 없습니다. 상황별 관리를 위해 관리 인터페이스의 하위 인터페이스를 만들고 각 상황에 관리 하위 인터페이스를 할당할 수 있습니다. ASA 5512-X부터 ASA 5555-X까지는 관리 인터페이스에서 하위 인터페이스를 지원하지 않습니다. 따라서 상황별 관리를 위해서는 데이터 인터페이스에 연결해야 합니다.

전제 조건

- 9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"의 절차를 완료합니다.
- 다중 상황모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황인터페이스만 구성할 수 있습니다.
- 다중 상황모드에서는 상황실행 영역에서 이 절차를 완료합니다. 시스템에서 상황컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

세부 단계

	명령	목적
1단계	**interface** {{**port-channel** *number* | **management** *slot*/*port*}[.*subinterface*] | *mapped_name*} **예:** `ciscoasa(config)# interface management 0/0.1`	아직 인터페이스 컨피그레이션 모드가 아닐 경우 관리 인터페이스를 위한 인터페이스 컨피그레이션 모드를 시작합니다. **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. 또한 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 없습니다. 다중 상황모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**nameif** *name* **예:** `ciscoasa(config-if)# nameif management`	인터페이스의 이름을 지정합니다. *name*은 최대 48자의 텍스트이며 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.

	명령	목적
3단계	다음 중 하나를 수행합니다.	
	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`	직접 IP 주소를 설정합니다. **참고** 장애 조치에서 사용할 경우 IP 주소와 대기 주소를 직접 설정해야 합니다. DHCP가 지원되지 않습니다. *ip_address* 및 *mask* 인수는 인터페이스 IP 주소와 서브넷 마스크를 설정합니다. **standby** *ip_address* 인수는 장애 조치에 사용됩니다. 자세한 내용은 7-26 페이지의 액티브/스탠바이 장애 조치 구성 또는 7-30 페이지의 액티브/액티브 장애 조치 구성을 참조하십시오.
	ip address dhcp [**setroute**] 예: `ciscoasa(config-if)# ip address dhcp`	DHCP 서버에서 IP 주소를 얻습니다. **setroute** 키워드는 ASA에서 DHCP 서버가 제공한 기본 경로를 사용할 수 있게 합니다. DHCP 임대를 재설정하고 새 임대를 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.
4단계	**security-level** *number* 예: `ciscoasa(config-if)# security-level 50`	보안 레벨을 설정합니다. *number*는 0(가장 낮음)~100(가장 높음) 범위의 정수입니다.

다음에 할 일

- (선택 사항) MAC 주소 및 MTU를 구성합니다. 12-11 페이지의 MAC 주소, MTU, TCP MSS 구성을 참조하십시오.
- (선택 사항) IPv6 주소 지정을 구성합니다. 12-14 페이지의 IPv6 주소 지정 구성을 참조하십시오.

MAC 주소, MTU, TCP MSS 구성

이 섹션에서는 인터페이스의 MAC 주소를 구성하는 방법 및 MTU와 TCP MSS를 설정하는 방법을 설명합니다.

MAC 주소에 대한 정보

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

ASASM에서는 모든 VLAN이 백플레인에서 제공한 동일한 MAC 주소를 사용합니다.

이중 인터페이스는 사용자가 추가한 첫 번째 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 이 명령을 사용하여 이중 인터페이스에 MAC 주소를 지정하면 멤버 인터페이스 MAC 주소와 상관없이 이 주소가 사용됩니다.

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 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 다중 상황모드에서는 EtherChannel 포트 인터페이스를 비롯한 인터페이스에 고유한 MAC 주소를 자동으로 지정할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 다중 상황모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그 다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

다중 상황모드에서는 여러 상황가 하나의 인터페이스를 공유할 경우 각 상황에서 인터페이스에 고유한 MAC 주소를 지정할 수 있습니다. 이 기능 덕분에 ASA에서 손쉽게 알맞은 상황로 패킷을 분류할 수 있습니다. 고유한 MAC 주소 없이 공유 인터페이스를 사용할 수 있으나, 몇 가지 제한이 있습니다. 자세한 내용은 6-3 페이지의 ASA의 패킷 분류를 참조하십시오. 각 MAC 주소를 직접 지정하거나 상황에서 공유 인터페이스의 MAC 주소를 자동으로 생성할 수 있습니다. MAC 주소를 자동으로 생성하려면 6-24 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정을 참조하십시오. MAC 주소를 자동으로 생성한 경우 생성된 주소를 재정의하는 데 이 절차를 사용할 수 있습니다.

단일 상황모드에서는 또는 다중 상황모드에서 공유되지 않는 인터페이스에 대해서는 하위 인터페이스에 고유 MAC 주소를 지정해야 하는 경우가 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다.

MTU 및 TCP MSS에 대한 정보

9-7 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
  - ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
  - ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"
- 다중 상황모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황인터페이스만 구성할 수 있습니다.
- 다중 상황모드에서는 상황실행 영역에서 이 절차를 완료합니다. 시스템에서 상황컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.
- MTU를 1500보다 크게 늘리려면 점보 프레임을 지원하는 모델에서 9-24 페이지의 점보 프레임 지원 활성화에 따라 점보 프레임을 활성화합니다. ASASM에서는 기본적으로 점보 프레임을 지원하므로, 활성화할 필요 없습니다.

세부 단계

	명령	목적
1단계	ASA 5512-X 이상 및 ASAv: **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} ASASM: ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **예:** ciscoasa(config)# interface vlan 100	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. **redundant** *number* 인수는 이중 인터페이스 ID(예: **redundant 1**)입니다. **port-channel** *number* 인수는 EtherChannel 인터페이스 ID(예: **port-channel 1**)입니다. 물리적 인터페이스 ID에 대한 설명은 9-14 페이지의 물리적 인터페이스 활성화 및 이더넷 파라미터 구성 섹션을 참조하십시오. 물리적 인터페이스 ID 또는 이중 인터페이스 ID의 끝에 *하위 인터페이스* ID를 추가하고 마침표(.)로 구분합니다. 다중 상황모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**mac-address** *mac_address* [**standby** *mac_address*] **예:** ciscoasa(config-if)# mac-address 000C.F142.4CDE	이 인터페이스에 사설 MAC 주소를 지정합니다. *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. 장애 조치와 함께 사용하려면 **standby** MAC 주소를 설정합니다. 활성 유닛이 장애 조치되고 대기 유닛이 활성 상태가 되면, 네트워크 중단을 최소화하기 위해 새 활성 유닛에서 활성 MAC 주소를 사용하기 시작하고 기존 활성 유닛은 대기 주소를 사용합니다.
3단계	**mtu** *interface_name bytes* **예:** ciscoasa(config)# mtu inside 9200	MTU를 300바이트~9198(ASAv는 9000)바이트 범위에서 설정합니다. 기본값은 1500바이트입니다. **참고** 이중 또는 포트 채널 인터페이스를 위해 MTU를 설정하면 ASA는 모든 멤버 인터페이스에 이 설정을 적용합니다. 점보 프레임을 지원하는 모델에서 어떤 인터페이스에 1500보다 큰 값을 입력한 경우 점보 프레임 지원을 활성화해야 합니다. 9-24 페이지의 점보 프레임 지원 활성화를 참조하십시오.
4단계	**sysopt connection tcpmss** [**minimum**] *bytes* **예:** ciscoasa(config)# sysopt connection tcpmss 8500 ciscoasa(config)# sysopt connection tcpmss minimum 1290	최대 TCP 세그먼트 크기(바이트)를 48~임의의 최대값 범위에서 설정합니다. 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. minimum 기능은 기본적으로 비활성화되어 있습니다(0으로 설정됨).

다음에 할 일

(선택 사항) IPv6 주소 지정을 구성합니다. 12-14 페이지의 IPv6 주소 지정 구성을 참조하십시오.

IPv6 주소 지정 구성

이 섹션에서는 IPv6 주소 지정의 구성 방법을 설명합니다.

IPv6에 대한 정보

이 섹션에서는 IPv6를 구성하는 방법을 다룹니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- Global—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 이 주소는 인터페이스별로 구성하는 게 아니라 브리지 그룹마다 구성해야 합니다. 관리 인터페이스를 위해 전역 IPv6 주소를 구성할 수도 있습니다.
- Link-local—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 컨피그레이션에 또는 주소 확인, Neighbor Discovery와 같은 ND 기능에 사용할 수 있습니다. 링크-로컬 주소는 세그먼트에서만 사용 가능하고 인터페이스 MAC 주소에 연결되어 있으므로 인터페이스별로 링크-로컬 주소를 구성해야 합니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 구성한 경우 각 인터페이스에서 링크-로컬 주소가 자동으로 구성됩니다. 따라서 구체적으로 링크-로컬 주소를 구성할 필요 없습니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

참고 링크-로컬 주소만 구성하려면 명령 참조에서 **ipv6 enable**(자동 구성) 또는 **ipv6 address link-local**(수동 구성) 명령을 참조하십시오.

Modified 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.

```
%ASA-3-325003: 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. 라우터 뒤에 있는 호스트로부터 받은 패킷은 주소 형식 검증을 통과하지 못해 폐기됩니다. 그 소스 MAC 주소가 호스트 MAC 주소가 아닌 라우터 MAC 주소이기 때문입니다.

지원되지 않는 명령

다음 IPv6 명령은 라우터 기능을 필요로 하므로 투명 방화벽 모드에서 지원되지 않습니다.

- **ipv6 address autoconfig**
- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

전역 IPv6 주소 구성

브리지 그룹 또는 관리 인터페이스에 대해 전역 IPv6 주소를 구성하려면 다음 단계를 수행합니다.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다.

제한 사항

ASA는 IPv6 애니캐스트 주소를 지원하지 않습니다.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—9 장, "기본 인터페이스 컨피그레이션(ASA 5512-X 이상)"
  - ASASM—3 장, "Cisco ASA Services Module에 대한 스위치 컨피그레이션"
  - ASAv—10 장, "기본 인터페이스 컨피그레이션(ASAv)"
- 다중 상황모드에서는 시스템 컨피그레이션에서 6-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황인터페이스만 구성할 수 있습니다.
- 다중 상황모드에서는 상황실행 영역에서 이 절차를 완료합니다. 시스템에서 상황컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

세부 단계

	명령	목적
1단계	브리지 그룹: **interface bvi** *bridge_group_id* 관리 인터페이스: **interface** *management_interface_id* **예:** `ciscoasa(config)# interface bvi 1`	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다.
2단계	**ipv6 address** *ipv6-address/prefix-length* [**standby** *ipv6-address*] **예:** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48`	인터페이스에 전역 주소를 지정합니다. 전역 주소를 지정하면 인터페이스에 대해 (브리지 그룹은 멤버 인터페이스마다) 링크-로컬 주소가 자동으로 생성됩니다. **standby**는 장애 조치 쌍에서 보조 유닛 또는 장애 조치 그룹에서 사용하는 인터페이스 주소를 지정합니다. **참고** Modified EUI-64 인터페이스 ID를 인터페이스 ID로 사용하는 **eui-64** 키워드는 투명 모드에서 지원되지 않습니다.
3단계	(선택 사항) **ipv6 enforce-eui64** *if_name* **예:** `ciscoasa(config)# ipv6 enforce-eui64 inside`	로컬 링크의 IPv6 주소에서 반드시 Modified EUI-64 형식 인터페이스 식별자를 사용하게 합니다. *if_name* 인수는 **nameif** 명령으로 지정된, 주소 형식 강제 적용을 활성화하고 있는 인터페이스의 이름입니다. 자세한 내용은 12-14 페이지의 Modified EUI-64 인터페이스 ID를 참조하십시오.

IPv6 Neighbor Discovery 구성

IPv6 Neighbor Discovery를 구성하려면 25 장, "IPv6 인접 디바이스 검색"을 참조하십시오.

동일한 보안 레벨 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 방법을 설명합니다.

인터페이스 간 통신에 대한 정보

동일한 보안 레벨의 인터페이스 간 통신을 허용하는 기능은 모든 동일한 보안 인터페이스 간에 ACL 없이 자유로운 트래픽 이동을 지원하려는 경우에 유용합니다.

동일한 보안 인터페이스 통신을 활성화하더라도 기존처럼 여러 보안 레벨에서 인터페이스를 구성할 수 있습니다.

세부 단계

명령	목적
same-security-traffic permit inter-interface	동일한 보안 레벨에서 인터페이스를 활성화하여 서로 통신할 수 있게 합니다.

인터페이스 끄기 및 켜기

이 섹션에서는 인터페이스를 끄고 켜는 방법을 설명합니다.

모은 인터페이스는 기본적으로 활성화되어 있습니다. 다중 상황모드에서는 어떤 상황내에서 인터페이스를 비활성화하거나 다시 활성화할 경우 그 상황인터페이스에만 적용됩니다. 그러나 시스템 실행 영역에서 인터페이스를 비활성화하거나 다시 활성화하면 모든 상황의 해당 인터페이스에 적용됩니다.

세부 단계

	명령	목적
1단계	`ciscoasa(config)# interface {vlan number | mapped_name}` 예: `ciscoasa(config)# interface vlan 100`	아직 인터페이스 컨피그레이션 모드가 아닐 경우 인터페이스 컨피그레이션 모드를 시작합니다. 다중 상황모드에서는 **allocate-interface** 명령을 통해 지정된 인터페이스가 있으면 *mapped_name*을 입력합니다.
2단계	**shutdown** 예: `ciscoasa(config-if)# shutdown`	인터페이스를 비활성화합니다.
3단계	**no shutdown** 예: `ciscoasa(config-if)# no shutdown`	인터페이스를 다시 활성화합니다.

인터페이스 모니터링

명령	목적
show interface	인터페이스 통계를 표시합니다.
show interface ip brief	인터페이스 IP 주소와 상태를 표시합니다.
show bridge-group	브리지 그룹 정보를 표시합니다.

투명 모드 인터페이스 컨피그레이션의 예

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
```

투명 모드 인터페이스의 기능 내역

표 12-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 12-1 투명 모드 인터페이스의 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base License의 VLAN은 0개에서 10개로. • ASA5510 Security Plus License의 VLAN은 10개에서 25개로. • ASA5520 VLAN을 25개에서 100개로. • ASA5540 VLAN을 100개에서 200개로.
VLAN 증가	7.2(2)	ASA 5505 Security Plus License의 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. 이제 20개의 전 기능 인터페이스를 지원하므로, 백업 ISP 인터페이스를 무력화하기 위해 백업 인터페이스 명령을 사용할 필요 없습니다. 이 목적으로 전 기능 인터페이스를 사용할 수 있습니다. 백업 인터페이스 명령은 Easy 컨피그레이션에서 여전히 유용합니다. ASA 5510의 VLAN 한도도 늘어났습니다. Base License는 10개에서 50개로, Security Plus License는 25개에서 100개로 늘어났습니다. ASA 5520은 100개에서 150개로, ASA 5550은 200개에서 250개로 늘어났습니다.
ASA 5510 Security Plus License의 기가비트 이더넷 지원	7.2(3)	ASA 5510 Security Plus License는 포트 0과 포트 1에서 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 5505의 VLAN 기본 지원	7.2(4)/8.0(4)	ASA 5505 트렁크 포트에 기본 VLAN을 포함할 수 있습니다. 도입된 명령: **switchport trunk native vlan**
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 표준 최대 크기인 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 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. 도입된 명령: **jumbo-frame reservation**

표 12-1 투명 모드 인터페이스의 기능 내역(계속)

기능 이름	플랫폼 릴리스	기능 정보
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
투명 모드의 IPv6 지원	8.2(1)	투명 방화벽 모드를 위한 IPv6 지원을 도입했습니다.
ASA 5580 10기가비트 이더넷 인터페이스에서 흐름 제어를 위한 Pause 프레임 지원	8.2(2)	흐름 제어를 위해 Pause(XOFF) 프레임을 활성화할 수 있습니다. 도입된 명령: **flowcontrol**
투명 모드의 브리지 그룹	8.4(1)	보안 상황의 오버헤드를 원치 않을 경우 또는 보안 상황 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**
투명 모드 브리지 그룹 최대 개수 250개로 증가	9.3(1)	브리지 그룹의 최대 개수가 8개에서 250개로 늘어났습니다. 단일 모드에서 또는 다중 모드의 각 상황에서 최대 250개의 브리지 그룹을 구성할 수 있으며, 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 수정된 명령: **interface bvi**, **bridge-group**

4 파 트

기본 설정

13 장

기본 설정

이 장에서는 일반적으로 컨피그레이션의 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

- 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 컨텍스트 모드에서 스위치로부터 ASASM로 세션을 연결할 때 ASASM에서는 관리 컨텍스트에서 설정한 로그인 비밀번호를 사용합니다.
- 시스템에서 컨텍스트 컨피그레이션으로 변경하려면 **changeto context** *name* 명령을 입력합니다.

절차

1단계 ASA 또는 어떤 컨텍스트를 위한 호스트 이름을 지정합니다. 기본 호스트 이름은 "asa"입니다.

hostname *name*

예:

```
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 그 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.

2단계 ASA를 위한 도메인 이름을 지정합니다. 기본 도메인 이름은 default.domain.invalid입니다.

domain-name *name*

예:

```
ciscoasa(config)# domain-name example.com
```

ASA는 도메인 이름을 정규화되지 않은 이름에 접미사로 추가합니다. 예를 들어, 도메인 이름을 "example.com"으로 설정하고 "jupiter"라는 정규화되지 않은 이름으로 syslog 서버를 지정한 경우 ASA는 그 이름을 "jupiter.example.com"으로 정규화합니다.

3단계 enable 비밀번호를 변경합니다. 기본적으로 enable 비밀번호는 비어 있습니다.

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.

enable password *password*

예:

```
ciscoasa(config)# enable passwd Pa$$w0rd
```

password 인수는 대/소문자를 구분하는 비밀번호이며 영숫자와 특수 문자를 사용하여 최대 16자까지 가능합니다. 물음표와 공백을 제외하고 어떤 문자도 비밀번호에 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*

비밀번호는 암호화된 형태로 컨피그레이션에 저장되므로 비밀번호를 입력하더라도 원래의 비밀번호를 볼 수 없습니다. 비밀번호를 기본값으로 설정하려면, 즉 비워 두려면 어떤 비밀번호도 없이 **enable password** 명령을 입력합니다.

4단계 텔넷 액세스를 위한 로그인 비밀번호를 설정합니다. 기본 비밀번호가 없습니다.

로그인 비밀번호는 텔넷 인증을 구성하지 않은 경우 텔넷 액세스에 사용됩니다. **session** 명령을 사용하여 스위치에서 ASASM에 액세스할 때에도 이 비밀번호를 사용합니다.

{**passwd** | **password**} *password* [**encrypted**]

예:

```
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 제외하고 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.

관련 주제

35-18 페이지의 특별 권한 EXEC 모드에 액세스하기 위한 인증 구성(enable 명령))

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.

절차

1단계 ASA 콘솔 포트에 연결합니다.

2단계 ASA를 껐다가 다시 켭니다.

3단계 시작한 다음 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 컨피그레이션 레지스터 값을 업데이트하려면 다음 명령을 입력합니다.

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

5단계 ASA에서 시작 컨피그레이션을 무시하도록 설정하려면 다음 명령을 입력합니다.

```
rommon #1> confreg
```

ASA는 현재 컨피그레이션 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
```

6단계 나중에 복원할 수 있도록 현재 컨피그레이션 레지스터 값을 기록해 둡니다.

7단계 값을 변경하기 위해 프롬프트에서 **Y**를 입력합니다.

ASA 프롬프트에 새 값을 입력합니다.

8단계 "disable system configuration?" 값을 제외하고 모든 설정에 기본값을 적용합니다.

9단계 프롬프트에 **Y**를 입력합니다.

10단계 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 컨피그레이션 대신 기본 컨피그레이션을 로드합니다.

11단계 다음 명령을 입력하여 특별 권한 EXEC 모드에 액세스합니다.

```
ciscoasa# enable
```

12단계 비밀번호를 물으면 **Enter**를 누릅니다.

비밀번호는 비어 있습니다.

13단계 다음 명령을 입력하여 시작 컨피그레이션을 로드합니다.

```
ciscoasa# copy startup-config running-config
```

14단계 다음 명령을 입력하여 전역 컨피그레이션 모드에 액세스합니다.

```
ciscoasa# configure terminal
```

15단계 필요하다면 다음 명령을 입력하여 기본 컨피그레이션에서 비밀번호를 변경합니다.

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

16단계 다음 명령을 입력하여 기본 컨피그레이션을 로드합니다.

```
ciscoasa(config)# no config-register
```

기본 컨피그레이션 레지스터 값은 0x1입니다. 컨피그레이션 레지스터에 대한 자세한 내용은 명령 참조를 참조하십시오.

17단계 다음 명령을 입력하여 새 비밀번호를 시작 컨피그레이션에 저장합니다.

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506, 5506-W, ASA 5508의 비밀번호 복구

ASA 5506, 5506-W, 5508의 비밀번호를 복구하려면 다음 단계를 수행합니다.

절차

1단계 ASA 콘솔 포트에 연결합니다.

2단계 ASA를 껐다가 다시 켭니다.

3단계 시작한 다음 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 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 컨피그레이션 레지스터 값과 컨피그레이션 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
```

5단계 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 컨피그레이션 대신 기본 컨피그레이션을 로드합니다.

6단계 다음 명령을 입력하여 특별 권한 EXEC 모드에 액세스합니다.

```
ciscoasa# enable
```

7단계 비밀번호를 물으면 **Enter**를 누릅니다.

비밀번호는 비어 있습니다.

8단계 다음 명령을 입력하여 시작 컨피그레이션을 로드합니다.

```
ciscoasa# copy startup-config running-config
```

9단계 다음 명령을 입력하여 전역 컨피그레이션 모드에 액세스합니다.

```
ciscoasa# configure terminal
```

10단계 필요하다면 다음 명령을 입력하여 기본 컨피그레이션에서 비밀번호를 변경합니다.

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

11단계 다음 명령을 입력하여 기본 컨피그레이션을 로드합니다.

```
ciscoasa(config)# no config-register
```

기본 컨피그레이션 레지스터 값은 0x1입니다. 컨피그레이션 레지스터에 대한 자세한 내용은 명령 참조를 참조하십시오.

12단계 다음 명령을 입력하여 새 비밀번호를 시작 컨피그레이션에 저장합니다.

```
ciscoasa(config)# copy running-config startup-config
```

ASAv의 비밀번호 또는 이미지 복구

ASAv의 비밀번호 또는 이미지를 복구하려면 다음 단계를 수행합니다.

절차

1단계 실행 중인 컨피그레이션을 ASAv의 백업 파일에 복사합니다.

copy running-config *filename*

예:

```
ciscoasa# copy running-config backup.cfg
```

2단계 ASAv를 다시 시작합니다.

```
reload
```

3단계 GNU GRUB 메뉴에서 아래쪽 화살표를 누르고 **<filename> with no configuration load** 옵션을 선택한 다음 **Enter**를 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
```

예:

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

4단계 백업 컨피그레이션 파일을 실행 중인 컨피그레이션에 복사합니다.

```
copy filename running-config
```

예:

```
ciscoasa (config)# copy backup.cfg running-config
```

5단계 비밀번호를 초기화합니다.

```
enable password
```

예:

```
ciscoasa(config)# enable password cisco123
```

6단계 새 컨피그레이션을 저장합니다.

```
write memory
```

예:

```
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 컨피그레이션을 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 비활성화함으로써 허가받지 않은 사용자가 컨피그레이션을 보거나 다른 비밀번호를 삽입하는 것을 막을 수 있습니다. 이러한 경우 시스템을 정상 상태로 복원하려면 새 이미지와 백업 컨피그레이션 파일(있는 경우)을 로드합니다.

참고로 **service password-recovery** 명령이 컨피그레이션 파일에 나타납니다. CLI 프롬프트에서 이 명령을 입력하면 설정이 NVRAM에 저장됩니다. 설정을 변경할 유일한 방법은 CLI 프롬프트에 명령을 입력하는 것입니다. 이 명령의 다른 버전으로 새 컨피그레이션을 로드하면 설정이 변경되지 않습니다. (비밀번호 복구를 염두에 두고) ASA에서 시작할 때 시작 컨피그레이션을 무시하도록 구성된 상태에서 비밀번호 복구를 비활성화하면 ASA는 설정을 변경하여 평소와 같이 시작 컨피그레이션을 로드합니다. 장애 조치를 사용하는 경우, 대기 유닛이 시작 컨피그레이션을 무시하도록 구성되어 있다면 **no service password recovery** 명령이 대기 유닛에 복제될 때 컨피그레이션 레지스터도 동일하게 변경됩니다.

절차

1단계 비밀번호 복구를 비활성화합니다.

no service password-recovery

예:

```
ciscoasa (config)# no service password-recovery
```

날짜 및 시간 설정

참고 ASASM의 날짜와 시간을 설정하지 마십시오. 이 설정은 호스트 스위치로부터 받습니다.

표준 시간대 및 일광 절약 날짜 설정

표준 시간대 및 날짜 범위를 설정하려면 다음 단계를 수행합니다.

절차

1단계 표준 시간대를 설정합니다. 기본적으로 표준 시간대는 UTC이며, 일광 절약 시간 날짜 범위는 4월 첫 번째 일요일 2:00 a.m.부터 10월 마지막 일요일 2:00 a.m.까지입니다.

clock timezone *zone* [**-**]*hours* [*minutes*]

예:

```
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.

2단계 일광 절약 시간의 날짜 범위를 기본값에서 변경하려면 다음 명령 중 하나를 입력합니다. 기본 반복 날짜 범위는 3월 두 번째 일요일 2:00 a.m.부터 11월 첫 번째 일요일 2:00 a.m.의 일광 절약 시간에 맞게 시간이 자동으로 조정됩니다.

- 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 컨텍스트 모드에서는 시스템 컨피그레이션에서만 시간을 설정할 수 있습니다.

절차

1단계 NTP 서버를 통한 인증을 활성화합니다.

ntp authenticate

예:

```
ciscoasa(config)# ntp authenticate
```

2단계 신뢰 키가 될 인증 키 ID를 지정합니다. 이는 NTP 서버와의 인증에 필요합니다.

ntp trusted-key *key_id*

예:

```
ciscoasa(config)# ntp trusted-key 1
```

key_id 인수는 1~4294967295 범위의 값입니다. 여러 서버에서 사용할 수 있도록 여러 신뢰 키를 입력할 수 있습니다.

3단계 NTP 서버와 인증하기 위한 키를 설정합니다.

ntp authentication-key *key_id* **md5** *key*

예:

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
```

key_id 인수는 2단계에서 **ntp trusted-key** 명령으로 설정한 ID이고, *key* 인수는 최대 길이가 32자인 문자열입니다.

4단계 NTP 서버를 지정합니다.

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

예:

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
```

key_id 인수는 **ntp trusted-key** 명령으로 설정한 ID입니다.

source *interface_name* 키워드-인수 쌍은 라우팅 테이블의 기본 인터페이스를 사용하지 않을 경우 NTP 패킷의 발신 인터페이스를 지정합니다. 다중 컨텍스트 모드에서는 어떤 인터페이스도 포함하지 않으므로 관리 컨텍스트에 정의된 인터페이스 이름을 지정합니다.

prefer 키워드는 여러 서버의 정확도가 비슷할 경우 이 NTP 서버를 기본 서버로 설정합니다. NTP는 알고리즘을 사용하여 어떤 서버가 가장 정확한지 알아내고 그 서버와 동기화합니다. 서버의 정확도가 비슷할 경우 **prefer** 키워드로 그중에서 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.

절차

1단계 날짜 및 시간을 직접 설정합니다.

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

예:

```
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.

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
- 공유 라이센스

참고 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.

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.

절차

1단계 암호화 키를 생성하는 데 사용한 패스프레이즈를 설정합니다. 패스프레이즈는 8자~128자여야 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*]]

예:

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

참고 빔리번호가 명령 기록 버퍼에 로깅되지 않도록 대화형 프롬프트에서 비밀번호를 입력합니다.

no key config-key password-encrypt 명령을 사용할 때는 주의해야 합니다. 암호화된 비밀번호를 일반 텍스트 비밀번호로 바꾸기 때문입니다. 비밀번호 암호화를 지원하지 않는 소프트웨어 버전으로 다운그레이드할 때는 이 명령의 **no** 형식을 사용할 수 있습니다.

2단계 비밀번호 암호화를 활성화합니다.

password encryption aes

예:

```
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.

3단계 마스터 패스프레이즈의 런타임 값 및 그 결과 컨피그레이션을 저장합니다.

write memory

예:

```
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 컨텍스트에서 입력되지는 않았다면, 사용자 컨텍스트의 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 13-13 페이지의 마스터 패스프레이즈 삭제를 참조하십시오.
- 이 절차는 텔넷, SSH, HTTPS를 통한 ASDM과 같은 보안 세션에서만 가능합니다.

절차

1단계 마스터 패스프레이즈를 삭제합니다. 명령에 패스프레이즈를 입력하지 않으면 입력하라는 메시지가 나타납니다.

no key config-key password-encryption [*old_passphrase*]]

예:

```
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
```

2단계 마스터 패스프레이즈의 런타임 값 및 그 결과 컨피그레이션을 저장합니다.

write memory

예:

```
ciscoasa(config)# write memory
```

패스프레이즈가 들어 있는 비휘발성 메모리가 지워지고 0xFF 패턴으로 덮어쓰기됩니다.

다중 컨텍스트 모드에서는 시스템 컨텍스트 컨피그레이션에서 마스터 패스프레이즈가 변경됩니다. 따라서 모든 컨텍스트의 패스프레이즈가 영향을 받습니다. **write memory** 명령이 시스템 컨텍스트 모드에서 입력되었지만 모든 사용자 컨텍스트에서 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.

절차

1단계 마스터 키 및 암호화된 비밀번호가 들어 있는 컨피그레이션을 삭제합니다.

write erase

예:

```
ciscoasa(config)# write erase
```

2단계 마스터 키 또는 암호화된 비밀번호 없는 시작 컨피그레이션으로 ASA를 다시 로드합니다.

reload

예:

```
ciscoasa(config)# reload
```

DNS 서버 구성

ASA에서 호스트 이름으로 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다.

DNS 서버 설정

일부 ASA 기능에서는 도메인 이름으로 외부 서버에 액세스하려면 DNS 서버를 사용해야 합니다. 예를 들어, 봇넷 트래픽 필터 기능은 동적 데이터베이스 서버에 액세스하고 고정 데이터베이스의 항목을 확인하는 데 DNS 서버가 필요합니다. **ping**, **traceroute** 명령과 같은 기타 기능에서는 ping하거나 traceroute하려는 이름을 입력할 수 있는데, ASA는 DNS 서버와 통신하면서 그 이름을 확인합니다. 여러 SSL VPN 및 인증서 명령도 이름을 지원합니다.

또한 액세스 규칙에서 정규화된 도메인 이름(FQDN) 네트워크 객체를 사용하려면 DNS 서버를 구성해야 합니다.

참고 ASA는 기능에 따라 DNS 서버 사용을 제한적으로 지원합니다. 예를 들어, 대부분의 명령에서는 IP 주소를 입력해야 하며 사용자가 어떤 이름과 IP 주소를 연결하기 위해 **name** 명령을 직접 구성하거나 **names** 명령을 사용하여 이름의 사용을 활성화하는 경우에만 이름을 사용할 수 있습니다.

시작하기 전에

DNS 서버에 연결할 수 있도록 DNS 도메인 조회를 활성화하는 어떤 인터페이스에서든 알맞은 라우팅 및 액세스 규칙을 구성해야 합니다.

절차

1단계 ASA에서 지원되는 명령에서 이름 조회가 가능하도록 DNS 서버에 DNS 요청을 보낼 수 있게 합니다.

dns domain-lookup *interface_name*

예:

```
ciscoasa(config)# dns domain-lookup inside
```

2단계 ASA에서 발신 요청에 사용하는 DNS 서버 그룹을 지정합니다.

dns server-group DefaultDNS

예:

```
ciscoasa(config)# dns server-group DefaultDNS
```

VPN 터널 그룹을 위해 다른 DNS 서버 그룹을 구성할 수 있습니다. 자세한 내용은 명령 참조에서 **tunnel-group** 명령을 참조하십시오.

3단계 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*]

예:

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

DNS 캐시 모니터링

ASA는 특정 클라이언트리스 SSSL VPN 및 인증서 명령에서 보낸 외부 DNS 쿼리의 DNS 정보를 로컬 캐시에 저장합니다. 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.

ASP(Accelerated Security Path) 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.

- 13-15 페이지의 규칙 엔진 트랜잭션 커밋 모델 선택
- 13-16 페이지의 ASP 로드 밸런싱 활성화

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 명령을 사용합니다.

asp rule-engine transactional-commit *option*

옵션:

- **access-group**—전역에 또는 인터페이스에 적용되는 액세스 규칙
- **nat**—네트워크 주소 변환 규칙

예:

```
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 흐름에 의한 오버런
- 비교적 과부하 상태인 인터페이스 수신 링으로 인한 오버런. 단일 코어에서 부하를 수용할 수 없음

asp load-balance per-packet 명령은 여러 코어가 단일 인터페이스 수신 링에서 받은 패킷을 동시에 작업할 수 있게 합니다. 시스템에서 패킷을 폐기하고 **show cpu** 명령 출력이 100%보다 훨씬 적은 경우, 패킷이 관련 없는 다수의 연결에 속한 것이라면 이 명령으로 처리량을 늘릴 수 있습니다. **auto** 옵션은 ASA에서 패킷별 로드 밸런싱을 자동으로 켜거나 끌 수 있게 합니다.

패킷별 로드 밸런싱의 자동 켜기/끄기를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# asp load-balance per-packet auto
```

기본 설정 기능 내역

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 강화하는 차원에서 텔넷을 사용하는 로그인에서는 먼저 기본 로그인 비밀번호를 직접 설정해야 합니다. **참고** 로그인 비밀번호는 텔넷 사용자 인증(**aaa authentication telnet console** 명령)을 구성하지 않은 경우에 텔넷에서만 사용됩니다. 이전에는 비밀번호를 지우면 ASA에서 기본값인 "cisco"로 변경했습니다. 이제는 비밀번호를 지우면 해당 비밀번호가 삭제됩니다. 이 로그인 비밀번호는 스위치에서 ASASM로 연결하는 텔넷 세션에도 사용됩니다(**session** 명령 참조). 최초로 ASASM에 액세스할 경우 로그인 비밀번호를 설정할 때까지 **service-module session** 명령을 사용해야 합니다. 수정된 명령: **passwd**
ASP 로드 밸런싱	9.3(2)	이 기능을 도입했습니다. ASP 로드 밸런싱 메커니즘은 CPU의 여러 코어에서 인터페이스 수신 링으로부터 패킷을 받고 독자적으로 작업할 수 있게 함으로써 패킷의 폐기를 줄이고 처리량을 늘립니다. 도입된 명령: **asp load-balance per-packet-auto**

14 장

동적 DNS

이 장에서는 DDNS(동적 DNS) 업데이트 메서드를 어떻게 구성하는지 설명합니다.

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.

관련 주제

- 15-4 페이지의 DHCP 서버 구성

DDNS 업데이트 컨피그레이션

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(정규화된 도메인 이름)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.

DDNS 지침

컨텍스트 모드 지침

DNS Client 창에서 투명 모드에서만 지원됩니다.

DDNS 구성

이 섹션에서는 DDNS 구성 방법을 설명합니다.

고정 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.

절차

1단계 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예:

```
ciscoasa(config)# ddns update method ddns-2
```

2단계 클라이언트가 DNS A RR과 PTR RR 모두 업데이트하도록 지정합니다.

ddns both

예:

```
ciscoasa(DDNS-update-method)# ddns both
```

3단계 인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 입력합니다.

interface *mapped_name*

예:

```
ciscoasa(DDNS-update-method)# interface eth1
```

4단계 DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

5단계 인터페이스에 대해 고정 IP 주소를 구성합니다.

ip address *ip_address* [*mask*] [**standby** *ip_address*]

예:

```
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.

절차

1단계 DHCP 클라이언트가 DHCP 서버에서 어떤 업데이트도 하지 않게끔 요청하도록 구성합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예:

```
ciscoasa(config)# dhcp-client update dns server none
```

2단계 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예:

```
ciscoasa(config)# ddns update method ddns-2
```

3단계 클라이언트가 DNS A RR과 PTR RR 모두 업데이트하도록 지정합니다.

ddns both

예:

```
ciscoasa(DDNS-update-method)# ddns both
```

4단계 인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 입력합니다.

interface *mapped_name*

예:

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

5단계 DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

6단계 DHCP를 사용하여 인터페이스의 IP 주소를 얻습니다.

ip address dhcp

예:

```
ciscoasa(if-config)# ip address dhcp
```

7단계 DHCP 서버에서 DDNS 업데이트를 수행하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예:

```
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.

절차

1단계 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예:

```
ciscoasa(config)# ddns update method ddns-2
```

2단계 클라이언트가 DNS A RR과 PTR RR 모두 업데이트하도록 지정합니다.

ddns both

예:

```
ciscoasa(DDNS-update-method)# ddns both
```

3단계 인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 입력합니다.

interface *mapped_name*

예:

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

4단계 DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

5단계 DHCP 클라이언트가 DHCP 서버에서 어떤 업데이트도 하지 않게끔 요청하도록 구성합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예:

```
ciscoasa(config)# dhcp-client update dns server none
```

6단계 DHCP를 사용하여 인터페이스의 IP 주소를 얻습니다.

ip address dhcp

예:

```
ciscoasa(if-config)# ip address dhcp
```

7단계 DHCP 서버가 클라이언트 업데이트 요청을 재정의하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예:

```
ciscoasa(if-config)# dhcpd update dns both override
```

PTR RR만 업데이트

서버에서 기본적으로 PTR RR 업데이트만 하도록 구성하려면 다음 단계를 수행합니다.

절차

1단계 인터페이스를 구성합니다.

interface *mapped_name*

예:

```
ciscoasa(config)# interface Ethernet0
```

2단계 DHCP 서버가 DNS A 및 PTR RR 모두 업데이트하도록 요청합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예:

```
ciscoasa(config-if)# dhcp-client update dns both
```

3단계 구성된 인터페이스에서 DHCP 클라이언트를 구성합니다.

ddns update [*method-name* | **hostname** *hostname*]

예:

```
ciscoasa(config-if)# ddns update hostname asa
```

4단계 DHCP 서버에서 DDNS 업데이트를 수행하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예:

```
ciscoasa(config-if)# dhcpd update dns
```

5단계 DHCP 클라이언트의 DNS 도메인 이름을 정의합니다.

dhcpd domain *domain_name* [**interface** *if_name*]

예:

```
ciscoasa(config-if)# dhcpd domain example.com
```

클라이언트로 A RR 업데이트, 서버로 PTR RR 업데이트

클라이언트에서 A RR을 업데이트하고 서버에서 PTR RR을 업데이트하도록 구성하려면 다음 단계를 수행합니다.

절차

1단계 동적으로 DNS RR을 업데이트하는 DDNS 업데이트 메서드를 만듭니다.

ddns update method *name*

예:

```
ciscoasa(config)# ddns update method ddns-2
```

2단계 DDNS 업데이트 메서드를 지정합니다.

ddns both

예:

```
ciscoasa(DDNS-update-method)# ddns both
```

3단계 인터페이스를 구성합니다.

interface *mapped_name*

예:

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

4단계 DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개 변수를 구성합니다.

dhcp-client update dns [**server** {**both** | **none**}]

예:

```
ciscoasa(config-if)# dhcp-client update dns
```

5단계 DDNS 메서드를 인터페이스 및 업데이트 호스트 이름과 연결합니다.

ddns update [*method-name* | **hostname** *hostname*]

예:

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa
```

6단계 DHCP 서버에서 DDNS 업데이트를 수행하도록 구성합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

예:

```
ciscoasa(if-config)# dhcpd update dns
```

7단계 DHCP 클라이언트의 DNS 도메인 이름을 정의합니다.

dhcpd domain *domain_name* [**interface** *if_name*]

예:

```
ciscoasa(config-if)# dhcpd domain example.com
```

DDNS 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.

DDNS 기능 내역

표 14-1 DDNS 기능 내역

기능 이름	릴리스	기능 정보
DDNS	7.0(1)	이 기능을 도입했습니다. 도입된 명령: **ddns**, **ddns update**, **dhcp client update dns**, **dhcpd update dns**, **show running-config ddns**, **show running-config dns server-group**

15 장

DHCP 서비스

이 장에서는 DHCP 서버 또는 DHCP 릴레이를 구성하는 방법을 설명합니다.

DHCP 서버 소개

DHCP는 IP 주소와 같은 네트워크 컨피그레이션 매개 변수를 DHCP 클라이언트에 제공합니다. Cisco ASA는 ASA 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버를 제공할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 직접 네트워크 컨피그레이션 매개 변수를 제공합니다.

클라이언트는 DHCP 서버를 찾아 예약된 링크 범위(link-scoped) 멀티캐스트 주소를 사용하여 컨피그레이션 정보의 지정을 요청합니다. 따라서 클라이언트와 서버는 동일한 링크에 연결되어야 합니다. 그러나 사용 편의성, 경제성 또는 확장성이 중요한 경우에는 DHCP 클라이언트가 동일한 링크에 연결되지 않은 서버에 메시지를 보낼 수 있게 하는 것이 좋습니다. 클라이언트 네트워크에 상주할 수 있는 DHCP 릴레이가 클라이언트와 서버 사이에서 메시지를 전달하면 됩니다. 릴레이 에이전트 작업은 클라이언트에 투명하게 이루어집니다.

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.

RFC 3315에 규정된 DHCPv6(DHCP for IPv6)는 IPv6 DHCP 서버에서 IPv6 노드(즉 DHCP 클라이언트)에 네트워크 주소 또는 접두사, DNS 서버 주소와 같은 컨피그레이션 매개 변수를 보낼 수 있게 합니다. DHCPv6는 다음 멀티캐스트 주소를 사용합니다.

- All_DHCP_Relay_Agents_and_Servers(FF02::1:2)는 클라이언트에서 인접한(즉 on-link) 릴레이 에이전트 및 서버와 통신하는 데 사용하는 링크 범위 멀티캐스트 주소입니다. 모든 DHCPv6 서버와 릴레이 에이전트는 이 멀티캐스트 그룹의 멤버입니다.
- DHCPv6 릴레이 서비스 및 서버는 UDP 포트 547에서 메시지를 수신합니다. ASA DHCPv6 릴레이 에이전트는 UDP 포트 547과 All_DHCP_Relay_Agents_and_Servers 멀티캐스트 주소 모두에서 수신합니다.

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.

브로드캐스트를 수신하는 ASA의 인터페이스를 구성하여 DHCP 요청을 다른 인터페이스의 DHCP 서버에 전달하게 함으로써 이러한 문제를 해결할 수 있습니다.

DHCP 서비스를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

모든 ASA 모델에서 DHCP 클라이언트 주소의 최대 개수는 라이센스에 따라 달라집니다.

- 한도가 호스트 10개일 경우 최대 가용 DHCP 풀은 주소 32개입니다.
- 한도가 호스트 50개일 경우 최대 가용 DHCP 풀은 주소 128개입니다.
- 호스트 수가 무제한일 경우 최대 가용 DHCP 풀은 주소 256개입니다.

DHCP 서비스 지침

방화벽 모드 지침

투명 방화벽 모드에서 지원되지 않습니다. 자세한 내용은 15-3 페이지의 DHCP 릴레이 지침을 참조하십시오.

IPv6 지침

IPv6에서는 인터페이스 특정 DHCP 릴레이 서버를 지원하지 않습니다.

DHCP 서버 지침

- 최대 가용 DHCP 풀은 주소 256개입니다.
- ASA의 각 인터페이스에서 DHCP 서버를 1개만 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.
- ASA는 QIP DHCP 서버를 DHCP 프록시 서비스와 함께 사용하는 것을 지원하지 않습니다.
- DHCP 서버가 활성화되지 않으면 릴레이 에이전트도 활성화될 수 없습니다.

- ASA DHCP 서버는 BOOTP 요청을 지원하지 않습니다. 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스에서 DHCP 서버 또는 DHCP 릴레이 서비스를 활성화할 수 없습니다.
- ASA는 DHCP 요청을 수신하면 DHCP 서버에 검색(discovery) 메시지를 보냅니다. 이 메시지에는 그룹 정책에서 **dhcp-network-scope** 명령으로 구성된 IP 주소(서브네트워크 내)가 들어 있습니다. 서버가 그 서브네트워크에 속하는 주소 풀을 가진 경우, 검색 메시지의 소스 IP 주소가 아니라 그 주소에 풀 정보와 함께 제안(offer) 메시지를 보냅니다.
- 클라이언트가 연결하면 ASA는 서버 목록의 모든 서버에 검색 메시지를 보냅니다. 이 메시지에는 그룹 정책에서 **dhcp-network-scope** 명령으로 구성된 IP 주소(서브네트워크 내)가 들어 있습니다. ASA는 수신한 첫 번째 제안을 선택하고 나머지 제안은 폐기합니다. 서버가 그 서브네트워크에 속하는 주소 풀을 가진 경우, 검색 메시지의 소스 IP 주소가 아니라 그 주소에 풀 정보와 함께 제안(offer) 메시지를 보냅니다. 주소의 갱신이 필요한 경우 임대 서버(확보한 주소의 출처인 서버)와 주소 갱신을 시도합니다. DHCP 갱신이 지정된 재시도 횟수(4회)만큼 실패한 경우 ASA는 미리 지정된 기간이 지나면 DHCP 리바인드 단계로 진행합니다. 리바인드 단계에서는 ASA가 그룹의 모든 서버에 동시에 요청을 보냅니다. 고가용성 환경에서는 임대 정보가 공유됩니다. 즉 다른 모든 서버가 임대를 확인할 수 있으며, ASA는 바운드 상태로 돌아갑니다. 리바인드 단계에서 (3회 재시도 후) 서버 목록의 어떤 서버로부터도 응답이 없을 경우 ASA는 항목을 삭제합니다.

  예를 들어, 서버에 범위가 209.165.200.225~209.165.200.254, 마스크가 255.255.255.0인 풀이 있고 **dhcp-network-scope** 명령에 의해 지정된 IP 주소가 209.165.200.1이라면, 서버는 ASA에 보내는 제안 메시지를 통해 그 풀을 전송합니다.

  dhcp-network-scope 명령 설정은 VPN 사용자에게만 적용됩니다.

DHCP 릴레이 지침

- 단일 모드 및 각 컨텍스트에서 전역 서버와 인터페이스 특정 서버를 포함하여 최대 10개의 DHCPv4 릴레이 서버를 구성할 수 있으며, 각 인터페이스에는 최대 4개의 서버가 가능합니다.
- 단일 모드 및 각 컨텍스트에서 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 서비스가 활성화되었고 둘 이상의 DHCP 릴레이 서버가 정의되었으면, ASA는 정의된 DHCP 릴레이 서버 각각에 클라이언트 요청을 전달합니다. 클라이언트 DHCP 릴레이 바인딩이 제거될 때까지는 서버의 회신도 클라이언트에 전달됩니다. 이 바인딩은 ASA에서 DHCP 메시지 ACK, NACK, ICMP unreachable 또는 decline 중 하나를 받으면 제거됩니다.
- DHCP 프록시 서비스로 실행 중인 인터페이스에서 DHCP 릴레이 서비스를 활성화할 수 없습니다. 먼저 VPN DHCP 컨피그레이션을 삭제해야 합니다. 그러지 않으면 오류 메시지가 나타납니다. 이 오류는 DHCP 릴레이 및 DHCP 프록시 서비스 모두 활성화된 경우 발생합니다. DHCP 릴레이 또는 DHCP 프록시 서비스 중 하나만 활성화되어야 합니다.
- DHCP 릴레이 서비스는 투명 방화벽 모드에서 사용할 수 없습니다. 그러나 액세스 목록을 사용하는 방법으로 DHCP 트래픽을 허용할 수 있습니다. 투명 모드에서 DHCP 요청과 회신이 ASA를 지날 수 있게 하려면 2개의 액세스 목록을 구성해야 합니다. 하나는 내부 인터페이스에서 외부로 보내는 DHCP 요청을 허용하는 것이고 다른 하나는 반대 방향으로 서버의 회신을 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.
- 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.
- DHCP 클라이언트는 ASA에서 요청을 릴레이하는 DHCP 서버와 다른 인터페이스에 있어야 합니다.

DHCP 서버 구성

이 단원에서는 ASA에서 제공하는 DHCP 서버의 구성 방법을 설명합니다.

1단계 DHCP 서버를 활성화합니다. 15-4 페이지의 DHCP 서버 활성화를 참조하십시오.

2단계 고급 DHCP 옵션을 구성합니다. 15-5 페이지의 고급DHCP 옵션 구성을 참조하십시오.

3단계 DHCPv4 릴레이 에이전트와 DHCPv6 릴레이 에이전트 중 하나를 구성합니다. 15-9 페이지의 DHCPv4 릴레이 에이전트 구성 또는 15-11 페이지의 DHCPv6 릴레이 에이전트 구성을 참조하십시오.

DHCP 서버 활성화

ASA 인터페이스에서 DHCP 서버를 활성화하려면 다음 단계를 수행합니다.

절차

1단계 DHCP 주소 풀을 만듭니다. 그러면 ASA는 이 풀의 주소 중에서 지정된 기간 동안 사용할 주소 하나를 클라이언트에 지정합니다. 이 주소는 직접 연결 네트워크를 위한 변환되지 않은 로컬 주소입니다.

dhcpd address *ip_address if_name*

예:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

주소 풀이 ASA 인터페이스와 동일한 서브넷에 있어야 합니다.

2단계 (선택 사항) DNS 서버의 IP 주소를 지정합니다.

dhcpd dns *dns1* [*dns2*]

예:

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

3단계 (선택 사항) WINS 서버의 IP 주소를 지정합니다. 최대 2개의 WINS 서버를 지정할 수 있습니다.

dhcpd wins *wins1* [*wins2*]

예:

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

4단계 (선택 사항) 클라이언트에 적용할 임대 기간을 변경합니다. 임대 기간은 클라이언트가 할당받은 IP 주소를 임대 만료 전까지 사용할 수 있는 기간(초)과 같습니다. 0~1,048,575의 값을 입력합니다. 기본값은 3600초입니다.

dhcpd lease *lease_length*

예:

```
ciscoasa(config)# dhcpd lease 3000
```

5단계 (선택 사항) 도메인 이름을 구성합니다.

dhcpd domain *domain_name*

예:

```
ciscoasa(config)# dhcpd domain example.com
```

6단계 (선택 사항) ICMP 패킷을 위한 DHCP ping 시간 초과 값을 구성합니다. 주소 충돌을 방지하고자 ASA는 DHCP 클라이언트에 주소를 지정하기 전에 주소에 2개의 ICMP ping 패킷을 보냅니다.

dhcpd ping_timeout *milliseconds*

예:

```
ciscoasa(config)# dhcpd ping timeout 20
```

7단계 DHCP 클라이언트에 보내지는 기본 게이트웨이를 정의합니다. 기본 게이트웨이를 정의하는 데 **dhcpd option 3** 명령을 사용하지 않으면, DHCP 클라이언트는 기본적으로 DHCP 클라이언트에 가장 가까운 ASA 인터페이스 IP 주소를 사용합니다. ASA는 관리 인터페이스 IP 주소를 사용하지 않습니다. 따라서 DHCP ACK는 이 옵션을 포함하지 않습니다.

dhcpd option 3 ip *gateway_ip*

예:

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

8단계 ASA 내 DHCP 데몬이 활성화된 인터페이스에서 DHCP 클라이언트 요청을 수신할 수 있게 합니다.

dhcpd enable *interface_name*

예:

```
ciscoasa(config)# dhcpd enable outside
```

고급DHCP 옵션 구성

ASA는 정보 전송을 위해 RFC 2132, RFC 2562, RFC 5510에 규정된 DHCP 옵션을 지원합니다.

고급 DHCP 옵션을 사용하여 DHCP 클라이언트에 DNS, WINS, 도메인 이름 매개 변수를 제공할 수 있습니다. 또한 DHCP 자동 컨피그레이션 설정을 사용하여 이 값을 얻거나 직접 정의할 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.

IP 주소 반환

IP 주소 한두 개를 반환하는 DHCP 옵션을 구성하려면 다음 단계를 수행합니다.

절차

1단계 IP 주소 한두 개를 반환하는 DHCP 옵션을 구성합니다.

dhcpd option *code* **ip** *addr_1* [*addr_2*]

예:

```
ciscoasa(config)# dhcpd option 2 ip 10.10.1.1 10.10.1.2
```

문자열 반환

문자열을 반환하는 DHCP 옵션을 구성하려면 다음 단계를 수행합니다.

절차

1단계 문자열을 반환하는 DHCP 옵션을 구성합니다.

dhcpd option *code* **ascii** *text*

예:

```
ciscoasa(config)# dhcpd option 2 ascii examplestring
```

16진수 값 반환

16진수 값을 반환하는 DHCP 옵션을 구성하려면 다음 단계를 수행합니다.

절차

1단계 16진수 값을 반환하는 DHCP 옵션을 구성합니다.

dhcpd option *code* **hex** *value*

예:

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

참고 ASA는 사용자가 제공하는 옵션의 유형 및 값이 RFC 2132에 정의된 옵션 코드의 예상 유형 및 값과 일치하는지 확인하지 않습니다. 이를테면 **dhcpd option 46 ascii hello** 명령을 입력할 수 있습니다. RFC 2132에 따르면 옵션 46이 1자리의 16진수 값을 가져야 하지만 ASA는 이 컨피그레이션을 승인합니다. 옵션 코드와 그 유형 및 예상 값에 대한 자세한 내용은 RFC 2132를 참조하십시오.

표 15-1에서는 **dhcpd option** 명령에서 지원하지 않는 DHCP 옵션을 보여줍니다.

표 15-1 지원되지 않는 DHCP 옵션

옵션 코드	설명
0	DHCPOPT_PAD
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

DHCP 옵션 3, 66, 150은 Cisco IP Phone을 구성하는 데 사용됩니다. 이 옵션의 구성에 대한 자세한 내용은 15-7 페이지의 DHCP 서버로 Cisco IP Phone 구성을 참조하십시오.

DHCP 서버로 Cisco IP Phone 구성

Cisco IP Phone은 TFTP 서버에서 컨피그레이션을 다운로드합니다. Cisco IP Phone이 시작할 때 IP 주소 및 TFTP 서버 IP 주소 모두 미리 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.

참고 Cisco IP Phone은 DHCP 옵션 3도 요청에 포함할 수 있는데, 이는 기본 경로를 설정합니다.

하나의 요청에서 옵션 150과 66을 모두 포함할 수 있습니다. 그러면 ASA DHCP 서버는 두 옵션의 값이 ASA에 구성되어 있다면 둘 다 포함시켜 응답합니다.

임의의 옵션 번호

어떤 옵션 번호에도 사용할 정보를 보내려면 다음 단계를 수행합니다.

절차

1단계 RFC 2132에 규정된 대로 옵션 번호를 포함하는 DHCP 요청을 위한 정보를 제공합니다.

dhcpd option *number value*

예:

```
ciscoasa(config)# dhcpd option 2
```

옵션 66

옵션 66에 사용할 정보를 보내려면 다음 단계를 수행합니다.

절차

1단계 옵션 66을 위해 TFTP 서버의 IP 주소 또는 이름을 제공합니다.

dhcpd option 66 ascii *server_name*

예:

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

옵션 150

옵션 150에 사용할 정보를 보내려면 다음 단계를 수행합니다.

절차

1단계 옵션 150을 위해 TFTP 서버 한두 개의 IP 주소 또는 이름을 제공합니다.

dhcpd option 150 ip *server_ip1* [*server_ip2*]

예:

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
```

*server_ip1*은 기본 TFTP 서버의 IP 주소 또는 이름이고, *server_ip2*는 보조 TFTP 서버의 IP 주소 또는 이름입니다. 옵션 150을 사용하여 최대 2개의 TFTP 서버를 식별할 수 있습니다.

옵션 3

옵션 3에 사용할 정보를 보내려면 다음 단계를 수행합니다.

절차

1단계 기본 경로를 설정합니다.

dhcpd option 3 ip *router_ip1*

예:

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

DHCPv4 릴레이 에이전트 구성

DHCP 요청이 인터페이스에 들어올 때 ASA에서 그 요청을 릴레이할 DHCP 서버는 컨피그레이션에 따라 달라집니다. 다음 유형의 서버를 구성할 수 있습니다.

- 인터페이스 특정 DHCP 서버—DHCP 요청이 특정 인터페이스에 들어오면 ASA는 그 인터페이스에 특정된 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.

절차

1단계 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.

2단계 DHCP 클라이언트에 연결된 인터페이스에서 DHCP 릴레이 서비스를 활성화합니다. 여러 인터페이스에서 DHCP 릴레이를 활성화할 수 있습니다.

dhcprelay enable *interface*

예:

```
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
```

3단계 (선택 사항) DHCP 릴레이 주소를 처리할 수 있는 시간(초)을 설정합니다.

dhcprelay timeout *seconds*

예:

```
ciscoasa(config)# dhcprelay timeout 25
```

4단계 (선택 사항) DHCP 서버에서 ASA 인터페이스의 주소에 보낸 패킷의 첫 번째 기본 라우터 주소를 변경합니다.

dhcprelay setroute *interface_name*

예:

```
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 것을 추가합니다.

5단계 (선택 사항) 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 Option 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 그 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 ASA는 모든 DHCPv6 전역 서버에 그 요청을 릴레이합니다.

절차

1단계 클라이언트 메시지가 전달되는 IPv6 DHCP 서버 목적지 주소를 지정합니다.

ipv6 dhcprelay server *ipv6_address* [*interface*]

예:

```
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.

2단계 클라이언트 인터페이스에서 DHCPv6 릴레이 서비스를 활성화합니다.

ipv6 dhcprelay enable *interface*

예:

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

3단계 (선택 사항) DHCPv6 서버에서 릴레이 주소 처리를 위해 릴레이 바인딩을 거쳐 DHCPv6 클라이언트에 전달하는 응답에 허용된 시간(초)을 지정합니다.

ipv6 dhcprelay timeout *seconds*

예:

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 인수에 유효한 값의 범위는 1~3600입니다. 기본값은 60초입니다.

DHCP 서비스 모니터링

DHCP 서비스를 모니터링하려면 다음 명령을 참조하십시오.

- **show running-config dhcpd**

  이 명령은 현재 DHCP 컨피그레이션을 보여줍니다.
- **show running-config dhcprelay**

  이 명령은 현재 DHCP 릴레이 서비스 상태를 보여줍니다.
- **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.
- **clear config ipv6 dhcprelay**

  이 명령은 IPv6 DHCP 릴레이 컨피그레이션을 지웁니다.

DHCP 서비스 기능 내역

표 15-2 DHCP 서비스 기능 내역

기능 이름	플랫폼 릴리스	설명
DHCP	7.0(1)	ASA에서 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** 명령을 추가했습니다.
DHCPv6(DHCP for IPv6)	9.0(1)	IPv6 지원을 추가했습니다. 도입된 명령: **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**
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. 도입되거나 수정된 명령: **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 Option 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 그 패킷을 폐기합니다. 이제는 어떤 인터페이스를 신뢰받는 인터페이스로 지정함으로써 Option 82를 보존하고 패킷을 전달할 수 있습니다. 도입되거나 수정된 명령: **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 임대 갱신에 실패했을 때 클라이언트가 대체 서버에 리바인드하지 않았습니다. 어떤 명령도 도입하거나 수정하지 않았습니다.

5 파 트

개체 및 ACL

16 장

액세스 제어용 객체

객체는 재사용 가능한 컨피그레이션 요소로서 컨피그레이션에 사용됩니다. Cisco ASA 컨피그레이션에서 인라인 IP 주소, 서비스, 이름 등을 대신하여 객체를 정의하고 사용할 수 있습니다. 객체로 편리하게 컨피그레이션을 유지 관리할 수 있습니다. 한군데서 객체를 수정한 다음 이를 참조하는 다른 모든 곳에 적용할 수 있기 때문입니다. 객체가 없으면 한 번이 아니라 필요할 때마다 각 기능의 매개 변수를 수정해야 합니다. 예를 들어, 네트워크 객체에서 IP 주소와 서브넷 마스크를 정의하는 경우에 주소를 변경하려면 주소를 참조하는 모든 기능이 아니라 객체 정의에서만 주소를 변경하면 됩니다.

객체 관련 지침

IPv6 지침

다음 제약 사항과 함께 IPv6를 지원합니다.

- ASA는 IPv6 중첩 네트워크 객체 그룹을 지원하지 않습니다. 따라서 IPv6 항목의 객체를 다른 IPv6 객체 그룹으로 묶을 수 없습니다.
- IPv4 항목과 IPv6 항목을 하나의 네트워크 객체 그룹에서 혼합할 수 있습니다. NAT에 대해서는 혼합 객체 그룹을 사용할 수 없습니다.

추가 지침 및 제한

- 객체는 고유한 이름을 가져야 합니다. 객체와 객체 그룹이 동일한 이름 공간을 공유하기 때문입니다. "Engineering"이라는 이름의 네트워크 객체 그룹과 역시 "Engineering"이라는 이름의 서비스 객체 그룹을 만들고 싶다면 적어도 하나의 객체 그룹 이름은 그 끝에 식별자(또는 "태그")를 추가하여 고유하게 만들어야 합니다. 이를테면 "Engineering_admins"와 "Engineering_hosts"를 사용하여 식별하기에 편리한 고유한 객체 이름 그룹으로 만들 수 있습니다.
- 객체 이름은 영숫자와 .!@#$%^&()-_{} 문자를 포함하여 64자까지 가능합니다. 객체 이름은 대소문자를 구분합니다.
- 명령에서 사용되는 객체는 제거하거나 비워 둘 수 없습니다. 단, (**forward-reference enable** 명령을 사용하여) 전방 참조를 활성화한 경우는 제외합니다.

객체 구성

다음 섹션에서는 액세스 제어에서 주로 사용되는 객체를 구성하는 방법에 대해 설명합니다.

네트워크 객체 및 그룹 구성

네트워크 객체와 그룹은 IP 주소 또는 호스트 이름을 식별합니다. 액세스 제어 목록에서 이 객체를 사용하여 규칙을 간소화합니다.

네트워크 객체 구성

네트워크 객체는 호스트, 네트워크 IP 주소, IP 주소의 범위 또는 FQDN(정규화된 도메인 이름)을 포함할 수 있습니다.

또한 (FQDN 객체를 제외하고) 객체에 대해 NAT 규칙을 활성화할 수도 있습니다. 객체 NAT 구성에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

절차

1단계 객체 이름을 사용하여 네트워크 객체를 만들거나 수정합니다.

```
ciscoasa(config)# object network object_name
```

예

```
ciscoasa(config)# object network email-server
```

2단계 다음 명령 중 하나를 사용하여 객체에 주소를 추가합니다. 객체를 제거하려면 명령의 **no** 형식을 사용합니다.

- **host** {*IPv4_address* | *IPv6_address*}—단일 호스트의 IPv4 또는 IPv6 주소. 예를 들면 10.1.1.1 또는 2001:DB8::0DB8:800:200C:417A입니다.
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*}—네트워크의 주소. IPv4 서브넷의 경우 마스크 앞에 공백을 넣습니다(예: 10.0.0.0 255.0.0.0). IPv6의 경우 공백 없이 하나의 단위로 주소와 접두사를 넣습니다(예: 2001:DB8:0:CD30::/60).
- **range** *start_address end_address*—주소 범위. IPv4 또는 IPv6 범위를 지정할 수 있습니다. 마스크 또는 접두사를 포함하지 않습니다.
- **fqdn** [**v4** | **v6**] *fully_qualified_domain_name*—www.example.com과 같은 FQDN, 즉 호스트의 이름입니다. IPv4로 주소를 제한하려면 **v4**를, IPv6는 **v6**를 지정합니다. 주소 유형을 지정하지 않을 경우 IPv4로 간주합니다.

예

```
ciscoasa(config-network-object)# host 10.2.2.2
```

3단계 (선택 사항) 설명을 추가합니다.

```
ciscoasa(config-network-object)# description string
```

네트워크 객체 그룹 구성

네트워크 객체 그룹에는 여러 네트워크 객체뿐 아니라 인라인 네트워크 또는 호스트도 포함될 수 있습니다. 네트워크 객체 그룹이 IPv4 주소와 IPv6 주소를 모두 포함할 수도 있습니다.

그러나 NAT를 위한 객체 그룹 또는 FQDN 객체를 포함하는 객체 그룹은 IPv4와 IPv6의 혼합이 불가합니다.

절차

1단계 객체 이름을 사용하여 네트워크 객체 그룹을 만들거나 수정합니다.

```
ciscoasa(config)# object-group network group_name
```

예

```
ciscoasa(config)# object-group network admin
```

2단계 다음 명령을 하나 이상 사용하여 네트워크 객체 그룹에 객체 및 주소를 추가합니다. 객체를 제거하려면 명령의 **no** 형식을 사용합니다.

- **network-object host** {*IPv4_address* | *IPv6_address*}—단일 호스트의 IPv4 또는 IPv6 주소. 예를 들면 10.1.1.1 또는 2001:DB8::0DB8:800:200C:417A입니다.
- **network-object** {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}—네트워크 또는 호스트의 주소. IPv4 서브넷의 경우 마스크 앞에 공백을 넣습니다(예: 10.0.0.0 255.0.0.0). IPv6의 경우 공백 없이 하나의 단위로 주소와 접두사를 넣습니다(예: 2001:DB8:0:CD30::/60).
- **network-object object** *object_name*—기존 네트워크 객체의 이름.
- **group-object** *object_group_name*—기존 네트워크 객체 그룹의 이름.

예

```
ciscoasa(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
ciscoasa(config-network-object-group)# network-object 2001:db8:0:cd30::/60
ciscoasa(config-network-object-group)# network-object host 10.1.1.1
ciscoasa(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
ciscoasa(config-network-object-group)# network-object object existing-object-1
ciscoasa(config-network-object-group)# group-object existing-network-object-group
```

3단계 (선택 사항) 설명을 추가합니다.

```
ciscoasa(config-network-object-group)# description string
```

예

관리자 3명의 IP 주소를 포함하는 네트워크 그룹을 만들려면 다음 명령을 입력합니다.

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

여러 부서에서 특별 권한을 갖는 사용자의 네트워크 객체 그룹을 만들기 위해 다음 명령을 입력합니다.

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

이제 다음과 같이 세 그룹 모두 중첩시킵니다.

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

서비스 객체 및 서비스 그룹 구성

서비스 객체 및 그룹은 프로토콜과 포트를 식별합니다. 액세스 제어 목록에서 이 객체를 사용하여 규칙을 간소화합니다.

- 16-4 페이지의 서비스 객체 구성
- 16-5 페이지의 서비스 그룹 구성

서비스 객체 구성

서비스 객체는 단일 프로토콜, ICMP, ICMPv6, TCP, UDP 포트 또는 포트 범위를 포함할 수 있습니다.

절차

1단계 객체 이름을 사용하여 서비스 객체를 만들거나 수정합니다.

```
ciscoasa(config)# object service object_name
```

예

```
ciscoasa(config)# object service web
```

2단계 다음 명령 중 하나를 사용하여 객체에 서비스를 추가합니다. 객체를 제거하려면 명령의 **no** 형식을 사용합니다.

- **service** *protocol*—IP 프로토콜의 이름 또는 번호(0-255). 모든 프로토콜에 적용하려면 **ip**라고 지정합니다. 지원되는 키워드의 목록은 43-10 페이지의 프로토콜 및 애플리케이션을 참조하십시오.
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]—ICMP 또는 ICMP 버전 6 메시지를 위한 것입니다. 원한다면 이름 또는 번호(0-255)로 ICMP 유형을 지정하여 해당 메시지 유형으로 객체를 제한할 수 있습니다. 유형을 지정할 경우 그 유형(1-255)에 대한 ICMP 코드를 지정할 수 있습니다. 코드를 지정하지 않을 경우 모든 코드가 사용됩니다. ICMP 유형의 목록은 43-14 페이지의 ICMP 유형을 참조하십시오.

- **service** {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*]—TCP 또는 UDP. 원한다면 출발지, 목적지 또는 둘 다의 포트를 지정할 수 있습니다. 이름 또는 번호로 포트를 지정할 수 있습니다(목록은 43-11 페이지의 TCP 및 UDP 포트 참조). operator는 다음 중 하나가 될 수 있습니다.
  - **lt**—보다 작음
  - **gt**—보다 큼
  - **eq**—같음
  - **neq**—같지 않음
  - **range**—경계를 포함하는 값 범위. 이 연산자를 사용할 때는 2개의 포트 번호를 지정합니다(예: **range 100 200**).

예

```
ciscoasa(config-service-object)# service tcp destination eq http
```

3단계 (선택 사항) 설명을 추가합니다.

```
ciscoasa(config-service-object)# description string
```

서비스 그룹 구성

서비스 객체 그룹은 TCP 또는 UDP의 출발지/목적지 포트를 비롯하여 여러 프로토콜의 혼합을 포함할 수 있습니다.

시작하기 전에

여기서 설명하는 일반 서비스 객체 그룹을 사용하여 모든 서비스를 모델링할 수 있습니다. 그러나 ASA 8.3(1) 이전에 제공되었던 서비스 그룹 객체 유형도 여전히 구성 가능합니다. 이러한 레거시 객체로는 TCP/UDP/TCP-UDP 포트 그룹, 프로토콜 그룹, ICMP 그룹이 있습니다. 이 그룹의 내용은 일반 서비스 객체 그룹의 관련 컨피그레이션과 동일합니다. 단, ICMP 그룹은 ICMP6 또는 ICMP 코드를 지원하지 않습니다. 이 레거시 객체를 계속 사용하는 방법에 대한 자세한 지침은 Cisco.com에서 명령 참조의 **object-service** 명령에 대한 설명을 참조하십시오.

절차

1단계 객체 이름을 사용하여 서비스 객체 그룹을 만들거나 수정합니다.

```
ciscoasa(config)# object-group service group_name
```

예

```
ciscoasa(config)# object-group service general-services
```

2단계 다음 명령을 하나 이상 사용하여 서비스 객체 그룹에 객체 및 서비스를 추가합니다. 객체를 제거하려면 명령의 **no** 형식을 사용합니다.

- **service-object** *protocol*—IP 프로토콜의 이름 또는 번호(0-255). 모든 프로토콜에 적용하려면 **ip**라고 지정합니다. 지원되는 키워드의 목록은 43-10 페이지의 프로토콜 및 애플리케이션을 참조하십시오.
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]—ICMP 또는 ICMP 버전 6 메시지를 위한 것입니다. 원한다면 이름 또는 번호(0-255)로 ICMP 유형을 지정하여 해당 메시지 유형으로 객체를 제한할 수 있습니다. 유형을 지정할 경우 그 유형(1-255)에 대한 ICMP 코드를 지정할 수 있습니다. 코드를 지정하지 않을 경우 모든 코드가 사용됩니다. ICMP 유형의 목록은 43-14 페이지의 ICMP 유형을 참조하십시오.

- **service-object** {**tcp** | **udp** | **tcp-udp**} [**source** *operator port*] [**destination** *operator port*]—TCP, UDP 또는 둘 다를 위한 것입니다. 원한다면 출발지, 목적지 또는 둘 다의 포트를 지정할 수 있습니다. 이름 또는 번호로 포트를 지정할 수 있습니다(목록은 43-11 페이지의 TCP 및 UDP 포트 참조). operator는 다음 중 하나가 될 수 있습니다.
  - **lt**—보다 작음
  - **gt**—보다 큼
  - **eq**—같음
  - **neq**—같지 않음
  - **range**—경계를 포함하는 값 범위. 이 연산자를 사용할 때는 2개의 포트 번호를 지정합니다(예: **range 100 200**).
- **service-object object** *object_name*—기존 서비스 객체의 이름
- **group-object** *object_group_name*—기존 서비스 객체 그룹의 이름

예

```
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
ciscoasa(config-service-object-group)# service-object object my-service
ciscoasa(config-service-object-group)# group-object Engineering_groups
```

3단계 (선택 사항) 설명을 추가합니다.

```
ciscoasa(config-service-object-group)# description string
```

예

다음 예는 서비스 객체 그룹에 TCP 및 UDP 서비스를 모두 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

다음 예는 서비스 객체 그룹에 여러 서비스 객체를 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# object service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object service HTTPS
ciscoasa(config-service-object)# service tcp source range 1 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

로컬 사용자 그룹 구성

ID 방화벽을 지원하는 기능에서 사용할 로컬 사용자 그룹을 만들 수 있습니다. 확장 ACL에 이를 포함하는 방식이며, 그러면 확장 ACL은 액세스 규칙 등에 사용할 수 있습니다.

ASA는 Active Directory 도메인 컨트롤러에서 전역으로 정의된 사용자 그룹에 대한 LDAP 쿼리를 Active Directory 서버에 보냅니다. ASA에서는 ID 기반 규칙을 위해 이 그룹을 가져옵니다. 그러나 ASA에 로컬화된 네트워크 리소스가 있는 경우도 있습니다. 이러한 리소스는 전역으로 정의되지 않으며, 로컬화된 보안 정책에 따른 로컬 사용자 그룹을 필요로 합니다. 로컬 사용자 그룹은 중첩된 그룹 및 Active Directory에서 가져온 사용자 그룹을 포함할 수 있습니다. ASA에서는 로컬 그룹과 Active Directory 그룹을 통합합니다.

사용자는 로컬 사용자 그룹과 Active Directory에서 가져온 사용자 그룹에 속할 수 있습니다.

ACL에서 직접 사용자 이름과 사용자 그룹 이름을 사용할 수 있으므로, 다음과 같은 경우에만 로컬 사용자 그룹을 구성해야 합니다.

- LOCAL 데이터베이스에 정의된 사용자의 그룹을 만들려는 경우
- AD 서버에 정의된 단일 사용자 그룹에 속하지 않은 사용자 또는 사용자 그룹으로 하나의 그룹을 만들려 합니다.

ID 방화벽을 활성화하는 방법에 대한 자세한 내용은 31 장, "ID 방화벽"을 참조하십시오.

절차

1단계 객체 이름을 사용하여 사용자 객체 그룹을 만들거나 수정합니다.

```
ciscoasa(config)# object-group user group_name
```

예

```
ciscoasa(config)# object-group user admins
```

2단계 다음 명령을 하나 이상 사용하여 사용자 객체 그룹에 사용자 및 그룹을 추가합니다. 객체를 제거하려면 명령의 **no** 형식을 사용합니다.

- **user** [*domain_NETBIOS_name*\]*username*—사용자 이름. 도메인 이름 또는 사용자 이름에 공백이 있을 경우 도메인 이름과 사용자 이름을 따옴표로 묶어야 합니다. 도메인 이름은 (로컬 데이터베이스에 정의된 사용자의 경우) LOCAL이거나 **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* 명령에서 지정한 AD(Active Directory) 도메인 이름일 수 있습니다. AD 도메인에 정의된 사용자를 추가할 때 *user_name*은 고유하지 않을 수 있는 일반 이름(cn)이 아닌 고유한 Active Directory sAMAccountName이어야 합니다. 도메인 이름을 지정하지 않을 경우 기본값이 사용됩니다. 이는 LOCAL 또는 **user-identity default-domain** 명령에서 정의된 값입니다.
- **user-group** [*domain_NETBIOS_name*\\]*username*—사용자 그룹. 도메인 이름 또는 그룹 이름에 공백이 있을 경우 도메인 이름과 그룹 이름을 따옴표로 묶어야 합니다. 이중 \\가 도메인 이름과 그룹 이름을 구분합니다.
- **group-object** *object_group_name*—기존 사용자 객체 그룹의 이름.

예

```
ciscoasa(config-user-object-group)# user EXAMPLE\admin
ciscoasa(config-user-object-group)# user-group EXAMPLE\\managers
ciscoasa(config-user-object-group)# group-object local-admins
```

3단계 (선택 사항) 설명을 추가합니다.

```
ciscoasa(config-user-object-group)# description string
```

보안 그룹 객체 그룹 구성

Cisco TrustSec를 지원하는 기능에서 사용할 보안 그룹 객체 그룹을 만들 수 있습니다. 확장 ACL에 이를 포함하는 방식이며, 그러면 확장 ACL은 액세스 규칙 등에 사용할 수 있습니다.

Cisco TrustSec와 통합할 경우 ASA는 ISE에서 보안 그룹 정보를 다운로드합니다. ISE는 Cisco TrustSec 태그-사용자 ID 매핑 및 Cisco 태그-사용자 리소스 매핑을 수행하면서 ID 저장소의 역할을 합니다. 중앙의 ISE에서 보안 그룹 ACL을 프로비저닝하고 관리합니다.

그러나 ASA에 로컬화된 네트워크 리소스가 있는 경우도 있습니다. 이러한 리소스는 전역으로 정의되지 않으며, 로컬화된 보안 정책에 따른 로컬 보안 그룹을 필요로 합니다. 로컬 보안 그룹은 ISE에서 다운로드한 중첩 보안 그룹을 포함할 수 있습니다. ASA는 로컬 및 중앙 보안 그룹을 통합합니다.

ASA에서 로컬 보안 그룹을 만들려면 로컬 보안 객체 그룹을 만듭니다. 로컬 보안 객체 그룹은 중첩 보안 객체 그룹, 보안 ID 또는 보안 그룹 이름을 하나 이상 포함할 수 있습니다. 또한 ASA에 없는 보안 ID 또는 보안 그룹 이름을 새로 만들 수도 있습니다.

ASA에서 만든 보안 객체 그룹을 사용하여 네트워크 리소스에 대한 액세스를 제어할 수 있습니다. 보안 객체 그룹을 액세스 그룹 또는 서비스 정책의 일부로 사용할 수 있습니다.

ASA를 Trustsec와 통합하는 방법에 대한 자세한 내용은 32 장, "ASA 및 Cisco TrustSec"를 참조하십시오.

팁 ASA에 알려지지 않은 태그 또는 이름으로 그룹을 만들 경우, 그 그룹을 사용하는 어떤 규칙도 ISE에서 해당 태그 또는 이름을 확인할 때까지는 비활성 상태입니다.

절차

1단계 객체 이름을 사용하여 보안 그룹 객체 그룹을 만들거나 수정합니다.

```
ciscoasa(config)# object-group security group_name
```

예

```
ciscoasa(config)# object-group security mktg-sg
```

2단계 다음 명령을 하나 이상 사용하여 서비스 그룹 객체 그룹에 객체를 추가합니다. 객체를 제거하려면 명령의 **no** 형식을 사용합니다.

- **security-group** {**tag** *sgt_number* | **name** *sg_name*}—SGT(보안 그룹 태그) 또는 보안 그룹 이름. 태그는 1 ~ 65533의 번호이며 ISE에서 IEEE 802.1X 인증, 웹 인증 또는 MAB(MAC 인증 우회)를 통해 디바이스에 할당됩니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 유효한 태그 및 이름에 대해서는 ISE 컨피그레이션을 참조합니다.
- **group-object** *object_group_name*—기존 보안 그룹 객체 그룹의 이름.

예

```
ciscoasa(config-security-object-group)# security-group tag 1
ciscoasa(config-security-object-group)# security-group name mgkt
ciscoasa(config-security-object-group)# group-object local-sg
```

3단계 (선택 사항) 설명을 추가합니다.

```
ciscoasa(config-security-object-group)# description string
```

시간 범위 구성

시간 범위 객체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. ACL 규칙에서 이 객체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. 예를 들어, 업무 시간에만 특정 서버에 대한 액세스를 허용하는 액세스 규칙을 만들 수 있습니다.

참고 시간 범위 객체에 여러 기간 항목을 포함할 수 있습니다. 시간 범위에 절대값과 기간 값이 모두 지정된 경우, 절대 시작 시간에 도달해야 기간 값의 평가가 이루어지며 절대 종료 시간에 도달하면 더 이상 평가되지 않습니다.

시간 범위를 만들더라도 디바이스에 대한 액세스가 제한되지 않습니다. 이 절차에서는 시간 범위만 정의합니다. 그런 다음 액세스 제어 규칙에서 이 객체를 사용해야 합니다.

절차

1단계 시간 범위를 만듭니다.

time-range *name*

2단계 (선택 사항) 시간 범위에 시작 시간이나 종료 시간 또는 둘 다 추가합니다.

absolute [**start** *time date*] [**end** *time date*]

시작 시간을 지정하지 않을 경우 기본 시작 시간은 지금입니다.

*time*은 *hh*:*mm*의 24시간 형식입니다. 예를 들어, 8:00은 오전 8:00입니다. 그리고 20:00은 오후 8:00입니다.

*date*는 *일 월 연도* 형식입니다. 예를 들면, **1 January 2014**입니다.

3단계 (선택 사항) 반복 기간을 추가합니다.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

*days-of-the-week*에 다음 값을 지정할 수 있습니다. 첫 번째 인수에 하나의 요일을 지정한 경우에만 두 번째 요일을 지정할 수 있습니다.

- **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday** 또는 **Sunday**입니다. *days-of-the-week* 인수에 대해 둘 이상의 요일을 공백으로 구분하여 지정할 수 있습니다.
- **daily**
- **weekdays**
- **weekend**

*time*은 *hh*:*mm*의 24시간 형식입니다. 예를 들어, 8:00은 오전 8:00입니다. 그리고 20:00은 오후 8:00입니다.

이 명령을 반복하여 둘 이상의 반복 기간을 구성할 수 있습니다.

예

다음은 2006년 1월 1일 오전 8:00에 시작하는 절대 시간 범위의 예입니다. 종료 시간과 날짜가 지정되지 않았으므로 이 시간 범위는 무한정 유효합니다.

```
ciscoasa(config)# time-range for2006
ciscoasa(config-time-range)# absolute start 8:00 1 january 2006
```

다음은 주중 오전 8:00부터 오후 6:00까지의 주 단위 정기 시간 범위의 예입니다.

```
ciscoasa(config)# time-range workinghours
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
```

다음 예에서는 시간 범위의 종료일을 설정하고 주중 기간은 오전 8시~오후 5시로 설정하며 5시 이후의 시간은 월요일, 수요일, 금요일과 화요일, 목요일을 다르게 설정합니다.

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

객체 모니터링

객체와 그룹을 모니터링하려면 다음 명령을 입력합니다.

- **show access-list**

  액세스 목록 항목을 표시합니다. 객체를 포함한 항목이 그 객체 내용에 따라 개별 항목으로 확장됩니다.

- **show running-config object** [**id** *object_id*]

  모든 현재 객체를 표시합니다. 이름을 기준으로 단일 객체를 보려면 **id** 키워드를 사용합니다.

- **show running-config object** *object_type*

  그 유형, **네트워크** 또는 **서비스**를 기준으로 현재 객체를 표시합니다.

- **show running-config object-group** [**id** *group_id*]

  모든 현재 객체 그룹을 표시합니다. 이름을 기준으로 단일 객체 그룹을 보려면 **id** 키워드를 사용합니다.

- **show running-config object-group** *grp_type*

  그룹 유형을 기준으로 현재 객체 그룹을 표시합니다.

객체 관련 이력

기능 이름	플랫폼 릴리스	설명
객체 그룹	7.0(1)	객체 그룹으로 간단하게 ACL을 만들고 유지 관리할 수 있습니다. 도입되거나 수정된 명령: **object-group** *protocol*, **object-group** *network*, **object-group** *service*, **object-group** *icmp_type*
정규식 및 정책 맵	7.2(1)	검사 정책 맵에서 사용하기 위해 정규식과 정책 맵을 도입했습니다. **class-map type regex**, **regex**, **match regex** 명령을 도입했습니다.

기능 이름	플랫폼 릴리스	설명
객체	8.3(1)	객체 지원을 도입했습니다. 도입되거나 수정된 명령: **object-network**, **object-service**, **object-group** *network*, **object-group** *service*, **network object**, **access-list extended**, **access-list webtype**, **access-list remark**
ID 방화벽을 위한 사용자 객체 그룹	8.4(2)	ID 방화벽을 위한 사용자 객체 그룹을 도입했습니다. 도입된 화면: **object-network user**, **user**
Cisco TrustSec를 위한 보안 그룹 객체 그룹	8.4(2)	Cisco TrustSec를 위한 보안 그룹 객체 그룹을 도입했습니다. 도입된 화면: **object-network security**, **security**
IPv4/IPv6 혼합 네트워크 객체 그룹	9.0(1)	이전에는 네트워크 객체 그룹이 IPv4 주소만 또는 IPv6 주소만 포함할 수 있었습니다. 이제는 네트워크 객체 그룹에서 IPv4 주소와 IPv6 주소의 혼합을 지원합니다. **참고** NAT에는 혼합 객체 그룹을 사용할 수 없습니다. 수정된 명령: **object-group network**
확장 ACL 및 ICMP 코드를 기준으로 ICMP 트래픽을 필터링하기 위한 객체 개선 사항	9.0(1)	이제 ICMP 코드에 따라 ICMP 트래픽을 허용하거나 거부할 수 있습니다. 도입되거나 수정된 명령: **access-list extended**, **service-object**, **service**

액세스 제어 목록

ACL(액세스 제어 목록)은 다양한 기능에서 사용합니다. 인터페이스에 적용되거나 전역 범위에 액세스 규칙으로 적용되는 ACL은 어플라이언스를 지나는 트래픽을 허용하거나 거부합니다. 다른 기능에서는 해당 기능이 적용될 트래픽을 선택하면서 제어 서비스보다는 매칭 서비스를 수행합니다.

다음 섹션에서는 ACL의 기초와 ACL을 구성하고 모니터링할 방법을 설명합니다. 전역 범위에 또는 인터페이스에 적용되는 ACL인 액세스 규칙은 방화벽 컨피그레이션 가이드에서 자세히 설명합니다.

ACL 소개

ACL은 ACL 유형에 따라 소스 및 수신 IP 주소, IP 프로토콜, 포트, 이더 타입, 기타 매개 변수 등 하나 이상의 특성을 기준으로 삼아 트래픽 흐름을 식별합니다. ACL은 다양한 기능에서 사용됩니다. ACL은 하나 이상의 ACE(액세스 제어 항목)로 구성됩니다.

ACL 유형

ASA에서는 다음 유형의 ACL을 사용합니다.

- 확장 ACL—확장 ACL이 주요 사용할 유형입니다. 이 ACL은 해당 디바이스를 거치는 트래픽을 허용하거나 거부하는 액세스 규칙에 그리고 서비스 정책, AAA 정책, WCCP, 봇넷 트래픽 필터, VPN 그룹, DAP 정책과 같은 여러 기능에서 트래픽 매칭에 사용됩니다. 17-7 페이지의 확장 ACL 구성을 참조하십시오.
- 이더 타입 ACL—이더 타입 ACL은 투명 방화벽 모드에서 비 IP 레이어 2 트래픽에 적용됩니다. 레이어 2 트래픽의 이더 타입 값에 따라 트래픽을 허용하거나 거부하는 데 이 규칙을 사용할 수 있습니다. 이더 타입 ACL을 사용하면 해당 디바이스를 지나는 비 IP 트래픽의 흐름을 제어할 수 있습니다. 17-17 페이지의 이더 타입 ACL 구성을 참조하십시오.
- 웹 타입 ACL—웹 타입 ACL은 클라이언트리스 SSL VPN 트래픽을 필터링하는 데 사용됩니다. 이 ACL은 URL 또는 목적지 주소에 따라 액세스를 거부할 수 있습니다. 17-13 페이지의 웹 타입 ACL 구성을 참조하십시오.

- 표준 ACL—표준 ACL은 목적지 주소만으로 트래픽을 식별합니다. 경로 맵, VPN 필터와 같은 몇몇 기능에서만 이를 사용합니다. VPN 필터는 확장 액세스 목록도 지원하므로, 표준 ACL 사용은 경로 맵에 한정됩니다. 17-13 페이지의 표준 ACL 구성을 참조하십시오.

다음 표는 대표적인 ACL의 용도 및 사용되는 유형을 정리한 것입니다.

표 17-1 ACL 유형 및 대표적인 용도

ACL 용도	ACL 유형	설명
IP 트래픽의 네트워크 액세스 제어(라우팅 및 투명 모드)	확장	ASA에서는 확장 ACL에서 명시적으로 허용하지 않는 한 어떤 트래픽도 하위 보안 인터페이스에서 상위 보안 인터페이스로 이동할 수 없습니다. **참고** 관리 액세스를 위해 ASA 인터페이스에 액세스하는 경우에도 ACL에서 호스트 IP 주소를 허용할 필요 없습니다. 35 장, "관리 액세스"에 따라 관리 액세스를 구성하면 됩니다.
AAA 규칙을 위한 트래픽 식별	확장	AAA 규칙에서는 트래픽 식별에 ACL을 사용합니다.
특정 사용자를 위해 IP 트래픽에 대한 네트워크 액세스 제어 보완	확장, 사용자별 AAA 서버에서 다운로드	사용자에게 적용할 동적 ACL을 다운로드하도록 RADIUS 서버를 구성할 수 있습니다. 또는 서버가 이미 ASA에서 구성된 ACL의 이름을 전송할 수 있습니다.
VPN 액세스 및 필터링	확장 표준	원격 액세스 및 사이트 대 사이트 VPN을 위한 그룹 정책은 필터링에 표준 또는 확장 ACL을 사용합니다. 원격 액세스 VPN은 클라이언트 방화벽 컨피그레이션 및 동적 액세스 정책에도 확장 ACL을 사용합니다.
Modular Policy Framework를 위한 트래픽 클래스 맵에서 트래픽 식별	확장	Modular Policy Framework를 지원하는 기능에 쓰이는 클래스 맵에서 트래픽을 식별하는 데 ACL을 사용할 수 있습니다. Modular Policy Framework를 지원하는 기능으로는 TCP 및 일반 연결 설정, 검사 등이 있습니다.
투명 방화벽 모드에서 비 IP 트래픽을 위한 네트워크 액세스 제어	이더 타입	이더 타입에 따라 트래픽을 제어하는 ACL을 구성할 수 있습니다.
경로 필터링 및 재배포 식별	표준 확장	다양한 라우팅 프로토콜에서 (경로 맵을 통한) IPv4 주소의 경로 필터링 및 재배포에 표준 ACL을, IPv6에는 확장 ACL을 사용합니다.
클라이언트리스 SSL VPN의 필터링	웹 타입	웹 타입 ACL에서 URL 및 목적지를 필터링하도록 구성할 수 있습니다.

ACL 이름

각 ACL에는 이름 또는 숫자로 된 ID(예: outside_in, OUTSIDE_IN, 101)가 있습니다. 이름은 241자 이하여야 합니다. 모두 대문자를 사용하면 실행 중인 컨피그레이션을 볼 때 더 쉽게 이름을 찾을 수 있습니다.

ACL의 목적을 쉽게 이해할 수 있는 명명 규칙을 개발합니다. 예를 들어, ASDM에서는 *interface-name_purpose_direction* 규칙을 사용합니다. 이를테면 인바운드 방향에서 "외부" 인터페이스에 적용되는 ACL의 이름은 "outside_access_in"입니다.

예전에는 ACL ID가 숫자였습니다. 표준 ACL은 1-99 또는 1300-1999 범위였습니다. 확장 ACL은 100-199 또는 2000-2699 범위였습니다. ASA에서는 이러한 범위를 강제적으로 적용하지 않지만, 숫자를 사용하려는 경우 IOS Software를 실행하는 라우터에서 일관성을 유지하기 위해 이러한 규칙을 준수할 수 있습니다.

액세스 제어 입력 순서

ACL은 하나 이상의 ACE로 구성됩니다. 어떤 라인에 명시적으로 ACE를 삽입하지 않는 한, 어떤 ACL 이름에 대해 입력하는 ACE 각각은 ACL의 끝에 추가됩니다.

ACE의 순서는 중요합니다. ASA에서 패킷을 전달할지 폐기할지 결정할 때 ASA는 각 ACE에 대해, 각 항목이 나열된 순서에 따라 패킷을 테스트합니다. 일치하는 항목을 찾으면 더 이상 ACE를 검사하지 않습니다.

따라서 더 일반적인 규칙 다음에 더 구체적인 규칙을 배치할 경우 이 구체적인 규칙이 전혀 적용되지 않을 수 있습니다. 예를 들어, 네트워크 10.1.1.0/24를 허용하되 그 서브넷에서 호스트 10.1.1.15의 트래픽을 폐기하려는 경우 10.1.1.15를 거부하는 ACE가 10.1.1.0/24를 허용하는 ACE의 앞에 와야 합니다. 10.1.1.0/24를 허용하는 ACE가 맨 앞에 올 경우 10.1.1.15가 허용되며, 거부 ACE에 대한 매칭은 이루어지지 않습니다.

확장 ACL에서는 **access-list** 명령의 **line** *number* 매개 변수를 사용하여 알맞은 위치에 규칙을 삽입합니다. 알맞은 사용 순서를 결정하기 위해 ACL 항목과 그 라인 번호를 보려면 **show access-list** *name* 명령을 사용합니다. 다른 ACL 유형에서는 ACE 순서를 변경하려면 ACL을 다시 작성해야 합니다. 더 나은 방법으로는 ASDM을 사용하면 됩니다.

허용/거부와 매칭/매칭하지 않음

액세스 제어 항목은 규칙에 매칭하는 트래픽을 "허용"하거나 "거부"합니다. 트래픽이 ASA에서 허용될지 또는 폐기될지 결정하는 기능(예: 전역 및 인터페이스 액세스 규칙)에 ACL을 적용할 경우 "허용"과 "거부"는 본래의 의미가 있습니다.

서비스 정책 규칙과 같은 다른 기능에서는 "허용"과 "거부"가 사실상 "매칭" 또는 "매칭하지 않음"을 의미합니다. 그러한 경우 ACL은 해당 기능의 서비스(예: 애플리케이션 검사, 서비스 모듈로 리디렉션)을 받을 트래픽을 선택하게 됩니다. "거부된" 트래픽은 ACL에 매칭하지 않아 서비스를 받지 못할 트래픽일 뿐입니다.

액세스 제어 암시적 거부

모든 ACL은 그 끝에 암시적 거부 문이 있습니다. 즉 인터페이스에 적용되는 것과 같은 트래픽 제어 ACL에서는 어떤 트래픽 유형을 명시적으로 허용하지 않으면 해당 트래픽이 폐기됩니다. 예를 들어, 모든 사용자가 하나 이상의 특정 주소를 제외하고 ASA를 통해 네트워크에 액세스하는 것을 허용하려는 경우 그 특정 주소를 거부하고 나머지 모든 주소를 허용해야 합니다.

어떤 서비스에 대한 트래픽을 선택하는 데 쓰이는 ACL에서는 그 트래픽을 명시적으로 "허용"해야 합니다. "허용"되지 않은 모든 트래픽은 해당 서비스에 매칭하지 않습니다. "거부"된 트래픽은 그 서비스를 우회합니다.

이더 타입 ACL에서는 ACL 끝의 암시적 거부가 IP 트래픽 또는 ARP에 영향을 주지 않습니다. 예를 들어, 이더 타입 8037을 허용할 경우 ACL 끝의 암시적 거부는 앞서 확장 ACL로 허용했던 (또는 상위 보안 인터페이스에서 하위 보안 인터페이스에 암시적으로 허용했던) 어떤 IP 트래픽도 차단하지 않습니다. 그러나 어떤 이더 타입 ACE로 모든 트래픽을 *명시적으로* 거부할 경우, IP 및 ARP 트래픽이 거부됩니다. 자동 협상과 같은 물리적 프로토콜 트래픽만 계속 허용됩니다.

NAT 사용 시 확장 ACL에 쓰이는 IP 주소

NAT 또는 PAT를 사용할 때 주소 또는 포트를 변환하는데, 주로 내부 주소와 외부 주소를 매핑합니다. 변환된 주소 또는 포트에 적용되는 확장 ACL을 만들어야 할 경우 실제 (변환되지 않은) 주소나 포트 또는 매핑된 것을 사용할지 결정해야 합니다. 요구 사항은 기능에 따라 달라집니다.

실제 주소와 포트를 사용할 경우 NAT 컨피그레이션이 바뀌더라도 ACL을 변경할 필요 없습니다.

실제 IP 주소를 사용하는 기능

다음 명령과 기능에서는 ACL에 실제 IP 주소를 사용합니다. 인터페이스에 나타나는 주소가 매핑된 주소인 경우에도 그렇습니다.

- 액세스 규칙(**access-group** 명령에서 참조하는 확장 ACL)
- 서비스 정책 규칙(Modular Policy Framework의 **match access-list** 명령)
- 봇넷 트래픽 필터의 트래픽 분류(**dynamic-filter enable classify-list** 명령)
- AAA 규칙(**aaa ... match** 명령)
- WCCP(**wccp redirect-list group-list** 명령)

이를테면 내부 서버 10.1.1.5가 외부에서 공개적으로 라우팅 가능한 IP 주소 209.165.201.5를 갖도록 NAT를 구성할 경우, 외부 트래픽이 내부 서버에 액세스하는 것을 허용하는 액세스 규칙은 서버의 매핑된 주소(209.165.201.5)가 아니라 실제 IP 주소(10.1.1.5)를 참조해야 합니다.

```
ciscoasa(config)# object network server1
ciscoasa(config-network-object)# host 10.1.1.5
ciscoasa(config-network-object)# nat (inside,outside) static 209.165.201.5

ciscoasa(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
ciscoasa(config)# access-group OUTSIDE in interface outside
```

매핑된 IP 주소를 사용하는 기능

다음 기능에서 ACL을 사용하는데, 이 ACL에서는 인터페이스에 나타나는 매핑된 값을 사용합니다.

- IPsec ACL
- **capture** 명령 ACL
- 사용자별 ACL
- 라우팅 프로토콜 ACL
- 다른 모든 기능의 ACL

시간 기준 ACE

특정 기간에만 규칙을 활성화하기 위해 확장 ACE 및 웹 타입 ACE에 시간 범위 객체를 적용할 수 있습니다. 이러한 유형의 규칙을 통해 하루 중 특정 시간에만 허용되고 그 밖의 시간에는 허용되지 않는 활동을 구별할 수 있습니다. 예를 들어, 근무 시간에 추가적인 제한을 적용하되 근무 시간 이후 또는 점심시간에는 해제할 수 있습니다. 그와 반대로 근무 시간이 아닐 때 사실상 네트워크를 종료할 수도 있습니다. 시간 범위 객체 생성에 대한 자세한 내용은 16-9 페이지의 시간 범위 구성을 참조하십시오.

참고 지정된 종료 시간이 지나고 약 80초~100초 정도 사용자가 지연을 경험한 후 ACL이 비활성화될 수도 있습니다. 예를 들어, 지정된 종료 시간이 3:50이라면 이 종료 시간이 범위에 포함되므로 3:51:00~3:51:59의 어느 시점에서 명령이 실행됩니다. 명령이 실행되면 ASA에서는 현재 실행 중인 모든 작업을 종료한 다음 명령에 따라 ACL을 비활성화합니다.

ACL 지침

방화벽 모드 지침

확장 ACL과 표준 ACL은 라우팅 및 투명 방화벽 모드에서 지원됩니다.

웹 타입 ACL은 라우팅 모드에서만 지원됩니다.

이더 타입 ACL은 투명 모드에서만 지원됩니다.

IPv6 지침

확장 ACL과 웹 타입 ACL은 IPv4 주소와 IPv6 주소의 혼합을 허용합니다.

표준 ACL에서는 IPv6 주소를 허용하지 않습니다.

EtherType ACL은 IP 주소를 포함하지 않습니다.

(확장 ACL만) ID 방화벽, FQDN, Cisco TrustSec ACL을 지원하지 않는 기능

다음 기능에서는 ACL을 사용하지만 ID 방화벽(사용자 또는 그룹 이름 지정), FQDN(정규화된 도메인 이름) 또는 Cisco TrustSec 값을 갖는 ACL을 허용할 수 없습니다.

- **route-map** 명령
- VPN **crypto map** 명령
- VPN **group-policy** 명령(**vpn-filter** 제외)
- WCCP
- DAP

추가 지침 및 제한

- 네트워크 마스크를 지정할 때의 방식은 Cisco IOS 소프트웨어 **access-list** 명령과 다릅니다. ASA에서는 네트워크 마스크(예: 클래스 C 마스크는 255.255.255.0)를 사용합니다. Cisco IOS 마스크는 와일드카드 비트(예: 0.0.0.255)를 사용합니다.

ACL 구성

다음 섹션에서는 다양한 ACL 유형의 구성 방법을 설명합니다. ACL 기초에 대한 섹션을 읽고 전체적인 개요를 파악한 다음 구체적인 ACL 유형에 대한 섹션에서 자세한 내용을 확인하십시오.

- 17-6 페이지의 기본 ACL 컨피그레이션 및 관리 옵션
- 17-7 페이지의 확장 ACL 구성
- 17-13 페이지의 표준 ACL 구성
- 17-13 페이지의 웹 타입 ACL 구성
- 17-17 페이지의 이더 타입 ACL 구성

기본 ACL 컨피그레이션 및 관리 옵션

ACL은 동일한 ACL ID 또는 이름을 갖는 하나 이상의 ACE로 구성됩니다. 새 ACL을 만들기 위해서는 새 ACL 이름으로 ACE를 만들면 됩니다. 그러면 새 ACL의 첫 번째 규칙이 됩니다.

ACL을 사용하여 다음 작업을 수행할 수 있습니다.

- **ACL 내용 검사, 라인 번호 및 적중 횟수 확인**—**show access-list** *name* 명령을 사용하여 ACL의 내용을 봅니다. 각 행이 ACE이며 라인 번호를 포함하고 있습니다. 확장 ACL에 새 항목을 삽입하려면 이 번호를 알고 있어야 합니다. 이 정보에는 각 ACE의 적중 횟수도 포함됩니다. 이는 트래픽이 해당 규칙에 매칭한 횟수를 의미합니다. 예:

```
ciscoasa# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group LOCAL\\usergroup
any any (hitcnt=0) 0xb0f5b1e1
```

- **ACE 추가**—ACE를 추가하는 명령은 **access-list** *name* [**line** *line-num*] *type parameters*입니다. 라인 번호 인수는 확장 ACL에만 적용됩니다. 라인 번호를 포함할 경우 ACL의 그 위치에 ACE가 삽입됩니다. 그리고 그 위치에 있던 ACE는 나머지 ACE와 함께 아래로 이동합니다. 즉 라인 번호에 ACE를 삽입하더라도 그 라인의 기존 ACE를 대체하지 않습니다. 라인 번호를 포함하지 않을 경우 ACE는 ACL의 끝에 추가됩니다. 사용 가능한 매개 변수는 ACL 유형에 따라 달라집니다. 자세한 내용은 각 ACL 유형의 항목을 참조하십시오.
- **ACL에 코멘트 추가(웹 타입을 제외한 모든 유형)**—**access-list** *name* [**line** *line-num*] **remark** *text* 명령을 사용하여 ACE의 용도를 이해하는 데 도움이 될 설명을 ACL에 추가합니다. ACE 앞에 설명을 삽입하는 것이 가장 좋습니다. ASDM에서 컨피그레이션을 볼 경우 설명은 그 다음에 오는 ACE와 연결됩니다. ACE 앞에 여러 설명을 입력하여 확장된 코멘트를 넣을 수 있습니다. 각 설명은 100자로 제한됩니다. 설명이 눈에 잘 띄도록 맨 앞에 공백을 넣을 수 있습니다. 라인 번호를 포함하지 않을 경우 설명은 ACL의 끝에 추가됩니다. 예를 들어, 각 ACE를 추가하기 전에 설명을 추가할 수 있습니다.

```
ciscoasa(config)# access-list OUT remark - this is the inside admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.3 any
ciscoasa(config)# access-list OUT remark - this is the hr admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

- **ACE와 설명 수정 또는 이동**—ACE 또는 설명을 수정하거나 이동할 수는 없습니다. (라인 번호를 사용하여) 원하는 값이 정확한 위치에 있는 ACE 또는 설명을 새로 만든 다음 기존 ACE 또는 설명을 삭제해야 합니다. 확장 ACL에서만 ACE 삽입이 가능하므로 ACE를 수정하거나 이동하려면 표준, 웹 타입 또는 이더 타입 ACL을 다시 작성해야 합니다. 긴 ACL을 재구성하려면 ASDM을 사용하는 것이 훨씬 편리합니다.
- **ACE 또는 설명 삭제**—**no access-list** *parameters* 명령을 사용하여 ACE 또는 설명을 제거합니다. **show access-list** 명령을 사용하여 입력할 매개 변수 문자열을 봅니다. 문자열은 삭제할 ACE 또는 설명과 완벽하게 일치해야 합니다. 단, **line** *line-num* 인수는 **no access-list** 명령에서 선택 사항입니다.
- **설명을 포함한 전체 ACL 삭제**—**clear configure access-list** *name* 명령을 사용합니다. 주의 사항! 명령에서 확인 메시지를 표시하지 않습니다. 이름을 포함하지 않으면 ASA의 모든 액세스 목록이 제거됩니다.
- **ACL 이름 변경**—**access-list** *name* **rename** *new_name* 명령을 사용합니다.
- **정책에 ACL 적용**—ACL을 생성하는 것만으로는 트래픽에 어떤 영향도 주지 않습니다. 정책에 ACL을 적용해야 합니다. 예를 들어, **access-group** 명령을 사용하여 인터페이스에 확장 ACL을 적용함으로써 인터페이스를 지나는 트래픽을 거부하거나 허용합니다. 일부 ACL 용도에 대한 자세한 내용은 17-1 페이지의 ACL 유형을 참조하십시오.

확장 ACL 구성

확장 ACL은 동일한 ACL ID 또는 이름을 갖는 모든 ACE로 구성됩니다. 확장 ACL은 가장 복잡하고 다기능적인 ACL 유형이며, 여러 기능에 사용할 수 있습니다. 확장 ACL의 가장 대표적인 용도는 전역 범위에서 또는 인터페이스에 적용되는 액세스 그룹으로 사용되는 것입니다. 이는 트래픽이 시스템을 지나는 것을 거부할지 아니면 허용할지 결정합니다. 그러나 확장 ACL은 다른 서비스가 제공될 트래픽을 결정하는 데에도 사용됩니다.

확장 ACL은 복잡하기 때문에 다음 섹션에서는 특정 유형의 트래픽 매칭을 위한 ACE를 생성하는 것을 중점적으로 설명합니다. 기본 주소 기준 ACE 및 TCP/UDP AC를 다루는 첫 번째 섹션은 나머지 섹션의 기초가 되는 내용입니다.

IP 주소 또는 FQDN 기준 매칭을 위한 확장 ACE 추가

기본 확장 ACE는 IPv4 주소 및 IPv6 주소, FQDN(예: www.example.com) 등 소스 주소와 목적지 주소를 기준으로 트래픽에 매칭합니다. 실제로 모든 유형의 확장 ACE는 소스 및 목적지 주소에 대한 일부 사양을 포함해야 합니다. 따라서 여기서는 최소 확장 ACE에 대해 설명합니다.

팁 FQDN을 기준으로 트래픽에 매칭하려는 경우 FQDN별로 네트워크 객체를 만들어야 합니다.

IP 주소 또는 FQDN 매칭을 위한 ACE를 추가하려면 다음 명령을 사용합니다.

```
access-list access_list_name [line line_number] extended {deny | permit}
protocol_argument source_address_argument dest_address_argument
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

예:

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

옵션은 다음과 같습니다.

- *access_list_name*—신규 또는 기존 ACL의 이름.
- 라인 번호—**line** *line_number* 옵션은 ACE를 삽입할 라인 번호를 지정합니다. 지정하지 않으면 ACE는 ACL의 끝에 추가됩니다.
- 허용 또는 거부—**deny** 키워드는 조건에 매칭할 경우 패킷을 거부하거나 제외합니다. **permit** 키워드는 조건에 매칭할 경우 패킷을 허용하거나 포함합니다.
- 프로토콜—*protocol_argument*는 IP 프로토콜을 지정합니다.
  - *name* 또는 *number*—프로토콜 이름 또는 번호를 지정합니다. 모든 프로토콜에 적용하려면 **ip**라고 지정합니다. 지원되는 키워드의 목록은 43-10 페이지의 프로토콜 및 애플리케이션를 참조하십시오.

  - **object-group** *protocol_grp_id*—**object-group protocol** 명령으로 생성된 프로토콜 객체 그룹을 지정합니다. 를 참조하십시오.16-4 페이지의 서비스 객체 및 서비스 그룹 구성
  - **object** *service_obj_id*—**object service** 명령으로 생성된 서비스 객체를 지정합니다. TCP, UDP 또는 ICMP 서비스 객체는 프로토콜 및 소스 혹은 수신 포트 또는 ICMP 유형 및 코드를 포함할 수 있습니다.
  - **object-group** *service_grp_id*—**object-group service** 명령으로 생성된 서비스 객체 그룹을 지정합니다.
- 소스 주소, 목적지 주소—*source_address_argument*는 패킷을 보내는 IP 주소 또는 FQDN을 지정하고, *dest_address_argument*는 패킷을 받을 IP 주소 또는 FQDN을 지정합니다.
  - **host** *ip_address*—IPv4 호스트 주소를 지정합니다.
  - *ip_address mask*—IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다(예: 10.100.10.0 255.255.255.0).
  - *ipv6-address/prefix-length*—IPv6 호스트 또는 네트워크 주소와 접두사를 지정합니다.
  - **any**, **any4**, **any6**—**any**는 IPv4 트래픽과 IPv6 트래픽을 모두 지정합니다. **any4**는 IPv4 트래픽만, **any6**는 IPv6 트래픽만 지정합니다.
  - **interface** *interface_name*—ASA 인터페이스의 이름을 지정합니다. 어떤 인터페이스가 트래픽의 소스 또는 목적지인가에 따라 트래픽에 매칭하도록 IP 주소보다 인터페이스 이름을 사용합니다.
  - **object** *nw_obj_id*—**object network** 명령으로 생성된 네트워크 객체를 지정합니다. 16-2 페이지의 네트워크 객체 및 그룹 구성을 참조하십시오.
  - **object-group** *nw_grp_id*—**object-group network** 명령으로 생성된 네트워크 객체 그룹을 지정합니다.
- 로깅—**log** 인수는 ACE가 네트워크 액세스를 위해 패킷에 매칭할 때의 로깅 옵션을 설정합니다(**access-group** 명령으로 적용되는 ACL). 인수 없이 **log** 옵션을 입력할 경우 syslog 메시지 106100을 기본 레벨(6)과 기본 간격(300초)으로 활성화합니다. 로그 옵션은 다음과 같습니다.
  - *level*—0부터 7까지의 심각도. 기본값은 6(참조용)입니다. 활성 ACE에 대해 이 레벨을 변경할 경우 새로운 레벨은 신규 연결에 적용됩니다. 기존 연결은 계속 예전의 레벨에서 로깅됩니다.
  - **interval** *secs*—syslog 메시지의 시간 간격(초)이며 1부터 600까지입니다. 기본값은 300입니다. 이 값은 폐기 통계 수집에 쓰이는 캐시에서 비활성 흐름을 삭제하기 위한 시간 초과 값으로도 사용됩니다.
  - **disable**—모든 ACE 로깅을 비활성화합니다.
  - **default**—거부된 패킷에 대해 메시지 106023 로깅을 활성화합니다. 이 설정은 **log** 옵션을 포함하지 않는 것과 같습니다.
- 시간 범위—**time-range** *time_range_name* 옵션은 시간 범위 객체를 지정합니다. 이는 ACE가 활성 상태인 요일과 시간대를 결정합니다. 시간 범위를 지정하지 않을 경우 ACE는 항상 활성 상태입니다.
- 활성화—ACE를 삭제하지 않고 비활성화하려면 **inactive** 옵션을 사용합니다. 다시 활성화하려면 inactive 키워드 없이 전체 ACE를 입력합니다.

포트를 사용하는 TCP 또는 UDP 기준 매칭을 위한 확장 ACE 추가

TCP/UDP 확장 ACE는 기본 주소 매칭 ACE일 뿐이며, 여기서 프로토콜은 **tcp** 또는 **udp**입니다. 이 프로토콜은 포트를 사용하므로 ACE에 포트 사양을 추가할 수 있습니다. 예를 들어, TCP 포트 80의 HTTP 트래픽을 대상으로 할 수 있습니다.

프로토콜이 TCP 또는 UDP일 때 IP 주소 또는 FQDN 매칭을 위해 ACE를 추가하려면 다음 명령을 사용합니다.

```
access-list access_list_name [line line_number] extended {deny | permit}
{tcp | udp} source_address_argument [port_argument] dest_address_argument [port_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

예:

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

port_argument 옵션은 소스 또는 목적지 포트를 지정합니다. 포트를 지정하지 않을 경우 모든 포트가 매칭됩니다. 이용 가능한 인수는 다음과 같습니다.

- *operator port*—*operator*는 다음 중 하나가 될 수 있습니다.
  - **lt**—보다 작음
  - **gt**—보다 큼
  - **eq**—같음
  - **neq**—같지 않음
  - **range**—경계를 포함하는 값 범위. 이 연산자를 사용할 때는 다음과 같이 2개의 포트를 지정합니다.

    ```
    range 100 200
    ```

  *port*는 TCP 또는 UDP 포트의 번호(정수)이거나 이름일 수 있습니다. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, Talk 각각에서 TCP를 위한 정의와 UDP를 위한 정의가 하나씩 필요합니다. TACACS+는 TCP의 포트 49에서 하나의 정의가 필요합니다.
- **object** *service_obj_id*—**object service** 명령으로 생성된 서비스 객체를 지정합니다. 16-4 페이지의 서비스 객체 및 서비스 그룹 구성을 참조하십시오.
- **object-group** *service_grp_id*—**object-group service** 명령으로 생성된 서비스 객체 그룹을 지정합니다.

다른 키워드에 대한 설명은 17-7 페이지의 IP 주소 또는 FQDN 기준 매칭을 위한 확장 ACE 추가를 참조하십시오.

ICMP 기준 매칭을 위한 확장 ACE 추가

ICMP 확장 ACE는 기본 주소 매칭 ACE일 뿐이며, 여기서 프로토콜은 **icmp** 또는 **icmp6**입니다. 이 프로토콜은 유형 및 코드 값이 있으므로 ACE에 유형 및 코드 사양을 추가할 수 있습니다. 예를 들어, ICMP Echo Request 트래픽(ping)을 대상으로 할 수 있습니다.

프로토콜이 ICMP 또는 ICMP6일 때 IP 주소 또는 FQDN 매칭을 위해 ACE를 추가하려면 다음 명령을 사용합니다.

```
access-list access_list_name [line line_number] extended {deny | permit}
{icmp | icmp6} source_address_argument dest_address_argument [icmp_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

예:

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
ciscoasa(config)# access-list abc extended permit icmp any any echo
```

icmp_argument 옵션은 ICMP 유형과 코드를 지정합니다.

- *icmp_type* [*icmp_code*]—ICMP 유형을 이름 또는 번호로 지정하며, 선택 사항으로 그 유형에 대한 ICMP 코드를 지정합니다. 코드를 지정하지 않을 경우 모든 코드가 사용됩니다. ICMP 유형의 목록은 43-14 페이지의 ICMP 유형을 참조하십시오.
- **object-group** *icmp_grp_id*—**object-group service** 또는 (더 이상 사용되지 않지만) **object-group icmp** 명령으로 생성된 ICMP/ICMP6용 객체 그룹을 지정합니다.

다른 키워드에 대한 설명은 17-7 페이지의 IP 주소 또는 FQDN 기준 매칭을 위한 확장 ACE 추가를 참조하십시오.

사용자 기준 매칭을 위한 확장 ACE 추가(ID 방화벽)

사용자 기준 확장 ACE는 기준에 매칭하는 소스에 사용자 이름 또는 사용자 그룹을 추가하는 기본 주소 매칭 ACE일 뿐입니다. 사용자 ID를 기준으로 규칙을 만들면 고정 호스트 또는 네트워크 주소에 규칙을 연결하지 않아도 됩니다. 이를테면 user1을 위한 규칙을 정의한 경우, ID 방화벽 기능에서 그 사용자를 매핑한 호스트가 하루는 10.100.10.3이고 다음 날에는 192.168.1.5라면 사용자 기준 규칙은 계속 적용됩니다.

소스 주소와 목적지 주소는 여전히 제공해야 하므로, (대개 DHCP를 통해) 사용자에게 할당될 가능성이 있는 주소를 포함하도록 소스 주소를 확장합니다. 예를 들어, 사용자 "LOCAL\user1 any"는 어떤 주소가 할당되더라도 LOCAL\user1 사용자에 매칭합니다. 그러나 "LOCAL\user1 10.100.1.0 255.255.255.0"은 주소가 10.100.1.0/24 네트워크에 있을 경우에만 그 사용자에게 매칭합니다.

그룹 이름을 사용하여 전체 사용자 클래스(예: 학생, 교사, 관리자, 엔지니어 등)를 기준으로 규칙을 정의할 수 있습니다.

사용자 또는 그룹 매칭을 위한 ACE를 추가하려면 다음 명령을 사용합니다.

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[user_argument] source_address_argument [port_argument]
dest_address_argument [port_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

예:

```
ciscoasa(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

user_argument 옵션은 소스 주소 외에도 트래픽에 매칭할 사용자 또는 그룹을 지정합니다. 사용 가능한 인수는 다음과 같습니다.

- **object-group-user** *user_obj_grp_id*—**object-group user** 명령으로 생성된 사용자 객체 그룹을 지정합니다.
- **user** {[*domain_nickname*\]*name* | **any** | **none**}—사용자 이름을 지정합니다. 사용자 자격 증명이 있는 모든 사용자에 매칭하려면 **any**를, 사용자 이름에 매핑되지 않은 주소에 매칭하려면 **none**을 지정합니다. 이 옵션은 **access-group** 정책과 **aaa authentication match** 정책을 연계할 때 특히 유용합니다.
- **user-group** [*domain_nickname*\\]*user_group_name*—사용자 그룹 이름을 지정합니다. 이중 \\는 도메인과 그룹 이름을 구분합니다.

다른 키워드에 대한 설명은 17-7 페이지의 IP 주소 또는 FQDN 기준 매칭을 위한 확장 ACE 추가를 참조하십시오.

팁 사용자 및 Cisco Trustsec 보안 그룹 모두를 하나의 ACE에 포함할 수 있습니다. 17-11 페이지의 보안 그룹(Cisco TrustSec) 기준 매칭을 위한 확장 ACE 추가를 참조하십시오.

보안 그룹(Cisco TrustSec) 기준 매칭을 위한 확장 ACE 추가

보안 그룹(Cisco TrustSec) 확장 ACE는 기준에 매칭하는 소스 또는 목적지에 보안 그룹 또는 태그를 포함하는 기본 주소 매칭 ACE일 뿐입니다. 보안 그룹 기준 규칙을 만들면 고정 호스트 또는 네트워크 주소에 규칙을 연결하지 않아도 됩니다. 소스 주소와 목적지 주소는 여전히 제공해야 하므로, (대개 DHCP를 통해) 사용자에게 할당될 가능성이 있는 주소를 포함하도록 주소를 확장합니다.

팁 이 유형의 ACE를 추가하기 전에 32 장, "ASA 및 Cisco TrustSec"의 설명에 따라 Cisco TrustSec를 구성합니다.

보안 그룹 매칭을 위한 ACE를 추가하려면 다음 명령을 사용합니다.

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[security_group_argument] source_address_argument [port_argument]
[security_group_argument] dest_address_argument [port_argument] [log [[level]
[interval secs] | disable | default]] [inactive | time-range time_range_name]
```

예:

```
ciscoasa(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security_group_argument 옵션은 소스 주소 또는 목적지 주소 외에도 트래픽에 매칭할 보안 그룹을 지정합니다. 사용 가능한 인수는 다음과 같습니다.

- **object-group-security** *security_obj_grp_id*—**object-group security** 명령으로 생성되는 보안 객체 그룹을 지정합니다.
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*}—보안 그룹 이름 또는 태그를 지정합니다.

다른 키워드에 대한 설명은 17-7 페이지의 IP 주소 또는 FQDN 기준 매칭을 위한 확장 ACE 추가를 참조하십시오.

팁 사용자 및 Cisco Trustsec 보안 그룹 모두를 하나의 ACE에 포함할 수 있습니다. 17-10 페이지의 사용자 기준 매칭을 위한 확장 ACE 추가(ID 방화벽)를 참조하십시오.

확장 ACL의 예

다음 ACL은 (ACL을 적용하는 인터페이스의) 모든 호스트가 ASA를 지나는 것을 허용합니다.

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

다음 ACL은 TCP 기반 트래픽에서 192.168.1.0/24의 호스트가 209.165.201.0/27 네트워크에 액세스할 수 없게 합니다. 다른 모든 주소는 허용됩니다.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

선택된 호스트만 액세스할 수 있도록 제한하려면 제한 허용 ACE를 입력합니다. 기본적으로 다른 모든 트래픽은 명시적으로 허용되지 않는 한 거부됩니다.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

다음 ACL은 (ACL을 적용하는 인터페이스의) 모든 호스트가 주소 209.165.201.29의 웹 사이트에 액세스할 수 없게 합니다. 다른 모든 트래픽은 허용됩니다.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

객체 그룹을 사용하는 다음 ACL은 내부 네트워크의 일부 호스트가 일부 웹 서버에 액세스할 수 없게 합니다. 다른 모든 트래픽은 허용됩니다.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

다음 예에서는 한 네트워크 객체 그룹(A)에서 다른 네트워크 객체 그룹(B)으로 가는 트래픽을 허용하는 ACL을 일시적으로 비활성화합니다.

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

시간 기준 ACE를 구현하려면 **time-range** 명령을 사용하여 구체적인 요일과 시간대를 정의합니다. 그런 다음 **access-list extended** 명령을 사용하여 시간 범위를 ACE에 바인딩합니다. 다음 예에서는 "Sales" ACL의 ACE를 "New_York_Minute"라는 이름의 시간 범위에 바인딩합니다.

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

다음 예는 IPv4/IPv6 혼합 ACL을 보여줍니다.

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

확장 ACL을 위해 주소를 개체로 변환하는 작업의 예

객체 그룹을 사용하지 않는 다음 일반 ACL은 내부 네트워크의 일부 호스트가 일부 웹 서버에 액세스할 수 없게 합니다. 다른 모든 트래픽은 허용됩니다.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
```

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

내부 호스트용과 웹 서버용으로 하나씩 2개의 네트워크 객체 그룹을 만들 경우 컨피그레이션을 간소화하고 손쉽게 수정하여 호스트를 추가할 수 있습니다.

```
ciscoasa(config)# object-group network denied
ciscoasa(config-network)# network-object host 10.1.1.4
ciscoasa(config-network)# network-object host 10.1.1.78
ciscoasa(config-network)# network-object host 10.1.1.89

ciscoasa(config-network)# object-group network web
ciscoasa(config-network)# network-object host 209.165.201.29
ciscoasa(config-network)# network-object host 209.165.201.16
ciscoasa(config-network)# network-object host 209.165.201.78

ciscoasa(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

표준 ACL 구성

표준 ACL은 동일한 ACL ID 또는 이름을 갖는 모든 ACE로 구성됩니다. 표준 ACL은 경로 맵, VPN 필터 등 몇몇 기능에 사용됩니다. 표준 ACL에서는 IPv4 주소만 사용하며, 목적지 주소만 정의합니다.

표준 액세스 목록 항목을 추가하려면 다음 명령을 사용합니다.

```
ciscoasa(config)# access-list access_list_name standard {deny | permit}
{any4 | host ip_address | ip_address mask}
```

예:

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

옵션은 다음과 같습니다.

- 이름—*access_list_name* 인수는 ACL 번호의 이름을 지정합니다. 일반적인 표준 ACL 번호는 1-99 또는 1300-1999이지만, 어떤 이름이나 번호도 사용할 수 있습니다. ACL이 없다면 새 ACL을 만듭니다. 그러지 않으면 ACL의 끝에 항목을 추가하게 됩니다.
- 허용 또는 거부—**deny** 키워드는 조건에 매칭할 경우 패킷을 거부하거나 제외합니다. **permit** 키워드는 조건에 매칭할 경우 패킷을 허용하거나 포함합니다.
- 목적지 주소—**any4** 키워드는 모든 IPv4 주소에 매칭합니다. **host** *ip_address* 인수는 어떤 호스트 IPv4 주소에 매칭합니다. *ip_address ip_mask* 인수는 IPv4 서브넷(예: 10.1.1.0 255.255.255.0)에 매칭합니다.

웹 타입 ACL 구성

웹 타입 ACL은 클라이언트리스 SSL VPN 트래픽의 필터링에 사용되어 특정 네트워크, 서브넷, 호스트, 웹 서버에 대한 사용자 액세스를 제한합니다. 필터를 정의하지 않을 경우 모든 연결이 허용됩니다. 웹 타입 ACL은 동일한 ACL ID 또는 이름을 갖는 모든 ACE로 구성됩니다.

웹 타입 ACL을 사용하여 URL 또는 목적지 주소를 기준으로 트래픽에 매칭할 수 있습니다. 단일 ACE에서 이 사양을 혼합할 수 없습니다. 다음 섹션에서는 각 ACE 유형에 대해 설명합니다.

- 17-14 페이지의 URL 매칭을 위한 웹 타입 ACE 추가
- 17-15 페이지의 IP 주소 매칭을 위한 웹 타입 ACE 추가
- 17-16 페이지의 웹 타입 ACL의 예

URL 매칭을 위한 웹 타입 ACE 추가

사용자가 액세스하려는 URL을 기준으로 트래픽에 매칭하려면 다음 명령을 사용합니다.

```
access-list access_list_name webtype {deny | permit} url {url_string | any}
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]]
[inactive]
```

예:

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

옵션은 다음과 같습니다.

- *access_list_name*—신규 또는 기존 ACL의 이름. ACL이 이미 있을 경우 ACL의 끝에 ACE를 추가하게 됩니다.
- 허용 또는 거부—**deny** 키워드는 조건에 매칭할 경우 패킷을 거부하거나 제외합니다. **permit** 키워드는 조건에 매칭할 경우 패킷을 허용하거나 포함합니다.
- URL—**url** 키워드는 매칭할 URL을 지정합니다. 모든 URL 기준 트래픽에 매칭하려면 **url any**를 사용합니다. 그러지 않으면 URL 문자열을 입력하며, 와일드카드를 넣을 수 있습니다. 다음은 URL 지정에 관한 팁과 제한 사항입니다.
  - 모든 URL에 매칭하려면 **any**를 지정합니다.
  - 'Permit url any'은 protocol://server-ip/path 형식의 모든 URL을 허용하며, port-forwarding과 같이 이 패턴과 일치하지 않은 트래픽은 차단합니다. 암시적 거부가 일어나지 않도록 필요한 포트(Citrix의 경우 포트 1494)와의 연결을 허용하는 ACE가 있어야 합니다.
  - 스마트 터널과 ica plug-in인 'permit url any' ACL의 영향을 받지 않습니다. mart-tunnel:// and ica:// 유형에만 매칭하기 때문입니다.
  - cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp:// 프로토콜을 사용할 수 있습니다. 또한 프로토콜에 와일드카드를 사용할 수 있습니다. 예를 들어, htt*는 http 및 https에, 별표 *는 모든 프로토콜에 매칭됩니다. 예를 들어, *://*.example.com은 example.com 네트워크로 가는 모든 유형의 URL 기준 트래픽에 매칭합니다.
  - smart-tunnel:// URL을 지정할 경우 서버 이름만 포함할 수 있습니다. URL은 경로를 포함할 수 없습니다. 예를 들어, smart-tunnel://www.example.com은 허용되지만, smart-tunnel://www.example.com/index.html은 허용되지 않습니다.
  - 별표 *는 무엇과도 매칭하지 않거나 임의의 문자 수에 매칭합니다. 모든 http URL에 매칭하려면 http://*/*를 입력합니다.
  - 물음표 ?는 임의의 한 문자에만 매칭합니다.
  - 대괄호 []는 범위 연산자로서 해당 범위에 속한 모든 문자에 매칭합니다. 예를 들어, http://www.cisco.com:80/와 http://www.cisco.com:81/ 모두에 매칭하려면 **http://www.cisco.com:8[01]/**를 입력합니다.
- 로깅—**log** 인수는 ACE가 어떤 패킷에 매칭할 때의 로깅 옵션을 설정합니다. 인수 없이 **log** 옵션을 입력할 경우 syslog 메시지 106102를 기본 레벨(6)과 기본 간격(300초)으로 활성화합니다. 로그 옵션은 다음과 같습니다.
  - *level*—0부터 7까지의 심각도. 기본값은 6입니다.
  - **interval** *secs*—syslog 메시지의 시간 간격(초)이며 1부터 600까지입니다. 기본값은 300입니다.
  - **disable**—모든 ACL 로깅을 비활성화합니다.
  - **default**—메시지 106103 로깅을 활성화합니다. 이 설정은 **log** 옵션을 포함하지 않는 것과 같습니다.

- 시간 범위—**time-range** *time_range_name* 옵션은 시간 범위 객체를 지정합니다. 이는 ACE가 활성 상태인 요일과 시간대를 결정합니다. 시간 범위를 지정하지 않을 경우 ACE는 항상 활성 상태입니다.
- 활성화—ACE를 삭제하지 않고 비활성화하려면 **inactive** 옵션을 사용합니다. 다시 활성화하려면 inactive 키워드 없이 전체 ACE를 입력합니다.

IP 주소 매칭을 위한 웹 타입 ACE 추가

사용자가 액세스하려는 목적지 주소를 기준으로 트래픽에 매칭할 수 있습니다. 웹 타입 ACL은 URL 사양 외에도 IPv4 주소와 IPv6 주소의 혼합을 포함할 수 있습니다.

IP 주소 매칭을 위해 웹 타입 ACE를 추가하려면 다음 명령을 사용합니다.

```
access-list access_list_name webtype {deny | permit}
tcp dest_address_argument [operator port]
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]]
[inactive]]
```

예:

```
ciscoasa(config)# access-list acl_company webtype permit tcp any
```

여기에서 설명하지 않은 키워드에 대해서는 17-14 페이지의 URL 매칭을 위한 웹 타입 ACE 추가를 참조하십시오. 이 ACE 유형에서 특별히 사용하는 키워드와 인수는 다음과 같습니다.

- **tcp**—TCP 프로토콜. 웹 타입 ACL은 TCP 트래픽에만 매칭합니다.
- 목적지 주소—*dest_address_argument*는 패킷을 받을 IP 주소를 지정합니다.
  - **host** *ip_address*—IPv4 호스트 주소를 지정합니다.
  - *dest_ip_address mask*—IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다(예: 10.100.10.0 255.255.255.0).
  - *ipv6-address/prefix-length*—IPv6 호스트 또는 네트워크 주소와 접두사를 지정합니다.
  - **any**, **any4**, **any6**—**any**는 IPv4 트래픽과 IPv6 트래픽을 모두 지정합니다. **any4**는 IPv4 트래픽만, **any6**는 IPv6 트래픽만 지정합니다.
- *operator port*—목적지 포트. 포트를 지정하지 않을 경우 모든 포트가 매칭됩니다. *operator*는 다음 중 하나가 될 수 있습니다.
  - **lt**—보다 작음
  - **gt**—보다 큼
  - **eq**—같음
  - **neq**—같지 않음
  - **range**—경계를 포함하는 값 범위. 이 연산자를 사용할 때는 다음과 같이 2개의 포트를 지정합니다.

    ```
    range 100 200
    ```

  *port*는 TCP 포트의 번호(정수)이거나 이름일 수 있습니다.

웹 타입 ACL의 예

다음 예는 특정 회사 URL에 대한 액세스를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

다음 예는 특정 웹 페이지에 대한 액세스를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

다음 예는 포트 8080을 지나는, 특정 서버에 있는 임의의 URL에 대한 HTTP 액세스를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

다음 예는 웹 타입 ACL에 와일드카드를 사용하는 방법을 보여줍니다.

- 다음 예에서는 http://www.example.com/layouts/1033과 같은 URL에 매칭합니다.

  ```
  access-list VPN-Group webtype permit url http://www.example.com/*
  ```

- 다음 예에서는 http://www.example.com/, http://www.example.net/와 같은 URL에 매칭합니다.

  access-list test webtype permit url http://www.example.*

- 다음 예에서는 http://www.example.com, ftp://wwz.example.com과 같은 URL에 매칭합니다.

  ```
  access-list test webtype permit url *://ww?.e*co*/
  ```

- 다음 예에서는 http://www.cisco.com:80, https://www.cisco.com:81과 같은 URL에 매칭합니다.

  ```
  access-list test webtype permit url *://ww?.c*co*:8[01]/
  ```

  앞의 예에서 범위 연산자 "[]"는 해당 위치에서 문자 **0** 또는 **1**이 올 수 있음을 나타냅니다.

- 다음 예에서는 http://www.example.com, http://www.example.net과 같은 URL에 매칭합니다.

  ```
  access-list test webtype permit url http://www.[a-z]xample?*/
  ```

  앞의 예에서 범위 연산자 "[]"는 **a**부터 **z**까지의 임의의 문자가 올 수 있음을 나타냅니다.

- 다음 예에서는 파일 이름 또는 경로에 "cgi"가 포함된 http 또는 https URL에 매칭합니다.

  ```
  access-list test webtype permit url htt*://*/*cgi?*
  ```

참고 임의의 http URL에 매칭하려면 http://* 대신 **http://*/***를 입력해야 합니다.

다음 예는 특정 CIFS 공유에 대한 액세스를 비활성화하는 웹 타입 ACL을 강제적으로 적용하는 방법을 보여줍니다.

이 시나리오에서는 "shares"라는 루트 폴더에 "Marketing_Reports"와 "Sales_Reports"라는 2개의 하위 폴더가 있습니다. 여기서는 구체적으로 "shares/Marketing_Reports" 폴더에 대한 액세스를 거부하려 합니다.

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

그러나 ACL의 끝에 있는 암시적 "deny all" 때문에 위 ACL은 루트 폴더("shares")를 비롯하여 모든 하위 폴더("shares/Sales_Reports", "shares/Marketing_Reports")에 액세스할 수 없게 합니다.

이 문제를 해결하려면 루트 폴더와 나머지 하위 폴더에 대한 액세스를 허용하는 새 ACL을 추가합니다.

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

이더 타입 **ACL** 구성

이더 타입 ACL은 투명 방화벽 모드에서 비 IP 레이어 2 트래픽에 적용됩니다. 레이어 2 트래픽의 이더 타입 값에 따라 트래픽을 허용하거나 거부하는 데 이 규칙을 사용할 수 있습니다. 이더 타입 ACL을 사용하면 ASA를 지나는 비 IP 트래픽의 흐름을 제어할 수 있습니다. 802.3 형식의 프레임은 ACL에서 다루지 않습니다. 유형 필드가 아닌 길이 필드를 사용하기 때문입니다.

이더 타입 ACE를 추가하려면 다음 명령을 사용합니다.

access-list *access_list_name* **ethertype** {**deny** | **permit**}
{**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **isis** | **any** | *hex_number*}

예:

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
```

옵션은 다음과 같습니다.

- *access_list_name*—신규 또는 기존 ACL의 이름. ACL이 이미 있을 경우 ACL의 끝에 ACE를 추가하게 됩니다.
- 허용 또는 거부—**deny** 키워드는 조건에 매칭할 경우 패킷을 거부합니다. **permit** 키워드는 조건에 매칭할 경우 패킷을 허용합니다.
- 트래픽 매칭 기준—다음 옵션을 사용하여 트래픽에 매칭할 수 있습니다.
  - **ipx**—IPX(Internet Packet Exchange)
  - **bpdu**—브리지 프로토콜 데이터 단위이며, 기본적으로 허용됩니다.
  - **mpls-multicast**— MPLS 멀티캐스트
  - **mpls-unicast**—MPLS 유니캐스트
  - **isis**—IS-IS(Intermediate System to Intermediate System)
  - **any**—모든 트래픽에 매칭합니다.
  - *hex_number*—16비트 16진수0x600~0xffff로 식별될 수 있는 모든 이더 타입. 이더 타입의 목록은 RFC 1700, "Assigned Numbers"(http://www.ietf.org/rfc/rfc1700.txt)를 참조하십시오.

이더 타입 **ACL**의 예

다음 예는 이더 타입 ACL을 구성하는 방법을 보여주며, 인터페이스에 적용하는 방법도 소개합니다.

다음 샘플 ACL은 내부 인터페이스에서 시작한 일반 트래픽을 허용합니다.

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

다음 ACL은 ASA를 지나는 일부 이더 타입을 허용하지만 IPX는 거부합니다.

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
ciscoasa(config)# access-list ETHER ethertype permit 1234
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

다음 ACL은 이더 타입 0x1256의 트래픽을 거부하지만 두 인터페이스에서 다른 모든 트래픽은 허용합니다.

```
ciscoasa(config)# access-list nonIP ethertype deny 1256
ciscoasa(config)# access-list nonIP ethertype permit any
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

ACL 모니터링

ACL을 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
show access-list [*name*]	ACE의 라인 번호와 적중 횟수를 포함하여 액세스 목록을 표시합니다. ACL 이름을 포함합니다. 그러지 않으면 모든 액세스 목록이 표시됩니다.
show running-config access-list [*name*]	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다. ACL 이름을 포함합니다. 그러지 않으면 모든 액세스 목록이 표시됩니다.

ACL 관련 이력

기능 이름	릴리스	설명
확장, 표준, 웹 타입 ACL	7.0(1)	네트워크 액세스를 제어하거나 여러 기능이 실행될 트래픽을 지정하는 데 ACL을 사용합니다. 확장 ACL은 through-the-box 액세스 제어 및 그 밖의 몇몇 기능에 사용합니다. 표준 ACL은 경로 맵 및 VPN 필터에 사용합니다. 웹 타입 ACL은 클라이언트리스 SSL VPN 필터링에 사용합니다. 이더 타입 ACL은 비 IP 레이어 2 트래픽을 제어합니다. 도입된 화면: **access-list extended, access-list standard, access-list webtype**, **access-list ethertype**
확장 ACL의 실제 IP 주소	8.3(1)	NAT 또는 PAT를 사용할 경우, 일부 기능의 ACL에서 매핑된 주소 및 포트를 더 이상 사용하지 않습니다. 이러한 기능에는 변환되지 않은 실제 주소와 포트를 사용해야 합니다. 실제 주소와 포트를 사용할 경우 NAT 컨피그레이션이 바뀌더라도 ACL을 변경할 필요 없습니다. 자세한 내용은 17-4 페이지의 NAT 사용 시 확장 ACL에 쓰이는 IP 주소를 참조하십시오.
확장 ACL에서의 ID 방화벽 지원	8.4(2)	이제 소스 및 목적지에 대해 ID 방화벽 사용자와 그룹을 사용할 수 있습니다. 액세스 규칙, AAA 규칙에 또한 VPN 인증을 위해 ID 방화벽 ACL을 사용할 수 있습니다. 수정된 명령: **access-list extended**
이더 타입 ACL의 IS-IS 트래픽 지원	8.4(5), 9.1(2)	투명 방화벽 모드에서 ASA는 이더 타입 ACL을 사용하여 IS-IS 트래픽을 제어할 수 있습니다. 수정된 명령: **access-list ethertype** {**permit** | **deny**} **isis**

기능 이름	릴리스	설명
확장 ACL에서의 Cisco TrustSec 지원	9.0(1)	소스 및 목적지에 대해 Cisco TrustSec 보안 그룹을 사용할 수 있습니다. 액세스 규칙과 함께 ID 방화벽 ACL을 사용할 수 있습니다. 수정된 명령: **access-list extended**
IPv4와 IPv6를 위해 통일된 확장 ACL 및 웹 타입 ACL	9.0(1)	확장 ACL 및 웹 타입 ACL에서 IPv4 주소와 IPv6 주소를 지원합니다. 소스 및 목적지에 IPv4 주소와 IPv6 주소를 혼합하여 지정할 수도 있습니다. **any** 키워드는 IPv4 트래픽과 IPv6 트래픽을 나타내도록 변경되었습니다. **any4** 키워드와 **any6** 키워드가 각각 IPv4 트래픽만, IPv6 트래픽만 나타내도록 추가되었습니다. IPv6 전용 ACL은 더 이상 사용하지 않습니다. 기존 IPv6 ACL은 확장 ACL로 마이그레이션되었습니다. 마이그레이션에 대한 자세한 내용은 릴리스 정보를 참조하십시오. 수정된 명령: **access-list extended**, **access-list webtype** 제거된 명령: **ipv6 access-list**, **ipv6 access-list webtype**, **ipv6-vpn-filter**.
확장 ACL 및 ICMP 코드를 기준으로 ICMP 트래픽을 필터링하기 위한 객체 개선 사항	9.0(1)	이제 ICMP 코드에 따라 ICMP 트래픽을 허용하거나 거부할 수 있습니다. 도입되거나 수정된 명령: **access-list extended**, **service-object**, **service**

6 파 트

IP 라우팅

18 장

라우팅 개요

이 장에서는 Cisco ASA 내에서 라우팅의 동작 원리와 지원되는 프로토콜에 관한 기본 개념을 설명합니다.

라우팅 정보

라우팅은 소스에서 대상까지 인터네트워크에 걸친 정보의 이동입니다. 그 과정에서 적어도 하나의 중간 노드를 만나게 됩니다. 라우팅에는 2가지 기본적인 작업이 포함됩니다. 최적의 라우팅 경로를 결정하는 것과 인터네트워크를 통한 정보 그룹(패킷이라고 함)을 전송하는 것입니다. 라우팅 프로세스에서는 후자를 패킷 스위칭이라고 합니다. 패킷 스위칭은 비교적 간단하지만 경로 결정은 매우 복잡할 수 있습니다.

스위칭

스위칭 알고리즘은 상대적으로 단순하며 대부분의 라우팅 프로토콜에 대해 동일합니다. 대부분의 경우 호스트가 패킷을 다른 호스트로 보내야 한다고 결정합니다. 라우터 주소를 확보한 소스 호스트는 패킷 주소를 라우터의 물리적 (Media Access Control [MAC]-layer) 주소로 보내는 데 이번에는 대상 호스트의 프로토콜(네트워크 레이어) 주소를 함께 보냅니다.

라우터는 패킷 대상 프로토콜 주소를 검사하면서 패킷을 다음 홉으로 전달하는 방법을 알고 있는지 모르고 있는지 결정합니다. 라우터가 패킷 전달 방법을 모르는 경우 일반적으로 패킷을 버리게 됩니다. 하지만 라우터가 패킷 전달 방법을 안다면 대상 물리적 주소를 다음 홉의 주소로 바꾸고 패킷을 전송합니다.

다음 홉 주소는 궁극적인 대상 호스트가 될 수 있습니다. 아니라면 다음 홉은 보통 동일한 스위칭 결정 프로세스를 실행하는 다른 라우터입니다. 패킷이 인터네트워크를 통과하면서 물리적 주소가 변경되지만 프로토콜 주소는 유지됩니다.

경로 결정

라우팅 프로토콜은 메트릭을 사용하여 패킷이 이동할 최적의 경로를 평가합니다. 메트릭은 경로 대역폭과 같이 측정 기준으로서 대상으로의 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. 대상 또는 차기 홉 연결은 패킷을 특정 라우터로 보내 차기 홉이 최종 대상을 향해 가고 있음을 알림으로써 특정 대상에 최적으로 도달할 수 있음을 라우터에 알려줍니다. 라우터가 수신 패킷을 수신하면 대상 주소를 확인하고 이 주소를 차기 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 대상으로의 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.

- 18-2 페이지의 고정 대 동적
- 18-3 페이지의 단일 경로 대 다중 경로
- 18-3 페이지의 평면 대 계층
- 18-3 페이지의 연결 상태 대 거리 벡터

고정 대 동적

고정 라우팅 알고리즘은 알고리즘이라고 하기 어렵고 네트워크 관리자가 라우팅 전에 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 라우터)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 대상에 대한 다중 경로를 지원합니다. 단일 경로 알고리즘과 달리 이러한 다중 경로 알고리즘은 여러 회선에 걸친 트래픽 멀티플렉싱을 허용합니다. 다중 경로 알고리즘의 이점은 보통 부하 공유라고 부르는 훨씬 뛰어난 처리량과 신뢰성입니다.

평면 대 계층

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. nonbackbone 라우터의 패킷은 백본 라우터로 이동하고 여기서 백본을 통해 대상 영역에 도달할 때까지 전송됩니다. 이 시점에서는 마지막 백본 라우터에서 하나 이상의 백본 라우터를 통해 최종 대상으로 이동합니다.

라우팅 시스템은 종종 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 주된 이점은 그것이 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 알 필요가 있으므로 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)이 각 라우터를 호출하여 라우팅 테이블의 전체 또는 일부를 인접 라우터에 한해 전송하도록 합니다. 기본적으로 링크 상태 알고리즘은 모든 곳으로 소규모 업데이트를 전송하는 반면 거리 벡터 알고리즘은 대규모 업데이트를 인접 라우터로만 보냅니다. 거리 벡터 알고리즘은 인접 디바이스에 대해서만 알고 있습니다. 일반적으로 링크 상태 알고리즘은 OSPF 라우팅 프로토콜과 함께 사용됩니다.

ASA 내에서 라우팅의 작동 방식

ASA은(는) 라우팅 결정을 위해 라우팅 테이블과 XLATE 테이블을 모두 사용합니다. 대상 IP 변환 트래픽, 즉 미변환 트래픽을 처리하기 위해 ASA는 기존 XLATE 또는 고정 변환을 검색하여 이그레스 인터페이스를 선택합니다.

- 18-3 페이지의 이그레스 인터페이스 선택 프로세스
- 18-4 페이지의 차기 홉 선택 프로세스

이그레스 인터페이스 선택 프로세스

선택 프로세스는 다음 단계를 따릅니다.

1. XLATE를 변환하는 대상 IP가 이미 존재하는 경우 패킷에 대한 이그레스 인터페이스는 라우팅 테이블이 아니라 XLATE 테이블에서 결정됩니다.

2. XLATE를 변환하는 대상 IP가 존재하지 않지만 일치하는 고정 변환이 존재하는 경우 이그레스 인터페이스는 고정 NAT 규칙으로부터 결정되고 XLATE이 생성되며 라우팅 테이블은 사용되지 않습니다.
3. XLATE를 변환하는 대상 IP가 존재하지 않고 일치하는 고정 변환도 없는 경우 패킷은 대상 IP 변환이 되지 않습니다. ASA가 이그레이 인터페이스 선택 경로를 조회함으로써 이 패킷을 처리한 후 소스 IP 변환이 수행됩니다(필요한 경우).

   일반 동적 아웃바운드 NAT의 경우 초기 발신 패킷이 경로 테이블을 사용한 다음 XLATE를 생성함으로써 라우팅됩니다. 수신 반환 패킷은 기존 XLATE만 사용하여 전달됩니다. 고정 NAT의 경우 대상 변환된 수신 패킷은 항상 기존 XLATE 또는 고정 변환 규칙을 사용하여 전달됩니다.

차기 홉 선택 프로세스

이전에 설명한 방법을 사용하여 이그레스 인터페이스를 선택한 후 이전에 선택한 이그레스 인터페이스에 속하는 적당한 차기 홉을 찾기 위한 추가 경로 조회가 실시됩니다. 선택한 인터페이스에 속하는 라우팅 테이블에 경로가 없는 경우 다른 이그레스 인터페이스에 속하는 대상 네트워크로의 다른 경로가 있는 경우에도 패킷이 버려지고 레벨 6 syslog 메시지 110001(호스트 경로 없음)이 생성됩니다. 선택한 이그레스 인터페이스에 속하는 경로가 발견되면 패킷이 대응 차기 홉으로 전달됩니다.

단일 이그레스 인터페이스를 사용하여 여러 차기 홉을 사용할 수 있는 경우에만 ASA의 부하 공유가 가능합니다. 부하 공유로 여러 이그레스 인터페이스를 공유할 수 없습니다.

ASA에서 동적 라우팅이 사용 중이고 XLATE 생성 후 경로 테이블이 변경되는 경우(예: 경로 플랩) 경로 테이블을 통하지 않고 기존 XLATE를 사용하여 XLATE 시간 초과까지 대상 변환 트래픽이 전달됩니다. 이전 경로가 이전 인터페이스에서 삭제되고 라우팅 프로세스에 의해 다른 인터페이스에 연결될 경우 잘못된 인터페이스로 전달되거나 레벨 6 syslog 메시지 110001(호스트 경로 없음)와 함께 버려질 수 있습니다.

ASA 자체에서 경로 플랩이 없지만 주변에서 라우팅 프로세스 플래핑이 일어나고 동일 흐름에 속하는 소스 변환 패킷이 다른 인터페이스를 사용하는 ASA를 통해 전송되는 경우에도 같은 문제가 발생할 수 있습니다. 대상 변환 반환 패킷이 잘못된 이그레스 인터페이스를 사용하여 전달될 수 있습니다.

이 문제는 흐름에서 초기 패킷의 방향에 따라 사실상 모든 트래픽이 소스 변환이거나 대상 변환인 일부 보안 트래픽 컨피그레이션에서 가능성이 높습니다. 이 문제가 경로 플랩 후에 발생하는 경우 **clear xlate** 명령을 사용하여 수동으로 해결하거나 XLATE 시간 초과로 자동으로 해결될 수 있습니다. 필요하면 XLATE 시간 초과를 줄일 수 있습니다. 이 문제가 잘 발생하지 않도록 하려면 ASA와 그 주변에서 경로 플랩이 없도록 하십시오. 다시 말해 같은 흐름에 속하는 대상 변환 패킷이 항상 ASA를 통해 똑같이 전달되도록 하십시오.

라우팅을 위한 지원되는 인터넷 프로토콜

ASA는 라우팅을 위해 몇 가지 인터넷 프로토콜을 지원합니다. 각 프로토콜은 이 섹션에 간단히 설명되어 있습니다.

- EIGRP(Enhanced Interior Gateway Routing Protocol)

  EIGRP는 IGRP 라우터와의 호환성과 원활한 상호 작용을 제공하는 Cisco 고유의 프로토콜입니다. 자동 재배포 메커니즘은 IGRP 경로를 Enhanced IGRP로 가져올 수 있게 하고 그 반대도 지원합니다. 따라서 기존 IGRP 네트워크로 Enhanced IGRP를 단계적으로 추가할 수 있습니다.

  EIGRP 구성에 관한 자세한 정보는 23-3 페이지의 EIGRP 구성에서 참조하십시오.

- OSPF(Open Shortest Path First)

  OSPF는 IETF(Internet Engineering Task Force)의 내부 게이트웨이 프로토콜(IGP) 작업 그룹이 인터넷 프로토콜 (IP) 네트워크를 위해 개발한 라우팅 프로토콜입니다. OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터는 라우터가 사용 가능한 인터페이스와 접근할 수 있는 인접 디바이스의 목록인 동일한 링크 상태 데이터베이스를 포함합니다.

  OSPF 구성에 관한 자세한 정보는 22-6 페이지의 OSPFv2 구성에서 참조하십시오.

- 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.

  RIP 구성에 관한 자세한 정보는 기존 기능 가이드에서 참조하십시오.

- 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. 자율 시스템(AS) 사이에서 BGP가 사용될 때 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때 프로토콜은 IBGP(Interior BGP)라고 합니다.

  BGP 구성에 관한 자세한 정보는 21-3 페이지의 BGP 구성에서 참조하십시오.

라우팅 테이블 정보

라우팅 테이블 표시

절차

1단계 라우팅 테이블 내의 엔트리 보기:

```
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
```

라우팅 테이블을 채우는 방법

ASA 라우팅 테이블은 고정 정의 경로, 직접 연결 경로, 그리고 RIP, EIGRP, OSPF 및 BGP 라우팅 프로토콜로 발견된 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 대상으로의 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 논리가 둘 중 사용할 경로를 결정합니다.

  예를 들어 RIP와 OSPF 프로세스가 다음 경로에서 발견된 경우:

  – RIP: 192.168.32.0/24

  – OSPF: 192.168.32.0/19

  비록 OSPF 경로가 관리 거리가 더 낮지만 서로의 접두사 길이(서브넷 마스크)가 다르기 때문에 두 경로 모두 라우팅 테이블에 설치됩니다. 이들은 다른 대상으로 간주되며 패킷 전달 논리가 사용할 경로를 결정합니다.

- ASA이(가) 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 연결되어 최우선부터 최하위까지 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 값의 메트릭을 갖는 동일한 목적지로의 경로가 여럿인 경우 이러한 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

- ASA이(가) 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 거리를 변경할 수 있습니다. 서로 다른 두 라우팅 프로토콜에서 두 경로의 관리 거리가 같은 경우 *기본* 관리 거리가 낮은 경로가 라우팅 테이블에 입력됩니다. EIGRP와 OSPF 경로의 경우 EIGRP 경로와 OSPF 경로가 같은 관리 거리를 갖는다면 기본적으로 EIGRP 경로가 선택됩니다.

관리 거리는 2개의 서로 다른 라우팅 프로토콜에서 동일한 목적지로 2개 이상의 다른 경로가 있는 경우 최적의 경로를 선택하기 위해 ASA에서 사용하는 경로 매개변수입니다. 라우팅 프로토콜은 다른 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 다른 라우팅 프로토콜에서 생성된 두 경로 중에 항상 최적의 경로를 확인할 수 있는 것은 아닙니다.

각 라우팅 프로토콜은 관리 거리 값을 사용하여 우선순위가 지정됩니다. 표 18-1은 ASA에서 지원되는 라우팅 프로토콜의 기본 관리 거리 값을 표시합니다.

표 18-1 지원되는 라우팅 프로토콜의 기본 관리 거리

경로 소스	기본 관리 거리
연결된 인터페이스	0
고정 경로	1
EIGRP 요약 경로	5
외부 BGP	20
내부 EIGRP	90
OSPF	110
RIP	120
EIGRP 외부 경로	170
내부 BGP	200
알 수 없음	255

관리 거리 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. 이 경우 라우터가 라우팅 테이블에 경로의 OSPF 버전을 추가합니다.

이 예제에서, OSPF 파생 경로의 소스가 손실된 경우(예: 전원 꺼짐) ASA는 OSPF 파생 경로가 다시 나타날 때까지 RIP 파생 경로를 사용합니다.

관리 거리는 로컬 설정입니다. 예를 들어 **distance-ospf** 명령을 사용하여 OSPF를 통해 얻은 관리 거리를 변경하면 이는 명령을 입력한 ASA의 라우팅 테이블에만 영향을 줍니다. 관리 거리는 라우팅 업데이트에서 알려지지 않습니다.

관리 거리는 라우팅 프로세스에 영향을 주지 않습니다. EIGRP, OSPF, RIP 및 BGP 라우팅 프로세스는 라우팅 프로세스를 통해서 검색되었거나 라우팅 프로세스로 재배포된 경로만 알립니다. 예를 들어, RIP 라우팅 프로세스는 OSPF 라우팅 프로세스를 통해 발견된 경로가 ASA 라우팅 테이블에 사용된다 할지라도, RIP 경로를 알립니다.

백업 경로

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 거리를 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 거리로 설정된 고정 경로입니다. 동적 라우팅 프로세스가 발견한 해당 경로가 실패하면 라우팅 테이블에 고정 경로가 설치됩니다.

전달 결정 방법

전달 결정은 다음과 같이 이루어집니다.

- 대상이 라우팅 테이블 내의 엔트리와 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 전달됩니다. 기본 경로가 구성되지 않은 경우 패킷이 버려집니다.
- 대상이 라우팅 테이블의 단일 엔트리와 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 전달됩니다.
- 대상이 라우팅 테이블에 있는 두 개 이상의 엔트리와 일치하고 엔트리의 네트워크 접두사 길이가 모두 같다면 네트워크 접두사가 같고 인터페이스가 다른 두 엔트리는 라우팅 테이블 내에 공존할 수 없습니다.
- 대상이 라우팅 테이블에 있는 두 개 이상의 엔트리와 일치하고 엔트리의 네트워크 접두사 길이가 다를 경우 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷이 라우팅 테이블에서 다음 경로를 가진 ASA의 인터페이스에 도착합니다.

```
ciscoasa# show route
        ....
        R   192.168.32.0/24 [120/4] via 10.1.1.2
        O   192.168.32.0/19 [110/229840] via 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. 라우팅 테이블 내 다른 경로에도 해당되지만 라우팅 테이블에서 192.168.32.0/24의 접두사가 가장 깁니다(24비트 vs. 19비트). 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

동적 라우팅 및 장애 조치

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 라우터)는 모든 라우팅 불가 패킷에 대한 저장소 역할을 하도록 지정되어 모든 메시지가 어떻게든 처리되도록 할 수 있습니다.

동적 경로는 활성 유닛의 라우팅 테이블이 변경될 때 스탠바이 유닛에서 동기화되므로 활성 유닛의 모든 추가, 삭제 또는 변경 사항은 대기 유닛에 즉시 전파됩니다. 기본 유닛이 활성화된 시간이 지나고 스탠바이 유닛이 활성화되면 장애 조치 일괄 동기화 프로세스의 일부로서 경로가 동기화되어 활성/스탠바이 장애 조치 쌍의 라우팅 테이블이 동시에 표시됩니다.

고정 경로와 그 구성 방법에 관한 자세한 정보는 19-2 페이지의 고정 경로 컨피그레이션에서 참조하십시오.

동적 라우팅 및 클러스터링

동적 라우팅은 클러스터에서 완벽하게 통합되고 경로는 여러 유닛에서 공유됩니다(클러스터 하나에서 최대 8개 유닛이 허용됨). 라우팅 테이블 엔트리 또한 클러스터 내 유닛에서 복제됩니다.

유닛이 마스터에서 슬레이브로 전환되면 이 RIB 테이블에 대한 시대 번호(32비트 시퀀스 번호)가 증가합니다. 전환 후 처음에는 새 마스터 유닛이 이전 마스터 유닛의 미러 이미지인 RIB 테이블 엔트리를 갖습니다. 또한 새 마스터 유닛에서 리컨버전스 타이머가 시작됩니다. RIB 테이블의 시대 번호가 증가하면 모든 기존 엔트리가 오래된 항목으로 간주됩니다. IP 패킷의 전달은 정상적으로 계속됩니다. 새 마스터 유닛에서는 동적 라우팅 프로토콜이 시작되어 기존 경로 엔트리를 업데이트하거나 새 경로 엔트리를 새로운 시대 번호로 업데이트합니다. 수정된 엔트리나 새로운 엔트리에 최신 시대 번호가 있으면 엔트리가 갱신되어 모든 슬레이브 유닛에 동기화되었다는 뜻입니다. 리컨버전스 타이머가 만료된 후 RIB 테이블의 기존 엔트리가 삭제됩니다. OSPF 경로, RIP 경로 및 EIGRP 경로를 위한 RIB 테이블 엔트리가 슬레이브 유닛에 동기화됩니다.

일괄 동기화는 유닛이 클러스터에 참여하고 참여하는 유닛에 대한 마스터 유닛에서 온 경우에만 이루어집니다.

동적 라우팅 업데이트의 경우 마스터 유닛이 OSPF, RIP 또는 EIGRP를 통한 새 경로를 학습할 때, 마스터 유닛은 신뢰할 수 있는 메시지 전송을 통해 모든 슬레이브 유닛으로 업데이트를 보냅니다. 슬레이브 유닛은 클러스터 경로 업데이트 메시지를 받은 후 해당 RIB 테이블을 업데이트합니다.

지원되는 동적 라우팅 프로토콜(OSPF, EIGRP, RIP)의 경우 슬레이브 유닛에서 레이어 2 로드 밸런싱 인터페이스의 라우팅 패킷이 마스터 유닛에 전달됩니다. 마스터 유닛만 동적 라우팅 프로토콜 패킷을 보고 처리합니다. 슬레이브 유닛이 일괄 동기화를 요청하면 레이어 2 로드 밸런싱 인터페이스를 통해 학습된 모든 라우팅 엔트리가 복제됩니다.

마스터 유닛의 레이어 2 로드 밸런싱 인터페이스를 통해 새로운 라우팅 엔트리가 학습되면 새로운 엔트리가 모든 슬레이브 유닛으로 브로드캐스트됩니다. 기존 라우팅 엔트리가 네트워크 토폴로지 변경으로 인해 수정될 경우 수정된 엔트리는 모든 슬레이브 유닛에 동기화됩니다. 기존 라우팅 엔트리가 네트워크 토폴로지 변경으로 인해 삭제될 경우 삭제된 엔트리는 모든 슬레이브 유닛에 동기화됩니다.

레이어 2 및 레이어 3 로드 밸런싱 인터페이스의 조합이 배포되고 동적 라우팅을 위해 구성되면, 슬레이브 유닛은 라우팅 프로세스에서 부분적인 토폴로지 및 인접 디바이스 정보(레이어 3 로드 밸런싱 인터페이스를 통해 얻은 정보 포함)만 갖습니다. 레이어 2 로드 밸런싱 인터페이스에 대해 오직 RIB 테이블 엔트리만 마스터 유닛에서 동기화되기 때문입니다. 레이어 2 및 레이어 3가 다른 라우팅 프로세스에 속하도록 네트워크를 구성하고 각 라우팅 프로세스의 부하를 재분배해야 합니다.

표 18-2는 지원되는 컨피그레이션에 대한 요약을 제공합니다. Yes는 두 프로세스의 조합(레이어 2와 레이어 3 프로세스 하나씩)이 작동함을 의미하고 No는 작동하지 않음을 의미합니다.

표 18-2 지원되는 컨피그레이션 요약

레이어 2 또는 레이어 3	OSPF(레이어 3)	EIGRP(레이어 3)	RIP(레이어 3)
OSPF(레이어 2)	예	예	예
EIGRP(레이어 2)	예	아니요	예
RIP(레이어 2)	예	예	아니요

클러스터의 모든 유닛이 동일한 모드(단일 또는 다중 컨텍스트 모드)에 있어야 합니다. 다중 컨텍스트 모드에서는 마스터 슬레이브 동기화가 동기화 메시지의 모든 컨텍스트와 모든 컨텍스트의 RIB 테이블 엔트리를 포함합니다.

클러스터링에서는 레이어 3 인터페이스를 구성한 경우 라우터 ID 풀 설정도 구성해야 합니다.

동적 라우팅 및 클러스터링에 관한 자세한 내용은 8 장, "ASA 클러스터"에서 참조하십시오.

다중 컨텍스트 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 있습니다. 혼합 컨텍스트 모드에서 라우팅 모드의 컨텍스트에서 어떤 동적 라우팅 프로토콜이라도 활성화할 수 있습니다. RIP 및 OSPFv3는 다중 컨텍스트 모드에서 지원되지 않습니다.

다음 표는 EIGRP 특성, OSPFv2, OSPFv2 및 EIGRP 프로세스로 경로 배포를 위해 사용되는 경로 맵, 그리고 다중 컨텍스트 모드로 사용할 때 영역에 들어가거나 영역을 나가는 라우팅 업데이트를 필터링하기 위해 OSPFv2에서 사용하는 접두사 목록을 나열합니다.

EIGRP	OSPFv2	경로 맵 및 접두사 목록
컨텍스트당 하나의 인스턴스가 지원됩니다.	컨텍스트당 2개의 인스턴스가 지원됩니다.	N/A
시스템 컨텍스트에서 비활성화됩니다.		N/A
2개의 컨텍스트가 사용하는 자율 시스템 번호가 같을 수도 있고 다를 수도 있습니다.	2개의 컨텍스트가 사용하는 지역 ID가 같을 수도 있고 다를 수도 있습니다.	N/A
2개의 컨텍스트가 공유하는 인터페이스는 여러 EIGRP 인스턴스를 실행할 수도 있습니다.	2개의 컨텍스트가 공유하는 인터페이스는 여러 OSPF 인스턴스를 실행할 수도 있습니다.	N/A
공유 인터페이스 간 EIGRP 인스턴스의 상호 작용이 지원됩니다.	공유 인터페이스 간 OSPFv2 인스턴스의 상호 작용이 지원됩니다.	N/A
단일 모드에서 사용 가능한 모든 CLI는 다중 컨텍스트 모드에서도 사용 가능합니다.		
각 CLI는 그것이 사용되는 컨텍스트에만 영향을 미칠 수 있습니다.		

경로 리소스 관리

*경로*라고 하는 리소스 클래스가 도입되었고 컨텍스트에 존재할 수 있는 라우팅 테이블의 최대 개수를 지정합니다. 이것은 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.

프록시 **ARP** 요청 비활성화

호스트가 같은 이더넷 네트워크의 다른 디바이스로 IP 트래픽을 전송하는 경우 호스트가 디바이스의 MAC 주소를 알아야 합니다. ARP는 IP 주소를 MAC 주소에 대해 확인하는 레이어 2 프로토콜입니다. 호스트는 ARP에 요청을 전송하여 IP 주소가 누구인지 묻고 해당 IP 주소를 소유한 디바이스가 자신이 IP 주소의 소유자라고 응답하고 MAC 주소를 알려주는 것입니다.

프록시 ARP는 디바이스가 해당 IP 주소를 소유하지 않더라도 자신의 MAC 주소로 ARP 요청에 응답할 때 사용됩니다. ASA는 NAT를 구성할 때 프록시 ARP를 사용하고 ASA 인터페이스와 같은 네트워크에 있는 매핑된 주소를 지정합니다. 트래픽이 호스트에 도달할 수 있는 유일한 방법은 ASA가 프록시 ARP를 사용하여 MAC 주소가 주소에 매핑된 대상에 할당되어 있음을 주장하는 것입니다.

아주 드문 경우 NAT 주소에 대한 프록시 ARP를 비활성화할 수 있습니다.

기존 네트워크와 겹치는 VPN 클라이언트 주소 풀이 있는 경우 ASA는 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 호스트를 향한 VPN 클라이언트의 반환 트래픽이 잘못된 인터페이스로 전달되고 버려집니다. 이 경우 원치 않는 인터페이스에 대한 프록시 ARP 요청을 비활성화해야 합니다.

절차

1단계 프록시 ARP 요청 비활성화:

sysopt noproxyarp *interface*

예:

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

19 장

고정 경로 및 기본 경로

이 장에서는 Cisco ASA에서 고정 경로와 기본 경로를 구성하는 방법을 설명합니다.

고정 경로 및 기본 경로 정보

트래픽을 연결되지 않은 호스트 또는 네트워크로 라우팅하려면 호스트 또는 네트워크로의 고정 경로를 정의해야 합니다. 또는 최소한 ASA가 직접 연결되지 않은 네트워크에 대한 기본 경로를 정의해야 합니다(예: 네트워크와 ASA 사이에 라우터가 있는 경우).

고정 경로 또는 기본 경로가 정의되지 않은 경우 연결되지 않은 호스트 또는 네트워크로의 트래픽에서 다음 syslog 메시지가 생성됩니다.

```
%ASA-6-110001: No route to dest_address from source_address
```

다음의 경우 단일 컨텍스트 모드의 고정 경로를 사용할 수 있습니다.

- 네트워크가 EIGRP, RIP 또는 OSPF에서 다른 라우터 검색 프로토콜을 사용합니다.
- 네트워크 규모가 작고 고정 경로를 쉽게 관리할 수 있습니다.
- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.

가장 간단한 옵션은 트래픽을 라우팅하는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 경로를 구성하는 것입니다. 그러나 기본 게이트웨이가 대상 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.

투명 방화벽 모드에서는 ASA에서 발생하고 직접 연결되지 않은 네트워크가 목적지인 트래픽에 대해 기본 경로 또는 고정 경로를 구성하여 ASA가 어떤 인터페이스로 트래픽을 보낼지 알 수 있도록 해야 합니다. ASA에서 발생하는 트래픽은 syslog 서버, Websense 또는 N2H2 서버나 AAA 서버로의 통신을 포함할 수 있습니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다. 또한 ASA은 로드 밸런싱을 위해 동일 인터페이스에서 최대 3개의 동일 비용 경로를 지원합니다.

고정 경로 및 기본 경로를 위한 지침

장애 조치 지침

동적 라우팅 프로토콜의 상태 기반 장애 조치를 지원합니다.

추가 지침

- IPv6 고정 경로는 ASDM의 투명 모드에서 지원되지 않습니다.
- 클러스터링에서 고정 경로 모니터링은 마스터 유닛에서만 지원됩니다. 클러스터링에 대한 내용은 8 장, "ASA 클러스터"를 참고하십시오.

고정 경로 컨피그레이션

고정 라우팅 알고리즘은 기본적으로 네트워크 관리자가 라우팅 시작 전에 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. 이러한 이유로 고정 라우팅 시스템은 네트워크 상의 변화에 대처할 수 없습니다.

고정 경로는 지정된 게이트웨이를 사용할 수 없게 되더라도 라우팅 테이블에서 유지됩니다. 지정된 게이트웨이를 사용할 수 없게 되면 라우팅 테이블에서 고정 경로를 수동으로 제거해야 합니다. 그러나 고정 경로는 지정된 인터페이스가 다운될 경우 라우팅 테이블에서 제거되고 인터페이스가 복구되면 재개됩니다.

참고 ASA에서 실행 중인 라우팅 프로토콜보다 관리 거리가 큰 고정 경로를 만드는 경우 라우팅 프로토콜로 검색된 지정된 경로로의 경로가 고정 경로보다 우선합니다. 고정 경로는 동적으로 검색된 경로가 라우팅 테이블에서 제거된 경우에만 사용됩니다.

인터페이스당 도일 대상에 대하여 최대 3개의 동일 비용 경로를 정의할 수 있습니다. ECMP(equal-cost multipath)는 여러 인터페이스에 걸쳐 지원되지 않습니다. ECMP를 사용하면 트래픽이 경로 간에 고르게 분할되지 않을 수도 있습니다. 트래픽은 소스와 대상 IP 주소를 해싱하는 알고리즘을 기반으로 지정된 게이트웨이 사이에서 분배됩니다.

고정 null0 경로 컨피그레이션

ACL은 일반적으로 트래픽 필터링에 사용되며 헤더에 포함된 정보에 기초하여 패킷을 필터링할 수 있습니다. 패킷 필터링에서 ASA 방화벽은 패킷 헤더를 검사하여 필터링 결정을 내리고 패킷 처리에 오버헤드를 추가함으로써 성능에 영향을 줍니다.

고정 null 0 라우팅은 필터링을 보완하는 솔루션입니다. 고정 null0 경로는 black hole로 원하지 않거나 바람직하지 않은 트래픽을 전달하는 데 사용됩니다. null 인터페이스 null0은 black hole 생성에 사용됩니다. 고정 경로는 바람직하지 않은 대상에 대해 생성되며 고정 경로 컨피그레이션은 null 인터페이스를 향합니다. black hole 고정 경로와의 최적의 일치를 포함한 대상 주소의 트래픽은 자동으로 삭제됩니다. ACL과는 달리 고정 null0 경로는 성능 저하를 일으키지 않습니다.

고정 null0 경로 컨피그레이션은 라우팅 루프를 방지하는 데 사용됩니다. BGP는 Remotely Triggered Black Hole 라우팅을 위해 고정 null0 컨피그레이션을 활용합니다.

예:

```
route null0 192.168.2.0 255.255.255.0
```

고정 경로를 구성하려면 다음 섹션을 참조하십시오..

- 19-3 페이지의 고정 경로 추가 또는 편집

고정 경로 추가 또는 편집

절차

1단계 고정 경로 추가 또는 편집

route *if_name dest_ip mask gateway_ip* [*distance*]

예:

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]
```

dest_ip 및 *mask* 인수는 대상 네트워크의 IP 주소를 나타내고 *gateway_ip* 인수는 다음 홉 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 1입니다. 관리 거리는 서로 다른 라우팅 프로토콜의 경로를 비교하는 데 사용되는 매개변수입니다. 고정 경로에서 기본 관리 거리는 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다.

OSPF가 발견한 경로에 대한 기본 관리 거리는 110입니다. 고정 경로의 관리 거리가 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

예

다음 예는 외부 인터페이스의 3가지 게이트웨이로 트래픽을 안내하는 동일 비용 경로인 고정 경로를 보여줍니다. ASA는 지정된 게이트웨이 간에 트래픽을 배포합니다.

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

기본 고정 경로 구성

기본 고정 경로는 ASA가 학습 경로나 고정 경로를 가지고 있지 않은 모든 IP 패킷을 보낼 게이트웨이 IP 주소를 식별합니다. 기본 고정 경로는 단순히 대상 IP 주소가 0.0.0.0/0인 고정 경로입니다. 특정 대상을 식별하는 경로가 기본 경로보다 우선합니다.

참고 버전 7.0(1) 이상에서는 메트릭이 서로 다른 인터페이스에서 2개의 기본 경로를 구성한 경우 더 높은 메트릭 인터페이스에서 ASA(으)로의 연결은 실패하지만 낮은 메트릭에서 ASA로의 연결은 예상대로 성공합니다.

디바이스당 최대 3개의 동일 비용 기본 경로 엔트리를 정의할 수 있습니다. 동일 비용 기본 경로 엔트리를 하나 이상 정의하면 기본 경로로 전송되는 트래픽이 지정된 게이트웨이 사이에서 분산될 수 있습니다. 기본 경로를 하나 이상 정의할 경우 각 엔트리에 대해 동일한 인터페이스를 지정해야 합니다.

3개 이상의 동일 비용 기본 경로 또는 이전에 정의된 기본 경로와 인터페이스가 다른 기본 경로를 정의하려고 하면 다음 메시지가 표시됩니다.

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

표준 기본 경로를 가지고 터널링된 트래픽을 위한 별도의 기본 경로를 정의할 수 있습니다. 터널링 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 ASA에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 터널에서 발생하는 트래픽에 대하여 이 경로는 다른 구성된 기본 경로나 학습된 기본 경로를 무시합니다.

기본 고정 경로 설정 구성 제한 사항

터널링 옵션을 포함한 기본 경로에는 다음 제한 사항이 적용됩니다.

- 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.
- 터널링 옵션에서 두 개 이상의 기본 경로를 정의할 수 없습니다.
- 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

절차

1단계 터널링 기본 고정 경로 추가 또는 편집:

route *if_name* 0.0.0.0 0.0.0.0 *gateway_ip* [*distance* | *tunneled*]

예:

```
ciscoasa(config)# route outside 0 0 192.168.2.4 tunneled
```

dest_ip 및 *mask* 인수는 대상 네트워크의 IP 주소를 나타내고 gateway_ip 인수는 다음 홉 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 1입니다. 관리 거리는 서로 다른 라우팅 프로토콜의 경로를 비교하는 데 사용되는 매개변수입니다. 고정 경로에서 기본 관리 거리는 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다. OSPF가 발견한 경로에 대한 기본 관리 거리는 110입니다. 고정 경로의 관리 거리가 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

팁 다음 예에서와같이 대상 네트워크 주소와 마스크로 0.0.0.0 0.0.0.0 대신 00을 입력할 수 있습니다.

```
ciscoasa(config)# route outside 0 0 192.168.1 1
```

IPv6 기본 및 고정 경로 구성

호스트가 연결되고 IPv6 및 IPv6 ACL에 대해 활성화된 인터페이스가 트래픽을 허용할 경우 ASA는 자동으로 직접 연결된 호스트 사이에 IPv6 트래픽을 라우팅합니다.

절차

1단계 기본 IPv6 경로 추가:

ipv6 route *if_name* **::/0** *next_hop_ipv6_addr*

예:

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1
```

예제에서는 네트워크 7fff::0/32의 패킷을 3FFE:1100:0:CC00::1에 위치한 내부 인터페이스의 네트워킹 디바이스로 라우팅합니다.

주소 ::/0은 IPv6에서 'any'에 해당합니다.

2단계 IPv6 라우팅 테이블에 IPv6 고정 경로를 추가:

ipv6 route *if_name destination next_hop_ipv6_addr* [*admin_distance*]

예:

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]
```

예제에서는 네트워크 7fff::0/32의 패킷을 3FFE:1100:0:CC00::1에 위치한 관리 거리가 110인 내부 인터페이스의 네트워킹 디바이스로 라우팅합니다.

참고 **ipv6 route** 명령은 IPv4 고정 경로 정의에 사용되는 **route** 명령과 마찬가지로 작동합니다.

고정 또는 기본 경로 모니터링

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.

ASA는 사용자가 정의하는 모니터링 대상과 고정 경로를 연결하여 이 기능을 실행하고 ICMP 에코 요청을 사용하여 대상을 모니터링합니다. 에코 응답이 지정된 시간 동안 수신되지 않으면 객체는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다. 이전에 구성된 백업 경로가 삭제된 경로의 자리에 사용됩니다.

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)
- AAA 서버와 같이 ASA이(가) 통신해야 하는 대상 네트워크에 있는 서버
- 대상 네트워크에 있는 지속적인 네트워크 객체

참고 저녁에 전원이 꺼지는 데스크톱이나 노트북 컴퓨터는 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.

절차

1단계 모니터링 프로세스를 정의함으로써 추적 객체 모니터링 매개변수를 구성:

sla monitor *sla_id*

예:

```
ciscoasa(config)# sla monitor 5
```

유형이 이미 정의되어 있는 예정되지 않은 모니터링 프로세스를 위해 모니터링 매개변수를 변경하는 경우 자동으로 sla 프로토콜 컨피그레이션 모드에 진입합니다.

2단계 모니터링 프로토콜을 지정:

type echo protocol ipIcmpEcho *target_ip* **interface** *if_name*

예:

```
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 172.29.139.134
```

유형이 이미 정의되어 있는 예정되지 않은 모니터링 프로세스를 위해 모니터링 매개변수를 변경하는 경우 자동으로 sla 프로토콜 컨피그레이션 모드에 진입하고 이 설정을 변경할 수 없게 됩니다.

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.

3단계 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**]

예:

```
ciscoasa(config)# sla monitor schedule 5 start-time now
```

일반적으로 모니터링 예약을 위해 **sla monitor schedule** *sla_id* **life forever start-time now** 명령을 사용하고 모니터링 컨피그레이션이 테스트 실행 빈도를 결정하도록 허용합니다.

하지만 모니터링 프로세스를 나중에 지정된 시간에만 실행되도록 예약할 수 있습니다.

4단계 추적 고정 경로를 SLA 모니터링 프로세스와 연결:

track *track_id* **rtr** *sla_id* **reachability**

예:

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 인수는 이 명령으로 할당하는 추적 번호입니다. *sla_id* 인수는 SLA 프로세스의 ID 번호입니다.

5단계 고정 경로 추적:

route *if_name dest_ip mask gateway_ip* [*admin_distance*] **track** *track_id*

예:

```
ciscoasa(config)# route if_name dest_ip mask gateway_ip [admin_distance] track track_id
```

고정 경로 추적에서 **tunneled** 옵션을 **route** 명령과 함께 사용할 수 없습니다.

6단계 DHCP를 통해 얻은 기본 경로 추적:

```
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# dhcp client route track track_id
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config-if)# exit
```

setroute 키워드를 **ip address dhcp** 명령과 함께 사용하여 DHCP를 사용한 기본 경로를 얻어야 합니다.

7단계 PPPoE를 통해 얻은 기본 경로 추적:

```
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# pppoe client route track track_id
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config-if)# exit
```

setroute 키워드를 **ip address pppoe** 명령과 함께 사용하여 PPPoE를 사용한 기본 경로를 얻어야 합니다.

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 외부 인터페이스의 3가지 게이트웨이로 안내하는 동일 비용 고정 경로 3개를 정의하며 터널링 트래픽에 기본 경로를 추가합니다. ASA는 지정된 게이트웨이 간에 트래픽을 배포합니다.

```
ciscoasa(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.2
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.3
ciscoasa(config)# route outside 0 0 192.168.2.4 tunneled
```

IP 주소가 192.168.2.1, 192.168.2.2 및 192.168.2.3인 게이트웨이 간에 배포된 고정 또는 학습 경로가 없는 ASA가 수신한 암호화되지 않은 트래픽입니다. IP 주소가 192.168.2.4인 게이트웨이로 전달된 고정 또는 학습 경로가 없는 ASA가 수신한 암호화된 트래픽입니다.

다음 예는 내부 인터페이스에 연결된 라우터(10.1.2.45)에 10.1.1.0/24가 목적지인 모든 트래픽을 보내는 고정 경로를 생성합니다.

```
ciscoasa(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

고정 경로 및 기본 경로 내역

표 19-1 고정 경로 및 기본 경로 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
라우팅	7.0(1)	고정 및 기본 경로를 도입했습니다. 도입된 명령: **route**
클러스터링	9.0(1)	마스터 유닛에서만 고정 경로 모니터링을 지원합니다.
고정 null0 경로 컨피그레이션	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. 수정된 명령: **route**.

20 장

경로 맵

경로 맵 정보

경로 맵은 경로를OSPF, 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 구문으로 각각 허용 또는 거부라는 결과를 갖습니다. ACL 또는 경로 맵의 평가는 미리 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.
- 일반 메커니즘 - 기준 일치와 일치 해석은 적용 방식에 따라 정해집니다. 같은 경로 맵이라도 다른 작업에 적용되면 다르게 해석될 수 있습니다.

다음은 경로 맵과 ACL의 차이점입니다.

- 경로 맵은 자주 ACL을 일치 기준으로 사용합니다.
- ACL 평가의 주된 결과는 예/아니요 응답입니다. ACL은 입력 데이터를 허용하거나 거부합니다. 재배포에 적용할 경우 ACL은 특정 경로를 재배포할 수 있는지(경로가 ACL 허용 구문과 일치) 아니면 재배포할 수 없는지(거부 구문과 일치) 결정합니다. 일반적인 경로 맵은 재배포된 경로를 허용할 뿐만 아니라 다른 프로토콜로 재배포될 때 경로와 연결된 정보를 수정하기도 합니다.
- 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. 경로 맵에 대해서는 이런 관행이 없습니다. 일치 시도 중에 경로 맵의 끝에 도달하는 경우 결과는 경로 맵의 애플리케이션이 무엇인지에 따라 달라집니다. 다행히도 재배포에 적용되는 경로 맵은 ACL과 동일하게 작동합니다. 경로가 경로 맵의 조항과 일치하지 않으면 마치 경로 맵이 끝에 거부 구문을 포함한 것처럼 경로 재배포가 거부됩니다.

동적 **redistribute** 명령을 통해 경로 맵을 적용할 수 있습니다. Cisco ASDM에서 이 재배포 기능은 새로운 경로 맵을 추가하거나 편집할 때 발견할 수 있습니다(20-4 페이지의 경로 맵을 정의 참조). 재배포 중 경로 정보를 수정하려거나 ACL이 제공할 수 있는 것보다 강력한 일치 기능을 원할 경우 경로 맵이 선호됩니다. 단순히 접두사나 마스크를 기준으로 경로를 선택적으로 허용하려는 경우 경로 맵을 사용하여 **redistribute** 명령에서 직접 ACL(또는 동등한 접두사 목록)로 매핑할 것을 추천합니다. 접두사나 마스크를 기준으로 경로를 선택적으로 허용하기 위해 경로 맵을 사용하는 경우 같은 목적을 달성하기 위해 일반적으로 더 많은 컨피그레이션 명령을 사용하게 됩니다.

참고 경로 맵에 대한 일치 기준으로 표준 ACL을 사용해야 합니다. 확장 ACL을 사용하면 효과가 없으며 경로가 재배포되지 않을 것입니다. 나중에 절을 추가해야 할 경우에 대비하여 10 간격의 숫자 절을 추천합니다.

허용 및 거부 절

경로 맵은 허용 및 거부 절을 가질 수 있습니다. **route-map ospf-to-eigrp** 명령에는 하나의 거부 절(순차 번호 10)과 두 개의 허용 절이 있습니다. 거부 절은 재배포에서 경로 일치를 거부합니다. 따라서 다음 규칙이 적용됩니다.

- 허용 절을 사용하는 경로 맵에서 ACL을 사용할 경우 ACL이 허용한 경로가 재배포됩니다.
- 경로 맵 거부 절에서 ACL을 사용할 경우 ACL이 허용한 경로가 재배포되지 않습니다.
- 경로 맵 허용 또는 거부 절에서 ACL을 사용하고 ACL이 경로를 거부할 경우 경로 맵 절 일치 항목이 발견되지 않고 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 ASDM의 Set Value 탭 또는 **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. **match** 명령 또는 ASDM의 Match Clause 탭에 설정된 Match Clause가 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 검색이 계속됩니다.

다음 조건 중 하나가 존재할 경우 각 절의 일치 또는 설정 값은 누락되거나 여러 번 반복될 수 있습니다.

- 절에 여러 **match** 명령 또는 ASDM의 Match Clause 값이 존재하는 경우 주어진 경로에 대해 모두 성공해야 경로가 절에 일치할 수 있습니다(논리 AND 알고리즘이 여러 일치 명령에 적용됨).
- ASDM에서 **match** 명령 또는 Match Clause 값이 하나의 명령에서 여러 객체를 참조하는 경우 둘 중 하나가 일치합니다(논리 OR 알고리즘 적용). 예를 들어 **match ip address 101 121** 명령에서 ACL 101 또는 ACL 121이 허용할 경우 경로가 허용됩니다.

- **match** 명령이나 ASDM의 Match Clause 값이 없는 경우 모든 경로가 절에 일치합니다. 이전 예제에서 절 30에 도달하는 모든 경로가 일치하고 경로 맵의 끝에 도달하지 않습니다.
- 경로 맵 허용 절에 **set** 명령 또는 ASDM의 Set Value 값이 없는 경우 현재 속성의 수정 없이 경로가 재배포됩니다.

참고 경로 맵의 **set** 명령이 절을 거부하도록 구성하지 마십시오. 거부 절은 경로 재배포를 금지하므로 수정할 정보가 없기 때문입니다.

match 또는 **set** 명령 또는 ASDM의 Match or Set Value 탭에 설정된 Match 또는 Set Value가 없는 경로 맵의 경우 작업을 수행합니다. 빈 허용 절은 수정 없이 남은 경로의 재배포를 허용합니다. 빈 거부 절은 다른 경로의 재배포를 허용하지 않습니다(경로 맵을 완전히 스캔했으나 정확한 일치 항목을 찾지 못한 경우 이것이 기본 작업).

BGP 일치 및 BGP 설정 절

위에 설명한 일치 및 설정 값 외에 BGP는 경로 맵에 대한 추가 일치 및 설정 기능을 제공합니다.

다음 새로운 경로-맵 일치 절은 BGP에서 지원됩니다.

- match as-path
- match community
- match policy-list
- match tag

다음 새로운 경로-맵 설정치 절은 BGP에서 지원됩니다.

- set as-path
- set automatic-tag
- set community
- set local-preference
- set origin
- set weight

재배포되는 각 BGP 경로에 대해 ASA는 먼저 경로 맵에 있는 절의 BGP 일치 기준을 평가합니다. BGP 일치 기준이 성공하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부되고 ASDM의 BGP Set Clause 탭 또는 **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. **match** 명령 또는 ASDM의 BGP Match Clause 탭에 설정된 Match Clause가 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 검색이 계속됩니다.

경로 맵에 대한 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

추가 지침

경로 맵은 사용자, 사용자 그룹 또는 정규화된 도메인 이름 객체를 포함하는 ACL을 지원하지 않습니다.

경로 맵을 정의

지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 지정할 때 경로 맵을 정의해야 합니다.

절차

1단계 경로 맵 엔트리 생성:

route-map *name* {**permit** | **deny**} [*sequence_number*]

예:

```
ciscoasa(config)# route-map name {permit} [12]
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 인수를 사용하여 순서를 파악합니다. 그러지 않으면 ASA가 경로 맵 엔트리를 추가하는 순서를 사용합니다.

경로 맵 사용자 정의

이 섹션은 경로 맵을 사용자 정의하는 방법을 설명합니다.

- 20-4 페이지의 특정 대상 주소와 일치하도록 경로를 정의
- 20-5 페이지의 경로 작업에 대한 메트릭 값 구성

특정 대상 주소와 일치하도록 경로를 정의

절차

1단계 경로 맵 엔트리 생성:

route-map *name* {**permit** | **deny**} [*sequence_number*]

예:

```
ciscoasa(config)# route-map name {permit} [12]
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 옵션을 사용하여 순서를 파악합니다. 그러지 않으면 ASA이(가) 경로 맵 엔트리를 추가하는 순서를 사용합니다.

2단계 표준 ACL 또는 접두사 목록과 일치하는 대상 네트워크를 가진 모든 경로와 일치:

match ip address *acl_id* [*acl_id*] [...] [prefix-list]

예:

```
ciscoasa(config-route-map)# match ip address acl1
```

ACL을 하나 이상 지정한 경우 경로가 모든 ACL과 일치할 수 있습니다.

3단계 구체적인 메트릭을 가진 경로와 일치:

match metric *metric_value*

예:

```
ciscoasa(config-route-map)# match metric 200
```

*metric_value*의 범위는 0~4294967295입니다.

4단계 표준 ACL과 일치하는 차기 홉 라우터 주소를 가진 경로와 일치:

match ip next-hop *acl_id* [*acl_id*] [...]

예:

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

ACL을 하나 이상 지정한 경우 경로가 모든 ACL과 일치할 수 있습니다.

5단계 지정된 차기 홉 인터페이스를 가진 모든 경로와 일치:

match interface *if_name*

예:

```
ciscoasa(config-route-map)# match interface if_name
```

하나 이상의 인터페이스를 지정하는 경우 경로가 아무 인터페이스나 일치할 수 있습니다.

6단계 표준 ACL과 일치하는 라우터가 알린 경로와 일치:

match ip route-source *acl_id* [*acl_id*] [...]

예:

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

ACL을 하나 이상 지정한 경우 경로가 모든 ACL과 일치할 수 있습니다.

7단계 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.

절차

1단계 경로 맵 엔트리 생성:

route-map *name* {**permit** | **deny**} [*sequence_number*]

예:

```
ciscoasa(config)# route-map name {permit} [12]
```

경로 맵 엔트리는 순서대로 읽힙니다. *sequence_number* 인수를 사용하여 순서를 파악합니다. 그러지 않으면 ASA가 경로 맵 엔트리를 추가하는 순서를 사용합니다.

2단계 경로 맵에 대한 메트릭 값 설정:

set metric *metric_value*

예:

```
ciscoasa(config-route-map)# set metric 200
```

metric_value 인수의 범위는 0~294967295입니다.

3단계 경로 맵에 대한 메트릭 유형 설정:

set metric-type {**type-1** | **type-2**}

예:

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 인수는 type-1 또는 type-2가 될 수 있습니다.

경로 맵 컨피그레이션 예

다음 예는 합 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 맵에 대한 기능 내역

표 20-1 경로 맵에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
경로 맵	7.0(1)	이 기능을 도입했습니다. 도입된 명령: **route-map**.
고정 및 동적 경로 맵에 대한 지원 개선	8.0(2)	동적 및 고정 경로 맵에 대한 향상된 지원이 추가되었습니다.
동적 라우팅 프로토콜(EIGRP, OSPF 및 RIP)에 대한 Stateful Failover 지원, 일반 라우팅 관련 작업 디버깅	8.4(1)	도입된 명령: **debug route**, **show debug route**. 수정된 명령: **show route**.
다중 컨텍스트 모드의 동적 라우팅	9.0(1)	경로 맵은 다중 컨텍스트 모드에서 지원됩니다.
BGP 지원	9.2(1)	이 기능을 도입했습니다. 도입된 명령: **router bgp**
		다음 명령을 도입했습니다.

21 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 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. 자율 시스템(AS) 사이에서 BGP가 사용될 때 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때 프로토콜은 IBGP(Interior BGP)라고 합니다.

라우팅 테이블 변경 사항

인접 디바이스 간 TCP 연결이 처음 설정되면 BGP 인접 디바이스가 전체 라우팅 정보를 교환합니다. 라우팅 테이블 변경 사항이 감지되면 BGP 라우터가 변경된 경로만 이웃으로 전송합니다. BGP 라우터는 주기적인 라우팅 업데이트를 전송하지 않고 BGP 라우팅 업데이트는 대상 네트워크로의 최적의 경로만 알립니다.

BGP를 통해 학습된 경로에는 특정 대상으로 향하는 경로가 여럿일 때 최적의 경로를 결정하는 데 사용되는 속성이 포함되어 있습니다. 이러한 속성을 BGP 속성이라고 하며 경로 선택 과정에서 사용됩니다.

- Weight -- Cisco가 정의한 라우터에 대한 로컬 속성입니다. 가중치 속성은 주변의 라우터에 알려지지 않습니다. 라우터가 동일한 대상에 대하여 하나 이상의 경로를 학습한 경우 가중치가 가장 높은 경로가 우선합니다.
- Local preference -- 로컬 설정 속성은 로컬 AS로부터 출구 지점을 선택하는 데 사용됩니다. 가중치 속성과 달리 로컬 설정 속성은 로컬 AS 전체에 걸쳐 전파됩니다. AS에서 출구 지점이 여럿인 경우 로컬 설정 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 학습하는지 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 학습됩니다.
  - Incomplete- 경로의 발신지를 알 수 없거나 학습되지 않았습니다. 경로가 BGP로 재배포되면 불완전한 발신지가 됩니다.
- AS_path -- 경로 광고가 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(승인, 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 이웃에 전파합니다. BGP는 제시된 순서대로 다음 기준에 따라 대상에 대한 경로를 선택합니다.

- 경로가 접근할 수 없는 next hop을 지정하면 업데이트를 삭제합니다.
- 가중치가 가장 높은 경로가 우선합니다.
- 가중치가 동일한 경우 로컬 설정이 가장 높은 경로가 우선합니다.
- 로컬 설정이 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 이웃을 통한 경로가 우선합니다.
- 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 이웃 주소에서 시작하는 경로가 우선합니다.

BGP용 가이드라인

상황 모드 가이드라인

단일 및 다중 상황 모드에서 지원

방화벽 모드 가이드라인

투명 방화벽 모드를 지원하지 않습니다. BGP는 라우터 모드에서만 지원됩니다.

장애 조치 가이드라인

단일 및 다중 상황 모드에서 상태 기반 장애 조치를 지원합니다.

참고 클러스터가 활성화되면, 장애 조치는 지원되지 않습니다.

클러스터링 가이드라인

BGP는 L2(EtherChannel 유형) 및 L3(개별 인터페이스 유형) 클러스터링 모드에서만 지원됩니다.

참고 사용자 상황에서 BGP 컨피그레이션을 삭제하고 다시 적용하는 경우 슬레이브/스탠바이 ASA 유닛이 동기화할 수 있도록 60초간 기다리십시오.

IPv6 가이드라인

IPv6를 지원합니다. IPv6 주소군에 대해서는 graceful restart가 지원되지 않습니다.

BGP 구성

이 섹션에서는 시스템에서 BGP 프로세스를 활성화하고 구성하는 방법을 설명합니다.

절차

1단계 CLI에서 BGP를 활성화하고 일반 BGP 파라미터를 구성합니다.

2단계 BGP 라우팅 프로세스를 위한 최적의 경로를 정의하고 최적의 경로 컨피그레이션 파라미터를 구성합니다.

3단계 정책 목록을 추가 및 구성합니다.

4단계 AS 경로 필터를 추가 및 구성합니다.

5단계 커뮤니티 규칙을 추가 및 구성합니다.

6단계 IPv4 주소군 설정을 구성합니다.

BGP 사용

이 섹션에서는 BGP 라우팅 활성화, BGP 라우팅 프로세스 설정 및 일반 BGP 파라미터 구성에 필요한 단계를 설명합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

*autonomous-num*에 대한 유효한 값은 1~4294967295와 1.0~XX.YY입니다.

2단계 지정된 값을 초과하는 as-path 세그먼트를 포함한 경로는 버립니다.

bgp maxas-limit *number*

예:

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 인수는 허용된 최대 자율 시스템 세그먼트 개수를 지정합니다. 유효한 값은 1부터 254까지입니다.

3단계 로그 BGP 인접 디바이스 재설정:

bgp log-neighbor-changes

4단계 BGP가 자동으로 각 BGP 세션에 대한 최적의 TCP 경로 MTU를 발견하도록 합니다.

bgp transport path-mtu-discovery

5단계 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

6단계 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

7단계 BGP 4바이트 자율 시스템 번호의 기본 표시 및 정규식 일치 형식을 asplain(10진수)에서 dot notation으로 바꿉니다.

bgp asnotation dot

8단계 BGP 네트워크 타이머 조정:

timers bgp *keepalive holdtime* [*min-holdtime*]

예:

```
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 인접 디바이스를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)입니다.

9단계 BGP graceful restart 기능 활성화:

bgp graceful-restart [**restart-time** *seconds*|**stalepath-time** *seconds*][**all**]

예:

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- **restart-time** — graceful-restart-capable 인접 디바이스가 이벤트 발생 후 정상 작업으로 복귀하기까지 ASA가 대기할 최대 시간(초)입니다. 기본값은 120초입니다. 유효한 값은 1부터 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 1부터 3600초입니다.

BGP 라우팅 프로세스를 위한 최적의 경로 정의

이 섹션에서는 BGP 최적의 경로 구성에 필요한 단계를 설명합니다. 최정의 경로에 대한 자세한 정보는 21-2 페이지의 BGP 경로 선택에서 참조하십시오.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 기본 로컬 설정 값을 변경:

bgp default local-preference *number*

예:

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 인수는 0과 4294967295 사이의 모든 값이 될 수 있습니다. 값이 높을수록 우선순위가 높습니다. 기본값은 100입니다.

3단계 다른 자율 시스템의 인접 디바이스에서 학습된 경로 간 MED(Multi Exit Discriminator) 비교 활성화:

bgp always-compare-med

4단계 최적의 경로 선정 과정 중 eBGP(external BGP) 피어에서 수신된 비슷한 경로를 비교하고 라우터 ID가 가장 낮은 최적의 경로로 전환:

bgp bestpath compare-routerid

5단계 주변의 AS에서 전달된 최적의 MED 경로를 선택:

bgp deterministic-med

6단계 MED 속성이 누락된 경로를 우선순위가 가장 낮은 경로로 설정:

bgp bestpath med missing-as-worst

정책 목록 구성

경로 지도 내에서 정책 목록이 참조되는 경우 정책 목록의 모든 일치 문장이 평가 및 처리됩니다. 경로 지도 내에 둘 이상의 정책 목록을 구성할 수 있습니다. 정책 목록은 같은 경로 지도 내에 있으나 정책 목록 밖에서 구성된 기존 일치 항목 및 설정 문구와도 공존할 수 있습니다. 이 섹션은 정책 목록 구성에 필요한 단계를 설명합니다.

절차

1단계 정책-지도 컨피그레이션 모드를 활성화하고 BGP 정책 목록 생성을 허용:

policy-list *policy_list_name* {**permit** | **deny**}

예:

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

permit 키워드는 일치 조건에 대해 액세스를 허용합니다.

deny 키워드는 일치 조건에 대해 액세스를 거부합니다.

2단계 next hop이 지정된 인터페이스 중 하나를 벗어난 경로를 배포:

match interface [...*interface_name*]

예:

```
ciscoasa(config-policy-list)# match interface outside
```

3단계 대상 주소, next hop 라우터 주소 및 라우터/액세스 서버 소스 중 하나 또는 모두를 일치시켜 경로를 재배포:

match ip {**address** | **next-hop** | **route-source**}

4단계 BGP 자율 시스템 경로 일치:

match as-path

5단계 BGP 커뮤니티 일치:

match community {*community-list_name* | **exact-match**}

예:

```
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.

6단계 지정된 메트릭을 포함한 경로 재배포:

```
match metric
```

7단계 지정된 태그와 일치하는 라우팅 테이블에서 경로 재배포:

```
match tag
```

AS 경로 필터 구성

AS 경로 필터는 액세스 목록을 사용하고 업데이트 메시지 내에 개별 프리픽스를 살펴봄으로써 라우팅 업데이트 메시지를 필터링할 수 있습니다. 업데이트 메시지 내 프리픽스가 필터 기준과 일치하면 필터 엔트리에서 수행하도록 구성된 작업에 따라 해당 개별 프리픽스가 필터링되거나 승인됩니다. 이 섹션에서는 AS 경로 필터 구성에 필요한 단계를 설명합니다.

참고 **as-path access-lists**는 일반 방화벽 ACL과 다릅니다.

절차

1단계 글로벌 컨피그레이션 모드의 정규식을 사용하여 자율 시스템 경로 필터를 컨피그레이션:

```
as-path access-list acl-number {permit|deny} regexp
```

예:

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number* — AS-path 액세스 목록 번호. 유효한 값은 1부터 500까지입니다.
- *regexp* — AS-path 필터를 정의하는 정규식. 자율 시스템 번호는 1~65535 범위로 표현됩니다.

커뮤니티 규칙 구성

커뮤니티는 공통 속성을 공유하는 대상 그룹입니다. 커뮤니티 목록을 사용하여 경로 지도의 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.

절차

1단계 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}
```

예:

```
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 인접 디바이스 설정에 대한 하위 섹션이 포함됩니다. 이 하위 섹션을 통해 IPv4 주소군에 대한 파라미터를 사용자 정의할 수 있습니다.

이 섹션에서는 BGP IPv4 주소군 설정 사용자 정의 방법을 설명합니다.

- 21-9 페이지의 IPv4 주소군 일반 설정 구성
- 21-11 페이지의 IPv4 주소군 종합 주소 설정 구성
- 21-12 페이지의 IPv4 주소군 필터링 설정 구성
- 21-12 페이지의 IPv4 주소군 BGP 인접 디바이스 설정 구성
- 21-17 페이지의 IPv4 네트워크 설정 구성
- 21-18 페이지의 재분배 설정 구성
- 21-19 페이지의 경로 삽입 설정 구성

IPv4 주소군 일반 설정 구성

이 섹션에서는 일반 IPv4 설정에 필요한 단계를 설명합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 라우터를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [**unicast**]

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 (선택 사항) 로컬 BGP 라우팅 프로세스에 대한 고정 라우터 ID를 구성:

bgp router-id *A.B.C.D*

예:

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

인수 *A.B.C.D*는 IP 주소 형식으로 라우터 ID를 지정합니다. 라우터 ID를 지정하지 않으면 자동으로 할당됩니다.

4단계 (선택 사항) 개별 인터페이스(L3) 모드에서 IP 주소의 클러스터 풀을 구성:

bgp router-id *cluster-pool*

예:

```
ciscoasa(config-router-af)# bgp router-id cp
```

참고 L3 클러스터에서 BGP 인접 디바이스를 클러스터 풀 IP 주소 중 하나로 정의할 수 없습니다.

5단계 BGP 경로에 대한 관리 거리를 구성:

distance bgp *external-distance internal-distance local-distance*

예:

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- *external-distance* — 외부 BGP 경로를 위한 관리 거리. 외부 자율 시스템에서 학습한 경로는 외부 경로입니다. 이 인수 값 범위는 1~255입니다.
- *internal-distance* — 내부 BGP 경로를 위한 관리 거리. 로컬 자율 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.

6단계 BGP 학습 경로를 통해 IP 라우팅 테이블이 업데이트될 때 메트릭 및 태그 값 수정:

table-map {**WORD**|*route-map_name*}

예:

```
ciscoasa(config-router-af)# table-map example1
```

route-map_name 인수는 **route-map** 명령의 경로 지도를 지정합니다.

7단계 기본 경로를 배포하도록 BGP 라우팅 프로세스를 구성(네트워크 0.0.0.0):

default-information originate

8단계 네트워크 수준 경로로 서브넷 경로 자동 요약을 구성:

auto-summary

9단계 RIB(routing information base)에 설치되지 않은 경로 알림을 억제:

bgp suppress-inactive

10단계 BGP와 IGP(Interior Gateway Protocol) 시스템 간 동기화:

synchronization

11단계 OSPF와 같은 IGP로의 iBGP 재배포 구성:

bgp redistribute-internal

12단계 next hop 확인을 위한 BGP 라우터 스캔 간격을 구성:

bgp scan-time *scanner-interval*

예:

```
ciscoasa(config-router-af)# bgp scan-time 15
```

scanner-interval 인수는 BGP 라우팅 정보의 스캔 간격을 지정합니다. 유효한 값은 5부터 60초입니다. 기본값은 60초입니다.

13단계 BGP next-hop 주소 추적 구성:

bgp nexthop trigger {**delay** *seconds*|**enable**}

예:

```
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.

14단계 라우팅 테이블에 설치할 수 있는 병렬 iBGP 경로의 최대 수를 제어:

maximum-paths {*number_of_paths*|ibgp *number_of_paths*}

예:

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

참고 *number_of_paths* argument는 라우팅 테이블에 설치할 경로의 수를 지정합니다. ASA 9.3(1)에서 유효한 값은 1~3입니다.
ibgp 키워드를 사용하지 않으면 *number_of_paths* 인수가 병렬 EBGP 경로의 최대 개수를 제어합니다.

IPv4 주소군 종합 주소 설정 구성

이 섹션에서는 하나의 경로로의 특정 경로 종합을 정의하는 데 필요한 단계를 설명합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [**unicast**]

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 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*]

예:

```
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 지도.
- (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.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [**unicast**]

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 발신 BGP 업데이트에서 수신된 경로나 네트워크를 필터링:

distribute-list *acl-number* **in**|**out**[]

예:

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

acl-number 인수는 IP 액세스 목록 번호를 지정합니다. 액세스 목록은 라우팅 업데이트에서 어떤 네트워크를 수신하고 어떤 네트워크를 억제할지 정의합니다.

in 키워드는 필터를 수신 BGP 업데이트에 적용하도록 지정하고 **out** 키워드는 필터를 발신 BGP 업데이트에 적용하도록 지정합니다.

IPv4 주소군 BGP 인접 디바이스 설정 구성

이 섹션은 BGP 인접 디바이스 및 인접 디바이스 설정 정의에 필요한 단계를 설명합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 라우터를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [**unicast**]

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 BGP 인접 디바이스 테이블에 엔트리 추가:

neighbor *ip-address* **remote-as** *autonomous-number*

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

4단계 (선택 사항) 인접 또는 피어 그룹 비활성화:

neighbor *ip-address* **shutdown**

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

5단계 BGP 인접 디바이스와 정보 교환:

neighbor *ip-address* **activate**

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

6단계 BGP 인접 디바이스에 대한 BGP(Border Gateway Protocol) graceful restart 기능 활성화 또는 비활성화:

neighbor *ip-address* **ha-mode graceful-restart** [**disable**]

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

(선택 사항) **disable** 키워드는 **인접 디바이스에 대한** BGP graceful restart 기능을 비활성화합니다.

7단계 BGP 인접 디바이스 정보를 액세스 목록에 지정된 대로 배포:

neighbor {*ip-address*} **distribute-list** {*access-list-name*}{**in**|**out**}

예:

```
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 프리픽스 목록의 이름.
- **in** — 액세스 목록이 해당 인접 디바이스의 수신 알림에 적용됩니다.
- **out** — 액세스 목록이 해당 인접 디바이스의 발신 알림에 적용됩니다.

8단계 수신 또는 발신 경로에 경로 지도 적용:

neighbor {*ip-address*} **route-map** *map-name* {**in**|**out**}

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

in 키워드는 수신 경로에 대한 경로 지도에 적용됩니다.

out 키워드는 발신 경로에 대한 경로 지도에 적용됩니다.

9단계 BGP 인접 디바이스 정보를 프리픽스 목록에 지정된 대로 배포:

neighbor {*ip-address*} **prefix-list** *prefix-list-name* {**in**|**out**}

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

in 키워드는 프리픽스 목록이 해당 인접 디바이스의 수신 알림에 적용됨을 의미합니다.

out 키워드는 프리픽스 목록이 해당 인접 디바이스의 수신 알림에 적용됨을 의미합니다.

10단계 필터 목록 설정:

neighbor {*ip-address*} **filter-list** *access-list-number* {**in**|**out**}

예:

```
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 인접 디바이스의 수신 알림에 적용됩니다.
- **out** — 액세스 목록이 해당 인접 디바이스의 발신 알림에 적용됩니다.

11단계 인접 디바이스에서 수신할 수 있는 프리픽스 개수를 제어:

neighbor {*ip-address*} **maximum-prefix** *maximum* [*threshold*][**restart** *restart interval*][**warning-only**]

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- *maximum* — 이 인접 디바이스에서 최대 개수의 프리픽스가 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 인접 디바이스가 재시작되는 시간 간격을 지정하는 정수 값(분)입니다.
- (선택 사항) **warning-only** — 프리픽스 최대 개수를 초과하면 피어링을 종료하는 대신 라우터가 로그 메시지를 생성하도록 허용합니다.

12단계 BGP 스피커(로컬 라우터)가 기본 경로 0.0.0.0을(를) 인접 디바이스로 전송하도록 허용:

neighbor {*ip-address*} **default-originate** [**route-map** *map-name*]

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

인수 *map-name*은 route-map의 이름입니다. 이 경로 지도는 경로 0.0.0.0을(를) 조건부로 삽입하도록 허용합니다.

13단계 BGP 라우팅 업데이트 전송 최소 간격을 설정:

neighbor {*ip-address*} **advertisement-interval** *seconds*

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

seconds 인수는 시간(초)입니다. 유효한 값은 0~600입니다.

14단계 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**]

예:

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- **advertise-map** *map name* — exist 지도 또는 non-exist 지도의 조건이 충족될 경우 알릴 경로 지도의 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) **모든 경로 확인** — BGP 테이블의 프리픽스를 통해 모든 경로를 exist-map으로 확인할 수 있도록 허용합니다.

15단계 아웃바운드 라우팅 업데이트에서 비공개 자율 시스템 번호를 제거:

neighbor {*ip-address*} **remove-private-as**

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

16단계 특정 BGP 피어 또는 피어 그룹에 대한 타이머를 설정합니다.

neighbor {*ip-address*} **timers** *keepalive holdtime min holdtime*

예:

```
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.

17단계 두 BGP 피어 간 TCP 연결에 대한 MD5(Message Digest 5) 인증 활성화:

neighbor {*ip-address*} **password** *string*

예:

```
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 있으면 인증이 실패할 수 있습니다.

18단계 커뮤니티 속성을 BGP 인접 디바이스로 전송하도록 지정:

neighbor {*ip-address*} **send-community**[**both**|**standard**|**extended**]

예:

```
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.

19단계 라우터를 BGP 인접 또는 피어 그룹에 대한 next hop으로 구성:

neighbor {*ip-address*}**next-hop-self**

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

20단계 직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도:

neighbor {*ip-address*} **ebgp-multihop** [*ttl*]

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

ttl 인수는 1~255홉 범위의 time-to-live를 지정합니다.

21단계 연결 확인을 비활성화하여 루프백 인터페이스를 사용하는 단일 홉 피어를 통한 eBGP 피어링 세션을 설정:

neighbor {*ip-address*} **disable-connected-check**

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

22단계 BGP 피어링 세션을 보안하고 두 외부 BGP(eBGP) 피어를 분리하는 최대 홉 개수를 구성:

neighbor {*ip-address*} **ttl-security hops** *hop-count*

예:

```
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 1부터 254까지입니다.

23단계 인접 디바이스 연결에 가중치 할당:

neighbor {*ip-address*} **weight** *number*

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

number 인수는 인접 디바이스 연결에 할당하는 가중치입니다. 유효한 값은 0~65535입니다.

24단계 ASA가 특정 BGP 버전만 승인하도록 구성:

neighbor {*ip-address*} **version** *number*

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

number 인수는 BGP 버전 번호를 지정합니다. 버전을 2로 설정하여 소프트웨어가 지정된 인접 디바이스에서 버전 2만 사용하도록 강제할 수 있습니다. 기본값은 버전 4를 사용하고 요청 시 동적으로 버전 2까지 사용할 수 있도록 하는 것입니다.

25단계 BGP 세션에 대한 TCP 전송 세션 옵션 활성화:

neighbor {*ip-address*} **transport** {**connection-mode**{**active**|**passive**}|
path-mtu-discovery[**disable**]}

예:

```
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.

26단계 eBGP(Border Gateway Protocol) 인접 디바이스에서 수신된 AS_PATH 속성을 사용자 정의:

neighbor {*ip-address*} **local-as** [*autonomous-system-number*[**no-prepend**]]

예:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (선택 사항) *autonomous-system-number* — AS_PATH 속성에 프리픽스로 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 인접 디바이스에서 수신한 경로에 붙이지 않습니다.

IPv4 네트워크 설정 구성

이 섹션은 BGP 라우팅 프로세스가 알릴 네트워크를 정의합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 BGP 라우팅 프로세스가 알릴 네트워크를 지정:

network {*network-number [***mask** *network-mask]}[***route-map** *map-tag]*

예:

```
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 지도의 식별자. 알릴 네트워크를 필터링하려면 경로 지도를 검사해야 합니다. 지정하지 않으면 모든 네트워크를 알립니다.

재분배 설정 구성

이 섹션은 다른 라우팅 도메인의 경로로부터 BGP로 재배포하는 조건을 정의하기 위한 단계를 설명합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

address-family ipv4 [unicast]

예:

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 다른 라우팅 도메인의 경로를 BGP 자율 시스템으로 재배포:

redistribute *protocol [process-id] [metric] [***route-map [map-tag]]**
예:

```
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 지도의 식별자.

참고 재배포할 네트워크를 필터링하려면 경로 지도를 검사해야 합니다. 지정하지 않으면 모든 네트워크를 재배포합니다.

경로 삽입 설정 구성

이 섹션에서는 BGP 라우팅 테이블에 조건부로 삽입할 경로를 정의하기 위한 단계를 설명합니다.

절차

1단계 BGP 라우팅 프로세스를 활성화하여 ASA를 라우터 컨피그레이션 모드로 놓습니다.

router bgp *autonomous-num*

예:

```
ciscoasa(config)# router bgp 2
```

2단계 주소군 컨피그레이션 모드에 진입하여 표준 IP 버전 4(IPv4) 주소 프리픽스를 사용한 라우팅 세션 컨피그레이션:

```
address-family ipv4 [unicast]
```

예:

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

unicast 키워드는 IPv4 유니캐스트 주소 프리픽스를 지정합니다. 지정하지 않아도 이것이 기본값입니다.

3단계 조건부 경로 삽입을 구성하여 BGP 라우팅 테이블로 더 많은 특정 경로를 삽입:

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

예:

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- *inject-map* — 로컬 BGP 라우팅 테이블로 삽입할 프리픽스를 지정하는 경로 지도 이름.
- *exist-map* — BGP 스피커가 추적하는 프리픽스를 포함하는 경로 지도의 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 참조에서 참조하십시오. 또한 인접 디바이스 변경 메시지 및 인접 디바이스 경고 메시지의 로깅을 비활성화할 수 있습니다.

다양한 BGP 라우팅 통계를 모니터링하려면 다음 명령 중 하나를 입력:

- **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 neighbors** *ip_address*

  인접 디바이스에 대한 BGP 및 TCP 연결에 관한 정보를 표시합니다.
- **show bgp paths** [LINE]

  데이터베이스의 모든 BGP 경로를 표시합니다.
- **show bgp pending-prefixes**

  삭제 대기 중인 프리픽스를 표시합니다.
- **show bgp prefix-list** *prefix_list_name* [WORD]

  명시된 프리픽스 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 지도를 기반으로 BGP 라우팅 테이블에 엔트리를 입력합니다.
- **show bgp summary**

  모든 BGP 연결의 상태를 표시합니다.

- **show bgp system-config**

  다중 상황 모드에서 시스템 상황별 BGP 컨피그레이션을 표시합니다.

  이 명령은 다중 상황 모드의 모든 사용자 상황에서 이용 가능합니다.

- **show bgp update-group**

  BGP 업데이트 그룹에 대한 정보를 표시합니다.

참고 BGP 로그 메시지를 비활성화하려면 **no bgp log-neighbor-changes** 명령을 라우터 컨피그레이션 모드에 입력합니다. 이는 인접 디바이스 변경 메시지 로깅을 비활성화합니다. 이 명령을 BGP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드에 입력합니다.
기본적으로 인접 디바이스 변경 사항은 로깅됩니다.

BGP에 대한 컨피그레이션 예

이 예는 다양한 프로세스 옵션으로 BGPv4를 활성화하고 구성하는 방법을 보여줍니다.

1단계 하나의 라우팅 프로토콜에서 다른 프로토콜로 경로를 재배포하거나 정책 라우팅을 활성화하는 조건을 정의:

```
ciscoasa(config)# route-map mymap2 permit 10
```

2단계 경로 주소가 있거나 지정된 액세스 목록 중 하나로 통과한 패킷과 일치하는 경로를 재배포:

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

3단계 정책 라우팅에 대한 경로 지도의 일치 조항을 통과하는 패킷을 출력할 장소를 표시:

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4단계 글로벌 컨피그레이션 모드에서 BGP 라우팅 프로세스를 활성화:

```
ciscoasa(config)# router bgp 2
```

5단계 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
```

6단계 BGP 인접 디바이스 테이블에 엔트리 추가:

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7단계 수신 또는 발신 경로에 경로 지도 적용:

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

BGP 내역

표 21-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 21-1 BGP 기능 내역

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**. 수정된 명령: **show route**, **show route summary**, **show running-config router**, **clear config router**, **clear route all**, **timers lsa arrival**, **timers pacing**, **timers throttle**, **redistribute bgp**.
ASA 클러스터링을 위한 BGP 지원	9.3(1)	L2 및 L3 클러스터링에 대한 지원을 추가했습니다. 도입된 명령: **bgp router-id clusterpool**
NSF를 위한 BGP 지원	9.3(1)	무중단 전달을 위한 지원을 추가했습니다. 새로 도입된 명령: **bgp graceful-restart, neighbor ha-mode graceful-restart**
광고 맵을 위한 BGP 지원	9.3(1)	BGPv4 광고 맵 지원을 추가했습니다. 새로 도입된 명령: **neighbor advertise-map**

22 장

OSPF

이 장에서는 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 데이터를 라우팅하고, 인증을 수행하고, 라우팅 정보를 재배포할 수 있도록 Cisco ASA를 구성하는 방법에 대해 설명합니다.

이 장에는 다음 섹션이 포함됩니다.

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 인접 디바이스 목록이 있습니다.

RIP를 능가하는 OSPF의 장점은 다음과 같습니다.

- OSPF 링크 상태 데이터베이스 업데이트는 RIP 업데이트보다 전송되는 빈도가 적으며, 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 재배포하고자 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 재배포할 수 있습니다.

ASA에서는 다음과 같은 OSPF 기능을 지원합니다.

- 영역 내, 영역 간 및 외부(유형 I 및 유형 II) 경로
- 가상 링크
- L SA 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 재배포 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 재배포하는 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 광고하지 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.

OSPF Support for Fast Hello Packets 기능

OSPF Support for Fast Hello Packets 기능에서는 hello 패킷을 1초 미만의 간격으로 전송하도록 구성하는 방법을 제공합니다. 이러한 컨피그레이션을 통해 OSPF(Open Shortest Path First) 네트워크에서 통합 속도를 단축할 수 있습니다.

OSPF Support for Fast Hello Packets 기능의 사전 요구 사항

OSPF는 네트워크에서 기존에 구성해야 하거나 OSPF Support for Fast Hello Packets 기능과 동시에 구성해야 합니다.

OSPF Support for Fast Hello Packets 기능 정보

다음 섹션에서는 OSPF Support for Fast Hello Packets 기능과 관련된 개념에 대해 설명합니다.

OSPF Hello 간격 및 Dead 간격

OSPF Hello 패킷은 OSPF 프로세스에서 OSPF 인접 디바이스와의 연결을 유지하기 위해 이러한 인접 디바이스에 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 인접 디바이스 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 인접 디바이스에서 Hello 패킷을 수신하지 못할 경우, 해당 인접 디바이스는 중단된 것으로 선언됩니다.

OSPF Fast Hello Packets

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. 22-3 페이지의 OSPF Hello 간격 및 Dead 간격을 참조하십시오.

OSPF Fast Hello Packets 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 인터페이스의 Hello 간격은 무시됩니다.

Dead 간격은 세그먼트에서 일정해야 하며, 1초로 설정되거나(Fast Hello 패킷의 경우) 다른 값으로 설정됩니다. Hello 승수의 경우에는 Dead 간격 내에 최소 하나 이상의 Hello 패킷이 전송된다면 전체 세그먼트에서 동일하지 않아도 됩니다.

OSPF Fast Hello Packets 기능의 이점

OSPF Fast Hello Packets 기능의 이점은 OSPF 네트워크에서 Fast Hello 패킷을 사용하지 않는 경우와 비교했을 때 더 빠른 통합이 가능하다는 점입니다. 이 기능을 사용하면 1초 내에 손실된 인접 디바이스를 감지할 수 있습니다. 이 기능은 특히 OSI(Open System Interconnection) 물리적 레이어 및 데이터 링크 레이어로 감지할 수 없는 인접 디바이스가 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 인접 디바이스 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

컨텍스트 모드 지침

OSPFv2에서는 단일 또는 다중 컨텍스트 모드를 지원합니다.

OSPFv3에서는 단일 모드만 지원합니다.

방화벽 모드 지침

OSPF에서는 라우팅 방화벽 모드만 지원합니다. OSPF에서는 투명 방화벽 모드를 지원하지 않습니다.

장애 조치 지침

OSPFv2 및 OSPFv3에서는 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

- OSPFv2 및 OSPFv3에서는 클러스터링을 지원합니다.
- OSPFv3 암호화는 지원되지 않습니다. 클러스터링 환경에서 OSPFv3 암호화를 구성하려고 할 경우 오류 메시지가 표시됩니다.
- Spanned 인터페이스 모드의 경우, 전용 관리 인터페이스에 동적 라우팅을 지원하지 않습니다.
- 개별 인터페이스 모드의 경우, 마스터 및 슬레이브 유닛을 OSPFv2 또는 OSPFv3 인접 디바이스로 설정해야 합니다.
- OSPFv2 및 EIGRP를 모두 설정할 경우, Spanned 인터페이스 모드 또는 개별 인터페이스 모드를 사용할 수 있으며 두 가지 모드를 동시에 사용할 수는 없습니다.
- 개별 인터페이스 모드의 경우, OSPFv2 인접성은 마스터 유닛의 공유 인터페이스에 있는 두 컨텍스트 간에만 설정할 수 있습니다. 고정 인접 디바이스 구성은 포인트-투-포인트 링크에서만 지원되므로, 하나의 인터페이스에서는 하나의 인접 디바이스 명령문만 허용됩니다.
- 라우터 ID는 OSPFv2, OSPFv3 및 EIGRP 경로 컨피그레이션 모드의 선택 사항입니다. 라우터 ID를 명시적으로 설정하지 않을 경우, 라우터 ID가 자동으로 생성되며 각 클러스터 유닛의 모든 데이터 인터페이스에서 가장 높은 IPv4 주소로 설정됩니다.
- 클러스터 인터페이스 모드를 구성하지 않은 경우, 점으로 구분된 단일한 십진수 IPv4 주소만 라우터 ID로 사용할 수 있으며 **cluster pool** 옵션이 비활성화됩니다.
- 클러스터 인터페이스 모드가 Spanned 컨피그레이션으로 설정된 경우, 점으로 구분된 단일한 십진수 IPv4 주소만 라우터 ID로 사용할 수 있으며 **cluster pool** 옵션이 비활성화됩니다.
- 클러스터 인터페이스 모드가 개별 컨피그레이션으로 설정된 경우, **cluster pool** 옵션을 필수이며 점으로 구분된 단일한 십진수 IPv4 주소를 라우터 ID로 사용할 수 없습니다.
- **check-detail** 또는 **nocheck** 옵션을 지정하지 않은 상태로 클러스터 인터페이스 모드가 Spanned에서 개별 컨피그레이션으로 변경되거나 그 반대로 변경될 경우, 라우터 ID를 포함한 전체 컨피그레이션이 제거됩니다.
- 동적 라우팅 프로토콜 라우터 ID 컨피그레이션이 새 인터페이스 모드와 호환되지 않을 경우, 콘솔에 오류 메시지가 표시되며 인터페이스 모드 CLI에 오류가 발생합니다. 오류 메시지에는 동적 라우팅 프로토콜(OSPFv2, OSPFv3, EIGRP)당 내용이 한 줄씩 포함되며 컨피그레이션 비호환이 발생한 각 컨텍스트의 이름이 나열됩니다.
- **cluster interface mode** 명령에 **nocheck** 옵션이 지정되지 않은 경우, 모든 라우터 ID 컨피그레이션이 새 모드와 호환되지 않는 경우에도 인터페이스 모드를 변경할 수 있습니다.
- 클러스터가 활성화되어 있으면 라우터 ID 호환성 확인이 반복됩니다. 비호환성이 감지되면 **cluster enable** 명령이 실패합니다. 관리자는 클러스터를 활성화하기 전에 호환되지 않는 ID 컨피그레이션을 올바르게 수정해야 합니다.
- 유닛에 클러스터가 슬레이브로 들어올 경우, **cluster interface mode** 명령에 **nocheck** 옵션을 지정하여 라우터 ID 호환성 확인 오류를 방지하는 것이 좋습니다. 슬레이브 유닛은 마스터 유닛에서 라우터 컨피그레이션을 계속 상속합니다.
- 클러스터에서 마스터 권한 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.

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.

OSPFv2 구성

이 섹션에서는 ASA에 OSPFv2 프로세스를 활성화하는 방법에 대해 설명합니다.

OSPFv2를 활성화한 후에는 경로 맵을 정의해야 합니다. 자세한 내용은 20-4 페이지의 경로 맵을 정의를 참조하십시오. 그런 다음 기본 경로를 생성합니다. 자세한 내용은 19-2 페이지의 고정 경로 컨피그레이션을 참조하십시오.

OSPFv2 프로세스의 경로 맵을 정의한 후에는 특정한 요구 사항에 맞게 이를 맞춤화할 수 있습니다. ASA에서 OSPFv2 프로세스를 맞춤화하는 방법을 알아보려면 22-7 페이지의 OSPFv2 맞춤화를 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.

절차

1단계 OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예:

```
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.

2단계 OSPF가 실행되는 IP 주소 및 해당 인터페이스의 영역 ID를 정의합니다.

network *ip_address mask* **area** *area_id*

예:

```
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.

OSPF Fast Hello Packets 구성

이 섹션에서는 OSPF Fast Hello Packets 기능을 구성하는 방법에 대해 설명합니다.

절차

1단계 인터페이스를 구성합니다.

interface port-channel *number*

예:

```
ciscoasa(config)# interface port-channel 10
```

number 인수는 포트 채널 인터페이스 수를 나타냅니다.

2단계 최소 하나 이상의 hello 패킷이 수신되어 간격을 설정합니다. 아니면 수신되지 않을 경우 해당 인접 디바이스는 중단된 것으로 간주됩니다.

ospf dead-interval minimal hello-multiplier *no.of times*

예:

```
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 맞춤화

이 섹션에서는 OSPFv2 프로세스를 맞춤화하는 방법에 대해 설명합니다.

- 22-8 페이지의 OSPFv2에 경로 재배포
- 22-9 페이지의 경로를 OSPFv2로 재배포 시 경로 요약 구성
- 22-10 페이지의 OSPFv2 영역 간의 경로 요약 구성
- 22-11 페이지의 OSPFv2 인터페이스 매개변수 구성
- 22-14 페이지의 OSPFv2 영역 매개변수
- 22-14 페이지의 OSPFv2 NSSA 구성
- 22-16 페이지의 클러스터링(OSPFv2 및 OSPFv3)에 대한 IP 주소 풀 구성
- 22-16 페이지의 고정 OSPFv2 인접 디바이스 정의

OSPFv2에 경로 재배포

ASA에서는 OSPFv2 라우팅 프로세스 간의 경로 재배포를 제어할 수 있습니다.

참고 지정된 라우팅 프로토콜에서 어떤 경로를 대상 라우팅 프로세스로 재배포할 수 있는지 정의하여 경로를 재배포하려면, 우선 기본 경로를 생성해야 합니다. 19-2 페이지의 고정 경로 컨피그레이션을 참조한 다음 20-4 페이지의 경로 맵을 정의에 따라 경로 맵을 정의합니다.

고정 경로, 연결된 경로, RIP 또는 OSPFv2 경로를 OSPFv2 프로세스에 재배포하려면 다음 단계를 수행합니다.

절차

1단계 OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예:

```
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.

2단계 연결된 경로를 OSPF 라우팅 프로세스에 재배포합니다.

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예:

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

3단계 고정 경로를 OSPF 라우팅 프로세스에 재배포합니다.

redistribute static [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*

예:

```
ciscoasa(config)# redistribute static 5 type-1 route-map-practice
```

4단계 OSPF 라우팅 프로세스의 경로를 다른 OSPF 라우팅 프로세스에 재배포합니다.

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*]

예:

```
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 재배포를 수행하는 경우가 나와 있습니다. ASA에서는 이러한 경로를 메트릭이 5이고 메트릭 유형이 Type 1인 외부 LSA로서 재배포합니다.

5단계 RIP 라우팅 프로세스의 경로를 OSPF 라우팅 프로세스에 재배포합니다.

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예:

```
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
```

6단계 EIGRP 라우팅 프로세스의 경로를 OSPF 라우팅 프로세스에 재배포합니다.

redistribute eigrp *as-num* [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

예:

```
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 재배포될 경우, 각 경로는 외부 LSA에 개별적으로 광고됩니다. 그러나 ASA를 구성하여 지정된 네트워크 주소 및 마스크에 포함되는 모든 재배포된 경로에 대한 단일 경로를 광고할 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 재배포를 제어할 수 있습니다.

경로 요약을 구성하려면 다음을 수행합니다.

- 22-10 페이지의 경로 요약 주소 추가

경로 요약 주소 추가

네트워크 주소 및 마스크에 포함되는 모든 재배포 경로의 단일한 요약 경로에 대한 소프트웨어 광고를 구성하려면, 다음 단계를 수행합니다.

절차

1단계 OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예:

```
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.

2단계 요약 주소를 설정합니다.

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

예:

```
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, 영역을 구성하여 지정된 범위에 속하는 영역 내의 모든 개별 네트워크가 포함된 요약 경로를 광고할 수 있습니다.

경로 요약을 위한 주소 범위를 정의하려면 다음 단계를 수행합니다.

절차

1단계 OSPF 라우팅 프로세스를 생성하고 이 OSPF 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.

router ospf *process_id*

예:

```
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.

2단계 주소 범위를 설정합니다.

```
area area-id range ip-address mask [advertise | not-advertise]
```

예:

```
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 매개변수 구성

필요한 경우 일부 인터페이스별 OSPFv2 매개변수를 변경할 수 있습니다. 이러한 매개변수는 변경할 필요가 없지만 **ospf hello-interval**, **ospf dead-interval**, and **ospf authentication-key** 같은 인터페이스 매개변수는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 구성할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

OSPFv2 인터페이스 매개변수를 구성하려면 다음 단계를 수행합니다.

절차

1단계 OSPF 라우팅 프로세스를 생성합니다.

```
router ospf process_id
```

예:

```
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.

2단계 OSPF가 실행되는 IP 주소 및 해당 인터페이스의 영역 ID를 정의합니다.

```
network ip_address mask area area_id
```

예:

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

3단계 인터페이스 컨피그레이션 모드로 들어갑니다.

```
interface interface_name
```

예:

```
ciscoasa(config)# interface my_interface
```

4단계 인터페이스의 인증 유형을 지정합니다.

```
ospf authentication [message-digest | null]
```

예:

```
ciscoasa(config-interface)# ospf authentication message-digest
```

5단계 OSPF 단순 비밀번호 인증을 사용하는 네트워크 세그먼트의 인접한 OSPF 라우터에서 사용할 비밀번호를 할당합니다.

ospf authentication-key *key*

예:

```
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.

6단계 OSPF 인터페이스에서 패킷을 전송하는 비용을 명시적으로 지정합니다.

ospf cost *cost*

예:

```
ciscoasa(config-interface)# ospf cost 20
```

*cost*는 1~65535 사이의 정수입니다.

이 예에서 비용은 20으로 설정되었습니다.

7단계 Hello 패킷이 수신되지 않는 인접 디바이스 OSPF 라우터를 중단된 라우터로 선언하기 전까지 디바이스가 대기해야 하는 시간을 초 단위로 설정합니다.

ospf dead-interval *seconds*

예:

```
ciscoasa(config-interface)# ospf dead-interval 40
```

이 값은 네트워크의 모든 노드에서 동일해야 합니다.

8단계 OSPF 인터페이스의 ASA에서 전송하는 Hello 패킷 간의 시간을 지정합니다.

ospf hello-interval *seconds*

예:

```
ciscoasa(config-interface)# ospf hello-interval 10
```

이 값은 네트워크의 모든 노드에서 동일해야 합니다.

9단계 OSPF MD5 인증을 활성화합니다.

ospf message-digest-key *key_id* **md5** *key*

예:

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

다음과 같은 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. 인접 디바이스 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.

10단계 네트워크에 대한 OSPF 전용 라우터를 결정하는 데 도움이 되는 우선순위를 설정합니다.

ospf priority *number_value*

예:

```
ciscoasa(config-interface)# ospf priority 20
```

number_value 인수의 범위는 0~255입니다.

11단계 OSPF 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다.

ospf retransmit-interval *seconds*

예:

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds 값은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 범위는 1에서 8192초입니다. 기본값은 5초입니다.

12단계 OSPF 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 설정합니다.

ospf transmit-delay *seconds*

예:

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds 값의 범위는 1~8192초입니다. 기본값은 1초입니다.

13단계 1초 동안 전송되는 Hello 패킷의 수를 설정합니다.

ospf dead-interval minimal hello-interval *multiplier*

예:

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

유효한 값은 3~20 사이의 정수입니다.

14단계 인터페이스를 포인트-투-포인트 비 브로드캐스트 네트워크로 지정합니다.

```
ospf network point-to-point non-broadcast
```

예:

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

인터페이스를 포인트-투-포인트 및 비 브로드캐스트로 지정할 경우, OSPF 인접 디바이스를 수동으로 정의해야 합니다. 동적 인접 디바이스 검색은 지원되지 않습니다. 자세한 내용은 22-16 페이지의 고정 OSPFv2 인접 디바이스 정의를 참조하십시오. 또한 해당 인터페이스에서는 하나의 OSPF 인접 디바이스만 정의할 수 있습니다.

OSPFv2 영역 매개변수

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.

절차

1단계 OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예:

```
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.

2단계 OSPF 영역에 인증 활성화

area *area-id* **authentication**

예:

```
ciscoasa(config-rtr)# area 0 authentication
```

3단계 OSPF 영역에 MD5 인증 활성화

area *area-id* **authentication message-digest**

예:

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

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 재배포를 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 간소할 수 있습니다.

NSSA를 구현하기 전에는, 원격 사이트의 경로를 스텁 영역으로 재배포할 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 재배포를 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.

절차

1단계 OSPF 라우팅 프로세스를 생성합니다.

router ospf *process_id*

예:

```
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.

2단계 NSSA 영역을 정의합니다.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]

예:

```
ciscoasa(config-rtr)# area 0 nssa
```

3단계 요약 주소를 설정하고 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

예:

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

OSPF에 이 명령을 사용하면 OSPF ASBR에서는 단일한 외부 경로를 해당 주소에서 다루는 모든 재배포 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

Individual Interface 클러스터링을 사용할 경우 라우터 ID 클러스터 풀에 대한 IPv4 주소의 범위를 할당할 수 있습니다.

절차

OSPFv2 및 OSPFv3를 지원하는 Individual Interface 클러스터링에서 라우터 ID 클러스터 풀에 대한 IPv4 주소의 범위를 할당하려면 다음 명령을 입력합니다.

1단계 Individual Interface 클러스터링에 대한 라우터 ID 클러스터 풀을 지정합니다.

router-id cluster-pool hostname | **A.B.C.D** *ip_pool*

예:

```
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 Individual Interface 클러스터링이 컨피그레이션될 때 IP 주소 풀을 구성할 수 있습니다. The **hostname** | **A.B.C.D.** 이 OSPF 프로세스에 대한 OSPF 라우터 ID를 지정하는 키워드입니다. *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 인접 디바이스를 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 인접 디바이스에 대한 고정 경로를 생성해야 합니다. 고정 경로 생성에 대한 자세한 내용은 19 장, "고정 경로 및 기본 경로"를 참조하십시오.

절차

세부 단계

	2단계	목적	명령
1단계	3단계	OSPFv2 라우팅 프로세스를 생성하고 이 OSPFv2 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.	**router ospf** *process_id* `ciscoasa(config)# router ospf 2`
	4단계	*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.	
2단계	5단계	OSPFv2 인접 디바이스후드 정의	**neighbor** *addr* [**interface** *if_name*] `ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]`
	6단계	*addr* 인수는 OSPFv2 인접 디바이스의 IP 주소입니다. *if_name* 인수는 인접 디바이스와 통신을 수행하는 데 사용되는 인터페이스입니다. OSPFv2 인접 디바이스가 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.

경로 계산 타이머를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**router ospf** *process_id* **예:** `ciscoasa(config)# router ospf 2`	OSPFv2 라우팅 프로세스를 생성하고 이 OSPFv2 프로세스의 라우터 컨피그레이션 모드로 들어갑니다. *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.

	명령	목적
2단계	**timers throttle spf** *spf-start spf-hold spf-maximum* **예:** `ciscoasa(config-router)# timers throttle spf 500 500 600`	경로 계산 시간을 구성합니다. *spf-start* 인수는 OSPF에서 토폴로지 변경을 수신하는 시간과 SPF 계산을 시작하는 시간 사이의 지연 시간(밀리초 단위)입니다. 입력 가능한 값은 0~600000까지의 정수입니다. *spf-hold* 인수는 두 번 연속으로 SPF를 계산하는 작업 사이의 최소 시간(밀리초 단위)입니다. 입력 가능한 값은 0~600000까지의 정수입니다. *spf-maximum* 인수는 두 번 연속으로 SPF를 계산하는 작업 사이의 최소 시간(밀리초 단위)입니다. 입력 가능한 값은 0~600000까지의 정수입니다.

인접 디바이스 작동 또는 중단 기록

OSPFv2 인접 디바이스가 작동 또는 중단될 경우 기본적으로 syslog 메시지가 생성됩니다.

debug ospf adjacency 명령을 켜지 않고 OSPFv2 인접 디바이스의 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.

OSPFv2 인접 디바이스의 작동 또는 중단을 기록하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**router ospf** *process_id* **예:** `ciscoasa(config)# router ospf 2`	OSPFv2 라우팅 프로세스를 생성하고 이 OSPFv2 프로세스의 라우터 컨피그레이션 모드로 들어갑니다. *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.
2단계	**log-adj-changes** [**detail**] **예:** `ciscoasa(config-rtr)# log-adj-changes [detail]`	인접 디바이스의 작동 또는 중단을 기록하도록 구성합니다.

OSPFv3 구성

이 섹션에서는 OSPFv3 라우팅 프로세스를 구성하는 방법에 대해 설명합니다.

OSPFv3 활성화

OSPFv3를 활성화하려면 OSPFv3 라우팅 프로세스를 생성하고, OSPFv3에 대한 영역을 생성하고, OSPFv3에 대한 인터페이스를 활성화하고, 경로를 대상 OSPFv3 라우팅 프로세스에 재배포해야 합니다.

OSPFv3를 활성화하려면다음 명령을 입력하거나 다음 단계를 수행합니다.

명령	목적
ipv6 router ospf *process-id* **예:** `ciscoasa(config)# ipv6 router ospf 10`	OSPFv3 라우팅 프로세스를 생성하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *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.

	명령	목적
1단계	**interface** *interface_name* 예: ciscoasa(config)# interface Gigabitethernet0/0	인터페이스를 활성화합니다.
2단계	**ipv6 ospf** *process-id* **area** *area_id* 예: ciscoasa(config)# ipv6 ospf 200 area 100	지정된 프로세스 ID로 OSPFv3 라우팅 프로세스를 생성하고, 지정된 영역 ID로 OSPFv3에 대한 영역을 생성합니다.

OSPFv3 인터페이스 매개변수 구성

필요한 경우 특정 인터페이스별 OSPFv3 매개변수를 변경할 수 있습니다. 이러한 매개변수는 변경할 필요가 없지만, **ipv6 ospf hello-interval** and **ipv6 ospf dead-interval** 같은 인터페이스 매개변수는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 구성할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

IPv6에 대한 OSPFv3 인터페이스 매개변수를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: ciscoasa(config-if)# ipv6 router ospf 10	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *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.
2단계	**ipv6 ospf area** [*area-num*] [**instance**] 예: 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	OSPFv3 영역을 생성합니다. *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.
3단계	OSPFv3 인터페이스 매개변수를 구성하려면 다음 작업 중 하나를 수행합니다.	

명령	목적
ipv6 ospf cost *interface-cost* 예: 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	인터페이스에서 패킷을 전송하는 비용을 명시적으로 지정합니다. *interface-cost* 인수는 링크 상태 메트릭으로 표시되는 무부호 정수 값을 지정하며, 입력 가능한 값의 범위는 1~65535입니다. 기본 비용은 대역폭을 기준으로 합니다.
ipv6 ospf database-filter all out 예: 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	OSPFv3 인터페이스에 발신되는 LSA를 필터링합니다. 기본적으로 모든 발신 LSA는 인터페이스에 플러딩됩니다.
ipv6 ospf dead-interval *seconds* 예: 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	인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간을 초 단위로 설정합니다. 이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 **ipv6 ospf hello-interval** 명령으로 설정된 간격 집합의 4배입니다.

명령	목적
ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**} 예: 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	인터페이스의 암호화 유형을 지정합니다. **ipsec** 키워드는 IP 보안 프로토콜을 지정합니다. **spi** *spi* 키워드 인수 쌍은 보안 정책 색인을 지정하며, 이 값의 범위는 256~42949667295 중에서 선택해야 하고 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. **참고** 인터페이스에서 OSPFv3 암호화가 활성화되어 있고 인접 디바이스가 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.
ipv6 ospf flood-reduction 예: 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	인터페이스에 대한 LSA의 플러딩 감소를 지정합니다.

명령	목적
ipv6 ospf hello-interval *seconds* 예: 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	인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. 이 값은 특정 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다. 기본 간격은 이더넷 인터페이스의 경우 10초이고, 비 브로드캐스트 인터페이스의 경우 30초입니다.
ipv6 ospf mtu-ignore 예: 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	DBD 패킷이 수신될 때 OSPF MTU 불일치 감지를 비활성화합니다. OSPF MTU 불일치 감지는 기본적으로 활성화되어 있습니다.
ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**} 예: 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	OSPF 네트워크 유형을 기본값 이외의 유형으로 설정하며, 이 경우 네트워크 유형에 따라 달라집니다. **point-to-point non-broadcast** 키워드는 네트워크 유형을 포인트-투-포인트 비 브로드캐스트로 설정합니다. **broadcast** 키워드는 네트워크 유형을 브로드캐스트로 설정합니다.

명령	목적
ipv6 ospf priority *number-value* 예: 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	네트워크의 전용 라우터를 결정하는 데 도움이 되는 라우터 우선순위를 설정합니다. 유효한 값의 범위는 0~255입니다.
ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] 예: 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	비 브로드캐스트 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성합니다.

명령	목적
ipv6 ospf retransmit-interval *seconds* 예: 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	인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 5초입니다.
ipv6 ospf transmit-delay *seconds* 예: 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	인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 설정합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 1초입니다.

OSPFv3 라우터 매개변수 구성

IPv6에 대한 OSPFv3 라우터 인터페이스 매개변수를 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: ciscoasa(config)# ipv6 router ospf 10	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	선택적인 OSPFv3 라우터 인터페이스 매개변수를 구성하려면 다음 작업 중 하나를 수행합니다.	

명령	목적
`area` 예: `ciscoasa(config-rtr)# area 10`	OSPFv3 영역 매개변수를 구성합니다. 지원되는 매개변수에는 십진수 숫자(0~4294967295)로 된 영역 ID 및 IP 주소 형식(**A.B.C.D**)으로 된 영역 ID가 포함됩니다.
default 예: `ciscoasa(config-rtr)# default originate`	명령을 기본값으로 설정합니다. **originate** 매개변수는 기본 경로를 재배포합니다.
default-information 예: `ciscoasa(config-rtr)# default-information`	기본 정보의 재배포를 제어합니다.
distance 예: `ciscoasa(config-rtr)# distance 200`	경로 유형을 기준으로 OSPFv3 경로 관리 영역을 정의합니다. 지원되는 매개변수에는 관리 영역 값(1~254) 및 OSPFv3 영역에 대한 **ospf**가 포함됩니다.
`exit` 예: `ciscoasa(config-rtr)# exit`	IPv6 라우터 컨피그레이션 모드를 종료합니다.
ignore 예: `ciscoasa(config-rtr)# ignore lsa`	라우터에 Type 6 Multicast OSPF(MOSPF)에 대한 링크 상태 광고(LSA)가 수신될 경우, **lsa** 매개변수를 사용하여 syslog 시지가 전송되는 것을 억제합니다.
log-adjacency-changes 예: `ciscoasa(config-rtr)#` `log-adjacency-changes detail`	OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다. **detail** 매개변수를 사용하면 모든 상태 변경 사항이 기록됩니다.
passive-interface [*interface_name*] 예: `ciscoasa(config-rtr)# passive-interface` `inside`	인터페이스에서 라우팅 업데이트를 전송하고 수신하는 작업을 억제합니다. *interface_name* 인수는 OSPFv3 프로세스가 실행 중인 인터페이스의 이름을 지정합니다.
redistribute 예: `ciscoasa(config-rtr)# redistribute ospf`	다음 매개변수에 따라 하나의 라우팅 도메인에서 다른 도메인으로 경로를 재배포하도록 구성합니다. • **connected** — 연결된 경로를 지정합니다. • **ospf** — OSPFv3 경로를 지정합니다. • **static** — 고정 경로를 지정합니다.

명령	목적
router-id 예: `ciscoasa(config-rtr)# router-id 10.1.1.1`	다음 매개변수를 사용하여 지정된 프로세스에 대한 고정된 라우터 ID를 생성합니다. • **A.B.C.D** — OSPF 라우터 ID를 IP 주소 형식으로 지정합니다. • **cluster-pool** — Individual Interface 클러스터링이 구성될 때 IP 주소 풀을 구성합니다. 클러스터링에 사용되는 IP 주소 풀에 대한 자세한 내용은 22-16 페이지의 클러스터링 (OSPFv2 및 OSPFv3)에 대한 IP 주소 풀 구성을 참조하십시오.
summary-prefix 예: `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`	IPv6 주소 요약을 0~128 사이의 유효한 값으로 구성합니다. **X:X:X:X::X/** 매개변수는 IPv6 접두사를 지정합니다.
timers 예: `ciscoasa(config)# ipv6 router ospf 10` `ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000`	라우팅 타이머를 조정합니다. 라우팅 타이머 매개변수는 다음과 같습니다. • **lsa** — OSPFv3 LSA 타이머를 지정합니다. • **pacing** — OSPFv3 속도 타이머를 지정합니다. • **throttle** — OSPFv3 속도 제한 타이머를 지정합니다.

OSPFv3 영역 매개변수 구성

OSPFv3 영역 매개변수를 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	`Do one of the following to configure optional OSPFv3 area parameters:`	
	area *area-id* **default-cost** *cost* 예: `ciscoasa(config-rtr)# area 1 default-cost nssa`	NSSA 영역 또는 스텁 영역의 요약 기본 비용을 설정합니다.

명령	목적
area *area-id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*] 예: `ciscoasa(config-rtr)# area 1 range FE01:1::1/64`	경계선 라우터 전용 주소 및 마스크와 일치하는 경로를 요약합니다. *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.
area *area-id* **nssa** 예: `ciscoasa(config-rtr)# area 1 nssa`	NSSA 영역을 지정합니다.
area *area-id* **stub** 예: `ciscoasa(config-rtr)# area 1 stub`	스텁 영역을 지정합니다.

명령	목적
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*] 예: `ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5`	가상 링크 및 매개변수를 정의합니다. *area-id* 인수는 경로를 요약할 영역을 지정합니다. **virtual link** 키워드는 가상 링크 인접 디바이스의 생성을 지정합니다. *router-id* 인수는 가상 링크 인접 디바이스와 연결된 라우터 ID를 지정합니다. 라우터 ID를 표시하려면 **show ospf** 또는 **show ipv6 ospf** 명령을 입력합니다. 기본값이 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 인접 디바이스에서 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 패시브 인터페이스

OSPFv3 패시브 인터페이스를 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**ipv6 router ospf** *process_id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**passive-interface** [*interface_name*] 예: `ciscoasa(config-rtr)# passive-interface inside`	인터페이스에서 라우팅 업데이트를 전송하고 수신하는 작업을 억제합니다. *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

IPv6 경로에 대한 OSPFv3 관리 영역을 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process_id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**distance** [**ospf** {**external** | **inter-area** | **intra-area**}] *distance* 예: `ciscoasa(config-rtr)# distance ospf external 200`	OSPFv3 경로에 대한 관리 영역을 설정합니다. **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. **intra-area** 키워드는 OSPFv3에 대한 영역 내 경로를 지정합니다. *distance* 인수는 관리 영역을 지정하며, 이 값은 10~254 사이의 정수입니다.

OSPFv3 타이머 구성

OSPFv3에 대한 LSA 도착, LSA 속도 및 속도 제한 타이머를 설정할 수 있습니다.

ASA에서 OSPFv3 인접 디바이스의 동일한 LSA를 수락하는 최소 간격을 설정하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id*	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다.
	예: `ciscoasa(config-if)# ipv6 router ospf 1`	*process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**timers lsa arrival** *milliseconds*	ASA에서 OSPF 인접 디바이스의 동일한 LSA를 수락하는 최소 간격을 설정합니다.
	예: `ciscoasa (config rtr) # 타이머 lsa 도착 2000`	*milliseconds* 인수는 인접 디바이스에서 도착하는 동일한 LSA를 수락하는 동안 소요될 수밖에 없는 최소 지연 시간을 밀리초 단위로 지정합니다. 범위는 0에서 6,000,000밀리초입니다. 기본값은 1000밀리초입니다.

LSA 플러딩 패킷 속도를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id*	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다.
	예: `ciscoasa(config-if)# ipv6 router ospf 1`	*process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**timers pacing flood** *milliseconds*	LSA 플러딩 패킷 속도를 구성합니다.
	예: `ciscoasa(config-rtr)# timers lsa flood 20`	*milliseconds* 인수는 업데이트 중 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5~100밀리초입니다. 기본값은 33밀리초입니다.

OSPFv3 LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 변경하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id*	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다.
	예: `ciscoasa(config-if)# ipv6 router ospf 1`	*process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**timers pacing lsa-group** *seconds*	OSPFv3 LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 변경합니다.
	예: `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 10~1800초입니다. 기본값은 240초입니다.

LSA 재전송 패킷 속도를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id*	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다.
	예: `ciscoasa(config-if)# ipv6 router ospf 1`	*process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**timers pacing retransmission** *milliseconds*	LSA 재전송 패킷 속도를 구성합니다.
	예: `ciscoasa(config-rtr)# timers pacing retransmission 100`	*milliseconds* 인수는 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5~200밀리초입니다. 기본값은 66밀리초입니다.

LSA 및 SPF 속도 제한 기능에서는 밀리초 단위의 LSA 속도 제한을 제공하여 네트워크가 불안정한 시간 동안 OSPFv3 LSA 업데이트 속도를 줄이고, OSPFv3 통합 시간을 단축할 수 있는 동적 메커니즘을 제공합니다.

LSA 및 SPF 속도 제한 타이머를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	다음 옵션 중 하나를 선택합니다.	
	timers throttle lsa *milliseconds1 milliseconds2 milliseconds3* 예: `ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000`	OSPFv3 LSA 속도 제한을 구성합니다. *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 속도 제한의 경우, 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3에서 첫 번째 어커런스 값을 자동으로 수정합니다. 이와 마찬가지로, 최대 지연 값이 최소 지연 값보다 작게 지정될 경우 OSPFv3에서 최소 지연 값을 자동으로 수정합니다. LSA 속도 제한의 기본값은 다음과 같습니다. • *milliseconds1*의 경우 기본값은 0밀리초입니다. • *milliseconds2* 및 *milliseconds3*의 경우 기본값은 5000밀리초입니다.

명령	목적
timers throttle spf *milliseconds1 milliseconds2 milliseconds3* **예:** `ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000`	OSPFv3 SPF 속도 제한을 구성합니다. *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 속도 제한의 경우, *milliseconds2* 또는 *milliseconds3*이 *milliseconds1*보다 작으면 OSPFv3에서 *milliseconds1* 값을 자동으로 수정합니다. 이와 마찬가지로, *milliseconds3*이 *milliseconds2*보다 작을 경우 OSPFv3에서 *milliseconds2* 값을 자동으로 수정합니다. SPF 속도 제한의 기본값은 다음과 같습니다. • *milliseconds1*의 경우 기본값은 5000밀리초입니다. • *milliseconds2* 및 *milliseconds3*의 경우 기본값은 10000밀리초입니다.

고정 OSPFv3 인접 디바이스 정의

고정 OSPFv3 인접 디바이스를 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 인접 디바이스에 대한 고정 경로를 생성해야 합니다. 고정 경로 생성에 대한 자세한 내용은 19 장, "고정 경로 및 기본 경로"를 참조하십시오.

고정 OSPFv3 인접 디바이스를 정의하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* **예:** `ciscoasa(config)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **예:** `ciscoasa(config-if)# interface ethernet0/0` `ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	비 브로드캐스트 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성합니다.

OSPFv3 기본 매개변수 초기화

OSPFv3 매개변수를 기본값으로 되돌리려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**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**] 예: `ciscoasa(config-rtr)# default metric 5`	선택적 매개변수를 기본값으로 되돌립니다. **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 재배포합니다. **router-id** 키워드는 지정된 라우팅 프로세스에 대한 라우터 ID를 지정합니다. **summary-prefix** 키워드는 IPv6 요약 접두사를 지정합니다. **timers** 키워드는 OSPFv3 타이머를 지정합니다.

Syslog 메시지 전송

OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**log-adjacency-changes** [**detail**] 예: `ciscoasa(config-rtr)# log-adjacency-changes detail`	OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다. **detail** 키워드는 OSPFv3 인접 디바이스가 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.

세부 단계

	명령	목적
1단계	**router ospf** *process_id* 예: `ciscoasa(config-if)# router ospf 1`	OSPFv2 라우팅 프로세스를 활성화하고 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**ignore lsa mospf** 예: `ciscoasa(config-rtr)# ignore lsa mospf`	지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷이 경로에 전송될 경우 syslog 메시지가 전송되는 것을 억제합니다.

요약 경로 비용 계산

RFC 1583에 따라 요약 경로 비용을 계산하려면 다음 명령을 입력합니다.

명령	목적
compatible rfc1583 예: `ciscoasa (config-rtr)# compatible rfc1583`	RFC 1583에 따라 요약 경로 비용을 계산하는 데 사용된 방법을 복원합니다.

OSPFv3 라우팅 도메인에 기본 외부 경로 생성

OSPFv3 라우팅 도메인에 기본 경로를 생성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**default-information originate** [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*] 예: `ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2`	OSPFv3 라우팅 도메인에 기본 외부 경로를 생성합니다. **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 접두사 구성

IPv6 요약 접두사를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.
2단계	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*] 예: `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`	IPv6 요약 접두사를 구성합니다. *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 재배포를 제어하기 위한 일치 값으로 사용할 수 있는 태그 값을 지정합니다. 이 키워드는 OSPFv3에만 적용됩니다.

IPv6 경로 재배포

연결된 경로를 OSPFv3 프로세스에 재배포하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ipv6 router ospf** *process-id* 예: `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다. *process-id* 인수는 이 라우팅 프로세스에 내부적으로 사용되는 식별자이며 로컬로 할당됩니다. 입력 가능한 값은 1~65535 사이의 양수입니다. 이 ID는 다른 디바이스의 ID와 일치하지 않아도 되며, 내부 관리자용으로만 사용됩니다. 최대 2개의 프로세스를 사용할 수 있습니다.

	명령	목적
2단계	**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*] 예: ciscoasa(config-rtr)# redistribute connected 5 type-1	하나의 OSPFv3 프로세스에서 다른 프로세스로 IPv6 경로를 재배포합니다. *source-protocol* 인수는 경로가 재배포되는 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 재배포할 수 있습니다. **level-1** 키워드는 Intermediate System-to-Intermediate System(IS-IS)의 경우, Level 1 경로가 다른 IP 라우팅 프로토콜에 개별적으로 재배포되도록 지정합니다. **level-1-2** 키워드는 IS-IS의 경우, Level 1 및 Level 2 경로가 모두 다른 IP 라우팅 프로토콜에 재배포되도록 지정합니다. **level-2** 키워드는 IS-IS의 경우, Level 2 경로가 다른 IP 라우팅 프로토콜에 개별적으로 재배포되도록 지정합니다. **metric** *metric-value* 키워드 인수 쌍의 경우, 하나의 OSPFv3 프로세스에서 동일한 라우터의 다른 OSPFv3 프로세스로 경로를 재배포할 때 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPFv3 프로세스에 다른 프로세스를 재배포할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다. **metric transparent** 키워드는 RIP가 재배포된 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 재배포하며 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. 아무 것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값의 범위는 0~4294967295입니다. **route-map** 키워드는 경로 맵을 지정하여 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜까지 경로 가져오기의 필터링을 확인합니다. 이 키워드를 지정하지 않으면 모든 경로가 재배포됩니다. 이 키워드를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. *map-tag* 인수는 구성된 경로 맵을 식별합니다.

Graceful Restart 구성

ASA에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(무중단 전달) 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 OSPFv2 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 인접 디바이스에 나타낼 수 있으며, NSF 인식 디바이스는 인접 디바이스를 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 RS비트 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.

명령	목적
router ospf *process_id* **예:** `ciscoasa(config)# router ospf 2`	OSPF 라우팅 프로세스를 생성하고 재배포하려는 OSPF 프로세스의 라우터 컨피그레이션 모드로 들어갑니다. *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.
capability {**lls**|**opaque**} **예:** `ciscoasa(config-router)# capability lls`	LLS 데이터 블록 또는 불투명 LSA를 사용하여 NSF를 활성화합니다. **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 Graceful Restart 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.

OSPFv2에 Cisco NSF Graceful Restart 구성

OSPFv2, NSF 지원 디바이스 또는 NSF 인식 디바이스에 Cisco NSF Graceful Restart를 구성하려면 다음 명령을 입력합니다.

명령	목적
nsf cisco [**enforce global**] 예: `ciscoasa(config-router)# nsf cisco`	NSF 지원 디바이스에서 Cisco NSF 활성화 **enforce global** 키워드는 비 NSF 인식 인접 디바이스 디바이스가 감지될 경우 NSF 재시작을 취소합니다.
capability {**lls**|**opaque**} 예: `ciscoasa(config-router)# capability lls`	(선택 사항) NSF 인식 디바이스에서 Cisco NSF 헬퍼 모드를 활성화합니다. 이 명령은 기본적으로 활성화되어 있습니다. 이 명령을 no 형식으로 사용하면 명령이 비활성화됩니다.

OSPFv2에 IETF NSF Graceful Restart 구성

OSPFv2, NSF 지원 디바이스 또는 NSF 인식 디바이스에 IETF NSF Graceful Restart를 구성하려면 다음 명령을 입력합니다.

명령	목적
nsf ietf [**restart interval** *seconds*] 예: `ciscoasa(config-router)# nsf ietf restart interval 80`	NSF 지원 디바이스에서 IETF NSF 활성화 (선택 사항) **restart interval** *seconds*는 Graceful Restart의 길이를 초 단위로 지정합니다. 유효한 값의 범위는 1~1800초입니다. 기본값은 120초입니다. **참고** 인접성이 가동되는 데 소요된 시간보다 재시작 간격이 작게 구성될 경우 Graceful Restart가 종료될 수 있습니다. 예를 들어, 30초 미만의 재시작 간격은 지원되지 않습니다.
nsf ietf helper [**strict-lsa-checking**] 예: `ciscoasa(config-router)# nsf ietf helper`	(선택 사항) NSF 인식 디바이스에서 IETF NSF 헬퍼 모드를 활성화합니다. (선택 사항) **strict-LSA-checking** 키워드는 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다. **참고** 이 명령은 기본적으로 활성화되어 있습니다. 이 명령을 no 형식으로 사용하면 명령이 비활성화됩니다.

OSPFv3에 Graceful Restart 구성

OSPFv3에 NSF Graceful Restart 기능을 구성하려면 디바이스를 NSF 지원 디바이스로 구성하고, 디바이스를 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. OSPFv3에 Graceful Restart를 구성하려면 다음 명령을 입력합니다.

명령	목적
interface *physical_interface* **ipv6 enable** 예: ciscoasa(config)# interface ethernet 0/0 ciscoasa(config-if)# ipv6 enable	명시적인 IPv6 주소로 구성되지 않은 인터페이스에서 IPv6 처리를 활성화합니다. *physical_interface* 인수는 OSPFv3 NSF에 참여하는 인터페이스를 나타냅니다.
graceful-restart [**restart interval** *seconds*] 예: ciscoasa(config-router)# graceful-restart restart interval 80	NSF 지원 디바이스에서 OSPFv3에 Graceful-Restart를 활성화합니다. (선택 사항) **restart interval** *seconds*는 Graceful Restart의 길이를 초 단위로 지정합니다. 유효한 값의 범위는 1~1800초입니다. 기본값은 120초입니다. **참고** 인접성이 가동되는 데 소요된 시간보다 재시작 간격이 작게 구성될 경우 Graceful Restart가 종료될 수 있습니다. 예를 들어, 30초 미만의 재시작 간격은 지원되지 않습니다.
graceful-restart helper [**strict-lsa-checking**] 예: ciscoasa(config-router)# graceful-restart helper strict-lsa-checking	NSF 인식 디바이스에서 OSPFv3에 Graceful-Restart를 활성화합니다. (선택 사항) **strict-LSA-checking** 키워드는 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다. **참고** Graceful-Restart 헬퍼 모드는 기본적으로 활성화되어 있습니다.

OSPF 컨피그레이션 제거

기존에 활성화한 전체 OSPFv2 컨피그레이션을 제거하려면, 다음 명령을 입력합니다.

명령	목적
clear configure router ospf *pid* 예: ciscoasa(config)# clear configure router ospf 1000	활성화한 전체 OSPFv2 컨피그레이션을 제거합니다. 컨피그레이션을 지운 후에는 **router ospf** 명령을 사용하여 OSPF를 다시 구성해야 합니다.

기존에 활성화한 전체 OSPFv3 컨피그레이션을 제거하려면, 다음 명령을 입력합니다.

명령	목적
clear configure ipv6 router ospf *process-id* 예: ciscoasa(config)# clear configure ipv6 router ospf 1000	활성화한 전체 OSPFv3 컨피그레이션을 제거합니다. 컨피그레이션을 지운 후에는 **ipv6 router ospf** 명령을 사용하여 OSPFv3를 다시 구성해야 합니다.

OSPFv2의 컨피그레이션 예

다음 예에는 다양한 선택적 프로세스로 OSPFv2를 활성화하고 구성하는 방법이 나와 있습니다.

1단계 OSPFv2를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2단계 (선택 사항) 하나의 OSPFv2 프로세스에서 다른 OSPFv2 프로세스로 경로를 재배포하려면 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
```

3단계 (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
```

4단계 (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
```

5단계 (선택 사항) 경로 계산 타이머를 구성하고 인접 디바이스 동작 및 중단 메시지 로그를 표시하려면 다음 명령을 입력합니다.

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6단계 (선택 사항) 현재 OSPFv2 컨피그레이션 설정을 표시하려면 **show ospf** 명령을 입력합니다.

다음은 **show ospf** 명령의 샘플 출력 결과입니다.

```
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
```

7단계 OSPFv2 컨피그레이션을 지우려면 다음 명령을 입력합니다.

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 컨피그레이션의 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 출력 결과입니다.

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

다음은 **show running-config interface** 명령의 샘플 출력 결과입니다.

```
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
12345678901234567890123456789012
```

```
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.

명령	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.

명령	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 인접 디바이스에 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 인접 디바이스에서 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 인접 디바이스 정보가 표시됩니다.
show ospf request-list *neighbor if_name*	라우터에서 요청한 모든 LSA 목록이 표시됩니다.
show ospf retransmission-list *neighbor if_name*	재전송을 위해 대기 중인 모든 LSA 목록이 표시됩니다.
show ospf [*process-id*] **summary-address**	OSPFv2 프로세스에 따라 구성된 모든 요약 주소 재배포 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.

명령	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.

명령	목적
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 인접 디바이스에 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 인접 디바이스에서 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 인접 디바이스 정보가 표시됩니다.
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*]	재전송을 위해 대기 중인 모든 LSA 목록이 표시됩니다.
show ipv6 ospf statistic [*process-id*] [**detail**]	다양한 OSPFv3 통계가 표시됩니다.

명령	목적
show ipv6 ospf [*process-id*] **summary-prefix**	OSPFv3 프로세스에 따라 구성된 모든 요약 주소 재배포 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.

추가 참조 자료

RFC

RFC	제목
2328	OSPFv2
4552	OSPFv3 Authentication
5340	OSPF for IPv6

OSPF의 기능 기록

표 22-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 22-1 OSPF의 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 재배포 및 모니터링에 대한 지원이 추가되었습니다. 도입된 명령: **route ospf**

표 22-1 OSPF의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
다중 컨텍스트 모드의 동적 라우팅	9.0(1)	다중 컨텍스트 모드에서 OSPFv2 라우팅이 지원됩니다.
클러스터링		클러스터링 환경에서 OSPFv2 및 OSPFv3에 대해 벌크 동기화, 경로 동기화, Spanned EtherChannel 로드 밸런싱이 지원됩니다. 도입되거나 수정된 명령: **show route cluster**, **show ipv6 route cluster**, **debug route cluster, router-id cluster-pool**
IPv6에 OSPFv3 지원		IPv6에 OSPFv3 라우팅이 지원됩니다. 도입되거나 수정된 명령: **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**

표 22-1 OSPF의 기능 기록(계속)

기능 이름	플랫폼 릴리스	기능 정보
OSPF Support for Fast Hellos	9.2(1)	OSPF Supports the Fast Hello Packets 기능을 컨피그레이션에 사용하면 OSPF 네트워크에서 통합 속도를 단축할 수 있습니다. 수정된 명령: **ospf dead-interval**
타이머		새 OSPF 타이머가 추가되었으며, 기존 타이머는 사용이 중단되었습니다. 도입된 명령: **timers lsa arrival**, **timers pacing**, **timers throttle** 제거된 명령: **Timers spf**, **timers lsa-grouping-pacing**
액세스 목록을 사용한 경로 필터링		이제 ACL을 사용한 경로 필터링이 지원됩니다. 도입된 명령: **distribute-list**
OSPF 모니터링 개선 사항		추가적인 OSPF 모니터링 정보가 추가되었습니다. 수정된 명령: **show ospf events**, **show ospf rib**, **show ospf statistics**, **show ospf border-routers [detail]**, **show ospf interface brief**
OSPF 재배포 BGP		OSPF 재배포 기능이 추가되었습니다. 추가된 명령: **redistribute bgp**
NSF를 위한 OSPF 지원	9.3(1)	NSF를 위한 OSPFv2 및 OSPFv3 지원을 추가했습니다. 추가된 명령: **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**

23 장

EIGRP

이 장에서는 EIGRP(Enhanced Interior Gateway Routing Protocol)를 이용하여 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 Cisco ASA를 구성하는 방법을 설명합니다.

EIGRP 정보

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 인접 라우팅 테이블을 저장하여 다른 경로에 빠르게 적응할 수 있습니다. 적절한 경로가 존재하지 않는 경우 EIGRP는 인접 디바이스를 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 부부적인 업데이트를 전송합니다. 부분 업데이트 전파가 자동으로 바운딩되므로 정보가 필요한 라우터만 업데이트됩니다. 이 두 기능 덕분에 EIGRP는 IGRP보다 훨씬 적은 대역폭을 사용합니다.

인접 디바이스 탐색은 ASA가 직접 연결된 네트워크의 다른 라우터를 동적으로 학습하기 위해 사용하는 프로세스입니다. EIGRP 라우터는 멀티캐스트 hello 패킷을 전송하여 네트워크에서 존재를 알립니다. ASA가 새로운 인접 디바이스에서 hello 패킷을 수신하면 초기화 비트 세트와 함께 토폴로지 테이블을 인접 디바이스로 보냅니다. 초기화 비트 세트와 함께 토폴로지 업데이트를 수신한 인접 디바이스는 토폴로지 테이블을 다시 ASA로 전달합니다.

hello 패킷은 멀티캐스트 메시지로 전달됩니다. hello 메시지에는 응답할 필요가 없습니다. 고정으로 정의된 인접 디바이스의 경우 예외입니다. **neighbor** 명령을 사용하거나 ASDM에서 hello 간격을 구성하여 인접 디바이스를 구성할 경우 인접 디바이스로 전송되는 hello 메시지는 유니캐스트 메시지로 전송됩니다. 라우팅 업데이트 및 확인은 유니캐스트 메시지로 전송됩니다.

이 인접 관계가 설정되면 네트워크 토폴로지의 변화가 없는 한 라우팅 업데이트가 교환되지 않습니다. 인접 관계는 hello 패킷을 통해 유지됩니다. 인접 디바이스에서 수신된 각 hello 패킷은 보류 시간을 포함합니다. 이 시간은 ASA가 해당 인접 디바이스로부터 hello 패킷을 수신할 것으로 예상되는 시간입니다. ASA가 해당 인접 디바이스가 알린 보류 시간 내에 인접 디바이스로부터 hello 패킷을 수신하지 않으면 ASA는 해당 인접 디바이스를 사용할 수 없는 것으로 간주합니다.

EIGRP 프로토콜은 경로 연산에 중요한 인접 디바이스 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 인접 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 인접 디바이스에 경로를 쿼리하면 EIGRP 인접 디바이스가 다시 자신의 인접 디바이스에 쿼리합니다. 경로에 대한 가능한 successor가 없는 라우터는 도달할 수 없음 메시지를 반환합니다.

경로 재계산 중 DUAL은 경로를 활성으로 표시합니다. 기본적으로 ASA는 인접 디바이스로부터 응답을 수신하기 위해 3분을 대기합니다. ASA가 인접 디바이스로부터 응답을 수신하지 않는 경우 경로가 stuck-in-active로 표시됩니다. 가능한 successor로서 응답이 없는 인접 디바이스를 가리키는 토폴로지 테이블의 모든 경로는 제거됩니다.

참고 EIGRP 인접 관계는 GRE 터널 없이 IPsec 터널을 통해 지원되지 않습니다.

클러스터 사용

EIGRP과 클러스터링 사용에 관한 정보는 18-9 페이지의 동적 라우팅 및 클러스터링에서 참조하십시오.

EIGRP 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

장애 조치 지침

단일 및 다중 컨텍스트 모드에서 상태 기반 장애 조치를 지원합니다.

IPv6 지침

IPv6를 지원하지 않습니다.

클러스터링 지침

- EIGRP 및 OSPFv2를 모두 사용하도록 구성된 경우 Spanned EtherChannel 및 Individual Interface 클러스터링을 지원합니다.
- Individual Interface 클러스터 설정에서 EIGRP 인접성은 마스터 유닛의 공유 인터페이스에 있는 두 컨텍스트 사이에서만 설정할 수 있습니다. 각 클러스터 노드에 대응하는 여러 인접 구문을 별도로 구성하여 이 문제를 해결할 수 있습니다.

추가 지침

- EIGRP 인스턴스는 멀티캐스트 트래픽의 컨텍스트 간 교환이 지원되지 않기 때문에 공유 인터페이스에서 서로 인접 관계를 형성할 수 없습니다.
- 최대 하나의 EIGRP 프로세스가 지원됩니다.

EIGRP 구성

이 섹션에서는 시스템에서 EIGRP 프로세스를 활성화하는 방법을 설명합니다. EIGRP를 활성화한 후에는 다음 섹션을 참조하여 시스템에서 EIGRP 프로세스를 사용자 정의하는 방법을 알아보십시오.

- 23-4 페이지의 EIGRP 활성화
- 23-4 페이지의 EIGRP Stub 라우팅 활성화

EIGRP 활성화

ASA에서 하나의 EIGRP 라우팅 프로세스만 활성화할 수 있습니다.

EIGRP를 활성화하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* **예:** `ciscoasa(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**network** *ip-addr* [*mask*] **예:** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-6 페이지의 EIGRP를 위한 인터페이스 구성을 참조하십시오.

EIGRP Stub 라우팅 활성화

ASA를 EIGRP stub 라우터로 활성화하고 구성할 수 있습니다. Stub 라우팅은 ASA에 대한 메모리 및 처리 능력 요구 사항을 낮춥니다. stub 라우터로서 ASA은(는) 모든 로컬이 아닌 트래픽을 배포 라우터로 전달하기 때문에 전체 EIGRP 라우팅 테이블을 유지할 필요가 없습니다. 일반적으로 배포 라우터는 기본 경로 외에 아무 것도 stub 라우터로 보낼 필요가 없습니다.

지정된 경로만 stub 라우터에서 배포 라우터로 전파됩니다. stub 라우터로서 ASA는 요약, 연결된 경로, 재배포된 고정 경로, 외부 경로 및 "inaccessible" 메시지를 포함한 내부 경로에 대한 모든 쿼리에 응답합니다. ASA가 stub으로 구성된 경우 특수 피어 정보 패킷을 모든 인접 디바이스 라우터로 보내 그 상태를 stub 라우터에 보고합니다. stub 상태를 알려주는 패킷 정보를 수신하는 모든 인접 디바이스는 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.

ASA를 EIGRP stub 라우팅 프로세스로 활성화하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* 예: ciscoasa(config)# router eigrp *2*	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**network** *ip-addr* [*mask*] 예: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-8 페이지의 패시브 인터페이스 구성 섹션을 참조하십시오.
3단계	**eigrp stub** {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]} 예: 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 프로세스를 구성합니다. stub 라우팅 프로세스가 어떤 네트워크를 배포 라우터로 알릴지 지정해야 합니다. 고정 네트워크 및 연결 네트워크는 stub 라우팅 프로세스로 자동 재배포되지 않습니다.

참고 stub 라우팅 프로세스는 전체 토폴로지 테이블을 유지하지 않습니다. stub 라우팅은 최소한 라우팅 결정을 내리는 배포 라우터로의 기본 경로를 필요로 합니다.

EIGRP 사용자 정의

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.

네트워크를 추가하거나 정의하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* 예: `ciscoasa(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**network** *ip-addr* [*mask*] 예: `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-8 페이지의 패시브 인터페이스 구성을 참조하십시오.

EIGRP를 위한 인터페이스 구성

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 인터페이스가 연결된 네트워크를 포함하는a **network** 명령을 구성하고 **passive-interface** 명령을 사용하여 인터페이스가 EIGRP 업데이트를 보내거나 받지 않도록 할 수 있습니다.

EIGRP에 대한 인터페이스를 구성하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* **예:** `ciscoasa(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*] **예:** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-6 페이지의 EIGRP 라우팅 프로세스를 위한 네트워크 정의를 참조하십시오.
3단계	(선택 사항) 다음 중 하나를 수행하여 EIGRP 라우팅에 참여할 인터페이스를 사용자 지정합니다.	
	no default-information {**in** | **out** | **WORD**} **예:** `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}`	후보 기본 경로 정보의 송수신을 제어할 수 있습니다. **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. 이 특정 옵션에 대한 자세한 정보는 23-15 페이지의 EIGRP에서 기본 정보 구성에서 참조하십시오.
	authentication mode eigrp *as-num* **md5** **예:** `ciscoasa(config)# authentication mode eigrp 2 md5`	EIGRP 패킷의 MD5 인증을 활성화합니다. *as-num* 인수는 ASA에 구성된 EIGRP 라우팅 프로세스의 자율 시스템 개수입니다. EIGRP가 활성화되지 않았거나 잘못된 번호를 입력한 경우 ASA이(가) 다음 오류 메시지를 반환합니다. `% Asystem(100) specified does not exist` 이 특정 옵션에 대한 자세한 정보는 23-10 페이지의 인터페이스에서 EIGRP 인증 활성화에서 참조하십시오.
	delay *value* **예:** `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. 이 특정 옵션에 대한 자세한 정보는 23-9 페이지의 인터페이스 지연 값 변경에서 참조하십시오.

명령	목적
hello-interval eigrp *as-num seconds* 예: `ciscoasa(config)# hello-interval eigrp 2 60`	hello 간격을 변경할 수 있습니다. 이 특정 옵션에 대한 자세한 정보는 23-14 페이지의 EIGRP hello 간격 및 보류 시간 사용자 정의에서 참조하십시오.
hold-time eigrp *as-num seconds* 예: `ciscoasa(config)# hold-time eigrp 2 60`	보류 시간을 변경할 수 있습니다. 이 특정 옵션에 대한 자세한 정보는 23-14 페이지의 EIGRP hello 간격 및 보류 시간 사용자 정의에서 참조하십시오.

패시브 인터페이스 구성

하나 이상의 인터페이스를 패시브 인터페이스로 구성할 수 있습니다. EIGRP에서 패시브 인터페이스는 라우팅 업데이트를 보내거나 받지 않습니다.

패시브 인터페이스를 구성하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* 예: `ciscoasa(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*] 예: `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-6 페이지의 EIGRP 라우팅 프로세스를 위한 네트워크 정의를 참조하십시오.
3단계	**passive-interface** {**default** | *if-name*} 예: `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0` `ciscoasa(config-router)# passive-interface {default}`	인터페이스가 EIGRP 라우팅 메시지를 보내거나 받지 못하게 합니다. **default** 키워드를 사용하면 모든 인터페이스의 EIGRP 라우팅 업데이트가 비활성화됩니다. **nameif** 명령이 지정한 대로 인터페이스 이름을 지정하면 지정된 인터페이스에서 EIGRP 라우팅 업데이트가 비활성화됩니다. EIGRP 라우터 컨피그레이션에서 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.

요약 주소를 생성하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**interface** *phy_if* 예: `ciscoasa(config)# interface inside`	EIGRP에서 사용하는 지연 값을 변경하는 인터페이스에 대한 인터페이스 컨피그레이션 모드에 진입합니다.
2단계	**summary-address eigrp** *as-num address mask* [*distance*] 예: `ciscoasa(config-if)# summary-address eigrp 2 address mask [20]`	요약 주소를 생성합니다. 기본적으로 EIGRP 요약 주소를 정의하면 관리 거리는 5입니다. 이 값은 선택적인 *distance* 인수를 **summary-address** 명령에서 지정함으로써 바꿀 수 있습니다.

인터페이스 지연 값 변경

인터페이스 지연 값은 EIGRP 거리 계산에 사용됩니다. 인터페이스별로 이 값을 수정할 수 있습니다.

인터페이스 지연 값을 변경하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**interface** *phy_if* 예: `ciscoasa(config)# interface inside`	EIGRP에서 사용하는 지연 값을 변경하는 인터페이스에 대한 인터페이스 컨피그레이션 모드에 진입합니다.
2단계	**delay** *value* 예: `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.

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 인증을 구성된 인터페이스의 모든 EIGRP 인접 디바이스는 인접성을 위한 동일한 인증 모드와 키로 구성되어야 설정 가능합니다.

참고 EIGRP 경로 인증을 활성화하기 전에 EIGRP를 활성화해야 합니다.

인터페이스에서 EIGRP 인증을 활성화하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* **예:** `hostname(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**network** *ip-addr* [*mask*] **예:** `hostname(config)# router eigrp 2` `hostname(config-router)# network 10.0.0.0 255.0.0.0`	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-3 페이지의 EIGRP 구성을 참조하십시오.
3단계	**interface** *phy_if* **예:** `hostname(config)# interface inside`	EIGRP 메시지 인증을 구성하는 인터페이스에 대한 인터페이스 컨피그레이션 모드로 진입합니다.
4단계	**authentication mode eigrp** *as-num* **md5** **예:** `hostname(config)# authentication mode eigrp 2 md5`	EIGRP 패킷의 MD5 인증을 활성화합니다. *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`

	명령	목적
5단계	**authentication key eigrp** *as-num key* **key-id** *key-id* 예: `hostname(config)# authentication key eigrp 2 cisco key-id 200`	MD5 알고리즘에서 사용하는 키를 구성합니다. *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* 인수는 영문자, 숫자, 특수 문자를 포함하여 최대 16자가 될 수 있습니다. **참고** key 인수에는 공백을 사용할 수 없습니다. *key-id* 인수는 0~255 범위의 숫자입니다.

EIGRP 인접 디바이스 정의

EIGRP hello 패킷은 멀티캐스트 패킷으로 전송됩니다. EIGRP 인접 디바이스가 터널과 같이 브로드캐스트가 아닌 네트워크에 위치한 경우 해당 인접 디바이스를 수동으로 정의해야 합니다. EIGRP 인접 디바이스를 수동으로 정의할 경우 hello 패킷은 유니캐스트 메시지로 해당 인접 디바이스에 전송됩니다.

EIGRP 인접 디바이스를 수동으로 정의하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* 예: `ciscoasa(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**neighbor** *ip-addr* **interface** *if_name* 예: `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1`	고정 인접 디바이스를 정의합니다. *ip-addr* 인수는 인접 디바이스의 IP 주소입니다. *if-name* 인수는 **nameif** 명령으로 지정된 인터페이스 이름이며 이 이름을 통해 인접 디바이스를 이용할 수 있습니다. EIGRP 라우팅 프로세스에 여러 인접 디바이스를 정의할 수 있습니다.

EIGRP로 경로 재배포

RIP 및 OSPF에서 검색된 경로를 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. 고정 경로 및 연결된 경로도 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. EIGRP 컨피그레이션에서 **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 재배포될지 정의하기 위해 경로 지도를 생성해야 합니다. 경로 지도 생성에 관한 자세한 정보는 20 장, "경로 맵"에서 참조하십시오.

EIGRP 라우팅 프로세스로 경로를 재배포하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* **예:** `ciscoasa(config)# router eigrp 2`	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**default-metric** *bandwidth delay reliability loading mtu* **예:** `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu`	(선택 사항) EIGRP 라우팅 프로세스로 재배포된 경로에 적용할 기본 메트릭을 지정합니다. EIGRP 라우터 컨피그레이션에서 기본 메트릭을 지정하지 않으면 각 **redistribute** 명령에서 메트릭 값을 지정해야 합니다. EIGRP 메트릭을 **redistribute** 명령에서 지정하고 EIGRP 라우터 컨피그레이션에 **default-metric** 명령이 있는 경우 **redistribute** 명령의 메트릭이 사용됩니다.
3단계	다음 중 하나를 수행하여 선택한 경로 유형을 EIGRP 라우팅 프로세스로 재배포합니다.	
	redistribute connected [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **예:** `ciscoasa(config-router): redistribute connected [metric bandwidth delay reliability loading mtu] [route-map map_name]`	연결된 경로를 EIGRP 라우팅 프로세스로 재배포합니다. **redistribute** 명령에서 EIGRP 메트릭 값을 지정해야 합니다(EIGRP 라우터 컨피그레이션에 **default-metric** 명령이 없는 경우).
	redistribute static [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **예:** `ciscoasa(config-router): redistribute static [metric bandwidth delay reliability loading mtu] [route-map map_name]`	EIGRP 라우팅 프로세스로 고정 경로를 재배포합니다.

명령	목적
redistribute ospf *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] 예: 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*]	OSPF 라우팅 프로세스의 경로를 EIGRP 라우팅 프로세스로 재배포합니다.
redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**] 예: (config-router): redistribute rip [metric bandwidth delay reliability load mtu] [route-map map_name]	RIP 라우팅 프로세스의 경로를 EIGRP 라우팅 프로세스로 재배포합니다.

EIGRP의 필터링 네트워크

참고 이 프로세스를 시작하기 전에 알리고자 하는 경로를 정의하는 표준 ACL을 생성해야 합니다. 업데이트 송신 또는 수신에서 필터링하려는 경로를 정의하는 표준 ACL을 생성하는 것입니다.

EIGRP에서 네트워크를 필터링하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num* 예: ciscoasa(config)# router eigrp 2	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다. *as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	ciscoasa(config-router)# **network** *ip-addr* [*mask*] 예: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-6 페이지의 EIGRP를 위한 인터페이스 구성을 참조하십시오.
3단계	다음 중 하나를 수행하여 EIGRP 라우팅 업데이트에서 보내거나 받는 네트워크를 필터링:	

명령	목적
distribute-list *acl* **out** [**connected** | **ospf** | **rip** | **static** | **interface** *if_name*] 예: `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]`	EIGRP 라우팅 업데이트에서 전송되는 네트워크를 필터링합니다. 해당 특정 인터페이스에서 전송되는 업데이트에만 필터를 적용하도록 인터페이스를 지정할 수 있습니다. EIGRP 라우터 컨피그레이션에 여러 **distribute-list** 명령을 입력할 수 있습니다.
distribute-list *acl* **in** [**interface** *if_name*] 예: `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]`	EIGRP 라우팅 업데이트에서 수신되는 네트워크를 필터링합니다. 해당 특정 인터페이스에서 수신되는 업데이트에만 필터를 적용하도록 인터페이스를 지정할 수 있습니다.

EIGRP hello 간격 및 보류 시간 사용자 정의

ASA는 주기적으로 hello 패킷을 전송하여 인접 디바이스를 발견하고 인접 디바이스가 도달 불가 또는 작동 불능 상태가 되는 시간을 파악합니다. 기본적으로 hello 패킷은 5초 간격으로 전송됩니다.

hello 패킷은 ASA보류 시간을 알립니다. 보류 시간은 EIGRP 인접 디바이스에 ASA를 도달 가능으로 간주할 시간 길이를 알려줍니다. 인접 디바이스가 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.

hello 간격과 알려진 보류 시간을 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**interface** *phy_if* 예: `ciscoasa(config)# interface inside`	hello 간격 또는 알려진 보류 시간을 구성하는 인터페이스에 대한 인터페이스 컨피그레이션 모드로 진입합니다.
2단계	**hello-interval eigrp** *as-num seconds* 예: `ciscoasa(config)# hello-interval eigrp 2 60`	hello 간격을 변경합니다.
3단계	**hold-time eigrp** *as-num seconds* 예: `ciscoasa(config)# hold-time eigrp 2 60`	보류 시간을 변경합니다.

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.

자동 경로 요약을 비활성화하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num*	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다.
	예: `ciscoasa(config)# router eigrp 2`	*as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.
2단계	**no auto-summary**	이 값을 구성할 수 없습니다. 자동 요약 주소의 관리 거리는 5입니다.
	예: `ciscoasa(config-router)# no auto-summary`	

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 경로에서의 기본 경로 비트 설정이 비활성화됩니다.

기본 라우팅 정보를 구성하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**router eigrp** *as-num*	EIGRP 라우팅 프로세스를 생성하고 이 EIGRP 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다.
	예: `ciscoasa(config)# router eigrp 2`	*as-num* 인수는 EIGRP 라우팅 프로세스의 자율 시스템 번호입니다.

	명령	목적
2단계	`ciscoasa(config-router)# network ip-addr [mask]` 예: `ciscoasa(config)# router eigrp 2` `ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`	EIGRP 라우팅에 참여하는 인터페이스와 네트워크를 구성합니다. 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 23-6 페이지의 EIGRP를 위한 인터페이스 구성을 참조하십시오.
3단계	`no default-information {in | out | WORD}` 예: `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}`	후보 기본 경로 정보의 송수신을 제어합니다. **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. 하지만 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.

세부 단계

	명령	목적
1단계	`interface phy_if` 예: `ciscoasa(config)# interface phy_if`	EIGRP에서 사용하는 지연 값을 변경하는 인터페이스에 대한 인터페이스 컨피그레이션 모드에 진입합니다.
2단계	`no split-horizon eigrp as-number` 예: `ciscoasa(config-if)# no split-horizon eigrp 2`	split horizon을 비활성화합니다.

EIGRP 프로세스 재시작

EIGRP 프로세스를 다시 시작하거나 재배포 또는 카운터를 지우려면 다음 명령을 입력합니다.

명령	목적
clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events**)} 예: `ciscoasa(config)# clear eigrp pid 10 neighbors`	EIGRP 프로세스를 다시 시작하거나 재배포 또는 카운터를 지웁니다.

EIGRP 모니터링

다음 명령을 사용하여 EIGRP 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조에서 참조하십시오. 또한 인접 디바이스 변경 메시지 및 인접 디바이스 경고 메시지의 로깅을 비활성화할 수 있습니다.

다양한 EIGRP 라우팅 통계를 모니터링하거나 비활성화하려면 다음 명령 중 하나를 입력:

명령	목적
EIGRP 라우팅 모니터링	
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 인접 디바이스 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	엔트리 및 인터페이스 전달 측면에서 MFIB 정보를 표시합니다.
show route cluster	클러스터링을 위한 추가 경로 동기화 정보를 표시합니다.
EIGRP 로깅 메시지 비활성화	
no eigrp log-neighbor-changes	인접 디바이스 변경 메시지 로깅을 비활성화합니다. 이 명령을 EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드에 입력합니다.
no eigrp log-neighbor-warnings	인접 디바이스 경고 메시지 로깅을 비활성화합니다.

참고 기본적으로 인접 디바이스 변경 및 경고 메시지는 로깅됩니다.

EIGRP에 대한 컨피그레이션 예

다음 예는 다양한 프로세스 옵션으로 EIGRP를 활성화하고 구성하는 방법을 보여줍니다.

1단계 EIGRP를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

2단계 인터페이스의 EIGRP 라우팅 메시지 송수신을 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# passive-interface {default}
```

3단계 EIGRP 인접 디바이스를 정의하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

4단계 EIGRP 라우팅에 참여하는 인터페이스 및 네트워크를 구성하려면 다음 명령을 입력합니다.

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

5단계 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 기능 내역

표 23-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 23-1 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 재배포 및 모니터링에 대한 지원이 추가되었습니다. 도입된 명령: **route eigrp**.
다중 컨텍스트 모드의 동적 라우팅	9.0(1)	EIGRP 라우팅이 다중 컨텍스트 모드에서 지원됩니다.

표 23-1 EIGRP 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
클러스터링	9.0(1)	EIGRP의 경우 일괄 동기화, 경로 동기화 및 계층 2 로드 밸런싱은 클러스터링 환경에서 지원됩니다. 도입되거나 수정된 명령: **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.

24 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 멀티캐스트프로토콜이 지원하는 Cisco 라우터에 의해 네트워크에서 복제되어 여러 수신자에게 데이터를 가장 효율적으로 제공할 수 있게 됩니다.

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 PIM에 대해 구성될 수 없습니다.

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. 멀티캐스트 그룹당 단일 Rendezvous Point를 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 선택 프로세스를 사용하여 구축됩니다. 멀티캐스트 데이터는 DF의 도움을 받아 소스에서 Rendezvous Point로 전달되고 따라서 소스별 상태 없이도 공유 트리에서 수신자를 따르게 됩니다. DF 선택은 Rendezvous Point 검색 중에 이루어지고 Rendezvous Point에 대한 기본 경로를 제공합니다.

참고 ASA가 PIM Rendezvous Point인 경우 ASA의 번역되지 않은 외부 주소를 Rendezvous Point 주소로 사용하십시오.

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. 레이어 2 클러스터링에서는 fast-path 전달이 설정될 때까지 마스터 유닛이 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 전송합니다. fast-path 전달이 설정된 후에는 슬레이브 유닛이 멀티캐스트 데이터 패킷을 전송할 수 있습니다. 모든 데이터 흐름은 완전한 흐름입니다. Stub 전달 흐름도 지원됩니다. 레이어 2 클러스터링에서는 하나의 유닛만 멀티캐스트 패킷을 받기 때문에 마스터 유닛으로의 리디렉션이 일반적입니다. 레이어 3 클러스터링에서는 유닛이 독립적으로 작동하지 않습니다. 모든 데이터 및 라우팅 패킷은 마스터 유닛에 의해 처리 및 전달됩니다. 슬레이브 유닛은 전송된 모든 패킷을 삭제합니다.

클러스터링에 대한 자세한 내용은 8 장, "ASA 클러스터"를 참고하십시오.

멀티캐스트 라우팅을 위한 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 컨텍스트 모드에서 지원됩니다. 다중 컨텍스트 모드에서 미공유 인터페이스와 공유 인터페이스는 지원되지 않습니다.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

클러스터링에서는 IGMP 및 PIM에 대해 이 기능은 마스터 유닛에서만 지원됩니다.

멀티캐스트 라우팅 활성화

멀티캐스트 라우팅을 활성화하면 ASA에서 멀티캐스트 라우팅을 사용할 수 있습니다. 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 기본적으로 IGMP 및 PIM이 활성화됩니다. 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.

참고 멀티캐스트 라우팅에 대해서는 UDP 전송 레이어만 지원됩니다.

멀티캐스트 라우팅을 활성화하려면 다음 명령을 입력합니다..

명령	목적
multicast-routing **예:** `ciscoasa(config)# multicast-routing`	멀티캐스트 라우팅을 활성화합니다. 멀티캐스트 라우팅 테이블의 엔트리 개수는 ASA의 RAM에 의해 제한됩니다.

표 24-1은 ASA의 RAM을 기준으로 특정 멀티캐스트 테이블에 대한 최대 엔트리 개수를 열거합니다. 이 제한에 도달하면 새로운 엔트리가 삭제됩니다.

표 24-1 멀티캐스트 테이블 엔트리 제한

표	16MB	128MB	128MB 이상
MFIB	1000	3000	30000
IGMP 그룹	1000	3000	30000
PIM 경로	3000	7000	72000

멀티캐스트 라우팅 사용자 정의

이 섹션에서는 멀티캐스트 라우팅을 사용자 정의하는 방법을 설명합니다.

Stub 멀티캐스트 라우팅 구성 및 IGMP 메시지 전달

참고 Stub 멀티캐스트 라우팅 및 PIM은 동시에 지원되지 않습니다.

stub 영역으로의 게이트웨이 역할을 하는 ASA은 PIM에 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 참가를 전달하고 stub 영역 인터페이스에서 업스트림 인터페이스로 메시지를 남깁니다.

호스트 참가를 전달하고 메시지를 남기려면 stub 영역에 연결된 인터페이스에서 다음 명령을 입력합니다..

명령	목적
igmp forward interface *if_name* 예: `ciscoasa(config-if)# igmp forward interface interface1`	stub 멀티캐스트 라우팅을 구성하고 IGMP 메시지를 전달합니다.

Static Multicast Route 구성

고정 멀티캐스트 경로를 구성함으로써 유니캐스트 트래픽에서 멀티캐스트 트래픽을 분리할 수 있습니다. 예를 들어 소스와 대상 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.

고정 멀티캐스트 경로 또는 stub 영역에 대한 고정 멀티캐스트 경로를 구성하려면 다음 명령 중 하나를 입력합니다.

명령	목적
mroute *src_ip src_mask* {*input_if_name* | *rpf_neighbor*} [*distance*] **예:** ciscoasa(config)# mroute *src_ip src_mask* {*input_if_name* | *rpf_neighbor*} [*distance*]	고정 멀티캐스트 경로를 구성합니다.
mroute *src_ip src_mask input_if_name* [**dense** *output_if_name*] [*distance*] **예:** ciscoasa(config)# mroute *src_ip src_mask input_if_name* [dense *output_if_name*] [*distance*]	stub 영역에 대한 고정 멀티캐스트 경로를 구성합니다. **dense** *output_if_name* 키워드와 인수 쌍은 stub 멀티캐스트 라우팅에 대해서만 지원됩니다.

IGMP 기능 구성

IP 호스트가 IGMP(Internet Group Management Protocol)를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터로 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.

IGMP는 그룹 주소(Class D IP 주소)를 그룹 식별자로 사용합니다. 호스트 그룹 주소 범위는 224.0.0.0~239.255.255.255입니다. 224.0.0.0 주소는 어떤 그룹에도 할당되지 않습니다. 224.0.0.1 주소는 서브넷의 모든 시스템에 할당됩니다. 224.0.0.2 주소는 서브넷의 모든 라우터에 할당됩니다.

ASA에서 멀티캐스트 라우팅을 활성화할 경우 IGMP 버전 2가 모든 인터페이스에서 자동으로 활성화됩니다.

참고 **show run** 명령을 사용할 경우 인터페이스 컨피그레이션에 **no igmp** 명령만 표시됩니다. 디바이스 컨피그레이션에 **multicast-routing** 명령이 나타날 경우 IGMP가 자동으로 모든 인터페이스에서 활성화됩니다.

이 섹션은 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.

인터페이스에서 IGMP를 비활성화하려면 다음 명령을 입력합니다..

명령	목적
no igmp 예: `ciscoasa(config-if)# no igmp`	인터페이스에서 IGMP를 비활성화합니다. 인터페이스에서 IGMP를 다시 활성화하려면 **igmp** 명령을 사용합니다.

참고 인터페이스 컨피그레이션에 **no igmp** 명령만 표시됩니다.

IGMP 그룹 멤버십 구성

ASA를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. ASA를 멀티캐스트 그룹에 참여하도록 구성하면 업스트림 라우터가 해당 그룹에 대한 멀티캐스트 라우팅 테이블 정보를 유지하고 해당 그룹에 대한 경로를 활성 상태로 유지하게 됩니다.

참고 특정 그룹에 대한 멀티캐스트 패킷을 인터페이스로 전달하면서 ASA가 패킷을 해당 그룹의 일부로 수락하지 않도록 하려면 24-7 페이지의 고정 참여 IGMP 그룹 구성을 참조하십시오.

ASA가 멀티캐스트 그룹에 참여하도록 하려면 다음 명령을 입력하십시오..

명령	목적
igmp join-group *group-address* 예: `ciscoasa(config-if)# igmp join-group mcast-group`	ASA을(를) 멀티캐스트 그룹의 멤버로 구성합니다. *group-address* 인수는 그룹의 IP 주소입니다.

고정 참여 IGMP 그룹 구성

때로는 일부 컨피그레이션으로 인해 또는 네트워크 세그먼트의 그룹에 멤버가 없기 때문에 그룹 멤버가 멤버십을 보고할 수 없는 경우도 있습니다. 하지만 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.

인터페이스의 고정 연결 멀티캐스트 그룹을 구성하려면다음 명령을 입력합니다..

명령	목적
igmp static-group **예:** `ciscoasa(config-if)# igmp static-group group-address`	ASA가 인터페이스에서 멀티캐스트 그룹에 고정으로 연결하도록 구성합니다. *group-address* 인수는 그룹의 IP 주소입니다.

멀티캐스트 그룹에 대한 액세스 제어

ASA 인터페이스의 호스트가 참여할 수 있는 멀티캐스트 그룹을 제어하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	다음 중 하나를 수행하여 표준 또는 확장 ACL을 생성합니다.	
	access-list *name* **standard** [**permit** | **deny**] *ip_addr mask* **예:** `ciscoasa(config)# access-list acl1 standard permit 192.52.662.25`	멀티캐스트 트래픽에 대한 표준 ACL을 생성합니다. 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.
	access-list *name* **extended** [**permit** | **deny**] *protocol* src_*ip_addr* src_*mask dst_ip_addr dst_mask* **예:** `ciscoasa(config)# access-list acl2 extended permit protocol src_ip_addr src_mask dst_ip_addr dst_mask`	확장 ACL을 만듭니다. *dst_ip_addr* 인수는 허용 또는 거부되는 멀티캐스트 그룹의 IP 주소입니다.
2단계	**igmp access-group** *acl* **예:** `ciscoasa(config-if)# igmp access-group acl`	ACL을 인터페이스에 적용합니다. *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.

인터페이스에서 IGMP 상태의 수를 제한하려면 다음 명령을 입력합니다..

명령	목적
igmp limit *number* 예: ciscoasa(config-if)# igmp limit *50*	인터페이스에서 IGMP 상태의 수를 제한합니다. 유효한 값 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

참고 **igmp query-timeout** 및 **igmp query-interval** 명령은 IGMP 버전 2를 필요로 합니다.

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 주기적으로 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 안에 ASA가 호스트 쿼리에 대한 응답을 받지 못하면 그 그룹이 삭제됩니다.

쿼리 간격, 쿼리 응답 시간 및 쿼리 시간 초과 값을 변경하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**igmp query-interval** *seconds* 예: ciscoasa(config-if)# igmp query-interval *30*	쿼리 간격 시간을 초로 설정합니다. 유효한 값 범위는 0~500이고 기본값은 125입니다. ASA가 인터페이스에서 지정된 시간 초과 값(기본값: 255초) 동안 쿼리 메시지를 수신하지 못하면 ASA가 지정된 라우터가 되고 쿼리 메시지를 전송하기 시작합니다.
2단계	**igmp query-timeout** *seconds* 예: ciscoasa(config-if)# igmp query-timeout *30*	쿼리의 시간 초과 값을 변경합니다. 유효한 값 범위는 0~500이고 기본값은 225입니다.

	명령	목적
3단계	**igmp query-max-response-time** *seconds* 예: `ciscoasa(config-if)# igmp query-max-response-time 30`	최대 쿼리 응답 시간을 변경합니다.

IGMP 버전 변경

기본적으로 ASA는 **igmp query-timeout** 및 **igmp query-interval** 명령과 같은 몇 가지 추가 기능을 지원하는 IGMP Version 2를 실행합니다.

서브넷의 모든 멀티캐스트 라우터는 같은 버전의 IGMP를 지원해야 합니다. ASA는 자동으로 Version 1 라우터를 감지하고 Version 1로 전환하지 않습니다. 그러나 IGMP Version 1과 2 호스트를 서브넷에서 혼용할 수는 있습니다. ASA 실행 중인 IGMP 버전 2는 IGMP 버전 1 호스트가 있을 때에도 정상 작동합니다.

인터페이스에서 실행되는 IGMP 버전을 제어하려면 다음 명령을 입력합니다..

명령	목적
igmp version {**1** | **2**} 예: `ciscoasa(config-if)# igmp version 2`	인터페이스에서 실행하려는 IGMP 버전을 제어합니다.

PIM 기능 구성

라우터는 PIM을 사용하여 멀티캐스트 다이어그램 전달을 위한 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.

- 24-10 페이지의 인터페이스에서 PIM 활성화 및 비활성화
- 24-10 페이지의 고정 Rendezvous Point 주소 구성
- 24-11 페이지의 지정된 라우터 우선순위 구성
- 24-11 페이지의 PIM 레지스터 메시지 구성 및 필터링
- 24-11 페이지의 PIM 메시지 간격 구성
- 24-12 페이지의 PIM 인접 디바이스 필터링

인터페이스에서 PIM 활성화 및 비활성화

특정 인터페이스에서 PIM을 활성화하거나 비활성화할 수 있습니다. 인터페이스에서 PIM을 활성화하거나 비활성화하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**pim** 예: `ciscoasa(config-if)# pim`	특정 인터페이스에서 PIM을 활성화하거나 다시 활성화합니다.
2단계	**no pim** 예: `ciscoasa(config-if)# no pim`	특정 인터페이스에서 PIM을 비활성화합니다.

참고 인터페이스 컨피그레이션에 **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 Auto-RP 또는 PIM BSR을 지원하지 않습니다. **pim rp-address** 명령을 사용하여 RP 주소를 지정해야 합니다.

ASA가 하나 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.

PIM PR의 주소를 구성하려면 다음 명령을 입력합니다..

명령	목적
pim rp-address *ip_address* [*acl*] [**bidir**] 예: `ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]`	특정 인터페이스에서 PIM을 활성화하거나 다시 활성화합니다. *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 sparse mode에서 작동하게 됩니다.

참고 실제 양방향 컨피그레이션에 관계없이 ASA는 PIM hello 메시지에서 항상 양방향 기능을 알립니다.

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 우선순위를 따릅니다. 여러 디바이스의 DR 우선순위가 동일한 경우 IP 주소가 가장 높은 디바이스가 DR이 됩니다.

기본적으로 ASA의 DR 우선순위는 1입니다. 이 값을 변경하려면 다음 명령을 입력합니다..

명령	목적
pim dr-priority *num* **예:** `ciscoasa(config-if)# pim dr-priority 500`	지정된 라우터 우선순위를 변경합니다. *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 창을 통해 ASA가 PIM 레지스터 메시지를 수락하는 멀티캐스트 소스를 정의할 수 있습니다.

PIM 레지스터 메시지를 필터링하려면 다음 명령을 입력합니다..

명령	목적
pim accept-register {**list** *acl* | **route-map** *map-name*} **예:** `ciscoasa(config)# pim accept-register {list acl1 | route-map map2}`	PIM 레지스터 메시지를 필터링하도록 ASA를 구성합니다. 예제에서 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 참여 또는 prune 메시지를 보냅니다.

이 간격을 변경하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**pim hello-interval** *seconds* **예:** `ciscoasa(config-if)# pim hello-interval 60`	라우터 쿼리 메시지를 보냅니다. *seconds* 인수로 유효한 값은 1~3600초입니다.

	명령	목적
2단계	**pim join-prune-interval** *seconds* 예: `ciscoasa(config-if)# pim join-prune-interval 60`	ASA이(가) PIM 참여 또는 prune 메시지를 전송하는 시간(초)을 변경합니다. *seconds* 인수로 유효한 값은 10~600초입니다.

PIM 인접 디바이스 필터링

PIM 인접 디바이스가 될 수 있는 라우터를 정의할 수 있습니다. PIM 인접 디바이스가 될 수 있는 라우터를 필터링함으로써 다음을 할 수 있습니다.

- 권한이 없는 라우터가 PIM 인접 디바이스가 되는 것을 막습니다.
- 연결된 stub 라우터가 PIM에 참여하는 것을 막습니다.

PIM 인접 디바이스가 될 수 있는 인접 디바이스를 정의하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**access-list pim_nbr deny** *router-IP_addr PIM neighbor* 예: `ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255`	표준 ACL을 사용하여 PIM에 참여시킬 라우터를 정의합니다. 이 예제에서 다음 ACL은 **pim neighbor-filter** 명령과 함께 사용할 경우 10.1.1.1 라우터가 PIM 인접 디바이스가 될 수 없도록 막습니다.
2단계	**pim neighbor-filter pim_nbr** 예: `ciscoasa(config)# interface GigabitEthernet0/3` `ciscoasa(config-if)# pim neighbor-filter pim_nbr`	인접한 라우터를 필터링합니다. 이 예제에서 10.1.1.1 라우터는 GigabitEthernet0/3 인터페이스에서 PIM 인접 디바이스가 될 수 없습니다.

양방향 인접 필터 구성

Bidirectional Neighbor Filter 창은 ASA에 구성된 PIM 양방향 인접 필터를 보여줍니다. PIM 양방향 인접 디바이스 필터는 인접 디바이스가 DF 선택에 참여할 수 있다고 정의하는 ACL입니다. 인터페이스에 대해 PIM 양방향 인접 디바이스 필터가 구성되지 않은 경우에는 제한 사항이 없습니다. PIM 양방향 인접 디바이스 필터가 구성된 경우 ACL에서 허용된 인접 디바이스만 DF 선택 프로세스에 참여할 수 있습니다.

PIM 양방향 인접 필터 컨피그레이션이 ASA에 적용된 경우 ACL이 *interface-name*_multicast라는 이름으로 실행 중인 컨피그레이션에 표시되며 *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 인접 디바이스가 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 인접 디바이스 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 자기들 끼리 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 인접 디바이스 필터가 활성화된 경우 ACL에 의해 허용된 라우터는 양방향을 지원하는 것으로 간주됩니다. 따라서 다음은 참입니다.

- 허용된 인접 디바이스가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 인접 디바이스가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 인접 디바이스가 bidir을 지원하지 않을 경우 DF 선택이 일어날 수 있습니다.

PIM 양방향 인접 디바이스 필터가 될 수 있는 인접 디바이스를 정의하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**access-list pim_nbr deny** *router-IP_addr PIM neighbor* 예: `ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255`	표준 ACL을 사용하여 PIM에 참여시킬 라우터를 정의합니다. 이 예제에서 다음 ACL은 **pim neighbor-filter** 명령과 함께 사용할 경우 10.1.1.1 라우터가 PIM 인접 디바이스가 될 수 없도록 막습니다.
2단계	**pim bidirectional-neighbor-filter pim_nbr** 예: `ciscoasa(config)# interface GigabitEthernet0/3` `ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr`	인접한 라우터를 필터링합니다. 이 예제에서 10.1.1.1 라우터는 GigabitEthernet0/3 인터페이스에서 PIM 양방향 인접 디바이스가 될 수 없습니다.

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.

entering the **multicast boundary** command를 선택하여 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 고유한 글로벌 값이 아니라 로컬로 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 Auto-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.

멀티캐스트 경계를 구성하려면 다음 명령을 입력합니다..

명령	목적
multicast boundary *acl* [**filter-autorp**] **예:** ciscoasa(config-if)# multicast boundary *acl1* [filter-autorp]	멀티캐스트 경계를 구성합니다.

멀티캐스트 라우팅의 컨피그레이션 예

다음 예는 다양한 프로세스 옵션으로 멀티캐스트 라우팅을 활성화하고 구성하는 방법을 보여줍니다.

1단계 멀티캐스트 라우팅 활성화:

```
ciscoasa(config)# multicast-routing
```

2단계 고정 멀티캐스트 경로 구성:

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

3단계 ASA를 멀티캐스트 그룹의 멤버로 구성:

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

추가 참조 자료

라우팅에 관한 자세한 내용은 다음 섹션을 참조하십시오.

- 24-15 페이지의 관련 문서
- 24-15 페이지의 RFC

관련 문서

관련 항목	문서 제목
SMR 기능 구현을 위해 사용되는 IGMP 및 멀티캐스트 라우팅 표준에 관한 기술 정보	IETF draft-ietf-idmr-igmp-proxy-01.txt

RFC

RFC	제목
RFC 2113	IP 라우터 경고 옵션
RFC 2236	IGMPv2
RFC 2362	PIM-SM
RFC 2588	IP 멀티캐스트와 방화벽

멀티캐스트 라우팅에 대한 기능 내역

표 24-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 24-2 멀티캐스트 라우팅에 대한 기능 내역

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. 도입된 명령: **multicast-routing**
클러스터링 지원	9.0(1)	클러스터링 지원이 추가되었습니다. 도입된 명령: **debug mfib cluster**, **show mfib cluster**.

25 장

IPv6 인접 디바이스 검색

IPv6 인접 디바이스 검색에 관한 정보

IPv6 인접 디바이스 검색 프로세스는 ICMPv6 메시지와 solicited-node 멀티캐스트 주소를 사용하여 동일 네트워크(로컬 링크)에 있는 인접 디바이스의 링크 계층 주소를 확인하고 인접 디바이스의 가독성을 확인하며 주변 라우터를 추적합니다.

노드(호스트)는 인접 디바이스 검색을 사용하여 연결된 링크에 상주하는 것으로 알려진 인접 디바이스에 대한 링크 계층 주소를 확인하고 무효화되는 충돌 값을 빠르게 삭제합니다. 호스트는 또한 인접 디바이스 검색을 사용하여 대신 패킷을 전달할 의사가 있는 주변 라우터를 찾기도 합니다. 또한 노드는 프로토콜을 이용하여 인접 디바이스의 접근 가능 여부를 능동적으로 추적하고 변경된 링크 계층 주소를 감지합니다. 라우터 또는 라우터 경로가 실패할 경우 호스트가 정상 작동하는 대안을 능동적으로 검색합니다.

인접 디바이스 요청 메시지

인접 디바이스 요청 메시지(ICMPv6 Type 135)는 로컬 링크에 있는 다른 노드의 링크 계층 주소를 발견하려는 노드가 로컬 링크에서 전송합니다. 인접 디바이스 요청 메시지는 요청된 노드의 멀티캐스트 주소로 전송됩니다. 인접 디바이스 요청 메시지의 소스 주소는 인접 디바이스 요청 메시지를 보내는 노드의 IPv6 주소입니다. 인접 디바이스 요청 메시지는 또한 소스 노드의 링크 계층 주소도 포함합니다.

인접 디바이스 요청 메시지를 수신한 후 대상 노드는 로컬 링크에서 인접 디바이스 광고 메시지(ICPMv6 Type 136)를 전송함으로써 응답합니다. 인접 디바이스 알림 메시지의 소스 주소는 인접 디바이스 알림 메시지를 보내는 노드의 IPv6 주소입니다. 대상 주소는 인접 디바이스 요청 메시지를 보낸 노드의 IPv6 주소입니다. 인접 디바이스 알림 메시지의 데이터 부분은 인접 디바이스 알림 메시지를 보내는 노드의 링크 계층 주소를 포함합니다.

소스 노드가 인접 디바이스 알림을 수신한 후 소스 노드와 대상 노드가 통신할 수 있습니다.

인접 디바이스 요청 메시지는 인접 디바이스의 링크 계층 주소를 식별한 후 인접 디바이스의 연결성을 확인하는 데 사용됩니다. 노드가 인접 디바이스의 연결성을 확인하고자 하는 경우 인접 디바이스 요청 메시지의 대상 주소는 인접 디바이스의 유니캐스트 주소입니다.

인접 디바이스 알림 메시지는 로컬 링크에 있는 노드의 링크 계층 주소가 변경될 경우에도 전송됩니다. 이러한 변화가 있을 인접 알림에 대한 대상 주소는 올-노드 멀티캐스트 주소입니다.

인접 디바이스 연결 가능 시간

인접 디바이스 연결 가능 시간은 사용할 수 없는 인접 디바이스를 감지할 수 있게 합니다. 시간을 짧게 구성하면 사용할 수 없는 인접 디바이스를 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.

중복 주소 감지

무상태 자동 컨피그레이션 프로세스 중 Duplicate Address Detection이 새로운 유니캐스트 IPv6 주소의 고유성을 먼저 확인한 후 주소가 인터페이스에 할당됩니다(Duplicate Address Detection 수행 중에는 새로운 주소가 임시 상태를 유지). Duplicate Address Detection은 먼저 새로운 링크-로컬 주소에서 수행됩니다. 링크-로컬 주소가 고유한 것으로 확인되면 인터페이스의 모든 다른 IPv6 유니캐스트 주소에서 Duplicate Address Detection이 수행됩니다.

관리상 다운된 인터페이스에서는 Duplicate Address Detection이 중지됩니다. 인터페이스가 관리상 다운된 동안에는 인터페이스에 할당된 유니캐스트 IPv6 주소가 대기 상태로 설정됩니다. 관리상 가동 상태로 복귀하는 인터페이스는 인터페이스의 모든 유니캐스트 IPv6 주소에 대한 Duplicate Address Detection을 재시작합니다.

중복 주소가 확인되면 주소 상태가 DUPLICATE으로 설정되고 주소가 사용되지 않으며 다음 오류 메시지가 생성됩니다.

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 비활성화됩니다. 중복 주소가 글로벌 주소인 경우 주소가 사용되지 않습니다. 하지만 주소 상태가 DUPLICATE로 설정된 동안 중복 주소와 연결된 모든 컨피그레이션 명령은 구성된 상태를 유지합니다.

인터페이스의 링크-로컬 주소가 변경된 경우 새로운 링크-로컬 주소에서 Duplicate Address Detection이 수행되고 인터페이스와 연결된 모든 다른 IPv6 주소가 다시 생성됩니다(Duplicate Address Detection은 새로운 링크-로컬 주소에서만 수행됨).

ASA은(는) 인접 디바이스 요청 메시지를 사용하여 Duplicate Address Detection을 수행합니다. 기본적으로 인터페이스가 Duplicate Address Detection을 수행하는 횟수는 1입니다.

라우터 광고 메시지

Cisco ASA는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 라우터 알림 메시지(ICMPv6 Type 134)는 주기적으로 ASA의 각 구성된 IPv6 인터페이스로 전송됩니다. 라우터 알림 메시지가 all-nodes 멀티캐스트 주소로 전송됩니다.

라우터 알림 메시지는 일반적으로 다음 정보를 포함합니다.

- 로컬 링크의 노드가 IPv6 주소 자동 구성에 사용할 수 있는 하나 이상의 IPv6 접두사
- 알림에 포함된 각 접두사에 대한 수명 정보
- 완료할 수 있는 자동 컨피그레이션의 유형(무상태 또는 상태 기반)을 나타내는 플래그 세트
- 기본 라우터 정보(알림을 보내는 라우터를 기본 라우터로 사용할지, 만약 그렇다면 라우터를 얼마 동안 기본 라우터로 사용할지(초))
- 호스트가 해당 호스트에서 발생하는 패킷에서 사용할 홉 제한과 MTU와 같이 호스트에 대한 추가 정보
- 주어진 링크에서 인접 디바이스 요청 메시지 재전송 사이의 시간
- 노드가 인접 디바이스를 접근 가능으로 고려하는 시간

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 전송됩니다(ICMPv6 타입 133). 다음 예정된 라우터 알림 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다. 라우터 요청 메시지는 보통 시스템 시동 시에 호스트에 의해 전송되고 호스트에 구성된 유니캐스트 주소가 없기 때문에 라우터 요청 메시지의 소스 주소는 보통 지정되지 않은 IPv6 주소(0:0:0:0:0:0:0:0)입니다. 호스트에 유니캐스트 주소가 구성되어 있는 경우 라우터 요청 메시지를 보내는 인터페이스의 유니캐스트 주소가 메시지에서 소스 주소로 사용됩니다. 라우터 요청 메시지의 대상 주소는 링크 범위의 모든 라우터 멀티캐스트 주소입니다. 라우터 요청에 대한 응답으로 라우터 알림이 전송되면 라우터 알림 메시지의 대상 주소가 라우터 요청 메시지 소스의 유니캐스트 주소입니다.

라우터 알림 메시지에 대한 다음 설정을 구성할 수 있습니다.

- 정기적인 라우터 알림 메시지 사이의 시간 간격
- IPv6 노드가 ASA를 기본 라우터로 간주할 시간을 나타내는 라우터 수명 값
- 해당 링크에서 사용되는 IPv6 네트워크 접두사
- 인터페이스의 라우터 알림 메시지 전송 여부

따로 언급이 없으면 라우터 알림 메시지 설정은 인터페이스마다 다르며 인터페이스 컨피그레이션 모드에서 입력됩니다.

고정 IPv6 인접 디바이스

IPv6 인접 디바이스 캐시의 인접 디바이스를 수동으로 정의할 수 있습니다. 지정된 IPv6 주소에 대한 엔트리가 인접 디바이스 검색 캐시에 존재하는 경우(IPv6 인접 디바이스 검색 프로세스를 통해 학습) 이 엔트리는 고정 엔트리로 자동 변환됩니다. IPv6 인접 디바이스 검색 캐시의 고정 엔트리는 인접 디바이스 검색 프로세스로 인해 변경되지 않습니다.

IPv6 인접 디바이스 검색에 대한 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

IPv6 인접 디바이스 검색 조건

11-11 페이지의 IPv6 주소 지정 구성에 따라 IPv6 주소를 구성합니다.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우팅 모드에서만 지원됩니다. 투명 모드는 지원되지 않습니다.

추가 지침 및 제한

- 간격 값은 이 인터페이스를 통해 발송되는 모든 IPv6 라우터 알림에 포함됩니다.
- 구성된 시간을 통해 사용할 수 없는 인접 디바이스를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 인접 디바이스를 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.
- 전송 사이의 간격은 ASA가 **ipv6 nd ra-lifetime** 명령을 사용하여 기본 라우터로 구성된 경우 IPv6 라우터 알림 수명보다 작거나 같아야 합니다. 다른 IPv6 노드와의 동기화를 방지하려면 사용되는 실제 값을 지정된 값의 20% 범위로 임의로 조정하십시오.
- **ipv6 nd prefix** 명령을 통해 접두사 알림 여부를 포함하여 접두사별로 개별 매개변수를 제어할 수 있습니다.
- 기본적으로 **ipv6 address** 명령을 사용해서 인터페이스에서 주소로 구성된 접두사는 라우터 알림에서 알려집니다. **ipv6 nd prefix** 명령을 사용하여 접두사를 구성할 경우 해당 접두사만 알려집니다.

- **default** 키워드는 모든 접두사에 대한 기본 매개변수 설정에 사용할 수 있습니다.
- 날짜는 접두사의 만료를 지정하도록 설정할 수 있습니다. 유효 수명과 기본 수명은 실시간으로 계산됩니다. 만료 날짜가 되면 접두사가 더 이상 알려지지 않습니다.
- onlink가 켜진 경우(기본값) 지정된 접두사가 링크에 할당됩니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 대상을 링크에서 로컬로 도달 가능한 것으로 간주합니다.
- 자동 컨피그레이션이 켜진 경우(기본값) 지정된 접두사를 IPv6 자동 컨피그레이션에 사용할 수 있음을 호스트에 알려주는 것입니다.
- 무상태 자동 컨피그레이션이 바르게 작동하려면 라우터 알림 메시지의 알려진 접두사 길이가 항상 64비트여야 합니다.
- 라우터 수명 값은 인터페이스에서 발송된 모든 IPv6 라우터 알림에 포함됩니다. 이 값은 이 인터페이스에서 기본 라우터로서 ASA의 유용성을 나타냅니다.
- 0이 아닌 값으로 설정하면 ASA를 이 인터페이스의 기본값으로 간주해야 함을 나타냅니다. 0이 아닌 라우터 수명 값은 라우터 알림 간격보다 적으면 안 됩니다.

고정 IPv6 인접 디바이스 구성에는 다음 지침과 제한 사항이 적용됩니다.

- **ipv6 neighbor** 명령은 **arp** 명령과 유사합니다. 지정된 IPv6 주소에 대한 엔트리가 인접 디바이스 검색 캐시에 존재하는 경우(IPv6 인접 디바이스 검색 프로세스를 통해 학습) 이 엔트리는 고정 엔트리로 자동 변환됩니다. 이 엔트리는 컨피그레이션 저장을 위해 copy 명령이 사용될 때 컨피그레이션에 저장됩니다.
- **show ipv6 neighbor** 명령을 사용하여 IPv6 인접 디바이스 검색 캐시의 고정 엔트리를 봅니다.
- **clear ipv6 neighbor** 명령은 IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 제외한 모든 엔트리를 삭제합니다. **no ipv6 neighbor** 명령은 인접 디바이스 검색 캐시에서 특정 고정 엔트리를 삭제합니다. 이 명령은 동적 엔트리(IPv6 인접 디바이스 검색 프로세스에서 학습한 엔트리)를 캐시에서 삭제하지 않습니다. **no ipv6 enable** 명령을 사용하여 인터페이스에서 IPv6를 비활성화하면 고정 엔트리를 제외하고 해당 인터페이스에 대한 모든 IPv6 인접 디바이스 검색 캐시 엔트리가 삭제됩니다(엔트리 상태가 INCMP [Incomplete]로 변경됨).
- IPv6 인접 디바이스 검색 캐시의 고정 엔트리는 인접 디바이스 검색 프로세스로 인해 변경되지 않습니다.
- **clear ipv6 neighbor** 명령은 IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 삭제하지 않습니다. 동적 엔트리만 삭제합니다.
- 생성된 ICMP syslog는 IPv6 인접 디바이스 엔트리의 정기적인 갱신에 의한 것입니다. IPv6 인접 디바이스 엔트리에 대한 ASA 기본 타이머는 ASA가 30초마다 ICMPv6 인접 디바이스 검색과 응답 패킷을 생성하도록 30초입니다. ASA가 IPv6 주소로 구성된 장애 조치 LAN과 상태 인터페이스를 모두 가지고 있는 경우 30초마다 ICMPv6 인접 디바이스 검색과 응답 패킷이 구성된 주소와 링크-로컬 IPv6 주소 모두에 대해 생성됩니다. 또한 각 패킷이 여러 syslog(ICMP 연결 및 로컬-호스트 생성 또는 해체)를 생성하여 연속적인 ICMP syslog가 생성되는 것으로 보일 수 있습니다. IPV6 인접 디바이스 엔트리에 대한 갱신 시간은 일반 데이터 인터페이스에서 구성 가능하나 장애 조치 인터페이스에서는 구성할 수 없습니다. 그러나 이 ICMP 인접 디바이스 검색 트래픽의 CPU에 대한 영향은 거의 없습니다.

IPv6 인접 디바이스 검색 기본 설정

표 25-1은 IPv6 인접 디바이스 검색을 위한 기본 설정을 나열합니다.

표 25-1 기본 IPv6 인접 디바이스 검색 매개변수

매개변수	기본
인접 디바이스 요청 전송 메시지 간격 *값*	인접 디바이스 요청 전송 사이의 1000초
인접 디바이스 도달 가능 시간 *값*	기본값은 0입니다.
라우터 알림 전송 간격 *값*	기본값은 200초입니다.
라우터 수명 *값*	기본값은 1800초입니다.
DAD 중 전송되는 연속 인접 디바이스 요청 메시지의 개수 *값*	기본값은 메시지 1개입니다.
접두사 수명	기본 수명은 2592000초(30일)이며 기본 수명은 604800초(7일)입니다.
온링크 플래그	이 플래그는 기본적으로 켜져 있어 접두사가 알림 인터페이스에서 사용됩니다.
자동 구성 플래그	이 플래그는 기본적으로 켜져 있어 접두사가 자동 컨피그레이션에 사용됩니다.
고정 IPv6 인접 디바이스	고정 엔트리는 IPv6 인접 디바이스 검색 캐시에 구성되지 않습니다.

IPv6 Neighbor Discovery 구성

인터페이스 컨피그레이션 모드 진입

인터페이스별로 인접 디바이스 검색 설정을 구성합니다. 인터페이스 컨피그레이션 모드에 진입하려면 다음 단계를 수행합니다.

세부 단계

명령	목적
interface *name* 예: hostname(config)# interface gigabitethernet 0/0 hostname(config-if)#	인터페이스 컨피그레이션 모드로 진입합니다.

인접 디바이스 요청 메시지 간격 구성

인터페이스에서 IPv6 인접 디바이스 요청 재전송 간격을 구성하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd ns-interval *value* 예: hostname (config-if)# ipv6 nd ns-interval 9000	인터페이스에서 IPv6 인접 디바이스 요청 재전송 간격을 설정합니다. 값 인수로 유효한 값은 1000~3600000밀리초입니다. 이 정보는 라우터 알림 메시지로도 전송됩니다.

예

다음 예는 GigabitEthernet 0/0에 대한 IPv6 인접 디바이스 요청 전송 간격을 9000밀리초로 구성합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ns-interval 9000
```

인접 디바이스 도달 가능 시간 구성

도달 가능성 확인 이벤트 발생 후 원격 IPv6 노드를 도달 가능한 것으로 간주하는 시간을 구성하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd reachable-time *value* 예: hostname (config-if)# ipv6 nd reachable-time 1700000	원격 IPv6 노드가 도달 가능한 시간을 설정합니다. *value* 인수로 유효한 값은 0~3600000밀리초입니다. 값으로 0을 사용하는 경우 도달 가능 시간은 undetermined로 전송됩니다. 도달 가능한 시간 값을 설정하고 추적하는 것은 수신 디바이스에 달려 있습니다.

예

다음 예는 선택한 인터페이스인 GigabitEthernet 0/0에 대해 IPv6 도달 가능 시간을 1700000밀리초로 구성합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd reachable-time 1700000
```

라우터 알림 전송 간격 구성

인터페이스에서 IPv6 라우터 알림 전송 간격을 구성하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd ra-interval [**msec**] *value* **예:** `hostname (config-if)# ipv6 nd ra-interval 201`	IPv6 라우터 알림 전송 사이의 간격을 설정합니다. 선택 사항인 **msec** 키워드는 값을 밀리초 단위로 입력할 것을 나타냅니다. 이 키워드가 없으면 값은 초 단위로 입력됩니다. 유효한 *value* 인수 범위는 3~1800초 또는 **msec** 키워드가 있는 경우 500~1800000밀리초입니다. 전송 사이의 간격은 ASA이(가) 기본 라우터로 구성된 경우 IPv6 라우터 알림 수명보다 적거나 같아야 합니다. 자세한 내용은 25-9 페이지의 라우터 수명 값 구성을 참조하십시오. 다른 IPv6 노드와의 동기화를 방지하려면 사용되는 실제 값을 원하는 값의 20% 범위로 임의로 조정하십시오.

예

다음 예는 선택한 인터페이스인 GigabitEthernet 0/0에 대하여 IPv6 라우터 알림 간격을 201초로 설정합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

라우터 수명 값 구성

인터페이스에서 IPv6 라우터 알림의 라우터 수명 값을 구성하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd ra-lifetime [**msec**] *value* **예:** `hostname (config-if)# ipv6 nd ra-lifetime 2000`	로컬 디스크의 노드가 ASA를 해당 링크의 기본 라우터로 간주해야 하는 시간을 지정합니다. 선택 사항인 **msec** 키워드는 값을 밀리초 단위로 입력할 것을 나타냅니다. 이 키워드가 없으면 값은 초 단위로 입력됩니다. *value* 인수로 유효한 값은 0~9000초입니다. 0을 입력하면 ASA를 선택한 인터페이스에서 기본 라우터로 간주하지 않아야 함을 나타냅니다.

예

다음 예는 선택한 인터페이스인 GigabitEthernet 0/0에 대하여 IPv6 라우터 수명 값을 2000초로 설정합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-lifetime 2000
```

DAD 설정 구성

인터페이스의 DAD 설정을 지정하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd dad attempts *value* **예:** `hostname (config-if)# ipv6 nd dad attempts 20`	새로운 유니캐스트 IPv6 주소의 고유성을 할당 전에 지정하고 링크 단위로 네트워크의 중복 IPv6 주소가 감지되도록 확인합니다. 유효한 *value* 인수 값은 0~600입니다. 값을 0으로 입력하면 지정된 인터페이스에서 DAD 처리가 비활성화됩니다.

예

다음 예는 선택한 인터페이스인 GigabitEthernet 0/0에 대한 DAD 시도 값을 20으로 구성합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd dad attempts 20
```

라우터 알림 메시지 억제

라우터 알림 메시지는 라우터 요청 메시지에 대한 응답으로 자동 전송됩니다. ASA이(가) IPv6 접두사를 전송하길 원치 않는 인터페이스에서 이 메시지를 비활성화할 수 있습니다(예: 인터페이스 외부).

인터페이스에서 IPv6 라우터 알림의 라우터 수명 값을 억제하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd suppress-ra *seconds* **예:** `hostname (config-if)# ipv6 nd suppress-ra 900`	라우터 수명 값을 억제합니다. *seconds* 인수는 이 인터페이스의 기본 라우터로서 ASA의 유효성을 지정합니다. 유효한 값은 0~9000초입니다. 0은 지정된 인터페이스에서 ASA를 기본 라우터로 간주하지 않아야 함을 나타냅니다. 이 명령을 입력하면 ASA가 링크에서 IPv6 라우터가 아닌 일반 IPv6 인접 디바이스로 나타나게 됩니다.

예

다음 예는 지정된 인터페이스인 GigabitEthernet 0/0에 대한 IPv6 라우터 알림 전송을 억제합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd suppress-ra 900
```

IPv6 DHCP 릴레이에 대한 주소 구성 플래그 구성

IPv6 라우터 알림에 플래그를 추가하여 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 IPv6 주소 및/또는 DNS 서버 주소와 같은 추가 정보를 획득하라고 알릴 수 있습니다.

세부 단계

명령	목적
ipv6 nd managed-config-flag **예:** `hostname (config-if)# ipv6 nd managed-config-flag`	IPv6 라우터 알림 패킷에서 Managed Address Config 플래그를 설정합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 주소와 무상태 자동 컨피그레이션 주소를 획득하라고 알려줍니다.
ipv6 nd other-config-flag **예:** `hostname (config-if)# ipv6 nd other-config-flag`	IPv6 라우터 알림 패킷에서 Other Address Config 플래그를 설정합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6에서 DNS 서버 주소와 같은 추가 정보를 획득하라고 알려줍니다.

라우터 알림에서 IPv6 접두사 구성

어떤 IPv6 접두사를 IPv6 라우터 알림에 포함할지 구성하려면 다음 명령을 입력합니다..

세부 단계

명령	목적
ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**] **예:** `hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900`	IPv6 라우터 알림에 포함할 IPv6 접두사를 구성합니다. 인접 디바이스가 접두사 알림을 사용하여 인터페이스 주소를 자동으로 구성할 수 있습니다. 무상태 자동 컨피그레이션은 라우터 알림 메시지에서 제공된 IPv6 접두사를 사용하여 링크-로컬 주소에서 글로벌 유니캐스트 주소를 생성합니다. **at** *valid-date preferred-date* 구문은 수명 및 기본 설정이 만료되는 날짜와 시간을 나타냅니다. 접두사는 지정된 날짜와 시간에 도달할 때까지 유효합니다. 날짜는 *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* 형식으로 표현됩니다. **default** 키워드는 기본값이 사용됨을 나타냅니다. 선택적인 **infinite** 키워드는 유효 수명이 만료되지 않음을 나타냅니다. *ipv6-prefix* 인수는 IPv6 네트워크 숫자가 라우터 알림을 포함하도록 지정합니다. 이 인수는 콜론 사이의 16비트 값을 사용하여 16진수로 주소가 지정된 RFC 2373의 형식이어야 합니다. 선택적인 **no-advertise** 키워드는 로컬 링크의 호스트에게 지정된 접두사가 IPv6 자동 컨피그레이션에 사용되지 않을 것임을 알려줍니다. 선택적인 **no-autoconfig** 키워드는 로컬 링크의 호스트에게 지정된 접두사가 IPv6 자동 컨피그레이션에 사용될 수 없음을 알려줍니다. 선택적인 **off-link** 키워드는 지정된 접두사가 온-링크 결정에 사용되지 않음을 알려줍니다. *preferred-lifetime* 인수는 지정된 IPv6 접두사가 기본값으로 알려지는 시간(초)을 지정합니다. 유효한 값은 0부터 4294967295초입니다. 최대값은 무한대에 해당하며 무한으로 지정될 수도 있습니다. 기본값은 604800(7일)입니다. *prefix-length* 인수는 IPv6 접두사의 길이를 지정합니다. 이 값은 주소에서 얼마나 많은 상위 연속 비트가 접두사의 네트워크 부분을 구성하는지 나타냅니다. 슬래시(/)가 접두사 길이 앞에 와야 합니다. *valid-lifetime* 인수는 지정된 IPv6 접두사가 유효한 접두사로 알려지는 시간을 지정합니다. 유효한 값은 0부터 4294967295초입니다. 최대값은 무한대에 해당하며 무한으로 지정될 수도 있습니다. 기본값은 2592000(30일)입니다.

예

다음 예는 지정된 인터페이스인 GigabitEthernet 0/0에서 전송되는 라우터 알림에서 IPv6 접두사 2001:DB8::/32와 유효한 수명 1000초, 기본 수명 900초를 포함합니다.

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

고정 IPv6 인접 디바이스 구성

IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 구성하려면 다음 명령을 입력합니다.

세부 단계

명령	목적
ipv6 neighbor *ipv6_address if_name mac_address* **예:** `hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472`	IPv6 인접 디바이스 탐색 캐시에서 고정 엔트리를 구성합니다. *ipv6_address* 인수는 인접 디바이스의 링크-로컬 IPv6 주소이고 *if_name* 인수는 인접 디바이스가 제공되는 인터페이스이며 *mac_address* 인수는 인접 디바이스 인터페이스의 MAC 주소입니다.

예

다음 예는 IPv6 주소가 3001:1::45A이고 MAC 주소가 002.7D1a.9472인 내부 호스트에 대한 고정 엔트리를 인접 디바이스 검색 캐시에 추가합니다.

```
hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

IPv6 인접 디바이스 검색 모니터링

IPv6 인접 디바이스 검색 매개 변수를 모니터링하려면 다음 명령을 입력하십시오.

명령	목적
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다. "outside"와 같은 인터페이스 이름을 포함하여 지정된 인터페이스에 대한 설정을 표시합니다. 명령에서 이름을 제외하고 IPv6가 활성화된 모든 인터페이스에 대한 설정을 표시합니다. 명령에 대한 출력이 다음을 표시합니다. • 인터페이스의 이름과 상태 • 링크-로컬 및 글로벌 유니캐스트 주소 • 인터페이스가 속한 멀티캐스트 그룹 • ICMP 리디렉션 및 오류 메시지 설정 • 인접 디바이스 검색 설정 • 명령이 0으로 설정될 때의 실제 시간 • 사용되는 인접 디바이스 검색 도달 가능 시간

추가 참조 자료

IPv6 접두사 구현에 관한 추가 정보는 다음 항목을 참조하십시오.

IPv6 접두사 관련 문서

관련 항목	문서 제목
ipv6 명령	*명령 참조*

IPv6 접두사 및 문서를 위한 RFC

RFC	제목
RFC 2373은 라우터 알림에서 IPv6 네트워크 주소 숫자를 표시하는 방법을 보여주는 전체 문서를 포함합니다. *ipv6-prefix* 명령 인수는 콜론 사이에 16비트 값을 사용하여 16진수 형식으로 주소를 지정해야 하는 네트워크 숫자를 나타냅니다.	IP 버전 6 주소 아키텍처
RFC 3849는 문서에서 IPv6 주소 접두사 사용에 관한 요구 사항을 지정합니다. 문서에서 사용이 예약된 IPv6 유니캐스트 주소 접두사는 2001:DB8::/32입니다.	문서를 위해 예약된 IPv6 주소 접두사

IPv6 인접 디바이스 검색을 위한 기능 내역

표 25-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 25-2 IPv6 인접 디바이스 검색을 위한 기능 내역

기능 이름	릴리스	기능 정보
IPv6 인접 디바이스 검색	7.0(1)	이 기능을 도입했습니다. 도입된 명령: **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**.
IPv6 DHCP 릴레이에 대한 주소 구성 플래그	9.0(1)	도입된 명령: **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**.

7 파 트

AAA 서버 및 로컬 데이터베이스

26 장

AAA 정보

이 장에서는 인증, 권한 부여 및 어카운팅(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.

인증

인증은 액세스를 부여하기 전에 보통 사용자 이름과 비밀번호를 입력하도록 요구하는 방식으로 효과적인 사용자 확인 방법을 제공합니다. AAA 서버는 사용자의 인증 자격 증명을 데이터베이스에 저장된 다른 사용자의 자격 증명과 비교합니다. 자격 증명이 일치하면 사용자는 네트워크에 액세스할 수 있습니다. 자격 증명이 일치하지 않으면, 인증에 실패하고 네트워크 액세스가 거부됩니다.

Cisco ASA이(가) 다음 항목을 인증하도록 구성할 수 있습니다.

- 다음 세션을 포함한ASA 모든 관리 연결:
  - 텔넷
  - SSH
  - 시리얼 콘솔
  - HTTPS를 사용하는 ASDM
  - VPN 관리 액세스
- **enable** 명령어
- 네트워크 액세스
- VPN 접속

권한 부여

승인은 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 항목을 승인하도록 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 승인 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. 인증은 항상 사용자를 먼저 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. 인증은 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.

로컬 데이터베이스 지원

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.

27 장

AAA의 로컬 데이터베이스

이 장에서는 AAA에 로컬 서버를 구성하는 방법에 대해 설명합니다.

로컬 데이터베이스 정보

다음 기능에 로컬 데이터베이스를 사용할 수 있습니다.

- ASDM 사용자당 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 수준을 참조하여 어떤 명령을 사용할 수 있는지 확인합니다. 그렇지 않을 경우 권한 수준은 일반적으로 사용되지 않습니다. 기본적으로 모든 명령의 권한 수준은 0 또는 15입니다.
- 네트워크 액세스 인증
- VPN 클라이언트 인증

다중 컨텍스트 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.

폴백(Fallback) 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(인증 및 권한 부여에만 사용)으로 구성되어 있으면 ASA에서는 로컬 데이터베이스를 사용하려고 시도합니다. 폴백 방법이 없는 경우, ASA에서는 AAA 서버에 대한 시도를 계속 수행합니다.

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 인증 — 그룹의 TACACS+ 서버를 모두 사용할 수 없는 경우, 로컬 데이터베이스를 사용하여 권한 수준을 기준으로 명령을 인증합니다.
- VPN 인증 및 권한 부여 — 정상적으로 VPN 서비스를 지원하는 AAA 서버를 사용할 수 없는 경우, ASA에 원격 액세스할 수 있도록 VPN 인증 및 권한 부여가 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 폴백이 작동하는 방식

서버 그룹에 여러 개의 서버를 구성하고 서버 그룹의 로컬 데이터베이스에 폴백을 사용하도록 설정할 경우, 해당 그룹의 서버가 ASA의 인증 요청에 반응하지 않으면 폴백이 실행됩니다. 명확히 이해하기 위해 다음 시나리오를 가정해 보십시오.

2개의 Active Directory 서버가 서버 1, 서버 2의 순서대로 포함된 LDAP 서버 그룹을 구성합니다. 원격 사용자가 로그인하면 ASA에서는 서버 1에 인증을 시도합니다.

서버 1이 인증 오류에 응답할 경우(예: *사용자가 없음*), ASA에서는 서버 2에 인증을 시도하지 않습니다.

서버 1이 시간 제한 내에 응답하지 않을 경우(또는 인증 시도 횟수가 구성된 최대 횟수를 초과할 경우), ASA에서는 서버 2의 응답을 시도합니다.

그룹의 두 서버가 모두 응답하지 않고 로컬 데이터베이스에 폴백을 수행하도록 ASA가 구성된 경우, ASA에서는 로컬 데이터베이스를 인증하려고 시도합니다.

로컬 데이터베이스에 대한 지침

인증 또는 권한 부여에 로컬 데이터베이스를 사용할 경우 ASA가 잠기는 것을 방지해야 합니다.

관련 주제

35-32 페이지의 잠금에서 복구

로컬 데이터베이스에 사용자 어카운트 추가

로컬 데이터베이스에 사용자를 추가하려면 다음 단계를 수행합니다.

절차

1단계 사용자 어카운트를 생성합니다.

username *username* {**nopassword** | **password** *password*} [**privilege** *priv_level*]

예:

```
ciscoasa(config)# username exampleuser1 privilege 1
```

username *user*name 키워드는 4~64자 길이의 문자열입니다. **password** *password* 키워드는 3~32자 길이의 문자열입니다. **privilege** *priv_level* 키워드에서는 권한 수준을 설정하며 권한 수준의 범위는 0~15입니다. 기본값은 2입니다. 이러한 권한 수준은 명령 인증과 함께 사용됩니다.

주의 명령 인증(**aaa authorization console LOCAL** 명령)을 사용하지 않을 경우, 기본 수준 2에서는 특권 EXEC 모드에 관리 액세스를 허용합니다. 특권 EXEC 모드에 대한 액세스를 제한하려면 권한 수준을 0 또는 1로 설정하거나, **service-type** 명령을 사용합니다.

nopassword 키워드는 비밀번호 없는 사용자 어카운트를 생성합니다. **encrypted** 키워드는 해당 비밀번호가 암호화되었음을 나타냅니다. **username** 명령에서 비밀번호를 정의할 경우, 컨피그레이션에 해당 비밀번호가 저장되면 ASA에서는 보안을 위해 이를 암호화합니다. **show running-config** 명령을 입력하면 **username** 명령에서는 실제 비밀번호를 표시하지 않습니다. 암호화된 비밀번호 뒤에 **encrypted** 키워드가 표시됩니다. 예를 들어 "test"라는 비밀번호를 입력할 경우 다음과 비슷한 내용의 **show running-config** 출력이 표시됩니다.

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

CLI에서 **encrypted** 키워드를 실제로 입력하는 유일한 경우는 다른 ASA에서 사용할 컨피그레이션 파일을 자르기 및 붙여넣기한 다음 동일한 비밀번호를 사용하는 경우입니다.

2단계 (선택 사항) 사용자 이름 속성을 구성합니다.

username *username* **attributes**

예:

```
ciscoasa(config)# username exampleuser1 attributes
```

username 인수는 첫 번째 단계에서 생성한 사용자 이름입니다.

기본적으로 이 명령으로 추가하는 VPN 사용자에게는 속성이나 그룹 정책 연결이 없습니다. **username attributes** 명령을 사용하여 모든 값을 명시적으로 구성해야 합니다. 자세한 내용은 VPN 컨피그레이션 가이드를 참조하십시오.

3단계 (선택 사항) **aaa authorization exec** 명령을 사용하여 관리 권한 부여를 구성한 경우 사용자 수준을 구성합니다.

service-type {**admin** | **nas-prompt** | **remote-access**}

예:

```
ciscoasa(config-username)# service-type admin
```

admin 키워드의 경우 **aaa authentication console LOCAL** 명령으로 지정된 모든 서비스에 완전한 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 컨피그레이션 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).

4단계 사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증을 사용합니다.

ssh authentication {**pkf** | **publickey** *key* [**hashed**]}

예:

```
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-username)#
```

PKF(공개 키 파일) 형식 키(**pkf** 키워드) 또는 Base64 키(**publickey** 키워드)를 지정할 수 있습니다. **publickey**의 경우 *키*는 Base64-인코딩 공개 키입니다. 인증서 없이 SSH-RSA 로 키(raw key)를 생성하는 것이 가능한 SSH 키 생성 소프트웨어(예: ssh keygen)를 사용하여 키를 생성할 수 있습니다.

pkf 키의 경우, 최대 4096비트의 PKF 형식 키로 붙여넣으라는 메시지가 표시됩니다. 이 형식은 키의 크기가 Base64 형식으로 일렬로 붙여넣기에는 너무 클 때 사용합니다. 예를 들어, ssh keygen을 사용하여 4096비트 키를 생성한 후 이를 PKF로 변환하고 **pkf** 키워드를 사용하여 키에 메시지가 표시되도록 합니다.

참고 **pkf** 옵션을 장애 조치와 함께 사용할 수 있으나 PKF 키는 스탠바이 시스템에 자동으로 복제되지 않습니다. PKF 키를 동기화하려면 **write standby** 명령을 입력해야 합니다.

show running-config username 명령을 사용하여 ASA에서 키를 볼 경우, 해당 키는 SHA-256 해시를 사용하여 암호화됩니다. 키를 **pkf**로 입력한 경우에도 ASA에서는 키를 해시하며 이를 해시된 **publickey**로 표시합니다. **show** 출력에서 키를 복사해야 할 경우 **hashed** 키워드로 **publickey** 유형을 지정합니다.

5단계 (선택 사항) 이 사용자 이름을 VPN 인증에 사용할 경우, 사용자에 대한 다양한 VPN 속성을 구성할 수 있습니다. 자세한 내용은 VPN 컨피그레이션 가이드를 참조하십시오.

예

다음 예에서는 권한 수준 15를 관리자 어카운트에 할당합니다.

```
ciscoasa(config)# username admin password password privilege 15
```

다음 예에서는 비밀번호가 없는 사용자 어카운트를 생성합니다.

```
ciscoasa(config)# username user34 nopassword
```

다음 예에서는 관리 권한 부여를 활성화하고, 비밀번호가 있는 사용자 어카운트를 생성하고, 사용자 이름 컨피그레이션 모드를 입력하고, **nas-prompt**의 **service-type**을 지정합니다.

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

다음 예에서는 Linux 또는 Macintosh 시스템에서 SSH용 공유 키를 생성하고 이를 ASA에 가져옵니다.

1단계 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           |
+-----------------+
```

2단계 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$
```

3단계 키를 클립보드에 복사합니다.

4단계 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"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza371B/Q/f1jpLAv1BbyAd5PJCJXh/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.
```

5단계 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>
```

로컬 데이터베이스 모니터링

로컬 데이터베이스를 모니터링하려면 다음 commands를 참조하십시오.

- **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 27-1 로컬 데이터베이스에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
AAA의 로컬 데이터베이스 컨피그레이션	7.0(1)	AAA 사용을 위해 로컬 데이터베이스를 구성하는 방법에 대해 설명합니다. 도입된 명령: **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, aaa authentication {telnet | ssh | serial} console LOCAL**, **aaa authentication http console LOCAL**, **aaa authentication enable console LOCAL**, **show running-config aaa-server**, **show aaa-server**, **clear configure aaa-server**, **clear aaa-server statistics**
SSH 공개 키 인증 지원	9.1(2)	이제 사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증을 사용할 수 있습니다. PKF(공개 키 파일) 형식의 키 또는 Base64 키를 지정할 수 있습니다. PKF 키는 최대 4096비트입니다. ASA의 Base64 형식 지원 범위(최대 2048비트)에 비해 너무 큰 키에는 PKF 형식을 사용합니다. 도입된 명령: **ssh authentication** *8.4(4.1)에서도 사용 가능. PKF 키 형식은 9.1(2)에서만 지원됩니다.*

28 장

AAA를 위한 RADIUS 서버

이 장에서는 AAA를 위한 RADIUS 서버 구성 방법을 설명합니다.

RADIUS 서버에 대한 정보

Cisco ASA는 AAA를 위해 다음의 RFC 규격 RADIUS 서버를 지원합니다.

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2 및 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.
- Authentication Proxy modes—RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS-to-Token 서버 및 RSA/SDI-to-RADIUS 연결에 대해 지원됩니다.

참고 VPN 연결을 위해 ASA 및 RADIUS 서버 사이에 사용되는 프로토콜로 MS-CHAPv2를 활성화하려면 터널 그룹 일반 속성에서 비밀번호 관리가 활성화되어 있어야 합니다. 비밀번호 관리를 활성화하면 ASA에서 RADIUS 서버로 MS-CHAPv2 인증 요청이 생성됩니다. 자세한 내용은 **password-management** 명령 설명을 참조하십시오.

터널 그룹에서 이중 인증을 사용하고 비밀번호 관리를 활성화하는 경우 기본 및 보조 인증 요청은 MS-CHAPv2 요청 속성을 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 설정을 위한 다른 많은 속성도 지원합니다.

지원되는 RADIUS 속성 집합

ASA는 다음 RADIUS 속성 집합을 지원합니다.

- RFC 2138에 정의된 인증 속성
- RFC 2139에 정의된 어카운팅 속성
- RFC 2868에 정의된 터널링된 프로토콜 지원을 위한 RADIUS 속성
- 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
- 1은 최저, 15는 최저 수준을 나타내는 표준 0~15의 숫자 권한 순위를 제공하는 Cisco VSA(Cisco-Priv-Level) 0 수준은 권한이 없음을 나타냅니다. 첫 번째 수준(로그인)은 이 수준에서 이용 가능한 명령에 대해 권한이 있는 EXEC 액세스를 허용합니다. 두 번째 수준(활성화)은 CLI 컨피그레이션 권한을 허용합니다.

지원되는 RADIUS 권한 부여 속성

권한 부여는 권한 또는 속성을 적용하는 프로세스를 가리킵니다. RADIUS 서버는 권한이나 속성이 구성된 경우 이를 적용하는 인증 서버로 정의됩니다. 이러한 속성은 공급업체 ID 3076을 가지고 있습니다.

표 28-1은 사용자 권한 부여에 사용할 수 있는 지원되는 RADIUS 속성을 나열합니다.

참고 RADIUS 속성 이름은 cVPN3000 접두사를 포함하지 않습니다. Cisco Secure ACS 4.x는 이 새로운 명명법을 지원하지만 4.0 이전 ACS 릴리스의 속성은 여전히 cVPN3000 접두사를 포함합니다. ASA은(는) 속성 이름이 아닌 속성 숫자 ID를 기반으로 RADIUS 속성을 적용합니다.

표 28-1의 모든 속성은 146, 150, 151 및 152 속성 번호를 제외하고 RADIUS 서버에서 ASA(으)로 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 속성 146, 150, 151 및 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 프레임드 IP 주소를 지원하지 않습니다.

표 28-1 지원되는 RADIUS 권한 부여 속성

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
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 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	Y	50	정수	단일	1~35791394분
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 = No 1 = 예
Authorization-Type	Y	65	정수	단일	0 = None 1 = RADIUS 2 = LDAP
Banner1	Y	15	문자열	단일	Cisco VPN 원격 액세스 세션에 대해 표시할 배너 문자열: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2 및 Clientless SSL

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
Banner2	Y	36	문자열	단일	Cisco VPN 원격 액세스 세션에 대해 표시할 배너 문자열: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2 및 Clientless SSL Banner2 문자열은 Banner1 문자열로 연결됩니다(구성된 경우).
Cisco-IP-Phone-Bypass	Y	51	정수	단일	0 = Disabled 1 = Enabled
Cisco-LEAP-Bypass	Y	75	정수	단일	0 = Disabled 1 = Enabled
Client Type	Y	150	정수	단일	1 = Cisco VPN Client (IKEv1) 2 = AnyConnect Client SSL VPN 3 = Clientless 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 = Disabled 1 = Enabled
Group-Policy	Y	25	문자열	단일	원격 액세스 VPN 세션에 대한 그룹 정책을 설정합니다. 버전 8.2.x 이상에서는 IETF-Radius-Class 대신 이 속성을 사용하십시오. 다음 형식 중 하나를 사용할 수 있습니다. • *group policy name* • OU=*group policy name* • OU=*group policy name*;
IE-Proxy-Bypass-Local		83	정수	단일	0 = None 1 = Local
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 = No Modify 2 = No Proxy 3 = Auto detect 4 = Use Concentrator Setting
IKE-KeepAlive-Confidence-Interval	Y	68	정수	단일	10~300초
IKE-Keepalive-Retry-Interval	Y	84	정수	단일	2~10초

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
IKE-Keep-Alives	Y	41	부울	단일	0 = Disabled 1 = Enabled
Intercept-DHCP-Configure-Msg	Y	62	부울	단일	0 = Disabled 1 = Enabled
IPsec-Allow-Passwd-Store	Y	16	부울	단일	0 = Disabled 1 = Enabled
IPsec-Authentication		13	정수	단일	0 = None 1 = RADIUS 2 = LDAP(인증 전용) 3 = NT Domain 4 = SDI 5 = Internal 6 = RADIUS with Expiry 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	부울	단일	0 = Disabled 1 = Enabled
IPsec-Backup-Server-List	Y	60	문자열	단일	서버 주소(공백 구분)
IPsec-Backup-Servers	Y	59	문자열	단일	1 = Use Client-Configured list 2 = Disable and clear client list 3 = Use Backup Server list
IPsec-Client-Firewall-Filter-Name		57	문자열	단일	클라이언트에 방화벽 정책으로 푸시할 필터의 이름을 지정
IPsec-Client-Firewall-Filter-Optional	Y	58	정수	단일	0 = Required 1 = Optional
IPsec-Default-Domain	Y	28	문자열	단일	클라이언트로 보낼 단일 기본 도메인 이름을 지정합니다(1~255자).
IPsec-IKE-Peer-ID-Check	Y	40	정수	단일	1 = Required 2 = If supported by peer certificate 3 = Do not check
IPsec-IP-Compression	Y	39	정수	단일	0 = Disabled 1 = Enabled
IPsec-Mode-Config	Y	31	부울	단일	0 = Disabled 1 = Enabled
IPsec-Over-UDP	Y	34	부울	단일	0 = Disabled 1 = Enabled
IPsec-Over-UDP-Port	Y	35	정수	단일	4001- 49151. 기본값은 10000입니다.
IPsec-Required-Client-Firewall-Capability	Y	56	정수	단일	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = Policy from server
IPsec-Sec-Association		12	문자열	단일	보안 연결의 이름

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
IPsec-Split-DNS-Names	Y	29	문자열	단일	클라이언트로 보낼 보조 도메인 이름의 목록을 지정합니다(1~255자).
IPsec-Split-Tunneling-Policy	Y	55	정수	단일	0 = No split tunneling 1 = Split tunneling 2 = Local LAN permitted
IPsec-Split-Tunnel-List	Y	27	문자열	단일	분할 터널 포함 목록을 설명하는 네트워크 또는 ACL의 이름을 지정합니다.
IPsec-Tunnel-Type	Y	30	정수	단일	1 = LAN-to-LAN 2 = Remote access
IPsec-User-Group-Lock		33	부울	단일	0 = Disabled 1 = Enabled
IPv6-Address-Pools	Y	218	문자열	단일	IP 로컬 풀-IPv6의 이름
IPv6-VPN-Filter	Y	219	문자열	단일	ACL 가치
L2TP-Encryption		21	정수	단일	비트맵: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Req 15= 40/128-Encr/Stateless-Req
L2TP-MPPC-Compression		38	정수	단일	0 = Disabled 1 = Enabled
Member-Of	Y	145	문자열	단일	쉼표로 구분된 문자열, 예: 엔지니어링, 판매 동적 액세스 정책에서 사용할 수 있는 관리 속성입니다. 이것은 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 = No 1 = 예
NAC-Revalidation-Timer		91	정수	단일	300~86400초
NAC-Settings	Y	141	문자열	단일	NAC 정책의 이름
NAC-Status-Query-Timer		90	정수	단일	30~1800초
Perfect-Forward-Secrecy-Enable	Y	88	부울	단일	0 = No 1 = 예

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
PPTP-Encryption		20	정수	단일	비트맵: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Required 15= 40/128-Encr/Stateless-Req
PPTP-MPPC-Compression		37	정수	단일	0 = Disabled 1 = Enabled
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 포함) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems(Cisco Intrusion Prevention Security Agent 포함)
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 = Disabled 1 = Enabled
Require-HW-Client-Auth	Y	48	부울	단일	0 = Disabled 1 = Enabled
Secondary-DNS	Y	6	문자열	단일	IP 주소
Secondary-WINS	Y	8	문자열	단일	IP 주소
SEP-Card-Assignment		9	정수	단일	사용되지 않음

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
세션 하위 유형	Y	152	정수	단일	0 = None 1 = Clientless 2 = Client 3 = Client Only 세션 하위 유형은 세션 유형(151) 속성에 1, 2, 3, 4의 값이 포함될 때만 적용됩니다.
Session Type	Y	151	정수	단일	0 = None 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN (IKEv2) 3 = Clientless SSL VPN 4 = Clientless Email Proxy 5 = Cisco VPN Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN Load Balancing
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 = Disabled 1 = Enabled 2 = AutoStart
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 = Disabled 1 = Enabled
SVC-Ask	Y	131	문자열	단일	0 = Disabled 1 = Enabled 3 = Enable default service 5 = Enable default clientless (2 및 4는 사용되지 않음)
SVC-Ask-Timeout	Y	132	정수	단일	5~120초
SVC-DPD-Interval-Client	Y	108	정수	단일	0 = Off 5~3600초
SVC-DPD-Interval-Gateway	Y	109	정수	단일	0 = Off) 5~3600초
SVC-DTLS	Y	123	정수	단일	0 = False 1 = True
SVC-Keepalive	Y	107	정수	단일	0 = Off 15~600초
SVC-Modules	Y	127	문자열	단일	문자열(모듈 이름)
SVC-MTU	Y	125	정수	단일	MTU 가치 256~1406바이트

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
SVC-Profiles	Y	128	문자열	단일	문자열(프로필 이름)
SVC-Rekey-Time	Y	110	정수	단일	0 = Disabled 1~10080분
터널 그룹 이름	Y	146	문자열	단일	1~253자
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) 8과 4는 함께 사용할 수 없습니다. 0 - 11, 16 - 27, 32 - 43, 48 - 59는 올바른 값입니다.
Use-Client-Address		17	부울	단일	0 = Disabled 1 = Enabled
VLAN	Y	140	정수	단일	0-4094
WebVPN-Access-List	Y	73	문자열	단일	Access-List 이름
WebVPN ACL	Y	73	문자열	단일	디바이스의 WebVPN ACL 이름
WebVPN-ActiveX-Relay	Y	137	정수	단일	0 = Disabled Otherwise = Enabled
WebVPN-Apply-ACL	Y	102	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Auto-HTTP-Signon	Y	124	문자열	단일	예약
WebVPN-Citrix-Metaframe-Enable	Y	101	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Content-Filter-Parameters	Y	69	정수	단일	1 = Java ActiveX 2 = Java Script 4 = Image 8 = Cookies in images
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	올바른 문자열(최대 500 자)
WebVPN-Download_Max-Size	Y	157	정수	단일	0x7fffffff
WebVPN-File-Access-Enable	Y	94	정수	단일	0 = Disabled 1 = Enabled
WebVPN-File-Server-Browsing-Enable	Y	96	정수	단일	0 = Disabled 1 = Enabled

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
WebVPN-File-Server-Entry-Enable	Y	95	정수	단일	0 = Disabled 1 = Enabled
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)
WebVPN-Hidden-Shares	Y	126	정수	단일	0 = None 1 = Visible
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	부울	단일	클라이언트리스 홈페이지가 스마트 터널을 통해 만들어지는 경우 활성화됩니다.
WebVPN-HTML-Filter	Y	69	비트맵	단일	1 = Java ActiveX 2 = Scripts 4 = Image 8 = Cookies
WebVPN-HTTP-Compression	Y	120	정수	단일	0 = Off 1 = Deflate Compression
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 = Disabled.
WebVPN-Keepalive-Ignore	Y	121	정수	단일	0-900
WebVPN-Macro-Substitution	Y	223	문자열	단일	무제한. 다음 URL의 *SSL VPN 배포 가이드*에서 예제를 참조하십시오. http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution	Y	224	문자열	단일	무제한. 다음 URL의 *SSL VPN 배포 가이드*에서 예제를 참조하십시오. http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Enable	Y	97	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-List	Y	72	문자열	단일	포트 전달 목록 이름

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
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 = Disabled.
WebVPN Smart-Card-Removal-Disconnect	Y	225	부울	단일	0 = Disabled 1 = Enabled
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 = Disabled 1 = Enabled 2 = Auto Start
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	문자열	단일	"e networkname," "i networkname," 또는 "a" 중 하나로 여기서 networkname은 Smart Tunnel 네트워크 목록의 이름을, e는 제외된 터널을, i는 지정된 터널을, a는 모든 터널을 나타냅니다.
WebVPN-SSL-VPN-Client-Enable	Y	103	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Required	Y	104	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SSO-Server-Name	Y	114	문자열	단일	올바른 문자열
WebVPN-Storage-Key	Y	162	문자열	단일	
WebVPN-Storage-Objects	Y	161	문자열	단일	
WebVPN-SVC-Keepalive-Frequency	Y	107	정수	단일	15~600초, 0=Off
WebVPN-SVC-Client-DPD-Frequency	Y	108	정수	단일	5~3600초, 0=Off
WebVPN-SVC-DTLS-Enable	Y	123	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SVC-DTLS-MTU	Y	125	정수	단일	MTU 값은 256~1406바이트입니다.
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	정수	단일	5~3600초, 0=Off
WebVPN-SVC-Rekey-Time	Y	110	정수	단일	4~10080분, 0=Off
WebVPN-SVC-Rekey-Method	Y	111	정수	단일	0 (Off), 1 (SSL), 2 (New Tunnel)
WebVPN-SVC-Compression	Y	112	정수	단일	0 (Off), 1 (Deflate Compression)
WebVPN-UNIX-Group-ID (GID)	Y	222	정수	단일	유효한 UNIX 그룹 ID

표 28-1 지원되는 RADIUS 권한 부여 속성(계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
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 = Disabled 1 = Enabled
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

표 28-2는 지원되는 IETF RADIUS 속성을 나열합니다.

표 28-2 지원되는 IETF RADIUS 속성

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
IETF-Radius-Class	Y	25		단일	버전 8.2.x 이상에서는 표 28-1의 설명대로 Group-Policy 속성(VSA 3076, #25)을 사용하십시오. • *group policy name* • OU=*group policy name* • OU=*group policy name*
IETF-Radius-Filter-Id	Y	11	문자열	단일	ASA에 정의된 ACL 이름으로 풀 터널 IPsec 및 SSL VPN 클라이언트에만 적용됩니다.
IETF-Radius-Framed-IP-Address	Y	N/A	문자열	단일	IP 주소
IETF-Radius-Framed-IP-Netmask	Y	N/A	문자열	단일	IP 주소 마스크
IETF-Radius-Idle-Timeout	Y	28	정수	단일	초
IETF-Radius-Service-Type	Y	6	정수	단일	초 사용 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	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
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

RADIUS 서버의 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

추가 지침

- 단일 모드로 최대 100개의 서버 그룹 또는 다중 모드로 컨텍스트당 4개의 서버 그룹을 포함할 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다.
- 로컬 데이터베이스를 이용하여 폴백 지원을 구성해야 하는 경우 27-2 페이지의 폴백(Fallback) 지원 및 27-2 페이지의 그룹의 여러 서버에서 폴백이 작동하는 방식을 참조하십시오.
- RADIUS 인증을 이용할 때 ASA에서 잠금을 방지하려면 35-32 페이지의 잠금에서 복구를 참조하십시오.

RADIUS 서버 구성

RADIUS 서버 구성을 위한 작업 흐름

1단계 RADIUS 서버로 ASA 속성을 로드합니다. 속성을 로드하는 데 사용하는 방법은 사용하는 RADIUS 서버 유형에 따라 다릅니다.

- Cisco ACS를 사용하는 경우: 서버에 이미 이러한 속성이 통합되어 있습니다. 이 단계를 건너뛸 수 있습니다.
- 다른 공급업체의 RADIUS 서버(예: Microsoft Internet Authentication Service): 각 ASA 속성을 수동으로 정의해야 합니다. 속성을 정의하려면 속성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

2단계 RADIUS 서버 그룹을 추가합니다. 28-15 페이지의 RADIUS 서버 그룹 구성을 참조하십시오.

3단계 서버 그룹의 경우 그룹에 서버를 추가합니다. 28-18 페이지의 그룹에 RADIUS 서버 추가를 참조하십시오.

RADIUS 서버 그룹 구성

인증, 권한 부여 또는 어카운팅을 위해 외부 RADIUS 서버를 사용하려면 먼저 RADIUS 프로토콜당 최소 1개의 AAA 서버 그룹을 만들고 하나 이상의 서버를 각 그룹에 추가해야 합니다. AAA 서버 그룹은 이름으로 구분합니다.

RADIUS 서버 그룹을 추가하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**aaa-server** *server_tag* **protocol radius** 예: `ciscoasa(config)# aaa-server servergroup1 protocol radius` `ciscoasa(config-aaa-server-group)#`	서버 그룹 이름과 프로토콜을 지정합니다. **aaa-server protocol** 명령을 입력하면 aaa-server 서버 컨피그레이션 모드가 됩니다.
2단계	**merge-dacl** {**before-avpair** | **after-avpair**} 예: `ciscoasa(config)# aaa-server servergroup1 protocol radius` `ciscoasa(config-aaa-server-group)# merge-dacl before-avpair`	RADIUS 패킷에서 Cisco AV 쌍으로 수신된 ACL과 다운로드 가능한 ACL을 병합합니다. 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 엔트리를 Cisco AV 쌍 엔트리보다 먼저 배치해야 함을 지정합니다. **after-avpair** 옵션은 다운로드 가능한 ACL 엔트리를 Cisco AV 쌍 엔트리보다 나중에 배치해야 함을 지정합니다. 이 옵션은 VPN 연결에만 적용됩니다. VPN 사용자의 경우 ACL은 Cisco AV 쌍 ACL, 다운로드 가능한 ACL, ASA에 구성된 ACL의 형태로 존재할 수 있습니다. 이 옵션은 다운로드 가능한 ACL과 AV 쌍 ACL의 병합 여부를 결정하며 ASA에 구성된 ACL에는 적용되지 않습니다.
3단계	**max-failed-attempts** *number* 예: `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	다음 서버를 시도하기 전에 그룹의 RADIUS 서버로 보낼 수 있는 최대 요청 횟수를 지정합니다. *number* 인수는 1~5입니다. 기본값은 3입니다. 로컬 데이터베이스를 사용하여 대체 수단을 구성한 경우(관리 액세스만 해당) 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 수단을 시도합니다. 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.

	명령	목적
4단계	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} 예: ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20	그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다. **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. 기본값은 10분입니다. **timed** 키워드는 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.
5단계	**accounting-mode simultaneous** 예: ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	그룹의 모든 서버에 어카운팅 메시지를 전송합니다. 활성 서버로만 메시지를 전송하는 기본 설정을 복원하려면 **accounting-mode single** 명령을 입력합니다.
6단계	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* 예: ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1	서버 및 그 서버가 속한 AAA 서버 그룹을 지정합니다. **aaa-server host** 명령을 입력하면 aaa-server 호스트 컨피그레이션 모드가 됩니다.
7단계	**dynamic-authorization** {port *port-number*} 예: (config-aaa-server-group)# dynamic-authorization port 1700	AAA 서버 그룹에 대한 RADIUS Dynamic Authorization(CoA) 서비스를 활성화합니다. 일단 정의되면 해당 RADIUS 서버 그룹이 CoA 알림에 등록되고 ASA가 ISE로부터 CoA 정책 업데이트를 위해 포트를 청취합니다. CoA listening *port-number*의 유효한 값 범위는 1~65535입니다. 이 명령의 'no' 형식으로 지정된 포트 번호나 인터페이스가 현재 컨피그레이션의 라인과 일치하지 않으면 오류 메시지가 표시됩니다.
8단계	**authorize-only** 예: (config-aaa-server-group)# authorize-only	RADIUS 서버 그룹을 위한 authorize-only 모드를 활성화합니다. 이것은 이 서버 그룹이 권한 부여에 사용될 때 RADIUS Access Request 메시지가 현재 이용 가능한 구성된 비밀번호 방식이 아니라 "Authorize Only" 요청으로 작성됨을 의미합니다. Authorize-Only 요청은 Authorize-Only (17) 값을 가진 Service-Type 속성과 Access-Request 내의 메시지 인증자를 포함합니다. authorize-only 모드 지원으로 RADIUS 공통 비밀번호를 Access-Request에 포함할 필요가 없습니다. 따라서 aaa-server-host 모드에서 radius-common-pw CLI를 사용하여 공통 비밀번호를 구성할 필요가 없습니다. **참고** authorize-only 모드는 서버 그룹에 대해 구성되는 반면 공통 비밀번호는 호스트별로 구성됩니다. 따라서 authorize-only 모드가 일단 구성되면 개별 AAA 서버에 대해 구성된 공통 비밀번호는 무시됩니다.

	명령	목적
9단계	**without-csd** {**anyconnect**} 예: (config-tunnel-webvpn)# without-csd anyconnect	구체적인 터널 그룹에 대한 연결을 위한 호스트 스캔 처리를 끕니다. 현재 이 설정은 클라이언트리스 및 L3 연결에 적용됩니다. 이 명령은 AnyConnect 연결에만 이 설정을 적용할 수 있도록 수정되었습니다.
10단계	**interim-accounting-update** {periodic *interval*} 예: (config-aaa-server-group)# interim-accounting-update periodic 12	RADIUS interim-accounting-update 메시지 생성을 활성화합니다. 현재 이 메시지는 VPN 터널 연결이 클라이언트리스 VPN 세션에 추가될 때만 생성됩니다. 이 경우 어카운팅 업데이트가 생성되어 RADIUS 서버에 새로 할당된 IP 주소를 알려줍니다. 어카운팅 메시지를 지정된 서버 그룹으로 보내도록 구성된 모든 세션에 대해 현재 기능을 허용하거나 주기적인 임시 어카운팅 업데이트 생성을 허용하도록 구성하기 위하여 이 명령에 키워드가 추가되었습니다. *periodic* - 이 키워드 옵션은 어카운팅 레코드를 문제의 서버 그룹으로 보내도록 구성된 모든 VPN 세션을 위한 어카운팅 레코드의 주기적인 생성과 전송을 가능하게 합니다. *interval* - 주기적인 어카운팅 업데이트 사이의 간격을 시간 단위로 나타내는 숫자입니다. 유효한 값 범위는 1~120이고 기본값은 24입니다.

예

다음 예는 단일 서버를 가진 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 권한 부여 전용, 동적 권한 부여(CoA) 업데이트 및 시간별 어카운팅을 위한 ISE 서버 객체 구성 방법을 보여줍니다.

```
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-group)# authorize-only
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
```

다음 예는 ISE를 통한 비밀번호 인증을 위해 터널 그룹을 구성하는 방법을 보여줍니다.

```
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 로컬 인증서 확인과 ISE 권한 부여를 위해 터널 그룹을 구성하는 방법을 보여줍니다.

```
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

RADIUS 서버를 그룹에 추가하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* 예: `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	RADIUS 서버와 그것이 속한 AAA 서버 그룹을 식별합니다. **aaa-server host** 명령을 입력하면 aaa-server 호스트 컨피그레이션 모드가 됩니다.
2단계	**acl-netmask-convert** {**auto-detect** | **standard** | **wildcard**} 예: `ciscoasa(config-aaa-server-host)# acl-netmask-convert standard`	ASA가 **aaa-server host** 명령을 사용하여 액세스되는 RADIUS 서버의 다운로드 가능 ACL로부터 수신한 넷마스크를 취급하는 방법을 지정합니다. **auto-detect** 키워드는 ASA가 사용된 넷마스크 표현의 유형 파악을 시도하도록 지정합니다. ASA가 와일드카드 넷마스크 표현을 발견하면 이를 표준 넷마스크 표현으로 변환합니다. **standard** 키워드는 ASA가 RADIUS 서버에서 수신한 다운로드 가능 ACL이 표준 넷마스크 표현만 포함하는 것으로 간주함을 지정합니다. 와일드카드 넷마스크 표현에 대한 변환이 이루어지지 않습니다. **wildcard** 키워드는 ASA가 RADIUS 서버에서 수신한 다운로드 가능 ACL이 와일드카드 넷마스크 표현만 포함하는 것으로 간주하고 ACL이 다운로드될 때 이를 모두 표준 넷마스크 표현으로 변환하도록 지정합니다.
3단계	**radius-common-pw** *string* 예: `ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc`	ASA를 통해 RADIUS 권한 부여 서버에 액세스하는 모든 사용자에 대해 사용되는 공통 비밀번호를 지정합니다. *string* 인수는 대/소문자를 구분하는 최대 127자의 영숫자 키워드로 RADIUS 서버와의 모든 권한 부여 트랜잭션에 대한 공통 비밀번호로 사용됩니다.
4단계	**mschapv2-capable** 예: `ciscoasa(config-aaa-server-host)# mschapv2-capable`	RADIUS 서버로의 MS-CHAPv2 인증 요청을 활성화합니다.
5단계	**timeout** *hh:mm:ss* 예: `ciscoasa(config-aaa-server-host)# timeout 15`	ASA가 백업 서버로 요청을 보내기 전에 기본 서버에서 응답을 기다리는 시간을 초 단위로 지정합니다.

	명령	목적
6단계	**retry-interval** *seconds* 예: ciscoasa(config-aaa-server-host)# retry-interval 8	이전 **aaa-server host** 명령에서 지정된 특정 AAA 서버를 위한 재시도 사이의 간격을 구성합니다. *seconds* 인수는 요청에 대한 재시도 간격(1~10초)을 지정합니다. 연결 요청을 재시도하기 전에 ASA가 대기하는 시간입니다. **참고** 다음 재시도까지의 간격은 입력한 재시도 간격 설정과 무관하게 항상 50 또는 100밀리초입니다. 이것은 의도된 것입니다.
7단계	**accounting-mode simultaneous** 예: ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	그룹의 모든 서버에 어카운팅 메시지를 전송합니다. 활성 서버로만 메시지를 전송하는 기본 설정을 복원하려면 **accounting-mode single** 명령을 입력합니다.
8단계	**authentication-port** *port* 예: ciscoasa(config-aaa-server-host)# authentication-port 1645	인증 포트를 포트 번호 1645 또는 사용자 인증에 사용되는 서버 포트로 지정합니다.
9단계	**accounting-port** *port* 예: ciscoasa(config-aaa-server-host)# accounting-port 1646	어카운팅 포트를 포트 번호 1646 또는 이 호스트에 대한 어카운팅에 사용되는 서버 포트로 지정합니다.
10단계	**key** 예: ciscoasa(config-aaa-host)# key myexamplekey1	RADIUS 서버를 ASA에 인증하는 데 사용하는 서버 비밀번호를 지정합니다. 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)#
```

RADIUS 서버 모니터링

RADIUS 서버를 모니터링하려면 다음 명령 중 하나를 입력합니다.

Command	목적
show aaa-server	구성된 RADIUS 서버 통계를 보여줍니다. RADIUS 서버 컨피그레이션을 지우려면 **clear aaa-server statistics** 명령을 입력합니다.
show running-config aaa-server	컨피그레이션을 실행 중인 RADIUS 서버를 보여줍니다. RADIUS 서버 통계를 지우려면 **clear configure aaa-server** 명령을 입력합니다.

추가 참조 자료

RADIUS 서버를 통한 AAA 구현에 관한 추가 정보는 28-20 페이지의 RFC에서 참조하십시오.

RFC

RFC	제목
2138	*원격 인증 다이얼-인 사용자 서비스(RADIUS)*
2139	*RADIUS 어카운팅*
2548	*Microsoft 공급업체별 RADIUS 속성*
2868	*터널 프로토콜 지원을 위한 RADIUS 속성*

RADIUS 서버에 대한 기능 내역

표 28-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 28-3 RADIUS 서버에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
AAA를 위한 RADIUS 서버	7.0(1)	AAA에 대한 RADIUS 서버를 구성하는 방법을 설명합니다. 도입된 명령: **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**.

표 28-3 RADIUS 서버에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
ASA에서 RADIUS 액세스 요청 및 어카운팅 요청 패킷으로 전송되는 주요 VSA(vendor-specific attribute)	8.4(3)	4개의 새로운 VSA—Tunnel Group Name (146) 및 Client Type (150)은 ASA에서 RADIUS 액세스 요청 패킷으로 전송됩니다. Session Type (151) 및 Session Subtype (152)은 ASA에서 RADIUS 어카운팅 요청 패킷으로 전송됩니다. 4가지 속성은 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 속성을 시행하거나 이를 어카운팅 및 청구 목적으로 사용할 수 있습니다.

29 장

AAA용 TACACS+ 서버

이 장에서는 AAA에서 사용되는 TACACS+ 서버 구성 방법을 설명합니다.

TACACS+ 서버에 관한 정보

ASA는 ASCII, PAP, CHAP 및 MS-CHAPv1 프로토콜을 통한 TACACS+ 서버 인증을 지원합니다.

TACACS+ 속성 사용

Cisco ASA 는 TACACS+ 속성을 지원합니다. TACACS+ 속성은 인증・권한 검증・과금 기능을 분리합니다. 이 프로토콜은 필수 및 선택의 두 가지 속성 유형을 지원합니다. 서버와 클라이언트가 모두 필수 속성을 이해해야 하고 필수 속성이 사용자에게 적용되어야 합니다. 선택 속성은 이해 또는 사용될 수도 있고 그렇지 않을 수도 있습니다.

참고 TACACS+ 속성을 사용하려면 NAS에서 AAA 서비스를 활성화해야 합니다.

표 29-1은 cut-through-proxy 연결을 위한 지원되는 TACACS+ 권한 부여 응답 속성을 나열합니다. 표 29-2는 지원되는 TACACS+ 과금 특성을 나열합니다.

표 29-1 지원되는 TACACS+ 권한 부여 응답 특성

특성	설명
ACL	연결에 적용할 로컬로 구성된 ACL을 식별합니다.
idletime	비활성 상태가 몇 분간 지속되면 인증된 사용자 세션을 종료할지 나타냅니다.
timeout	인증된 사용자 세션을 종료하기 전에 인증 자격 증명을 활성 상태로 유지할 절대적인 시간(분)을 지정합니다.

표 29-2 이(가) 지원되는 TACACS+ 과금 특성

특성	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 과금만 해당).
disc-cause	연결이 끊긴 원인을 식별하는 숫자 코드를 나타냅니다(중단 레코드만 해당).
elapsed_time	연결에 대한 경과 시간을 초로 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 포트	해당 연결을 위한 세션 ID를 포함합니다.
packs_in	이 연결 중에 전송되는 입력 패킷의 수를 지정합니다.
packs_out	이 연결 중에 전송되는 출력 패킷의 수를 지정합니다.
priv-level	명령 과금 요청에 대한 사용자 권한 수준으로 설정합니다. 아니면 1로 설정됩니다.
rem_iddr	클라이언트의 IP 주소를 나타냅니다.
제공	사용하는 서비스를 지정합니다. 명령 과금에 한해 항상 "shell"로 설정합니다.
task_id	과금 거래에 대한 고유한 작업 ID를 지정합니다.
username	사용자의 이름을 나타냅니다.

TACACS+ 서버의 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base License

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

상황 모드 지침

단일 및 다중 상황 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

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.
- 로컬 데이터베이스를 이용하여 폴백 지원을 구성해야 하는 경우 27-2 페이지의 폴백(Fallback) 지원 및 27-2 페이지의 그룹의 여러 서버에서 폴백이 작동하는 방식을 참조하십시오.
- TACACS+ 인증 또는 권한 부여를 이용할 때 ASA에서 잠금을 방지하려면 35-32 페이지의 잠금에서 복구를 참조하십시오.

TACACS+ 서버 구성

TACACS+ 서버 구성을 위한 작업 흐름

1단계 TACACS+ 서버 그룹을 추가합니다. 29-3 페이지의 TACACS+ 서버 그룹 구성을 참조하십시오.

2단계 서버 그룹의 경우 그룹에 서버를 추가합니다. 29-5 페이지의 그룹에 TACACS+ 서버 추가를 참조하십시오.

TACACS+ 서버 그룹 구성

인증, 권한 검증, 과금을 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 수행하십시오.

세부 단계

	명령	목적
1단계	**aaa-server** *server_tag* **protocol tacacs+** 예: `ciscoasa(config)# aaa-server servergroup1 protocol tacacs+` `ciscoasa(config-aaa-server-group)#`	서버 그룹 이름과 프로토콜을 지정합니다. **aaa-server protocol** 명령을 입력하면 aaa-server 서버 컨피그레이션 모드가 됩니다.

	명령	목적
2단계	**max-failed-attempts** *number* 예: ciscoasa(config-aaa-server-group)# max-failed-attempts 2	다음 서버를 시도하기 전에 그룹의 AAA 서버로 보낼 수 있는 최대 요청 횟수를 지정합니다. *number* 인수는 1~5입니다. 기본값은 3입니다. 로컬 데이터베이스를 사용하여 대체 수단을 구성한 경우(관리 액세스만 해당) 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 수단을 시도합니다. 서버 그룹은 10분(기본값) 동안 무응답으로 표시됩니다. 이 기간에 다른 AAA 요청에서 서버 그룹 접속을 시도하지 않도록 하기 위한 것이며 대비책이 즉시 사용됩니다. 무응답 기간을 기본값이 아닌 값으로 변경하려면 다음 단계의 **reactivation-mode** 명령을 참조하십시오. 대비책이 없는 경우 ASA는 그룹의 서버를 계속 재시도합니다.
3단계	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} 예: ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20	그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다. **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. 기본값은 10분입니다. **timed** 키워드는 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.
4단계	**accounting-mode simultaneous** 예: ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	그룹의 모든 서버에 과금 메시지를 전송합니다. 활성 서버로만 메시지를 전송하는 기본 설정을 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

TACACS+ 서버를 그룹에 추가하려면 다음 단계를 수행하십시오.

세부 단계

	명령	목적
1단계	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* 예: `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	TACACS+ 서버와 그것이 속한 서버 그룹을 식별합니다. **aaa-server host** 명령을 입력하면 aaa-server 호스트 컨피그레이션 모드가 됩니다.
2단계	**timeout** *hh:mm:ss* 예: `ciscoasa(config-aaa-server-host)# timeout 15`	ASA가 백업 서버로 요청을 보내기 전에 기본 서버에서 응답을 기다리는 시간을 초 단위로 지정합니다.
3단계	**server-port** *port_number* 예: `ciscoasa(config-aaa-server-host)# server-port 49`	서버 포트를 포트 번호 49로 지정하거나 ASA에서 TACACS+ 서버와 통신에 사용하는 TCP 포트 번호로 지정합니다.
4단계	**key** 예: `ciscoasa(config-aaa-host)# key myexamplekey1`	TACACS+ 서버에서 NAS를 인증하는 데 사용하는 서버 비밀 값을 지정합니다. 이 값은 대/소문자를 구별하는 최대 127자의 영숫자 키워드로 TACACS+ 서버의 키와 같은 값입니다. 127자 이상의 문자는 무시됩니다. 키는 클라이언트와 서버 사이에서 데이터 암호화에 사용되며 클라이언트와 서버 시스템에서 동일해야 합니다. 키는 공백을 포함할 수 없지만 다른 특수 문자는 허용됩니다.

TACACS+ 서버 모니터링

TACACS+ 서버를 모니터링하려면 다음 명령 중 하나를 입력합니다.

Command	목적
show aaa-server	구성된 TACACS+ 서버 통계를 보여줍니다. TACACS+ 서버 컨피그레이션을 지우려면 **clear aaa-server statistics** 명령을 입력합니다.
show running-config aaa-server	컨피그레이션을 실행 중인 TACACS+ 서버를 보여줍니다. TACACS+ 서버 통계를 지우려면 **clear configure aaa-server** 명령을 입력합니다.

TACACS+ 서버에 대한 기능 내역

표 29-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 29-3 TACACS+ 서버에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
TACACS+ 서버	7.0(1)	AAA에 대한 TACACS+ 서버를 구성하는 방법을 설명합니다. 도입된 명령: **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**.

30 장

AAA를 위한 LDAP 서버

이 장에서는 AAA에서 사용되는 LDAP 서버의 구성 방법을 설명합니다.

LDAP 및 AAA에 대한 정보

Cisco ASA는 다음을 포함하여 대부분의 LDAPv3 디렉토리 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 디렉토리 서버와의 연결 여부를 자동으로 감지합니다. 그러나 자동 감지 기능에서 LDAP 서버 유형을 확인하지 못한 경우 수동으로 구성할 수 있습니다.

LDAP 서버 지침

LDAP 서버를 구성할 때 다음 지침에 유의하십시오.

- Sun 디렉토리 서버에 액세스하기 위해 ASA에 구성된 DN은 그 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 DN과 같은 디렉토리 관리자 권한이 있는 사용자를 이용하는 것이 좋습니다. 또는 기본 비밀번호 정책에 ACL을 포함할 수 있습니다.
- Microsoft Active Directory 및 Sun 서버로 비밀번호를 관리할 수 있도록 SSL을 통한 LDAP을 구성해야 합니다.
- ASA에서는 Novell, OpenLDAP, 기타 LDAPv3 디렉토리 서버를 사용한 비밀번호 관리를 지원하지 않습니다.

- VPN 3000 집중 디바이스와 ASA/PIX 7.0 소프트웨어는 권한 부여 작업에 Cisco LDAP 스키마가 필요했습니다. 버전 7.1.x부터 ASA는 기본 LDAP 스키마를 사용하여 인증 및 권한 부여를 수행하므로 Cisco 스키마가 더 이상 필요하지 않습니다.

인증에서의 LDAP 사용

ASA는 인증 과정에서 해당 사용자의 LDAP 서버에 대한 클라이언트 프록시의 역할을 하며, 일반 텍스트로 또는 SASL 프로토콜을 사용하여 LDAP 서버에 인증합니다. 기본적으로 ASA는 일반 텍스트 형식으로 인증 매개 변수(대개 사용자 이름과 비밀번호)를 LDAP 서버에 전달합니다.

ASA는 강도가 낮은 순서로 나열된 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 이 SASL 메커니즘의 어떤 조합도 지원합니다. 여러 메커니즘을 구성한 경우, ASA는 그 서버에 구성된 SASL 메커니즘의 목록을 검색하고 ASA 및 서버 모두에 구성된 가장 강력한 것으로 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 LDAP을 사용하면 단일 단계에서 인증과 권한 부여가 이루어집니다.

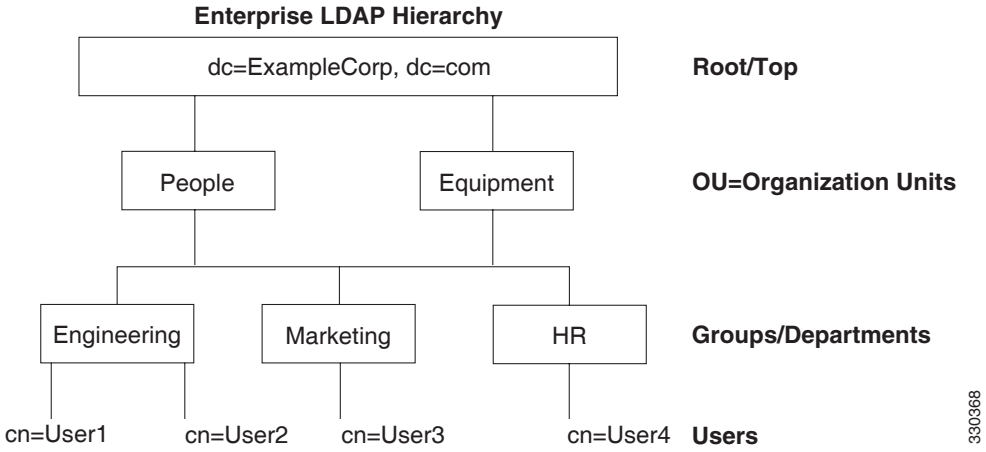
참고 LDAP 프로토콜에 대한 자세한 내용은 RFC 1777, 2251, 2849를 참조하십시오.

LDAP 계층 구조 소개

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 그림 30-1을 참조하십시오.

다단계 계층 구조가 더 상세한 내용을 포함하지만, 검색 결과는 단일 단계 계층 구조에서 더 빨리 얻을 수 있습니다.

그림 30-1 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 DN은 서버가 ASA로부터 권한 부여 요청을 받았을 때 LDAP 계층 구조의 어디에서 사용자 정보 검색을 시작할 것인가를 정의합니다.
- Search Scope는 LDAP 계층 구조에서 검색의 범위를 정의합니다. 검색에서는 계층 구조상 LDAP Base 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)는 LDAP 서버의 항목을 고유하게 식별하는 RDN을 정의합니다. cn(Common Name), sAMAccountName, userPrincipalName과 같은 명명 특성이 주로 사용됩니다.

그림 30-1에서는 Example Corporation의 샘플 LDAP 계층 구조를 보여줍니다. 이 계층 구조에서 여러 가지 방법으로 검색을 정의할 수 있습니다. 표 30-1에서는 2가지 샘플 검색 컨피그레이션을 보여줍니다.

첫 번째 컨피그레이션 예에서는 Employee1이 LDAP 권한 부여가 필요한 IPsec 터널을 설정하자 ASA에서 LDAP 서버에 검색 요청을 보내면서 Engineering 그룹에서 Employee1을 찾도록 지시합니다. 이 검색은 빠르게 수행됩니다.

두 번째 컨피그레이션 예에서는 ASA가 검색 요청을 보내면서 서버에 Example Corporation 내에서 Employee1을 검색하도록 지시합니다. 이 검색은 더 오래 걸립니다.

표 30-1 검색 컨피그레이션의 예

번호	LDAP 기본 DN	검색 범위	명명특성	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 서버와의 바인딩 소개

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 권한의 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 서버를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침
단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침
라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침
IPv6를 지원합니다.

LDAP 서버 구성

LDAP 서버 구성의 작업 흐름

1단계 LDAP 서버 그룹을 추가합니다. 30-7 페이지의 LDAP 서버 그룹 구성을 참조하십시오.

2단계 (선택 사항) 인증 메커니즘과는 별개인 LDAP 서버의 권한 부여를 구성합니다. 30-9 페이지의 VPN을 위해 LDAP을 사용하는 권한 부여 구성을 참조하십시오.

3단계 LDAP 특성 맵을 구성합니다. 30-5 페이지의 LDAP 특성 맵 구성을 참조하십시오.
LDAP 서버 그룹에 LDAP 서버를 추가하기 전에 특성 맵을 추가해야 합니다.

LDAP 특성 맵 구성

ASA에서는 사용자 인증을 위해 LDAP 디렉토리를 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 특성을 Cisco ASA 특성으로 변환하는 데 LDAP 특성 맵을 사용합니다. 이 특성 맵을 LDAP 서버에 바인딩하거나 삭제할 수 있습니다. 특성 맵을 표시하거나 지울 수도 있습니다.

지침

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)—디렉토리 부서 또는 사용자 그룹(예: Microsoft Active Directory memberOf) 특성 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 고정 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.

LDAP 기능을 매핑하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**ldap attribute-map** *map-name* 예: `ciscoasa(config)# ldap attribute-map att_map_1`	채워지지 않은 LDAP 특성 맵 테이블을 만듭니다.
2단계	**map-name** *user-attribute-name Cisco-attribute-name* 예: `ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class`	사용자 정의 특성 이름 부서를 Cisco 특성에 매핑합니다.
3단계	**map-value** *user-attribute-name Cisco-attribute-name* 예: `ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1`	사용자 정의 맵 값 부서를 사용자 정의 특성 값 및 Cisco 특성 값에 매핑합니다.
4단계	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* 예: `ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4`	서버 및 그 서버가 속한 AAA 서버 그룹을 지정합니다.
5단계	**ldap-attribute-map** *map-name* 예: `ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1`	특성 맵을 LDAP 서버에 바인딩합니다.

예

다음 예에서는 accessType이라는 LDAP 특성을 기반으로 ASA에 대한 관리 세션을 제한하는 방법을 보여줍니다. accessType 특성은 다음 값 중 하나를 가질 수 있습니다.

- VPN
- admin
- helpdesk

다음 예에서는 각 값이 ASA에서 지원하는 유효한 IETF-Radius-Service-Type 특성, 즉 remote-access (Service-Type 5) Outbound, admin (Service-Type 6) Administrative, nas-prompt (Service-Type 7) NAS Prompt 중 하나에 매핑되는 방법을 보여줍니다.

```
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

인증, 권한 부여 및/또는 어카운팅에 외부 LDAP 서버를 사용하려면 먼저 하나 이상의 LDAP 서버 그룹을 만들고 각 그룹에 하나 이상의 서버를 추가해야 합니다. LDAP 서버 그룹은 이름으로 식별합니다. 각 서버 그룹은 하나의 서버 유형에 특정됩니다.

지침

- 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 서버가 사용할 수 없는 경우 ASA는 로컬 데이터베이스를 시도합니다. 단, 로컬 데이터베이스가 대비책으로 구성되었어야 합니다(관리 인증 및 권한 부여만 해당). 대비책이 없을 경우 ASA는 계속 LDAP 서버 액세스를 시도합니다.

세부 단계

다음 단계에서는 LDAP 서버 그룹을 만들어 구성하고 그 그룹에 LDAP 서버를 추가하는 방법을 보여줍니다.

	명령	목적
1단계	**aaa-server** *server_tag* **protocol ldap** 예: `ciscoasa(config)# aaa-server servergroup1 protocol ldap` `ciscoasa(config-aaa-server-group)#`	서버 그룹 이름과 프로토콜을 지정합니다. **aaa-server protocol** 명령을 입력하면 aaa-server 서버 컨피그레이션 모드가 됩니다.
2단계	**max-failed-attempts** *number* 예: `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	그룹의 어떤 LDAP 서버에 최대 몇 번의 요청을 보낸 후 다음 서버를 시도할지 지정합니다. *number* 인수는 1~5입니다. 기본값은 3입니다. 대비 메커니즘 구성에서 로컬 데이터베이스를 사용하여 대비책을 구성한 경우(관리 액세스만 해당), 그룹의 모드 서버가 응답하지 않으면 그 그룹은 무응답으로 간주하고 대비책을 시도합니다. 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.
3단계	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} 예: `ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20`	그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다. **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. 기본값은 10분입니다. **timed** 키워드는 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.
4단계	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* 예: `ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1` `Move to new procedure for adding a server to a grouyp`	LDAP 서버 및 그 서버가 속한 AAA 서버 그룹을 지정합니다. **aaa-server host** 명령을 입력하면 aaa-server 호스트 컨피그레이션 모드가 됩니다. 필요하다면 호스트 컨피그레이션 모드 명령을 사용하여 AAA 서버를 추가 구성합니다. 표 30-2에서는 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 30-2 호스트 모드 구성 및 기본값

명령	기본값	설명
ldap-attribute-map	—	**aaa server host** 명령에 따른 절차의 개별 단계
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	—	—
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 매개 변수에 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 LDAP을 사용하는 권한 부여 구성

VPN 액세스를 위한 사용자 LDAP 인증이 성공하면 ASA는 LDAP 서버를 쿼리하여 LDAP 특성을 받습니다. 대개 이 특성에는 VPN 세션에 적용되는 권한 부여 데이터가 들어 있습니다. 이와 같이 LDAP을 사용하면 단일 단계에서 인증과 권한 부여가 이루어집니다.

그러나 인증 메커니즘과 별개인 LDAP 디렉토리 서버의 권한 부여가 필요할 때가 있습니다. 예를 들어, 인증에 SDI 또는 인증서 서버를 사용하는 경우 어떤 권한 부여 정보도 반환되지 않습니다. 이러한 경우 인증이 성공한 후 사용자 권한 부여를 위해 LDAP 디렉토리에 쿼리하는 식으로 인증과 권한 부여를 2단계로 수행할 수 있습니다.

LDAP을 사용하는 VPN 사용자 권한 부여를 설정하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**tunnel-group** *groupname* **예:** `ciscoasa(config)# tunnel-group remotegrp`	remotegrp라는 이름의 IPsec 원격 액세스 터널 그룹을 만듭니다.
2단계	**tunnel-group** *groupname* **general-attributes** **예:** `ciscoasa(config)# tunnel-group remotegrp general-attributes`	서버 그룹과 터널 그룹을 연결합니다.
3단계	**authorization-server-group** *group-tag* **예:** `ciscoasa(config-general)# authorization-server-group ldap_dir_1`	권한 부여를 위해 앞서 생성한 AAA 서버 그룹에 새 터널 그룹을 지정합니다.

예

특정 요구 사항을 위한 다른 권한 부여 관련 명령과 옵션도 있지만, 다음 예에서는 LDAP을 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 컨피그레이션 작업을 완료했으면 다음 명령을 사용하여 디렉토리 비밀번호, 디렉토리 검색의 시작점, 디렉토리 검색의 범위와 같은 추가 LDAP 권한 부여 매개 변수를 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)#
```

LDAP 서버 모니터링

LDAP 서버를 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
show aaa-server	구성된 AAA 서버 통계를 표시합니다. AAA 서버 컨피그레이션을 지우려면 **clear aaa-server statistics** 명령을 입력합니다.
show running-config aaa-server	AAA 서버의 실행 중 컨피그레이션을 표시합니다. AAA 서버 통계를 지우려면 **clear configure aaa-server** 명령을 입력합니다.

LDAP 서버 기능 내역

표 30-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 30-3 AAA 서버 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
AAA를 위한 LDAP 서버	7.0(1)	LDAP 서버에서 AAA 지원과 LDAP 서버 구성 방법에 대해 설명합니다. 도입된 명령: **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 console LOCAL, 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**

31 장

ID 방화벽

이 장에서는 ID 방화벽을 위해 ASA를 구성하는 방법을 설명합니다.

ID 방화벽에 대한 정보

ID 방화벽 개요

엔터프라이즈 환경에서는 사용자가 하나 이상의 서버 리소스에 액세스해야 하는 경우가 많습니다. 일반적으로 방화벽은 사용자의 ID를 인식하지 않으므로 ID에 따라 보안 정책을 적용할 수 없습니다. 사용자별 액세스 정책을 구성하기 위해서는 사용자 인증 프록시를 구성해야 하는데, 이는 사용자 상호작용(사용자 이름/비밀번호 쿼리)을 필요로 합니다.

ASA의 ID 방화벽은 사용자의 ID를 기반으로 더 세부적인 액세스 제어를 제공합니다. 소스 IP 주소가 아닌 사용자 이름과 사용자 그룹 이름을 기반으로 한 액세스 규칙 및 보안 정책을 구성할 수 있습니다. ASA에서는 IP 주소와 Windows Active Directory 로그인 정보의 연결을 기반으로 한 보안 정책을 적용하고, 네트워크 IP 주소 대신 매핑된 사용자 이름을 기반으로 하여 이벤트를 보고합니다.

ID 방화벽은 실제 ID 매핑을 담당하는 외부 AD(Active Directory) 에이전트와 연계하여 Microsoft Active Directory와 통합됩니다. ASA에서는 특정 IP 주소에 대한 현재 사용자 ID 정보를 검색하는 소스로 Windows Active Directory를 사용하며, Active Directory 사용자를 위한 투명한 인증을 허용합니다.

ID 기반 방화벽 서비스는 소스 IP 주소 대신 사용자 또는 그룹을 지정할 수 있게 하여 기존 액세스 제어 및 보안 정책 메커니즘을 확장합니다. ID 기반 보안 정책은 기존 IP 주소 기반 규칙의 사이에 제약 없이 끼워 넣을 수 있습니다.

ID 방화벽은 다음과 같은 주요 이점을 제공합니다.

- 보안 정책에서 네트워크 토폴로지 분리
- 보안 정책 생성 간소화
- 네트워크 리소스에 대한 사용자 활동을 손쉽게 식별
- 사용자 활동 모니터링 간소화

ID 방화벽 구축을 위한 아키텍처

ID 방화벽은 실제 ID 매핑을 담당하는 외부 AD(Active Directory) 에이전트와 연계하여 Windows Active Directory와 통합됩니다.

ID 방화벽은 3가지 구성 요소로 이루어졌습니다.

- ASA
- Microsoft Active Directory

  Active Directory가 ASA의 ID 방화벽에 포함되어 있지만 Active Directory 관리자가 이를 관리합니다. 데이터의 신뢰성 및 정확성은 Active Directory의 데이터에 좌우됩니다.

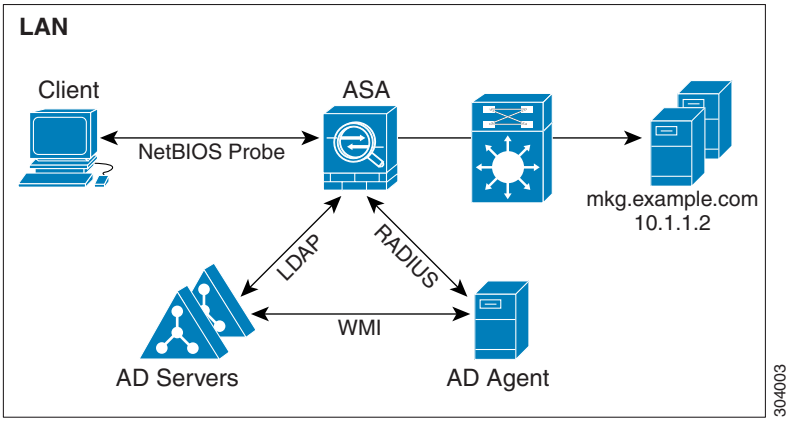
  지원되는 버전으로는 Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 서버 등이 있습니다.
- AD 에이전트

  AD 에이전트는 Windows 서버에서 실행됩니다. 지원되는 Windows 서버로는 Windows 2003, Windows 2008, Windows 2008 R2 등이 있습니다.

참고 Windows 2003 R2는 AD 에이전트 서버로 지원되지 않습니다.

그림 31-1에서는 ID 방화벽의 구성 요소를 보여줍니다. 그 다음 표에서는 이 구성 요소의 역할 및 서로 통신하는 방법을 설명합니다.

그림 31-1 ID 방화벽의 구성 요소



1	**ASA에서**: 관리자가 로컬 사용자 그룹 및 ID 방화벽 정책을 구성합니다.	4	**클라이언트 <-> ASA**: 클라이언트가 Microsoft Active Directory를 통해 네트워크에 로그인합니다. AD 서버가 사용자를 인증하고 사용자 로그인 보안 로그를 생성합니다. 또는 클라이언트가 컷스루 프록시 또는 VPN을 통해 네트워크에 로그인할 수도 있습니다.
2	**ASA <-> AD 서버**: ASA에서 AD 서버에 구성된 Active Directory 그룹에 대한 LDAP 쿼리를 보냅니다. ASA에서 로컬 및 AD 그룹을 통합하고 사용자 ID 기반의 액세스 규칙 및 Modular Policy Framework 보안 정책을 적용합니다.	5	**ASA <-> 클라이언트**: ASA에 구성된 정책에 따라 클라이언트에 대한 액세스를 허용하거나 거부합니다. 구성된 경우 ASA는 클라이언트의 NetBIO를 프로브하여 비활성 사용자와 무응답 사용자를 통과시킵니다.
3	**ASA <-> AD 에이전트**: ID 방화벽 컨피그레이션에 따라 ASA는 IP-사용자 데이터베이스를 다운로드하거나 사용자의 IP 주소를 묻는 AD 에이전트에 RADIUS 요청을 보냅니다. ASA에서는 웹 인증 및 VPN 세션을 통해 습득한 새로운 매핑된 항목을 AD 에이전트에 전달합니다.	6	**AD 에이전트 <-> AD 서버**: AD 에이전트는 사용자 ID와 IP 주소의 매핑 항목에 대한 캐시를 유지합니다. 그리고 ASA에 변경 사항을 알립니다. AD 에이전트는 syslog 서버에 로그를 보냅니다.

ID 방화벽의 기능

ID 방화벽은 다음과 같은 주요 기능을 제공합니다.

유연성

- ASA는 AD 에이전트에 새로운 IP 주소 각각을 쿼리하거나 전체 사용자 ID 및 IP 주소 데이터베이스의 로컬 사본을 유지하는 방법으로 AD 에이전트로부터 사용자 ID 및 IP 주소 매핑을 검색할 수 있습니다.
- 사용자 ID 정책의 목적지로 호스트 그룹, 서브넷 또는 IP 주소를 지원합니다.
- 사용자 ID 정책의 소스 및 목적지로 FQDN(정규화된 도메인 이름)을 지원합니다.
- 5-튜플 정책과 ID 기반 정책의 조합을 지원합니다. ID 기반 기능은 기존 5-튜플 솔루션과 연계하면서 작동합니다.
- IPS 및 애플리케이션 검사 정책의 사용을 지원합니다.
- 원격 액세스 VPN, AnyConnect VPN, L2TP VPN, 컷스루 프록시에서 사용자 ID 정보를 검색합니다. 검색된 모든 사용자는 AD 에이전트와 연결된 모든 ASA에 보내집니다.

확장성

- 각 AD 에이전트는 100대의 ASA를 지원합니다. 여러 ASA가 단일 AD 에이전트와 통신하면서 대규모 네트워크 구축 환경에서 확장성을 제공할 수 있습니다.
- 30대의 Active Directory 서버를 지원합니다. 단 IP 주소가 모든 도메인의 전 범위에서 고유해야 합니다.
- 한 도메인에 있는 각 사용자 ID는 최대 8개의 IP 주소를 가질 수 있습니다.

- ASA 5500 Series 모델의 경우 활성 정책에서 최대 64,000개의 사용자 ID-IP 주소 매핑 항목을 지원합니다. 이 제한으로 정책이 적용되는 사용자의 최대 수를 제어합니다. 총 사용자 수는 각기 다른 모든 컨텍스트에 구성된 전체 사용자를 합한 것입니다.
- 활성 ASA 정책에서 최대 256개의 사용자 그룹을 지원합니다.
- 단일 액세스 규칙에서 하나 이상의 사용자 그룹 또는 사용자를 수용할 수 있습니다.
- 다중 도메인을 지원합니다.

가용성

- ASA에서는 AD에서 그룹 정보를 검색하고, AD 에이전트에서 소스 IP 주소를 사용자 ID에 매핑하지 못할 경우에는 웹 인증을 통해 IP 주소를 얻습니다.
- AD 서버 중 하나가 또는 ASA가 응답하지 않더라도 AD 에이전트는 계속 작동합니다.
- ASA에서 기본 AD 에이전트와 보조 AD 에이전트를 구성하는 것을 지원합니다. 기본 AD 에이전트가 더 이상 응답하지 않을 경우 ASA는 보조 AD 에이전트로 전환할 수 있습니다.
- AD 에이전트를 사용할 수 없는 경우 ASA는 컷스루 프록시, VPN 인증과 같은 기존 ID 소스를 대신 사용할 수 있습니다.
- AD 에이전트는 watchdog 프로세스를 실행하는데, 이 프로세스의 서비스는 중지하더라도 자동으로 재시작합니다.
- 분산 IP 주소/사용자 매핑 데이터베이스를 ASA끼리 사용하는 것을 허용합니다.

구축 시나리오

환경의 요구 사항에 따라 다음 방법으로 ID 방화벽의 구성 요소를 구축할 수 있습니다.

그림 31-2에서는 이중화를 지원하기 위해 ID 방화벽의 구성 요소를 구축하는 방법을 보여줍니다. 시나리오 1은 구성 요소의 이중화 없는 간단한 설치입니다. 시나리오 2 역시 이중화 없는 간단한 설치입니다. 그러나 이 구축 시나리오에서는 AD 서버와 AD 에이전트가 동일한 Windows 서버에 함께 배치되어 있습니다.

그림 31-2 이중화 없는 구축 시나리오

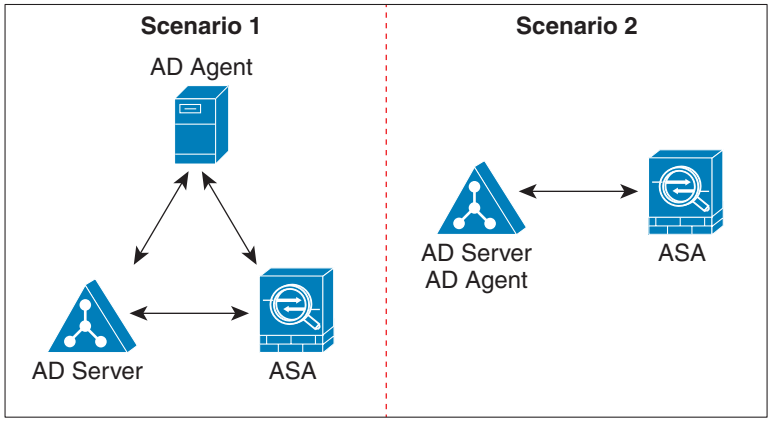


그림 31-3에서는 이중화를 지원하기 위해 ID 방화벽 구성 요소를 구축하는 방법을 보여줍니다. 시나리오 1은 여러 AD 서버 및 별도의 Windows 서버에 설치된 단일 AD 에이전트로 구성된 구축 환경입니다. 시나리오 2는 여러 AD 서버 및 별도의 Windows 서버에 설치된 여러 AD 에이전트로 구성된 구축 환경입니다.

그림 31-3 이중 구성 요소의 구축 시나리오

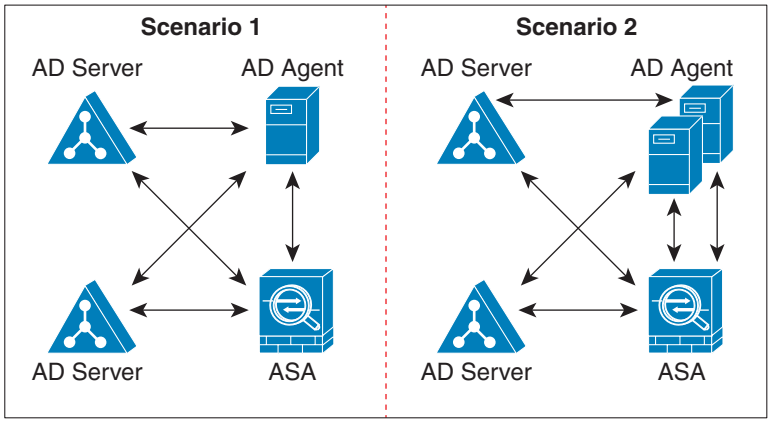


그림 31-4에서는 모든 ID 방화벽 구성 요소(AD 서버, AD 에이전트, 클라이언트)가 어떻게 설치되고 LAN을 통해 통신하는지 보여줍니다.

그림 31-4 LAN 기반 구축

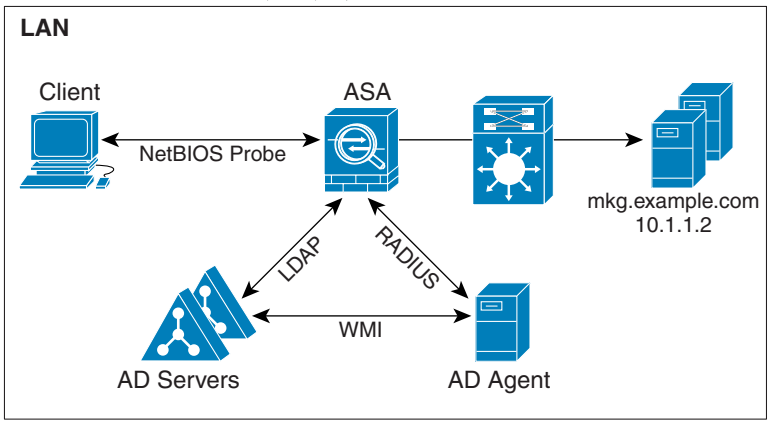


그림 31-5에서는 원격 사이트를 지원하는 WAN 기반 구축을 보여줍니다. AD 서버와 AD 에이전트가 기본 사이트 LAN에 설치되어 있습니다. 클라이언트는 원격 사이트에 있으며 WAN을 통해 ID 방화벽 구성 요소에 연결됩니다.

그림 31-5 WAN 기반 구축

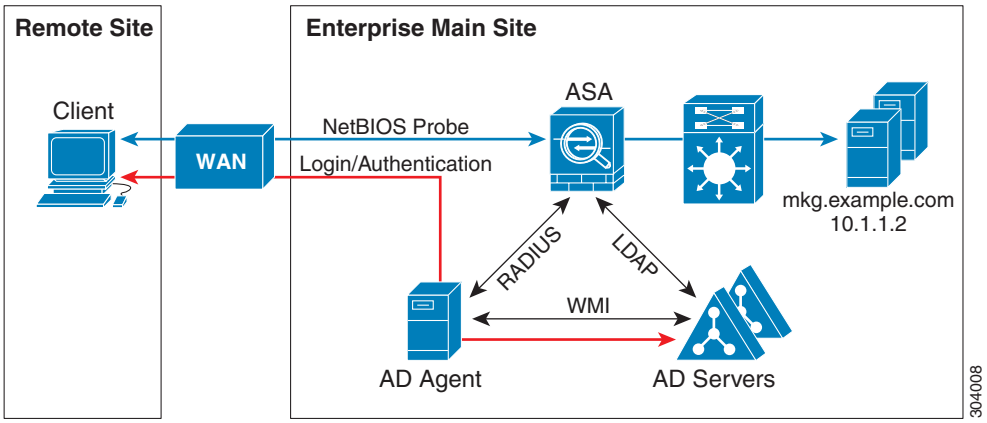


그림 31-6에서는 원격 사이트를 지원하는 WAN 기반 구축도 보여줍니다. Active Directory 서버는 기본 사이트 LAN에 설치됩니다. 그러나 AD 에이전트는 설치된 다음 원격 사이트의 클라이언트에 의해 액세스됩니다. 원격 클라이언트는 WAN을 통해 기본 사이트에 있는 AD 서버에 연결합니다.

그림 31-6 원격 AD 에이전트로 구성된 WAN 기반 구축

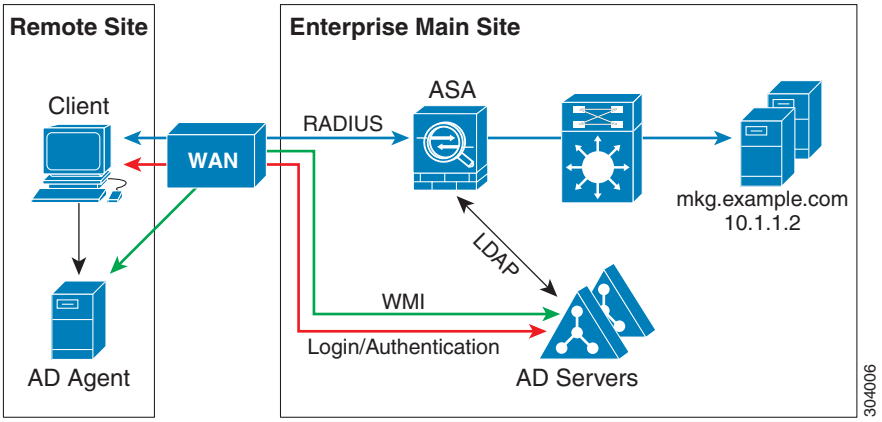
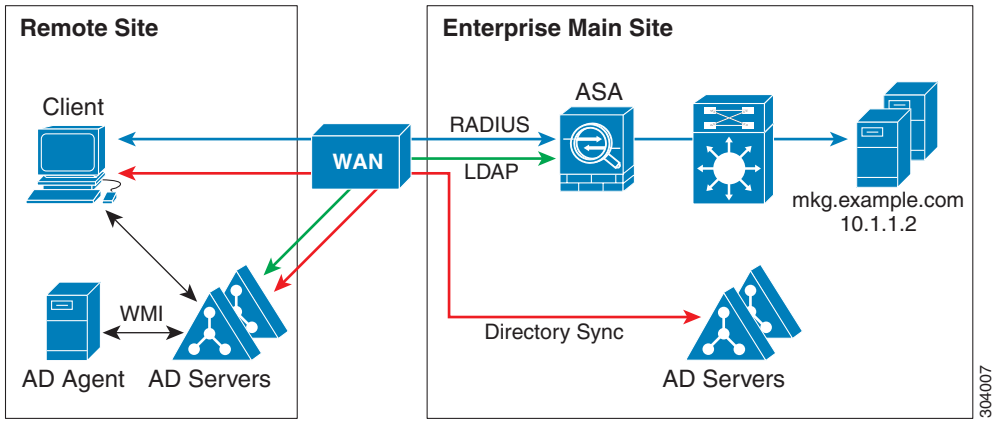


그림 31-7에서는 확장된 원격 사이트 설치를 보여줍니다. AD 에이전트와 AD 서버가 원격 사이트에 설치됩니다. 클라이언트는 기본 사이트에 위치한 네트워크 리소스에 로그인할 때 로컬에서 이 구성 요소에 액세스합니다. 원격 AD 서버는 기본 사이트에 있는 중앙 AD 서버와 데이터를 동기화해야 합니다.

그림 31-7 원격 AD 에이전트와 AD 서버로 구성된 WAN 기반 구축



ID 방화벽을 위한 라이센싱

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원됩니다.

장애 조치 지침

- ID 방화벽은 사용자 ID-IP 주소 매핑을 지원하고 상태 기반 시스템 대체 작동(Stateful Failover)이 활성화된 경우 활성 시스템에서 대기 시스템으로 AD 에이전트 상태를 복제하는 것도 지원합니다. 그러나 사용자 ID-IP 주소 매핑, AD 에이전트 상태, 도메인 상태만 복제됩니다. 사용자 및 사용자 그룹 레코드는 대기 ASA에 복제되지 않습니다.
- 장애 조치가 구성되면 대기 ASA 역시 AD 에이전트에 직접 연결하여 사용자 그룹을 검색하도록 구성되어야 합니다. ID 방화벽에 대한 NetBIOS 검사 옵션이 구성된 경우에도 대기 ASA는 클라이언트에 NetBIOS 패킷을 보내지 않습니다.
- 클라이언트가 활성 ASA에 의해 비활성 상태로 확인되면 그 정보가 대기 ASA에 전달됩니다. 사용자 통계는 대기 ASA에 전달되지 않습니다.
- 장애 조치가 구성되면 AD 에이전트가 활성 및 대기 ASA 모두와 통신하도록 구성해야 합니다. AD 에이전트 서버에 ASA를 구성하는 단계는 *AD 에이전트 설치 및 설정 설명서*를 참조하십시오.

IPv6 지침

- IPv6를 지원합니다.
- AD 에이전트는 엔드포인트에 IPv6 주소를 지원합니다. 로그 이벤트에서 IPv6 주소를 수신하고 캐시에 저장했다가 RADIUS 메시지를 통해 보낼 수 있습니다.
- IPv6를 통한 NetBIOS는 지원되지 않습니다.

추가 지침 및 제한

- 목적지 주소에서 전체 URL은 지원되지 않습니다.
- NetBIOS 검사 기능이 작동하려면 ASA, AD 에이전트, 클라이언트를 연결하는 네트워크에서 UDP 캡슐화 NetBIOS 트래픽을 지원해야 합니다.
- 중간 라우터가 있으면 ID 방화벽의 MAC 주소 검사가 수행되지 않습니다. 동일한 라우터의 뒤에 있는 클라이언트에 로그인한 사용자는 MAC 주소가 같습니다. 이러한 구현에서는 동일한 라우터에서 보내는 모든 패킷이 검사를 통과할 수 있습니다. ASA에서 라우터 뒤에 있는 실제 MAC 주소를 확인할 수 없기 때문입니다.
- 다음 ASA 기능은 확장 ACL에서 ID 기반 객체와 FQDN을 사용하는 것을 지원하지 않습니다.
  - 경로 맵
  - 암호 맵
  - WCCP
  - NAT
  - 그룹 정책(VPN 필터에 대한 것 제외)
  - DAP

- **user-identity update active-user-database** 명령을 사용하여 AD 에이전트로부터 사용자-IP 주소를 다운로드하는 프로세스를 능동적으로 시작할 수 있습니다.

  이전의 다운로드 세션이 끝난 경우 ASA에서 이 명령의 재실행을 허용하지 않도록 설계되었습니다.

  따라서 사용자-IP 주소가 매우 클 경우, 이전 다운로드 세션이 끝나지 않은 상태에서 다시 **user-identity update active-user-database** 명령을 실행하면 다음 오류 메시지가 나타납니다.

  ```
  "ERROR: one update active-user-database is already in progress."
  ```

  이전 세션이 완전히 끝날 때까지 기다려야 합니다. 그러면 다시 **user-identity update active-user-database** 명령을 실행할 수 있습니다.

  AD 에이전트에서 ASA로 보내는 패킷이 손실된 경우에도 이와 같은 동작이 일어납니다.

  user-identity update active-user-database 명령을 실행하면 ASA는 다운로드할 사용자-IP 매핑 항목의 총 개수를 요청합니다. 그러면 AD 에이전트는 ASA와의 UDP 연결을 시작하고 권한 부여 요청 패킷의 변경 사항을 보냅니다.

  어떤 이유로 패킷이 손실된 경우 ASA에서 이를 알 방법이 없습니다. 따라서 ASA는 4~5분간 세션을 유지합니다. 이 상태에서 **user-identity update active-user-database** 명령을 실행하면 이 오류 메시지가 계속 나타납니다.

- Cisco CDA(Context Directory Agent)를 ASA 또는 Cisco Ironport WSA(Web Security Appliance)와 함께 사용할 경우 다음 포트를 열어 두어야 합니다.
  - UDP 인증 포트—1645
  - UDP 어카운팅 포트—1646
  - UDP 수신 포트—3799

    수신 포트는 CDA에서 ASA에 또는 WSA에 권한 부여 요청의 변경 사항을 보낼 때 사용합니다.
- 도메인 이름에는 \/:*?"<>| 문자를 사용할 수 없습니다. 명명 규칙에 대해서는 http://support.microsoft.com/kb/909264를 참조하십시오.
- 사용자 이름에는 \/[]::=,+*?"<>|@ 문자를 사용할 수 없습니다.
- 사용자 그룹 이름에는 \/[]:;=,+*?"<>| 문자를 사용할 수 없습니다.

전제 조건

ASA에서 ID 방화벽을 구성하기 전에 AD 에이전트 및 Microsoft Active Directory의 전제 조건을 충족해야 합니다.

AD 에이전트

- AD 에이전트는 ASA에서 액세스할 수 있는 Windows 서버에 설치해야 합니다. 또한 AD 에이전트가 AD 서버로부터 정보를 얻고 ASA와 통신할 수 있도록 구성해야 합니다.
- 지원되는 Windows 서버로는 Windows 2003, Windows 2008, Windows 2008 R2 등이 있습니다.

참고 Windows 2003 R2는 AD 에이전트 서버로 지원되지 않습니다.

- AD 에이전트를 설치하고 구성하는 단계에 대해서는 *AD 에이전트 설치 및 설정 설명서*를 참조하십시오.
- ASA에서 AD 에이전트를 구성하기 전에 AD 에이전트와 ASA의 통신에 사용할 암호 키 값을 얻습니다. 이 값은 AD 에이전트와 ASA 모두에서 일치해야 합니다.

Microsoft Active Directory

- Microsoft Active Directory는 Windows 서버에 설치되고, ASA에서 액세스할 수 있어야 합니다. 지원되는 버전으로는 Windows 2003, 2008, 2008 R2 서버 등이 있습니다.
- ASA에서 AD 서버를 구성하기 전에 Active Directory에서 ASA를 위한 사용자 어카운트를 만듭니다.
- 또한 ASA는 LDAP을 통해 활성화된 SSL을 사용하여 AD 서버에 암호화된 로그인 정보를 보냅니다. SSL이 AD 서버에서 활성화되어야 합니다. AD를 위해 SSL을 활성화하는 방법에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.

참고 AD 에이전트 설치 프로그램을 실행하기 전에 AD 에이전트가 모니터링하는 각 Microsoft Active Directory 서버에 *Cisco AD 에이전트를 위한 README First*에 명시된 패치를 설치해야 합니다. 이 패치는 AD 에이전트가 도메인 컨트롤러 서버에 설치되는 경우에도 필요합니다.

ID 방화벽 구성

이 단원에서는 다음 항목을 다룹니다.

ID 방화벽 구성의 작업 흐름

ID 방화벽을 구성하려면 다음 단계를 수행합니다.

1단계 ASA에 AD 도메인을 구성합니다.

31-10 페이지의 AD 도메인 구성을 참조하십시오.

또한 31-4 페이지의 구축 시나리오에서 해당 환경의 요구 사항에 맞게 AD 서버를 구축하는 방법도 알아보십시오.

2단계 ASA에 AD 에이전트를 구성합니다.

31-12 페이지의 AD 에이전트 구성을 참조하십시오.

또한 31-4 페이지의 구축 시나리오에서 해당 환경의 요구 사항에 맞게 AD 에이전트를 구축하는 방법도 알아보십시오.

3단계 ID 옵션을 구성합니다.

31-13 페이지의 ID 옵션 구성을 참조하십시오.

4단계 ID 기반 보안 정책을 구성합니다. AD 도메인과 AD 에이전트가 구성된 다음에는 여러 기능에서 사용할 ID 기반 객체 그룹과 ACL을 만들 수 있습니다.

31-17 페이지의 ID 기반 보안 정책 구성을 참조하십시오.

AD 도메인 구성

ASA에서 AD 그룹을 다운로드하려면 그리고 AD 에이전트로부터 IP-사용자 매핑을 받을 때 특정 도메인의 사용자 ID를 승인하기 위해서는 ASA에 AD 도메인 컨피그레이션이 필요합니다.

전제 조건

- Active Directory 서버 IP 주소
- LDAP 기반 DN의 고유 이름
- ID 방화벽에서 AD 도메인 컨트롤러에 연결하는 데 사용하는 AD 사용자의 고유 이름 및 비밀번호

AD 도메인을 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**aaa-server** *server-tag* **protocol ldap** 예: `ciscoasa(config)# aaa-server adserver protocol ldap`	AD 서버를 위해 AAA 서버 그룹을 만들고 AAA 서버 매개 변수를 구성합니다.
2단계	**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] 예: `ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6`	AD 서버를 위해 AAA 서버를 AAA 서버 그룹의 일부로 구성하고 호스트별 AAA 서버 매개 변수를 구성합니다.
3단계	**ldap-base-dn** *string* 예: `ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com`	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 시작할 위치를 지정합니다. 선택 사항으로 **ldap-base-dn** 명령을 지정할 수 있습니다. 이 명령을 지정하지 않을 경우 ASA는 Active Directory에서 defaultNamingContext를 검색하고 이를 기본 DN으로 사용합니다.
4단계	**ldap-scope subtree** 예: `ciscoasa(config-aaa-server-host)# ldap-scope subtree`	서버가 권한 부여 요청을 받고 LDAP 계층 구조에서 검색을 수행할 범위를 지정합니다.
5단계	**ldap-login-password** *string* 예: `ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword`	LDAP 서버의 로그인 비밀번호를 지정합니다.

	명령	목적
6단계	**ldap-login-dn** *string* 예: ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1	시스템에서 어떤 디렉토리 객체의 이름으로 바인딩해야 하는지 지정합니다. ASA에서는 사용자 인증 요청에 Login DN 필드를 추가하는 방법으로 인증 바인딩에서 스스로를 식별합니다. Login DN 필드는 ASA의 인증 특성을 설명합니다. *string* 인수는 대/소문자를 구분하는 최대 128자의 문자열로서 LDAP 계층 구조에서 디렉토리 객체의 이름을 지정합니다. 문자열에서 공백은 허용되지 않지만, 다른 특수 문자는 사용 가능합니다. 일반 형식 또는 축약 형식으로 지정할 수 있습니다. **ldap-login-dn** 명령의 일반 형식은 CN=username,OU=Employees,OU=Sample Users,DC=sample,DC=com을 포함합니다.
7단계	**server-type microsoft** 예: ciscoasa(config-aaa-server-host)# server-type microsoft	Microsoft Active Directory 서버를 위한 LDAP 서버 모델을 구성합니다.
8단계	**ldap-group-base-dn** *string* 예: ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com	AD 도메인 컨트롤러에서 AD 그룹 컨피그레이션의 위치를 지정합니다. 지정하지 않으면 **ldap-group-base-dn** 명령의 값을 사용합니다. 선택 사항으로 **ldap-group-base-dn** 명령을 지정할 수 있습니다.
9단계	**ldap-over-ssl enable** 예: ciscoasa(config-aaa-server-host)# ldap-over-ssl enable	ASA에서 SSL을 통해 AD 도메인 컨트롤러에 액세스할 수 있게 합니다. SSL을 통한 LDAP을 지원하려면 AD 서버가 이를 지원하도록 구성되어야 합니다. 기본적으로 Active Directory는 SSL이 구성되어 있지 않습니다. Active Directory에서 SSL이 구성되지 않은 경우 ID 방화벽을 위해 ASA에서 SSL을 구성할 필요 없습니다.
10단계	**server-port** *port-number* 예: ciscoasa(config-aaa-server-host)# server-port 389 ciscoasa(config-aaa-server-host)# server-port 636	기본적으로, **ldap-over-ssl** 명령이 활성화되지 않은 경우 기본 서버 포트는 389입니다. **ldap-over-ssl** 명령이 활성화된 경우에는 기본 서버 포트가 636입니다.
11단계	**group-search-timeout** *seconds* 예: ciscoasa(config-aaa-server-host)# group-search-timeout 300	LDAP 쿼리가 시간 초과될 때까지의 시간을 설정합니다.

AD 에이전트 구성

AD 에이전트 서버 그룹을 위해 기본 및 보조 AD 에이전트를 구성합니다. ASA에서 기본 AD 에이전트가 응답하지 않음을 탐지한 경우, 보조 에이전트가 지정되어 있다면 ASA는 보조 AD 에이전트로 전환합니다. AD 에이전트의 AD 서버는 RADIUS를 통신 프로토콜로 사용합니다. 따라서 ASA와 AD 에이전트의 공유 암호에 대한 키 특성을 지정해야 합니다.

전제 조건

AD 에이전트를 구성하기 전에 다음 정보가 있어야 합니다.

- AD 에이전트 IP 주소
- ASA와 AD 에이전트의 공유 암호

AD 에이전트를 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**aaa-server** *server-tag* **protocol radius** **예:** `ciscoasa(config)# aaa-server adagent protocol radius`	AD 에이전트를 위해 AAA 서버 그룹을 만들고 AAA 서버 매개 변수를 구성합니다.
2단계	**ad-agent-mode** **예:** `ciscoasa(config)# ad-agent-mode`	AD 에이전트 모드를 활성화합니다.
3단계	**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] **예:** `ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101`	AD 에이전트를 위해 AAA 서버를 AAA 서버 그룹의 일부로 구성하고 호스트별 AAA 서버 매개 변수를 구성합니다.
4단계	**key** *key* **예:** `ciscoasa(config-aaa-server-host)# key mysecret`	AD 에이전트 서버에 ASA를 인증하는 데 사용하는 서버 암호 값을 지정합니다.
5단계	**user-identity ad-agent aaa-server** *aaa_server_group_tag* **예:** `ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent`	AD 에이전트의 서버 그룹을 정의합니다. *aaa_server_group_tag* 인수에 정의된 첫 번째 서버가 기본 AD 에이전트이고, 두 번째로 정의된 서버는 보조 AD 에이전트입니다. ID 방화벽에서는 AD 에이전트 호스트를 2개만 정의할 수 있습니다. ASA에서 기본 AD 에이전트가 중지했음을 탐지한 경우, 보조 에이전트가 지정되어 있다면 보조 AD 에이전트로 전환합니다. AD 에이전트의 AAA 서버는 RADIUS를 통신 프로토콜로 사용합니다. 따라서 ASA와 AD 에이전트의 공유 암호에 대한 키 특성을 지정해야 합니다.

	명령	목적
6단계	**test aaa-server ad-agent** 예: `ciscoasa(config-aaa-server-host)# test aaa-server ad-agent`	ASA와 AD 에이전트 서버 간의 통신을 테스트합니다.

다음에 할 일

ID 방화벽을 위한 액세스 규칙을 구성합니다. 31-17 페이지의 ID 기반 보안 정책 구성을 참조하십시오.

ID 옵션 구성

이 절차를 수행하여 ID 방화벽 기능을 추가하거나 수정합니다. 이 기능을 활성화하려면 **Enable** 확인란을 선택합니다. 기본적으로 ID 방화벽 기능은 비활성화되어 있습니다.

전제 조건

ID 방화벽을 위한 ID 옵션을 구성하기 전에 AD 에이전트 및 Microsoft Active Directory의 전제 조건을 충족해야 합니다. AD 에이전트 및 Microsoft Active Directory 설치의 요구 사항은 31-8 페이지의 전제 조건을 참조하십시오.

ID 방화벽을 위한 ID 옵션을 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**user-identity enable** 예: `ciscoasa(config)# user-identity enable`	ID 방화벽 기능을 활성화합니다.

	명령	목적
2단계	**user-identity default-domain** *domain_NetBIOS_name* **예:** ciscoasa(config)# user-identity default-domain SAMPLE	ID 방화벽의 기본 도메인을 지정합니다. *domain_NetBIOS_name* 인수에는 최대 32자이고 [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.]로 구성된 이름을 입력합니다. 맨 앞에 '.'와 ' '이 올 수 없습니다. 도메인 이름이 공백을 포함할 경우 전체 이름을 따옴표로 묶어야 합니다. 도메인 이름은 대/소문자를 구분하지 않습니다. 기본 도메인은 모든 사용자 및 사용자 그룹에 사용되는데, 해당 사용자 또는 그룹에 대해 어떤 도메인도 명시적으로 구성되지 않은 경우에 쓰입니다. 기본 도메인이 지정되지 않았으면 사용자 및 그룹의 기본 도메인은 LOCAL이 됩니다. 다중 컨텍스트 모드의 경우, 컨텍스트마다 또는 시스템 실행 영역 내에서 기본 도메인 이름을 설정할 수 있습니다. **참고** 기본 도메인 이름은 AD 도메인 컨트롤러에 구성된 NetBIOS 도메인 이름과 일치하도록 지정해야 합니다. 도메인 이름이 일치하지 않을 경우, AD 에이전트는 사용자 ID-IP 주소 매핑 항목을 ASA 구성 시 입력한 도메인 이름과 잘못 연결합니다. NetBIOS 도메인 이름을 보려면 임의의 텍스트 편집기에서 AD 사용자 이벤트 보안 로그를 엽니다. ID 방화벽에서는 모든 로컬에 정의된 사용자 그룹 또는 로컬에 정의된 사용자에 대해 LOCAL 도메인을 사용합니다. 웹 포털(컷스루 프록시)을 통해 로그인한 사용자는 그 사용자가 인증한 AD 도메인에 속한 것으로 표시됩니다. VPN을 통해 로그인한 사용자는 LOCAL 도메인에 속한 것으로 표시됩니다. 단, LDAP에서 Active Directory를 사용하여 VPN을 인증한 경우는 제외합니다. 그러한 경우에는 ID 방화벽에서 사용자를 해당 AD 도메인과 연결할 수 있습니다.
3단계	**user-identity domain** *domain_nickname* **aaa-server** *aaa_server_group_tag* **예:** ciscoasa(config)# user-identity domain SAMPLE aaa-server ds	사용자 그룹 쿼리를 가져오기 위해 AAA 서버에 대해 정의된 LDAP 매개변수를 도메인 이름과 연결합니다. *domain_nickname* 인수에는 최대 32자이고 [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.]로 구성된 이름을 입력합니다. 맨 앞에 '.'와 ' '이 올 수 없습니다. 도메인 이름이 공백을 포함할 경우 그 공백 문자를 따옴표로 묶어야 합니다. 도메인 이름은 대/소문자를 구분하지 않습니다.
4단계	**user-identity logout-probe netbios local-system probe-time minutes** *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed** | **match-any** | **exact-match**] **예:** ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10 retry-interval seconds 10 retry-count 2 user-not-needed	NetBIOS 프로브를 활성화합니다. 이 옵션을 활성화하면 ASA에서 클라이언트가 계속 활성 상태인지 확인하기 위해 사용자 클라이언트 IP 주소를 프로브하는 빈도를 구성합니다. 기본적으로 NetBIOS 조사는 비활성화되어 있습니다. NetBIOS 패킷을 최소화하기 위해 ASA는 사용자가 지정된 시간(분)을 초과하여 유휴 상태였을 때만 클라이언트에 NetBIOS 프로브를 보냅니다. • **Exact-match**—IP 주소에 지정된 사용자의 사용자 이름은 NetBIOS 응답에서 하나뿐이어야 합니다. 그렇지 않으면 IP 주소의 사용자 ID는 유효하지 않은 것으로 간주됩니다. • **User-not-needed**—ASA에서 클라이언트로부터 NetBIOS 응답을 받는 한 사용자 ID는 유효한 것으로 간주됩니다. ID 방화벽은 활성 상태이고 하나 이상의 보안 정책에 존재하는 사용자 ID에 대해서만 NetBIOS 프로브를 수행합니다. ASA에서는 사용자가 컷스루 프록시를 통해 또는 VPN을 사용하여 로그인한 경우에는 클라이언트에 대한 NetBIOS 프로브를 수행하지 않습니다.

	명령	목적
5단계	**user-identity inactive-user-timer minutes** *minutes* 예: `ciscoasa(config)# user-identity inactive-user-timer minutes 120`	사용자가 유휴 상태로 간주될 때까지의 시간을 지정합니다. ASA는 여기에 지정된 시간 동안 사용자의 IP 주소로부터 트래픽을 받지 못했습니다. 타이머가 만료되면 사용자의 IP 주소는 비활성 상태로 표시되고 로컬 캐시에 저장된 사용자 ID-IP 주소 매핑 데이터베이스에서 삭제됩니다. 그리고 ASA는 더 이상 AD 에이전트에 그 IP 주소에 대해 알리지 않습니다. 기존 트래픽은 계속 전달될 수 있습니다. 이 명령이 지정되면 ASA는 NetBIOS Logout Probe가 구성된 경우에도 비활성 타이머를 실행합니다. 기본적으로 유휴 타이머는 60분으로 설정됩니다. **참고** Idle Timeout 옵션은 VPN 또는 컷스루 프록시 사용자에게는 적용되지 않습니다.
6단계	**user-identity poll-import-user-group-timer hours** *hours* 예: `ciscoasa(config)# user-identity poll-import-user-group-timer hours 1`	ASA에서 AD 서버에 사용자 그룹 정보를 쿼리할 때까지의 시간을 지정합니다. 사용자가 AD 그룹에 추가되거나 삭제된 경우 ASA는 import group 타이머가 실행된 후에 업데이트된 사용자 그룹을 수신합니다. 기본적으로 **poll-import-user-group-timer hours** 값은 8시간입니다. 사용자 그룹 정보를 즉시 업데이트하려면 **user-identity update import-user** 명령을 입력합니다.
7단계	**user-identity action netbios-response-fail remove-user-ip** 예: `ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip`	클라이언트가 NetBIOS 프로브에 응답하지 않을 때 어떻게 할지 지정합니다. 이를테면 해당 클라이언트에 대한 네트워크 연결이 차단될 수 있습니다. 또는 클라이언트가 활성 상태가 아닙니다. **user-identity action remove-user-ip** 명령이 구성되면 ASA는 해당 클라이언트에 대한 사용자 ID-IP 주소 매핑을 삭제합니다. 기본적으로 이 명령은 비활성화되어 있습니다.
8단계	**user-identity action domain-controller-down** *domain_nickname* **disable-user-identity-rule** 예: `ciscoasa(config)# user-identity action domain-controller-down SAMPLE disable-user-identity-rule`	AD 도메인 컨트롤러가 응답하지 않는 것으로 볼 때 도메인이 중지 상태일 때 어떻게 할지 지정합니다. 도메인이 중지한 상태에서 **disable-user-identity-rule** 키워드가 구성되어 있다면 ASA는 해당 도메인에 대해 사용자 ID-IP 주소 매핑을 비활성화합니다. 또한 **show user-identity user** 명령에 의해 표시된 출력에서 그 도메인에 있는 모든 사용자 IP 주소의 상태가 disabled로 표시됩니다. 기본적으로 이 명령은 비활성화되어 있습니다.
9단계	**user-identity user-not-found enable** 예: `ciscoasa(config)# user-identity user-not-found enable`	user-not-found 추적을 활성화합니다. 마지막 1024개의 IP 주소만 추적됩니다. 기본적으로 이 명령은 비활성화되어 있습니다.

	명령	목적
10단계	**user-identity action ad-agent-down disable-user-identity-rule** 예: `ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule`	AD 에이전트가 응답하지 않을 때 어떻게 할지 지정합니다. AD 에이전트가 중지한 상태에서 **user-identity action ad-agent-down** 명령이 구성되어 있다면 ASA는 해당 도메인의 사용자와 연결된 사용자 ID 규칙을 비활성화합니다. 또한 **show user-identity user** 명령에 의해 표시된 출력에서 그 도메인에 있는 모든 사용자 IP 주소의 상태가 disabled로 표시됩니다. 기본적으로 이 명령은 비활성화되어 있습니다.
11단계	**user-identity action mac-address-mismatch remove-user-ip** 예: `ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip`	사용자의 MAC 주소가 현재 그 MAC 주소에 매핑된 ASA IP 주소와 일치하지 않는 것으로 확인되면 어떻게 할지 지정합니다. **user-identity action mac-address-mismatch** 명령이 구성되면 ASA는 해당 클라이언트에 대한 사용자 ID-IP 주소 매핑을 삭제합니다. 기본적으로, 이 명령이 지정되면 ASA는 **remove-user-ip** 키워드를 사용합니다.
12단계	**user-identity ad-agent active-user-database** {**on-demand** | **full-download**} 예: `ciscoasa(config)# user-identity ad-agent active-user-database full-download`	ASA에서 AD 에이전트로부터 사용자 ID-IP 주소 매핑 정보를 검색하는 방법을 정의합니다. • **Full-download**—ASA에서 AD 에이전트에 요청을 보내 ASA 시작 시 전체 IP-사용자 매핑 테이블을 다운로드하도록 그리고 사용자가 로그인하고 로그아웃할 때 추가된 IP-사용자 매핑 정보를 수신하도록 지정합니다. • **On-demand**—ASA가 새로운 연결이 필요한 패킷을 수신할 때, 그 소스 IP 주소의 사용자가 사용자-ID 데이터베이스에 없다면 ASA에서 AD 에이전트로부터 IP 주소의 사용자 매핑 정보를 검색하도록 지정합니다. 기본적으로 ASA는 Full-download 옵션을 사용합니다. 전체 다운로드는 이벤트 기반입니다. 즉 후속으로 데이터베이스 다운로드 요청이 있을 경우, 사용자 ID-IP 주소 매핑 데이터베이스에서 업데이트된 사항만 보내집니다. ASA에서 AD 에이전트에 변경 요청을 등록하면 AD 에이전트는 ASA에 새 이벤트를 보냅니다.
13단계	**user-identity ad-agent hello-timer seconds** *seconds* **retry-times** *number* 예: `ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3`	ASA와 AD 에이전트 간의 hello 타이머를 정의합니다. ASA와 AD 에이전트 간의 hello 타이머는 ASA가 hello 패킷을 교환하는 빈도를 정의합니다. ASA는 ASA 복제 상태(in-sync 또는 out-of-sync) 및 도메인 상태(up 또는 down)를 확인하는 데 hello 패킷을 사용합니다. ASA가 AD 에이전트로부터 응답을 받지 못한 경우 지정된 간격이 지나면 hello 패키지를 다시 보냅니다. 기본적으로 hello 타이머는 30초, 재시도 5번으로 설정되어 있습니다.

	명령	목적
14단계	**user-identity ad-agent event-timestamp-check** 예: `ciscoasa(config)# user-identity ad-agent event-timestamp-check`	ASA에서 각 식별자에 대해 수신하는 최종 이벤트 타임 스탬프를 추적할 수 있게 합니다. 또한 이벤트 타임 스탬프가 ASA의 시계보다 5분 이상 오래되었거나 타임 스탬프가 최종 이벤트 타임 스탬프보다 빠를 경우 어떤 메시지든 삭제합니다. 최종 이벤트 타임 스탬프를 모르는 새로 부팅된 ASA의 경우, ASA에서 이벤트 타임 스탬프를 자체 시계와 비교합니다. 이벤트가 5분 이상 더 오래되었다면 ASA는 메시지를 수락하지 않습니다. ASA, Active Directory, AD 에이전트끼리 NTP를 사용하여 시계를 동기화하도록 구성하는 것이 좋습니다.
15단계	**user-identity ad-agent aaa-server** *aaa_server_group_tag* 예: `ciscoasa(config)# user-identity ad-agent aaa-server adagent`	AD 에이전트의 서버 그룹을 정의합니다. *aaa_server_group_tag* 인수에는 **aaa-server** 명령에서 정의한 값을 입력합니다.

다음에 할 일

Active Directory 도메인 및 서버 그룹을 구성합니다. 31-10 페이지의 AD 도메인 구성을 참조하십시오.

AD 에이전트를 구성합니다. 31-12 페이지의 AD 에이전트 구성을 참조하십시오.

ID 기반 보안 정책 구성

다양한 ASA 기능에 ID 기반 정책을 통합할 수 있습니다. (31-7 페이지의 지침 및 제한 사항에서 지원되지 않는다고 표시된 것을 제외하고) 확장 ACL을 사용하는 어떤 기능도 ID 방화벽을 활용할 수 있습니다. 이제 네트워크 기반 매개 변수뿐 아니라 사용자 ID 인수를 확장 ACL에 추가할 수 있습니다.

- 확장 ACL을 구성하려면 17 장, "액세스 제어 목록"을 참조하십시오.
- ACL에서 사용 가능한 로컬 사용자 그룹을 구성하려면 16-6 페이지의 로컬 사용자 그룹 구성을 참조하십시오.

다음과 같은 기능에서 ID를 사용할 수 있습니다.

- 액세스 규칙—액세스 규칙은 네트워크 정보를 사용하여 인터페이스에서 트래픽을 허용하거나 거부합니다. ID 방화벽을 사용하면 사용자 ID를 기반으로 액세스를 제어할 수 있습니다. 방화벽 컨피그레이션 가이드를 참조하십시오.
- AAA 규칙—(컷스루 프록시라고도 하는) 인증 규칙은 사용자를 기반으로 네트워크 액세스를 제어합니다. 이 기능은 액세스 규칙에 ID 방화벽을 더한 것과 매우 비슷하므로, 사용자의 AD 로그인이 만료될 경우 대체 인증 방법으로 AAA 규칙을 사용할 수 있습니다. 예를 들어, 유효한 로그인이 없는 사용자에 대해 AAA 규칙을 트리거할 수 있습니다. 유효한 로그인이 없는 사용자에 한해 AAA 규칙이 트리거되도록 액세스 규칙 및 AAA 규칙에 쓰이는 확장 ACL에 해당 사용자 이름을 지정할 수 있습니다(None(유효한 로그인이 없는 사용자) 및 Any(유효한 로그인이 있는 사용자)). 액세스 규칙에서는 사용자 및 그룹에 대해 평소와 같이 정책을 구성하되 모든 None 사용자를 허용하는 AAA 규칙을 포함합니다. 이 사용자를 허용해야 나중에 AAA 규칙이 트리거될 수 있습니다. 그리고 Any 사용자(이 사용자는 AAA 규칙의 대상이 아니며, 이미 액세스 규칙에 의해 처리되었음)를 거부하되 모든 None 사용자를 허용하는 AAA 규칙을 구성합니다. 예:

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
```

```
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

자세한 내용은 기존 기능 가이드를 참조하십시오.

- Cloud Web Security—어떤 사용자를 Cloud Web Security 프록시 서버에 보낼지 제어할 수 있습니다. 또한 Cloud Web Security에 보내진 ASA 트래픽 헤더에 포함된 사용자 그룹을 기반으로 하는 정책을 Cloud Web Security ScanCenter에서 구성할 수 있습니다. 방화벽 컨피그레이션 가이드를 참조하십시오.
- VPN 필터—VPN은 일반적으로 ID 방화벽 ACL을 지원하지 않지만, ASA에서 VPN 트래픽에 대해 ID 기반 액세스 규칙을 강제적으로 적용하도록 구성할 수 있습니다. 기본적으로 VPN 트래픽은 액세스 규칙의 대상이 아닙니다. VPN 클라이언트에서 ID 방화벽 ACL을 사용하는 액세스 규칙을 반드시 준수하게 할 수 있습니다(**no sysopt connection permit-vpn** 명령 사용). 또한 VPN 필터 기능과 함께 ID 방화벽 ACL을 사용할 수 있습니다. VPN 필터는 대체로 허용 액세스 규칙과 비슷한 효과를 발휘합니다.

사용자 통계 수집

Modular Policy Framework에 의한 사용자 통계 수집 및 ID 방화벽에 대한 매칭 조회 작업을 활성화하려면 다음 명령을 입력합니다.

명령	목적
user-statistics [**accounting** | **scanning**] **예:** `ciscoasa(config)# class-map c-identity-example-1` `ciscoasaciscoasa(config-cmap)# match access-list identity-example-1` `ciscoasaciscoasa(config-cmap)# exit` `ciscoasaciscoasa(config)# policy-map p-identity-example-1` `ciscoasaciscoasa(config-pmap)# class c-identity-example-1` `ciscoasaciscoasa(config-pmap)# user-statistics accounting` `ciscoasaciscoasa(config-pmap)# exit` `ciscoasaciscoasa(config)# service-policy p-identity-example-1 interface outside`	Modular Policy Framework에 의한 사용자 통계 수집 및 ID 방화벽에 대한 매칭 조회 작업을 활성화합니다. **accounting** 키워드는 ASA에서 전송된 패킷 수, 전송된 드롭 수, 수신된 패킷 수를 수집하도록 지정합니다. **scanning** 키워드는 ASA에서 전송된 드롭 수만 수집하도록 지정합니다. 사용자 통계를 수집하도록 정책 맵을 구성하면 ASA에서는 선택된 사용자에 대한 세부적인 통계를 수집합니다. 사용자가 **user-statistics** 명령을 **accounting** 또는 **scanning** 키워드 없이 지정하면 ASA에서는 어카운팅 및 검사 통계를 모두 수집합니다.

컨피그레이션의 예

- 31-19 페이지의 AAA 규칙과 액세스 규칙 예 1
- 31-19 페이지의 AAA 규칙과 액세스 규칙 예 2
- 31-20 페이지의 VPN 필터의 예

AAA 규칙과 액세스 규칙 예 1

이 예에서는 사용자가 ASA를 통해 로그인하는 것을 허용하는 일반적인 컷스루 프록시 컨피그레이션을 보여줍니다. 여기서는 다음 조건이 적용됩니다.

- ASA IP 주소는 172.1.1.118입니다.
- AD 도메인 컨트롤러의 IP 주소는 71.1.2.93입니다.
- 최종 사용자 클라이언트는 IP 주소가 172.1.1.118이고, 웹 포털을 통해 로그인하는 데 HTTPS를 사용합니다.
- 사용자는 LDAP을 통해 AD 도메인 컨트롤러에 의해 인증됩니다.
- ASA에서는 내부 인터페이스를 사용하여 회사 네트워크에 있는 AD 도메인 컨트롤러에 연결합니다.

```
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq http
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq https
ciscoasa(config)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 171.1.2.93
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-dn cn=kao,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-login-password *****
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
ciscoasa(config-aaa-server-host)# aaa authentication match AUTH inside LDAP
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 0.0.0.0 0.0.0.0 inside
ciscoasa(config)#
ciscoasa(config)# auth-prompt prompt Enter Your Authentication
ciscoasa(config)# auth-prompt accept You are Good
ciscoasa(config)# auth-prompt reject Goodbye
```

AAA 규칙과 액세스 규칙 예 2

여기서는 다음 지침이 적용됩니다.

- 인증되지 않은 수신 사용자가 AAA 컷스루 프록시를 트리거할 수 있도록 **access list** 명령에서 permit user NONE 규칙을 먼저 작성한 다음 **access-list 100 ex deny any any** 명령을 입력해야 합니다.
- **auth access-list** 명령에서 permit user NONE 규칙은 오로지 인증되지 않은 경우에만 컷스루 프록시를 트리거하게 합니다. 원칙적으로 맨 마지막 라인이 되어야 합니다.

```
ciscoasa(config)# access-list listenerAuth extended permit tcp any any
ciscoasa(config)# aaa authentication match listenerAuth inside ldap
ciscoasa(config)# aaa authentication listener http inside port 8888
ciscoasa(config)# access-list 100 ex permit ip user SAMPLE\user1 any any
ciscoasa(config)# access-list 100 ex deny ip user SAMPLE\user2 any any
ciscoasa(config)# access-list 100 ex permit ip user NONE any any
ciscoasa(config)# access-list 100 ex deny any any
ciscoasa(config)# access-group 100 in interface inside
ciscoasa(config)# aaa authenticate match 200 inside user-identity
```

VPN 필터의 예

ID 방화벽을 우회해야 하는 트래픽이 있습니다.

ASA는 VPN 인증을 통해 또는 웹 포털(컷스루 프록시)을 통해 로그인하는 사용자를 AD 에이전트에 보고합니다. 그러면 AD 에이전트는 사용자 정보를 모든 등록된 ASA 디바이스에 배포합니다. 구체적으로 설명하자면, 인증된 사용자의 IP-사용자 매핑이 입력 인터페이스가 있는 모든 ASA 컨텍스트에 전달됩니다. 이 인터페이스에서 HTTP/HTTPS 패킷이 수신되고 인증됩니다. ASA에서는 VPN을 통해 로그인하는 사용자를 LOCAL 도메인에 속한 것으로 표시합니다.

VPN 사용자에게 IDFW(identity firewall) 규칙을 적용하는 2가지 방법이 있습니다.

- bypassing access-list check를 비활성화한 상태에서 VPN 필터 적용
- bypassing access-list check를 활성화한 상태에서 VPN 필터 적용

IDFW 규칙을 사용하는 VPN - 예 1

기본적으로 **sysopt connection permit-vpn** 명령은 활성화되어 있고 VPN 트래픽은 액세스 목록 검사에서 면제됩니다. VPN 트래픽에 인터페이스 기반 ACL 규칙을 적용하려면 VPN 트래픽 액세스 목록 우회를 비활성화해야 합니다.

이 예에서는 사용자가 외부 인터페이스에서 로그인할 경우 IDFW 규칙에 따라 액세스 가능한 네트워크 리소스를 제어합니다. 모든 VPN 사용자는 LOCAL 도메인에 저장되어야 합니다. 따라서 LOCAL 사용자에게 또는 LOCAL 사용자를 포함하는 객체 그룹에 규칙을 적용하는 것만이 의미 있습니다.

```
! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

IDFW 규칙을 사용하는 VPN - 예 2

기본적으로 **sysopt connection permit-vpn** 명령은 활성화되어 있고 VPN 트래픽 액세스 우회도 활성화되어 있습니다. VPN 필터는 IDFW 규칙을 VPN 트래픽에 적용하는 데 사용할 수 있습니다. IDFW 규칙이 있는 VPN 필터는 CLI 사용자 이름 및 그룹 정책에서 정의할 수 있습니다.

이 예에서는 사용자 idfw가 로그인하면 10.0.00/24 서브넷의 네트워크 리소스에 액세스할 수 있습니다. 그러나 사용자 user1이 로그인하면 10.0.00/24 서브넷의 네트워크 리소스에 대한 액세스가 거부됩니다. 모든 VPN 사용자는 LOCAL 도메인에 저장되어야 합니다. 따라서 LOCAL 사용자에게 또는 LOCAL 사용자를 포함하는 객체 그룹에 규칙을 적용하는 것만이 의미 있습니다.

참고 IDFW 규칙은 그룹 정책의 VPN 필터에만 적용할 수 있으며, 다른 그룹 정책 기능에는 사용하지 못할 수도 있습니다.

```
! Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYVi6IFLEsYv encrypted privilege 0 username user1 attributes
    vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
    vpn-group-policy testgroup vpn-filter value v1
```

```
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0 access-list
v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0 group-policy group1
internal
group-policy group1 attributes

    vpn-filter value v1
    vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
```

ID 방화벽 모니터링

AD 에이전트 모니터링

AD 에이전트를 위한 문제 해결 정보를 얻으려면 다음 명령 중 하나를 사용합니다.

- **show user-identity ad-agent**
- **show user-identity ad-agent statistics**

이 명령은 기본 및 보조 AD 에이전트에 대한 다음 정보를 표시합니다.

- AD 에이전트의 상태
- 도메인의 상태
- AD 에이전트의 통계

그룹 모니터링

ID 방화벽에 대해 구성된 사용자 그룹에 대한 문제 해결 정보를 얻으려면 **show user-identity group** 명령을 사용합니다.

ID 방화벽의 메모리 사용량 모니터링

ID 방화벽의 메모리 사용량에 대한 문제 해결 정보를 수집하려면 **show user-identity memory** 명령을 사용합니다.

이 명령은 ID 방화벽에 있는 여러 모듈의 메모리 사용량을 바이트로 표시합니다.

- 사용자
- 그룹
- 사용자 통계
- LDAP

  ASA에서는 AD 서버에 구성된 AD 그룹에 대한 LDAP 쿼리를 보냅니다. AD 서버가 사용자를 인증하고 사용자 로그인 보안 로그를 생성합니다.

- AD 에이전트
- 기타
- 총 메모리 사용량

참고 ID 방화벽에서 AD 에이전트로부터 사용자 정보를 검색하도록 어떻게 구성했느냐에 따라 이 기능의 메모리 사용량이 달라집니다. ASA에서 온디맨드 검색을 아니면 전체 다운로드 검색을 사용할 것인지 지정합니다. 온디맨드 검색을 선택하면 수신된 패킷의 사용자만 쿼리하고 저장하므로 메모리를 더 적게 사용한다는 이점이 있습니다. 자세한 내용은 31-13 페이지의 ID 옵션 구성을 참조하십시오.

ID 방화벽의 사용자 모니터링

AD 에이전트를 위한 문제 해결 정보를 얻으려면 다음 명령 중 하나를 입력합니다.

- **show user-identity user all list**
- **show user-identity user active user** *domain\user-name* **list detail**

이 명령은 사용자에 대한 다음 정보를 표시합니다.

domain\user_name 상태(활성 또는 비활성) Connections 유휴 시간(분)

domain\user_name 활성 연결 유휴 시간(분)

기본 도메인 이름은 실제 도메인 이름, 특별 예약어 또는 LOCAL일 수 있습니다. ID 방화벽은 모든 로컬에 정의된 사용자 그룹 또는 로컬에 정의된 사용자(VPN 또는 웹 포털을 사용하여 로그인하고 인증한 사용자)에게 LOCAL 도메인 이름을 사용합니다. 기본 도메인이 지정되지 않은 경우 기본 도메인은 LOCAL입니다.

유휴 시간은 사용자의 IP 주소를 기준으로 하지 않고 사용자별로 저장됩니다.

user-identity action domain-controller-down *domain_name* **disable-user-identity-rule** 명령이 구성되었고 지정된 도메인이 중지된 상태라면 또는 **user-identity action ad-agent-down disable-user-identity-rule** 명령이 구성되었고 AD 에이전트가 중지된 상태라면 로그인한 모든 사용자는 비활성 상태가 됩니다.

ID 방화벽 기능 내역

표 31-1에서는 이 기능의 출시 내역을 정리합니다.

표 31-1 ID 방화벽 기능 내역

기능 이름	릴리스	기능 정보
ID 방화벽	8.4(2)	ID 방화벽 기능을 도입했습니다. 도입되고 수정된 명령: **user-identity enable, user-identity default-domain, user-identity domain, user-identity logout-probe, user-identity inactive-user-timer, user-identity poll-import-user-group-timer, user-identity action netbios-response-fail, user-identity user-not-found, user-identity action ad-agent-down, user-identity action mac-address-mismatch, user-identity action domain-controller-down, user-identity ad-agent active-user-database, user-identity ad-agent hello-timer, user-identity ad-agent aaa-server, user-identity update import-user**, **user-identity static user**, **dns domain-lookup**, **dns poll-timer**, **dns expire-entry-timer**, **object-group user, show user-identity**, **show dns, clear configure user-identity**, **clear dns, debug user-identity**

32 장

ASA 및 Cisco TrustSec

Cisco TrustSec과 통합된 ASA 정보

Cisco TrustSec 정보

전통적으로 방화벽과 같은 보안 기능은 미리 정의된 IP 주소, 서브넷 및 프로토콜에 따라 액세스 제어를 수행했습니다. 하지만 기업이 경계 없는 네트워크로 전환함에 따라 사람과 조직을 연결하는 기술과 데이터 및 네트워크 보호를 위한 보안 요구 사항 모두 크게 달라졌습니다. 엔드포인트의 유동성이

점차 심해지고 사용자는 다양한 엔드포인트(예: 노트북과 데스크톱, 스마트폰 또는 태블릿)를 사용하기 때문에 사용자 속성과 엔트포인트 속성이 조합되면서 기존 6-tuple 기반 규칙에 더하여 방화벽 기능을 갖춘 스위치나 라우터 또는 전용 방화벽과 같은 디바이스를 안정적으로 액세스 제어 결정에도 활용할 수 있는 조건을 갖추게 되었습니다.

따라서 엔드포인트 속성 또는 클라이언트 ID 속성의 가용성과 전파가 고객 네트워크 전반, 네트워크의 액세스, 배포 및 핵심 레이어, 그리고 데이터 센터의 보안을 지원하는 중요한 요구 사항이 되고 있습니다.

Cisco TrustSec은 기존 identity-aware 인프라 위에 구축되어 네트워크 디바이스 간 데이터 기밀을 보장하고 하나의 플랫폼으로 보안 액세스 서비스를 통합합니다. Cisco TrustSec 기능에서 적용 디바이스는 사용자 속성과 엔드포인트 속성의 조합을 사용하여 역할 기반 및 ID 기반 액세스 제어 결정을 내립니다. 이 정보의 가용성과 전파는 네트워크의 액세스, 배포 및 핵심 레이어에서 네트워크 전반의 보안을 활성화합니다.

Cisco TrustSec을 구현하면 다음과 같은 이점을 얻을 수 있습니다.

- 점차 늘어나는 모바일 및 복합 인력이 어떤 디바이스에서든 더 안전하고 알맞은 액세스를 할 수 있게 해줍니다.
- 누가 무엇으로 유선 또는 무선 네트워크에 연결하는지 포괄적인 가시성을 제공하여 보안 위험을 완화합니다.
- 물리적 또는 클라우드 기반 IT 리소스에 액세스하는 네트워크 사용자의 활동에 대한 뛰어난 관리 기능을 제공합니다.
- 고도로 안전한 중앙 집중식 액세스 정책 관리 및 확장 가능한 적용 메커니즘을 통해 총 소유 비용을 줄입니다.

다양한 Cisco 제품에서의 Cisco TrustSec 기능 사용에 관한 자세한 정보는 32-29 페이지의 추가 참조 자료를 참조하십시오.

Cisco TrustSec에서의 SGT 및 SXP 지원 정보

Cisco TrustSec 기능에서 보안 그룹 액세스는 토폴로지 인식 네트워크를 역할 기반 네트워크로 바꾸어 역할 기반 액세스 제어(RBAC)로 엔드-투-엔드 정책을 적용할 수 있게 합니다. 인증 과정에서 얻은 디바이스와 사용자 자격 증명은 보안 그룹별로 패킷을 분류하는 데 사용됩니다. Cisco TrustSec 클라우드에 진입하는 모든 패킷은 SGT(security group tag)로 태그됩니다. 태깅은 믿을 수 있는 매개자가 패킷의 소스 ID를 확인하고 데이터 경로를 따라 보안 정책을 적용할 수 있게 합니다. SGT는 SGT가 보안 그룹 ACL 정의에 사용될 때 도메인 전반에서 권한 수준을 나타냅니다.

SGT는 RADIUS vendor-specific 속성으로 이루어지는 IEEE 802.1X 인증, 웹 인증 또는 MAC 인증 바이패스(MAB)를 통해 디바이스에 할당됩니다. SGT는 특정 IP 주소 또는 스위치 인터페이스에 전략적으로 할당될 수 있습니다. SGT는 인증 성공 후 스위치 또는 액세스 포인트에 동적으로 전달됩니다.

SXP(Security-group eXchange Protocol)는 SGT 지원 하드웨어가 없는 네트워크 디바이스 전반에서 IP-to-SGT 매핑 데이터베이스를 SGT와 보안 그룹 ACL을 지원하는 하드웨어로 전파하도록 Cisco TrustSec을 위해 개발된 프로토콜입니다. 컨트롤 플레인 프로토콜인 SXP는 인증 포인트(레거시 액세스 레이어 스위치 등)에서 네트워크의 업스트림 디바이스로 IP-SGT 매핑을 전달합니다.

SXP 연결은 point-to-point 연결이며 TCP를 기본 전송 프로토콜로 사용합니다. SXP는 잘 알려진 TCP 포트 번호인 64999를 사용하여 연결을 개시합니다. 또한 SXP 연결은 소스와 대상 IP 주소를 통해 고유하게 식별됩니다.

Cisco TrustSec 기능의 역할

ID 및 정책 기반 액세스 정책을 위해 Cisco TrustSec 기능은 다음 역할을 포함합니다.

- 액세스 요청자(AR)—액세스 요청자는 네트워크의 보호된 리소스에 대한 액세스를 요청하는 엔드포인트 디바이스입니다. 아키텍처의 주된 주체이며 이들의 액세스 권한은 ID 자격 증명에 달려 있습니다.

  액세스 요청자에는 PC, 랩톱, 휴대폰, 프린터, 카메라 및 MACsec-capable IP 전화와 같은 엔드포인트 디바이스가 포함됩니다.

- PDP(Policy Decision Point)—정책 결정 포인트는 액세스 제어 결정을 책임집니다. PDP는 802.1x, MAB 및 웹 인증과 같은 기능을 제공합니다. PDP는 VLAN, DACL을 통한 인증 및 정책 적용, 보안 그룹 액세스(SGACL/SXP/SGT)를 지원합니다.

  Cisco TrustSec 기능에서는 Cisco ISE(Identity Services Engine)가 PDP 역할을 합니다. Cisco ISE는 ID 및 액세스 제어 정책 기능을 제공합니다.

- PIP(Policy Information Point)—정책 정보 포인트는 외부 정보(예: 평판, 위치 및 LDAP 속성)를 정책 결정 포인트로 제공하는 소스입니다.

  정책 정보 포인트는 Session Directory, Sensor IPS 및 Communication Manager와 같은 디바이스를 포함합니다.

- PAP(Policy Administration Point)—정책 관리 포인트는 권한 부여 시스템으로의 정책을 정의하고 삽입합니다. PAP는 Cisco TrustSec tag-to-user ID 매핑과 Cisco TrustSec tag-to-server 리소스 매핑을 제공함으로써 ID 저장소 역할을 합니다.

  Cisco TrustSec 기능에서는 Cisco Secure Access Control System(802.1x 및 SGT 지원이 통합된 정책 서버)이 PAP 역할을 합니다.

- PEP(Policy Enforcement Point)—정책 시행 포인트는 각 AR에 대해 PDP가 결정한 사항(정책 규칙 및 작업)을 실행합니다. PEP 디바이스는 네트워크에 걸쳐 존재하는 기본 통신 경로를 통해 ID 정보를 학습합니다. PEP 디바이스는 엔드포인트 에이전트, 권한 부여 서버, 피어 시행 디바이스 및 네트워크 흐름과 같은 여러 소스로부터 각 AR의 ID 속성을 학습합니다. PEP 디바이스는 SXP를 사용하여 네트워크 전체의 신뢰할 수 있는 피어 디바이스로 IP-SGT 매핑을 전파합니다.

  정책 시행 포인트는 Catalyst 스위치, 라우터, 방화벽(특히 ASA), 서버, VPN 디바이스 및 SAN 디바이스와 같은 네트워크 디바이스를 포함합니다.

Cisco ASA은(는) ID 아키텍처에서 PEP 역할을 수행합니다. SXP를 사용하여 ASA는 인증 포인트로부터 직접 ID 정보를 학습하고 이를 이용하여 ID 기반 정책을 적용합니다.

보안 그룹 정책 적용

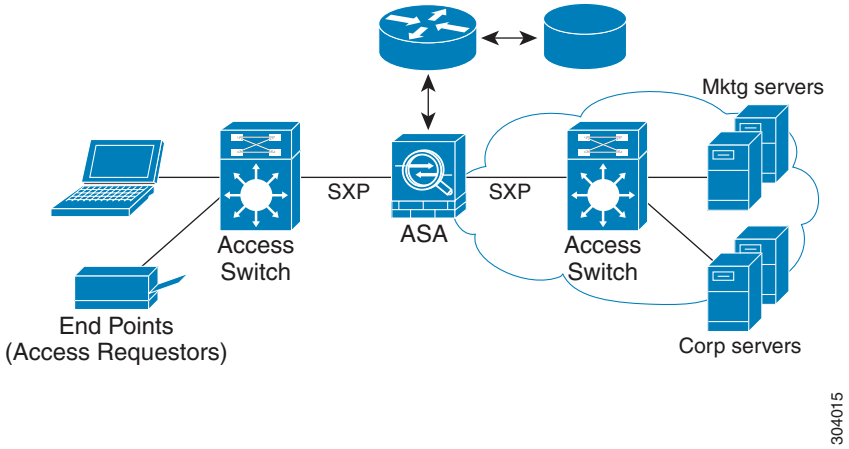
보안 정책 시행은 보안 그룹 이름을 기반으로 합니다. 엔드포인트 디바이스가 데이터 센터의 리소스 액세스를 시도합니다. 방화벽에 구성된 기존 IP 기반 정책과 달리 ID 기반 정책은 사용자 및 디바이스 ID를 기준으로 구성됩니다. 예를 들어 mktg-contractor는 mktg-servers에 액세스할 수 있고 mktg-corp-users는 mktg-server 및 corp-servers에 액세스할 수 있습니다.

이 배포 유형의 장점은 다음과 같습니다.

- 사용자 그룹과 리소스는 단일 객체(SGT) 간소화 정책 관리를 이용하여 정의 및 시행됩니다.
- 사용자 ID 및 리소스 ID는 Cisco TrustSec-capable 스위치 인프라 전반에서 보존됩니다.

그림 32-1은 보안 그룹 이름 기반 정책 시행 배포를 보여줍니다.

그림 32-1 보안 그룹 이름 기반 정책 시행 배포



Cisco TrustSec을 구현하면 서버 분할을 지원하고 다음을 포함하는 보안 정책을 구성할 수 있습니다.

- 정책 관리 간소화를 위해 서버 풀에 SGT를 할당할 수 있습니다.
- SGT 정보는 Cisco TrustSec 지원 스위치 인프라 내에 보존됩니다.
- ASA은(는) Cisco TrustSec 도메인 전체에 걸쳐 정책 시행을 위해 IP-SGT 매핑을 사용합니다.
- 서버에 대한 802.1x 권한 부여가 필수이므로 구축 간소화가 가능합니다.

ASA의 보안 그룹 기반 정책 시행 방법

참고 사용자 기반 보안 정책과 보안 그룹 기반 정책이 ASA에서 공존할 수 있습니다. 네트?, 사용자 기반 및 보안 그룹 기반 속성의 어떤 조합이라도 보안 정책에서 구성할 수 있습니다. 사용자 기반 보안 정책 구성에 관한 정보는 31 장, "ID 방화벽"에서 참조하십시오.

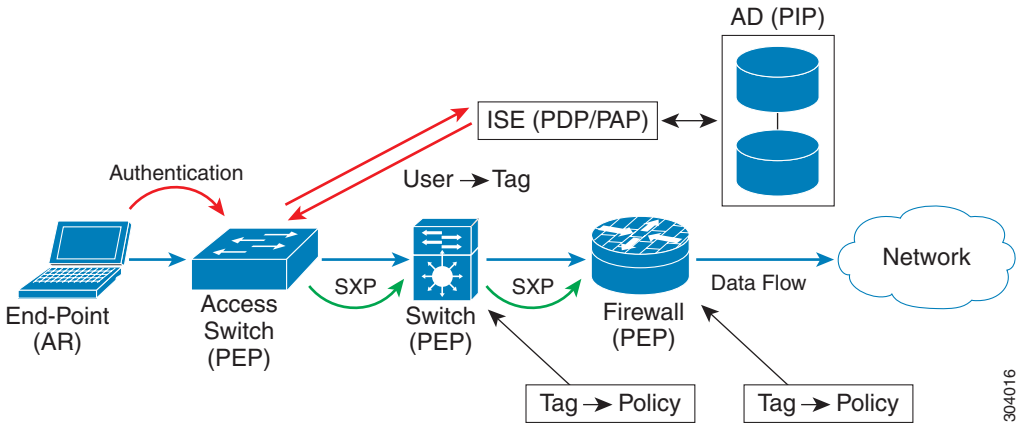
ASA를 Cisco TrustSec과 함께 작동하도록 구성하려면 ISE에서 PAC(Protected Access Credential) 파일을 가져와야 합니다. 자세한 내용은 32-15 페이지의 PAC 파일 가져오기를 참조하십시오.

PAC 파일을 ASA로 가져오면 ISE와의 안전한 통신 채널이 설정됩니다. 채널을 설정하고 나면 ASA가 ISE와 PAC 보안 RADIUS 트랜잭션을 시작하고 Cisco TrustSec 환경 데이터(보안 그룹 테이블)를 다운로드합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다.

ASA가 보안 그룹 테이블을 처음 다운로드할 때 테이블의 모든 엔트리를 점검하고 구성된 보안 정책에 포함된 모든 보안 그룹 이름을 확인하고 나면 ASA이(가) 이 보안 정책을 로컬로 활성화합니다. ASA가 보안 그룹 이름을 확인할 수 없다면 알 수 없는 보안 그룹 이름에 대한 syslog 메시지를 생성합니다.

그림 32-2는 Cisco TrustSec에서 보안 정책 시행 방식을 보여줍니다.

그림 32-2 보안 정책 시행



1. 엔드포인트 디바이스가 액세스 디바이스에 직접 연결하거나 원격 액세스를 통해 연결하고 Cisco TrustSec으로 인증합니다.
2. 액세스 레이어 디바이스는 802.1X 또는 웹 인증과 같은 인증 방식을 사용하여 ISE로 엔드포인트 디바이스를 인증합니다. 엔드포인트 디바이스가 역할 및 그룹 멤버십 정보를 전달하여 디바이스를 적절한 보안 그룹으로 분류합니다.
3. 액세스 레이어 디바이스는 SXP를 사용하여 IP-SGT 매핑을 업스트림 디바이스로 전파합니다.
4. ASA가 패킷을 수신하고 SXP가 전달한 IP-SGT 매핑을 이용하여 SGT에서 소스 및 대상 IP 주소를 찾습니다.

   신규 매핑의 경우 ASA가 로컬 IP-SGT Manager 데이터베이스에 기록합니다. 컨트롤 플레인에서 실행되는 IP-SGT Manager 데이터베이스는 각 IPv4 또는 IPv6 주소에 대해 IP-SGT 매핑을 추적합니다. 데이터베이스는 매핑을 학습한 소스를 기록합니다. SXP 연결의 피어 IP 주소가 매핑 소스로 사용됩니다. 각 IP-SGT 매핑 엔트리에 대해 여러 소스가 존재할 수 있습니다.

   ASA가 Speaker로 구성된 경우 ASA는 모든 IP-SGT 매핑 엔트리를 SXP 피어로 전송합니다. 자세한 내용은 32-6 페이지의 ASA에서 스피커 및 리스너 역할에 관해를 참조하십시오.
5. 보안 정책이 ASA에서 해당 SGT 또는 보안 그룹 이름으로 구성된 경우 ASA가 정책을 시행합니다. (ASA에서 SGT 또는 보안 그룹 이름을 포함하는 보안 정책을 생성할 수 있습니다. 보안 그룹 이름을 기준으로 정책을 시행하기 위해 ASA는 보안 그룹 이름을 SGT에 매핑할 보안 그룹 테이블을 필요로 합니다.)

   ASA가 보안 그룹 테이블에서 보안 그룹 이름을 찾을 수 없고 이것이 보안 정책에 포함된 경우 ASA는 보안 그룹 이름을 알 수 없는 것으로 간주하고 syslog 메시지를 생성합니다. ASA이(가) ISE에서 보안 그룹 테이블을 갱신하고 보안 그룹 이름을 알게된 후 ASA는 syslog 메시지를 생성하여 보안 그룸 이름이 확인되었음을 알립니다.

ISE의 보안 그룹 변경이 주는 영향

ASA는 ISE에서 업데이트된 테이블을 다운로드함으로써 보안 그룹 테이블을 주기적으로 갱신합니다. 다운로드할 때마다 ISE에서 보안 그룹이 변경될 수 있습니다. 이러한 변화는 보안 그룹 테이블을 갱신하기 전에는 ASA에 반영되지 않습니다.

팁 유지 관리 중에 ISE에서 정책 컨피그레이션 변경을 예약한 후 ASA에서 수동으로 보안 그룹 테이블을 갱신하여 보안 그룹 변경 사항이 통합되도록 확인하는 것이 좋습니다.

이 방법으로 정책 컨피그레이션 변경 사항을 다루면 보안 그룹 이름 확인 및 보안 정책의 즉각적인 활성화 가능성이 높아집니다.

보안 그룹 테이블은 환경 데이터 타이머가 만료되면 자동으로 갱신됩니다. 또한 온디맨드로 보안 그룹 테이블 갱신을 트리거할 수 있습니다.

ISE에서 보안 그룹이 변경되면 ASA가 보안 그룹 테이블을 갱신할 때 이벤트가 발생합니다.

- 보안 그룹 이름을 사용하여 구성된 보안 그룹 정책만 보안 그룹 테이블로 확인할 필요가 있습니다. 보안 그룹 태그를 포함하는 정책은 항상 활성 상태입니다.
- 보안 그룹 테이블을 처음 사용할 수 있게 되면 보안 그룹 이름을 가진 모든 정책이 설명되고 보안 그룹 이름이 확인되며 정책이 활성화됩니다. 태그가 지정된 모든 정책이 설명되고 알려진 태그에 대해 syslogs가 생성됩니다.
- 보안 그룹 테이블이 만료되면 직접 삭제할 때까지 또는 새로운 테이블을 사용할 수 있을 때까지 가장 최근에 다운로드한 보안 그룹 테이블에 따라 정책이 계속해서 시행됩니다.
- 확인된 보안 그룹 이름이 ASA에서 알 수 없음 상태가 되면 보안 정책이 비활성화됩니다. 하지만 보안 정책은 ASA 실행 중인 컨피그레이션에 계속 남습니다.
- PAP에서 기존 보안 그룹이 삭제되면 이전에 알려진 보안 그룹 태그가 알 수 없는 상태가 되지만 ASA에서 정책 상태는 변하지 않습니다. 이전에 알려진 보안 그룹 이름이 미확인 상태가 되고 정책이 비활성화됩니다. 보안 그룹 이름이 재사용되면 정책이 새로운 태그를 이용하여 다시 컴파일됩니다.
- PAP에 새로운 보안 그룹이 추가되면 이전에 알려지지 않았던 보안 그룹 태그가 알려지고 syslog 메시지가 생성되지만 정책 상태는 변하지 않습니다. 이전에 알려지지 않았던 보안 그룹 이름이 확인되고 연결된 정책이 활성화됩니다.
- PAP에서 태그 이름이 변경되면 태그를 이용하여 구성되었던 정책이 새로운 이름을 표시하고 정책 상태는 변경되지 않습니다. 보안 그룹 이름으로 구성되었던 정책이 새로운 태그 값을 사용하여 다시 컴파일됩니다.

ASA에서 스피커 및 리스너 역할에 관해

ASA는 다른 네트워크 디바이스로부터 IP-SGT 매핑 엔트리를 주고받도록 SXP를 지원합니다. SXP를 사용하면 보안 디바이스와 방화벽이 하드웨어 업그레이드나 변경 없이 액세스 스위치로부터 ID 정보를 학습할 수 있습니다. SXP는 또한 IP-SGT 매핑 엔트리를 업스트림 디바이스(데이터 센터 디바이스 등)에서 다운스트림 디바이스로 전달할 때도 사용됩니다. ASA는 업스트림 및 다운스트림 방향 모두에서 정보를 받을 수 있습니다.

ASA에서 SXP 피어로 SXP 연결을 구성할 때는 해당 연결에 대해 ASA을(를) 스피커 또는 리스너로 지정하여 ID 정보를 교환할 수 있도록 해야 합니다.

- 스피커 모드—ASA가 ASA에서 수집한 모든 활성 IP-SGT 매핑 엔트리를 정책 시행을 위해 업스트림 디바이스로 전달할 수 있도록 구성합니다.
- 리스너 모드—ASA가 다운스트림 디바이스(SGT 지원 스위치)로부터 IP-SGT 매핑 엔트리를 수신하고 이 정보를 사용하여 정책 정의를 생성할 수 있도록 구성합니다.

SXP 연결의 한 쪽이 스피커로 구성된 경우 다른 한쪽은 리스너로 구성되어야 합니다. SXP 연결의 양쪽에 있는 두 디바이스가 모두 같은 역할(둘 다 스피커 또는 리스너)로 구성된 경우 SXP 연결이 실패하고 ASA가 syslog 메시지를 생성합니다.

Multiple SXP 연결은 IP-SGT 매핑 데이터베이스에서 다운로드된 IP-SGT 매핑 엔트리를 학습할 수 있습니다. ASA에서 SXP 피어로의 SXP 연결이 설정된 후 리스너가 전체 IP-SGT 데이터베이스를 스피커에서 다운로드합니다. 이후 발생하는 모든 변경 사항은 네트워크에 새로운 디바이스가 나타날 때만 전송됩니다. 따라서 SXP 정보 흐름의 속도는 호스트가 네트워크에 인증되는 속도에 비례합니다.

SXP 연결을 통해 학습된 IP-SGT 매핑 엔트리는 SXP IP-SGT 매핑 데이터베이스에서 유지됩니다. 서로 다른 SXP 연결을 통해 동일한 매핑 엔트리를 학습할 수 있습니다. 매핑 데이터베이스는 학습한 각 매핑 엔트리에 대해 하나의 사본을 유지합니다. 동일한 IP-SGT 매핑 값을 가진 여러 매핑 엔트리는 매핑이 학습된 연결에서 피어 IP 주소에 의해 식별됩니다. SXP는 새로운 매핑이 처음 학습되면 IP-SGT Manager가 매핑 엔트리를 추가하고 SXP 데이터베이스의 마지막 사본이 삭제되면 매핑 엔트리를 삭제하도록 요청합니다.

SXP 연결이 스피커로 구성되어 있으면 SXP는 항상 IP-SGT Manager에게 디바이스에서 수집된 모든 매핑 엔트리를 피어로 전달할 것을 요청합니다. 새로운 매핑이 로컬로 학습되면 IP-SGT Manager는 SXP가 스피커로 구성된 연결을 통해 이를 전달할 것을 요청합니다.

ASA를 SXP 연결을 위한 스피커와 리스너로 동시에 구성하면 SXP 루핑이 발생하여 SXP 데이터를 처음에 전송한 SXP 피어가 다시 이 데이터를 수신하게 됩니다.

SXP Chattiness

SXP 정보 흐름의 속도는 호스트가 네트워크에 인증되는 속도에 비례합니다. SXP 피어링이 설정된 후 리스너 디바이스가 스피커 디바이스에서 전체 IP-SGT 데이터베이스를 다운로드합니다. 그 후 모든 변경 사항은 새로운 디바이스가 네트워크에 나타나거나 네트워크를 떠날 때만 증분적으로 전송됩니다. 또한 새로운 디바이스에 연결된 액세스 디바이스만 업스트림 디바이스로의 이러한 증분적인 업데이트를 시작할 수 있습니다.

다시 말하면 SXP 프로토콜은 인증 서버의 기능으로 제한되는 인증 속도보다 빠르지 않습니다. 따라서 SXP chattiness는 중요한 문제가 아닙니다.

SXP 타이머

- Retry Open Timer—열기 재시도 타이머는 디바이스의 특정 SXP 연결이 연결되지 않은 경우 트리거됩니다. 열기 재시도 타이머가 종료되면 디바이스가 전체 연결 데이터베이스를 점검하고 연결이 꺼져 있거나 "대기" 상태인 경우 열기 재시도 타이머가 재시작됩니다. 기본 타이머 값은 120초입니다. 값이 0이면 재시도 타이머가 시작되지 않습니다. 열기 재시도 타이머는 모든 SXP 연결이 설정될 때까지 또는 열기 재시도 타이머가 0으로 구성될 때까지 계속됩니다.
- Delete Hold-Down Timer—연결별 삭제 보류 타이머는 리스너의 연결이 해제될 때 트리거됩니다. 학습된 매핑 엔트리는 즉시 삭제되지 않고 삭제 보류 타이머가 만료될 때까지 유지됩니다. 이 타이머가 만료된 후 매핑 엔트리가 삭제됩니다. 삭제 보류 타이머 값은 120초로 설정되며 변경할 수 없습니다.
- Reconciliation Timer—삭제 보류 타이머 시간 내에 SXP 연결이 연결되면 이 연결에 대한 일괄 업데이트가 수행됩니다. 이는 가장 최근의 매핑 엔트리가 학습되어 새로운 연결 인스턴스 생성 식별자와 연결되었음을 의미합니다. 주기적인 연결별 조정 타이머가 백그라운드에서 시작됩니다. 이 조정 타이머가 만료되면 전체 SXP 매핑 데이터베이스를 검색하고 현재 연결 세션에서 학습되지 않은 모든 매핑 엔트리(연결 인스턴스 생성 식별자가 일치하지 않는 매핑 엔트리)를 식별한 후 삭제 표시를 합니다. 이 엔트리는 다음의 조정 검토에서 삭제됩니다. 기본 조정 타이머 값은 120초입니다. 사용하지 않는 엔트리가 기한 없이 남아 정책 시행에 예기치 못한 영향을 미치지 않도록 하기 위하여 ASA에서는 제로 값이 허용되지 않습니다.

- HA Reconciliation Timer—HA가 활성화된 경우 활성 및 스탠바이 유닛의 SXP 매핑 데이터베이스가 동기화된 것입니다. 새로운 활성 유닛이 모든 피어에 대한 새로운 SXP 연결 설정을 시도하고 최신 매핑 엔트리를 입수합니다. HA 조정 타이머는 이전 매핑 엔트리를 식별하고 삭제하는 수단을 제공합니다. 조정 타이머는 장애 조치가 발생한 후 시작되어 ASA가 최신 매핑 엔트리를 입수할 시간을 제공합니다. HA 조정 타이머가 만료된 후 ASA는 전체 SXP 매핑 데이터베이스를 스캔하고 현재 연결 세션에서 학습되지 않은 모든 매핑 엔트리를 식별합니다. 일치하지 않는 인스턴트 생성 식별자를 가진 매핑 엔트리에 삭제 표시가 됩니다. 이 조정 메커니즘은 조정 타이머와 동일합니다. 시간 값은 조정 타이머와 동일하며 구성이 가능합니다.

SXP 피어가 SXP 연결을 종료하고 나면 ASA가 삭제 보류 타이머를 시작합니다. 리스너로 지정된 SXP 피어만 연결을 종료할 수 있습니다. SXP 피어가 삭제 보류 타이머 실행 중에 연결되는 경우 ASA가 조정 타이머를 시작하고 ASA는 IP-SGT 매핑 데이터베이스를 업데이트하여 가장 최근의 매핑을 학습합니다.

IP-SGT Manager 데이터베이스

IP-SGT Manager 데이터베이스는 활성 유닛의 엔트리를 스탠바이 유닛으로 동기화하지 않습니다. IP-SGT Manager 데이터베이스가 IP-SGT 매핑 엔트리를 수신하는 각 소스는 활성 유닛에서 스탠바이 유닛으로 데이터베이스를 동기화한 후 최종 IP-SGT 매핑을 스탠바이 유닛의 IP-SGT Manager에 제공합니다.

버전 9.0(1)의 경우 IP-SGT Manager 데이터베이스는 SXP 소스에서만 IP-SGT 매핑 업데이트를 수신합니다.

ASA-Cisco TrustSec 통합의 기능

ASA는 ID 기반 방화벽 기능의 일부로서 Cisco TrustSec을 포함합니다. Cisco TrustSec은 다음과 같은 기능을 제공합니다.

유연성

- ASA는 SXP 스피커 또는 리스너 또는 스피커이자 리스너로 구성할 수 있습니다.
- ASA는 IPv6 및 IPv6 지원 네트워크 디바이스를 위한 SXP를 지원합니다.
- SXP는 IPv4 및 IPv6 주소를 위한 매핑 엔트리를 변경할 수 있습니다.
- SXP 엔드포인트는 IPv4 및 IPv6 주소를 지원합니다.
- ASA는 SXP 버전 2만 지원합니다.
- ASA는 서로 다른 SXP 지원 네트워크 디바이스를 사용하여 SXP 버전을 협상합니다. SXP 버전 협상을 하면 고정 버전 컨피그레이션이 필요 없게 됩니다.
- SXP 조정 타이머가 만료되면 ASA가 보안 그룹 테이블을 갱신하도록 구성하고 온디맨드로 보안 그룹 테이블을 다운로드할 수 있습니다. ASA의 보안 그룹 테이블이 ISE에서 업데이트되면 변경 사항이 적정 보안 정책에 반영됩니다.
- ASA는 소스 또는 대상 필드 또는 두 필드 모두에서 보안 그룹 이름을 기반으로 보안 정책을 지원합니다. 보안 그룹, IP 주소, Active Directory 그룹/사용자 이름 및 FQDN을 기준으로 ASA에서 보안 정책을 구성할 수 있습니다.

가용성

- Active/Active 및 Active/Standby 컨피그레이션으로 ASA에서 보안 그룹 기반 정책을 구성할 수 있습니다.
- ASA는 고가용성(HA)을 위해 구성된 ISE와 통신할 수 있습니다.

- 여러 ISE 서버를 ASA에서 구성하고 첫 번째 서버가 도달 불가능한 경우 다음 서버로 이동할 수 있습니다. 그러나 서버 목록이 Cisco TrustSec 환경 데이터의 일부로 다운로드된 경우 무시됩니다.
- ISE에서 다운로드된 PAC 파일이 ASA에서 만료되고 업데이트된 보안 그룹 테이블을 다운로드할 수 없는 경우 ASA는 ASA가 업데이트된 테이블을 다운로드할 때까지 마지막으로 다운로드된 보안 그룹 테이블을 기준으로 보안 정책을 시행합니다.

클러스터링

- 레이어 2 네트워크의 경우 모든 유닛이 동일한 IP 주소를 공유합니다. 인터페이스 주소를 변경하면 변경된 컨피그레이션이 다른 모든 유닛으로 전송됩니다. IP 주소가 특정 유닛의 인터페이스에서 업데이트되면 알림이 전송되어 이 유닛의 IP-SGT 로컬 데이터베이스를 업데이트합니다.
- 레이어 3 네트워크의 경우 마스터 유닛의 각 인터페이스에 대해 주소 풀이 구성되고 이 컨피그레이션이 슬레이브 유닛으로 동기화됩니다. 마스터 유닛에서 인터페이스에 할당된 IP 주소 알림이 전송되고 IP-SGT 로컬 데이터베이스가 업데이트됩니다. 각 슬레이브 유닛의 IP-SGT 로컬 데이터베이스는 여기에 동기화된 주소 풀 컨피그레이션을 사용하여 마스터 유닛에 대한 IP 주소로 업데이트될 수 있습니다. 여기서 각 인터페이스에 대한 풀의 첫 번째 주소는 항상 마스터 유닛에 속합니다.

  슬레이브 유닛이 부팅되면 마스터 유닛에 알립니다. 그러면 마스터 유닛이 각 인터페이스의 주소 풀을 검토하고 알림을 보낸 새로운 슬레이브 유닛에 대한 IP 주소를 계산하며 마스터 유닛에서 IP-SGT 로컬 데이터베이스를 업데이트합니다. 마스터 유닛은 또한 다른 슬레이브 유닛에 새로운 슬레이브 유닛에 대해 알려줍니다. 이 알림 처리의 일부로서 각 슬레이브 유닛은 새로운 슬레이브 유닛에 대한 IP 주소를 계산하고 이 각 슬레이브 유닛의 IP-SGT 로컬 데이터베이스에 이 엔트리를 추가합니다. 모든 슬레이브 유닛은 IP 주소 값을 결정하기 위한 주소 풀 컨피그레이션을 갖습니다. 각 인터페이스에 대해 이 값은 다음과 같이 결정됩니다.

  Master IP + (M-N):

  M—최대 유닛 수(최대 8개)

  N—알림을 보낸 슬레이브 유닛 번호

  인터페이스에서 IP 주소 풀이 변경되면 모든 슬레이브 유닛과 마스터 유닛에 대한 IP 주소가 다시 조정되고 마스터 유닛은 물론 다른 모든 슬레이브 유닛의 IP-SGT 로컬 데이터베이스에서 업데이트되어야 합니다. 이전 IP 주소를 삭제하고 새로운 IP 주소를 추가해야 합니다.

  컨피그레이션 변경 처리 과정의 일부로서 이 변경된 주소 풀 컨피그레이션이 슬레이브 유닛에 동기화되면 각 슬레이브 유닛은 IP 주소가 변경된 마스터 유닛과 다른 모든 슬레이브 유닛에 대한 IP 주소를 다시 계산하고 이전 IP 주소 엔트리를 삭제하고 새로운 IP 주소를 추가합니다.

확장성

표 32-1은 ASA가 지원하는 IP-SGT 매핑 엔트리의 수를 표시합니다.

표 32-1 IP-SGT 매핑 엔트리에 대한 용량 숫자

ASA 모델	IP-SGT 매핑 엔트리 수
5585-X(SSP-10 포함)	18,750
5585-X(SSP-20 포함)	25,000
5585-X(SSP-40 포함)	50,000
5585-X(SSP-60 포함)	100,000

표 32-2는 ASA가 지원하는 SXP 연결의 수를 표시합니다.

표 32-2 SXP 연결

ASA 모델	SXP TCP 연결 수
5585-X(SSP-10 포함)	150
5585-X(SSP-20 포함)	250
5585-X(SSP-40 포함)	500
5585-X(SSP-60 포함)	1000

Cisco TrustSec 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

Cisco TrustSec 사용 전제 조건

ASA를 Cisco TrustSec을 사용하도록 구성하기 전에 다음 작업을 수행해야 합니다.

- 32-10 페이지의 ISE에 ASA를 등록
- 32-11 페이지의 ISE에서 보안 그룹 생성
- 32-11 페이지의 PAC 파일 생성

ISE에 ASA를 등록

ASA가 SE에 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있어야 ASA가 성공적으로 PAC 파일을 가져올 수 있습니다. ISE에 ASA를 등록하려면 다음 단계를 수행하십시오.

1. ISE에 로그인합니다.
2. **Administration > Network Devices > Network Devices**를 선택합니다.
3. **Add**를 클릭합니다.
4. ASA의 IP 주소를 입력합니다.
5. 사용자 인증을 위해 ISE가 사용되는 경우 Authentication Settings 영역에 공유 암호를 입력합니다.

   ASA에서 AAA 서버를 구성할 때는 ISE에서 생성한 공유 암호를 입력하십시오. ASA의 AAA 서버는 이 공유 암호를 사용하여 ISE와 통신합니다.
6. ASA에 대한 디바이스 이름, 디바이스 ID, 비밀번호, 다운로드 간격을 지정합니다. 이 작업 수행 방법은 ISE 문서를 참조하십시오.

ISE에서 보안 그룹 생성

ISE와 통신하도록 ASA를 구성할 때는 AAA 서버를 지정합니다. ASA에서 AAA 서버를 구성할 때는 서버 그룹을 지정해야 합니다. 보안 그룹은 RADIUS 프로토콜을 사용하도록 구성되어야 합니다. ISE에서 보안 그룹을 생성하려면 다음 단계를 수행합니다.

1. ISE에 로그인합니다.
2. **Policy > Policy Elements > Results > Security Group Access > Security Group**을 선택합니다.
3. ASA에 대한 보안 그룹을 추가합니다 (보안 그룹은 글로벌이며 ASA별로 다르지 않습니다).

   ISE가 Security Groups 아래에 태그가 지정된 엔트리를 생성합니다.
4. Security Group Access 영역에서 ASA에 대한 디바이스 ID 자격 증명과 비밀번호를 구성합니다.

PAC 파일 생성

PAC 파일을 생성하기 전에 ASA를 ISE에 등록해야 합니다. PAC 파일을 생성하려면 다음 단계를 수행하십시오.

1. ISE에 로그인합니다.
2. **Administration > Network Resources > Network Devices**를 선택합니다.
3. 디바이스 목록에서 ASA를 선택합니다.
4. SGA(Security Group Access)에서 **Generate PAC**를 클릭합니다.
5. PAC 파일을 암호화하려면 비밀번호를 입력합니다.

   PAC 파일 암호화를 위해 입력하는 비밀번호(또는 암호화 키)는 ISE에서 디바이스 자격 증명의 일부로서 구성된 비밀번호와 별개입니다.

ISE가 PAC 파일을 생성합니다. ASA는 플래시 메모리 또는 TFTP, FTP, HTTP, HTTPS, SMB를 통한 원격 서버로부터 PAC 파일을 가져올 수 있습니다. PAC 파일은 파일을 가져오기 전에 ASA 플래시에 상주하지 않아도 됩니다.

PAC 파일에 대한 정보는 32-15 페이지의 PAC 파일 가져오기를 참조하십시오.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

SXP 엔드포인트를 위한 IPv6를 지원합니다.

클러스터링 지침

클러스터링 환경의 마스터 유닛 및 슬레이브 유닛에서 지원됩니다.

장애 조치 지침

컨피그레이션을 통한 서버 목록을 지원합니다. 첫 번째 서버에 도달할 수 없는 경우 ASA가 목록의 다음 서버에 도달을 시도합니다. 그러나 Cisco TrustSec 환경 데이터의 일부로 다운로드된 서버 목록은 무시됩니다.

Active/Standby 및 Active/Active 시나리오를 모두 지원합니다. 모든 SXP 데이터가 활성 유닛에서 스탠바이 유닛으로 복제됩니다.

추가 지침

Cisco TrustSec은 단일 컨텍스트 모드 및 다중 컨텍스트 모드에서 Smart Call Home 기능을 지원하지만 시스템 컨텍스트에서는 지원하지 않습니다.

제한 사항

- ASA는 단일 Cisco TrustSec 도메인에서만 상호 운용되도록 구성할 수 있습니다.
- ASA는 디바이스에서 SGT-이름 매핑의 고정 컨피그레이션을 지원하지 않습니다.
- NAT는 SXP 메시지에서 지원되지 않습니다.
- SXP는 네트워크의 시행 포인트로 IP-SGT 매핑을 전달합니다. 액세스 레이어 스위치가 시행 포인트와 다른 NAT 도메인에 속하는 경우 그것이 업로드하는 IP-SGT 맵은 유효하지 않고 시행 디바이스의 IP-SGT 매핑 데이터베이스 조회에서 유효한 결과가 반환되지 않습니다. 따라서 ASA가 시행 디바이스에서 보안 그룹-인식 보안 정책을 적용할 수 없습니다.
- ASA에 대해 SXP 연결에 사용할 기본 비밀번호를 구성하거나 비밀번호를 사용하지 않기로 선택할 수도 있지만 연결별 비밀번호는 SXP 피어에 대해 지원되지 않습니다. 구성된 기본 SXP 비밀번호는 배포 네트워크 전체에서 일관되어야 합니다. 연결별로 비밀번호를 구성하면 연결이 실패하고 경고 메시지가 나타납니다. 기본 비밀번호로 연결을 구성하면 비밀번호 없이 연결을 구성한 것과 마찬가지 결과가 나타납니다.
- 디바이스가 피어로 양방향 연결되었을 때 또는 양방향으로 연결된 디바이스 체인의 일부일 때 SXP 연결 루프가 발생합니다. (ASA가 데이터 센터의 액세스 레이어로부터 리소스에 대한 IP-SGT 매핑을 학습할 수 있습니다. ASA이(가) 이러한 태그를 다운스트림 디바이스로 전파해야 할 수 있습니다.) SXP 연결 루프는 SXP 메시지 전송에서 예기치 않은 동작을 야기할 수 있습니다. ASA가 스피커와 리스너로 구성된 경우 SXP 연결 루프가 발생하여 SXP 데이터를 전송한 피어가 이 데이터를 다시 받게 될 수 있습니다.
- ASA 로컬 IP 주소를 변경할 ?는 모든 SXP 피어가 피어 목록을 업데이트했는지 확인해야 합니다. 또한 SXP 피어가 IP 주소를 변경할 경우 이러한 변경 사항이 ASA에 반영되는지 확인해야 합니다.
- 자동 PAC 파일 프로비저닝은 지원되지 않습니다. ASA 관리자는 ISE 관리 인터페이스에서 PAC 파일을 요청하고 ASA로 가져와야 합니다. PAC 파일에 대한 정보는 32-11 페이지의 PAC 파일 생성 및 32-15 페이지의 PAC 파일 가져오기를 참조하십시오.
- PAC 파일에는 기한이 있습니다. 현재 PAC 파일이 만료되기 전에 업데이트된 PAC 파일을 가져와야 합니다. 그러지 않으면 ASA가 환경 데이터 업데이트를 가져올 수 없습니다.
- ISE에서 보안 그룹이 변경되는 경우(이름이 변경되거나 삭제되는 경우) ASA이(가) 변경된 보안 그룹과 연결된 SGT 또는 보안 그룹 이름을 포함하는 ASA 보안 정책의 상태를 변경하지 않습니다. 하지만 ASA는 syslog 메시지를 생성하여 해당 보안 정책이 변경되었음을 나타냅니다.

  32-21 페이지의 환경 데이터 갱신에서 ISE의 변경 사항을 포함하기 위한 보안 그룹 테이블 수동 업데이트에 관한 정보는 ASA를 참조하십시오.
- 멀티캐스트 유형은 ISE 1.0에서 지원되지 않습니다.
- SXP 연결은 다음 예에서와같이 ASA에 의해 서로 연결된 두 SXP 피어 사이에서 초기화 상태에 머뭅니다.

(SXP 피어 A) - - - - (ASA) - - - (SXP 피어 B)

따라서 Cisco TrustSec과의 통합을 위해 ASA을(를) 구성할 때는 ASA에서 no-NAT, no-SEQ-RAND 및 MD5-AUTHENTICATION TCP 옵션을 활성화하여 SXP 연결을 구성해야 합니다. SXP 피어 사이에서 SXP 포트 TCP 64999로 향하는 트래픽에 대해 TCP 상태 바이패스 정책을 생성합니다. 그런 다음 적절한 인터페이스에 정책을 적용하십시오.

예를 들어, 다음 명령 집합은 TCP 상태 바이패스 정책에 대해 ASA를 구성하는 방법을 보여줍니다.

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

- ASA 5585-X의 하드웨어 아키텍처는 일반 패킷의 로드 밸런싱을 최적화하도록 설계되었으나 Layer 2 Security Group Tagging Imposition을 포함한 인라인 태그 패킷의 경우는 다릅니다. 수신 인라인 태그 패킷을 처리할 때는 ASA 5585-X에 상단한 성능 저하가 발생할 수 있습니다. 이 문제는 다른 ASA 플랫폼의 인라인 태그 패킷과 ASA 5585-X의 태그가 지정되지 않은 패킷에서는 발생하지 않습니다. 한 가지 해결 방법은 액세스 정책을 오프로드하여 ASA 5585-X로 전달되는 인라인 태그 패킷을 최소화함으로써 스위치가 태그 정책 시행을 처리할 수 있도록 하는 것입니다. 다른 해결 방법은 ASA 5585-X가 태그 패킷을 수신할 필요 없이 IP 주소를 보안 태그에 매핑할 수 있도록 SXP를 사용하는 것입니다.
- ASASM은 Layer 2 Security Group Tagging Imposition을 지원하지 않습니다.

Cisco TrustSec 통합을 위한 ASA 구성

Cisco TrustSec 통합을 위한 AAA 서버 구성

Cisco TrustSec과의 통합을 위한 ASA 구성의 일부로써 ASA가 ISE와 통신할 수 있도록 구성해야 합니다.

전제 조건

- 참조 서버 그룹은 RADIUS 프로토콜을 사용하도록 구성되어야 합니다. 비 RADIUS 서버 그룹을 ASA에 추가하면 컨피그레이션이 실패합니다.
- ISE가 사용자 인증에도 사용되는 경우 ISE에 ASA를 등록할 때 ISE에 입력한 공유 암호를 얻으십시오. ISE 관리자에게 문의하여 이 정보를 확보하십시오.

ASA에서 ISE에 대한 AAA 서버 그룹을 구성하려면 다음 단계를 수행하십시오.

	명령	목적
1단계	`ciscoasa(config)# aaa-server server-tag protocol radius` **예:** `ciscoasa(config)# aaa-server ISEserver protocol radius`	AAA 서버 그룹을 만들고 ISE 서버와 통신할 수 있도록 ASA에 대한 AAA 서버 매개변수를 구성합니다. *server-tag*는 서버 그룹 이름을 지정합니다. 자세한 내용은 32-11 페이지의 ISE에서 보안 그룹 생성을 참조하십시오.
2단계	`ciscoasa(config-aaa-server-group)# exit`	aaa 서버 그룹 컨피그레이션 모드에서 나갑니다.
3단계	`ciscoasa(config)# aaa-server server-tag (interface-name) host server-ip` **예:** `ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1`	AAA 서버 그룹의 일부로서 AAA 서버를 구성하고 호스트별 연결 데이터를 설정합니다. *interface-name*은 ISE 서버가 상주하는 네트워크 인터페이스를 지정합니다. 이 매개변수에서는 괄호가 필요합니다. *server-tag*는 AAA 서버 그룹의 이름입니다. *server-ip*는 ISE 서버의 IP 주소를 지정합니다.
4단계	`ciscoasa(config-aaa-server-host)# key key` **예:** `ciscoasa(config-aaa-server-host)# key myexclusivemumblekey`	ISE 서버에서 ASA 인증에 사용되는 서버 비밀 값을 지정합니다. *key*는 최대 127자 길이의 영숫자 키워드입니다. ISE가 사용자 인증에도 사용되는 경우 ISE에 ASA을(를) 등록할 때 ISE에 입력한 공유 암호를 입력하십시오. 자세한 내용은 32-10 페이지의 ISE에 ASA를 등록을 참조하십시오.
5단계	`ciscoasa(config-aaa-server-host)# exit`	aaa 서버 호스트 컨피그레이션 모드에서 나갑니다.
6단계	`ciscoasa(config)# cts server-group AAA-server-group-name` **예:** `ciscoasa(config)# cts server-group ISEserver`	Cisco TrustSec에서 환경 데이터 검색을 위해 사용되는 AAA 서버 그룹을 식별합니다. *AAA-server-group-name*은 *server-tag* 인수의 1단계에서 지정한 AAA 서버 그룹의 이름입니다. Cisco TrustSec에 대해 서버 그룹의 인스턴스 1개만 ASA에서 구성할 수 있습니다.

예

다음 예는 Cisco TrustSec 통합을 위해 ASA를 ISE 서버와 통신하도록 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

PAC 파일 가져오기

PAC(protected access credential) 파일을 ASA로 가져오면 ISE와의 연결이 설정됩니다. 채널을 설정하고 나면 ASA가 ISE와 보안 RADIUS 트랜잭션을 시작하고 Cisco TrustSec 환경 데이터(보안 그룹 테이블)를 다운로드합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다.

보다 구체적으로는 RADIUS 트랜잭션 전에는 아무 채널도 설정되지 않습니다. ASA는 인증을 위한 PAC 파일을 사용하여 ISE와의 RADIUS 트랜잭션을 개시합니다.

팁 PAC 파일은 ASA 및 ISE가 둘 사이의 RADIUS 트랜잭션을 보안할 수 있는 공유 키를 포함합니다. 이 키는 매우 중요하므로 ASA에 안전하게 저장되어야 합니다.

파일을 성공적으로 가져온 후에는 ASA가 ISE에 구성된 디바이스 비밀번호 없이 ISE에서 Cisco TrustSec 환경 데이터를 다운로드합니다.

전제 조건

- ASA가 SE에 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있어야 ASA가 PAC 파일을 생성할 수 있습니다. ASA는 어떤 PAC 파일이든 가져올 수 있지만 바르게 구성된 ISE에 의해 파일이 생성되었을 때 ASA에서만 동작합니다. 자세한 내용은 32-10 페이지의 ISE에 ASA를 등록을 참조하십시오.
- ISE에서 생성할 때 PAC 파일 암호화에 사용되는 비밀번호를 확보합니다.

  ASA는 PAC 파일 가져오기 및 암호 해독에 이 비밀번호를 필요로 합니다.
- ISE가 PAC 파일에 대한 액세스를 생성합니다. ASA는 플래시 메모리 또는 TFTP, FTP, HTTP, HTTPS, SMB를 통한 원격 서버로부터 PAC 파일을 가져올 수 있습니다. PAC 파일은 파일을 가져오기 전에 ASA 플래시에 상주하지 않아도 됩니다.
- 서버 그룹이 ASA에 대해 구성되었습니다.

제한 사항

- ASA가 장애 조치 컨피그레이션의 일부인 경우 PAC 파일을 기본 ASA 디바이스로 가져와야 합니다.
- ASA가 클러스터링 컨피그레이션의 일부인 경우 PAC 파일을 마스터 디바이스로 가져와야 합니다.

PAC 파일을 가져오려면 다음 명령을 입력합니다.

명령	목적
ciscoasaciscoasa(config)# **cts import-pac** *filepath* **password** *value* **예:** ciscoasaciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99	Cisco TrustSec PAC 파일을 가져옵니다. *filepath*는 다음 실행 모드 명령 및 옵션 중 하나로 입력됩니다. **단일 모드** • **disk0**: disk0의 경로 및 파일 이름 • **disk1**: disk1의 경로 및 파일 이름 • **flash**: 플래시의 경로 및 파일 이름 • **ftp**: FTP의 경로 및 파일 이름 • **http**: HTTP의 경로 및 파일 이름 • **https**: HTTPS의 경로 및 파일 이름 • **smb**: SMB의 경로 및 파일 이름 • **tftp**: TFTP의 경로 및 파일 이름 **다중 모드** • **http**: HTTP의 경로 및 파일 이름 • **https**: HTTPS의 경로 및 파일 이름 • **smb**: SMB의 경로 및 파일 이름 • **tftp**: TFTP의 경로 및 파일 이름 *value*는 PAC 파일 암호화에 사용되는 비밀번호를 지정합니다. 비밀번호는 디바이스 자격 증명의 일부로서 ISE에 구성된 비밀번호와는 별개입니다.

예

다음 예는 ASA로 PAC 파일을 가져오는 방법을 보여줍니다.

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

다음 예는 PAC 파일을 ASA로 가져오기 위한 터미널 사용 방법을 보여줍니다.

```
ciscoasa(config)# cts import-pac terminal password A9875Za551
Enter the PAC file data in ASCII hex format
End with the word "quit" on a line by itself.
ciscoasa(exec_pac_hex)# 0100290405000001000000000000000000
ciscoasa(exec_pac_hex)# 00000000000000001111111111111111
ciscoasa(exec_pac_hex)# 11111111111111112222222222222222
ciscoasa(exec_pac_hex)# 222222222222222276d7d64b6be4804b
ciscoasa(exec_pac_hex)# 0b4fdca3aeee11950ecd0e47c34157e5
ciscoasa(exec_pac_hex)# 25f4964ed75835cde0adb7e198e0bcdb
ciscoasa(exec_pac_hex)# 6aa8e363b0e4f9b4ac241be9ab576d0b
ciscoasa(exec_pac_hex)# a1fcd34e5dd05dbe1312cbfea072fdb9
ciscoasa(exec_pac_hex)# ee356fb61fe987d2d8f0ac3ef0467627
ciscoasa(exec_pac_hex)# 7f8b137da2b840e16da520468b039bae
ciscoasa(exec_pac_hex)# 36a4d844acc85cdefd7cb2cc58787590
ciscoasa(exec_pac_hex)# ef123882a69b6c37bdbc9320e403024f
ciscoasa(exec_pac_hex)# 354d42f404ec2d67ef3606575014584b
ciscoasa(exec_pac_hex)# 2796e65ccd6e6c8d14d92448a8b24f6e
```

```
ciscoasa(exec_pac_hex)# 47015a21f4f66cf6129d352bdfd4520f
ciscoasa(exec_pac_hex)# 3f0c6f340a80715df4498956efe15dec
ciscoasa(exec_pac_hex)# c08bb9a58cb6cb83ac91a3c40ce61de0
ciscoasa(exec_pac_hex)# 284b743e52fd68e848685e2d78c33633
ciscoasa(exec_pac_hex)# f2b4c5824138fc7bac9d9b83ac58ff9f
ciscoasa(exec_pac_hex)# 1dbc84c416322f1f3c5951cf2132994a
ciscoasa(exec_pac_hex)# a7cf20409df1d0d6621eba2b3af83252
ciscoasa(exec_pac_hex)# 70d0130650122bdb13a83b2dae55533a
ciscoasa(exec_pac_hex)# 4a394f21b441e164
ciscoasa(exec_pac_hex)# quit
PAC Imported Successfully
ciscoasa(config)#
```

Security Exchange Protocol 구성

SXP(Security Exchange Protocol)를 구성하려면 ASA에서 프로토콜을 활성화하고 SXP에 대한 다음 기본값을 설정해야 합니다.

- SXP 연결의 소스 IP 주소
- SXP 피어 간의 인증 비밀번호
- SXP 연결을 위한 재시도 간격
- Cisco TrustSec SXP 조정 기간

참고 SXP가 ASA에서 작동하려면 최소 하나의 인터페이스가 UP/UP 상태여야 합니다.

현재 모든 인터페이스가 다운된 상태로 SXP가 활성화된 경우 ASA는 SXP가 작동하지 않거나 활성화할 수 없음을 나타내는 메시지를 표시하지 않습니다. **show running-config** 명령을 입력하여 컨피그레이션을 확인하면 명령 출력이 다음 메시지를 표시합니다.

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

이 메시지는 일반적인 메시지로 SXP가 작동하지 않는 이유를 명시하지는 않습니다.

SXP를 구성하려면 다음 단계를 수행하십시오.

	명령	목적
1단계	`ciscoasa(config)# cts sxp enable`	필요한 경우 ASA에서 SXP를 활성화합니다. 기본적으로 SXP는 비활성화되어 있습니다. 다중 컨텍스트 모드에서는 사용자 컨텍스트에서 SXP를 활성화합니다.
2단계	`ciscoasa(config)# cts sxp default source-ip ipaddress` 예: `ciscoasa(config)# cts sxp default source-ip 192.168.1.100`	SXP 연결을 위한 기본 소스 IP 주소를 구성합니다. *ipaddress*는 IPv4 또는 IPv6 주소입니다. SXP 연결을 위한 기본 소스 IP 주소를 구성하는 경우 ASA 아웃바운드 인터페이스와 동일한 주소를 지정해야 합니다. 소스 IP 주소가 아웃바운드 인터페이스의 주소와 일치하지 않으면 SXP 연결이 실패합니다. SXP 연결에 대한 소스 IP 주소가 구성되지 않은 경우 ASA는 경로/ARP 조회를 실시하여 SXP 연결에 대한 아웃바운드 인터페이스를 결정합니다. 자세한 내용은 32-20 페이지의 SXP 연결 피어 추가를 참조하십시오.
3단계	`ciscoasa(config)# cts sxp default password [0 | 8] password` 예: `ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99`	SXP 피어를 통한 TCP MD5 인증을 위한 기본 비밀번호를 구성합니다. 기본적으로 SXP 연결에는 설정된 비밀번호가 없습니다. 비밀번호에 대한 암호화 수준 구성은 선택 사항입니다. 암호화 수준을 구성할 경우 하나의 수준만 설정할 수 있습니다. • 수준 0—암호화되지 않은 일반 텍스트 • 수준 8—암호화된 텍스트 *password*는 최대 162 자의 암호화된 문자열 또는 최대 80자의 ASCII 키 문자열을 지정합니다.

	명령	목적
4단계	ciscoasa(config)# **cts sxp retry period** *timervalue* 예: ciscoasa(config)# cts sxp retry period 60	SXP 피어 간 새로운 SXP 연결 시도 ASA 사이의 기본 시간 간격을 지정합니다. ASA는 성공할 때까지 연결을 시도합니다. ASA에서 연결되지 않은 SXP 연결이 하나 있는 한 재시도 타이머가 트리거됩니다. *timervalue*는 0~64000초 범위에 있습니다. 기본적으로 *timervalue*? 120초입니다. 0초로 지정하면 타이머가 만료되지 않고 ASA가 SXP 피어 연결을 시도하지 않습니다. 재시도 타이머가 만료되면 ASA가 연결 데이터베이스를 검토하고 데이터베이스에 꺼져 있거나 "보류" 상태인 연결이 있는 경우 ASA가 재시도 타이머를 다시 시작합니다. 재시도 타이머를 SXP 피어 디바이스와 다른 값으로 구성하는 것이 좋습니다.
5단계	ciscoasa(config)# **cts sxp reconciliation period** *timervalue* 예: ciscoasa(config)# cts sxp reconciliation period 60	기본 조정 타이머의 값을 지정합니다. SXP 피어가 SXP 연결을 종료하고 나면 ASA가 보류 타이머를 시작합니다. SXP 피어가 보류 타이머 실행 중에 연결되는 경우 ASA가 조정 타이머를 시작하고 ASA는 SXP 매핑 데이터베이스를 업데이트하여 가장 최근의 매핑을 학습합니다. 조정 타이머가 만료되면 ASA가 SXP 매핑 데이터베이스를 스캔하여 오래된 매핑 엔트리(이전 연결 세션에서 학습한 엔트리)를 식별합니다. ASA가 이러한 연결을 오래된 연결로 표시합니다. 조정 타이머가 만료되면 ASA가 오래된 엔트리를 SXP 매핑 데이터베이스에서 삭제합니다. *timervalue*는 1~64000초 범위에 있습니다. 기본적으로 *timervalue*? 120초입니다. 타이머를 0초로 지정하면 조정 타이머가 시작되지 않기 때문에 안 됩니다. 조정 타이머 실행을 허용하지 않으면 오래된 엔트리가 무기한 남아서 정책 시행에서 예기치 못한 결과를 초래할 수 있습니다.

예

다음 예는 SXP에 대한 기본값을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

SXP 연결 피어 추가

피어 간 SXP 연결은 point-to-point 연결이며 TCP를 기본 전송 프로토콜로 사용합니다.

SXP 연결 피어를 추가하려면 다음 단계를 수행하십시오.

	명령	목적
1단계	`ciscoasa(config)# cts sxp enable`	필요한 경우 ASA에서 SXP를 활성화합니다. 기본적으로 SXP는 비활성화되어 있습니다.
2단계	`ciscoasa(config)# cts sxp connection peer peer_ip_address [source source_ip_address] password {default | none} [mode {local | peer}] {speaker | listener}` 예: `ciscoasaciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker`	SXP 피어에 대한 SXP 연결을 설정합니다. SXP 연결은 IP 주소별로 설정됩니다. 단일 디바이스 쌍이 여러 SXP 연결을 담당할 수 있습니다. *peer_ip_address*는 SXP 피어의 IPv4 또는 IPv6 주소입니다. 피어 IP 주소는 ASA 발신 인터페이스에서 도달 가능해야 합니다. *source_ip_address*는 SXP 연결의 로컬 IPv4 또는 IPv6 주소입니다. 소스 IP 주소는 ASA 아웃바운드 인터페이스 또는 연결 실패와 동일해야 합니다. SXP 연결에 대해 소스 IP 주소를 구성하지 않고 ASA가 경로/ARP 조회를 통해 SXP 연결에 대한 소스 IP 주소를 확인할 수 있도록 하는 것이 좋습니다. SXP 연결을 위한 인증 키 사용 여부를 지정합니다. • **default**—SXP 연결을 위해 구성된 기본 비밀번호를 사용합니다. 32-17 페이지의 Security Exchange Protocol 구성을 참조하십시오. • **none**—SXP 연결을 위해 비밀번호를 사용하지 않습니다. SXP 연결 모드를 지정: • **local**—로컬 SXP 디바이스를 사용합니다. • **peer**—피어 SXP 디바이스를 사용합니다. ASAASA가 SXP 연결에 대한 스피커 또는 리스너 중 어떤 역할을 할지 지정합니다. 32-6 페이지의 ASA에서 스피커 및 리스너 역할에 관해를 참조하십시오. • **speaker**— ASAASA가 IP-SGT 매핑을 업스트림 디바이스로 전달할 수 있습니다. • **listener**—ASAASA가 IP-SGT 매핑을 다운스트림 디바이스에서 수신할 수 있습니다.

예

다음 예는 ASA에서 SXP 피어를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default mode peer
ciscoasa(config)# no cts sxp connection peer 192.168.1.100
ciscoasa(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
ciscoasa(config)# no cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer
speaker
```

환경 데이터 갱신

ASA은(는) ISE에서 환경 데이터를 다운로드하며 여기에는 SGT(Security Group Tag) 이름 테이블이 포함됩니다. ASA에서 다음 작업을 완료하면 ASA은(는) ISE에서 수집한 환경 데이터를 자동으로 업데이트합니다.

- ISE와 통신할 AAA 서버를 구성합니다.
- ISE에서 PAC 파일을 가져옵니다.
- ASA이(가) Cisco TrustSec 환경 데이터의 검색에 사용할 AAA 서버 그룹을 식별합니다.

보통은 ISE의 환경 데이터를 수동으로 갱신할 필요가 없지만 ISE에서 보안 그룹이 달라질 수 있습니다. 이러한 변경 사항은 ASA 보안 그룹 테이블에서 데이터를 갱신하기 전에는 ASA에 반영되지 않으므로 ASA에서 데이터를 갱신하여 ISE의 보안 그룹 변경 사항이 ASA에 반영되도록 하십시오.

팁 ISE의 정책 컨피그레이션 변경과 ASA의 수동 데이터 갱신을 유지 관리 기간 중에 예약하는 것이 좋습니다. 이 방법으로 정책 컨피그레이션 변경 사항을 처리하면 ASA에서 보안 그룹 이름이 확인되고 보안 정책이 즉시 활성화될 가능성이 극대화됩니다.

전제 조건

ASA이(가) ISE에서 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있고 ASA이(가) PAC 파일 가져오기에 성공해야만 Cisco TrustSec에 대한 변경 사항이 ASA에 적용됩니다.

제한 사항

- ASA이(가) HA 컨피그레이션의 일부인 경우 기본 ASA 디바이스에서 환경 데이터를 갱신해야 합니다.
- ASA이(가) 클러스터링 컨피그레이션의 일부인 경우 마스터 디바이스에서 환경 데이터를 갱신해야 합니다.

환경 데이터를 갱신하려면 다음 명령을 입력합니다..

명령	목적
cts refresh environment-data 예: `ciscoasaciscoasa(config)# cts refresh environment-data`	ISE에서 환경 데이터를 갱신하고 조정 타이머를 설정된 기본값으로 재설정합니다.

보안 정책 구성

Cisco TrustSec 정책을 여러 ASA 기능에서 통합할 수 있습니다. 확장 ACL을 사용하는 모든 기능(이 장에서 미지원으로 명시된 경우 제외)은 Cisco TrustSec을 이용할 수 있습니다. 이제 보안 그룹 인수는 물론 기존의 네트워크 기반 매개변수를 확장 ACL에 추가할 수 있습니다.

- 확장 ACL을 구성하려면 방화벽 컨피그레이션 가이드을(를) 참조하십시오.
- ACL에서 사용할 수 있는 보안 그룹 객체 그룹을 구성하려면 16-8 페이지의 보안 그룹 객체 그룹 구성을 참조하십시오.

예를 들어 액세스 규칙은 네트워크 정보를 사용하여 인터페이스의 트래픽을 허용하거나 거부합니다. Cisco TrustSec을 통해 보안 그룹을 기반으로 액세스를 제어할 수 있습니다. 예를 들어 sample_securitygroup1 10.0.0.0 255.0.0.0을 위한 액세스 규칙을 만들 수 있으므로 보안 그룹은 서브넷 10.0.0.0/8의 어떤 IP 주소라도 가질 수 있습니다.

보안 그룹 이름의 조합(서버, 사용자, 비관리 디바이스 등), 사용자 기반 속성, 기존 IP 주소 기반 객체(IP 주소, Active Directory 객체 및 FQDN)를 기반으로 보안 정책을 구성할 수 있습니다. 보안 그룹 멤버십은 역할을 넘어 확장되어 디바이스 및 위치 속성을 포함할 수 있으며 사용자 그룹 멤버십과는 별개입니다.

예

다음 예는 로컬로 정의된 보안 객체 그룹을 사용하는 ACL을 생성하는 방법을 보여줍니다.

```
object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
   security-group name hr-admin-sg-name  // single sg_name
   group-object it-admin     // locally defined object-group as nested object
object-group security objgrp-hr-servers
    security-group name hr-servers-sg-name
object-group security objgrp-hr-network
    security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

이전 예제에서 구성된 ACL은 액세스 그룹 또는 Modular Policy Framework를 구성함으로써 활성화할 수 있습니다.

추가 예제

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
    access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53
!match src hr-admin-sg-name from host 10.1.1.1 to dst any
    access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any
!match src tag 22 from any network to dst hr-servers-sg-name any network
    access-list idfw-acl permit ip security-group tag 22 any security-group name hr-servers-sg-name any
!match src user mary from any host to dst hr-servers-sg-name any network
    access-list idfw-acl permit ip user CSCO\mary any security-group name hr-servers-sg-name any
!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
    access-list idfw-acl permit ip object-group-security objgrp-hr-admin any object-group-security
    objgrp-hr-servers any
!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24 to dst objgrp-hr-servers any network
    access-list idfw-acl permit ip user CSCO\Jack object-group-security objgrp-hr-network 10.1.1.0
    255.255.255.0 object-group-security objgrp-hr-servers any
!match src user Tom from security-group mktg any google.com
object network net-google
    fqdn google.com
    access-list sgacl permit ip sec name mktg any object net-google
! If user Tom or object_group security objgrp-hr-admin needs to be matched, multiple ACEs can be defined as
follows:
    access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0 object-group-security
    objgrp-hr-servers any
    access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
```

레이어 2 Security Group Tagging Imposition 구성

Cisco TrustSec은 각 네트워크 사용자와 리소스를 식별 및 인증하고 SGT(Security Group Tag)라는 16비트 숫자를 할당합니다. 그러면 이 식별자가 네트워크 홉 사이에 전파되어 ASA, 스위치 및 라우터와 같은 중개 디바이스가 이 ID 태그를 기반으로 정책을 시행할 수 있습니다.

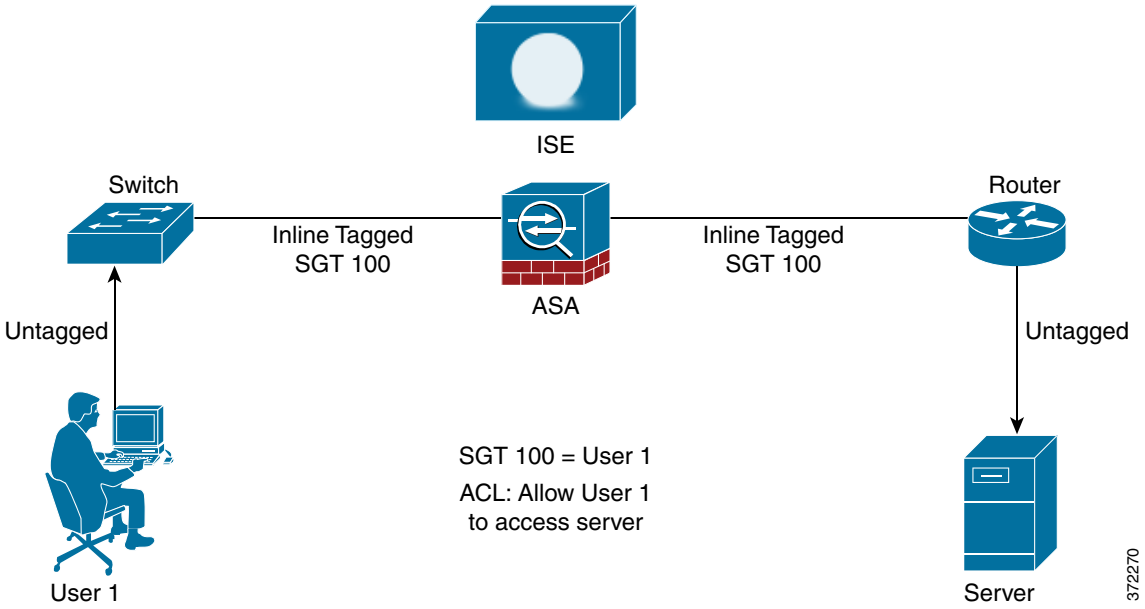
레이어 2 SGT Imposition이라고도 하는 SGT plus Ethernet Tagging은 ASA이(가) Cisco 고유의 이더넷 프레이밍(EtherType 0x8909)을 사용하여 이더넷 인터페이스에서 보안 그룹 태그를 보내고 받도록 하여 소스 보안 그룹 태그를 일반 텍스트 이더넷 프레임으로 삽입할 수 있게 됩니다. ASA은(는) 발신 패킷에 보안 그룹 태그를 삽입하고 수동 인터페이스별 컨피그레이션에 따라 수신 패킷에서 보안 그룹 태그를 처리합니다. 이 기능을 통해 네트워크 디바이스에 걸쳐 엔드포인트 ID를 인라인 hop-by-hop으로 전파할 수 있고 각 홉 사이에서 원활한 레이어 2 SGT Imposition이 가능합니다.

제한 사항

- 물리적 인터페이스, VLAN 인터페이스, 포트 채널 인터페이스 및 중복 인터페이스에서만 지원됩니다.
- BVI와 같은 논리적 인터페이스나 가상 인터페이스에서는 지원되지 않습니다.
- SAP 협상 및 MACsec을 이용한 링크 암호화를 지원하지 않습니다.
- 장애 조치 링크에서는 지원되지 않습니다.
- 클러스터 제어 링크에서는 지원되지 않습니다.
- ASA은(는) SGT가 변경된 경우 기존 흐름을 다시 분류하지 않습니다. 이전 SGT를 기반으로 만들어진 정책 결정은 흐름의 수명 동안 효력을 유지합니다. 그러나 ASA은(는) 이전 SGT를 기반으로 분류된 흐름에 속한 패킷이라도 SGT 변경 사항을 이그레스 패킷에 즉시 반영할 수 있습니다.

그림 32-3은 레이어 2 SGT Imposition의 일반적인 예입니다.

그림 32-3 레이어 2 SGT Imposition



활용 시나리오

표 32-3은 이 기능을 구성할 때 인그레스 트래픽의 예상 동작을 설명합니다.

표 32-3 인그레스 트래픽

인터페이스 컨피그레이션	수신된 태그 패킷	수신된 태그가 없는 패킷
명령이 발행되지 않습니다.	패킷이 버려집니다.	SGT 값은 IP-SGT Manager에서 가져옵니다.
cts manual 명령이 발행됩니다.	SGT 값은 IP-SGT Manager에서 가져옵니다.	SGT 값은 IP-SGT Manager에서 가져옵니다.
cts manual 명령과 **policy static sgt** *sgt_number* 명령이 모두 발행됩니다.	SGT 값은 **policy static sgt** *sgt_number* 명령에서 가져옵니다.	SGT 값은 **policy static sgt** *sgt_number* 명령에서 가져옵니다.
cts manual 명령과 **policy static sgt** *sgt_number* **trusted** 명령이 모두 발행됩니다.	SGT 값은 패킷의 인라인 SGT에서 가져옵니다.	SGT 값은 **policy static sgt** *sgt_number* 명령에서 가져옵니다.

참고 If IP-SGT Manager에서 일치하는 IP-SGT 매핑이 없는 경우 "Unknown"에 대해 예약된 SGT 값인 "0x0"이 사용됩니다.

표 32-4는 이 기능을 구성할 때 이그레스 트래픽의 예상 동작을 설명합니다.

표 32-4 이그레스 트래픽

인터페이스 컨피그레이션	전송된 태그 또는 태그가 없는 패킷
명령이 발행되지 않습니다.	태그 없음
cts manual 명령이 발행됩니다.	태그 있음
cts manual 명령과 **propagate sgt** 명령이 모두 발행됩니다.	태그 있음
cts manual 명령과 **no propagate sgt** 명령이 모두 발행됩니다.	태그 없음

표 32-5는 이 기능을 구성할 때 to-the-box 및 from-the-box 트래픽의 예상 동작을 설명합니다.

표 32-5 To-the-box 및 From-the-box 트래픽

인터페이스 컨피그레이션	수신된 태그 또는 태그가 없는 패킷
to-the-box 트래픽에 대한 인그레스 인터페이스에서 명령이 발행되지 않습니다.	패킷이 버려집니다.
to-the-box traffic에 대한 인그레스 트래픽에서 **cts manual** 명령이 발행됩니다.	패킷이 승인되지만 정책 시행 또는 SGT 전파가 없습니다.
cts manual 명령이 발행되지 않거나 from-the-box 트래픽에 대한 이그레스 인터페이스에서 **cts manual** 명령 및 **no propagate sgt** 명령이 모두 발행됩니다.	태그 없는 패킷이 전송되지만 정책 시행이 없습니다. SGT 번호는 IP-SGT Manager에서 가져옵니다.
cts manual 명령이 발행되거나 from-the-box 트래픽에 대한 이그레스 인터페이스에서 **cts manual** 명령 및 **propagate sgt** 명령이 모두 발행됩니다.	태그가 있는 패킷이 전송됩니다. SGT 번호는 IP-SGT Manager에서 가져옵니다.

참고 If IP-SGT Manager에서 일치하는 IP-SGT 매핑이 없는 경우 "Unknown"에 대해 예약된 SGT 값인 "0x0"이 사용됩니다.

SGT plus Ethernet Tagging 활성화

SGT plus Ethernet Tagging을 활성화하려면 다음 명령을 입력합니다..

명령	목적
`ciscoasa(config-if)# cts manual` **예:** `ciscoasaciscoasa(config-if)# cts manual` `ciscoasa(config-if-cts-manual)#`	레이어 2 SGT Imposition을 활성화하고 CTS 수동 인터페이스 컨피그레이션 모드로 진입합니다. 레이어 2 SGT Imposition을 비활성화하고 **no cts manual** 명령에 진입합니다.

인터페이스의 보안 그룹 태그 전파

인터페이스에서 보안 태그의 전파를 활성화 또는 비활성화하려면 다음 단계를 수행합니다.

	명령	목적
1단계	`ciscoasa(config-if)# cts manual` **예:** `ciscoasa(config-if)# cts manual` `ciscoasa(config-if-cts-manual)#`	레이어 2 SGT Imposition을 활성화하고 CTS 수동 인터페이스 컨피그레이션 모드로 진입합니다.
2단계	`ciscoasa(config-if-cts-manual)# propagate sgt` **예:** `ciscoasa(config-if-cts-manual)# propagate sgt`	인터페이스에서 보안 그룹 태그(**sgt**라고 함) 전파를 활성화합니다. 전파는 기본적으로 활성화되어 있습니다. 인터페이스에서 보안 그룹 태그(**sgt**라고 함) 전파를 비활성화하려면 **no propagate sgt** 명령을 사용합니다.

수동으로 구성된 Cisco TrustSec 링크에 정책 적용

수동 구성 CTS 링크에 정책을 적용하려면 다음 단계를 수행하십시오.

	명령	목적
1단계	`ciscoasa(config-if)# cts manual` 예: `ciscoasa(config-if)# cts manual` `ciscoasa(config-if-cts-manual)#`	레이어 2 SGT Imposition을 활성화하고 CTS 수동 인터페이스 컨피그레이션 모드로 진입합니다.
2단계	`ciscoasa(config-if-cts-manual)# policy static sgt` *sgt_number* [**trusted**] 예: `ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted`	수동으로 구성된 CTS 링크에 정책을 적용합니다. **static**은 링크의 수신 트래픽에 SGT 정책을 적용합니다. **sgt** *sgt_number*는 피어로부터의 수신 트래픽에 적용할 SGT 번호를 지정합니다. 유효한 값은 2~65519입니다. **trusted**는 명령에서 SGT가 지정된 인터페이스의 인그레스 트래픽이 SGT를 덮어쓰면 안 됨을 나타냅니다. 기본값은 신뢰할 수 없음입니다.

예

다음 예는 레이어 2 SGT Imposition에 대한 인터페이스를 활성화하고 인터페이스 신뢰 여부를 지정합니다.

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

수동으로 IP-SGT 바인딩 구성

IP-SGT 바인딩을 수동으로 구성하려면 다음 명령을 입력합니다..

명령	목적
`ciscoasa(config)# cts role-based sgt-map` [*IPv4_addr* | *IPv6_addr*] **sgt** *sgt_value* 예: `ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50`	IP-SGT 바인딩을 수동으로 구성할 수 있습니다. **sgt** *sgt_value*는 SGT 번호를 지정합니다. 유효한 값은 2~65519입니다.

1단계

문제 해결 정보

packet-tracer 명령을 사용하여 특정 세션 허용 또는 거부 이유, 사용할 SGT 값(패킷의 SGT에서, IP-SGT Manager에서 또는 인터페이스에 구성된 **policy static sgt** 명령에서), 적용할 보안 그룹 기반 보안 정책을 결정합니다.

다음 예는 IP 주소에 대한 보안 그룹 태그 매핑을 보여주는 **packet-tracer** 명령의 출력을 표시합니다.

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 security-group name alpha 30
security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

capture *capture-name* **type inline-tag** *tag* 명령을 사용하여 지정된 SGT 값이 있거나 없는 Cisco CMD 패킷(EtherType 0x8909)만 캡처합니다.

다음 예는 **show capture** 명령에서 지정된 SGT 값에 대한 출력을 표시합니다.

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

컨피그레이션 예

다음 예는 Cisco TrustSec을 사용하도록 ASA를 구성하는 방법을 보여줍니다.

```
// Import an encrypted CTS PAC file
    cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
    aaa-server cts-server-list protocol radius
    aaa-server cts-server-list host 10.1.1.100 cisco123
    cts server-group cts-server-list
// Configure SXP peers
    cts sxp enable
    cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
    object-group security objgrp-it-admin
          security-group name it-admin-sg-name
          security-group tag 1
    object-group security objgrp-hr-admin
        security-group name hr-admin-sg-name
        group-object it-admin
    object-group security objgrp-hr-servers
        security-group name hr-servers-sg-name
    access-list hr-acl permit ip object-group-security objgrp-hr-admin any
    object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
   interface gi0/1
   cts manual
   propagate sgt
   policy static sgt 100 trusted10.1.1.100 sgt 50
```

Cisco TrustSec을 위한 AnyConnect VPN 지원

ASA 버전 9.3(1)은 VPN 세션의 보안 그룹 태깅을 완벽히 지원합니다. SGT(Security Group Tag)는 외부 AAA 서버를 사용하거나 로컬 사용자 데이터베이스 컨피그레이션을 통해 VPN 세션에 할당할 수 있습니다. 그러면 이 태그를 레이어 2 이더넷을 통해 Cisco TrustSec 시스템으로 전파할 수 있습니다. 보안 그룹 태그는 AAA 서버가 SGT를 제공할 수 없을 때 그룹 정책과 로컬 사용자에게 유용합니다.

속성에 AAA 서버에서 VPN 사용자에 할당할 SGT가 없는 경우 ASA는 기본 그룹 정책의 SGT를 사용합니다. 그룹 정책에 SGT가 없다면 0x0 태그가 할당됩니다.

원격 사용자의 서버 연결을 위한 일반적인 단계

1. 사용자가 ASA에 연결합니다.
2. ASA가 ISE에서 SGT를 포함할 수 있는 AAA 정보를 요청합니다. ASA는 또한 사용자의 터널링된 트래픽에 대한 IP 주소도 할당합니다.
3. ASA은(는) AAA 정보를 이용하여 터널을 인증하고 생성합니다.
4. ASA은(는) AAA 정보의 SGT와 할당된 IP 주소를 이용하여 SGT를 레이어 2 헤더에 추가합니다.
5. SGT를 포함하는 패킷이 Cisco TrustSec 네트워크의 다음 피어 디바이스로 전달됩니다.

로컬 사용자 및 그룹에 SGT 추가

로컬 사용자 데이터베이스와 그룹 정책의 SGT 속성을 구성하려면 다음 명령을 입력하십시오.

명령	목적
`ciscoasa(config-group-policy)# **[no] security-group-tag value** *sgt*`	지정된 그룹 정책 또는 로컬 사용자 이름의 속성 세트에서 SGT 속성을 구성합니다. 이 명령의 기본 형식은 **security-group-tag none**이며 이 속성 세트에는 보안 그룹 태그가 없음을 의미합니다.
예: `ciscoasa(config-group-policy)# **security-group-tag value 101**`	**[no] security-group-tag value** *sgt* 명령은 컨피그레이션을 기본값으로 되돌립니다.

Cisco TrustSec 모니터링

ASA에서 Cisco TrustSec을 모니터링하려면 다음 명령을 하나 이상 입력합니다..

Command	목적
show running-config cts	Cisco TrustSec 인프라와 SXP 명령에 대해 구성된 기본값을 표시합니다.
show running-config [**all**] **cts role-based** [**sgt-map**]	사용자 정의 IP-SGT 바인딩 테이블 엔트리를 표시합니다.
show cts sxp connections	다중 컨텍스트 모드를 사용할 경우 특정 사용자 컨텍스트에 대해 ASA의 SXP 연결을 표시합니다.
show conn security-group	모든 SXP 연결의 데이터를 표시합니다.

Command	목적
show cts environment-data	ASA의 보안 그룹 테이블에 포함된 Cisco TrustSec 환경 정보를 봅니다.
show cts sgt-map	제어 경로의 IP 주소-보안 그룹 테이블 관리자 엔트리를 표시합니다.
show asp table cts sgt-map	데이터 경로에 유지되는 IP 주소-보안 그룹 테이블 매핑 데이터베이스에서 IP 주소-보안 그룹 테이블 매핑 엔트리를 표시합니다.
show cts pac	ISE에서 ASA로 가져온 PAC 파일에 관한 정보를 표시합니다. PAC 파일이 만료되거나 30일 내에 만료될 경우 경고 메시지를 표시합니다.

추가 참조 자료

참조	설명
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html	기업을 위한 Cisco TrustSec 시스템 및 아키텍처에 대해 설명합니다.
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html	구성 요소 설계 가이드 링크를 포함하여 기업에서 Cisco TrustSec 솔루션 배포를 위한 지침을 제공합니다.
http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf	ASA, 스위치, 무선 LAN(WLAN) 컨트롤러 및 라우터와 함께 사용하는 Cisco TrustSec 솔루션의 개요를 제공합니다.
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html	Cisco TrustSec 솔루션을 지원하는 Cisco 제품을 나열하는 Cisco TrustSec Platform Support Matrix를 제공합니다.

Cisco TrustSec 통합 기능 내역

표 32-6에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 32-6 Cisco TrustSec 통합 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
Cisco TrustSec Integration	9.0(1)	Cisco TrustSec은 기존 identity-aware 인프라 위에 구축되어 네트워크 디바이스 간 데이터 기밀을 보장하고 하나의 플랫폼으로 보안 액세스 서비스를 통합합니다. Cisco TrustSec 기능에서 적용 디바이스는 사용자 속성과 엔드포인트 속성의 조합을 사용하여 역할 기반 및 ID 기반 액세스 제어 결정을 내립니다. 이 릴리스에서는 ASA이(가) Cisco TrustSec과 통합되어 보안 그룹 기반 정책 시행을 제공합니다. Cisco TrustSec 도메인 내의 액세스 정책은 토폴로지에 종속되지 않으며 네트워크 IP 주소가 아닌 소스 및 대상 디바이스의 역할을 기반으로 합니다. ASA은(는) Cisco TrustSec 기능을 애플리케이션 검사와 같은 다른 유형의 보안 그룹 기반 정책에 사용할 수 있습니다. 예를 들어 보안 그룹 기반의 액세스 정책을 포함하는 클래스 맵을 구성할 수 있습니다. 도입되거나 수정된 명령: **access-list extended**, **cts sxp enable**, **cts server-group**, **cts sxp default**, **cts sxp retry period**, **cts sxp reconciliation period**, **cts sxp connection peer**, **cts import-pac**, **cts refresh environment-data**, **object-group security**, **security-group**, **show running-config cts**, **show running-config object-group**, **clear configure cts**, **clear configure object-group**, **show cts pac**, **show cts environment-data**, **show cts environment-data sg-table**, **show cts sxp connections**, **show object-group**, **show configure security-group**, **clear cts environment-data**, **debug cts** 및 **packet-tracer**.
레이어 2 보안 그룹 태그 도입	9.3(1)	보안 그룹 태그와 이더넷 태그를 함께 사용하면서 정책을 적용할 수 있습니다. 레이어 2 SGT Imposition이라고도 하는 SGT plus Ethernet Tagging은 ASA이(가) Cisco 고유의 이더넷 프레이밍(EtherType 0x8909)을 사용하여 이더넷 인터페이스에서 보안 그룹 태그를 보내고 받도록 하여 소스 보안 그룹 태그를 일반 텍스트 이더넷 프레임으로 삽입할 수 있게 됩니다. 도입되거나 수정된 명령: **cts manual**, **policy static sgt**, **propagate sgt**, **cts role-based sgt-map**, **show cts sgt-map**, **packet-tracer**, **capture**, **show capture**, **show asp drop**, **show asp table classify**, **show running-config all**, **clear configure all** 및 **write memory**.

33 장

ASA 및 Cisco 모바일 지원

ASA 및 Cisco 모바일 지원

Cisco ASA는 ISE(Cisco Identity Services Engine)의 구성 요소인 Cisco ME(Mobile Enablement)에서 관리되는 모바일 디바이스용 기업 네트워크에 대한 오프프레미스 액세스를 제공하는 에지 디바이스입니다. ISE ME를 지원하는 이러한 NAD(네트워크 액세스 디바이스) 역할에서 ASA는 모바일 디바이스 권한 부여, 등록 및 주기적인 체크인을 위한 프록시 역할을 수행합니다. ASA에서는 오프프레미스 원격 모바일 디바이스(AnyConnect Device Management 클라이언트)와 모바일 디바이스 관리자(ISE Mobile Enablement 서버) 간에 안전한 통신 경로를 제공합니다. 이를 통해 AnyConnect 클라이언트 애플리케이션을 실행 중인 오프프레미스 모바일 디바이스에서는 온프레미스 모바일 디바이스와 동일한 방식으로 모바일 디바이스 관리에 참여할 수 있습니다.

이 섹션에서는 ASA별 컨피그레이션 및 동작에 대해서만 설명합니다.

다음을 지정하여 ASA에서 ME 프록시 기능을 구성합니다.

- AnyConnect ME 클라이언트에서 등록 및 체크인 요청을 위해 사용하는 ASA 인터페이스 및 포트
- 클라이언트 인증에 사용되는 AAA 서버. 일반적으로 ISE Mobile Enablement 솔루션에 포함된 Radius 서버입니다.
- ASA를 식별하고 Mobile Enablement 서버에 인증하는 데 사용되는 트러스트 포인트

ASA MDM 프록시 지침 및 제한 사항

- ME Proxy 기능은 단일 컨텍스트 라우터 모드에서만 지원됩니다.
- ME Proxy를 사용하는 데 필요한 ASA 라이센스 요구 사항은 없습니다. ME 라이센스는 ISE에서 시행됩니다.

- 모바일 디바이스에서 실행되는 AnyConnect ME 클라이언트에서는 사용자가 온프레미스(기업 네트워크에 있음)인지 오프프레미스(공용 네트워크에 있음)인지 여부에 상관없이, ME 서버와 통신하는 데 필요한 것과 동일한 URI를 사용합니다. 이를 지원하려면 네트워크의 DNS 컨피그레이션에서는 오프프레미스 지원용 ASA 게이트웨이 및 온프레미스 지원용 ISE PSN(Policy Server Node)에 대한 ME URI를 해석해야 합니다.
- AnyConnect ME 클라이언트와 ASA 간의 인증 및 ASA와 ISE ME 서버 간의 인증을 위해서는 디지털 인증서가 필요합니다. ASA ME Proxy가 통합된 Mobile Enablement 솔루션의 인증서를 계획 및 구성할 경우, 다음을 고려하십시오.
  - ASA를 ISE Policy Service Node에 인증하는 인증서의 경우 동시에 프록시된 디바이스의 표시를 허용해야 합니다.
  - 등록 과정에서 SCEP의 결과로 수신된 모바일 디바이스의 AnyConnect 클라이언트 인증서의 경우, 오프프레미스 상태일 때 ASA에 대한 인증을 거부하고, 온프레미스 상태일 때 ISE를 인증해야 합니다. 마찬가지로, 이와 같은 방식으로 수신된 Applie iOS 모바일 디바이스의 추가 Apple iOS 클라이언트 인증서의 경우에도 이러한 방식으로 작동해야 합니다.
  - Subject Alternative Name(SAN) 필드에서 두 서버의 FQDN을 지정하여, 두 ASA 및 ISE를 모바일 디바이스의 클라이언트에 인증하도록 단일한 인증서를 정의할 수 있습니다.
- 오프프레미스로 관리되는 모바일 디바이스의 경우 ISE My Devices 포털을 사용할 수 없습니다. 이 포털에 액세스하려는 모바일 디바이스 사용자는 온프레미스 상태여야 합니다.

ASA를 MDM Proxy로 구성

시작하기 전에

- 권한 부여 및 어카운팅을 지원하려면 Radius 서버 그룹이 ISE AAA Radius 서버에 액세스할 수 있도록 구성해야 합니다.
- AnyConnect 클라이언트 대신 ASA를 ISE MDM 서버에 인증하려면 트러스트포인트를 구성해야 합니다.

절차

1단계 config 모드에서 config-mdm-proxy 모드로 들어가 MDM 프록시 기능을 구성 및 활성화합니다.

```
asa(config)# mdm-proxy
```

2단계 AnyConnect Device Management 등록 및 체크인을 위한 포트를 구성합니다.

기본 등록 포트는 443입니다. MDM 체크인 요청에 사용되는 포트를 지정해야 합니다. 두 포트의 값 범위는 1~65535 사이여야 합니다.

```
asa (config-mdm-proxy)# port enrollment 443 checkin 8906
```

3단계 MDM Proxy 세션을 지원하기 위해 이전에 정의된 인증 및 어카운팅 서버를 구성합니다.

```
asa (config-mdm-proxy)# accounting-server-group ISE-AAA
asa (config-mdm-proxy)# authentication-server-group ISE-AAA
```

4단계 모든 AnyConnect Device Management 세션 대신 ISE MDM Server에 대한 MDM Proxy 액세스를 지원하기 위해 이전에 정의된 트러스트포인트를 구성합니다.

```
asa (config-mdm-proxy)# trustpoint ASAtoISEMDM
```

5단계 (선택 사항) 비밀번호가 만료되기 전에 경고 메시지를 전송할 날짜를 지정합니다.

```
asa (config-mdm-proxy)# password-management 5
```

6단계 (선택 사항) MDM Proxy 세션 제한을 지정합니다.

a. 동시 MDM 세션 수를 설정합니다(범위는 1~10000이며, 기본값은 1000).

```
asa (config-mdm-proxy)# session-limit 5000
```

b. 등록 및 체크인의 최대 세션 기간을 설정합니다(기본값은 300).

```
asa (config-mdm-proxy)# session-timeout enrollment 600 checkin 600
```

7단계 외부 인터페이스에서 MDM Proxy 컨피그레이션을 활성화합니다.

```
asa (config-mdm-proxy)# enable outside
```

Mobile Enablement Proxy 활동 모니터링

ASA에서 Mobile Enhancement 통계를 보려면 다음 명령을 입력합니다.

show mdm-proxy statistics

현재 Mobile Enablement 컨피그레이션을 보려면 다음 명령을 입력합니다.

show running-config mdm-proxy

ASA Mobile Enablement Proxy의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
Mobile Enablement 프록시	9.3(1)	ISE Mobile Enablement 솔루션의 구성 요소인 Mobile Enablement 프록시를 사용하면 오프프레미스 모바일 디바이스에서 온프레미스 모바일 디바이스와 똑같은 방식으로 모바일 디바이스를 관리할 수 있습니다. config-mdm-proxy 모드를 시작하는 **mdm-proxy** 명령을 도입했습니다. 이 새 모드에는 다음 명령이 적용됩니다. **authentication-server-group, accounting-server-group, password-management, trusttpoint, port, session-limit, session-timeout** 및 **enable**

34 장

디지털 인증서

이 장에서는 디지털 인증서를 구성하는 방법에 대해 설명합니다.

디지털 인증서 소개

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 컨피그레이션 및 로드 밸런싱이 포함된 시나리오의 예는 다음 URL에서 확인하십시오. https://supportforums.cisco.com/docs/DOC-5964

공개 키 암호 방식

공개 키 암호 방식에 의한 디지털 인증서는 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 IPsec 피어 각각에서 통신 대상인 피어를 하나씩 구성해야 합니다. 따라서 네트워크에 새 피어를 추가할 때마다 이 피어가 안전하게 통신하려는 피어 각각의 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. 폐기된 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 키입니다.

- RSA 키는 SSH 또는 SSL에 사용할 수 있습니다.
- SCEP 등록에서는 RSA 키의 인증을 지원합니다.
- 키를 생성할 때 RSA 키의 최대 키 모듈러스는 2048비트입니다. 기본 크기는 1024입니다. RSA 키 쌍이 1024비트를 초과하는 ID 인증서를 사용하는 SSL 연결 중 상당수는 ASA 및 거부된 클라이언트리스(clientless) 로그인에서 CPU 사용량이 많아질 수 있습니다.
- 서명 작업에서 지원되는 최대 키 크기는 4096비트입니다. 크기가 2048 이상인 키를 사용하는 것이 좋습니다.
- 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 지점(Trustpoint)을 사용하여 CA와 인증서를 관리하고 추적할 수 있습니다. 신뢰 지점은 CA 또는 ID 쌍을 나타낸 것입니다. 신뢰 지점에는 CA의 ID, CA별 컨피그레이션 매개변수, 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 가리킬 경우, 그중 하나만 사용자 인증서의 유효성 검사에 사용할 수 있습니다. 동일한 CA를 가리키는 신뢰 지점 중 어느 것을 그 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 컨피그레이션을 다른 ASA에서 수동으로 복제하는 데 유용합니다.

인증서 등록

ASA에서는 신뢰 지점별로 1개의 CA 인증서가 필요하고, 신뢰 지점에서 사용하는 키의 컨피그레이션에 따라 그 자신을 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. 사이트 대 사이트 VPN에서는 각 ASA를 등록해야 합니다. 원격 액세스 VPN에서는 각 ASA와 각 원격 액세스 VPN 클라이언트를 등록해야 합니다.

SCEP 요청을 위한 프록시

ASA는 AnyConnect와 서드파티 CA 사이에서 SCEP 요청을 프록시할 수 있습니다. CA는 프록시의 역할을 하는 경우에만 ASA에 대한 액세스가 필요합니다. ASA에서 이러한 서비스를 제공하려면, ASA에서 등록 요청을 보내기에 앞서 사용자가 AAA에서 지원하는 방법 중 하나로 인증해야 합니다. 호스트 스캔 및 동적 액세스 정책을 사용하여 등록 자격 요건 규칙을 적용할 수도 있습니다.

ASA에서는 AnyConnect SSL 또는 IKEv2 VPN 세션을 사용하는 경우에만 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 인증서에 대한 폴링을 지원하지 않습니다.

ASA에서는 이 기능을 위한 로드 밸런싱을 지원합니다.

폐기 검사

발급된 인증서는 일정한 기간 동안 유효합니다. CA가 유효 기한 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 (그리고 폐기되지 않은) 인증서와 그 인증서 일련 번호의 전체 목록입니다. ASA는 ID 인증서부터 시작하여 하위 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 다음 CA 서버를 지원합니다.

Cisco IOS CS, ASA 로컬 CA, 다음을 비롯한 서드파티 X.509 규격 준수 CA 벤더:

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL은 ASA에서 유효 기한이 지나지 않은 어떤 인증서가 그 발급 CA에 의해 폐기되었는지를 확인할 수 있는 방법 중 하나입니다. CRL 컨피그레이션은 신뢰 지점 컨피그레이션에 포함되어 있습니다.

ASA에서 인증서를 확인할 때마다 반드시 CRL 검사를 수행하도록 **revocation-check crl** 명령을 사용하여 구성할 수 있습니다. 또한 **revocation-check crl none** 명령을 사용하여 CRL 검사를 선택 사항으로 설정할 수도 있습니다. 그러면 CA에서 업데이트된 CRL 데이터를 제공할 수 없는 경우에도 인증서 인증에 성공할 수 있습니다.

ASA에서는 HTTP, SCEP 또는 LDAP을 사용하여 CA로부터 CRL을 검색할 수 있습니다. 각 신뢰 지점에 대해 검색된 CRL은 신뢰 지점별로 구성 가능한 기간만큼 캐시에 저장할 수 있습니다.

ASA에서 구성된 기간보다 오랫동안 CRL을 캐시에 보관할 경우, ASA에서는 CRL을 너무 "오래되어" 신뢰할 수 없는 것으로 간주합니다. ASA는 다음번에 인증서 인증을 위해 오래된 CRL을 검사해야 할 때 더 새로운 버전의 CRL 검색을 시도합니다.

ASA에서 CRL을 캐시에 보관하는 기간은 다음 2가지 변수에 따라 결정됩니다.

- **cache-time** 명령에서 지정한 분 수. 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 오래된 CRL로 표시합니다.
- NextUpdate 필드가 필수 항목일 경우, ASA에서는 **cache-time** 명령으로 지정된 값과 NextUpdate 필드의 값 중 더 빠른 시점에 오래된 CRL로 표시합니다. 예를 들어, **cache-time** 명령에서 100분으로 설정되었고 NextUpdate 필드에서 다음 업데이트가 70분 후라고 지정되었다면 ASA는 70분이 지나면 CRL을 오래되었다고 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 어떤 인증서가 그 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. ASA는 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 시간 지연(time skew)을 허용합니다.

ASA에서 인증서를 확인할 때마다 반드시 OCSP 검사를 수행하도록 **revocation-check ocsp** 명령을 사용하여 구성할 수 있습니다. 또한 **revocation-check ocsp none** 명령을 사용하여 OCSP 검사를 선택 사항으로 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 OSCP 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 사용하게 합니다. 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 인증서

에 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 **revocation-check ocsp** 명령을 사용하여 클라이언트 인증서를 구성합니다.

로컬 CA

로컬 CA는 다음 작업을 수행합니다.

- ASA에서 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, 해지 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.

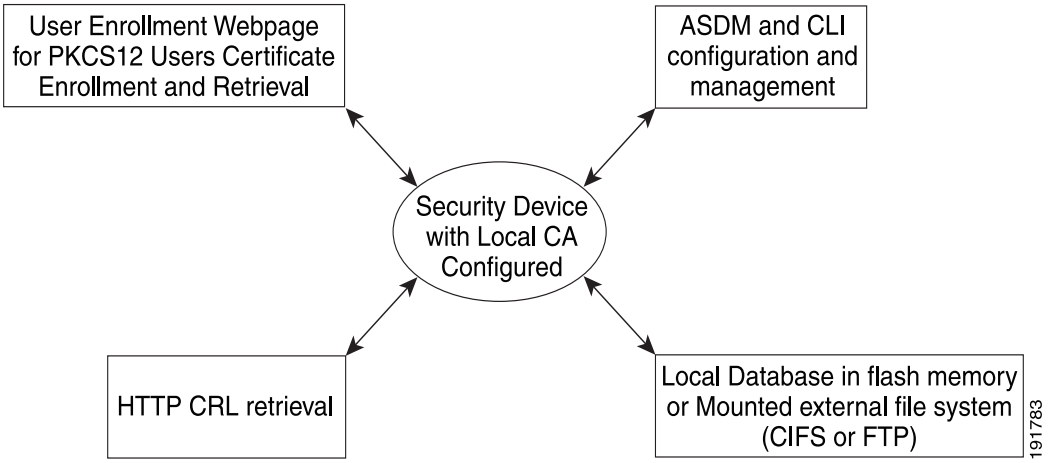
로컬 CA 사용자 데이터베이스에 저장할 수 있는 사용자 수에는 제한이 없습니다. 그러나 플래시 메모리 저장소 문제가 생길 경우, syslog가 생성되어 관리자에게 조치를 취하도록 알리며 저장소 문제가 해결될 때까지 로컬 CA를 사용하지 못할 수도 있습니다. 플래시 메모리는 사용자 수가 3,500명 이하인 데이터베이스를 저장할 수 있습니다. 사용자 수가 3,500명이 넘는 데이터베이스는 외부 저장소가 필요합니다.

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.

그림 34-1에서는 로컬 CA 서버가 ASA에 상주하고 있음을 알리고 웹 사이트 사용자의 등록 요청, 다른 인증서 유효성 검사 디바이스 및 ASA의 CRL 문의를 처리합니다. 로컬 CA 데이터베이스와 컨피그레이션 파일은 ASA 플래시 메모리(기본 저장소) 또는 별도의 스토리지 디바이스에서 유지 관리합니다.

그림 34-1 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 자격 증명을 사용자 인증 및 권한 부여 모두에 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.

로컬 인증서의 전제 조건

로컬 인증서는 먼저 다음 조건을 충족해야 합니다.

- 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. ASA에서 CA에 등록하여 인증서를 받을 때 ASA는 현재 시간이 인증서의 유효 기간에 속하는지 확인합니다. 그 범위를 벗어나면 등록이 실패합니다.

SCEP 프록시 지원의 전제 조건

ASA를 서드파티 인증서 요청을 제출하기 위한 프록시로 구성하려면 다음 요구 사항을 충족해야 합니다.

- 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.

디지털 인증서 지침

컨텍스트 모드 지침

- 서드파티 CA의 경우 단일 컨텍스트 모드에서만 지원됩니다.

장애 조치 지침

- 스테이트풀 장애 조치에서는 세션 복제를 지원하지 않습니다.
- 로컬 CA에 대해서는 장애 조치를 지원하지 않습니다.

IPv6 지침

IPv6를 지원하지 않습니다.

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 매개 변수를 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 그 가져온 인증서를 거부합니다. 예:

```
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

이 섹션에서는 로컬 CA 인증서를 구성하는 방법을 설명합니다. 이 유형의 디지털 인증서를 올바르게 구성하려면 제시된 순서대로 작업을 수행해야 합니다.

키 쌍 구성

키 쌍을 생성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto key generate rsa** 예: ciscoasa/contexta(config)# crypto key generate rsa	범용 RSA 키 쌍 1개를 생성합니다. 기본 키 모듈러스는 1024입니다. 다른 모듈러스 크기를 지정하려면 **modulus** 키워드를 사용합니다. **참고** RSA 키 쌍이 1024비트를 초과하는 ID 인증서를 사용하는 SSL 연결 중 상당수는 ASA 및 거부된 클라이언트리스 로그인에서 CPU 사용량이 많아질 수 있습니다.
2단계	**crypto key generate rsa label** *key-pair-label* 예: ciscoasa/contexta(config)# crypto key generate rsa label exchange	(선택 사항) 각 키 쌍에 레이블을 하나씩 지정합니다. 이 레이블은 해당 키 쌍을 사용하는 신뢰 지점에서 참조합니다. 레이블을 지정하지 않을 경우, 키 쌍은 자동으로 *Default-RSA-Key*라는 레이블을 갖습니다.
3단계	**show crypto key** *name of key* 예: ciscoasa/contexta(config)# show crypto key examplekey	생성한 키 쌍을 확인합니다.
4단계	**write memory** 예: ciscoasa(config)# write memory	생성한 키 쌍을 저장합니다.

키 쌍 제거

키 쌍을 제거하려면 다음 단계를 수행합니다.

명령	목적
crypto key zeroize rsa 예: ciscoasa(config)# crypto key zeroize rsa	키 쌍을 제거합니다.

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.

	명령	목적
1단계	**crypto ca trustpoint** *trustpoint-name* 예: ciscoasa/contexta(config)# crypto ca trustpoint Main	ASA에서 인증서를 받아야 하는 CA의 신뢰 지점을 생성합니다. crypto ca trustpoint 컨피그레이션 모드를 시작합니다. 여기서는 CA 관련 신뢰 지점 매개 변수를 제어하는데, 3단계부터 이 매개 변수를 구성할 수 있습니다. **참고** 연결을 시도할 때 신뢰 지점에서 ID 인증서를 검색하려 하면 신뢰 지점에 ID 인증서가 없다는 경고가 표시됩니다.
2단계	다음 옵션 중 하나를 선택합니다.	
	enrollment url *url* 예: ciscoasa/contexta(config-ca-trustpoint)# enrollment url http://10.29.67.142:80/certsrv/mscep/mscep.dll	지정된 신뢰 지점으로 SCEP를 사용한 자동 등록을 요청하고 등록 URL을 구성합니다.
	enrollment terminal 예: ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal	CA에서 가져온 인증서를 터미널에 붙여넣기하여 지정된 신뢰 지점으로 수동 등록을 요청합니다.
3단계	**revocation-check crl none** revocation-check crl revocation-check none 예: 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	사용 가능한 CRL 컨피그레이션 옵션을 지정합니다. **참고** 필수 또는 선택 사항인 CRL 검사를 활성화하려면 인증서 취득 후 CRL 관리를 위해 신뢰 지점을 구성해야 합니다.
4단계	**crl configure** 예: ciscoasa/contexta(config-ca-trustpoint)# crl configure	crl 컨피그레이션 모드를 시작합니다.
5단계	**email** *address* 예: ciscoasa/contexta(config-ca-trustpoint)# email example.com	등록 과정에서 CA에게 지정된 이메일 주소를 인증서의 SAN(Subject Alternative Name) 확장에 포함하도록 요청합니다.

	명령	목적
6단계	**enrollment retry period** 예: `ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5`	(선택 사항) 재시도 기간(분)을 지정하며, SCEP 등록에만 적용됩니다.
7단계	**enrollment retry count** 예: `ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2`	(선택 사항) 허용된 재시도 최대 횟수를 지정하며, SCEP 등록에만 적용됩니다.
8단계	**fqdn** *fqdn* 예: `ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com`	등록 과정에서 CA에게 특정 FQDN(Fully Qualified Domain Name)을 인증서의 SAN(Subject Alternative Name) 확장에 포함하도록 요청합니다.
9단계	**ip-address** *ip-address* 예: `ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1`	등록 과정에서 CA에게 ASA의 IP 주소를 인증서에 포함하도록 요청합니다.
10단계	**keypair** *name* 예: `ciscoasa/contexta(config-ca-trustpoint)# keypair exchange`	공개 키를 인증할 키 쌍을 지정합니다.
11단계	**match certificate map-name override ocsp** 예: `ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp`	OCSP responder 인증서의 유효성 검사에 사용할 OCSP URL 재정의 및 신뢰 지점을 구성합니다.
12단계	**ocsp disable-nonce** 예: `ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce`	OCSP 요청에서 nonce 확장을 비활성화합니다. nonce 확장은 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지합니다.
13단계	**ocsp url** 예: `ciscoasa/contexta(config-ca-trustpoint)# ocsp url`	ASA에서 신뢰 지점과 연결된 모든 인증서를 검사하는 데 클라이언트 인증서의 AIA 확장에 지정된 서버 대신 사용할 OCSP 서버를 구성합니다.
14단계	**password** *string* 예: `ciscoasa/contexta(config-ca-trustpoint)# password mypassword`	등록 과정에서 CA에 등록되는 챌린지 구문(challenge phrase)을 지정합니다. 일반적으로 CA는 후속 해지(revocation) 요청을 인증하는 데 이 구문을 사용합니다.

	명령	목적
15단계	**revocation check** 예: `ciscoasa/contexta(config-ca-trustpoint)# revocation check`	해지 확인 방법(CRL, OCSP, 없음)을 하나 이상 설정합니다.
16단계	**subject-name** *X.500 name* 예: `ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename`	등록 과정에서 CA에게 지정된 주체 DN을 인증서에 포함하도록 요청합니다. DN 문자열에 쉼표가 있을 경우 큰따옴표로 값 문자열을 묶습니다(예: O="Company, Inc.").
17단계	**serial-number** 예: `ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7`	등록 과정에서 CA에게 ASA 일련 번호를 인증서에 포함하도록 요청합니다.
18단계	**write memory** 예: `ciscoasa/contexta(config)# write memory`	실행 중인 컨피그레이션을 저장합니다.

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.

	명령	목적
1단계	**crypto ca trustpoint** *trustpoint-name* 예: `ciscoasa (config)# crypto ca trustpoint Main`	CRL 컨피그레이션을 수정할 신뢰 지점에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작합니다. **참고** 이 명령을 입력하기 전에 CRL을 활성화해야 합니다. 또한 CRL이 인증에 사용 가능한 상태여야 성공할 수 있습니다.
2단계	**crl configure** 예: `ciscoasa (config-ca-trustpoint)# crl configure`	현재 신뢰 지점에 대한 crl 컨피그레이션 모드를 시작합니다. **팁** 모든 CRL 컨피그레이션 매개 변수를 기본값으로 설정하려면 **default** 명령을 사용합니다. CRL 컨피그레이션 중에 언제라도 이 명령을 재입력하여 절차를 재시작할 수 있습니다.
3단계	다음 중 하나를 수행합니다.	

	명령	목적
	policy cdp 예: ciscoasa (config-ca-crl)# policy cdp	검색 정책을 구성합니다. CRL은 인증된 인증서에 지정된 CRL 배포 지점에서만 검색됩니다. **참고** SCEP 검색은 인증서에 지정된 배포 지점에서 지원하지 않습니다. 계속하려면 5단계로 진행합니다.
	policy static 예: ciscoasa (config-ca-crl)# policy static	검색 정책을 구성합니다. CRL은 사용자가 구성하는 URL에서만 검색됩니다. 계속하려면 4단계로 진행합니다.
	policy both 예: ciscoasa (config-ca-crl)# policy both	검색 정책을 구성합니다. CRL은 인증된 인증서에 지정된 CRL 배포 지점 및 사용자가 구성하는 URL에서 검색됩니다. 계속하려면 4단계로 진행합니다.
4단계	**url** *n url* 예: ciscoasa (config-ca-crl)# url 2 http://www.example.com	CRL 정책 구성 시 **static** 또는 **both** 키워드를 사용한 경우 CRL 검색용 URL을 구성해야 합니다. 1순위부터 5순위까지 최대 5개의 URL을 입력할 수 있습니다. *n*은 URL에 지정된 순위입니다. URL을 제거하려면 **no url** *n* 명령을 사용합니다.
5단계	**protocol http | ldap | scep** 예: ciscoasa (config-ca-crl)# protocol http	검색 방법을 구성합니다. HTTP, LDAP 또는 SCEP를 CRL 검색 방법으로 지정합니다.
6단계	**cache-time** *refresh-time* 예: ciscoasa (config-ca-crl)# cache-time 420	ASA에서 현재 신뢰 지점의 CRL을 캐시에 보관하는 기간을 구성합니다. *refresh-time*은 ASA에서 CRL을 오래된 것으로 간주할 때까지의 경과 시간(분)입니다.
7단계	다음 중 하나를 수행합니다.	
	enforcenextupdate 예: ciscoasa (config-ca-crl)# enforcenextupdate	CRL의 NextUpdate 필드가 필요합니다. 이는 기본 설정입니다.
	no enforcenextupdate 예: ciscoasa (config-ca-crl)# no enforcenextupdate	CRL의 NextUpdate 필드 부재를 허용합니다.
8단계	**ldap-defaults** *server* 예: ciscoasa (config-ca-crl)# ldap-defaults ldap1	LDAP이 검색 프로토콜로 지정된 경우 ASA에 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. **참고** IP 주소 대신 호스트 이름을 사용하여 LDAP 서버를 지정할 경우, ASA에서 DNS를 사용하도록 구성했어야 합니다.

	명령	목적
9단계	**ldap-dn** *admin-DN password* 예: ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ	LDAP 서버에서 자격 증명이 필요할 경우 CRL 검색을 허용합니다.
10단계	**crypto ca crl request** *trustpoint* 예: ciscoasa (config-ca-crl)# crypto ca crl request Main	지정된 신뢰 지점의 CA로부터 현재 CRL을 검색하고, 현재 신뢰 지점에 대해 CRL 컨피그레이션을 테스트합니다.
11단계	**write memory** 예: ciscoasa (config)# write memory	실행 중인 컨피그레이션을 저장합니다.

신뢰 지점 컨피그레이션 내보내기

신뢰 지점 컨피그레이션을 내보내려면 다음 명령을 입력합니다.

명령	목적
crypto ca export *trustpoint* 예: ciscoasa(config)# crypto ca export Main	모든 연결된 키와 인증서를 포함한 신뢰 지점 컨피그레이션을 PKCS12 형식으로 내보냅니다. ASA는 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.

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---
```

신뢰 지점 컨피그레이션 가져오기

신뢰 지점 컨피그레이션을 가져오려면 다음 명령을 입력합니다.

명령	목적
crypto ca import *trustpoint* **pkcs12** 예: ciscoasa(config)# crypto ca import Main pkcs12	신뢰 지점 컨피그레이션과 연결된 키 쌍 및 발급된 인증서를 가져옵니다. ASA는 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 그 CA가 발급한 사용자 인증서의 유효성 검사에 사용할 것인가는 **support-user-cert-validation** 키워드를 사용하여 제어합니다.

예

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 사용하여 IPsec 피어 인증서를 터널 그룹에 매핑할 수 있으며, 이를 위해 **tunnel-group-map** 명령을 사용합니다. ASA는 하나의 CA 인증서 맵을 지원하며, 여기에는 많은 규칙이 포함될 수 있습니다.

CA 인증서 맵 규칙을 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto ca certificate map** *sequence-number* 예: `ciscoasa(config)# crypto ca certificate map 1`	구성하려는 규칙에 대한 CA 인증서 맵 컨피그레이션 모드를 시작하고 규칙 색인 번호를 지정합니다.
2단계	**issuer-name** *DN-string* 예: `ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com`	발급된 모든 인증서의 DN을 지정합니다. 이는 자체 서명된 CA 인증서의 주체-이름 DN이기도 합니다. 쉼표를 사용하여 특성-값 쌍을 구분합니다. 쉼표를 포함하는 값을 따옴표로 묶습니다. issuer-name은 영숫자 500자 미만이어야 합니다. 기본 issuer-name은 cn=*hostame.domain-name*입니다.
3단계	**subject-name attr** *tag* **eq | co | ne | nc** *string* 예: `ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert`	ASA에서 인증서의 Subject 필드에서 발견한 값에 적용할 수 있는 테스트를 지정합니다. 테스트는 어떤 특성 또는 전체 필드에 적용할 수 있습니다. 규칙당 여러 개의 테스트를 구성할 수 있으며, 규칙에 따라 인증서가 일치하기 위해서는 이 명령으로 지정하는 모든 테스트의 결과가 True여야 합니다. 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.
4단계	**write memory** 예: `ciscoasa (config)# write memory`	실행 중인 컨피그레이션을 저장합니다.

수동으로 인증서 취득

수동으로 인증서를 취득하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto ca authenticate** *trustpoint* **예:** 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	구성된 신뢰 지점에 대한 CA 인증서를 가져옵니다. **참고** 이 단계에서는 신뢰 지점이 나타내는 CA로부터 base64 인코딩 CA 인증서를 취득한 상태임을 전제로 합니다. 신뢰 지점에서 인증서의 수동 취득을 요구할지는 신뢰 지점 구성 시 **enrollment terminal** 명령을 사용하여 결정합니다. 자세한 내용은 34-12 페이지의 신뢰 지점 구성을 참조하십시오.
2단계	**crypto ca enroll** *trustpoint* **예:** 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**	ASA를 신뢰 지점에 등록합니다. 데이터 서명을 위해 그리고 구성한 키 유형에 따라 데이터 암호화를 위해 인증서를 생성합니다. 서명과 암호화에 각기 다른 RSA 키를 사용할 경우 **crypto ca enroll** 명령은 각 키에 하나씩, 2개의 인증서 요청을 표시합니다. 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. 인증서는base64 형식이어야 합니다.

	명령	목적
3단계	**crypto ca import** *trustpoint* **certificate** 예: `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`	CA로부터 받은 각 인증서를 가져옵니다. 터미널에 base64 형식으로 인증서를 붙여넣도록 요청합니다.
4단계	**show crypto ca server certificate** 예: `ciscoasa(config)# show crypto ca server certificate Main`	ASA에 대해 발급된 인증서 세부사항 및 신뢰 지점을 위한 CA 인증서를 표시하여 등록 프로세스가 성공했음을 확인합니다.
5단계	**write memory** 예: `ciscoasa(config)# write memory`	실행 중인 컨피그레이션을 저장합니다. 수동 등록을 위해 구성하는 각 신뢰 지점에 대해 이 단계를 반복합니다.

SCEP로 인증서 자동 취득

SCEP를 사용하여 자동으로 인증서를 취득하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto ca authenticate** *trustpoint* 예: `ciscoasa/contexta(config)# crypto ca authenticate Main`	구성된 신뢰 지점에 대한 CA 인증서를 취득합니다. **참고** 이 단계에서는 신뢰 지점이 나타내는 CA로부터 base64 인코딩 CA 인증서를 취득한 상태임을 전제로 합니다. 신뢰 지점을 구성할 때 **enrollment url** 명령을 사용하여 SCEP를 통해 자동으로 인증서를 취득해야 하는지를 결정합니다. 자세한 내용은 34-12 페이지의 신뢰 지점 구성을 참조하십시오.

	명령	목적
2단계	**crypto ca enroll** *trustpoint* 예: ciscoasa/contexta(config)# crypto ca enroll Main	ASA를 신뢰 지점에 등록합니다. 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. ASA는 인증서 요청을 보내고 1분(기본값) 이내에 CA로부터 인증서를 받지 못할 경우 인증서 요청을 재전송합니다. ASA는 인증서를 수신할 때까지 계속 1분마다 인증서 요청을 보냅니다. 신뢰 지점에 대해 구성된 정규화된 도메인 이름이 ASA의 정규화된 이름과 같지 않을 경우(대소문자 구분) 경고가 나타납니다. 이 문제를 해결하려면 등록 프로세스를 종료하고 필요한 수정을 하고 **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.
3단계	**show crypto ca server certificate** 예: ciscoasa/contexta(config)# show crypto ca server certificate Main	ASA에 대해 발급된 인증서 세부사항 및 신뢰 지점을 위한 CA 인증서를 표시하여 등록 프로세스가 성공했음을 확인합니다.
4단계	**write memory** 예: ciscoasa/contexta(config)# write memory	실행 중인 컨피그레이션을 저장합니다.

SCEP 요청을 위한 프록시 지원 구성

ASA에서 서드파티 CA를 사용하여 원격 액세스 엔드포인트를 인증하도록 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto ikev2 enable outside client-services port** *portnumber* 예: ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services	클라이언트 서비스를 활성화합니다. **참고** IKEv2를 지원하는 경우에만 필요합니다. tunnel-group ipsec-attributes 컨피그레이션 모드에서 이 명령을 입력합니다. 기본 포트 번호는 443입니다.

	명령	목적
2단계	**scep-enrollment enable** 예: `ciscoasa(config-tunnel-general)# scep-enrollment enable` `INFO: 'authentication aaa certificate' must be configured to complete setup of this option.`	터널 그룹에 대해 SCEP 등록을 활성화합니다. tunnel-group general-attributes 컨피그레이션 모드에서 이 명령을 입력합니다.
3단계	**scep-forwarding-url value** *URL* 예: `ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/`	그룹 정책에 대해 SCEP CA를 등록합니다. 그룹 정책당 1번씩 이 명령을 입력하여 서드파티 디지털 인증서를 지원합니다. group-policy general-attributes 컨피그레이션 모드에서 명령을 입력합니다. *URL*은 CA의 SCEP URL입니다.
4단계	**secondary-pre-fill-username clientless hide use-common-password** *password* 예: `ciscoasa(config)# tunnel-group remotegrp webvpn-attributes` `ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide use-common-password secret`	WebLaunch의 SCEP 프록시 지원에 인증서를 사용할 수 없을 때 공통의 보조 비밀번호를 제공합니다. 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.
5단계	**secondary-pre-fill-username ssl-client hide use-common-password** *password* 예: `ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide use-common-password secret`	AnyConnect VPN 세션에서 미리 채워진 보조 사용자 이름을 숨깁니다. 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.
6단계	**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**] 예: `ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback cisco-secure-desktop machine-unique-id`	인증서를 사용할 수 없을 때 사용자 이름을 제공합니다.

로컬 CA 서버 활성화

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.

로컬 CA 서버를 활성화하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: ciscoasa (config)# crypto ca server	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**no shutdown** 예: ciscoasa (config-ca-server)# no shutdown	로컬 CA 서버를 활성화합니다. 로컬 CA 서버 인증서, 키 쌍 및 필요한 데이터베이스 파일을 생성하고 로컬 CA 서버 인증서 및 키 쌍을 PKCS12 파일 형식으로 저장소에 보관합니다. 8-65자의 영숫자 비밀번호가 필요합니다. 최초 시작 후 패스프레이즈 입력 화면 없이 로컬 CA를 비활성화할 수 있습니다. **참고** 로컬 CA 서버를 활성화한 다음 컨피그레이션을 저장하여 재부팅하더라도 로컬 CA 인증서와 키 쌍이 손실되지 않게 합니다.

예

다음 예에서는 로컬 CA 서버를 활성화합니다.

```
hostname (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:
```

로컬 CA 서버 구성

로컬 CA 서버를 구성하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 생성합니다.
2단계	**smtp from-address** *e-mail_address* 예: `ciscoasa (config-ca-server) # smtp from-address SecurityAdmin@example.com`	SMTP from-address를 지정합니다. 이는 로컬 CA에서 사용자에게 등록 초대를 위한 OTP를 전달하는 이메일 메시지를 보낼 때 발신 주소로 사용하는 유효한 이메일 주소입니다.
3단계	**subject-name-default** *dn* 예: `hostname (config-ca-server)# subject-name-default cn=engineer, o=asc systems, c="US"`	(선택 사항) 발급된 인증서에서 각 사용자 이름에 추가되는 주체-이름 DN을 지정합니다. 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 매개 변수를 면밀하게 검토해야 합니다. 처음으로 로컬 CA를 활성화한 다음에는 발급자-이름 및 키 크기 서버 값을 변경할 수 없기 때문입니다.
4단계	**no shutdown** 예: `hostname (config-ca-server)# no shutdown`	자체 서명 인증서를 생성하고 이를 ASA의 로컬 CA와 연결합니다. 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 매개 변수에 사전 정의된 기본값을 사용하면서 로컬 CA 서버를 구성하고 활성화하는 방법을 보여줍니다.

```
hostname (config)# crypto ca server
hostname (config-ca-server) # smtp from-address SecurityAdmin@example.com
hostname (config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
hostname (config-ca-server)# no shutdown
```

로컬 CA 서버 사용자 지정

사용자 지정 로컬 CA 서버를 구성하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**issuer-name** *DN-string* 예: `hostname (config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC Systems`	기본값이 없는 매개 변수를 지정합니다.
3단계	**smtp subject** *subject-line* 예: `hostname (config-ca-server) # smtp subject Priority E-Mail: Enclosed Confidential Information is Required for Enrollment`	로컬 CA 서버에서 보내는 모든 이메일 메시지의 Subject 필드에 나타나는 텍스트를 사용자 지정합니다.
4단계	**smtp from-address** *e-mail_address* 예: `hostname (config-ca-server) # smtp from-address SecurityAdmin@example.com`	로컬 CA 서버에서 생성하는 모든 이메일 메시지의 From: 필드에 사용할 이메일 주소를 지정합니다.
5단계	**subject-name-default** *dn* 예: `hostname (config-ca-server) # subject-name default cn=engineer, o=ASC Systems, c=US`	발급된 인증서의 사용자 이름에 추가될 선택적 주체-이름 DN을 지정합니다. 로컬 CA 서버에서 발급하는 모든 사용자 인증서에서 기본 주체-이름 DN이 사용자 이름의 일부가 됩니다. 허용된 DN 특성 키워드는 다음과 같습니다. • C = 국가(Country) • 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(Surname) • ST = 시/도(State/Province) **참고** 표준 주체-이름 기본값으로 사용할 subject-name-default를 지정하지 않을 경우, 사용자를 추가할 때마다 DN을 지정해야 합니다.

로컬 CA 서버 디버깅

새로 구성된 로컬 CA 서버를 디버깅하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: ciscoasa (config)# crypto ca server	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**debug crypto ca server** 예: ciscoasa (config-ca-server)# debug crypto ca server	로컬 CA 서버를 구성하고 활성화할 때 디버깅 메시지를 표시합니다. 레벨 1 디버깅 기능을 수행합니다. 레벨 1-255를 사용할 수 있습니다. **참고** 사용량이 많은 네트워크에서는 디버깅 명령 때문에 트래픽 속도가 느려질 수 있습니다. 레벨 5 이상은 원시 데이터 덤프 전용이며, 일반적인 디버깅 과정에서는 과다한 출력 때문에 삼가야 합니다.

로컬 CA 서버 비활성화

로컬 CA 서버를 비활성화하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: ciscoasa (config)# crypto ca server	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**shutdown** 예: ciscoasa (config-ca-server)# shutdown INFO: Local CA Server has been shutdown.	로컬 CA 서버를 비활성화합니다. 웹 사이트 등록을 비활성화하고, 로컬 CA 서버 컨피그레이션의 수정을 허용합니다. 현재 컨피그레이션 및 관련 파일을 저장합니다. 최초 시작 후 패스프레이즈 입력 화면 없이 로컬 CA를 다시 활성화할 수 있습니다.

로컬 CA 서버 삭제

(활성화되었거나 비활성화된) 기존 로컬 CA 서버를 삭제하려면 다음 명령 중 하나를 입력합니다.

명령	목적
다음 중 하나를 수행합니다.	

명령	목적
no crypto ca server 예: ciscoasa (config)# no crypto ca server	(활성화되었거나 비활성화된) 기존 로컬 CA 서버를 제거합니다. **참고** 로컬 CA 서버를 삭제하면 ASA에서 컨피그레이션이 제거됩니다. 삭제된 컨피그레이션은 복구 불가합니다.
clear configure crypto ca server 예: ciscoasa (config)# clear config crypto ca server	해당 로컬 CA 서버 데이터베이스와 컨피그레이션 파일(즉 와일드카드 이름 LOCAL-CA-SERVER.*의 모든 파일)도 삭제해야 합니다.

로컬 CA 인증서 특성 구성

로컬 CA 인증서의 다음 특성을 구성할 수 있습니다.

- 모든 사용자 인증서에 나타나는 인증서 발급자의 이름
- 로컬 CA 인증서(서버 및 사용자)와 CRL의 수명
- 로컬 CA 및 사용자 인증서와 연결된 공용/개인 키 쌍의 길이

발급자 이름 구성

인증서 발급자 이름을 구성하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**issuer-name** *DN-string* 예: `hostname (config-ca-server)# issuer-name CN=xx5520,CN=30.132.0.25,ou=DevTest, ou=QA,O=ABC Systems`	로컬 CA 인증서 주체 이름을 지정합니다. 구성된 인증서 발급자 이름은 자체 서명 로컬 CA 인증서의 주체 이름이자 발급자 이름이며, 발급된 모든 클라이언트 인증서 및 발급된 CRL의 발급자 이름입니다. 로컬 CA의 기본 발급자 이름은 *hostname.domainname* 형식입니다. **참고** 로컬 CA를 처음으로 활성화한 다음에는 발급자 이름 값을 변경할 수 없습니다.

CA 인증서 수명 구성

로컬 CA 서버 인증서의 수명을 구성하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**lifetime ca-certificate** *time* 예: `hostname (config-ca-server)# lifetime ca-certificate 365`	인증서에 포함된 만료 날짜를 확인합니다. 로컬 CA 인증서의 기본 수명은 3년입니다. 인증서의 유효 기한이 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빨라야 합니다.
3단계	**no lifetime ca-certificate** 예: `hostname (config-ca-server)# no lifetime ca-certificate`	(선택 사항) 로컬 CA 인증서 수명을 기본값인 3년으로 재설정합니다. 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 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 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**lifetime certificate** *time* 예: `hostname (config-ca-server)# lifetime certificate 60`	원하는 사용자 인증서 유효 기간을 설정합니다. **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 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**lifetime crl** *time* 예: `hostname (config-ca-server)# lifetime crl 10`	원하는 CRL 유효 기간을 설정합니다. 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.
3단계	**crypto ca server crl issue** 예: `ciscoasa(config)# crypto ca server crl issue` `A new CRL has been issued.`	언제라도 강제적으로 CRL을 배포합니다. 그러면 즉시 업데이트하여 최신 CRL을 재생성하여 기존 CRL을 덮어씁니다. **참고** CRL 파일이 실수로 제거되었거나 손상되어 재생성해야 하는 경우에만 이 명령을 사용합니다.

서버 키 크기 구성

서버 키 크기를 구성하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: ciscoasa (config)# crypto ca server	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**keysize server** 예: hostname (config-ca-server)# keysize server 2048	사용자 인증서 등록 시 생성되는 공용 키와 개인 키의 크기를 지정합니다. 선택 가능한 키 쌍 크기는 512비트, 768비트, 1024비트, 2048비트이며 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

다음은 데이터베이스의 사용자 인증서 2개를 표시하는 샘플 출력입니다.

```
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 --->
```

외부 로컬 CA 파일 저장소 설정

로컬 CA 서버 컨피그레이션, 사용자, 발급된 인증서, CRL을 플래시 메모리 또는 외부 로컬 CA 파일 시스템에 있는 로컬 CA 서버 데이터베이스에 저장할 수 있습니다. 외부 로컬 CA 파일 저장소를 구성하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**mount** *name* **type** 예: `hostname (config)# mount mydata type cifs`	특정 파일 시스템 유형의 컨피그레이션 모드에 액세스합니다.
2단계	**mount** *name* **type cifs** 예: `hostname (config-mount-cifs)# mount mydata type cifs` `server 10.1.1.10 share myshare` `domain example.com` `username user6` `password ********` `status enable`	CIFS 파일 시스템을 마운트합니다. **참고** 파일 시스템을 마운트한 사용자만 **no mount** 명령을 사용하여 마운트 해제할 수 있습니다.
3단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
4단계	**database path** *mount-name directory-path* 예: `hostname (config-ca-server)# database path` `mydata:newuser`	*mydata*, 즉 로컬 CA 서버 데이터베이스에 사용할 미리 마운트된 CIFS 파일 시스템의 위치를 지정합니다. 서버와의 경로를 설정한 다음 저장 및 보관에 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.
5단계	**write memory** 예: `ciscoasa (config)# write memory`	실행 중인 컨피그레이션을 저장합니다. 외부 로컬 CA 파일 저장소의 경우, ASA 컨피그레이션을 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

지정된 인터페이스 또는 포트에서 CRL을 HTTP 다운로드할 수 있게 하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** **예:** `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**publish-crl interface** *interface* **port** *portnumber* **예:** `hostname (config-ca-server)# publish-crl outside 70`	인터페이스의 포트를 열어 그 인터페이스에서 CRL에 액세스할 수 있게 합니다. 지정된 인터페이스와 포트는 CRL 요청을 수신하는 데 사용합니다. 인터페이스와 선택 사항인 포트 옵션은 다음과 같습니다. • inside—인터페이스/GigabitEthernet0/1 이름 • management—인터페이스/ Management0/0 이름 • outside—인터페이스/GigabitEthernet0/0 이름 • 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 그 경로, /user8/my_crl_file이 구성된 CDP URL과 일치하는지 확인합니다. 경로가 일치하면 ASA는 저장된 CRL 파일을 반환합니다. **참고** 프로토콜은 HTTP여야 합니다. 즉 표시되는 접두사는 http://입니다.

CRL 저장

자동으로 생성된 로컬 CA의 CRL에 대해 구체적인 위치를 설정하려면 단일 컨텍스트 또는 다중 컨텍스트 모드에서 다음 사이트 대 사이트 작업을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**cdp-url** *url* 예: `ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl`	모든 발급된 인증서에 포함할 CDP를 지정합니다. CDP에 대해 구체적인 위치를 구성하지 않을 경우 기본 URL 위치는 http://*hostname.domain*/+CSCOCA+/asa_ca.crl입니다. 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 대해서는 34-32 페이지의 CRL 다운로드를 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 매개 변수 설정

등록 매개 변수를 설정하려면 다음 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**otp expiration** *timeout* 예: `ciscoasa(config-ca-server)# otp expiration 24`	로컬 CA 등록 페이지를 위해 발급된 OTP의 유효 기간(시간)을 지정합니다. 기본 유효 기간은 72시간입니다. **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.
3단계	**enrollment-retrieval** *timeout* 예: `ciscoasa(config-ca-server)# enrollment-retrieval 120`	이미 등록된 사용자가 PKCS12 등록 파일을 검색할 수 있는 기간(시간)을 지정합니다. 이 기간은 사용자가 성공적으로 등록되면 시작합니다. 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 명령을 수행합니다.

	명령	목적
1단계	**crypto ca server user-db add** *username* [**dn** *dn*] [**email** *emailaddress*] 예: `hostname (config-ca-server)# crypto ca server user-db add user1 dn user1@example.com, Engineer, Example Company, US, email user1@example.com`	로컬 CA 데이터베이스에 새 사용자를 추가합니다. 옵션은 다음과 같습니다. • *username*—4자~64자의 문자열이며, 추가되는 사용자의 간단한 사용자 이름입니다. 사용자 이름으로 이메일 주소도 가능합니다. 그러면 등록 초대를 위해 필요할 때 사용자에게 연락하는 데 사용됩니다. • *dn*—고유 이름, 즉 OSI Directory(X.500) 항목의 글로벌 정식 이름입니다(예: cn=user1@example.com, cn=Engineer, o=Example Company, c=US). • *e-mail-address*—OTP 및 알림이 전송될 새 사용자의 이메일 주소입니다.

	명령	목적
2단계	**crypto ca server user-db allow** *user* 예: `hostname (config-ca-server)# crypto ca server user-db allow user6`	새로 추가된 사용자에게 사용자 권한을 부여합니다.
3단계	**crypto ca server user-db email-otp** *username* 예: `hostname (config-ca-server)# crypto ca server user-db email-otp exampleuser1`	로컬 CA 데이터베이스의 사용자에게 사용자 인증서를 등록하고 다운로드하도록 알립니다. 자동으로 사용자에게 이메일을 통해 OTP를 보냅니다. **참고** 관리자가 사용자에게 이메일을 통해 알림을 보내기 위해서는 그 사용자를 추가할 때 사용자 이름 필드 또는 이메일 필드에 이메일 주소를 지정해야 합니다.
4단계	**crypto ca server user-db show-otp** 예: `hostname (config-ca-server)# crypto ca server user-db show-otp`	발급된 OTP를 표시합니다.
5단계	**otp expiration** *timeout* 예: `hostname (config-ca-server)# otp expiration 24`	등록 기한(시간)을 설정합니다. 기본 유효 기간은 72시간입니다. **otp expiration** 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 기한 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.

	명령	목적
1단계	**crypto ca server** 예: ciscoasa (config)# crypto ca server	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**renewal-reminder** *time* 예: ciscoasa (config-ca-server)# renewal-reminder 7	로컬 CA 인증서가 만료되기 며칠(1-90) 전에 최초의 재등록 리마인더를 인증서 소유자에게 보낼 것인지 지정합니다. 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 유효하고 곧 만료되는 인증서를 보유한 모든 사용자에게 인증서 갱신 권한을 자동으로 부여합니다. 단, 사용자가 사용자 데이터베이스에 있어야 합니다. 따라서 관리자가 어떤 사용자에 대해서는 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.

	명령	목적
1단계	**crypto ca server** 예: ciscoasa (config)# crypto ca server	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**crypto ca server unrevoke** *cert-serial-no* 예: ciscoasa (config)# crypto ca server unrevoke 782ea09f	사용자를 복원하고 로컬 CA에서 발급했으나 폐기되었던 인증서를 폐기 해제합니다. 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 유효한 인증서를 폐기 (또는 폐기 해제)하면 CRL은 자동으로 이 변경 사항을 반영합니다.

사용자 삭제

사용자 이름을 사용하여 사용자 데이터베이스에서 어떤 사용자를 삭제하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**crypto ca server user-db remove** *username* 예: `ciscoasa (config)# crypto ca server user-db remove user1`	사용자 데이터베이스에서 사용자를 삭제하고, 그 사용자에게 발급되었던 모든 유효한 인증서를 폐기할 수 있게 합니다.

인증서 폐기

사용자 인증서를 폐기하려면 다음 단계를 수행합니다.

	명령	목적
1단계	**crypto ca server** 예: `ciscoasa (config)# crypto ca server`	local ca server 컨피그레이션 모드를 시작합니다. 로컬 CA를 구성하고 관리할 수 있습니다.
2단계	**crypto ca server revoke** *cert-serial-no* 예: `ciscoasa (config-ca-server)# crypto ca server revoke 782ea09f`	인증서 일련 번호를 16진수 형식으로 입력합니다. 로컬 CA 서버의 인증서 데이터베이스 및 CRL에서 해당 인증서를 폐기된 것으로 표시합니다. CRL은 자동으로 재배포됩니다. **참고** ASA의 인증서를 폐기해야 하는 경우 비밀번호도 필요합니다. 따라서 비밀번호를 기록하여 안전한 곳에 보관해야 합니다.

로컬 CA 인증서 데이터베이스 유지 관리

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.

로컬 CA 인증서 롤오버

로컬 CA 인증서가 만료되기 30일 전에 롤오버 대체 인증서가 생성되고 syslog 메시지를 통해 관리자에게 로컬 CA 롤오버 시점임을 알립니다. 새 로컬 CA 인증서는 현재 인증서가 만료되기 전에 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.

예

다음 예는 base64 인코딩 로컬 CA 인증서를 보여줍니다.

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG515Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

로컬 CA 서버 인증서 및 키 쌍 보관

로컬 CA 서버 인증서와 키 쌍을 보관하려면 다음 명령을 입력합니다.

명령	목적
copy **예:** `hostname# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/`	ASA에서 로컬 CA 서버 인증서와 키 쌍 및 모든 파일을 FTP 또는 TFTP를 사용하여 복사합니다. **참고** 가급적 자주 모든 로컬 CA 파일을 백업해야 합니다.

디지털 인증서 모니터링

인증서 컨피그레이션 및 데이터베이스 정보를 표시하려면 다음 명령을 하나 이상 입력합니다.

명령	목적
show crypto ca server	로컬 CA 컨피그레이션 및 상태를 표시합니다.
show crypto ca server cert-db	로컬 CA에서 발급한 사용자 인증서를 표시합니다.
show crypto ca server certificate	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	CRL을 표시합니다.

명령	목적
show crypto ca server user-db	사용자와 그 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	등록할 자격이 있는 사용자를 표시합니다.
show crypto ca server user-db enrolled	등록된 사용자를 유효한 인증서와 함께 표시합니다.
show crypto ca server user-db expired	인증서가 만료된 사용자를 표시합니다.
show crypto ca server user-db on-hold	인증서가 없고 등록이 허용되지 않은 사용자를 표시합니다.
show crypto key *name of key*	생성한 키 쌍을 표시합니다.
show running-config	로컬 CA 인증서 맵 규칙을 표시합니다.

예

다음 예는 RSA 범용 키를 보여줍니다.

```
ciscoasa/contexta(config)# show crypto key mypubkey
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ea51b7
  0781848f 78bccac2 4a1b5b8d 2f3e30b4 4cae9f86 f4485207 159108c9 f5e49103
  9eeb0f5d 45fd1811 3b4aafce 292b3b64 b4124a6f 7a777b08 75b88df1 8092a9f8
  5508e9e5 2c271245 7fd1c0c3 3aaf1e04 c7c4efa4 600f4c4a 6afe56ad c1d2c01c
  e08407dd 45d9e36e 8cc0bfef 14f9e6ac eca141e4 276d7358 f7f50d13 79020301 0001
Key pair was generated at: 16:34:54 central Feb 10 2010
```

다음 예는 로컬 CA CRL을 보여줍니다.

```
hostname (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.

```
hostname (config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
```

```
notified: 0
hostname (config)#
```

다음 예는 **show running-config** 명령의 출력을 표시합니다. 여기에 로컬 CA 인증서 맵 규칙이 나타납니다.

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

인증서 관리 기능 내역

표 34-1 인증서 관리 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
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 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다.
인증서 관리	7.2(1)	도입된 명령: **issuer-name** *DN-string*, **revocation-check crl none, revocation-check crl, revocation-check none** 다음 명령은 더 이상 사용되지 않습니다. **crl** {**required** | **optional** | **nocheck**}
인증서 관리	8.0(2)	도입된 명령: **cdp-url**, **crypto ca server**, **crypto ca server crl issue**, **crypto ca server revoke** *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*, **debug crypto 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**, **show crypto ca server crl**, **show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**], **show crypto key** *name of key*, **show running-config**, **shutdown**

표 34-1 인증서 관리 기능 내역(계속)

기능 이름	플랫폼 릴리스	기능 정보
SCEP 프록시	8.4(1)	서드파티 CA의 디바이스 인증서를 안전하게 배포하는 이 기능을 도입했습니다. 도입된 명령: **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**]

8 파 트

시스템 관리

35 장

관리 액세스

이 장에서는 텔넷, SSH, HTTPS(ASDM 사용)를 통한 시스템 관리를 위해 Cisco ASA에 액세스하는 방법, 사용자를 인증하고 권한을 부여하는 방법, 로그인 배너를 만드는 방법을 설명합니다.

참고 관리 액세스를 위해 ASA 인터페이스에 액세스할 때 호스트 IP 주소를 허용하는 액세스 규칙은 필요 없습니다. 이 장의 섹션에 따라 관리 액세스를 구성하면 됩니다.

ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성

이 섹션에서는 클라이언트에서 ASDM, 텔넷 또는 SSH를 사용하여 ASA에 액세스하는 방법을 설명합니다.

ASA에서 ASDM, 텔넷 또는 SSH에 액세스하기 위한 라이센싱 요구 사항

다음 표는 이 기능의 라이센싱 요구 사항을 보여줍니다.

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

모델 지침

ASASM에서는 스위치에서 ASASM로의 세션이 텔넷 세션입니다. 그러나 이 섹션에 따른 텔넷 액세스 컨피그레이션은 필요 없습니다.

추가 지침

- VPN 터널 내에서 텔넷을 사용하지 않는 한 텔넷을 최하위 보안 인터페이스에서 사용할 수 없습니다.
- ASA 를 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. 35-10 페이지의 VPN 터널을 통한 관리 액세스 구성을 참조하십시오.
- ASA에서는 다음을 허용합니다.
  - 컨텍스트당 최대 5개의 동시 텔넷 연결 가능. 모든 컨텍스트에서 최대 100개의 연결 할당 가능
  - 컨텍스트당 최대 5개의 동시 SSH 연결 가능. 모든 컨텍스트에서 최대 100개의 연결 할당 가능
  - 컨텍스트당 최대 5개의 동시 ASDM인스턴스 가능. 모든 컨텍스트에서 최대 32개의 ASDM 인스턴스 가능.
- ASA는 SSH 버전 1 및 버전 2에서 제공하는 SSH 원격 셸 기능을 지원하고, DES 및 3DES 암호를 지원합니다.
- SSL 및 SSH를 통한 XML 관리는 지원하지 않습니다.

- (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 구성해야 합니다. 그런 다음 **username** 명령을 입력하여를 사용하여 로컬 사용자를 정의합니다. 로컬 데이터베이스 대신에 AAA 서버를 인증에 사용하려는 경우, 만일에 대비하여 로컬 인증도 구성하는 것이 좋습니다.
- (9.1(2) 이상) 기본 텔넷 로그인 비밀번호가 제거되었습니다. 텔넷을 사용하기 전에 직접 비밀번호를 설정해야 합니다. 13-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정을 참조하십시오.
- ASA 인터페이스와의 텔넷 또는 SSH 연결이 안 될 경우 35-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성의 설명에 따라 ASA와의 텔넷 또는 SSH를 활성화했는지 확인하십시오.

텔넷 액세스 구성

텔넷을 사용하여 ASA에 연결하는 것이 허용된 클라이언트 IP 주소를 지정하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**telnet** *source_IP_address mask source_interface* **예:** `ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside`	각 주소 또는 서브넷에 대하여 ASA에서 어떤 IP 주소로부터의 연결을 허용할지 지정합니다. 인터페이스가 하나뿐일 경우, 그 인터페이스의 보안 레벨이 100이라면 텔넷에서 그 인터페이스에 액세스하도록 구성할 수 있습니다.
2단계	**telnet timeout** *minutes* **예:** `ciscoasa(config)# telnet timeout 30`	ASA에서 세션 연결을 끊기 전에 얼마 동안 텔넷 세션을 유휴 상태로 유지할 수 있는지 설정합니다. 1분~1440분 범위에서 시간 초과를 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 보여줍니다.

```
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 보여줍니다.

```
ciscoasa(config)# telnet 192.168.3.0 255.255.255.0 inside
```

텔넷 클라이언트 사용

텔넷을 사용하여 ASA CLI에 액세스하려면 **password** 명령으로 설정한 로그인 비밀번호를 입력합니다. 텔넷을 사용하기 전에 직접 비밀번호를 설정해야 합니다. 13-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정을 참조하십시오.

텔넷 인증을 구성하는 경우(35-17 페이지의 CLI 및ASDM, 액세스를 위한 인증 구성 참조) AAA 서버 또는 로컬 데이터베이스에 의해 정의된 사용자 이름과 비밀번호를 입력합니다.

SSH 액세스 구성

클라이언트 IP 주소를 확인하고 SSH를 사용하여 ASA에 연결할 수 있는 사용자를 정의하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**crypto key generate rsa modulus** *modulus_size* **예:** `ciscoasa(config)# crypto key generate rsa modulus 1024`	SSH에 필요한 RSA 키 쌍을 생성합니다(물리적 ASA만 해당). **참고** ASAv에서는 구축 후 자동으로 RSA 키 쌍이 생성됩니다. 모듈러스 값(비트)은 512, 768, 1024 또는 2048입니다. 지정하는 키 모듈러스 크기가 클수록 RSA 키 쌍을 생성하는 데 오래 걸립니다. 권장되는 값은 1024입니다.
2단계	**write memory** **예:** `ciscoasa(config)# write memory`	지속형 플래시 메모리에 RSA 키를 저장합니다.
3단계	**aaa authentication ssh console LOCAL**	SSH 액세스를 위한 로컬 인증을 활성화합니다. 혹은 AAA 서버를 사용하여 인증을 구성할 수도 있습니다. 자세한 내용은 35-17 페이지의 CLI 및ASDM, 액세스를 위한 인증 구성을 참조하십시오.
4단계	**username** *username* **password** *password*	SSH 액세스에 사용할 수 있는 사용자를 로컬 데이터베이스에 만듭니다.
5단계	**ssh** *source_IP_address mask source_interface* **예:** `ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside`	각 주소 또는 서브넷에 대해 ASA에서 어떤 IP 주소로부터의 연결을 허용할지 확인하고 SSH 가능한 인터페이스도 확인합니다. 텔넷과 달리 SSH는 가장 낮은 보안 레벨 인터페이스에서 가능합니다.

	명령	목적
6단계	**ssh timeout** *minutes* 예: ciscoasa(config)# ssh timeout 30	(선택 사항)ASA에서 세션 연결을 끊기 전에 얼마 동안 SSH 세션을 유휴 상태로 유지할 수 있는지 설정합니다. 1분~60분 범위에서 시간 초과를 설정합니다. 기본값은 5분입니다. 이 기본값은 대개의 경우 너무 짧으므로 모든 프로덕션 전 단계 테스트 및 문제 해결을 완료할 수 있도록 늘려야 합니다.
7단계	**ssh version** *version_number* 예: ciscoasa(config)# ssh version 2	(선택 사항) SSH 버전 1 또는 2로 액세스를 제한합니다. 기본적으로 SSH는 버전 1과 2 모두 허용합니다.

예

다음 예는 RSA 키를 생성하는 방법 및 주소가 192.168.1.2인 내부 인터페이스의 호스트가 ASA에 액세스하도록 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# aaa authentication ssh console LOCAL
WARNING: local database is empty! Use 'username' command to define local users.
ciscoasa(config)# username exampleuser1 password examplepassword1
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
ciscoasa(config)# ssh timeout 30
```

다음 예는 내부 인터페이스에서 192.168.3.0/24 네트워크의 모든 사용자가 ASA에 액세스하도록 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

SSH 클라이언트 사용

관리 호스트의 SSH 클라이언트에 35-4 페이지의 SSH 액세스 구성에서 구성했던 사용자 이름과 비밀번호를 입력합니다. SSH 세션을 시작하면 ASA 콘솔에 점(.)이 표시되고 다음 SSH 사용자 인증 프롬프트가 나타납니다.

```
ciscoasa(config)#.
```

점이 표시되더라도 SSH의 기능에 영향을 주지 않습니다. 점은 서버 키를 생성할 때 또는 사용자 인증에 앞서 SSH 키 교환 과정에서 개인 키를 사용하여 메시지를 해독할 때 콘솔에 나타납니다. 이 작업은 최대 2분 이상 걸릴 수 있습니다. 점은 ASA가 작업 중이고 멈춘 상태가 아님을 알리는 일종의 진행 표시입니다.

비밀번호를 사용하지 않고 그 대신 공개 키를 구성할 수도 있습니다. 27-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가를 참조하십시오.

ASDM를 위한 HTTPS 액세스 구성

ASDM를 사용하려면 HTTPS 서버를 활성화하고 ASA와의 HTTPS 연결을 허용해야 합니다. HTTPS 액세스는 공장 기본 컨피그레이션에서 활성화되거나 **setup** 명령을 통해 활성화됩니다. 이 섹션에서는 ASDM 액세스를 직접 구성하는 방법을 설명합니다.

세부 단계

	명령	목적
1단계	**http** *source_IP_address mask source_interface* 예: `ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside`	각 주소 또는 서브넷에 대하여 ASA에서 어떤 IP 주소로부터의 HTTPS 연결을 허용할지 지정합니다.
2단계	**http server enable** [*port*] 예: `ciscoasa(config)# http server enable 443`	HTTPS 서버를 활성화합니다. 기본적으로 *port*는 443입니다. 포트 번호를 변경한 경우 ASDM 액세스 URL에 포함해야 합니다. 예를 들어, 포트 번호를 444로 변경한 경우 다음과 같이 입력합니다. **https://10.1.1.1:444**
3단계	**http redirect** *interface* [*port*] 예: `ciscoasa(config)# http redirect inside`	(선택 사항) HTTP 요청을 HTTPS 요청으로 리디렉션합니다. 그러면 사용자가 ASDM URL에 "http://"를 입력하더라도 오류 없이 htttps URL로 이동합니다.

예

다음 예는 HTTPS 서버를 활성화하는 방법 및 주소가 192.168.1.2인 내부 인터페이스의 호스트가 ASDM에 액세스하도록 허용하는 방법을 보여줍니다.

```
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 보여줍니다.

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

CLI 매개 변수 구성

CLI 매개 변수를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

로그인 배너 구성

사용자가 ASA에 연결할 때 사용자 로그인 전에 또는 사용자가 특별 권한 EXEC 모드를 시작하기 전에 표시할 메시지를 구성할 수 있습니다.

제한 사항

배너가 추가된 다음 ASA와의 텔넷 또는 SSH 세션이 종료될 때가 있습니다.

- 배너 메시지를 처리하기에는 시스템 메모리가 충분하지 않을 경우
- 배너 메시지를 표시하려 할 때 TCP 쓰기 오류가 발생한 경우

지침

- 보안의 관점에서는 배너에서 무단 액세스를 방지하는 것이 중요합니다. "welcome" 또는 "please"와 같은 문구는 침입자를 불러들이는 것 같으므로 사용하지 마십시오. 다음과 같은 배너로 무단 액세스에 대해 적절한 어조를 유지할 수 있습니다.

  ```
  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.
  ```

- 배너 메시지에 대한 자세한 내용은 RFC 2196을 참조하십시오.

로그인 배너를 구성하려면 다음 단계를 수행합니다.

세부 단계

명령	목적
banner {**exec** | **login** | **motd**} *text* **예:** `ciscoasa(config)# banner motd Welcome to $(hostname).`	사용자가 처음 연결할 때(message-of-the-day (**motd**)), 사용자가 로그인할 때(**login**), 사용자가 특별 권한 EXEC 모드에 액세스할 때(**exec**)의 3가지 경우 중 하나에 표시할 배너를 추가합니다. 사용자가 ASA에 연결할 때 message-of-the-day 배너가 먼저 표시되고 뒤이어 로그인 배너와 프롬프트가 나타납니다. 사용자가 ASA에 성공적으로 로그인하면 EXEC 배너가 나타납니다. 두 라인 이상 추가하려면 각 라인의 앞에 **banner** 명령을 넣습니다. 배너 텍스트: • CLI에서 공백은 허용되지만 탭은 입력할 수 없습니다. • RAM 및 플래시 메모리에 대한 제한을 제외하면 배너 길이에 대한 제한은 없습니다. • 문자열 **$(hostname)**과 **$(domain)**을 넣어 ASA의 호스트 이름 또는 도메인 이름을 동적으로 추가할 수 있습니다. • 시스템 컨피그레이션에서 배너를 구성한 경우, 컨텍스트 컨피그레이션에서 **$(system)** 문자열을 사용하여 컨텍스트 내에 배너 텍스트를 사용할 수 있습니다.

예

다음 예는 message-of-the-day 배너를 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# banner motd Welcome to $(hostname).
ciscoasa(config)# banner motd Contact me at admin@example.com for any
ciscoasa(config)# banner motd issues.
```

CLI 프롬프트 사용자 지정

CLI 프롬프트 창에서는 CLI 세션에 사용되는 프롬프트를 사용자 지정할 수 있습니다. 기본적으로 프롬프트는 ASA의 호스트 이름을 표시합니다. 다중 컨텍스트 모드에서는 프롬프트가 컨텍스트 이름도 표시합니다. CLI 프롬프트에서 다음 항목을 표시할 수 있습니다.

cluster-unit	(단일 모드 및 다중 모드) 클러스터 유닛 이름을 표시합니다. 클러스터의 각 유닛은 고유한 이름을 가질 수 있습니다.
context	(다중 모드만) 현재 컨텍스트의 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 상태를 표시합니다. 상태에 대해 표시되는 값은 다음과 같습니다. • act—장애 조치가 활성화되었으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • stby—장애 조치가 활성화되었으며, 해당 유닛은 트래픽을 전달하는 중이 아니고 대기, 실패 또는 그 밖의 비활성 상태에 있습니다. • actNoFailover—장애 조치가 활성화되지 않았으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • stbyNoFailover—장애 조치가 활성화되지 않았고, 해당 유닛은 트래픽을 전달하는 중이 아닙니다. 대기 유닛의 임계값을 초과하는 인터페이스 오류가 있을 경우 이러한 조건이 발생할 수 있습니다. 클러스터에서 유닛의 역할(마스터 또는 슬레이브)을 표시합니다. 예를 들어, 프롬프트 ciscoasa/cl2/slave에서 호스트 이름은 ciscoasa, 유닛 이름은 cl2, 상태 이름은 slave입니다.

세부 단계

CLI 프롬프트를 사용자 지정하려면 다음 명령을 입력합니다.

명령	목적
prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]} 예: `ciscoasa(config)# firewall transparent`	CLI 프롬프트를 사용자 지정합니다.

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 초과가 없습니다. 이 설정은 사용자가 얼마나 오랫동안 콘솔 포트와의 연결 상태를 유지할 수 있는가에 영향을 주지 않습니다. 이 연결 상태는 시간 초과가 없습니다.

콘솔 시간 초과를 변경하려면 다음 단계를 수행합니다.

세부 단계

명령	목적
console timeout *number* 예: `ciscoasa(config)# console timeout 0`	특별 권한 세션이 끝난 이후의 유휴 시간(분, 0~60)을 지정합니다. 기본 시간 초과는 0입니다. 즉 세션에 시간 초과가 없습니다.

VPN 터널을 통한 관리 액세스 구성

VPN 터널이 어떤 인터페이스에서 종료했지만 다른 인터페이스에 액세스하여 ASA를 관리하려는 경우, 그 인터페이스를 관리 액세스 인터페이스로 지정할 수 있습니다. 예를 들어, 외부 인터페이스에서 ASA에 들어올 경우 이 기능은 ASDM, SSH, Telnet 또는 SNMP를 사용하여 내부 인터페이스에 연결할 수 있게 합니다. 또는 외부 인터페이스에서 들어올 때 내부 인터페이스를 ping할 수 있습니다. 관리 액세스는 IPsec 클라이언트, IPsec 사이트 대 사이트(site-to-site), AnyConnect SSL VPN 클라이언트의 VPN 터널 유형을 통해 사용할 수 있습니다.

- 35-10 페이지의 관리 인터페이스를 위한 라이센싱 요구 사항
- 35-2 페이지의 지침 및 제한 사항
- 35-11 페이지의 관리 인터페이스 구성

관리 인터페이스를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 모드에서 지원합니다.

방화벽 모드 지침

라우티드 모드에서 지원합니다.

IPv6 지침

IPv6를 지원합니다.

추가 지침

관리 액세스 인터페이스를 하나만 정의할 수 있습니다.

참고 후속 컨피그레이션에서는 192.168.10.0/24가 AnyConnect 또는 IPsec VPN 클라이언트를 위한 VPN 풀입니다. 각 컨피그레이션에서는 VPN 클라이언트 사용자가 관리 인터페이스 IP 주소를 사용하여 ASDM에 연결하거나 ASA에 SSH 연결하는 것을 허용합니다.

VPN 클라이언트 사용자만 ASDM 또는 HTTP에 액세스하게 하려면(다른 모든 사용자의 액세스 거부) 다음 명령을 입력합니다.

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface
```

VPN 클라이언트 사용자만 SSH를 사용하여 ASA에 액세스하게 하려면(다른 모든 사용자의 액세스 거부) 다음 명령을 입력합니다.

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

관리 인터페이스 구성

관리 인터페이스를 구성하려면 다음 단계를 수행합니다.

세부 단계

명령	목적
management-access *management_interface* 예: `ciscoasa(config)# management-access inside`	*management_interface*는 다른 인터페이스에서 ASA에 들어올 때 액세스하려는 관리 인터페이스의 이름을 지정합니다.

시스템 관리자를 위한 AAA 구성

이 섹션에서는 시스템 관리자를 위해 인증 및 명령 권한 부여를 활성화하는 방법을 설명합니다.

시스템 관리자를 위한 AAA에 대한 정보

이 섹션에서는 시스템 관리자를 위해 AAA에 대해 설명합니다.

관리 인증에 대한 정보

이 섹션에서는 관리 액세스를 위한 인증에 대해 설명합니다.

인증 있는 CLI 액세스와 인증 없는 CLI 액세스 비교

ASA에 로그인하는 방법은 인증을 활성화했는지에 따라 달라집니다.

- 인증 없음—텔넷에 대해 어떤 인증도 활성화하지 않을 경우 사용자 이름을 입력하지 않습니다. 로그인 비밀번호(**password** 명령으로 설정)를 입력합니다. SSH는 인증 없이 사용 불가합니다. 사용자 EXEC 모드에 액세스합니다.
- 인증—이 섹션에 따라 텔넷 또는 SSH 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. 사용자 EXEC 모드에 액세스합니다.

로그인한 다음 특별 권한 EXEC 모드를 시작하려면 **enable** 명령을 입력합니다. **enable**의 작동 방식은 인증을 활성화했는지에 따라 달라집니다.

- 인증 없음—enable 인증을 구성하지 않은 경우, **enable** 명령을 입력할 때 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 아닙니다. 사용자 이름을 유지하려면 enable 인증을 사용합니다.
- 인증—enable 인증을 구성한 경우(35-18 페이지의 특별 권한 EXEC 모드에 액세스하기 위한 인증 구성(enable 명령) 참조), ASA에서는 사용자 이름과 비밀번호를 다시 묻습니다. 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**은 사용자 이름을 유지하지만, 인증을 실행하는 데 어떤 컨피그레이션도 필요하지 않습니다. 자세한 내용은 35-18 페이지의 login 명령을 사용하는 사용자 인증을 참조하십시오.

인증 있는 ASDM 액세스와 인증 없는 CLI 액세스 비교

기본적으로 빈 사용자 이름과 **enable password** 명령을 통해 설정된 enable 비밀번호를 사용하여 ASDM에 로그인할 수 있습니다. 로그인 화면에서 (사용자 이름을 비워 두지 않고) 사용자 이름과 비밀번호를 입력한 경우 ASDM은 로컬 데이터베이스에 일치하는 항목이 있는지 확인합니다.

HTTP 인증을 구성하면 더 이상 빈 사용자 이름과 enable 비밀번호로 ASDM을 사용할 수 없게 됩니다.

스위치에서 ASA Services Module로의 세션 인증

스위치에서 ASASM에 연결하는 세션(**session** 명령 사용)을 위해 텔넷 인증을 구성할 수 있습니다. 스위치에서 ASASM로의 가상 콘솔 연결(**service-module session** 명령 사용)에는 시리얼 포트 인증을 구성할 수 있습니다.

다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 어떤 AAA 명령도 구성할 수 없습니다. 그러나 관리 컨텍스트에서 텔넷 또는 시리얼 인증을 구성한 경우, 스위치에서 ASASM로의 세션에도 인증이 적용됩니다. 이 경우에는 관리 컨텍스트 AAA 서버 또는 로컬 사용자 데이터베이스가 사용됩니다.

명령 권한 부여에 대한 정보

이 섹션에서는 명령 권한 부여에 대해 설명합니다.

- 35-13 페이지의 지원되는 명령 권한 부여 방식
- 35-13 페이지의 사용자 자격 증명 유지에 대한 정보
- 35-14 페이지의 보안 컨텍스트 및 명령 권한 부여

지원되는 명령 권한 부여 방식

다음 2가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 레벨—ASA에서 명령 권한 레벨을 구성합니다. 로컬, RADIUS 또는 LDAP(LDAP 특성을 RADIUS 특성에 매핑한 경우) 사용자가 CLI 액세스를 위해 인증할 경우, ASA에서는 로컬 데이터베이스, RADIUS 또는 LDAP 서버에 의해 정의된 권한 레벨을 사용자에게 부여합니다. 사용자는 부여받은 권한 레벨 이하의 명령에 액세스할 수 있습니다. 모든 사용자가 처음 로그인할 때는 사용자 EXEC 모드에 액세스합니다(레벨 0 또는 1의 명령). 사용자는 **enable** 명령을 사용하여 다시 인증해야 특별 권한 EXEC 모드(레벨 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 만들 수 있습니다. 즉 **enable** *n*(2~15)을 입력하면 ASA에서는 레벨 *n*을 부여합니다. 이러한 레벨은 로컬 명령 권한 부여를 활성화한 경우에만 사용됩니다(35-24 페이지의 로컬 명령 권한 부여 구성 참조). 명령 참조에서 **enable** 명령에 대해 자세히 알아볼 수 있습니다.

- TACACS+ 서버 권한 레벨—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.

사용자 자격 증명 유지에 대한 정보

사용자가 ASA에 로그인할 때 사용자는 인증을 위한 사용자 이름과 비밀번호를 제공해야 합니다. ASA에서는 세션에서 나중에 추가적인 인증이 필요할 경우에 대비하여 이 세션 자격 증명을 보존합니다.

다음 컨피그레이션이 있으면 사용자는 로컬 서버와의 인증만으로 로그인할 수 있습니다. 이후의 시리얼 권한 부여에서는 저장된 자격 증명을 사용합니다. 또한 사용자는 권한 레벨 15의 비밀번호를 입력해야 합니다. 특별 권한 모드를 종료할 때 사용자가 다시 인증됩니다. 특별 권한 모드에서는 사용자 자격 증명이 보존되지 않습니다.

- 로컬 서버가 사용자 액세스를 인증하도록 구성되었습니다.

- 권한 레벨 15 명령 액세스가 비밀번호가 필요하도록 구성되었습니다.
- 사용자 어카운트에서 (콘솔 또는 ASDM에 대한 액세스 없이) 시리얼 전용 권한 부여가 구성되었습니다.
- 사용자 어카운트에서 권한 레벨 15 명령 액세스가 구성되었습니다.

다음 표는 이러한 경우에 ASA에서 어떻게 자격 증명을 사용하는지 보여줍니다.

필요한 자격 증명	사용자 이름 및 비밀번호 인증	시리얼 권한 부여	특별 권한 모드의 명령 권한 부여	특별 권한 모드의 종료 권한 부여
Username	예	아니요	아니요	예
비밀번호	예	아니요	아니요	예
특별 권한 모드 비밀번호	아니요	아니요	예	아니요

보안 컨텍스트 및 명령 권한 부여

다음은 다중 보안 컨텍스트로 명령 권한 부여를 구현할 때 중요하게 고려할 사항입니다.

- AAA 설정은 컨텍스트끼리 공유하지 않고 컨텍스트마다 다릅니다.

  명령 권한 부여를 구성할 때 각 보안 컨텍스트를 따로 구성해야 합니다. 이러한 컨피그레이션에서는 여러 보안 컨텍스트에서 각기 다른 명령 권한 부여를 적용하는 것이 가능합니다.

  보안 컨텍스트 간 전환에서 관리자는 로그인 시 지정된 사용자 이름에 대해 허용된 명령이 새 컨텍스트 세션에서는 다를 수 있음을 또는 새 컨텍스트에서는 명령 권한 부여가 아예 구성되지 않았을 수도 있음을 알고 있어야 합니다. 명령 권한 부여가 보안 컨텍스트마다 다를 수 있음을 모르는 관리자는 혼란스러워 할 수도 있습니다. 이는 다음 사항 때문에 더욱 복잡해집니다.

- **changeto** 명령으로 시작한 새 컨텍스트 세션은 항상 기본 enable_15 사용자 이름을 관리자 ID로 사용합니다. 이전 컨텍스트 세션에서 어떤 사용자 이름을 사용했는가는 상관없습니다. 따라서 enable_15 사용자에 대해 명령 권한 부여가 구성되지 않은 경우 또는 enable_15 사용자에 대한 권한 부여가 이전 컨텍스트 세션 사용자에 대한 권한 부여와 다를 경우 혼란이 일어날 수 있습니다.

  이러한 동작은 명령 어카운팅에도 영향을 줍니다. 명령 어카운팅은 실행된 각 명령을 특정 관리자와 정확하게 연결할 수 있는 경우에만 유용합니다. **changeto** 명령을 사용할 권한이 있는 모든 관리자는 다른 컨텍스트에서 enable_15 사용자 이름을 사용할 수 있으므로 명령 어카운팅 레코드에서 누가 enable_15 사용자 이름으로 로그인했는지 즉시 식별하기 어렵습니다. 컨텍스트마다 다른 어카운팅 서버를 사용하는 경우, 누가 enable_15 사용자 이름을 사용하고 있었는지 추적하려면 여러 서버의 데이터를 연계하여 파악해야 합니다.

  명령 권한 부여를 구성할 때 다음 사항을 고려하십시오.

  - **changeto** 명령을 사용할 권한이 있는 관리자는 enable_15 사용자에게 허용된 모든 명령을 사실상 다른 모든 컨텍스트에서 사용할 수 있습니다.
  - 명령 권한 부여를 컨텍스트마다 다르게 하려는 경우, 각 컨텍스트에서 enable_15 사용자 이름에게 허용되지 않은 명령은 **changeto** 명령 사용 권한을 가진 관리자에게도 거부되어야 합니다.

  다른 보안 컨텍스트로 전환할 때 관리자는 특별 권한 EXEC 모드를 종료하고 **enable** 명령을 다시 입력하여 필요한 사용자 이름을 사용할 수 있습니다.

참고 시스템 실행 영역에서는 AAA 명령을 지원하지 않습니다. 따라서 시스템 실행 영역에서는 명령 권한 부여를 사용할 수 없습니다.

시스템 관리자를 위한 AAA의 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

전제 조건

AAA 서버 또는 로컬 데이터베이스의 전제 조건

AAA 서버 또는 로컬 데이터베이스에서 사용자를 구성해야 합니다. AAA 서버의 경우 ASA에서 이 서버와 통신하도록 구성하는 작업도 필요합니다. 다음 장을 참조하십시오.

- AAA 서버— 해당 AAA 서버 유형에 대한 장을 참조하십시오.
- 로컬 데이터베이스— 27-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가를 참조하십시오.

관리 인증의 전제 조건

ASA에서 텔넷, SSH 또는 HTTP 사용자를 인증하려면 먼저 ASA와의 통신이 허용되는 IP 주소를 확인해야 합니다. ASASM의 경우, 다중 컨텍스트 모드의 시스템 액세스는 예외입니다. 스위치에서 ASASM에 연결하는 세션은 텔넷 세션이지만, 텔넷 액세스 컨피그레이션은 필요하지 않습니다. 자세한 내용은 35-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성을 참조하십시오.

로컬 명령 권한 부여의 전제 조건

- **enable** 인증을 구성합니다. 35-17 페이지의 CLI 및ASDM, 액세스를 위한 인증 구성을 참조하십시오.

  enable 인증은 사용자가 **enable** 명령에 액세스한 다음 사용자 이름을 유지하려면 필요합니다.

  또는 컨피그레이션이 필요 없는 **login** 명령을 사용할 수도 있습니다. 이는 인증과 관련해서는 **enable** 명령과 동일한 기능을 하지만, 로컬 데이터베이스에서만 가능합니다. 이 옵션은 **enable** 인증만큼 안전하지 않으므로 이 옵션은 권장하지 않습니다.

  CLI 인증을 사용할 수도 있지만, 필수는 아닙니다.
- 사용자 유형별로 다음 전제 조건을 확인하십시오.
  - 로컬 데이터베이스 사용자—0~15의 권한 레벨로 로컬 데이터베이스의 각 사용자를 구성합니다.
  - RADIUS 사용자—값이 0~15인 Cisco VSA CVPN3000-Privilege-Level로 사용자를 구성합니다.
  - LDAP 사용자—0~15의 권한 레벨로 사용자를 구성한 다음 30-5 페이지의 LDAP 특성 맵 구성에 따라 LDAP 특성을 Cisco VSA CVPN3000-Privilege-Level에 매핑합니다.

TACACS+ 명령 권한 부여의 전제 조건

- CLI 인증을 구성합니다(35-17 페이지의 CLI 및ASDM, 액세스를 위한 인증 구성 참조).
- **enable** 인증을 구성합니다(35-18 페이지의 특별 권한 EXEC 모드에 액세스하기 위한 인증 구성(enable 명령) 참조).

관리 어카운팅의 전제 조건

- CLI 인증을 구성합니다(35-17 페이지의 CLI 및ASDM, 액세스를 위한 인증 구성 참조).
- **enable** 인증을 구성합니다(35-18 페이지의 특별 권한 EXEC 모드에 액세스하기 위한 인증 구성(enable 명령) 참조).

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

기본 설정

기본 명령 권한 레벨

기본적으로 다음 명령이 권한 레벨 0에 지정됩니다. 다른 모든 명령은 권한 레벨 15에 지정됩니다.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

어떤 컨피그레이션 모드 명령을 15보다 낮은 레벨로 이동한 경우, 그 **configure** 명령도 그 레벨로 이동해야 합니다. 그러지 않으면 사용자가 컨피그레이션 모드를 시작할 수 없게 됩니다.

모든 권한 레벨을 보려면 35-26 페이지의 로컬 명령 권한 레벨 보기를 참조하십시오.

CLI 및ASDM, 액세스를 위한 인증 구성

CLI, ASDM, enable 명령 액세스를 위한 인증이 필요할 수 있습니다.

전제 조건

- 35-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성에 따라 텔넷, SSH 또는 HTTP 액세스를 구성합니다.
- SSH 액세스의 경우 SSH 인증을 구성해야 합니다. 기본 사용자 이름이 없습니다.

세부 단계

	명령	목적
1단계	**aaa authentication** {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]} 예: `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`	관리 액세스를 위해 사용자를 인증합니다. **telnet** 키워드가 텔넷 액세스를 제어합니다. ASASM에서는 이 키워드가 **session** 명령을 사용하는 스위치로부터의 세션에도 영향을 줍니다. 다중 모드 액세스는 35-13 페이지의 스위치에서 ASA Services Module로의 세션 인증을 참조하십시오. **ssh** 키워드는 SSH 액세스를 제어합니다. **http** 키워드는 ASDM 액세스를 제어합니다. **serial** 키워드는 콘솔 포트 액세스를 제어합니다. ASASM에서는 이 키워드가 **service-module session** 명령을 사용하여 스위치로부터 액세스하는 가상 콘솔에 영향을 줍니다. 다중 모드 액세스는 35-13 페이지의 스위치에서 ASA Services Module로의 세션 인증을 참조하십시오. HTTP 관리 인증에서는 AAA 서버 그룹에 대해 SDI 프로토콜을 지원하지 않습니다. 인증에 AAA 서버 그룹을 사용하는 경우, AAA 서버를 사용할 수 없을 때 로컬 데이터베이스를 대신 사용하도록 ASA를 구성할 수 있습니다. **LOCAL** 다음에 서버 그룹 이름을 지정합니다(**LOCAL**은 대/소문자 구분). 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다. **LOCAL**만 입력하여 (대체 방법 없이) 로컬 데이터베이스를 기본 인증 방법으로 사용할 수도 있습니다.
2단계	**http authentication-certificate** *interface* 예: `http authentication-certificate inside`	지정된 인터페이스에서 HTTP를 통해 연결하는 ASDM 클라이언트로부터의 인증서가 필요합니다. 이 명령은 ASDM의 **aaa authentication** 명령에 추가하여 사용할 수 있습니다. 이 명령은 ASDM 액세스 전용입니다. 그 밖의 SSL 트래픽(예: 컷스루 프록시)에 인증서가 필요하게 하려면 **ssl certificate-authentication** 명령을 사용합니다.

특별 권한 EXEC 모드에 액세스하기 위한 인증 구성(enable 명령)

사용자가 **enable** 명령을 입력할 때 ASA에서 AAA 서버 또는 로컬 데이터베이스를 사용하여 사용자를 인증하도록 구성할 수 있습니다. 또는 사용자가 **login** 명령을 입력하면 자동으로 로컬 데이터베이스를 사용하여 인증이 이루어집니다. 그러면 로컬 데이터베이스에서 사용자의 레벨에 따라 특별 권한 EXEC 모드에도 액세스합니다.

- 35-18 페이지의 enable 명령을 위한 인증 구성
- 35-18 페이지의 login 명령을 사용하는 사용자 인증

enable 명령을 위한 인증 구성

사용자가 **enable** 명령을 입력할 때 사용자를 인증하도록 ASA를 구성할 수 있습니다. 자세한 내용은 35-12 페이지의 인증 있는 CLI 액세스와 인증 없는 CLI 액세스 비교를 참조하십시오.

enable 명령을 입력하는 사용자를 인증하려면 다음 명령을 입력합니다.

명령	목적
aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]} **예:** `ciscoasa(config)# aaa authentication enable console LOCAL`	**enable** 명령을 입력하는 사용자를 인증합니다. 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** 다음에 서버 그룹 이름을 지정합니다(**LOCAL**은 대/소문자 구분). 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다. **LOCAL**만 입력하여 (대체 방법 없이) 로컬 데이터베이스를 기본 인증 방법으로 사용할 수도 있습니다.

login 명령을 사용하는 사용자 인증

사용자 EXEC 모드에서 **login** 명령을 사용하면 로컬 데이터베이스에 있는 어떤 사용자 이름으로도 로그인할 수 있습니다.

이 기능은 사용자가 자신의 사용자 이름과 비밀번호로 로그인하여 특별 권한 EXEC 모드에 액세스할 수 있게 합니다. 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 레벨을 2(기본값)~15로 설정합니다. 로컬 명령 권한 부여를 구성한 경우, 사용자는 해당 권한 레벨 이하에 지정된 명령만 입력할 수 있습니다. 자세한 내용은 35-24 페이지의 로컬 명령 권한 부여 구성을 참조하십시오.

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 레벨이 2 이상(2가 기본값)인 사용자는 CLI에서 각자의 비밀번호를 사용하여 특별 권한 EXEC 모드(및 모든 명령)에 액세스할 수 있습니다. 또는 인증에 AAA 서버를 사용할 수 있습니다. 혹은 모든 로컬 사용자를 레벨 1로 설정해 놓고 누가 시스템 enable 비밀번호를 사용하여 특별 권한 EXEC 모드에 액세스할 수 있는가를 제어하는 방법도 있습니다.

로컬 데이터베이스의 사용자로 로그인하려면 다음 명령을 입력합니다.

명령	목적
login 예: ciscoasa# **login**	로컬 데이터베이스의 사용자로 로그인합니다. ASA에서는 사용자 이름과 비밀번호를 묻습니다. 비밀번호를 입력하면 ASA에서는 로컬 데이터베이스에 지정된 권한 레벨을 부여합니다.

관리 권한 부여로 사용자 CLI 및 ASDM 액세스 제한

ASA에서는 사용자가 RADIUS, LDAP, TACACS+ 또는 로컬 사용자 데이터베이스를 사용하여 인증할 때 관리 사용자와 원격 액세스 사용자를 구분할 수 있습니다. 사용자 역할 차별화를 통해 원격 액세스 VPN 및 네트워크 액세스 사용자가 ASA와의 관리 연결을 설정하는 것을 방지할 수 있습니다.

참고 시리얼 액세스는 관리 권한 부여에 포함되지 않습니다. 따라서 **aaa authentication serial console**명령을 구성한 경우 인증하는 모든 사용자가 콘솔 포트에 액세스할 수 있습니다.

세부 단계

1단계 로컬, RADIUS, LDAP(매핑됨), TACACS+ 사용자에 대한 관리 권한 부여를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# aaa authorization exec {authentication-server | LOCAL} [auto-enable]
```

LOCAL 옵션이 구성되었으면, 로컬 사용자 데이터베이스가 입력된 사용자 이름, 지정된 Service-Type 및 Privilege-Level 특성의 소스가 됩니다.

이 옵션을 선택하면 RADIUS의 관리 사용자 권한 레벨도 지원할 수 있는데, 이는 로컬 명령 레벨과 함께 명령 권한 부여에 사용할 수 있습니다. 자세한 내용은 35-24 페이지의 로컬 명령 권한 부여 구성을 참조하십시오.

authentication-server 옵션이 구성된 경우, 동일한 서버가 인증과 권한 부여에 사용됩니다.

auto-enable 옵션은 로그인 인증 서버에서 충분한 권한을 가진 사용자가 곧바로 특별 권한 EXEC 모드에 들어가는 것을 허용합니다. 그렇지 않은 사용자는 사용자 EXEC 모드가 됩니다. 이러한 권한은 각 EXEC 모드에 들어가는 데 필요한 Service-Type 및 Privilege-Level 특성에 의해 결정됩니다. 특별 권한 EXEC 모드를 시작하려면 사용자에게 지정된 Service-Type 특성이 Administrative이고 Privilege Level 특성이 1보다 커야 합니다.

이 옵션은 시스템 컨텍스트에서는 지원되지 않습니다. 그러나 관리 컨텍스트에서 텔넷 또는 시리얼 인증을 구성한 경우, 스위치에서 ASASM로의 세션에도 인증이 적용됩니다.

aaa authorization exec 명령만 입력하면 아무런 효과가 없습니다.

관리 권한 부여에 시리얼 인증을 사용할 때는 **auto-enable** 옵션이 포함되지 않습니다.

aaa authentication http 명령은 **auto-enable** 옵션의 영향을 받지 않습니다.

auto-enable 옵션을 구성하기 전에 두 프로토콜 로그인을 구성하고 인증을 활성화하는 것이 좋습니다. 그리고 다음 예와 같이 모든 인증 요청이 동일한 AAA 서버 그룹으로 전달되는 것이 좋습니다.

```
ciscoasa (config)# aaa authentication ssh console RADIUS
ciscoasa (config)# aaa authentication enable console RADIUS
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

다른 유형의 컨피그레이션을 사용하는 것은 권장되지 *않습니다*.

2단계 관리 권한 부여를 위해 사용자를 구성하려면 각 AAA 서버 유형 또는 로컬 사용자에 대한 다음 요구 사항을 확인하십시오.

RADIUS 또는 LDAP(매핑됨) 사용자

사용자가 LDAP을 통해 인증되면 기본 LDAP 특성과 그 값이 Cisco ASA 특성에 매핑되어 특정 권한 부여 기능을 제공할 수 있습니다. Cisco VSA CVPN3000-Privilege-Level을 0~15의 값으로 구성합니다. 그리고 **ldap map-attributes** 명령을 사용하여 LDAP 특성을 Cisco VAS CVPN3000-Privilege-Level에 매핑합니다. 자세한 내용은 30-5 페이지의 LDAP 특성 맵 구성을 참조하십시오.

RADIUS IETF **service-type** 특성은, RADIUS 인증 및 권한 부여 요청의 결과인 access-accept 메시지를 통해 전송될 때, 어떤 서비스 유형이 인증된 사용자에게 허가될지 지정하는 데 쓰입니다.

- Service-Type 6 (Administrative)— **aaa authentication console** 명령에 의해 지정되는 임의의 서비스에 대한 전체 액세스를 허용합니다.
- Service-Type 7 (NAS prompt)— **aaa authentication {telnet | ssh} console** 명령을 구성할 때 CLI에 대한 액세스를 허용합니다. 그러나 **aaa authentication http console** 명령을 구성한 경우에는 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **enable** 인증을 구성하는 데 **aaa authentication enable console** 명령을 사용한 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다. Framed (2) 서비스 유형과 Login (1) 서비스 유형은 동일하게 처리됩니다.
- Service-Type 5 (Outbound)—관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령에 의해 지정되는 임의의 서비스를 사용할 수 없습니다(**serial** 키워드 제외, 시리얼 액세스는 허용됨). 원격 액세스(IPsec 및 SSL) 사용자는 여전히 원격 액세스 세션을 인증하고 종료할 수 있습니다. 그 밖의 모든 서비스 유형(Voice, FAX 등)은 동일하게 처리됩니다.

RADIUS Cisco VSA **privilege-level** 특성(Vendor ID 3076, sub-ID 220)은, access-accept 메시지를 통해 전송될 때, 사용자의 권한 레벨을 지정하는 데 쓰입니다.

인증된 사용자가 ASDM, SSH 또는 텔넷을 통해 ASA에 대한 관리 액세스를 시도하지만 그에 적합한 권한 레벨이 아닐 경우, ASA에서는 syslog 메시지 113021을 생성합니다. 이 메시지는 부적합한 관리 권한 때문에 로그인 시도가 실패했음을 사용자에게 알립니다.

다음 예는 LDAP 특성 맵을 정의하는 방법을 보여줍니다. 이 예에서는 LDAP을 통해 인증되는 사용자는 사용자 레코드 필드 또는 title 및 company 매개 변수를 각각 IETF-RADIUS service-type 및 privilege-level에 매핑하도록 보안 정책에서 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 Privilege-Level
```

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
```

TACACS+ 사용자

"service=shell"로 권한 부여가 요청되고, 서버는 PASS 또는 FAIL로 응답합니다.

- PASS, 권한 레벨 1—컨피그레이션 및 모니터링 섹션에 대한 제한적인 읽기 전용 액세스 그리고 권한 레벨이 1인 **show** 명령을 위한 액세스로 ASDM에 대한 액세스를 허용합니다.
- PASS, 권한 레벨 2 이상— **aaa authentication {telnet | ssh} console** 명령을 구성할 때 CLI에 대한 액세스를 허용합니다. 그러나 **aaa authentication http console** 명령을 구성한 경우에는 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **enable** 인증을 구성하는 데 **aaa authentication enable console** 명령을 사용한 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다. enable 권한 레벨이 14 이하로 설정된 경우 **enable** 명령을 사용하여 특별 권한 EXEC 명령에 액세스할 수 없습니다.

- FAIL—관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령에 의해 지정되는 임의의 서비스를 사용할 수 없습니다(**serial** 키워드 제외, 시리얼 액세스는 허용됨).

로컬 사용자

어떤 사용자 이름에 대한 **service-type** 명령을 설정합니다. **service-type**의 기본값은 **admin**입니다. 이는 **aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다. 자세한 내용은 27-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가를 참조하십시오.

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.

- 35-21 페이지의 비밀번호 정책 구성
- 35-23 페이지의 비밀번호 변경

비밀번호 정책 구성

비밀번호 정책을 구성한 다음 (본인의 또는 다른 사용자의) 비밀번호를 변경할 때 비밀번호 정책이 새 비밀번호에 적용됩니다. 기존 비밀번호는 적용 대상에서 제외됩니다. 새 정책은 **username** 명령 및 **change-password** 명령을 사용하여 비밀번호를 변경하는 경우에 적용됩니다.

전제 조건

- 35-17 페이지의 CLI 및ASDM, 액세스를 위한 인증 구성에 따라 CLI/ASDM 인증을 구성합니다. 로컬 데이터베이스를 지정해야 합니다.
- 35-18 페이지의 특별 권한 EXEC 모드에 액세스하기 위한 인증 구성(enable 명령)에 따라 enable 인증을 구성합니다. 로컬 데이터베이스를 지정해야 합니다.

세부 단계

	명령	목적
1단계	**password-policy lifetime** *days* 예: ciscoasa(config)# password-policy lifetime 180	(선택 사항) 원격 사용자(SSH, 텔넷, HTTP)의 비밀번호가 만료될 때까지의 기한(일)을 설정합니다. 콘솔 포트의 사용자는 비밀번호 만료로 인해 잠기는 일이 없습니다. 유효한 값의 범위는 0일~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.
2단계	**password-policy minimum-changes** *value* 예: ciscoasa(config)# password-policy minimum-changes 2	(선택 사항) 새 비밀번호에서 기존 비밀번호와 다르게 해야 할 문자의 최소 개수를 설정합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다. 문자 매칭은 위치와 상관없습니다. 즉 새 비밀번호 문자가 기존 비밀번호의 어느 위치에도 없어야 변경된 것으로 간주됩니다.
3단계	**password-policy minimum-length** *value* 예: ciscoasa(config)# password-policy minimum-length 8	(선택 사항) 비밀번호의 최소 길이를 설정합니다. 유효한 값의 범위는 3자~64자입니다. 권장되는 비밀번호 최소 길이는 8자입니다.
4단계	**password-policy minimum-uppercase** *value* 예: ciscoasa(config)# password-policy minimum-uppercase 3	(선택 사항) 비밀번호에 포함해야 할 대문자의 최소 개수를 설정합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.
5단계	**password-policy minimum-lowercase** *value* 예: ciscoasa(config)# password-policy minimum-lowercase 6	(선택 사항) 비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.
6단계	**password-policy minimum-numeric** *value* 예: ciscoasa(config)# password-policy minimum-numeric 1	(선택 사항) 비밀번호에 포함해야 할 숫자의 최소 개수를 설정합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.

	명령	목적
7단계	**password-policy minimum-special** *value* 예: `ciscoasa(config)# password-policy minimum-special 2`	(선택 사항) 비밀번호에 포함해야 할 특수 문자의 최소 개수를 설정합니다. 유효한 값의 범위는 0자~64자입니다. 특수 문자에는 !, @, #, $, %, ^, &, *, '(' 및 ')'가 포함됩니다. 기본값은 0입니다. 즉 최소 개수 제한이 없습니다.
8단계	**password-policy authenticate enable** 예: `ciscoasa(config)# password-policy authenticate enable`	(선택 사항) 사용자가 **username** 명령으로 비밀번호를 바꾸는 것을 허용하지 않고 반드시 **change-password** 명령으로 비밀번호를 변경하게 할 것인지 설정합니다. 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 **사용자 이름**의 비밀번호를 새로운 비밀번호로 변경해야 합니다. 비밀번호 정책 인증을 활성화한 경우 (**password-policy authenticate enable** 명령) 반드시 이 비밀번호 변경 방법을 사용해야 합니다. 비밀번호 정책 인증이 활성화되지 않은 경우에는 이 방법을 사용하거나 **username** 명령을 사용하여 직접 사용자 어카운트를 변경할 수도 있습니다.

세부 단계

명령	목적
change-password [**old-password** *old_password* [**new-password** *new_password*]] 예: `hostname# change-password old-password j0hncr1chton new-password a3rynsun`	**사용자 이름** 비밀번호를 변경합니다. 명령에 기존 비밀번호와 새 비밀번호를 입력하지 않으면 ASA에서는 입력하라는 메시지를 표시합니다.

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(컨피그레이션 명령 포함)에 액세스할 수 있습니다.

다음 2가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 레벨
- TACACS+ 서버 권한 레벨

명령 권한 부여에 대한 자세한 내용은 35-13 페이지의 명령 권한 부여에 대한 정보를 참조하십시오.

- 35-24 페이지의 로컬 명령 권한 부여 구성
- 35-26 페이지의 로컬 명령 권한 레벨 보기
- 35-27 페이지의 TACACS+ 서버의 명령 구성
- 35-28 페이지의 TACACS+ 명령 권한 부여 구성

로컬 명령 권한 부여 구성

로컬 명령 권한 부여에서는 16가지 권한 레벨(0~15) 중 하나에 명령을 지정할 수 있습니다. 기본적으로 각 명령은 권한 레벨 0 또는 15 중 하나에 지정됩니다. 각 사용자를 특정 권한 레벨로 정의할 수 있으며, 각 사용자는 지정된 권한 레벨 이하의 어떤 명령도 입력할 수 있습니다. ASA에서는 로컬 데이터베이스, RADIUS 서버 또는 (LDAP 특성을 RADIUS 특성에 매핑한 경우) LDAP 서버에 정의된 사용자 권한 레벨을 지원합니다. 자세한 내용은 다음 절을 참조하십시오.

- 27-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가
- 28-1 페이지의 지원되는 인증 방법
- 30-5 페이지의 LDAP 특성 맵 구성

로컬 명령 권한 부여를 구성하려면 다음 단계를 수행합니다.

세부 단계

	명령	목적
1단계	**privilege** [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command* 예: `ciscoasa(config)# privilege show level 5 command filter`	어떤 명령을 어떤 권한 레벨에 지정합니다. 다시 지정하고 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 컨피그레이션 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 레벨. • **mode** {**enable | configure**}—사용자 EXEC 모드 또는 특별 권한 EXEC 모드뿐 아니라 컨피그레이션 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 컨피그레이션 모드를 지정합니다. • **command** *command*—구성 중인 명령입니다. *주(main)* 명령의 권한 레벨만 구성할 수 있습니다. 이를테면 모든 **aaa** 명령의 레벨을 구성할 수 있으나, **aaa authentication** 명령과 **aaa authorization** 명령의 레벨을 각각 구성할 수는 없습니다.
2단계	**aaa authorization exec authentication-server** 예: `ciscoasa(config)# aaa authorization exec authentication-server`	RADIUS의 관리 사용자 권한 레벨을 지원합니다. 관리 액세스를 위해 인증하는 사용자에게 사용자별 액세스 레벨을 적용합니다(**aaa authentication console LOCAL** 명령 참조). 이 명령을 사용하지 않을 경우 ASA에서는 로컬 데이터베이스 사용자의 권한 레벨만 지원하며, 그 밖의 모든 사용자 유형은 기본적으로 레벨 15가 됩니다. 이 명령은 로컬, RADIUS, LDAP(매핑됨), TACACS+ 사용자에 대한 관리 권한 부여도 활성화합니다. 로컬 데이터베이스에서 특성을 가져올 수 있게 하려면 **aaa authorization exec LOCAL** 명령을 사용합니다. AAA 서버의 사용자가 관리 권한 부여를 수용하도록 구성하는 것에 대한 자세한 내용은 35-19 페이지의 관리 권한 부여로 사용자 CLI 및 ASDM 액세스 제한을 참조하십시오.

	명령	목적
3단계	**aaa authorization command LOCAL** 예: `ciscoasa(config)# aaa authorization command LOCAL`	로컬 명령 권한 레벨을 사용할 수 있게 합니다. 이는 로컬 데이터베이스, RADIUS 서버 또는 LDAP 서버(매핑된 특성) 사용자의 권한 레벨로 확인할 수 있습니다. 명령 권한 레벨을 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 레벨을 개별적으로 설정하거나, 이 옵션을 생략하여 모든 형식에 동일한 권한 레벨을 설정할 수 있습니다. 다음 예는 각 형식을 개별적으로 설정하는 방법을 보여줍니다.

```
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 레벨에 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 명령은 화면에서 형식을 구분합니다.

다음 예는 **mode** 키워드의 사용 방법을 보여줍니다. **enable** 명령은 사용자 EXEC 모드에서 입력해야 하지만, 컨피그레이션 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 마지막 라인은 **configure terminal** 명령을 위한 것입니다.

로컬 명령 권한 레벨 보기

다음 명령을 명령에 대한 권한 레벨을 볼 수 있습니다.

명령	목적
show running-config all privilege all	모든 명령을 표시합니다.
show running-config privilege level *level*	특정 레벨의 명령을 표시합니다. *level*은 0~15의 정수입니다.
show running-config privilege command *command*	특정 명령의 레벨을 표시합니다.

예

show running-config all privilege all 명령의 경우, ASA는 현재 각 CLI 명령에 어떤 권한 레벨이 부여되었는지 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
....
```

다음 예는 권한 레벨 10의 명령 지정을 보여줍니다.

```
ciscoasa(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

다음 예는 **access-list** 명령의 명령 지정을 보여줍니다.

```
ciscoasa(config)# show running-config 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
```

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 ACS에 "pix-shell"이라는 명령 유형이 포함되었을 수 있습니다. ASA 명령 권한 부여에는 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 arguments 필드에 **permit aaa-server**를 입력합니다.

- **Permit Unmatched Args** 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(.

- 하나의 단어인 명령에 대해서는 *반드시* 일치하지 않음(unmatched) 인수를 허용해야 합니다. **enable**, **help**.
- 일부 인수를 허용하지 않으려면 그 인수 앞에 **deny**를 입력합니다.

  예를 들어, **enable**을 허용하되 **enable password**는 허용하지 않으려면 commands 필드에 **enable**을 입력하고 arguments 필드에 **deny password**라고 입력합니다. 반드시 **Permit Unmatched Args** 확인란을 선택하여 **enable**만 계속 허용되게 해야 합니다.
- 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 명령 **show logging message**가 아닌 **show logging mess**를 TACACS+ 서버에 보냅니다. 약어를 예상하여 동일 인수의 여러 철자를 구성할 수 있습니다.
- 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 컨피그레이션이 작동할 때까지는 컨피그레이션을 저장하지 마십시오. 실수로 잠긴 경우 대개는 ASA를 다시 시작하면 액세스를 복구할 수 있습니다. 그래도 잠겨 있다면 35-32 페이지의 잠금에서 복구를 참조하십시오.

TACACS+ 시스템이 확실히 안정적이고 신뢰할 수 있는지 확인합니다. 필요한 수준의 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 대비책

으로 로컬 명령 권한 부여를 구성할 수도 있습니다. 그러한 경우 35-24 페이지의 명령 권한 부여 구성의 절차에 따라 로컬 사용자 및 명령 권한 레벨을 구성해야 합니다.

TACACS+ 명령 권한 부여를 구성하려면 다음 명령을 입력합니다.

세부 단계

명령	목적
aaa authorization command *tacacs+_server_group* [**LOCAL**] **예:** `ciscoasa(config)# aaa authorization command group_1 LOCAL`	TACACS+ 서버를 사용하여 명령 권한 부여를 수행합니다. ASA에서 TACACS+ 서버를 사용할 수 없을 때 로컬 데이터베이스를 대신 사용하도록 구성할 수 있습니다. 대비책을 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 사용자(27-3페이지의 "로컬 데이터베이스에 사용자 어카운트 추가" 섹션 참조)와 명령 권한 레벨(35-24 페이지의 로컬 명령 권한 부여 구성 참조)을 구성해야 합니다.

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.

세부 단계

	명령	목적
1단계	**aaa accounting** {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag* **예:** `ciscoasa(config)# aaa accounting telnet console group_1`	관리 액세스를 위해 AAA 어카운팅 지원을 활성화합니다. 유효한 서버 그룹 프로토콜은 RADIUS와 TACACS+입니다.
2단계	**aaa accounting command** [**privilege** *level*] *server-tag* **예:** `ciscoasa(config)# aaa accounting command privilege 15 group_1`	명령 어카운팅을 활성화합니다. TACACS+ 서버만 명령 어카운팅을 지원합니다. 여기서 **privilege** *level*은 최소 권한 레벨, *server-tag*는 TACACS+ 서버 그룹의 이름입니다. ASA에서 이 서버 그룹에 명령 어카운팅 메시지를 보내야 합니다.

현재 로그인한 사용자 보기

현재 로그인한 사용자를 보려면 에 다음 명령을 입력합니다.

```
ciscoasa# show curpriv
```

예

다음은 **show curpriv** 명령 출력의 샘플입니다.

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

표 35-1에서는 **show curpriv** 명령 출력에 대해 설명합니다.

표 35-1 show curpriv 명령 출력 설명

필드	설명
Username	사용자 이름. 기본 사용자로 로그인할 경우 이름은 enable_1(사용자 EXEC) 또는 enable_15(특별 권한 EXEC)입니다.
Current privilege level	레벨은 0부터 15까지입니다. 로컬 명령 권한 부여를 구성하고 중간 권한 레벨에 명령을 지정하지 않는 한, 레벨 0과 15만 사용됩니다.
Current Modes	사용 가능한 액세스 모드는 다음과 같습니다. • P_UNPR—사용자 EXEC 모드(레벨 0과 1) • P_PRIV—특별 권한 EXEC 모드(레벨 2~15) • P_CONF—컨피그레이션 모드

관리 세션 할당량 설정

동시 관리 세션의 최대 개수를 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.

관리 세션 할당량을 설정하려면 다음 명령을 입력합니다.

명령	목적
quota management-session *number* **예:** `hostname(config)# quota management-session 1000`	ASA에서 허용되는 동시 ASDM, SSH, 텔넷 세션의 최대 개수를 설정합니다. 이 명령의 **no** 형식은 할당량 값을 0으로 설정합니다. 그러면 세션은 무제한입니다.

SSH 세션에서 키 교환

DH(Diffie-Hellman) 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 그룹 1 및 그룹 14 키 교환 방식 모두 ASA에서 지원됩니다. 어떤 DH 그룹 키 교환 방식도 지정되지 않은 경우 DH Group 1 키 교환 방식이 사용됩니다. DH 키 교환 방식 사용에 대한 자세한 내용은 RFC 4253을 참조하십시오.

SSH 세션에서 키를 교환하려면 다음 명령을 입력합니다.

명령	목적
ssh key-exchange group {**dh-group1** | **dh-group14**} **sha-1** 예: `ciscoasa(config)# ssh key-exchange group dh-group14 sha-1` `ciscoasa# show running-config key-exchange` `ssh key-exchange dh-group14-sha1`	DH 그룹 1 또는 DH 그룹 14 키 교환 방식 중 하나로 키를 교환합니다. **key-exchange** 키워드는 DH 그룹 1 또는 DH 그룹 14 키 교환 방식 중 하나가 뒤따르고 이를 키 교환에 적용할 것임을 나타냅니다. **group** 키워드는 DH 그룹 1 키 교환 방식 또는 DH 그룹 14 키 교환 방식 중 하나가 뒤따르고 이를 키 교환에 적용할 것임을 나타냅니다. **dh-group1** 키워드는 DH 그룹 1 키 교환 방식이 뒤따르고 이를 키 교환에 적용할 것임을 나타냅니다. DH 그룹 2는 레거시 이유 때문에 DH 그룹 1로 불립니다. **dh-group14** 키워드는 DH 그룹 14 키 교환 방식이 뒤따르고 이를 키 교환에 적용할 것임을 나타냅니다. **sha-1** 키워드는 SHA-1 암호화 알고리즘을 사용할 것임을 나타냅니다. DH 그룹 키 교환 방식이 현재 사용되고 있음을 표시하려면 **show running-config ssh key-exchange** 명령을 사용합니다.

잠금에서 복구

명령 권한 부여 또는 CLI 권한 부여를 활성화할 때 ASA CLI에서 잠기는 경우가 있습니다. 대개는 ASA를 다시 시작하여 액세스를 복구할 수 있습니다. 그러나 이미 컨피그레이션을 저장한 경우 잠길 수 있습니다. 표 35-2에서는 대표적인 잠금 조건과 그로부터 복구하는 방법을 소개합니다.

표 35-2 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.	로컬데이터베이스에 사용자가 없을 경우 로그인할 수 없고 어떤 사용자도 추가할 수 없습니다.	로그인하고 비밀번호 및 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 영역에서 컨텍스트로 변경하고 사용자를 추가할 수 있습니다.
TACACS+ 명령 권한 부여 TACACS+ CLI 인증 RADIUS CLI 인증	서버가 중지했거나 연결 불가한 상태이며, 구성된 대비책이 없습니다.	서버가 연결 불가한 상태라면 로그인할 수 없고 어떤 명령도 입력할 수 없습니다.	1. 로그인하고 비밀번호 및 AAA 명령을 재설정합니다. 2. 로컬 데이터베이스를 대비책으로 구성하여 서버가 중지하더라도 잠기지 않게 합니다.	1. ASA에서 네트워크 컨피그레이션이 올바르지 않아 서버 연결이 불가할 경우 스위치에서 ASA로 세션 연결합니다. 시스템 실행 영역에서 컨텍스트로 변경하고 네트워크 설정을 재구성할 수 있습니다. 2. 로컬 데이터베이스를 대비책으로 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 컨텍스트로 변경하고 컨피그레이션 변경 사항을 완료할 수 있습니다. 또한 TACACS+ 컨피그레이션의 문제를 해결할 때까지 명령 권한 부여를 비활성화할 수도 있습니다.
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 컨텍스트로 변경하고 사용자 레벨을 변경할 수 있습니다.

관리 액세스 기능 내역

표 35-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다.

표 35-3 관리 액세스 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
관리 액세스	7.0(1)	이 기능을 도입했습니다. 도입된 명령: **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 authentication enable 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**
SSH 보안을 강화했습니다. 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 > Device Management > Users/AAA > AAA Access > Authentication(ASDM)을 사용하여 AAA 인증을 구성해야 합니다. 그런 다음 **username** 명령(CLI)을 입력하거나 Configuration > Device Management > Users/AAA > User Accounts(ASDM)를 사용하여 로컬 사용자를 정의합니다. 로컬 데이터베이스 대신에 AAA 서버를 인증에 사용하려는 경우, 만일에 대비하여 로컬 인증도 구성하는 것이 좋습니다.
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. 도입된 명령: **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**, **show running-config password-policy**

표 35-3 관리 액세스 기능 내역(계속)

기능 이름	플랫폼 릴리스	기능 정보
SSH 공개 키 인증 지원	8.4(4.1), 9.1(2)	사용자별로 ASA와의 SSH 연결에 대해 공개 키 인증을 활성화할 수 있습니다. PKF(공개 키 파일) 형식의 키 또는 Base64 키를 지정할 수 있습니다. PKF 키는 최대 4096비트입니다. ASA의 Base64 형식 지원 범위(최대 2048비트)에 비해 너무 큰 키에는 PKF 형식을 사용합니다. 도입된 명령: **ssh authentication** *PKF 키 형식은 9.1(2) 이상에서만 지원됩니다.*
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. 도입된 명령: **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. 도입된 명령: **quota management-session**, **show running-config quota management-session**, **show quota management-session**
다중 컨텍스트 모드의 ASASM에서는 스위치로부터의 텔넷 및 가상 콘솔 인증 지원.	8.5(1)	다중 컨텍스트 모드의 스위치에서 ASASM로의 연결이 시스템 실행 영역으로 연결되지만, 관리 컨텍스트에서 이러한 연결에 적용할 인증을 구성할 수 있습니다.
SSH를 위한 AES-CTR 암호화	9.1(2)	ASA의 SSH 서버 인증에서 이제 AES-CTR 모드 암호화를 지원합니다.
SSH rekey 간격 향상		SSH 연결은 연결 시간이 60분이 지났거나 데이터 트래픽이 1GB를 초과하면 키가 다시 생성됩니다. 도입된 명령: **show ssh sessions detail**
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. 수정된 명령: **aaa authorization exec**

36 장

소프트웨어 및 컨피그레이션

이 장에서는 Cisco ASA 소프트웨어 및 컨피그레이션을 관리하는 방법을 설명합니다.

소프트웨어 업그레이드

업그레이드 경로 및 마이그레이션

- 9.0 이전 릴리스에서 업그레이드하는 경우, ACL 마이그레이션 때문에 향후 다운그레이드할 수 없습니다. 다운그레이드해야 할 경우에 대비하여 반드시 컨피그레이션 파일을 백업하십시오. 자세한 내용은 9.0 업그레이드 설명서의 ACL 마이그레이션 섹션을 참조하십시오.
- 9.1(2.8) 이전 버전에서 9.1(2.8) 이상으로 업그레이드하려면 다음 버전 중 하나를 실행하고 있어야 합니다.
  - 8.4(5) 이상
  - 9.0(2) 이상
  - 9.1(2)

  더 오래된 버전을 실행하고 있다면 9.1(2.8) 이상으로 곧바로 업그레이드할 수 없습니다. *먼저* 위 버전 중 하나로 업그레이드해야 합니다. 예:

9.1(2.8) 이전 ASA 버전	1 차 업그레이드할 버전 :	그 다음에 업그레이드할 버전 :
8.2(1)	8.4(7)	9.3(1) 이상
8.4(4)	8.4(7)	9.3(1) 이상
9.0(1)	9.0(4)	9.3(1) 이상
9.1(1)	9.1(2)	9.3(1) 이상

- 8.3 이전 버전에서 업그레이드하는 경우
  - 컨피그레이션 마이그레이션에 대한 자세한 내용은 *Cisco ASA 5500 버전 8.3으로의 마이그레이션 설명서*를 참조하십시오.
  - 9.0 이상으로 곧바로 업그레이드할 수 없습니다. 성공적인 마이그레이션을 위해서는 먼저 버전 8.4로 업그레이드해야 합니다.
- 제로 다운타임 업그레이드를 위한 소프트웨어 버전 요구 사항

  장애 조치 컨피그레이션 또는 ASA 클러스터에 포함된 유닛은 주 소프트웨어 버전(1번째 번호)과 부 소프트웨어 버전(2번째 번호)이 동일해야 합니다. 그러나 업그레이드 프로세스에서는 유닛의 버전을 일치시킬 필요는 없습니다. 각 유닛에서 여러 버전의 소프트웨어가 실행되고 있더라도 장애 조치는 계속 지원됩니다. 장기적인 호환성 및 안정성을 위해 가급적 서둘러 모든 유닛을 동일한 버전으로 업그레이드하는 것이 좋습니다.

  표 36-1에서는 지원되는 제로 다운타임 업그레이드 시나리오를 소개합니다.

표 36-1 제로 다운타임 업그레이드 지원

업그레이드 유형	지원
유지 보수 릴리스	임의의 유지 보수 릴리스에서 부(minor) 릴리스 범위의 다른 유지 보수 릴리스로 업그레이드할 수 있습니다. 예를 들면, 9.1(1)에서 9.1(5)로 업그레이드할 수 있습니다. 먼저 그 사이에 유지 보수 릴리스를 설치할 필요 없습니다.
부 릴리스	부 릴리스에서 다음 부 릴리스로 업그레이드할 수 있습니다. 부 릴리스를 건너뛸 수 없습니다. 예를 들어, 9.0에서 9.1로 업그레이드할 수 있습니다. 9.0에서 9.2로 곧바로 업그레이드하는 경우 제로 다운타임 업그레이드가 지원되지 않습니다. 먼저 9.1로 업그레이드해야 합니다. **참고** 제로 다운타임 업그레이드는 기능 컨피그레이션이 마이그레이션된 경우에도 가능합니다.
주 릴리스	이전 버전의 최종 부 릴리스에서 다음 주 릴리스로 업그레이드할 수 있습니다. 예를 들어, 8.6에서 9.0으로 업그레이드할 수 있습니다. 단, 8.6이 해당 모델의 8.x 릴리스에서 마지막 부 버전이어야 합니다. 8.6에서 9.1로 곧바로 업그레이드하는 경우에는 제로 다운타임 업그레이드가 지원되지 않습니다. 먼저 9.0으로 업그레이드해야 합니다. 부 릴리스에서 지원되지 않는 모델의 경우, 부 릴리스를 건너뛸 수 있습니다. 예를 들어, ASA 5585-X(8.5 또는 8.6에서 지원되지 않는 모델)는 8.4에서 9.0으로 업그레이드할 수 있습니다. **참고** 제로 다운타임 업그레이드는 기능 컨피그레이션이 마이그레이션된 경우에도 가능합니다.

현재 버전 보기

show version 명령을 사용하여 ASA의 소프트웨어 버전을 확인합니다.

Cisco.com에서 소프트웨어 다운로드

Cisco.com 로그인이 가능한 경우 다음 웹 사이트에서 OS 및 ASDM 이미지를 얻을 수 있습니다.

http://www.cisco.com/go/asa-software

이 절차에서는 TFTP 서버에 이미지를 저장한다고 가정합니다. 물론 다른 서버 유형도 지원됩니다.

독립형 유닛 업그레이드

이 섹션에서는 ASDM 및 OS(운영 체제) 이미지를 설치하는 방법을 설명합니다.

절차

이 절차에서는 TFTP를 사용합니다. FTP 또는 HTTP는 **copy** 명령을 참조하십시오.

1단계 (컨피그레이션 마이그레이션이 있는 경우) 컨피그레이션을 백업할 수 있도록 터미널에 컨피그레이션을 표시합니다.

more system:running-config

이 명령의 출력을 복사하고 텍스트 파일에 그 컨피그레이션을 붙여넣습니다. 다른 백업 방법에 대해서는 컨피그레이션 설명서를 참조하십시오.

2단계 활성 유닛 플래시 메모리에 ASA 소프트웨어를 복사합니다.

copy tftp://*server*[*/path*]*/asa_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asa_image_name*

예:

```
ciscoasa# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

TFTP가 아닌 방법에 대해서는 **copy** 명령을 참조하십시오.

3단계 활성 유닛 플래시 메모리에 ASDM 이미지를 복사합니다.

copy tftp://*server*[*/path*]*/asdm_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asdm_image_name*

예:

```
ciscoasa# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

4단계 아직 전역 컨피그레이션 모드가 아닐 경우 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

5단계 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

예:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa914-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(6단계 및 7단계 참조).

6단계 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 삭제합니다.

no boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

예:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa914-smp-k8.bin
```

7단계 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

예:

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어, 앞서 6단계에서 삭제했던 이미지를 다시 입력할 수 있습니다.

8단계 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

예:

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

9단계 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

10단계 ASA를 다시 로드합니다.

reload

장애 조치 쌍 또는 ASA 클러스터 업그레이드

활성/대기(Active/Standby) 장애 조치 쌍 업그레이드

활성/대기 장애 조치 쌍을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

활성 유닛에서 다음 작업을 수행합니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) 컨피그레이션을 백업할 수 있도록 터미널에 컨피그레이션을 표시합니다.

more system:running-config

예:

```
active# more system:running-config
```

이 명령의 출력을 복사하고 텍스트 파일에 그 컨피그레이션을 붙여넣습니다. 다른 백업 방법에 대해서는 컨피그레이션 설명서를 참조하십시오.

2단계 활성 유닛 플래시 메모리에 ASA 소프트웨어를 복사합니다.

copy tftp://*server*[/*path*]/*asa_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

예:

```
active# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

TFTP가 아닌 방법에 대해서는 **copy** 명령을 참조하십시오.

3단계 소프트웨어를 대기 유닛에 복사합니다. 활성 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm tftp://*server*[/*path*]/*filename* {**disk0:/** | **disk1:/**}[*path*/]*filename*

예:

```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

4단계 활성 유닛 플래시 메모리에 ASDM 이미지를 복사합니다.

copy tftp://*server*[/*path*]/*asdm_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

예:

```
active# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

5단계 ASDM 이미지를 대기 유닛에 복사합니다. 활성 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm tftp://*server*[/*path*]/*asdm_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

예:

```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin
disk0:/asdm-731.bin
```

6단계 아직 전역 컨피그레이션 모드가 아닐 경우 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

7단계 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

예:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(8단계 및 9단계 참조).

8단계 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 삭제합니다.

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

예:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

9단계 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

예:

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어, 앞서 8단계에서 삭제했던 이미지를 다시 입력할 수 있습니다.

10단계 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

예:

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

11단계 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

12단계 새 이미지를 부팅하기 위해 대기 유닛을 다시 로드합니다.

failover reload-standby

대기 유닛에서 로딩을 마칠 때까지 기다립니다. **show failover** 명령을 사용하여 대기 유닛이 Standby 상태임을 확인합니다.

13단계 강제적으로 활성 유닛을 대기 유닛에 장애 조치합니다.

no failover active

14단계 이전의 활성 유닛(지금은 새로운 대기 유닛)을 다시 로드합니다.

reload

다시 로드한 다음 이 유닛을 활성 상태로 복원하려면 **failover active** 명령을 입력합니다.

활성/활성(Active/Active) 장애 조치 쌍 업그레이드

활성/활성 장애 조치 컨피그레이션의 두 유닛을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

시스템 실행 영역에서 다음 단계를 수행합니다. 또한 *기본* 유닛에서도 이 단계를 수행합니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) 컨피그레이션을 백업할 수 있도록 터미널에 컨피그레이션을 표시합니다.

more system:running-config

이 명령의 출력을 복사하고 텍스트 파일에 그 컨피그레이션을 붙여넣습니다. 다른 백업 방법에 대해서는 컨피그레이션 설명서를 참조하십시오.

2단계 기본 유닛 플래시 메모리에 ASA 소프트웨어를 복사합니다.

copy tftp://*server*[**/***path*]**/***asa_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

예:

```
primary# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

TFTP가 아닌 방법에 대해서는 **copy** 명령을 참조하십시오.

3단계 소프트웨어를 보조 유닛에 복사합니다. 기본 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm tftp://*server*[**/***path*]**/***filename* {**disk0:/** | **disk1:/**}[*path***/**]*filename*

예:

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

4단계 기본 유닛 플래시 메모리에 ASDM 이미지를 복사합니다.

copy tftp://*server*[**/***path*]**/***asdm_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

예:

```
primary# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

5단계 ASDM 이미지를 보조 유닛에 복사합니다. 활성 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm tftp://*server*[**/***path*]**/***asdm_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

예:

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin
disk0:/asdm-731.bin
```

6단계 기본 유닛에서 두 장애 조치 그룹을 활성 상태로 만듭니다.

```
failover active group 1
failover active group 2
```

7단계 아직 전역 컨피그레이션 모드가 아닐 경우 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

예:

```
primary(config)# configure terminal
```

8단계 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

예:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(9단계 및 10단계 참조).

9단계 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 삭제합니다.

no boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

예:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

10단계 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

예:

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어, 앞서 9단계에서 삭제했던 이미지를 다시 입력할 수 있습니다.

11단계 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

예:

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

12단계 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

13단계 새 이미지를 부팅하기 위해 보조 유닛을 다시 로드합니다.

failover reload-standby

보조 유닛에서 로딩을 마칠 때까지 기다립니다. **show failover** 명령을 사용하여 두 장애 조치 그룹 모두 Standby Ready 상태임을 확인합니다.

14단계 강제적으로 보조 유닛에서 두 장애 조치 그룹이 활성 상태가 되게 합니다.

```
no failover active group 1
no failover active group 2
```

15단계 기본 유닛을 다시 로드합니다.

```
reload
```

장애 조치 그룹이 **preempt** 명령으로 구성된 경우, 우선적 지연 시간이 지나면 지정된 유닛에서 자동으로 활성 상태가 됩니다. 장애 조치 그룹이 **preempt** 명령으로 구성되지 않은 경우, **failover active group** 명령을 사용하여 지정된 유닛에서 활성 상태로 되돌릴 수 있습니다.

ASA 클러스터 업그레이드

ASA 클러스터의 모든 유닛을 업그레이드하려면 마스터 유닛에서 다음 단계를 수행합니다. 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 단계를 수행합니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) 컨피그레이션 파일을 백업합니다.

```
more system:running-config
```

이 명령의 출력을 복사하고 텍스트 파일에 그 컨피그레이션을 붙여넣습니다. 다른 백업 방법에 대해서는 일반 운영 컨피그레이션 가이드를 참조하십시오.

2단계 ASA 소프트웨어를 클러스터의 모든 유닛에 복사합니다.

```
cluster exec copy /noconfirm tftp://server[/path]/asa_image_name {disk0:/ |
disk1:/}[path/]asa_image_name
```

예:

```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

TFTP가 아닌 방법에 대해서는 **copy** 명령을 참조하십시오.

3단계 ASDM 이미지를 클러스터의 모든 유닛에 복사합니다.

```
cluster exec copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/ |
disk1:/}[path/]asdm_image_name
```

예:

```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

4단계 아직 전역 컨피그레이션 모드가 아닐 경우 전역 컨피그레이션 모드에 액세스합니다.

```
configure terminal
```

5단계 현재 구성된 부트 이미지를 표시합니다(최대 4개).

```
show running-config boot system
```

예:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(6단계 및 7단계 참조).

6단계 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 삭제합니다.

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

예:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

7단계 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

예:

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어, 앞서 6단계에서 삭제했던 이미지를 다시 입력할 수 있습니다.

8단계 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

예:

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

9단계 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

10단계 각 유닛 이름에 대해 이 명령을 반복할 때 각 슬레이브 유닛을 다시 로드합니다.

cluster exec unit *slave-unit* **reload noconfirm**

예:

```
master# cluster exec unit unit2 reload noconfirm
```

연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 시작할 때까지 기다렸다가(약 5분) 다음 유닛을 다시 로드합니다. 멤버 이름을 보려면 **cluster exec unit ?** 또는 **show cluster info** 명령을 입력합니다.

11단계 마스터 유닛에서 클러스터링을 비활성화합니다.

no enable

새 마스터가 선택되고 트래픽이 안정화될 때까지 5분가량 기다립니다. **write memory**를 입력하지 마십시오. 마스터 유닛이 다시 로드될 때 이 유닛에서 클러스터링이 활성화되어야 합니다.

12단계 마스터 유닛을 다시 로드합니다.

reload noconfirm

새 마스터 유닛을 위해 새로운 선택이 이루어집니다. 이전의 마스터 유닛은 다시 클러스터에 합류하면 슬레이브가 됩니다.

파일 관리

플래시 메모리의 파일 보기

다음과 같이 플래시 메모리의 파일을 보고 그 파일에 대한 정보를 확인할 수 있습니다.

- 플래시 메모리의 파일을 보려면 다음 명령을 입력합니다.

```
ciscoasa# dir [disk0: | disk1:]
```

내부 플래시 메모리는 **disk0:**을 입력합니다. **disk1:** 키워드는 외부 플래시 메모리를 나타냅니다. 내부 플래시 메모리가 기본값입니다.

예:

```
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
```

- 특정 파일에 대한 자세한 정보를 보려면 다음 명령을 입력합니다.

```
hostname# show file information [path:/]filename
```

기본 경로는 내부 플래시 메모리의 루트 디렉토리(disk0:/)입니다.

예:

```
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.

플래시 메모리의 파일 삭제

플래시 메모리에서 더 이상 필요 없는 파일을 삭제할 수 있습니다. 플래시 메모리에서 파일을 삭제하려면 다음 명령을 입력합니다.

```
hostname# delete disk0: filename
```

경로를 지정하지 않을 경우, 기본적으로 현재 작업 디렉토리에서 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 수행합니다.

1단계 2-2 페이지의 ASA Services Module 콘솔 액세스 또는 2-1 페이지의 어플라이언스 콘솔 액세스의 지침에 따라 ASA 콘솔 포트에 연결합니다.

2단계 ASA를 껐다가 다시 켭니다.

3단계 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 **erase** 명령을 입력합니다. 그러면 모든 파일을 덮어쓰고 숨겨진 시스템 파일을 포함하여 파일 시스템을 지웁니다.

```
rommon #1> erase [disk0: | disk1: | flash:]
```

파일 액세스 구성

- 36-12 페이지의 FTP 클라이언트 모드 구성
- 36-12 페이지의 ASA를 SCP 서버로 구성
- 36-13 페이지의 ASA SCP 클라이언트 사용자 지정
- 36-15 페이지의 ASA TFTP 클라이언트 경로 구성

FTP 클라이언트 모드 구성

ASA에서는 FTP를 사용하여 FTP 서버에 이미지 파일이나 컨피그레이션 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.

세부 단계

명령	목적
ftp mode passive **예:** `ciscoasa(config)# ftp mode passive`	FTP 모드를 패시브로 설정합니다.

ASA를 SCP 서버로 구성

ASA에서 SCP(Secure Copy) 서버를 활성화할 수 있습니다. SSH를 사용하여 ASA에 액세스하는 것이 허용된 클라이언트만 SCP 연결을 설정할 수 있습니다.

제한 사항

- 이 서버에서는 디렉토리가 지원되지 않습니다. 디렉토리가 지원되지 않으므로 ASA 내부 파일에 대한 원격 클라이언트 액세스가 제한됩니다.

- 이 서버는 배너를 지원하지 않습니다.
- 이 서버는 와일드카드를 지원하지 않습니다.

전제 조건

- ASA에서 35-4 페이지의 SSH 액세스 구성에 따라 SSH를 설정합니다.
- ASA 라이센스에 강력한 암호화(3DES/AES) 라이센스가 있어야 SSH 버전 2 연결을 지원할 수 있습니다.

세부 단계

명령	목적
ssh scopy enable 예: `ciscoasa(config)# ssh scopy enable`	SCP 서버를 활성화합니다.

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.

ASA SCP 클라이언트 사용자 지정

온보드 SCP 클라이언트를 사용하여 ASA에 파일을 복사하거나 복사해 올 수 있습니다(36-16 페이지의 ASA에 파일 복사 참조). 이 섹션에서는 SCP 클라이언트 작업을 사용자 지정할 수 있습니다.

전제 조건

다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 컨텍스트에서 시스템 실행 영역으로 변경하려면 **changeto system** 명령을 입력합니다.

세부 단계

	명령	목적
1단계	[**no**] **ssh stricthostkeycheck** **예:** `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]?`	SSH 호스트 키 검사를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 활성화되어 있습니다. 이 옵션이 활성화된 경우, 호스트 키가 아직 ASA에 저장되지 않았다면 호스트 키를 승인하거나 거부하라는 메시지가 나타납니다. 이 옵션이 비활성화된 경우, 호스트 키가 아직 저장되지 않았다면 ASA는 자동으로 호스트 키를 승인합니다.
2단계	**ssh pubkey-chain** [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*} **예:** `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. 원한다면 ASA 데이터베이스에서 직접 서버와 키를 추가하거나 삭제할 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.

예

다음 예에서는 서버 10.86.94.170을 위해 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 서버 10.7.8.9를 위해 호스트 문자열 키를 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 Rev에 기술되어 있습니다. 2. ASA를 TFTP *클라이언트*로 구성하여 TFTP *서버*에 파일을 복사하거나 복사해 오도록 할 수 있습니다(36-16 페이지의 ASA에 파일 복사 및 36-24 페이지의 컨피그레이션 또는 기타 파일 백업 및 복원 참조). 이와 같은 방법으로 컨피그레이션 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.

세부 단계

명령	목적
tftp-server *interface_name server_ip filename* **예:** 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...	**configure net** 및 **copy** 명령에서 사용할 TFTP 서버 주소와 파일 이름을 미리 정의합니다. 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.

지침

- 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 디렉토리에서 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 설명서*를 참조하십시오. ASA에 Cisco Secure Desktop을 설치하는 것에 대한 자세한 내용은 *Cisco ASA 5500 Series 관리자를 위한 Cisco Secure Desktop 컨피그레이션 설명서*를 참조하십시오.
- ASA에서 특정 애플리케이션 이미지 또는 ASDM 이미지를 사용하도록 구성하려면(둘 이상을 설치했거나 외부 플래시 메모리에 설치한 경우) 36-20 페이지의 사용할 이미지 및 시작 컨피그레이션 설정을 참조하십시오.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에 있어야 합니다.

세부 단계

명령	목적
copy [/noconfirm] 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)	Copies from a TFTP server.

명령	목적
copy [**/noconfirm**] **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)	Copies from an FTP server.
copy [**/noconfirm**] **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)	Copies from an HTTP(S) server.
copy [**/noconfirm**] **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)	Copies from an SMB server.

명령	목적
copy [**/noconfirm**] **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:2 d:bf:a9:2b:85:2e:19 Password: <type in password> !!!!!! 6006 bytes copied in 8.160 secs (750 bytes/sec)	Copies from a SCP server. **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.

시작 또는 실행 중인 컨피그레이션에 파일 복사

TFTP, FTP, SMB, HTTP(S), SCP 서버로부터 또는 플래시 메모리로부터 실행 중인 컨피그레이션 또는 시작 컨피그레이션에 텍스트 파일을 다운로드할 수 있습니다.

ASA에서 특정 컨피그레이션을 시작 컨피그레이션으로 사용하도록 구성하려면 36-20 페이지의 사용할 이미지 및 시작 컨피그레이션 설정을 참조하십시오.

지침

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 컨텍스트 실행에 영향을 줄 경 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다.

세부 단계

어떤 파일을 시작 컨피그레이션에 또는 실행 중인 컨피그레이션에 복사하려면 적합한 다운로드 서버에 대해 다음 명령 중 하나를 입력합니다.

명령	목적
copy [/noconfirm] tftp://*server[/path]/src_f***ilename {startup-config | running-config}** 예: ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config	Copies from a TFTP server.
copy [**/noconfirm**] **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	Copies from an FTP server.
copy [**/noconfirm**] **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	Copies from an HTTP(S) server.
copy [**/noconfirm**] **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	Copies from an SMB server.
copy [**/noconfirm**] **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	Copies from a SCP server. **;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
```

사용할 이미지 및 시작 컨피그레이션 설정

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.

기본 설정

ASA 이미지

- Physical ASA—내부 플래시 메모리에서 발견한 첫 번째 애플리케이션 이미지를 부팅합니다.
- ASAv—최초로 구축했을 때 생성한 읽기 전용 boot:/ 파티션의 이미지를 부팅합니다. 플래시 메모리의 이미지를 업그레이드하고 그 이미지에서 부팅할 ASAv를 구성할 수 있습니다. 나중에 컨피그레이션을 지울 경우(**clear configure all**), ASAv는 원래로 돌아가 최초의 구축 이미지를 로드합니다.

ASDM 이미지

All ASAs—내부 플래시 메모리에서 발견한 첫 번째 ASDM 이미지를 부팅합니다. 내부 플래시 메모리에 없을 경우 외부 플래시 메모리의 첫 번째 ASDM 이미지를 부팅합니다.

시작 컨피그레이션

기본적으로 ASA는 숨겨진 파일인 시작 컨피그레이션으로부터 부팅합니다.

세부 단계

	명령	목적
1단계	**boot system** *url* 예: `ciscoasa(config)# boot system disk:/images/asa921.bin`	ASA 부트 이미지 위치를 설정합니다. 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 ASA를 ROMMON 모드로 재부팅할 수 있습니다. ROMMON 모드에 대한 자세한 내용은 38-1 페이지의 디버깅 메시지 보기를 참조하십시오.

	명령	목적
2단계	**asdm image** {**disk0:/** | **disk1:/**}[*path/*]*filename* 예: ciscoasa(config)# asdm image disk0:/images/asdm721.bin	부팅할 ASDM 이미지를 설정합니다. 부팅할 이미지를 지정하지 않은 경우, 설치된 이미지가 하나밖에 없더라도 ASA는 **asdm image** 명령을 실행 중인 컨피그레이션에 삽입합니다. 자동 업데이트가 구성된 경우 이와 관련된 문제를 방지하고 시작할 때마다 이미지를 검색하는 번거로움을 피하기 위해서는 부팅할 ASDM 이미지를 시작 컨피그레이션에 지정해야 합니다.
3단계	(선택 사항) **boot config** {**disk0:/** | **disk1:/**}[*path/*]*filename* 예: ciscoasa(config)# boot config disk0:/configs/startup1.cfg	시작 컨피그레이션을 기본값인 숨겨진 파일이 아닌 확인된 파일로 설정합니다.

이미지 로드에 ROM 모니터 사용

ASA 5500-X Series에 ROM 모니터 사용

TFTP를 사용하여 ROM 모니터에서 ASA로 소프트웨어 이미지를 로드하려면 다음 단계를 수행합니다.

1단계 2-1 페이지의 어플라이언스 콘솔 액세스의 지침에 따라 ASA 콘솔 포트에 연결합니다.

2단계 ASA를 껐다가 다시 켭니다.

3단계 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 ROMMOM 모드에서 다음과 같이 ASA에 대한 인터페이스 설정을 정의합니다. 여기에는 IP 주소, TFTP 서버 주소, 게이트웨이 주소, 소프트웨어 이미지 파일, 포트 등이 포함됩니다.

참고 ASA 5506, ASA 5506-W, ASA 5508의 경우 PORT=Ethernet0/0 항목을 포함할 필요 없습니다. 관리 포트만 사용 가능합니다.

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```

참고 Be sure that the connection to the network already exists.

5단계 To validate your settings, enter the **set** command.

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

6단계 Ping the TFTP server by entering the **ping server** command.

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

7단계 Load the software image by entering the **tftp** command.

```
rommon #8> tftp
ROMMON Variable Settings:
  ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp f1/asa840-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2011

Loading...N
```

소프트웨어 이미지가 성공적으로 로드되면 ASA는 자동으로 ROMMON 모드를 종료합니다.

8단계 정확한 소프트웨어 이미지가 ASA에 로드되었는지 확인하려면 다음 명령을 입력하여 ASA의 버전을 확인합니다.

```
ciscoasa# show version
```

ASASM에 ROM 모니터 사용

TFTP를 사용하여 ROM 모니터에서 ASASM로 소프트웨어 이미지를 로드하려면 다음 단계를 수행합니다.

1단계 2-2 페이지의 ASA Services Module 콘솔 액세스의 지침에 따라 ASA 콘솔 포트에 연결합니다.

2단계 ASASM 이미지를 다시 로드해야 합니다.

3단계 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 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 #1> ADDRESS=172.16.145.149
rommon #2> SERVER=172.16.171.125
rommon #3> GATEWAY=172.16.145.129
rommon #4> IMAGE=f1/asa851-smp-k8.bin
rommon #5> PORT=Data0
rommon #6> VLAN=1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

참고 네트워크로의 연결이 이미 존재하는 것을 명심하십시오.

5단계 **set** 명령을 입력하여 설정을 유효하게 합니다.

```
rommon #7> set
ROMMON Variable Settings:
  ADDRESS=172.16.145.149
  SERVER=172.16.171.125
  GATEWAY=172.16.145.129
  PORT=Data0
  VLAN=1
  IMAGE=f1/asa851-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

6단계 **ping server** 명령을 입력하여 TFTP를 핑합니다.

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 172.16.171.125, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

7단계 **tftp** 명령을 입력하여 소프트웨어 이미지를 로드합니다.

```
rommon #9> tftp
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
  ADDRESS=172.16.145.149
  SERVER=172.16.171.125
  GATEWAY=172.16.145.129
  PORT=Data0
  VLAN=1
  IMAGE=f1/asa851-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
```

```
  PKTTIMEOUT=2
  RETRY=20

tftp f1/asa851-smp-k8.bin@172.16.171.125 via 172.16.145.129
Starting download. Press ESC to abort.
```

소프트웨어 이미지가 성공적으로 로드되면 ASASM는 자동으로 ROMMON 모드를 종료합니다.

참고 ROMMON 부트가 완료되면 별도로 시스템 플래시에 이미지를 다운로드해야 합니다. 모듈을 ROMMON 모드로 부팅하더라도 다시 로드할 때마다 시스템 이미지가 보존되지 않습니다.

8단계 정확한 소프트웨어 이미지가 ASASM에 로드되었는지 확인하려면 다음 명령을 입력하여 버전을 확인합니다.

```
hostname# show version
```

컨피그레이션 또는 기타 파일 백업 및 복원

단일 모드 컨피그레이션 또는 다중 모드 시스템 컨피그레이션 백업

단일 컨텍스트 모드에서 또는 다중 모드의 시스템 컨피그레이션에서 시작 컨피그레이션이나 실행 중인 컨피그레이션을 외부 서버에 또는 로컬 플래시 메모리에 복사할 수 있습니다.

세부 단계

명령	목적
copy [/noconfirm] {startup-config | running-config} tftp://*server*[**/***path*]**/***dst_f***ilename** **예:** ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg	TFTP 서버로 복사

명령	목적
copy [**/noconfirm**] {**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	FTP 서버로 복사
copy [**/noconfirm**] {**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	SMB 서버로 복사
copy [**/noconfirm**] {**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	SCP 서버로 복사 **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.
copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path/*]*dst_filename* 예: ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg	로컬 플래시 메모리로 복사 대상 디렉토리가 있어야 합니다. 없는 경우 먼저 **mkdir** 명령을 사용하여 디렉토리를 만듭니다.

플래시 메모리의 컨텍스트 컨피그레이션 또는 기타 파일 백업

시스템 실행 영역에서 다음 명령 중 하나를 입력하여 로컬 플래시 메모리에 있는 컨텍스트 컨피그레이션이나 기타 파일을 복사합니다.

세부 단계

명령	목적
copy [/noconfirm] {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 TFTP 서버로 복사
copy [**/noconfirm**] {**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 FTP 서버로 복사

명령	목적
copy [**/noconfirm**] {**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 SMB 서버로 복사
copy [**/noconfirm**] {**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	플래시에서 SCP 서버로 복사 **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP 서버에 연결합니다.
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename* **예:** ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg	플래시에서 로컬 플래시 메모리로 복사. 대상 디렉토리가 있어야 합니다. 없는 경우 먼저 **mkdir** 명령을 사용하여 디렉토리를 만듭니다.

컨텍스트 내에서 컨텍스트 컨피그레이션 백업

다중 컨텍스트 모드에서는 어떤 컨텍스트 내에서 다음 백업을 수행할 수 있습니다.

- 실행 중인 컨피그레이션을 시작 컨피그레이션 서버(관리 컨텍스트에 연결됨)에 복사하려면 다음 명령을 입력합니다.

  ciscoasa/contexta# **copy running-config startup-config**

- 실행 중인 컨피그레이션을 컨텍스트 네트워크에 연결된 TFTP 서버에 복사하려면 다음 명령을 입력합니다.

  ciscoasa/contexta# **copy running-config tftp:/***server*[/*path*]/*filename*

터미널 디스플레이에서 컨피그레이션 복사

컨피그레이션을 터미널에 인쇄하려면 다음 명령을 입력합니다.

ciscoasa# **show running-config**

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, 이를테면 **import webvpn** 명령으로 가져온 파일이나 인증서를 백업하려면 다음 단계를 수행합니다.

1단계 다음과 같이 알맞은 **show** 명령을 실행합니다.

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

2단계 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 컨피그레이션 XML 파일, DAP 컨피그레이션 XML 파일을 비롯한 ASA의 컨피그레이션 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 기존 CLI에서는 **copy**, **export**, **import** 명령을 사용하여 개별 파일을 백업하고 복원할 수 있습니다. 그러나 하나의 작업에서 모든 ASA 컨피그레이션 파일을 백업할 수 있는 기능은 없습니다. 스크립트를 실행하면 여러 CLI를 사용할 수 있습니다.

전제 조건

ASA 컨피그레이션의 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.

1단계 시스템의 임의의 위치에 스크립트 파일을 다운로드하거나 잘라내어 붙여넣습니다.

2단계 명령줄에 **Perl** *scriptname*를 입력합니다. 여기서 *scriptname*은 스크립트 파일의 이름입니다.

3단계 **Enter**를 누릅니다.

4단계 시스템에서 각 옵션에 대한 값을 묻습니다. 또는 **Perl** *scriptname* 명령을 입력할 때 옵션에 대한 값을 입력한 다음 **Enter**를 누르는 방법도 있습니다. 어느 쪽이든 스크립트에서는 각 옵션에 대한 값을 입력해야 합니다.

5단계 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
#Function: Backup/restore configuration/extensions to/from a TFTP server.
#Description: The objective of this script is to show how to back up
configurations/extensions before the backup/restore command is developed.
# 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};
  }
}
```

소프트웨어 다운그레이드

버전 8.3으로 다운그레이드할 때 컨피그레이션이 마이그레이션됩니다. 기존 컨피그레이션은 자동으로 플래시 메모리에 저장됩니다. 예를 들어, 버전 8.2(1)에서 8.3(1)로 업그레이드하면 기존 8.2(1) 컨피그레이션은 플래시 메모리에서 8_2_1_0_startup_cfg.sav라는 파일에 저장됩니다.

참고 다운그레이드하기 전에 직접 기존 컨피그레이션을 복원해야 합니다.

이 섹션에서는 다운그레이드 방법을 설명합니다.

- 36-33 페이지의 활성화 키 호환성 정보
- 36-34 페이지의 다운그레이드 수행

활성화 키 호환성 정보

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

- 버전 8.1 이하로 다운그레이드—업그레이드한 다음 *8.2 이전*에 도입되었던 추가 기능 라이센스를 활성화한 경우, 다운그레이드하더라도 활성화 키는 계속 이전 버전과 호환 가능합니다. 그러나 버전 8.2 이상에서 도입되었던 기능 라이센스를 활성화할 경우, 활성화 키는 역호환성을 가지지 않습니다. 호환되지 않는 라이센스 키가 있다면 다음 지침을 참조하십시오.
  - 이전 버전에서 활성화 키를 입력한 적이 있는 경우, ASA에서는 (버전 8.2 이상에서 활성화했던 어떤 신규 라이센스도 포함하지 않고) 그 키를 사용합니다.
  - 신규 시스템이 있는데 이전의 활성화 키가 없을 경우, 그 이전 버전과 호환되는 새 활성화 키를 요청해야 합니다.

- 버전 8.2 이하로 다운그레이드—버전 8.3에서는 더 강력한 시간 기준 키 사용법과 장애 조치 라이센스 변경 사항이 도입되었습니다.
  - 둘 이상의 시간 기준 활성화 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다.
  - 장애 조치 쌍에서 라이센스가 일치하지 않을 경우 다운그레이드하면 장애 조치가 불가능해집니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.

다운그레이드 수행

버전 8.3에서 다운그레이드하려면 다음 단계를 수행합니다.

세부 단계

1단계 다음의 명령을 입력합니다.

```
ciscoasa(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key old_key]
```

여기서 **/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 컨피그레이션의 경로입니다. 기본적으로 이 컨피그레이션은 disk0에 저장됩니다. 8.3 활성화 키 이전으로 되돌려야 하는 경우 기존 활성화 키를 입력할 수 있습니다.

이 명령을 사용하면 다음 기능을 간단하게 완수할 수 있습니다.

1. 부트 이미지 컨피그레이션 지우기(**clear configure boot**)
2. 부트 이미지를 기존 이미지가 되게 설정(**boot system**)
3. (선택 사항) 새 활성화 키 입력(**activation-key**)
4. 실행 중인 컨피그레이션을 시작에 저장(**write memory**). 이 작업은 BOOT 환경 변수를 기존 이미지로 설정합니다. 따라서 다시 로드할 때 기존 이미지가 로드됩니다.
5. 기존 컨피그레이션을 시작 컨피그레이션에 복사(**copy** *old_config_url* **startup-config**)
6. 다시 로드(**reload**)

예:

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

자동 업데이트 구성

자동 업데이트에 대한 정보

자동 업데이트는 자동 업데이트 서버에서 다수의 ASA에 컨피그레이션 및 소프트웨어 이미지를 다운로드할 수 있게 하고 중앙에서 ASA에 대한 기본적인 모니터링을 제공할 수 있는 프로토콜 사양입니다.

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 컨피그레이션과 소프트웨어 이미지를 다운로드하고 중앙에서 또는 여러 위치에서 기본적인 모니터링을 수행하는 데 필요한 인프라를 제공합니다.

자동 업데이트 사양은 자동 업데이트 서버가 ASA에 컨피그레이션 정보를 푸시하고 정보 요청을 보내거나 컨피그레이션 정보를 가져올 수 있도록 ASA에서 정기적으로 자동 업데이트 서버에 폴링하게 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 컨피그레이션이 있어야 합니다.

장애 조치 컨피그레이션에서 자동 업데이트 서버 지원

활성/대기(Active/Standby) 장애 조치 컨피그레이션에서 자동 업데이트 서버를 사용하여 ASA에 소프트웨어 이미지 및 컨피그레이션 파일을 배포할 수 있습니다. 활성/대기 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 활성/대기 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 홈(call home)을 수행합니다. 기본 유닛은 활성 상태에서 콜 홈을 수행할 수 있습니다. 활성 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 활성 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 활성 유닛 또는 대기 유닛의 플랫폼 이미지 파일을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   a. 기본 유닛이 자동 업데이트 서버가 보낸 URL을 사용하여 HTTP 서버에서 해당 파일을 검색합니다.
   b. 기본 유닛이 대기 유닛에 이미지를 복사한 다음 자신의 이미지를 업데이트합니다.
   c. 두 유닛 모두 새 이미지를 가지고 있는 경우 보조(대기) 유닛 먼저 다시 로드됩니다.
   – 보조 유닛이 부팅할 때 히트리스(hitless) 업그레이드를 수행할 수 있는 경우, 보조 유닛이 활성 유닛이 되고 기본 유닛이 다시 로드됩니다. 기본 유닛이 로딩을 마치면 활성 유닛이 됩니다.
   – 대기 유닛이 부팅할 때 히트리스 업그레이드를 수행할 수 없는 경우에는 두 유닛이 동시에 다시 로드됩니다.
   d. 보조(대기) 유닛에만 새 이미지가 있는 경우 보조 유닛만 다시 로드됩니다. 기본 유닛은 보조 유닛이 다시 로드되는 것이 끝날 때까지 기다립니다.
   e. 기본(활성) 유닛에만 새 이미지가 있을 경우, 보조 유닛이 활성 유닛이 되고 기본 유닛이 다시 로드됩니다.
   f. 업데이트 프로세스가 1단계부터 다시 시작합니다.
5. ASA에서 기본 유닛이나 보조 유닛 중 하나의 ASDM 파일을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   a. 기본 유닛이 자동 업데이트 서버가 보낸 URL을 사용하여 HTTP 서버에서 ASDM 이미지 파일을 검색합니다.
   b. 필요하다면 기본 유닛이 대기 유닛에 ASDM 이미지를 복사합니다.
   c. 기본 유닛이 자신의 ASDM 이미지를 업데이트합니다.
   d. 업데이트 프로세스가 1단계부터 다시 시작합니다.

6. 기본 유닛에서 컨피그레이션을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   a. 기본 유닛이 지정된 URL을 사용하여 컨피그레이션 파일을 검색합니다.
   b. 두 유닛에서 동시에 새 컨피그레이션이 기존 컨피그레이션을 대체합니다.
   c. 업데이트 프로세스가 1단계부터 다시 시작합니다.
7. 모든 이미지 및 컨피그레이션 파일에서 체크섬이 일치할 경우 어떤 업데이트도 필요 없습니다. 다음 폴링 시간까지 프로세스는 종료됩니다.

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.

지침 및 제한 사항

- HTTPS가 자동 업데이트 서버와의 통신 프로토콜로 선택된 경우 ASA는 SSL을 사용합니다. 따라서 ASA에 DES 또는 3DES 라이센스가 있어야 합니다.
- 자동 업데이트는 단일 컨텍스트 모드에서만 지원됩니다.

자동 업데이트 서버와의 통신 구성

세부 단계

ASA를 자동 업데이트 클라이언트로 구성하려면 다음 단계를 수행합니다.

1단계 자동 업데이트 서버의 URL을 지정하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# 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.

2단계 (선택 사항) 자동 업데이트 서버와 통신할 때 보낼 디바이스 ID를 식별하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# auto-update device-id {hardware-serial | hostname | ipaddress [if-name]
| mac-address [if-name] | string text}
```

사용되는 식별자는 다음 매개 변수 중 하나를 지정하여 결정합니다.

- *hardware-serial* 인수는 ASA 시리얼 번호를 지정합니다.
- *hostname* 인수는 ASA 호스트 이름을 지정합니다.

- **ipaddress** 키워드는 지정된 인터페이스의 IP 주소를 나타냅니다. 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 MAC 주소를 사용합니다.
- **string** 문자열은 지정된 텍스트 식별자를 나타냅니다. 공백이나 ‘, ", , >, &, ? 문자를 포함할 수 없습니다.

3단계 (선택 사항) 컨피그레이션 또는 이미지 업데이트를 위해 자동 업데이트 서버에 폴링하는 빈도를 지정하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# 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.

4단계 (선택 사항) 특정 시간에 ASA에서 자동 업데이트 서버에 폴링하도록 예약하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# 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 8:00입니다. 그리고 20:00은 오후 8:00입니다.

randomize *minutes* 키워드와 인수는 지정된 시작 시간 이후에 폴링 시간을 무작위화하는 기간을 지정합니다. 범위는 1분부터 1439분까지입니다.

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 1분부터 35791분까지입니다.

5단계 (선택 사항) 자동 업데이트 서버가 일정 기간 접속되지 않은 상태에서 다음 명령을 입력하면 트래픽 전송이 중단됩니다.

```
ciscoasa(config)# auto-update timeout period
```

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 컨피그레이션이 있는지 확인합니다. 이 조건은 시스템 로그 메시지 201008로 보고됩니다.

다음 예에서는 ASA가 외부 인터페이스에서 포트 번호 1742를 사용하여 IP 주소가 209.165.200.224인 자동 업데이트 서버에 폴링하고 인증서를 검증하도록 구성되었습니다.

또한 ASA는 호스트 이름을 디바이스 ID로 사용하고 매주 금요일 및 토요일, 오후 10시~11시의 임의 시간에 자동 업데이트 서버에 폴링하도록 구성되었습니다. 다음 예에서 볼 수 있는 것처럼, 폴링 시도가 실패하면 ASA는 자동 업데이트 서버와의 재연결을 10번 시도하며, 재연결 시도 간격은 3분입니다.

```
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.

1단계 클라이언트 업데이트를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# client-update enable
```

2단계 ASA에 적용하려는 **client-update** 명령을 위한 다음 매개 변수를 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**} 매개 변수는 ASA의 소프트웨어 구성 요소(ASDM 또는 부트 이미지)를 지정합니다.

device-id *dev_string* 매개 변수는 자동 업데이트 클라이언트가 스스로를 식별하는 데 사용하는 고유한 문자열을 지정합니다. 최대 길이는 63자입니다.

family *family_name* 매개 변수는 자동 업데이트 클라이언트가 스스로를 식별하는 데 사용하는 제품군 이름을 지정합니다. asa, pix 또는 최대 7자의 텍스트 문자열이 될 수 있습니다.

rev-nums *rev-nums* 매개 변수는 이 클라이언트의 소프트웨어 또는 펌웨어 이미지를 지정합니다. 임의의 순서로 최대 4개를 입력하고 쉼표로 구분합니다.

type *type* 매개 변수는 클라이언트 업데이트를 알릴 클라이언트의 유형을 지정합니다. 이 명령은 Windows 클라이언트를 업데이트하는 데에도 사용되므로 클라이언트 목록은 여러 Windows 운영 체제를 포함합니다.

url *url-string* 매개 변수는 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 매개 변수를 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 상태 보기

자동 업데이트 상태를 보려면 다음 명령을 입력합니다.

```
ciscoasa(config)# 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 컨피그레이션 기능 내역

표 36-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다..

표 36-2 소프트웨어 및 컨피그레이션 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
SCP(Secure Copy) 클라이언트	9.1(5)/9.2(1)	ASA에서 SCP 클라이언트와 SCP 서버 간의 파일 전송을 지원합니다. 도입된 명령: **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck** 수정된 명령: **copy scp**
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.` 컨피그레이션은 인증없이 명확한 구성으로 마이그레이션될 것입니다. **auto-update server no-verification** 수정된 명령: **auto-update server** {**verify-certificate** | **no-verification**}

37 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 시행하는 syslog 메시지를 식별합니다. 여러 syslog 이벤트를 구성할 수 있지만, syslog 메시지 ID는 단일 이벤트 관리자 애플릿에서 중복되지 않을 수 있습니다.
- Timers — 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. 타이머의 3가지 유형은 다음과 같습니다.
  - Watchdog(주기적) 타이머는 애플릿 작업이 완료된 후 지정된 기간이 지나면 이벤트 관리자 애플릿을 시행하며 자동으로 다시 시작됩니다.
  - Countdown(일회성) 타이머는 지정된 기간이 지나면 이벤트 관리자 애플릿을 한 번 시행하며 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 애플릿의 각 유형에는 하나의 타이머 이벤트만 구성할 수 있습니다.

- None — CLI 또는 ASDM을 사용하여 수동으로 이벤트 관리자 애플릿을 실행할 경우 이벤트가 시행됩니다.
- Crash — ASA가 충돌할 경우 충돌 이벤트가 시행됩니다. **output** 명령의 값에 상관없이, **action** 명령은 crashinfo 파일에 직접 적용됩니다. 출력 결과는 **show tech** 명령 앞에 생성됩니다.

이벤트 관리자 애플릿에 대한 작업

이벤트 관리자 애플릿이 시행되면 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. 명령은 비활성화되므로 입력을 승인하지 않습니다. 다음 세 위치 중 한 곳에 **action** CLI 명령을 보낼 수 있습니다.

- **None** - 기본값이며 출력을 무시합니다.
- **Console** - 출력을 ASA 콘솔로 보냅니다.
- **File** - 출력을 파일로 보냅니다. 다음과 같은 4개의 파일 옵션이 제공됩니다.
  - **Create a unique file** - 이벤트 관리자 애플릿이 호출될 때마다 새로운 고유한 이름의 파일을 생성합니다.
  - **Create/overwrite a file** - 이벤트 관리자 애플릿이 호출될 때마다 지정된 파일을 덮어씁니다.
  - **Create/append to a file** - 이벤트 관리자 애플릿이 호출될 때마다 지정된 파일에 추가합니다. 해당 파일이 아직 없는 경우 파일이 생성됩니다.
  - **Create a set of files** - 이벤트 관리자 애플릿이 호출될 때마다 순환되는 고유한 이름의 파일 집합을 생성합니다.

EEM에 대한 지침

컨텍스트 모드 지침

다중 컨텍스트 모드에서 지원되지 않습니다.

추가 지침

- 충돌이 발생한 동안 ASA의 상태는 일반적으로 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 입력합니다.
- 각 이벤트 관리자 애플릿에는 출력 옵션을 하나만 정의할 수 있습니다.

EEM 구성

EEM 구성은 다음과 같은 작업으로 이루어집니다.

1단계 이벤트 관리자 애플릿을 생성한 다음 다양한 이벤트를 구성합니다. 37-3 페이지의 이벤트 관리자 애플릿 생성 및 이벤트 구성을 참조하십시오.

2단계 이벤트 관리자 애플릿에 대한 작업을 구성한 다음 작업의 출력 대상을 구성합니다. 37-4 페이지의 작업 및 작업의 출력 대상 구성을 참조하십시오.

3단계 이벤트 관리자 애플릿을 실행합니다. 37-6 페이지의 이벤트 관리자 애플릿 실행을 참조하십시오.

이벤트 관리자 애플릿 생성 및 이벤트 구성

이벤트 관리자 애플릿을 생성하고 이벤트를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 이벤트 관리자 애플릿을 생성하고 이벤트 관리자 애플릿 컨피그레이션 모드로 들어갑니다.

event manager applet *name*

예:

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 인수의 길이는 최대 32자 영숫자로 구성할 수 있습니다. 공백은 허용되지 않습니다.

이벤트 관리자 애플릿을 제거하려면 이 명령의 **no** 형식을 입력합니다.

2단계 이벤트 관리자 애플릿을 설명합니다.

description *text*

예:

```
ciscoasa(config-applet)# description applet1example
```

text 인수의 길이는 최대 256자 영숫자로 구성할 수 있습니다. 설명 텍스트가 따옴표 안에 있는 경우 설명 텍스트에 공백을 포함할 수 있습니다.

3단계 지정된 이벤트를 구성하려면 다음 명령 중 하나를 입력합니다. 구성된 이벤트를 제거하려면 각 명령의 **no** 형식을 사용합니다.

- syslog 이벤트를 구성하려면, 이벤트 관리자 애플릿을 시행하는 단일한 syslog 메시지 또는 다양한 syslog 메시지를 식별합니다.

  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 0초마다 1 어러컨스입니다. 유효한 값의 범위는 1~4294967295입니다. **period** *seconds* 키워드-인수 쌍은 이벤트

가 발생해야 하는 시간 간격을 초 단위로 나타내며, 이벤트 관리자 애플릿의 호출 빈도를 구성된 기간 동안 최대한 한 번으로 제한합니다. 유효한 값의 범위는0~604800입니다. 0 값은 정의된 기간이 없음을 의미합니다.

- 구성된 기간당 이벤트가 한 번씩 발생하고 자동으로 다시 시작되도록 구성합니다.

  event timer watchdog time *seconds*

  예:

  ```
  ciscoasa(config-applet)# event timer watchdog time 30
  ```

  초 단위의 범위는 1~604800으로 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
  ```

  초 단위의 범위는 1~604800으로 지정할 수 있습니다. 이 명령의 **no** 형식을 사용하여 Countdown 타이머 이벤트를 제거합니다.

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)에서 23:59:59까지입니다.

- ASA가 충돌할 경우 충돌 이벤트를 시행합니다.

  event crashinfo

  예:

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

  output 명령의 값에 상관없이, **action** 명령은 crashinfo 파일에 직접 적용됩니다. 출력 결과는 **show tech** 명령 앞에 생성됩니다.

작업 및 작업의 출력 대상 구성

작업 및 작업의 출력을 전송할 특정 대상을 구성하려면 다음 단계를 수행합니다.

절차

1단계 이벤트 관리자 애플릿에 대한 작업을 구성합니다.

action *n* **cli command** "*command*"

예:

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

n 옵션은 작업 ID입니다. 유효한 ID 범위는 0~4294967295입니다. *command* 옵션의 값은 따옴표로 감싸야 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. 명령은 비활성화되어 있으므로 입력을 승인하지 않습니다. 명령에 사용 가능한 **noconfirm** 옵션이 있는 경우 이 옵션을 사용합니다.

2단계 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 애플릿에 대한 새 파일에 전송합니다.

  output file new

  예:

  ```
  ciscoasa(config-applet)# output file new
  ```

  파일 이름은 eem-*applet-timestamp*.log 형식으로 되어 있습니다. 여기서 *apple*t은 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 기존 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, 기존 파일은 가장 높은 숫자(*n*-1)로 표시됩니다. *n* 옵션은 순환 값입니다. 유효한 ID 범위는 2~100입니다. 파일 이름 형식은 eem-*applet-x*.log이며, 여기서 *applet*은 애플릿의 이름이고 *x*는 파일 번호입니다.

- **Single Overwritten File** 옵션은 **action** 명령 출력을 단일 파일에 작성하며, 이 파일은 매번 덮어써집니다.

  output file overwrite *filename*

  예:

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

filename 인수는 로컬(ASA에 해당) 파일 이름입니다. 이 명령에서는 FTP, TFTP 및 SMB 대상 파일을 사용할 수도 있습니다.

- **Single Appended File** 옵션은 **action** 명령 출력을 단일한 파일에 작성하지만, 이 파일은 매번 추가됩니다.

  output file append *filename*

  예:

  ```
  ciscoasa(config-applet)# output file append examplefile1
  ```

  filename 인수는 로컬(ASA에 해당) 파일 이름입니다.

이벤트 관리자 애플릿 실행

이벤트 관리자 애플릿을 실행하려면 다음 단계를 수행합니다.

절차

1단계 이벤트 관리자 애플릿을 실행합니다.

event manager run *applet*

예:

```
ciscoasa# event manager run exampleapplet1
```

event none 명령으로 구성하지 않은 이벤트 관리자 애플릿을 실행할 경우, 오류가 발생합니다. *applet* 인수는 이벤트 관리자 애플릿의 이름입니다.

EEM의 예

다음 예에는 매시간마다 차단 유출 정보를 기록하고, 순환되는 로그 파일 집합에 출력을 작성하여 그날 하루의 가치 있는 로그를 보관하는 이벤트 관리자 애플릿이 나와 있습니다.

```
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 예에는 오전 1시마다 ASA를 재부팅하여 필요한 경우 컨피그레이션을 저장하는 이벤트 관리자 애플릿이 나와 있습니다.

```
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 예에는 자정에서 오전 3시 사이에 지정된 인터페이스를 비활성화하는 이벤트 관리자 애플릿이 나와 있습니다.

```
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 commands를 참조하십시오.

- **clear configure event manager**

  이 명령은 이벤트 관리자에서 실행 중인 컨피그레이션을 제거합니다.

- **clear configure event manager applet** *appletname*

  이 명령은 컨피그레이션에서 이름이 지정된 이벤트 관리자 애플릿을 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 running-config event manager**

  이 명령은 이벤트 관리자의 실행 중인 컨피그레이션을 표시합니다.

EEM에 대한 기록

표 37-1 EEM에 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. 도입되거나 수정된 명령: **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**

38 장

문제 해결

이 장에서는 Cisco ASA의 문제 해결 방법을 설명합니다.

디버깅 메시지 보기

디버깅 출력은 CPU 프로세스에서 우선순위가 높기 때문에 시스템을 사용 불가능한 상태로 만들 수 있습니다. 그러므로 구체적인 문제를 해결하거나 Cisco TAC와 문제 해결 세션을 진행할 때만 **debug** 명령을 사용합니다. 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 참조하십시오.

패킷 캡처

패킷 캡처는 연결 문제를 해결하거나 의심스러운 활동을 모니터링할 때 유용할 수 있습니다. 패킷 캡처 서비스를 이용하려면 Cisco TAC에 문의하는 것이 좋습니다.

패킷을 캡처하려면 다음 단계를 수행합니다.

절차

1단계 패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화합니다.

[**cluster exec**] **capture** *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy** | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**interface asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match prot** {**host** *source-ip* | *source-ip mask* |**any**}{**host** *destination-ip* |*destination-ip mask* | **any**} [*operator* **port**]

예:

```
ciscoasa# capture captest interface inside
```

전체 구문 설명은 명령 참조 또는 CLI 도움말(**help capture**)을 참조하십시오. 모든 옵션을 하나의 명령에서 지정할 수 있는 것은 아닙니다. 허용되는 조합에 대해서는 CLI 도움말을 참조하십시오.

여러 트래픽 유형을 캡처하려면 동일한 *capture_name*을 여러 **capture** 문에 사용합니다.

type asp-drop 키워드는 가속화된 보안 경로에 의해 폐기된 패킷을 캡처합니다. 클러스터에서는 유닛 간의 폐기 전달 데이터 패킷도 캡처합니다. 다중 컨텍스트 모드에서는 이 옵션을 시스템 컨텍스트에서 실행하면 모든 폐기된 데이터 패킷이 캡처됩니다. 이 옵션을 사용자 컨텍스트에서 실행하면 그 사용자 컨텍스트에 속한 인터페이스에서 들어온 폐기 데이터 패킷만 캡처됩니다.

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. 캡처할 모든 패킷에 대해 인터페이스를 구성해야 합니다.

데이터 플레인에서 패킷을 캡처하려면 **asa_dataplane** 키워드를 사용합니다. ASA CX 백플레인에서 캡처된 패킷을 필터링하려면 **asa_dataplane** 옵션을 사용하고 다음 지침을 따릅니다. 단일 모드에서는 백플레인 제어 패킷이 액세스 목록을 우회하고 캡처됩니다. 다중 컨텍스트 모드에서는 제어 패킷만 시스템 컨텍스트에서 캡처됩니다. 데이터 패킷은 사용자 컨텍스트에서 캡처됩니다.
access-list 및 **match** 옵션은 사용자 컨텍스트에서만 사용 가능합니다.

클러스터 제어 링크에서 트래픽을 캡처하려면 **cluster** 키워드를 사용합니다. **type lacp**를 구성한 경우 nameif 이름 대신 물리적 인터페이스 ID를 지정합니다.

match 키워드는 프로토콜, 소스 및 목적지 IP 주소, 선택적 포트 매칭을 캡처합니다. 하나의 명령에서 이 키워드를 최대 3번 사용할 수 있습니다. *operator*는 다음 중 하나가 될 수 있습니다.

- **lt**—보다 작음
- **gt**—보다 큼
- **eq**—같음

type raw-data 키워드는 인바운드 및 아웃바운드 패킷을 캡처합니다. 이는 기본 설정입니다.

real-time 키워드는 캡처된 패킷을 실시간으로 계속 표시합니다. 실시간 패킷 캡처를 종료하려면 **Ctrl + c** 를 입력합니다.캡처를 영구적으로 삭제하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션은 **raw-data** 및 **asp-drop** 캡처에만 적용됩니다. **cluster exec capture** 명령을 사용할 때는 이 옵션이 지원되지 않습니다.

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 사용하려 하면 오류가 표시됩니다.

클러스터링 환경에서 패킷 캡처

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. **cluster exec** 키워드는 클러스터 전반의 캡처를 활성화하기 위해 **capture** 명령의 앞에 입력하는 새로운 키워드입니다.

"cluster" 인터페이스 이름은 클러스터 제어 링크의 기본 이름이며 구성 불가합니다. 클러스터 제어 링크 인터페이스에서 트래픽을 캡처하려면 "cluster"를 인터페이스 이름으로 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.

다중 컨텍스트 모드에서는 클러스터 인터페이스가 시스템 컨텍스트에 속해 있지만, 사용자 컨텍스트에서 그 인터페이스를 볼 수 있으므로 클러스터 링크의 캡처를 구성할 수 있습니다. 시스템 컨텍스트에서든 컨트롤 플레인 패킷과 데이터 플레인 패킷을 모두 사용할 수 있습니다. 데이터 플레인은 LU 패킷과 시스템 컨텍스트에 속한 전달 데이터 패킷만 캡처합니다. 사용자 컨텍스트에서는 컨트롤 플레인 패킷이 보이지 않습니다. 지정된 사용자 컨텍스트에 속한 전달 데이터 패킷과 LU 패킷만 캡처됩니다. 보안을 위해 각 컨텍스트에서는 그 컨텍스트에 속한 패킷만 볼 수 있습니다.

패킷 캡처 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.
- 다중 컨텍스트 모드의 클러스터 제어 링크 캡처에서는 클러스터 제어 링크에서 전송된, 해당 컨텍스트와 관련된 패킷만 캡처됩니다.
- 인라인 SGT 태그 처리된 패킷의 경우, 캡처된 패킷은 PCAP 뷰어에서 이해하지 못할 추가 CMD 헤더를 포함합니다.
- 다중 컨텍스트 모드에서는 시스템 영역에서만 **copy capture** 명령을 사용할 수 있습니다. 구문은 다음과 같습니다.

  copy /pcap capture:*Context-name*/*in-cap* **tftp**:

  여기서 *in-cap*은 컨텍스트 *context-name*에 구성된 캡처입니다.
- **cluster exec capture realtime** 명령은 지원되지 않습니다. 다음과 같은 오류 메시지가 표시됩니다.

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 공유 VLAN은 다음 지침이 적용됩니다.
  - VLAN에서는 하나의 캡처만 구성할 수 있습니다. 공유 VLAN에서 다중 컨텍스트 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.
- 일반적으로 캡처 구성은 캡처할 트래픽에 매칭하는 ACL을 구성하는 것입니다. 트래픽 패턴에 매칭하는 ACL이 구성된 다음에는 캡처를 정의하고 이 ACL을 캡처에 연결하며 캡처가 구성될 인터페이스와도 연결해야 합니다.
- 클러스터 전반의 캡처를 수행한 다음 동일한 클러스터 전반 캡처 파일을 TFTP 서버에 복사하려면 마스터 유닛에서 다음 명령을 입력합니다.

  ```
  ciscoasa (cfg-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.pcap
  ```

- 유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일 이름에는 유닛 이름이 자동으로 추가됩니다(예: filename_A.pcap, filename_B.pcap 등). 이 예에서는 A와 B가 클러스터 유닛 이름입니다. 파일 이름의 끝에 유닛 이름을 추가하면 다른 목적지 이름이 생성됩니다.
- 지정된 인터페이스에서 클러스터 전반의 캡처를 활성화하려는 경우, 예에 나온 각 명령의 앞에 **cluster exec** 키워드를 추가하면 됩니다. 이 **capture** 명령은 마스터 유닛에서 슬레이브 유닛으로만 복제될 수 있습니다. 그러나 이 **capture** 명령 중 하나를 사용하여 로컬 유닛에 대해 지정된 인터페이스의 캡처를 구성하는 것은 가능합니다.

예

다음 예는 클러스터 전반의 LACP 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# cluster exec capture lacp type lacp interface gigabitEthernet0/0
```

다음 예는 클러스터링 링크에서 제어 경로 패킷의 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
```

다음 예는 클러스터링 링크에서 데이터 경로 패킷의 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
```

다음 예는 클러스터를 지나는 데이터 경로 트래픽을 캡처하는 방법을 보여줍니다.

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match udp host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

다음 예는 실제 소스를 실제 목적지에 매칭하는 흐름의 로직 업데이트 메시지를 캡처하는 방법 그리고 실제 소스를 실제 목적지에 매칭하는, CCL을 통해 전달되는 패킷을 캡처하는 방법을 보여줍니다.

```
ciscoasa (config)# access-list dp permit ip real_src real_dst
```

다음 예는 icmp echo request/response와 같이 한 ASA에서 다른 ASA로 전달되는 특정 유형의 데이터 플레인 메시지를 **match** 키워드 또는 그 메시지 유형의 ACL을 사용하여 캡처하는 방법을 보여줍니다.

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

다음 예는 클러스터 제어 링크에서 ACL 103을 사용하여 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster access-list 103
```

앞의 예에서 A와 B가 CCL 인터페이스의 IP 주소일 경우 이 두 유닛 간에 전송된 패킷만 캡처됩니다.

A와 B가 디바이스를 지나는 트래픽의 IP 주소라면 다음과 같이 됩니다.

- 전달된 패킷은 평소와 같이 캡처됩니다. 단, 소스 및 목적지 IP 주소가 ACL과 매칭되어야 합니다.
- 데이터 경로 로직 업데이트 메시지는 A와 B 간의 흐름 또는 ACL(예: access-list 103)을 위한 것일 때만 캡처됩니다. 캡처는 임베드된 흐름의 5-튜플에 매칭합니다.

UDP 패킷의 소스 및 목적지 주소가 CCL 주소이지만 이 패킷이 주소 A 및 B와 연결된 흐름을 업데이트하는 것이라면 이 역시 캡처됩니다. 즉 패킷에 임베드된 주소 A와 B가 매칭되는 한 역시 캡처됩니다.

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 참조하십시오.

코어덤프 보기

코어덤프는 프로그램이 비정상적으로 종료했거나 충돌했을 때 실행 중이던 프로그램의 스냅샷입니다. 코어덤프는 오류를 진단하거나 디버깅하는데 그리고 향후 오프사이트 분석을 위해 충돌 상황을 저장하는 데 사용합니다. Cisco TAC에서 ASA 또는 ASAv의 애플리케이션이나 시스템 충돌 문제를 해결하기 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 보여줍니다.

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** 탭을 클릭하고 **Advanced**를 클릭하여 **Chart Options** 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 uage는 다음과 같이 계산합니다.

사용량(MHz) / 가상 CPU 수 x 코어 주파수

사용량(MHz)을 비교하면 vCenter 수치와 ASAv 수치가 동일합니다. vCenter 그래프에 의거하여 MHz % CPU usage는 다음과 같이 계산됩니다.

60/(2499 x 1 vCPU) = 2.4

9 파 트

로깅 , SNMP, Smart Call Home

39 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 컨피그레이션 파일에 따라 인쇄합니다. 이 로깅 양식을 통해 로그를 안전하게 장기 보관할 수 있습니다. 로그는 일상적인 문제 해결과 사고 처리에 모두 유용합니다.

Cisco ASA 시스템 로그는 ASA 모니터링 및 문제 해결에 필요한 정보를 제공합니다. 로깅 기능을 사용하면 다음을 할 수 있습니다.

- 어떤 syslog 메시지를 기록해야 하는지 지정합니다.
- syslog 메시지의 심각도를 비활성화하거나 변경합니다.
- 내부 버퍼, 하나 이상의 syslog 서버, ASDM, SNMP 관리 스테이션, 지정된 이메일 주소 또는 텔넷 및 SSH 세션을 포함하여 syslog 메시지를 보낼 장소를 하나 이상 지정합니다.
- 심각도 수준 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 사용자 지정 메시지 목록별로 syslog 메시지를 필터링합니다.

다중 컨텍스트 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 컨텍스트 이름을 포함하도록 ASA 및 ASASM을 구성하면 하나의 syslog 서버로 전송되는 컨텍스트 메시지를 구분하는 데 도움이 됩니다. 이 기능을 사용하면 관리자 컨텍스트에서 전송된 메시지와 시스템에서 전송된 메시지를 구분하는 데 도움이 됩니다. 시스템 실행 공간에서 발생한 메시지는 **시스템**의 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 및 ASASM 보안 정책에서 허용된 연결. 이러한 메시지는 보안 정책의 허점을 찾는 데 도움이 됩니다.
- ASA 및 ASASM 보안 정책에서 거부된 연결. 이러한 메시지는 보안된 내부 네트워크로 어떤 유형의 활동이 전송되는지 보여줍니다.
- ACE 거부 속도 로깅 기능을 사용하면 ASA 또는ASA Services Module에서 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 시설 코드입니다. 이 값은 항상 ASA입니다.
수준	1부터 7까지입니다. 수준은 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

표 39-1 syslog 메시지 심각도 수준을 나열합니다. ASDM 로그 뷰어에서 구별하기 쉽도록 각 심각도에 컬러를 할당할 수 있습니다. syslog 메시지 컬러 설정을 구성하려면 **Tools > Preferences > Syslog** 탭을 선택하거나 로그 뷰어의 툴바에서 **Color Settings**를 클릭하십시오.

표 39-1 Syslog 메시지 심각도 수준

수준 번호	심각도	설명
0	**긴급 상황**	시스템을 사용할 수 없습니다.
1	**알림**	즉각적인 행동이 필요합니다.
2	**위험**	심각한 상태입니다.
3	**오류**	오류 상태입니다.
4	**경고**	경고 상태입니다.
5	**알림**	일반적이지만 중요한 상태입니다.
6	**정보**	정보 메시지만 해당됩니다.
7	**디버깅**	디버깅 메시지만 해당됩니다.

참고 ASA 및 ASASM은 심각도 수준 0(응급)으로 syslog 메시지를 생성하지 않습니다. 이 수준은 UNIX syslog 기능과의 호환성을 위해 **logging** 명령에서 제공되지만 ASA에서 사용되지 않습니다.

메시지 클래스와 Syslog ID의 범위

각 syslog 메시지 클래스와 거기 연결된 syslog 메시지 ID의 범위 목록은 syslog 메시지 가이드에서 참조하십시오.

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 ASA 및 ASASM을 구성할 수 있습니다.

구체적으로 syslog 메시지가 다음 기준에 따라 출력 대상으로 전송되도록 ASA 및 ASASM을(를) 구성할 수 있습니다.

- Syslog 메시지 ID 번호
- Syslog 메시지 심각도 수준
- Syslog 메시지 클래스(ASA 및 ASASM의 기능 영역에 해당)

출력 대상을 설정할 때 지정할 수 있는 메시지 목록을 생성함으로써 이 기준을 사용자 지정할 수 있습니다. 또는 특정 메시지 클래스를 메시지 목록과는 별개로 각 출력 대상 유형으로 전송하도록 ASA 또는 ASASM을 구성할 수도 있습니다.

syslog 메시지 클래스를 2가지 방법으로 사용할 수 있습니다.

- **logging class** 명령을 사용하여 전체 syslog 메시지 카테고리에 대한 출력 위치를 지정합니다.

- **logging list** 명령을 사용하여 메시지 클래스를 지정하는 메시지 목록을 생성합니다.

syslog 메시지 클래스는 ASA 및 ASASM의 기능에 해당하는 유형에 따라 syslog 메시지를 분류하는 방식을 제공합니다. 예를 들어 vpnc 클래스는 VPN 클라이언트를 의미합니다.

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.

사용자 정의 메시지 목록

사용자 정의 메시지 목록을 만드는 것은 어떤 syslog 메시지를 어떤 출력 대상으로 보낼지 제어하는 유연한 방법입니다. 사용자 정의 syslog 메시지 목록에서 심각도, 메시지 ID, syslog 메시지 ID 또는 메시지 클래스 등의 기준을 사용하여 syslog 메시지 그룹을 지정합니다.

예를 들어 메시지 목록을 사용하여 다음을 할 수 있습니다.

- 심각도 수준이 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** 명령어를 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

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

- syslog 서버는 syslogd라는 서버 프로그램을 실행해야 합니다. Windows(Windows 95 및 Windows 98 제외) 운영 체제에는 syslog 서버가 포함되어 있습니다. Windows 95 및 Windows 98의 경우 다른 업체로부터 syslogd 서버를 구해야 합니다.
- ASA 또는 ASASM에서 생성된 로그를 보려면 로깅 출력 대상을 지정해야 합니다. 로깅 출력 대상을 지정하지 않고 로깅을 활성화하면 ASA 및 ASASM은 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 각 s.
- 대기 ASA에서는 TCP를 통한 syslog 전송이 지원되지 않습니다.
- ASA는 단일 컨텍스트 모드에서 **logging host** 명령을 통해 16개 syslog 서버의 컨피그레이션을 지원합니다. 다중 컨텍스트 모드에서는 컨텍스트당 서버 4개로 제한됩니다.
- syslog 서버는 ASA 및 ASASM을 통해 도달할 수 있습니다. syslog 서버가 도달할 수 없는 인터페이스의 ICMP 도달 불가 메시지를 거부하고 syslog를 동일한 서버로 전송하도록 ASASM을 구성할 수 있습니다. 모든 심각도 수준에 대해 로깅을 활성화했는지 확인합니다. syslog 서버가 충돌하지 않게 하려면 syslogs 313001, 313004 및 313005의 생성을 억제하십시오.
- 액세스 목록만 일치하도록 사용자 정의 메시지 목록을 사용할 경우 로깅 심각도 수준이 디버깅(수준 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 수준을 디버깅으로 확실히 변경할 경우 로깅 컨피그레이션 자체도 변경해야 합니다.

  다음은 로깅 심각도 수준이 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
```

로깅 구성

이 섹션에서는 로깅 구성 방법을 설명합니다.

1단계 로깅을 활성화합니다. 39-6 페이지의 로깅 활성화를 참조하십시오.

2단계 syslog 메시지의 출력 대상을 구성합니다. 39-6 페이지의 출력 대상 구성을 참조하십시오.

참고 최소 컨피그레이션은 ASA 및 ASASM에서 하려고 하는 작업과 syslog 메시지 처리 요구 사항이 무엇인지에 따라 달라집니다.

로깅 활성화

로깅을 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 로깅을 활성화합니다.

```
logging enable
```

예:

```
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.

절차

1단계 메시지를 syslog 서버로 전송하도록 ASA 및 ASASM을 구성합니다.

```
logging host interface_name syslog_ip [tcp[/port] | udp[/port] [format emblem]]
```

예:

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem
```

format emblem 키워드는 UDP만 있는 syslog 서버에 대한 키워드는 EMBLEM 형식 로깅을 가능하게 합니다. *interface_name* 인수t 는 syslog 서버를 액세스할 인터페이스를 지정합니다. *syslog_ip* 인수는 syslog 서버의 IP 주소를 지정합니다. **tcp**[*/port*] 또는 **udp**[*/port*] 키워드 및 인수 쌍은 ASA 및 ASASM이 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 Services Module을 통한 새로운 연결이 차단됩니다. TCP syslog 서버에 연결에 관계없이 새로운 연결을 허용하려면 3단계를 참조하십시오. UDP를 지정한 경우 ASA 및 ASASM은 syslog 서버 작동 여부에 관계없이 새로운 연결을 허용합니다. 각 프로토콜에 대한 유효한 포트 값은 1025부터 65535입니다. 기본 UDP 포트는 514입니다. 기본 TCP 포트는 1470입니다.

2단계 어떤 syslog 메시지를 syslog 서버에 전송할지 지정합니다.

logging trap {*severity_level* | *message_list*}

예:

```
ciscoasa(config)# logging trap errors
```

심각도 수준 숫자(1~7) 또는 이름을 지정할 수 있습니다. 예를 들어 심각도를 3으로 설정한 경우 ASA 및 ASASM은 심각도 수준 3, 2, 1에 대해 syslog 메시지를 보냅니다. syslog 서버로 전송할 syslog 메시지를 식별하는 사용자 지정 메시지 목록을 지정할 수 있습니다.

3단계 (선택 사항)TCP 연결 syslog 서버가 다운되었을 때 새로운 연결을 차단하려면 이 기능을 비활성화하십시오.

logging permit-hostdown

예:

```
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.

4단계 (선택 사항) 로깅 시설을 대부분의 UNIX 시스템이 기대하는 값인 20 외의 다른 값으로 설정합니다.

로그 시설 *번호*

예:

```
ciscoasa(config)# logging facility 21
```

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.

절차

1단계 임시 저장 위치 역할을 하는 내부 로그 버퍼로 어떤 syslog 메시지를 전송할지 지정합니다.

logging buffered {*severity_level* | *message_list*}

예:

```
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.

2단계 내부 녹음 버퍼의 크기를 변경합니다. 기본 버퍼 크기는 4KB입니다.

logging buffer-size *bytes*

예:

```
ciscoasa(config)# logging buffer-size 16384
```

3단계 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(가) 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 path username 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 디렉토리에 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
  ```

이메일 주소로 Syslog 메시지 보내기

이메일 주소로 syslog 메시지를 보내려면 다음 단계를 수행하십시오.

절차

1단계 이메일 주소로 어떤 syslog 메시지를 보낼지 지정합니다.

logging mail {*severity_level* | *message_list*}

예:

```
ciscoasa(config)# logging mail high-priority
```

이메일로 보낼 때는 이메일 메시지의 제목 줄에 syslog 메시지가 표시됩니다. 따라서 심각, 경고 및 긴급과 같이 높은 심각도 수준으로 syslog 메시지를 관리자에게 알리도록 이 옵션을 구성하는 것이 좋습니다.

2단계 syslog 메시지를 이메일 주소로 보낼 때 사용할 소스 이메일 주소를 지정합니다.

logging from-address *email_address*

예:

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

3단계 syslog 메시지를 이메일 주소로 보낼 때 사용할 수신자 이메일 주소를 지정합니다.

logging recipient-address *e-mail_address* [*severity_level*]

예:

```
ciscoasa(config)# logging recipient-address admin@example.com
```

4단계 syslog 메시지를 이메일 주소로 보낼 때 사용할 SMTP 서버를 지정합니다.

smtp-server *ip_address*

예:

```
ciscoasa(config)# smtp-server 10.1.1.1
```

Syslog 메시지를 ASDM에 전송

syslog 메시지를 ASDM에 보내려면 다음 단계를 수행합니다.

절차

1단계 ASDM으로 어떤 syslog 메시지를 보낼지 지정합니다.

logging asdm {*severity_level* | *message_list*}

예:

```
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.

2단계 ASDM 로그 버퍼에 보존할 syslog 메시지의 수를 지정합니다.

logging asdm-buffer-size *num_of_msgs*

예:

```
ciscoasa(config)# logging asdm-buffer-size 200
```

ASDM 로그 버퍼의 현재 내용을 비우려면 **clear logging asdm** 명령을 입력합니다.

Syslog 메시지를 콘솔 포트로 전송

syslog 메시지를 콘솔 포트로 보내려면 다음 단계를 수행하십시오.

절차

1단계 콘솔 포트로 어떤 syslog 메시지를 보낼지 지정합니다.

logging console {*severity_level* | *message_list*}

예:

```
ciscoasa(config)# logging console errors
```

Syslog 메시지를 SNMP 서버로 전송

SNMP 서버로 로깅을 활성화하려면 다음 단계를 수행하십시오.

1단계 SNMP 로깅을 활성화하고 어떤 메시지를 SNMP 서버로 보낼지 지정합니다.

logging history [*logging_list* | *level*]

예:

```
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 수행하십시오.

절차

1단계 어떤 syslog 메시지를 텔넷 혹은 SSH 세션으로 보낼지 지정합니다.

logging monitor {*severity_level* | *message_list*}

예:

```
ciscoasa(config)# logging monitor 6
```

2단계 현재 세션에 대한 로깅만 허용합니다.

terminal monitor

예:

```
ciscoasa(config)# terminal monitor
```

로그아웃하고 다시 로그인하면 이 명령을 다시 입력해야 합니다. 현재 세션에 대한 로깅을 비활성화하려면 **terminal no monitor** 명령을 입력합니다.

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.

절차

1단계 내부 로그 버퍼에 저장할 메시지를 선택할 기준을 지정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA은(는) 심각도 수준 3, 2, 1에 대해 syslog 메시지를 보냅니다.

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

예:

```
ciscoasa(config)# logging list notif-list level 3
```

name 인수는 목록의 이름을 지정합니다. **level** *level* 키워드 및 인수 쌍은 심각도 수준을 지정합니다. **class** *message_class* 키워드 및 인수 쌍은 특정 메시지 클래스를 지정합니다. **message** *start_id*[**-***end_id*] 키워드 및 인수 쌍은 개별 syslog 메시지 숫자 또는 숫자 범위를 지정합니다.

참고 심각도 수준 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.

2단계 (선택 사항) 목록에 메시지 선택 기준을 더 추가합니다.

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

예:

```
ciscoasa(config)# logging list notif-list message 104024-105999

ciscoasa(config)# logging list notif-list level critical

ciscoasa(config)# logging list notif-list 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 수준이 중요 이상인 모든 syslog 메시지(긴급, 경고 또는 중요).
- 심각도 수준이 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.

EMBLEM 형식의 Syslog 메시지를 Syslog 서버에 생성

EMBLEM 형식의 syslog 메시지를 syslog 서버에 생성하려면 다음 단계를 수행하십시오.

절차

1단계 포트 514를 사용하여 UDP를 통해 EMBLEM 형식의 syslog 메시지를 syslog 서버로 보냅니다.

logging host *interface_name ip_address* {**tcp**[*/port*] | **udp**[*/port*]} [**format emblem**]

예:

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
```

format emblem 키워드는 syslog 서버에 대한 EMBLEM 형식 로깅을 가능하게 합니다(UDP만 해당). *interface_name* 인수t 는 syslog 서버를 액세스할 인터페이스를 지정합니다. *ip_address* 인수는 syslog 서버의 IP 주소를 지정합니다. **tcp**[/port] 또는 *udp*[*/port*] 키워드 및 인수 쌍은 ASA 및 ASASM이 TCP 또는 UDP를 사용하여 syslog 서버로 syslog 메시지를 전송하도록 지정합니다.

UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA 및 ASASM을 구성할 수 있지만 둘 다 사용할 수는 없습니다. 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 수준을 경고로 제한하십시오.

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.

참고 대기 ASA에서는 TCP를 통한 syslog 전송이 지원되지 않습니다.

다른 출력 대상으로 EMBLEM 형식의 Syslog 메시지 생성

EMBLEM 형식의 syslog 메시지를 다른 출력 대상으로 생성하려면 다음 단계를 수행하십시오.

절차

1단계 EMBLEM 형식의 syslog 메시지를 텔넷 또는 SSH 세션과 같은 syslog 서버 이외의 출력 대상으로 보냅니다.

logging emblem

예:

```
ciscoasa(config)# logging emblem
```

로그에 사용할 수 있는 내부 플래시 메모리양을 변경

로그에 사용할 수 있는 내부 플래시 메모리의 양을 변경하려면 다음 단계를 수행하십시오.

절차

1단계 로그 파일 저장에 사용 가능한 내부 플래시 메모리의 최대량을 지정합니다.

logging flash-maximum-allocation *kbytes*

예:

```
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 최소 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.

2단계 ASA 또는 ASASM이 로그 파일을 저장하기 위해 필요한 최소 내부 플래시 메모리 여유 공간을 지정합니다.

logging flash-minimum-free *kbytes*

예:

```
ciscoasa(config)# logging flash-minimum-free 4000
```

로깅 대기열 구성

로깅 대기열을 구성하려면 다음 작업을 수행합니다.

절차

1단계 ASA 및 ASASM이 구성된 출력 대상으로 보내기 전에 대기열에 저장할 수 있는 syslog 메시지의 수를 지정합니다.

logging queue *message_count*

예:

```
ciscoasa(config)# logging queue 300
```

ASA 및 ASASM은 메모리에 고정된 개수의 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.

클래스의 모든 Syslog 메시지를 지정된 출력 대상으로 전송

클래스의 모든 syslog 메시지를 지정된 출력 대상으로 전송하려면 다음 단계를 수행하십시오.

절차

1단계 지정된 출력 대상 명령에서 컨피그레이션을 무시합니다. 예를 들어 심각도 수준 7의 메시지가 내부 로그 버퍼로 전송되도록 지정하고 심각도 수준 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*]

예:

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered, **history**, **mail**, **monitor** 및 **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 엔트리당 하나의 대상을 선택합니다. 클래스가 2개 이상의 대상으로 전송되도록 지정하려면 각 출력 대상에 대해 새로운 명령을 입력합니다.

안전한 로깅 활성화

안전한 로깅을 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 안전한 로깅을 활성화합니다.

logging host *interface_name syslog_ip* [**tcp**/port | **udp**/*port*] [**format emblem**] [**secure**]

예:

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
```

interface_name 인수는 syslog 서버가 상주하는 인터페이스를 지정합니다. *syslog_ip* 인수는 syslog 서버의 IP 주소를 지정합니다. *port* 인수는 syslog 서버가 syslog 메시지에 대해 듣는 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 가능하게 합니다. **secure** 키워드는 원격 로깅 호스트로의 연결이 TCP에 한해 SSL/TLS를 사용하도록 지정합니다.

참고 안전한 로깅은 UDP를 지원하지 않습니다. 이 프로토콜을 사용하려고 하면 오류가 발생합니다.

디바이스 ID를 Non-EMBLEM 형식 Syslog 메시지에 포함

디바이스 ID를 non-EMBLEM 형식 syslog 메시지에 포함하려면 다음 단계를 수행하십시오.

절차

1단계 ASA 또는 ASASM을 구성하여 non-EMBLEM-형식 syslog 메시지에 디바이스 ID를 포함합니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다.

logging device-id {**cluster-id** |**context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

예:

```
ciscoasa(config)# logging device-id hostname

ciscoasa(config)# logging device-id context-name
```

context-name 키워드는 현재 컨텍스트의 이름을 디바이스 ID로 사용하도록 지정합니다(다중 컨텍스트 모드에만 적용). 다중 컨텍스트 모드에서 관리자 컨텍스트 모드를 위해 디바이스 ID 로깅을 활성화하는 경우 시스템 실행 공간에서 발생하는 메시지는 **시스템**의 디바이스 ID를 사용하고 관리자 컨텍스트에서 발생하는 메시지는 관리자 컨텍스트의 이름을 디바이스 ID로 사용합니다.

참고 ASA 클러스터에서는 항상 선택된 인터페이스에 대해 마스터 유닛 IP 주소를 사용하십시오.

cluster-id 키워드는 클러스터에서 개별 ASA 유닛의 부트 컨피그레이션 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 지정된ASA 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.

Syslog 메시지에 날짜와 시간 포함

syslog 메시지에 날짜와 시간을 포함하려면 다음 단계를 수행하십시오.

절차

1단계 syslog 메시지가 생성된 날짜 및 시간을 포함하도록 지정합니다.

logging timestamp

예:

```
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 수행하십시오.

절차

1단계 ASA 또는 ASASM이 특정 syslog 메시지를 생성하지 못하게 합니다.

no logging message *syslog_id*

예:

```
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 수준을 변경하려면 다음 단계를 수행하십시오.

절차

1단계 Syslog 메시지의 심각도 수준을 지정합니다.

logging message *syslog_id* **level** *severity_level*

예:

```
ciscoasa(config)# logging message 113019 level 5
```

syslog 메시지의 심각도 수준을 설정으로 되돌리려면 **no logging message** *syslog_id* **level** *severity_level* 명령(예: **no logging message 113019 level 5**)을 입력합니다. 모든 수정된 syslog 메시지의 심각도 수준을 설정으로 되돌리려면 **clear configure logging level** 명령을 사용합니다.

Syslog 메시지 생성 속도 제한

syslog 메시지 생성 속도를 제한하려면 다음 단계를 수행하십시오.

절차

1단계 지정된 심각도 수준(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*

예:

```
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 입력하십시오. 로깅 속도 제한을 재설정하려면 **clear configure logging rate-limit** 명령을 입력합니다.

로그 모니터링

로깅 상태 모니터링을 위해 다음 commands를 참조합니다.

- **show logging**

  이 명령어는 심각도 수준을 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 수준이 수정된 syslog 메시지와 비활성화된 syslog 메시지 목록을 표시합니다.

- **show logging message** *message_ID*

  이 명령은 특정 syslog 메시지의 심각도 수준을 보여줍니다.

- **show logging queue**

  이 명령은 로깅 대기열과 대기열 통계를 보여줍니다.

- **show logging rate-limit**

  이 명령어는 허용되지 않는 syslog 메시지를 보여줍니다.

- **show running-config logging rate-limit**

  이 명령어는 현재 로깅 속도 제한 설정을 보여줍니다.

로깅의 예

다음 예는 **show logging** 명령에 대해 표시되는 로깅 정보의 예를 보여줍니다.

```
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
```

다음 예는 syslog 메시지 활성화 여부와 지정된 syslog 메시지의 심각도 수준을 제어하는 방법을 보여줍니다.

```
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 39-2 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. 도입된 명령: **logging rate-limit**
로깅 목록	7.2(1)	다른 명령에서 다양한 기준(로깅 수준, 이벤트 클래스 및 메시지 ID)으로 메시지를 지정하는 데 사용할 로깅 목록을 생성합니다. 도입된 명령: **logging list**
안전한 로깅	8.0(2)	원격 로깅 호스트로의 연결이 SSL/TLS를 사용할지 지정합니다. 이 옵션은 선택된 프로토콜이 TCP인 경우에만 유효합니다. 수정된 명령: **logging host**.
로깅 클래스	8.0(4), 8.1(1)	ipaa 이벤트 클래스 로깅 메시지에 대한 지원이 추가되었습니다. 수정된 명령: **logging class**

표 39-2 로깅 내역(계속)

기능 이름	플랫폼 릴리스	설명
로깅 클래스 및 저장된 로깅 버퍼	8.2(1)	dap 이벤트 클래스 로깅 메시지에 대한 지원이 추가되었습니다. 수정된 명령: **logging class** 저장된 로깅 버퍼 지우기에 대한 지원이 추가되었습니다(ASDM, 내부, FTP 및 플래시). 도입된 명령: **clear logging queue bufferwrap**
비밀번호 암호화	8.3(1)	비밀번호 암호화 지원이 추가되었습니다. 수정된 명령: **logging ftp server**
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** 명령. 수정된 명령: **show logging**. 다음 syslog 메시지를 도입했습니다. 414005, 414006, 414007 및 414008
클러스터링	9.0(1)	ASA 5580 및 5585-X에서의 클러스터링 환경에서 syslog 메시지 생성에 대한 지원을 추가했습니다. 수정된 명령: **logging device-id**

40 장

SNMP

이 장에서는 Cisco ASA를 모니터링하기 위한 SNMP(Simple Network Management Protocol) 구성 방법을 설명합니다.

SNMP 소개

SNMP는 네트워크 디바이스 간의 관리 정보 교환을 촉진하기 위한 애플리케이션 계층 프로토콜이며 TCP/IP 프로토콜 군의 일부입니다. ASA, ASAv 및 ASASM은(는) SNMP 버전 1, 2c 및 3을 사용하여 네트워크 모니터링을 지원하고 모든 3개 버전의 동시 사용도 지원합니다. 인터페이스에서 실행되는 SNMP 에이전트를 사용하면 HP OpenView와 같은 NMS(네트워크 관리 시스템)을 통해 ASA ASA 및 ASASM을(를) 모니터링할 수 있습니다. ASA, ASAv 및 ASASM은(는) 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.

ASA, ASAv 및 ASASM을(를) NMS로의 특정 이벤트(알림 포함)에 대해 관리 디바이스에서 관리 스테이션으로 전송되는 요청하지 않은 메시지인 트랩을 보내도록 구성하거나 NMS를 사용하여 ASA에서 MIB(Management Information Bases)를 찾아볼 수 있습니다. MIB는 정의 모음이고 ASA, ASAv 및 ASASM은 각 정의에 대한 값 데이터베이스를 유지합니다. MIB를 찾아보는 것은 NMS에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 발행하는 것을 의미합니다.

ASA, ASAv 및 ASASM에는 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,ASAv 또는ASASM SNMP 에이전트는 관리 스테이션이 정보를 요구할 때 응답하기도 합니다.

SNMP 용어

표 40-1은 SNMP에서 작업할 때 일반적으로 쓰이는 용어를 나열합니다.

표 40-1 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(Management Information Base)에 대한 액세스를 제어합니다. • SET 작업을 허용하지 않습니다.
브라우징	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(Management Information Base)	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(Network Management Station)	SNMP 이벤트를 모니터링하고 ASA, ASAv 및 ASASM 등의 디바이스를 관리하도록 설정된 PC나 워크스테이션입니다.
OID(Object Identifier)	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 messages와 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, ASAv또는 ASASM 소프트웨어로 컴파일됩니다.

필요한 경우 다음 위치에서 RFC, 표준 MIB 및 표준 트랩을 다운로드할 수 있습니다.

http://www.ietf.org/

ftp://ftp-sj.cisco.com/pub/mibs

다음 위치에서 Cisco MIB, 트랩 및 OID의 전체 목록을 다운로드하십시오.

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

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 대한 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 명령어는 Cisco TAC 전용입니다. 이 명령어를 사용하기 전에 Cisco TAC에 연락하십시오.

다음은 **show snmp-server oidlist** 명령의 출력 예시입니다.

```
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 수준 제품에는 MIB II sysObjectID로 사용하기 위한 SNMP OID (object identifier)가 있습니다. CISCO-PRODUCTS-MIB는 SNMPv2-MIB의 sysObjectID 객체에서 보고될 수 있는 OID를 포함합니다. 이 값을 사용하여 모델 유형을 식별할 수 있습니다. 표 40-2는 ASA 모델에 대한 sysObjectID OID를 나열합니다.

표 40-2 SNMP Object Identifier

제품 ID	sysObjectID	모델 번호
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 컨텍스트
ASA5585-SSP20	ciscoASA5585Ssp20sc (ciscoProducts 1199)	ASA 5585-X SSP-20 보안 컨텍스트
ASA5585-SSP40	ciscoASA5585Ssp40sc (ciscoProducts 1200)	ASA 5585-X SSP-40 보안 컨텍스트
ASA5585-SSP60	ciscoASA5585Ssp60sc (ciscoProducts 1201)	ASA 5585-X SSP-60 보안 컨텍스트

표 40-2 SNMP Object Identifier(계속)

ASA5585-SSP10	ciscoASA5585Ssp10sy (ciscoProducts 1202)	ASA 5585-X SSP-10 시스템 컨텍스트
ASA5585-SSP20	ciscoASA5585Ssp20sy (ciscoProducts 1203)	ASA 5585-X SSP-20 시스템 컨텍스트
ASA5585-SSP40	ciscoASA5585Ssp40sy (ciscoProducts 1204)	ASA 5585-X SSP-40 시스템 컨텍스트
ASA5585-SSP60	ciscoASA5585Ssp60sy (ciscoProducts 1205)	ASA 5585-X SSP-60 시스템 컨텍스트
Catalyst 스위치/7600 라우터용 ASA Services Module	ciscoAsaSm1 (ciscoProducts 1277)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈
Catalyst 스위치/7600 라우터용 ASA Services Module 보안 컨텍스트	ciscoAsaSm1sc (ciscoProducts 1275)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 보안 컨텍스트
Catalyst 스위치/7600 라우터용 ASA Services Module 보안 컨텍스트(페이로드 암호화 없음)	ciscoAsaSm1K7sc (ciscoProducts 1334)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 보안 컨텍스트(페이로드 암호화 없음)
Catalyst 스위치/7600 라우터용 ASA Services Module 시스템 컨텍스트	ciscoAsaSm1sy (ciscoProducts 1276)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 시스템 컨텍스트
Catalyst 스위치 시스템 컨텍스트/7600 라우터용 ASA Services Module(페이로드 암호화 없음)	ciscoAsaSm1K7sy (ciscoProducts 1335)	Catalyst 스위치/7600 라우터용 Adaptive Security Appliance(ASA) 서비스 모듈 시스템 컨텍스트(페이로드 암호화 없음)
Catalyst 스위치/7600 라우터용 ASA Services Module 시스템 컨텍스트(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
ASA 5525	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 보안 컨텍스트	ciscoASA5512sc (ciscoProducts 1411)	ASA 5512 Adaptive Security Appliance 보안 컨텍스트
ASA 5525 보안 컨텍스트	ciscoASA5525sc (ciscoProducts 1412)	ASA 5525 Adaptive Security Appliance 보안 컨텍스트
ASA 5545 보안 컨텍스트	ciscoASA5545sc(ciscoProducts 1413)	ASA 5545 Adaptive Security Appliance 보안 컨텍스트
ASA 5555 보안 컨텍스트	ciscoASA5555sc(ciscoProducts 1414)	ASA 5555 Adaptive Security Appliance 보안 컨텍스트
ASA 5512 시스템 컨텍스트	ciscoASA5512sy(ciscoProducts 1415)	ASA 5512 Adaptive Security Appliance 시스템 컨텍스트
ASA 5515 시스템 컨텍스트	ciscoASA5515sy(ciscoProducts 1416)	ASA 5515 Adaptive Security Appliance 시스템 컨텍스트

표 40-2 SNMP Object Identifier(계속)

ASA 5525 시스템 컨텍스트	ciscoASA5525sy (ciscoProducts1417)	ASA 5525 Adaptive Security Appliance 시스템 컨텍스트
ASA 5545 시스템 컨텍스트	ciscoASA5545sy(ciscoProducts 1418)	ASA 5545 Adaptive Security Appliance 시스템 컨텍스트
ASA 5555 시스템 컨텍스트	ciscoASA5555sy (ciscoProducts 1419)	ASA 5555 Adaptive Security Appliance 시스템 컨텍스트
ASA 5515 보안 컨텍스트	ciscoASA5515sc (ciscoProducts 1420)	ASA 5515 Adaptive Security Appliance 시스템 컨텍스트
ASA 5515	ciscoASA5515(ciscoProducts 1421)	ASA 5515 Adaptive Security Appliance
ASAv	ciscoASAv (ciscoProducts 1902)	Cisco Adaptive Security Virtual Appliance(ASAv)
ASAv 시스템 컨텍스트	ciscoASAvsy (ciscoProducts 1903)	Cisco Adaptive Security Virtual Appliance (ASAv) 시스템 컨텍스트
ASAv 보안 컨텍스트	ciscoASAvsc (ciscoProducts 1904)	Cisco Adaptive Security Virtual Appliance (ASAv) 보안 컨텍스트

실제 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 객체에서 반환됩니다. 이 값을 사용하여 구성 요소의 유형(모듈, 전원 공급 장치, 팬, 센서, CPU 등)을 식별할 수 있습니다. 표 40-3은 ASA 및 ASASM 모델에 대한 실제 공급업체 유형 값을 나열합니다.

표 40-3 실제 공급업체 유형 값

소항목	entPhysicalVendorType OID 설명
Catalyst 스위치/7600 라우터용 ASA Services Module	cevCat6kWsSvcAsaSm1 (cevModuleCat6000Type 169)
Catalyst 스위치/7600 라우터용 ASA Services Module(페이로드 암호화 없음)	cevCat6kWsSvcAsaSm1K7 (cevModuleCat6000Type 186)
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)

표 40-3 실제 공급업체 유형 값(계속)

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)
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 라우터를 위한 Cisco ASA Services Module용 CPU	cevCpuAsaSm1 (cevModuleCpuType 222)
Catalyst 스위치/7600 라우터를 위한 Cisco ASA Services Module(페이로드 암호화 없음)용 CPU	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)
Adaptive Security Appliance 5515(페이로드 암호화 없음)의 섀시 냉각 팬	cevFanASA5515K7ChassisFan (cevFan 171)
Adaptive Security Appliance 5525의 섀시 냉각 팬	cevFanASA5525ChassisFan (cevFan 165)

표 40-3 실제 공급업체 유형 값(계속)

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)
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)

표 40-3 실제 공급업체 유형 값(계속)

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)
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)

표 40-3 실제 공급업체 유형 값(계속)

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)
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)
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)

표 40-3 실제 공급업체 유형 값(계속)

Adaptive Security Appliance 5512-X 현장 교체 SSD	cevModuleASA5512XFRSSD (cevModuleCommonCards 400)
Cisco Adaptive Security Virtual Appliance	cevChassisASAv (cevChassis 1451)

MIB에서 지원되는 테이블 및 개체

표 40-4는 지정된 MIB에 대한 지원되는 테이블 및 객체를 나열합니다.

표 40-4 MIB에서 지원되는 테이블 및 개체

MIB 이름	지원되는 테이블 및 개체
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid, cempMemPoolUsed, cempMemPoolFree, cempMemPoolUsedOvrflw, cempMemPoolHCUsed, cempMemPoolFreeOvrflw, cempMemPoolHCFree
CISCO-ENTITY-SENSOR-EXT-MIB 참고 Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서는 지원되지 않습니다.	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB 참고 Cisco Adaptive Security Virtual Appliance(ASAv)에서는 지원되지 않습니다.	ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects
DISMAN-EVENT-MIB	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB 참고 Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서는 지원되지 않습니다.	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB 참고 Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서는 지원되지 않습니다.	entPhySensorTable
NAT-MIB	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus

지원되는 트랩(알림)

표 40-5는 지원되는 트랩(알림)과 연결된 MIB를 나열합니다.

표 40-5 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 버전 3의 경우 auth 또는 priv 비밀번호나 사용자 이름이 바르지 않은 경우 트랩 대신 보고서 PDU가 생성됩니다. **snmp-server enable traps snmp authentication** 명령어는 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	—	**snmp-server enable traps entity fru-insert** 명령어는 이 알림을 활성화하는 데 사용됩니다.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	—	**snmp-server enable traps entity fru-remove** 명령어는 이 알림을 활성화하는 데 사용됩니다.

표 40-5 지원되는 트랩(알림)(계속)

ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB) **참고** Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서는 지원되지 않습니다.	ceSensorExtThresholdValue, entPhySensorValue, entPhySensorType, entPhysicalName	**snmp-server enable traps entity [power-supply-failure | fan-failure | cpu-temperature]** 명령어는 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** 명령어는 팬 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity power-supply-failure** 명령어는 전원 공급 장치 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity chassis-fan-failure** 명령어는 새시 팬 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity cpu-temperature** 명령어는 CPU 고온 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity power-supply-presence** 명령어는 전원 공급 장치 감지 장애 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity power-supply-temperature** 명령어는 전원 공급 장치 온도 임계값 트랩 전송을 활성화하는 데 사용됩니다. **snmp-server enable traps entity chassis-temperature** 명령어는 새시 주변 온도 트랩 전송을 활성화하는 데 사용됩니다.
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	**snmp-server enable traps ipsec start** 명령어는 이 트랩 전송을 활성화하는 데 사용됩니다.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** 명령어는 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** 명령어는 이 트랩 전송을 활성화하는 데 사용됩니다.

표 40-5 지원되는 트랩(알림)(계속)

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** 명령어는 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	**snmp-server enable traps connection-limit-reached** 명령어는 connection-limit-reached 알림 전송을 활성화하는 데 사용됩니다. clogOriginID 객체는 트랩이 시작하는 컨텍스트 이름을 포함합니다.
coldStart (SNMPv2-MIB)	—	SNMP 에이전트가 시작되었습니다. **snmp-server enable traps snmp coldstart** 명령어는 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** 명령어는 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** 명령어는 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** 명령어는 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
linkUp (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	인터페이스에 대한 linkup 트랩. **snmp-server enable traps snmp linkup** 명령어는 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** 명령어는 메모리 임계값 알림을 활성화하는 데 사용됩니다. mteHotOID는 cempMemPoolHCUsed로 설정됩니다. cempMemPoolName 및 cempMemPoolHCUsed 객체는 다른 객체와 함께 전송됩니다.

표 40-5 지원되는 트랩(알림)(계속)

mteTriggerFired (DISMAN-EVENT-MIB) **참고** Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서는 지원되지 않습니다.	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	**snmp-server enable traps interface-threshold** 명령어는 인터페이스 임계값 알림을 활성화하는 데 사용됩니다. entPhysicalName 객체는 다른 객체와 함께 전송됩니다.
natPacketDiscard (NAT-MIB)	ifIndex	**snmp-server enable traps nat packet-discard** 명령어는 NAT 패킷 버림 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** 명령어는 이러한 트랩 전송을 활성화하거나 비활성화하는 데 사용됩니다.

인터페이스 유형 및 예제

SNMP 트래픽 통계를 생산하는 인터페이스 유형은 다음을 포함합니다.

- 논리—소프트웨어 드라이버가 수집한 통계로 물리적 통계의 하위 집합.
- 물리—하드웨어 드라이버가 수집한 통계. 각 물리적 명명 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-only—SNMP는 ifInOctets 및 ifOutOctets에 대해 논리적 통계를 사용합니다.

표 40-6의 예는 SNMP 트래픽 통계의 차이점을 보여줍니다. 예 1은 **show interface** 명령과 **show traffic** 명령에 대한 물리적 및 논리적 출력 통계의 차이를 보여줍니다. 예 2는 **show interface** 명령과 **show traffic** 명령에 대한 VLAN 전용 인터페이스에 대한 출력 통계를 보여줍니다. 예제는 통계가 **show traffic** 명령에 대한 출력과 비슷함을 보여줍니다.

표 40-6 물리 및 VLAN 인터페이스에 대한 SNMP 트래픽 통계

예 : 1:

```
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
```

예 : 2:

```
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 버전 3 개요

SNMP 버전 3은 SNMP 버전 1 또는 버전 2c에는 제공되지 않는 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(User-based Security Model) 및 VACM(View-based Access Control Model)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

컨피그레이션을 위해 인증 및 프라이버시 옵션은 보안 모델로 그룹화됩니다. 보안 모델은 사용자와 그룹에 적용되며 다음 3개 유형으로 나누어집니다.

- NoAuthPriv—No Authentication and No Privacy로 메시지에 보안이 적용되지 않음을 의미합니다.
- AuthNoPriv—Authentication but No Privacy로 메시지가 인증을 받음을 의미합니다.
- AuthPriv—Authentication and Privacy로 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 매개 변수는 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 매개 변수 이름은 ASA 및 ASA Services Module에서 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 자격 증명과 일치하도록 NMS의 사용자 자격 증명을 구성해야 합니다.

ASA, ASA Services Module 및 Cisco IOS 소프트웨어의 구현 차이

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(가) 시작할 때 또는 컨텍스트가 생성될 때 생성됩니다.
- 무제한 MIB 브라우징을 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 알려줍니다.

syslog 메시지에 대한 자세한 설명은 syslog 메시지 가이드을(를) 참조하십시오.

참고 SNMP syslog 메시지가 높은 속도(초당 약 4000)를 초과하면 SNMP 폴링이 실패합니다.

애플리케이션 서비스 및 타사 도구

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 버전 3 MIB를 위한 타사 도구 사용에 관한 정보는 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP용 지침

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

IPv6를 지원하지 않습니다.

추가 지침

- Cisco Works for Windows 또는 다른 SNMP MIB-II 규격 브라우저가 있어야 SNMP 트랩을 수신하거나 MIB를 찾아볼 수 있습니다.
- 보기 기반 액세스 제어를 지원하지 않지만 VACM MIB를 이용한 브라우징으로 기본 보기 설정을 결정할 수 있습니다.
- ENTITY-MIB는 비관리 컨텍스트에서 이용할 수 없습니다. 비관리 컨텍스트에서는 IF-MIB를 대신 사용하십시오.
- AIP SSM 또는 AIP SSC를 위한 SNMP 버전 3을 지원하지 않습니다.
- SNMP 디버깅을 지원하지 않습니다.
- ARP 정보 검색을 지원하지 않습니다.
- SNMP SET 명령어를 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 컨피그레이션을 변경했을 때 SNMP 기능이 일관성을 잃게 되면 변경이 거부됩니다.
- SNMP 버전 3의 경우 그룹, 사용자, 호스트 순서로 컨피그레이션이 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 컨텍스트에서 생성됩니다. 이 트랩을 생성하려면 연결 제한에 도달한 사용자 컨텍스트에서 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.
- 네트워크 객체를 지정하여 호스트 그룹으로 추가할 개별 호스트를 나타낼 수 있습니다.
- 하나의 호스트에 사용자를 두 명 이상 연결할 수 있습니다.
- 다른 **host-group** 명령어에서 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 컨피그레이션을 가져야 합니다.

문제 해결 정보

- NMS로부터의 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 입력하십시오.

```
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(를) 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 경우 다음 명령어를 입력함으로써 패킷 캡처를 이용하여 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(가) 예상대로 작동하지 않으면 다음을 수행함으로써 네트워크 토폴로지 및 트래픽에 대한 정보를 확보하십시오.
  - NMS 컨피그레이션의 경우 다음 정보를 확보합니다.

    시간 초과 횟수

    재시도 횟수

엔진 ID 캐싱

사용된 사용자 이름 및 비밀번호

– 다음 명령어를 수행합니다.

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 통해 허용되지 않는 경우 **icmp permit** 명령을 사용하여 원격 SNMP 서버의 ICMP 트래픽도 허용해야 합니다.

SNMP 구성

이 섹션에서는 SNMP 구성 방법을 설명합니다.

1단계 SNMP 에이전트 및 SNMP 서버를 활성화합니다. 40-20 페이지의 SNMP 에이전트 및 SNMP 서버를 활성화합니다를 참조하십시오.

2단계 SNMP 트랩을 구성합니다. 40-21 페이지의 SNMP 트랩 구성을 참조하십시오.

3단계 SNMP 버전 1 및 2c 매개 변수 또는 SNMP 버전 3 매개 변수를 구성합니다. 40-23 페이지의 SNMP 버전 1 또는 2c에 대한 매개 변수 구성 또는 40-24 페이지의 SNMP 버전 3에 대한 매개변수 구성을 참조하십시오.

SNMP 에이전트 및 SNMP 서버를 활성화합니다

SNMP 에이전트 및 SNMP 서버를 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 ASA, ASAv 또는 ASASM에서 SNMP 에이전트 및 SNMP 서버를 활성화합니다. SNMP 서버는 기본적으로 활성화되어 있습니다.

```
snmp-server enable
```

예:

```
ciscoasa(config)# snmp-server enable
```

SNMP 트랩 구성

SNMP 에이전트가 생성하는 트랩과 그것이 수집되어 NMS로 전송되는 방식을 지정하려면 다음 단계를 수행하십시오.

절차

1단계 개별 트랩, 트랩 집합 또는 모든 트랩을 NMS로 보냅니다.

snmp-server enable traps [**all** | **syslog** | **snmp** [*authentication* | *linkup* | *linkdown* | *coldstart* | *warmstart*] | | **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* |] | **ikev2** [*start* | *stop*] |**ipsec** [*start* | *stop*] | **remote-access** [*session-threshold-exceeded*]| **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [*packet-discard*]

예:

```
ciscoasa(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

이 명령어를 통해 syslog 메시지를 트랩으로서 NMS에 보낼 수 있습니다. 기본 컨피그레이션에는 예제에서와같이 모든 SNMP 표준 트랩이 활성화되어 있습니다. 이 트랩을 비활성화하려면 **no snmp-server enable traps snmp** 명령을 사용하십시오. 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 MIB로부터 트랩을 생성해야 합니다. SNMP 트랩의 기본 활성화를 복원하려면 **clear configure snmp-server** 명령을 사용하십시오. 모든 다른 트랩은 기본적으로 비활성화되어 있습니다.

관리 컨텍스트에서만 이용 가능한 트랩:

- **connection-limit-reached**
- **entity**
- **memory-threshold**

시스템 컨텍스트에서 물리적으로 연결된 인터페이스에 대해서만 관리 컨텍스트를 통해 생성되는 트랩:

- **interface-threshold**

참고 **interface-threshold** 트랩은 Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서 지원되지 않습니다.

모든 다른 트랩은 단일 모드의 관리자 및 사용자 컨텍스트에서 이용 가능합니다.

다중 컨텍스트 모드에서 **fan-failure** 트랩, **power-supply-failure** 트랩 및 **cpu-temperature** 트랩은 사용자 컨텍스트가 아닌 관리자 컨텍스트에서만 생성됩니다(ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에만 적용).

CPU 사용량이 구성된 모니터링 기간에 대한 구성된 임계값보다 큰 경우 **cpu threshold rising** 트랩이 생성됩니다.

사용된 시스템 컨텍스트 메모리가 전체 시스템 메모리의 80에 도달하면 관리자 컨텍스트에서 **memory-threshold** 트랩에 생성됩니다. 다른 사용자 컨텍스트의 경우 이 트랩은 특정 컨텍스트에서 사용된 메모리가 전체 시스템 메모리의 80%에 도달할 때 생성됩니다.

참고 SNMP는 전압 센서를 모니터링하지 않습니다.

CPU 사용량 임계값 구성

CPU 사용량 임계값을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 높음 CPU 임계값과 임계값 모니터링 지속 시간에 대한 임계값을 구성합니다.

snmp cpu threshold rising *threshold_value monitoring_period*

예:

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

CPU 사용률의 임계값과 모니터링 지속 시간을 지우려면 이 명령의 **no** 형식을 사용하십시오. **snmp cpu threshold rising** 명령이 구성되지 않은 경우 높음 임계값의 기본값은 70% 이상이고 심각 임계값의 기본값은 95% 이상입니다. 기본 모니터링 지속 시간은 1분으로 설정됩니다.

심각 CPU 임계값은 구성할 수 없으며 95%로 유지됩니다. 높음 CPU 임계값의 유효한 범위는 10~94%입니다. 모니터링 지속 시간 값의 유효한 범위는 1~60분입니다.

물리적 인터페이스 임계값 구성

물리적 인터페이스 임계값을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 SNMP 물리적 인터페이스에 대한 임계값을 구성합니다.

snmp interface threshold *threshold_value*

예:

```
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 관리자 컨텍스트에서만 이용 가능합니다.

물리적 인터페이스 사용량은 단일 모드 및 멀티 모드에서 모니터링되고 시스템 컨텍스트의 물리적 인터페이스에 대한 트랩은 관리자 컨텍스트를 통해 전송됩니다. 임계값 사용량 계산에는 물리적 인터페이스만 사용됩니다.

참고 이 명령은 Catalyst 6500 스위치/7600 라우터용 ASA Services Module에서는 지원되지 않습니다.

SNMP 버전 1 또는 2c에 대한 매개 변수 구성

SNMP 버전 1 또는 2c에 대한 매개 변수를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 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*]

예:

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2

ciscoasa(config)# snmp-server host corp 172.18.154.159 community public
```

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 ASASM와(과) NMS 사이의 공유 비밀 키입니다. 키는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본 커뮤니티 문자열은 공개됩니다. ASA은(는) 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(는) 지정된 문자열을 사용하여 커뮤니티 문자열이 바르지 않은 요청에는 응답하지 않습니다. 암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템에서 볼 수 있습니다(예: CLI, ASDM, CSM 등). 일반 텍스트 비밀번호는 보이지 않습니다. 암호화된 커뮤니티 문자열은 항상 ASA에 의해 생성됩니다. 일반적으로 일반 텍스트 형식을 입력합니다.

참고 버전 8.3(1)에서 이전 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 되돌린 후 결과를 저장해야 합니다.

snmp-server host 명령을 추가한 후 트랩을 수신하려면 ASA, ASAv 및 ASASM에 구성된 자격 증명과 같은 자격 증명으로 NMS의 사용자를 구성해야 합니다.

2단계 SNMP 버전 1 또는 2c에 *한해* 사용할 커뮤니티 문자열을 설정합니다.

snmp-server community *community-string*

예:

```
ciscoasa(config)# snmp-server community onceuponatime
```

3단계 SNMP 서버 위치 또는 연락처 정보를 설정합니다.

snmp-server [**contact** | **location**] *text*

예:

```
ciscoasa(config)# snmp-server location building 42
```

```
ciscoasa(config)# snmp-server contact EmployeeA
```

텍스트 인수는 연락 담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며 127자까지 가능합니다. 공백이 허용되지만 여러 개의 공백은 하나의 공백으로 단축됩니다.

4단계 SNMP 요청에 대한 듣기 포트를 설정합니다.

snmp-server listen-port *lport*

예:

```
ciscoasa(config)# snmp-server lport 192
```

lport 인수는 수신 요청이 접수되는 포트입니다. 기본 듣기 포트는 161입니다. **snmp-server listen-port** 명령은 관리자 컨텍스트에서만 사용 가능하며 시스템 컨텍스트에서는 사용할 수 없습니다. 현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성하면 다음 메시지가 나타납니다.

경고 **UDP 포트 *port*가 다른 기능에서 사용 중입니다. snmp-server listen-port 명령이 다른 포트를 사용하도록 구성될 때까지 디바이스로의 SNMP 요청이 실패합니다.**

기존 SNMP 스레드가 포트를 이용할 수 있을 때까지 60초 간격으로 계속 폴링을 시도하고 그래도 포트가 사용 중이면 syslog 메시지 %ASA-1-212001을 발행합니다.

SNMP 버전 3에 대한 매개변수 구성

SNMP 버전 3에 대한 매개변수를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 새로운 SNMP 버전 3에 *한하여* 사용할 수 있는 새 SNMP 그룹을 지정합니다.

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

예:

```
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. 보안 모델에 대한 자세한 내용은 40-16 페이지의 보안 모델을 참조하십시오. **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 기본값이 존재하지 않습니다.

2단계 SNMP 버전 3에서만 사용할 SNMP 그룹을 위한 새 사용자를 구성합니다.

snmp-server user *username group-name* {**v3** [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv**] [**des** | **3des** | **aes**] [**128** | **192** | **256**] *priv-password*

예:

```
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. **encrypted** 키워드는 암호화된 형식으로 비밀번호를 지정합니다. 암호화된 비밀번호는 16진수 형식이어야 합니다. **auth** 키워드는 사용할 인증 수준(**md5** 또는 **sha**)을 지정합니다. **priv** 키워드는 암호화 수준을 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** 중 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 컨피그레이션이 콘솔에 표시되거나 파일에 작성된 경우(예를 들어 startup-configuration 파일) 일반 텍스트 비밀번호대신 항상 현지화된 인증 및 프라이버시 다이제스트가 표시됩니다(두 번째 예시 참고). 비밀번호 최소 길이는 영숫자 1자이나 보안을 위해 8자 이상으로 사용하는 것이 좋습니다.

클러스터링에서는 각 클러스터를ASA SNMPv3 사용자로 직접 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 컨피그레이션 중에는 SNMPv3 사용자 명령이 복제되지 않음을 알려주는 오류 메시지가 표시됩니다. 그런 다음 슬레이브에서 SNMPv3 사용자 및 그룹 명령을 ASA독립적으로 구성할 수 있습니다. 이는 또한 복제 중에 기존 SNMPv3 사용자 및 그룹 명령이 지워지지 않고 클러스터의 모든 슬레이브에 SNMPv3 사용자 및 그룹 명령을 입력할 수 있음을 의미합니다. 예:

이미 현지화된 키로 입력된 명령을 사용하는 마스터 유닛에서:

```
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 중 슬레이드 유닛에서(컨피그레이션에 **snmp-server user** 명령이 존재하는 경우에만 나타남):

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

3단계 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*]

예:

```
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
```

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 공개됩니다. ASA, ASAv 및 ASASM은(는) 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(는) 지정된 문자열을 사용하여 커뮤니티 문자열이 바르지 않은 요청에는 응답하지 않습니다. 암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템에서 볼 수 있습니다(예: CLI, ASDM, CSM 등). 일반 텍스트 비밀번호는 보이지 않습니다. 암호화된 커뮤니티 문자열은 항상 ASA에 의해 생성됩니다. 일반적으로 일반 텍스트 형식을 입력합니다.

참고 버전 8.3(1)에서 이전 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 되돌린 후 결과를 저장해야 합니다.

version 키워드는 SNMP 트랩 버전을 지정합니다. ASA은(는) SNMP 요청(폴링) 기준 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 자격 증명과 같은 자격 증명으로 NMS의 사용자를 구성해야 합니다. SNMP 호스트에 관한 자세한 내용은 40-17 페이지의 SNMP 호스트에서 참조하십시오.

4단계 SNMP 서버 위치 또는 연락처 정보를 설정합니다.

```
snmp-server [contact | location] text
```

예:

```
ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA
```

텍스트 인수는 연락 담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며 127자까지 가능합니다. 공백이 허용되지만 여러 개의 공백은 하나의 공백으로 단축됩니다.

5단계 SNMP 요청에 대한 듣기 포트를 설정합니다.

```
snmp-server listen-port lport
```

예:

```
ciscoasa(config)# snmp-server lport 192
```

lport 인수는 수신 요청이 접수되는 포트입니다. 기본 듣기 포트는 161입니다. **snmp-server listen-port** 명령은 관리자 컨텍스트에서만 사용 가능하며 시스템 컨텍스트에서는 사용할 수 없습니다. 현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성하면 다음 메시지가 나타납니다.

경고 **UDP 포트 *port*가 다른 기능에서 사용 중입니다. snmp-server listen-port 명령이 다른 포트를 사용하도록 구성될 때까지 디바이스로의 SNMP 요청이 실패합니다.**

기존 SNMP 스레드가 포트를 이용할 수 있을 때까지 60초 간격으로 계속 폴링을 시도하고 그래도 포트가 사용 중이면 syslog 메시지 %ASA-1-212001을 발행합니다.

사용자 그룹 구성

지정된 사용자 그룹을 포함한 SNMP 사용자 목록을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 SNMP 사용자 목록을 구성합니다.

snmp-server user-list *list_name* **username** *user_name*

예:

```
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 사용자를 2명 이상 포함해야 하며 호스트 이름 또는 IP 주소 범위와 연결될 수 있습니다.

사용자와 네트워크 개체 연결

사용자 목록의 단일 사용자 또는 사용자 그룹을 네트워크 객체와 연결하려면 다음 단계를 수행하십시오.

절차

1단계 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*]

예:

```
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 인수*는 사용자 또는 사용자 그룹이 연결된 인터페이스 네트워크 객체 이름을 지정합니다. **trap** 키워드는 트랩만 전송될 수 있으며 이 호스트는 브라우징(폴링)이 허용되지 않음을 나타냅니다. **poll** 키워드는 이 호스트에서 브라우징(폴링)이 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 32개의 문자를 포함할 수 있습니다. **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 페어는 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 다음 commands를 참조하십시오.

- **show running-config snmp-server [default]**

  이 명령은 모든 SNMP 서버 컨피그레이션 정보를 표시합니다.

- **show running-config snmp-server group**

  이 명령은 SNMP 그룹 컨피그레이션 설정을 표시합니다.

- **show running-config snmp-server host**

  이 명령은 SNMP에서 원격 호스트로 전송되는 메시지 및 알림을 제어하는 데 사용되는 컨피그레이션 설정을 표시합니다.

- **show running-config snmp-server host-group**

  이 명령은 SNMP 호스트 그룹 컨피그레이션을 표시합니다.

- **show running-config snmp-server user**

  이 명령은 SNMP 사용자 기반 컨피그레이션 설정을 표시합니다.

- **show running-config snmp-server user-list**

  이 명령은 SNMP 사용자 목록 컨피그레이션을 표시합니다.

- **show snmp-server engineid**

  이 명령은 구성된 SNMP 엔진의 ID를 표시합니다.

- **show snmp-server group**

  이 명령어는 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 구성 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 컨피그레이션을 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP 버전 1과 2c의 예

다음 예는 ASA가 내부 인터페이스의 호스트 192.0.2.5으로부터 SNMP 요청을 받되 호스트로 SNMP syslog 요청을 전송하지 않는 방법을 보여줍니다.

```
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 3의 예

다음 예는 ASA가 SNMP 버전 3 보안 모델(그룹, 사용자, 호스트 순으로 구성해야 함)을 사용하여 SNMP 요청을 수신하는 방법을 보여줍니다.

```
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 내역

표 40-7 SNMP 내역

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.
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. 도입되거나 수정된 명령: **show snmp-server engineid, show snmp-server group, show snmp-server user, snmp-server group, snmp-server user**, **snmp-server host**.

표 40-7 SNMP 내역(계속)

기능 이름	플랫폼 릴리스	설명
비밀번호 암호화	8.3(1)	비밀번호 암호화를 지원합니다. 수정된 명령: **snmp-server community**, **snmp-server host**.
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. 도입되거나 수정된 명령: **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.
ASA Services Module (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(entPhySensorTable 그룹의 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**. 수정된 명령: **snmp-server enable traps**

표 40-7 SNMP 내역(계속)

기능 이름	플랫폼 릴리스	설명
VPN-related 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 엔트리 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 최대 4000개의 호스트를 추가할 수 있습니다. 지원되는 액티브 폴링 대상의 수는 128개입니다. 네트워크 객체를 지정하여 호스트 그룹으로 추가할 개별 호스트를 나타낼 수 있습니다. 하나의 호스트에 사용자를 두 명 이상 연결할 수 있습니다. 도입되거나 수정된 명령: **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
SNMP 메시지 크기	9.2(1)	SNMP가 전송하는 메시지 크기 제한이 1472바이트로 증가했습니다.
SNMP OID 및 MIB		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.

표 40-7 SNMP 내역(계속)

기능 이름	플랫폼 릴리스	설명
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.
SNMP MIB 및 트랩	9.3(2)	CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB가 새로운 ASA 5506-X, ASA 5506W-X 및 ASA 5508-X를 지원하도록 업데이트되었습니다. ASA 5506-X 및 ASA 5508-X이(가) SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새로운 제품으로 추가되었습니다. 이제 ASA에서 CISCO-CONFIG-MAN-MIB를 지원하므로 다음 작업을 수행할 수 있습니다. • 특정 컨피그레이션에 대해 어떤 명령이 입력되었는지 알 수 있습니다. • 컨피그레이션 실행 중 변경이 발생하면 NMS에게 알립니다. • 실행 중인 컨피그레이션이 마지막으로 변경되거나 저장된 시간에 대한 타임 스탬프를 추적합니다. • 터미널 정보 및 명령 소스와 같은 기타 명령 변경 사항을 추적합니다. 수정된 명령: **snmp-server enable traps**

41 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 포인트가 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 포인트 이름으로 ASA에 설치됩니다. Anonymous Reporting을 활성화하면 이 신뢰 포인트가 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 포인트가 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 참조 하십시오.
http://www.cisco.com/web/siteassets/legal/privacy.html

DNS 요구 사항

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 자세한 내용은syslog 메시지 가이드을 참조 하십시오.

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.

- 시스템 로그
- 진단

- 환경
- 인벤토리
- 컨피그레이션
- 위협
- 스냅샷
- 원격 분석
- 테스트

경고 그룹의 속성

경고 그룹 속성은 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 경고 그룹별로 Cisco에 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 ASA온도 상태, 전압 및 CPU 사용량 등 시스템 구성 요소의 환경 정보를 표시합니다.

컨피그레이션 경고는 다음 명령의 출력으로 구성됩니다.

- **show context** - 할당된 인터페이스 및 컨피그레이션 파일 URL, 구성된 컨텍스트 수 또는 시스템 구현 영역에서 Anonymous Reporting을 설정한 경우 모든 컨텍스트 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 컨피그레이션을 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 ASA온도 상태, 전압 및 CPU 사용량 등 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.

원격 분석 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 컨피그레이션에 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 컨피그레이션 파일 URL, 구성된 컨텍스트 수 또는 시스템 구현 영역에서 Anonymous Reporting을 설정한 경우 모든 컨텍스트 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**—Phone Proxy가 저장한 대응 미디어 세션 개수를 표시합니다.
- **show phone-proxy secure-phones count**—데이터베이스에 저장된 안전 모드를 지원하는 휴대폰 개수를 표시합니다.
- **show route**—라우팅 테이블을 표시합니다.
- **show xlate count**—NAT 세션(xlates) 수를 표시합니다.

메시지 심각도 임계값

특정 알림 그룹에 대상 프로필을 등록하면 메시지 심각도 수준에 따라 경고 그룹 메시지를 보내는 임계값을 설정할 수 있습니다. 대상 프로필의 지정 임계값 보다 낮은 값을 가진 메시지는 대상으로 전송되지 않습니다.

표 41-1 메시지 심각도 수준과 syslog 심각도 간의 매핑을 표시합니다.

표 41-1 메시지 심각도 수준 및 Syslog 수준 매핑

수준	메시지 심각도	Syslog 심각도	설명
9	치명	N/A	네트워크 전반의 치명적인 장애.
8	재해	N/A	중대한 네트워크 영향.
7	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** *경고 그룹 이름* **심각도** *심각도 수준*	0	긴급. 시스템을 사용할 수 없습니다.
6	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** *경고 그룹 이름* **심각도** *심각도 수준*	1	경고. 심각한 상태로 즉시 살펴봐야 합니다.
5	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** *경고 그룹 이름* **심각도** *심각도 수준*	2	심각. 중요한 문제.

표 41-1 메시지 심각도 수준 및 Syslog 수준 매핑(계속)

수준	메시지 심각도	Syslog 심각도	설명
4	지정된 CLI 키워드에 의해 결정: **subscribe-to-alert-group** *경고 그룹 이름* **심각도** *심각도 수준*	3	오류. 경미한 문제.
3	경고	4	경고 상태입니다.
2	알림	5	기본적인 알림 및 정보 메시지입니다. 독립적이고 중요하지 않을 수 있습니다.
1	일반	6	정보. 일반적인 이벤트, 정상 상태 복귀를 알립니다.
0	디버깅	7	디버깅 메시지(기본 설정).

서브스크립션 프로필

서브스크립션 프로필을 통해 대상 수신자를 관심 그룹과 연계할 수 있습니다. 프로필의 등록 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. 프로파일은 기본적으로 비활성화되어 있습니다.
- 최대 메시지 크기를 지정할 수 있습니다. 기본값은 3MB입니다.

기본 프로필 "Cisco TAC"가 제공됩니다. 기본 프로필에는 모니터 및 사전 정의된 대상 이메일 및 HTTPS URL에 대한 사전 정의된 그룹 집합(진단, 환경, 인벤토리, 컨피그레이션 및 원격 분석)이 있습니다. 기본 프로필은 Smart Call Home을 처음 구성할 때 자동으로 만들어집니다. 대상 이메일은 callhome@cisco.com이고 대상 URL은 https://tools.cisco.com/its/service/oddce/services/DDCEService입니다.

참고 기본 프로필의 이메일 또는 대상 URL을 변경할 수 없습니다.

컨피그레이션, 인벤토리, 원격 분석 또는 스냅샷 경고 그룹에 대상 프로필을 등록할 때 경고 그룹 메시지를 비동기식으로 받을지 아니면 지정된 시간에 정기적으로 받을지 선택할 수 있습니다.

표 41-2 기본 경고 그룹을 심각도 수준 서브스크립션 및 기간에 매핑(해당하는 경우):

표 41-2 심각도 수준 등록에 대한 경고 그룹 매핑

경고 그룹	심각도	기간
컨피그레이션	정보	매달
진단	정보 이상	N/A

표 41-2 심각도 수준 등록에 대한 경고 그룹 매핑(계속)

경고 그룹	심각도	기간
환경	알림 이상	N/A
인벤토리	정보	매달
스냅샷	정보	N/A
Syslog	동일한 syslog	N/A
원격 분석	정보	매일
테스트	N/A	N/A
위협	알림	N/A

Anonymous Reporting 및 Smart Call Home에 대한 지침

Anonymous Reporting

- 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 포인트를 제거할 수 없고 Anonymous Reporting이 비활성화되어도 신뢰 포인트가 유지됩니다. Anonymous Reporting이 비활성화된 경우 신뢰 포인트를 제거할 수 있으나 Anonymous Reporting을 비활성화한다고 신뢰 포인트가 자동으로 삭제되지는 않습니다.
- 여러 컨텍스트 모드 컨피그레이션을 사용하는 경우 **dns**, **interface** 및 **trustpoint** 명령어는 관리 컨텍스트에 상주하고 **call-home** 명령어는 시스템 컨텍스트에 상주합니다.

Smart Call Home

- 다중 컨텍스트 모드에서 **subscribe-to-alert-group snapshot periodic** 명령어는 두 명령어로 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

관련 주제

- 41-2 페이지의 DNS 요구 사항
- 13-13 페이지의 DNS 서버 구성

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 Home를 활성화하라는 메시지가 표시됩니다.

- 프롬프트에서 [Y]es, [N]o, [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 41-8 페이지의 Anonymous Reporting 구성 또는 41-9 페이지의 Smart Call Home 구성의 단계에 따라 Anonymous Reporting 또는 Smart Call을 활성화할 수 있습니다.

Anonymous Reporting 구성

Anonymous Reporting을 구성하려면 다음 단계를 수행합니다.

절차

1단계 Anonymous Reporting 기능을 활성화 하고 새 익명 프로필을 만듭니다.

```
call-home reporting anonymous
```

예:

```
ciscoasa(config)# call-home reporting anonymous
```

이 명령어를 입력하면 신뢰 포인트가 생성되고 Cisco 웹 서버의 ID를 확인하는 데 사용되는 인증서가 설치됩니다.

2단계 (선택 사항) 서버에 연결되어 있고 시스템이 메시지를 전송할 수 있는지 확인하십시오.

```
call-home test reporting anonymous
```

예:

```
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.

1단계 Smart Call Home 서비스를 활성화합니다. 41-9 페이지의 Smart Call Home 활성화를 참조하십시오.

2단계 가입자에게 Smart Call Home를 메시지가 전달되는 메일 서버를 구성합니다. 41-13 페이지의 메일 서버 구성을 참조하십시오.

3단계 Smart Call Home 메시지에 대한 연락 정보를 설정합니다. 41-12 페이지의 고객 연락처 정보 구성을 참조하십시오.

4단계 처리할 수 있는 최대 이벤트 속도와 같이 경고 처리 매개변수를 정의합니다. 41-11 페이지의 경고 그룹 등록 구성을 참조하십시오.

5단계 경고 서브스크립션 프로필을 설정합니다. 41-15 페이지의 대상 프로필 구성을 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.

절차

1단계 Smart Call Home 서비스를 활성화합니다.

```
service call-home
```

예:

```
ciscoasa(config)# service call-home
```

2단계 call-home 컨피그레이션 모드로 들어갑니다.

```
call-home
```

예:

```
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 생산 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 포인트를 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.

절차

1단계 (다중 컨텍스트 모드에만 해당) 관리자 컨텍스트 내에서 인증서를 설치합니다.

changeto context *admincontext*

예:

```
ciscoasa(config)# changeto context contextA
```

2단계 신뢰 포인트를 구성하고 인증서 등록을 준비합니다.

crypto ca trustpoint *trustpoint-name*

예:

```
ciscoasa(config)# crypto ca trustpoint cisco
```

참고 전송 방법으로 HTTPS를 이용하는 경우 신뢰 포인트를 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

3단계 인증서 등록 방법으로 수동 붙여넣기를 지정합니다.

enroll terminal

예:

```
ciscoasa(ca-trustpoint)# enroll terminal
```

4단계 지정된 CA를 인증합니다. CA 이름이 **crypto ca trustpoint** 명령에 지정된 신뢰 포인트 이름과 일치해야 합니다. 프롬프트에서 보안 인증서 텍스트를 붙여넣습니다.

crypto ca authenticate *trustpoint*

예:

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

5단계 보안 인증서 텍스트 끝을 지정하고 입력한 보안 인증서의 수락을 확인합니다.

quit

예:

```
ciscoasa(ca-trustpoint)# quit

%Do you accept this certificate [yes/no]:

yes
```

환경 및 스냅샷 경고 그룹 구성

환경 및 스냅샷 경고 그룹을 구성하려면 다음 단계를 수행 하십시오.

절차

1단계 경고 그룹 컨피그레이션 모드로 들어갑니다.

alert-group-config {**environment** | **snapshot**}

예:

```
ciscoasa(config)# alert-group-config environment
```

경고 그룹 등록 구성

대상 프로필을 경고 그룹에 등록하려면 다음 단계를 수행하십시오.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 지정된 Smart Call Home 경고 그룹을 활성화합니다.

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

예:

```
ciscoasa(cfg-call-home)# alert-group syslog
```

모든 경고 그룹을 활성화하려면 **all** 키워드를 사용합니다. 기본적으로 모든 경고 그룹이 활성화됩니다.

3단계 지정된 대상 프로필에 대한 프로필 컨피그레이션 모드로 들어갑니다.

profile *profile-name*

예:

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

4단계 이용 가능한 모든 경고 그룹에 등록합니다.

subscribe-to-alert-group all

예:

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

5단계 이 대상 프로필을 컨피그레이션 경고 그룹에 등록합니다.

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

예:

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

정기 키워드는 정기 알림을 위해 컨피그레이션 경고 그룹을 구성합니다. 기본 기간은 매일입니다.

매일 키워드는 *hh:mm* 형식의 24시간제로 전송 시간을 지정합니다(예: 14:30).

매주 키워드는 *day hh:mm* 형식으로 전송 요일과 시간을 지정하며 요일은 풀어서 씁니다(예: Monday).

매달 키워드는 1부터 31까지의 숫자와 시간을 *date hh:mm* 형식으로 지정합니다.

고객 연락처 정보 구성

고객 연락처 정보를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 고객 전화 번호를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

phone-number *phone-number-string*

예:

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

3단계 길이가 최대 255자인 자유 형식 문자열로 고객 주소를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

street-address *street-address*

예:

```
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

4단계 최대 128자 길이의 고객 이름을 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

contact-name *contact-name*

예:

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

5단계 최대 64자 길이의 Cisco 고객 ID를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

customer-id *customer-id-string*

예:

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

6단계 최대 64자 길이의 고객 사이트 ID를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

site-id *site-id-string*

예:

```
ciscoasa(cfg-call-home)# site-id site1234
```

7단계 최대 128자 길이의 고객 계약 ID를 지정합니다. 공백이 허용되지만 공백을 포함한 경우 문자열 주변에 따옴표를 사용해야 합니다.

contract-id *contract-id-string*

예:

```
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 대상을 구성한 다음 메일 서버가 이메일 메시지 전송을 사용하도록 구성할 수 있습니다.

메일 서버를 구성하려면 다음 작업을 수행합니다.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 SMTP 메일 서버를 지정합니다.

mail-server *ip-address* **name priority** [**1-100**] [**all**]

예:

```
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 낮을 수록 메일 서버의 우선순위가 높습니다.

ip-address 인수는 IPv4 또는 IPv6 메일 서버 주소가 될 수 있습니다.

예

다음 예는 기본 메일 서버("smtp.example.com")와 IP 주소 10.10.1.1의 보조 메일 서버를 구성하는 방법을 보여줍니다.

```
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 수행하십시오.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 Smart Call Home이 1분에 보낼 수 있는 메시지 수를 지정합니다. 기본값은 분당 10개의 메시지입니다.

rate-limit *msg-count*

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Smart Call Home 통신 전송

수동으로 Smart Call Home 테스트 메시지를 보내려면 다음 단계를 수행하십시오.

절차

1단계 프로필 컨피그레이션을 사용하여 테스트 메시지를 보냅니다.

call-home test [*test-message*] **profile** *profile-name*

예:

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

수동으로 경고 그룹 메시지를 트리거하려면 다음 단계를 수행하십시오.

절차

1단계 대상 프로필이 지정되어 있다면 하나의 대상 프로필로 경고 그룹 메시지를 보냅니다. 프로필이 지정되지 않은 경우 인벤토리, 컨피그레이션, 스냅샷 또는 원격 분석 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
```

CLI 명령을 발행하고 명령 출력을 Cisco TAC 또는 특정 이메일 주소로 보내려면 다음 단계를 수행하십시오.

절차

1단계 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 대상 프로필을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 지정된 대상 프로필에 대한 프로필 컨피그레이션 모드로 들어갑니다. 지정 대상 프로필이 존재하지 않는 경우 프로필이 생성됩니다.

profile *profile-name*

예:

```
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.

3단계 Smart Call Home 메시지 수신기의 대상, 메시지 크기, 메시지 형식, 전송 방식을 구성합니다. 기본 메시지 형식은 XML이며 기본적으로 활성화된 라우팅 방법은 이메일입니다.

destination {**email** *address* | **http** *url*} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

예:

```
ciscoasa(cfg-call-home-profile)# destination address email username@example.com

ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

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.

HTTP에 대한 전송 방식을 설정하려면 41-9 페이지의 Smart Call Home 활성화를 참조하십시오. 이 명령을 사용하여 전송 방식을 다시 이메일로 바꿀 수 있습니다.

대상 프로필 복사

기존 대상 프로필을 복사하여 새 프로필을 생성하려면 다음 단계를 수행하십시오.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 복사할 프로필을 지정합니다.

profile *profile-name*

예:

```
ciscoasa(cfg-call-home)# profile newprofile
```

3단계 기존 프로필 내용을 새 프로필에 복사합니다.

copy profile *src-profile-name dest-profile-name*

예:

```
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 바꾸기

기존 프로파일의 이름을 변경하려면 다음 단계를 수행하십시오.

절차

1단계 call-home 컨피그레이션 모드로 들어갑니다.

call-home

예:

```
ciscoasa(config)# call-home
```

2단계 이름을 바꿀 프로필을 지정합니다.

profile *profilename*

예:

```
ciscoasa(cfg-call-home)# profile newprofile
```

3단계 기존 프로파일 이름을 변경합니다.

rename profile *src-profile-name dest-profile-name*

예:

```
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 명령 을 참조하십시오.

- **show call-home detail**

  이 명령어는 현재 Smart Call Home 세부 사항 컨피그레이션을 표시합니다.

- **show call-home mail-server status**

  이 명령어는 현재 메일 서버 상태를 표시합니다.

- **show call-home profile** {*profile name* | **all**}

  이 명령어는 Smart Call Home 프로필의 컨피그레이션을 보여줍니다.
- **show call-home registered-module status** [**all**]

  이 명령어는 등록된 모듈 상태를 표시합니다.
- **show call-home statistics**

  이 명령어는 콜 홈 세부 정보 상태를 표시합니다.
- **show call-home**

  이 명령어는 현재 Smart Call Home 컨피그레이션을 표시합니다.
- **show running-config call-home**

  이 명령어는 현재 Smart Call Home 실행 컨피그레이션을 표시합니다.
- **show smart-call-home alert-group**

  이 명령어는 Smart Call Home 경고 그룹의 현재 상태를 표시합니다.
- **show running-config all**

  이 명령어는 Anonymous Reporting 사용자 프로필에 대한 세부 정보를 표시합니다.

Smart Call Home의 예(CLI)

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 41-3 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. 도입되거나 수정된 명령: **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. 도입된 화면: **call-home reporting anonymous**, **call-home test reporting anonymous**.
Smart Call Home	9.1(2)	**show local-host** 명령이 원격 분석 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

10 파 트

참조

42 장

Command-Line Interface 사용

이 장에서는 Cisco ASA에서 CLI를 사용하는 방법에 대해 설명합니다.

참고 CLI의 경우 Cisco IOS CLI와 유사한 구문 및 기타 표기 규칙을 사용하지만 ASA 운영 체제는 Cisco IOS 소프트웨어의 버전이 아닙니다. Cisco IOS CLI 명령은 ASA와 연동되지 않거나 동일한 기능이 없을 수 있습니다.

방화벽 모드 및 보안 컨텍스트 모드

ASA는 다음과 같은 모드를 조합한 환경에서 실행됩니다.

- 투명 방화벽 또는 라우팅 방화벽 모드

  이 방화벽 모드에서는 ASA가 레이어 2 또는 레이어 3 방화벽으로 실행되는지 결정합니다.

- 다중 컨텍스트 또는 단일 컨텍스트 모드

  보안 컨텍스트 모드에서는 ASA가 단일 디바이스 또는 가상 디바이스 역할을 하는 다중 보안 컨텍스트로 실행되는지 결정합니다.

일부 명령은 특정 모드에서만 사용할 수 있습니다.

명령 모드 및 프롬프트

ASA CLI에는 명령 모드가 포함됩니다. 일부 명령은 특정 모드에서만 입력할 수 있습니다. 예를 들어, 민감 정보를 표시하는 명령을 입력하려면 비밀번호를 입력하고 특권 모드로 들어가야 합니다. 그런 다음 컨피그레이션 변경 사항이 실수로 입력되지 않았는지 확인하려면 구성 모드로 들어가야 합니다. 모든 하위 명령은 상위 모드에서 입력할 수 있습니다. 예를 들어, 특권 실행 명령은 전역 컨피그레이션 모드에서 입력할 수 있습니다.

참고 다양한 프롬프트 유형은 모두 기본 프롬프트이며 구성 시 달라질 수 있습니다.

- 시스템 컨피그레이션 또는 단일 컨텍스트 모드에 있을 경우, 프롬프트는 호스트 이름으로 시작됩니다.

  ```
  ciscoasa
  ```

- 프롬프트 문자열을 인쇄할 경우, 프롬프트 컨피그레이션이 구문 분석되고 구성된 키워드 값은 **prompt** 명령에서 설정한 순서대로 인쇄됩니다. 키워드 인수는 hostname, domain, context, priority, state 중 어떤 것이든 가능하며 순서는 상관이 없습니다.

  ```
  asa(config)# prompt hostname context priority state
  ```

- 컨텍스트 내에 있을 경우, 프롬프트는 호스트 이름으로 시작하고 그 다음 컨텍스트 이름이 옵니다.

  ```
  ciscoasa/context
  ```

프롬프트 변경은 액세스 모드에 따라 달라집니다.

- 사용자 실행 모드

  사용자 실행 모드를 사용하면 최소 ASA 설정을 볼 수 있습니다. ASA에 처음 액세스할 경우 사용자 실행 모드 프롬프트는 다음과 같이 표시됩니다.

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- 특권 실행 모드

  특권 실행 모드를 사용하면 권한 수준에 대한 모든 현재 설정을 볼 수 있습니다. 모든 사용자 실행 모드 명령은 특권 실행 모드에서 작동합니다. 특권 실행 모드를 시작하려면 비밀번호가 필요한 사용자 실행 모드에서 **enable** 명령을 입력합니다. 프롬프트에 숫자 기호(#)가 포함됩니다.

  ```
  ciscoasa#

  ciscoasa/context#
  ```

- 전역 컨피그레이션 모드

  전역 컨피그레이션 모드를 사용하면 ASA 컨피그레이션을 변경할 수 있습니다. 이 모드에서는 모든 사용자 실행 명령, 특권 실행 명령, 전역 컨피그레이션 명령을 사용할 수 있습니다. 전역 컨피그레이션 모드를 시작하려면 특권 실행 모드에서 **configure terminal** 명령을 입력합니다. 프롬프트가 다음과 같이 바뀝니다.

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- 명령별 컨피그레이션 모드

  전역 컨피그레이션 모드에서 일부 명령을 사용하면 명령별 컨피그레이션 모드로 들어갑니다. 이 모드에서는 모든 사용자 실행 명령, 특권 실행 명령, 전역 컨피그레이션 명령, 명령별 컨피그레이션 명령을 사용할 수 있습니다. 예를 들어, **interface** 명령을 사용하면 인터페이스 컨피그레이션 모드로 들어갑니다. 프롬프트가 다음과 같이 바뀝니다.

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

구문 형식 지정

명령 구문 설명에서는 표 42-1에 나열된 표기 규칙을 사용합니다.

표 42-1 구문 표기 규칙

표기 규칙	설명
굵은 글꼴	굵은 글꼴 텍스트는 표시되는 글자 그대로 입력한 명령 및 키워드를 나타냅니다.
기울임꼴	기울임꼴 텍스트는 사용자가 값을 제공하는 인수를 나타냅니다.
[x]	대괄호는 선택 요소(키워드 또는 인수)를 묶습니다.
|	세로 막대는 선택 또는 필수 키워드나 인수 집합 내에 있는 선택 항목을 나타냅니다.
[x | y]	대괄호는 선택 항목을 나타내는 세로 막대로 분리된 키워드 또는 인수를 묶습니다.
{x | y}	중괄호는 필수 항목을 나타내는 세로 막대로 분리된 키워드 또는 인수를 묶습니다.
[x {y | z}]	중첩된 대괄호 또는 중괄호는 선택 또는 필수 요소 내에 있는 선택 또는 필수 선택 항목을 나타냅니다. 대괄호 안의 중괄호 및 세로 막대는 선택 요소 내에 있는 필수 선택 항목을 나타냅니다.

축약 명령

대부분의 명령은 한 가지 명령을 의미하는 가장 작은 형태의 고유한 문자로 축약할 수 있습니다. 예를 들어, 전체 명령 **write terminal**을 입력하는 대신 **wr t**를 입력하여 컨피그레이션을 볼 수 있습니다. 또는 **en**을 입력하여 특권 모드를 시작하고 **conf t**를 입력하여 컨피그레이션 모드를 시작할 수 있습니다. 또한 **0**을 입력하여 **0.0.0.0**을 나타낼 수 있습니다.

명령줄 수정

ASA에서는 Cisco IOS 소프트웨어와 동일한 명령줄 수정 표기 규칙을 사용합니다. **show history** 명령을 사용하여 이전에 입력한 모든 명령을 보거나, 위쪽 화살표 또는 **^p** 명령을 사용하여 이전에 입력한 명령을 개별적으로 볼 수 있습니다. 이전에 입력한 명령을 검사한 후에는 아래쪽 화살표 또는 **^n** 명령을 사용하여 목록에서 앞으로 이동할 수 있습니다. 재사용하려는 명령이 나오면 해당 명령을 수정하거나 **Enter** 키를 눌러 시작할 수 있습니다. 또한 **^w**를 사용하여 커서의 왼쪽에 있는 단어를 삭제하거나 **^u**를 사용하여 줄을 지울 수 있습니다.

ASA에서는 명령 하나당 최대 512자까지 허용하며 추가 문자는 무시됩니다.

명령 완료

부분 문자열을 입력한 후 명령 또는 키워드를 완료하려면 **Tab** 키를 누릅니다. ASA에서는 부분 문자열이 단 하나의 명령 또는 키워드와 매칭하는 경우에만 명령 또는 키워드를 완료합니다. 예를 들어, **s**를 입력하고 **Tab** 키를 누를 경우 둘 이상의 명령과 매칭하므로 ASA에서는 명령을 완료하지 않습니다. 그러나 **dis**를 입력하고 **Tab** 키를 누르면 **disable** 명령이 완료됩니다.

명령 도움말

다음 명령을 입력하면 명령줄에서 도움말 정보를 사용할 수 있습니다.

- **help** *command_name*

  특정 명령의 도움말이 표시됩니다.

- *command_name* **?**

  사용 가능한 인수 목록이 표시됩니다.

- *string***?** (공백 없음)

  문자열로 시작되는 가능한 명령이 나열됩니다.

- **?** 및 **+?**

  사용할 수 있는 모든 명령이 나열됩니다. **?**를 입력할 경우 ASA에서는 현재 모드에서 사용할 수 있는 명령만 표시합니다. 하위 모드에 사용할 수 있는 명령을 포함하여 모든 명령을 표시하려면 **+?**를 입력합니다.

참고 명령 문자열에 물음표(?)를 포함하려면 물음표를 입력하기 전에 **Ctrl-V**를 입력하여 CLI 도움말이 실수로 호출되지 않도록 해야 합니다.

실행 중인 컨피그레이션 보기

실행 중인 컨피그레이션을 보려면 다음 명령 중 하나를 사용합니다.

- **show running-config** [**all**] [*command*]

  all을 지정할 경우 모든 기본 설정도 함께 표시됩니다. *command*를 지정할 경우 출력에는 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**

관련 주제

13-10 페이지의 마스터 패스프레이즈 구성

필터 표시 및 추가 명령 출력

세로 막대(|)를 **show** 명령과 함께 사용하여 필터 옵션 및 필터링 정규식을 포함할 수 있습니다. 필터링은 Cisco IOS 소프트웨어와 마찬가지로 각 출력 행을 정규식과 매칭하여 수행합니다. 다른 필터 옵션을 선택하여 정규식과 매칭하는 모든 출력을 포함하거나 제외할 수 있습니다. 또한 해당 식과 매칭하는 행으로 시작되는 모든 출력도 표시할 수 있습니다.

show 명령과 함께 필터링 옵션을 사용하기 위한 구문은 다음과 같습니다.

```
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

또는

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

참고 **more** 명령을 입력하면 실행 중인 컨피그레이션뿐만 아니라 모든 파일의 내용을 볼 수 있습니다. 자세한 내용은 명령 참조를 참조하십시오.

이 명령 문자열에서 첫 번째 세로 막대(|)는 연산자이며 명령에 포함되어야 합니다. 이 연산자는 **show** 명령의 출력을 필터로 보냅니다. 구문 다이어그램의 다른 세로 막대(|)는 대체 옵션을 나타내며 명령에 포함되어 있지 않습니다.

include 옵션에는 정규식과 매칭하는 모든 출력 행이 포함됩니다. **-v**가 없는 **grep** 옵션은 동일한 작용을 합니다. **exclude** 옵션에는 정규식과 매칭하는 모든 출력 행이 제외됩니다. **-v**가 있는 **grep** 옵션은 동일한 작용을 합니다. **begin** 옵션은 정규식과 매칭하는 행으로 시작하는 모든 출력 행을 표시합니다.

*regexp*를 Cisco IOS 정규식으로 교체합니다. 정규식은 따옴표나 큰따옴표로 묶이지 않으므로 공백이 뒤에 오지 않도록 주의해야 합니다. 이러한 공백은 정규식에 포함되는 것으로 간주됩니다.

정규식을 생성할 경우, 매칭하고자 하는 모든 문자 또는 숫자를 사용할 수 있습니다. 또한 *metacharacters*라는 특정 키보드 문자가 정규식에 사용된 경우 특수한 의미를 지닙니다.

CLI에서 물음표(?) 또는 탭 같은 모든 문자를 이스케이프하려면 **Ctrl+V**를 사용합니다. 예를 들어, 컨피그레이션에 **d?g**를 입력하려면 **d[Ctrl+V]?g**를 입력합니다.

명령 출력 페이징

help 또는 **?**, **show**, **show xlate** 같은 명령이나 긴 목록을 제공하는 명령의 경우, 정보를 화면에 표시하고 일시 중지할지 또는 명령을 실행하여 완료할지 결정할 수 있습니다. **pager** 명령을 사용하면 More 프롬프트가 나타나기 전에 표시할 행의 개수를 선택할 수 있습니다.

페이징이 활성화되면 다음과 같은 프롬프트가 나타납니다.

```
<--- More --->
```

More 프롬프트에서는 UNIX **more** 명령과 유사한 구문을 사용합니다.

- 다른 화면을 보려면 **Space** 바를 누릅니다.
- 다음 행을 보려면 **Enter** 키를 누릅니다.
- 명령줄로 돌아가려면 **q** 키를 누릅니다.

코멘트 추가

행 앞에 콜론(:)을 넣어 코멘트를 생성할 수 있습니다. 그러나 코멘트는 컨피그레이션이 아닌 명령 기록 버퍼에만 표시됩니다. 따라서 **show history** 명령을 사용하거나 화살표 키를 눌러 이전 명령을 검색하여 코멘트를 볼 수 있습니다. 그러나 코멘트는 컨피그레이션에 있지 않으므로 **write terminal** 명령을 사용하여 이를 표시할 수 없습니다.

텍스트 컨피그레이션 파일

이 섹션에서는 ASA에 다운로드할 수 있는 텍스트 컨피그레이션 파일의 형식을 지정하는 방법에 대해 설명합니다.

명령이 텍스트 파일의 행과 대응하는 방식

텍스트 컨피그레이션 파일에는 이 가이드에 설명된 명령과 대응하는 행이 포함되어 있습니다.

예를 들어, 명령은 CLI 프롬프트 앞에 옵니다. 다음 예의 프롬프트는 다음과 같습니다. "ciscoasa(config)#":

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

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

```
context a
```

명령별 컨피그레이션 모드 명령

명령별 컨피그레이션 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, 아래의 들여 쓰지 않은 텍스트는 들여 쓴 텍스트와 동일하게 읽힙니다.

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

자동 텍스트 항목

컨피그레이션을 ASA에 다운로드할 경우, 일부 행이 자동으로 삽입됩니다. 예를 들어, ASA에서는 기본 설정 또는 컨피그레이션이 수정된 시간에 대한 행을 삽입합니다. 텍스트 파일을 생성할 때 이러한 자동 항목은 입력하지 않아도 됩니다.

행 순서

대부분의 경우 파일의 명령 순서는 임의로 지정해도 상관이 없습니다. 그러나 ACE 같은 일부 행의 경우 표시되는 순서대로 처리되며, 이러한 순서는 액세스 목록의 기능에 영향을 미칠 수 있습니다. 다른 명령의 경우에도 순서 요구 사항이 있을 수 있습니다. 예를 들어, 많은 후속 명령에서 인터페이스의 이름을 사용하게 되므로 인터페이스에는 **nameif** 명령을 첫 번째로 입력해야 합니다. 또한 명령별 컨피그레이션 모드의 명령은 기본 명령 바로 뒤에 와야 합니다.

텍스트 컨피그레이션에 포함되지 않는 명령

일부 명령의 경우 컨피그레이션에 행을 삽입하지 않습니다. 예를 들어, **show running-config** 같은 런타임 명령의 경우 텍스트 파일에 해당 행이 없습니다.

비밀번호

login, enable, user passwords는 컨피그레이션에 저장되기 전에 자동으로 암호화됩니다. 예를 들어, 비밀번호 "cisco"의 암호화된 형식은 jMorNbK0514fadBh로 표시될 수 있습니다. 컨피그레이션 비밀번호를 다른 ASA에 암호화된 형식으로 복사할 수 있으나, 비밀번호의 암호를 직접 해제할 수는 없습니다.

텍스트 파일에 암호화되지 않은 비밀번호를 입력할 경우, 컨피그레이션을 ASA에 복사할 경우 ASA에서 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 컨텍스트 파일

다중 보안 컨텍스트의 경우, 전체 컨피그레이션이 다음과 같은 여러 부분으로 구성됩니다.

- 보안 컨텍스트 컨피그레이션
- 시스템 컨피그레이션 - ASA의 기본 설정(컨텍스트 목록 포함) 식별
- 관리자 컨텍스트 - 시스템 컨피그레이션에 대한 네트워크 인터페이스 제공

  시스템 컨피그레이션에는 해당 컨피그레이션 자체에 대한 인터페이스 또는 네트워크 설정이 포함되지 않습니다. 그 대신 시스템에서 네트워크 리소스에 액세스해야 할 경우(예: 서버에서 컨텍스트를 다운로드할 경우), 관리자 컨텍스트로 지정된 컨텍스트를 사용합니다.

각 컨텍스트는 단일 컨텍스트 모드 컨피그레이션과 유사합니다. 시스템 컨피그레이션은 시스템 전용 명령(예: 모든 컨텍스트의 목록)을 포함하지만 기타 일반적인 명령(예: 대다수의 인터페이스 매개변수)은 없다는 점에서 컨텍스트 구성과 다릅니다.

지원되는 문자 집합

현재 ASA CLI에서는 UTF-8 인코딩만 지원합니다. UTF-8은 Unicode 기호를 지원하는 특정 인코딩 체계이며 ASCII 기호 하위 집합과 호환되도록 설계되었습니다. ASCII 문자는 UTF-8에서 1바이트 문자로 표시됩니다. 기타 모든 문자는 UTF-8에서 멀티바이트 기호로 표시됩니다.

ASCII 인쇄 가능 문자(0x20~0x7e)는 완벽히 지원됩니다. 인쇄 가능 ASCII 문자는 ISO 8859-1과 동일합니다. UTF-8은 ISO 8859-1의 상위 집합이므로 첫 번째 256자(0-255)는 ISO 8859-1과 동일합니다. ASA CLI에서는 ISO 8859-1의 최대 255자(멀티바이트 문자)를 지원합니다.

43 장

주소, 프로토콜 및 포트

이 장에서는 IP 주소, 프로토콜 및 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 클래스 A, 클래스 B, 클래스 C로 된 3개의 다른 주소 클래스로 나뉩니다. 각 클래스는 32비트 주소 내의 다른 지점에 있는 네트워크 접두사와 호스트 번호 간의 경계를 고정합니다. 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.

사설 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 단일한 클래스 A, B 또는 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 확장된 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.

예시 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.

예시 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. 예시 1에서 점으로 구분된 십진수 마스크의 경우, 각 이진수 옥텟을 십진수 번호로 변환합니다(255.255.255.0). */비트* 마스크의 경우 1s: /24 번호를 추가합니다. 예시 2에서 십진수는 255.255.248.0 이며 /비트는 /21입니다.

확장된 네트워크 접두사에 대한 세 번째 옥텟의 일부를 사용하여 여러 개의 클래스 C 네트워크를 대규모 네트워크로 수퍼네팅(supernet)할 수 있습니다. 예를 들어, 192.168.0.0/20과 같습니다.

서브넷 마스크를 결정

표 43-1을 참조하여 원하는 호스트 개수를 기준으로 서브넷 마스크를 결정합니다.

참고 단일 호스트를 식별하는 /32를 제외하고, 서브넷의 첫 번째 및 마지막 번호는 예약됩니다.

표 43-1 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

2~254개의 호스트로 구성된 네트워크의 경우, 네 번째 옥텟은 0으로 시작하는 호스트 주소 수의 배수에 들어갑니다. 예를 들어, 표 43-2에는 192.168.0.x 형태의 호스트 서브넷(/29) 8개가 나와 있습니다.

참고 서브넷의 첫 번째 및 마지막 주소는 예약됩니다. 첫 번째 서브넷 예제에서는 192.168.0.0 또는 192.168.0.7을 사용할 수 없습니다.

표 43-2 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 254~65,534개인 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.

1단계 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.

2단계 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.

표 43-3에는 네트워크 10.1의 서브넷 16개가 나와 있습니다.

참고 서브넷의 첫 번째 및 마지막 주소는 예약됩니다. 첫 번째 서브넷 예에는 10.1.0.0 또는 10.1.15.255를 사용할 수 없습니다.

표 43-3 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.

관련 주제

11-11 페이지의 IPv6 주소 지정 구성

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). 표 43-4에는 다른 유형의 IPv6 주소의 주소 압축에 대한 몇 가지 예가 나와 있습니다.

표 43-4 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:192.168.1.1으로 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.

관련 주제

- 43-9 페이지의 IPv6 주소 접두사
- 43-7 페이지의 인터페이스 식별자
- 43-7 페이지의 IPv4 호환 IPv6 주소

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 0:0:0:0:0:0:0:1는 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.

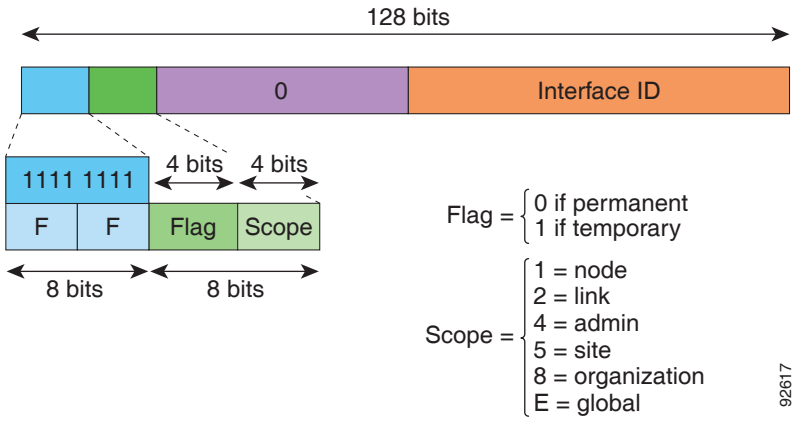
예를 들어, MAC 주소가 00E0.b601.3B7A인 인터페이스의 64비트 인터페이스 ID는 02E0:B6FF:FE01:3B7A가 될 수 있습니다.

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 플래그 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. 그림 43-1에는 IPv6 멀티캐스트 주소의 형식이 나와 있습니다.

그림 43-1 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 호스트에는 최소 다음과 같은 주소를 구성해야 합니다(자동 또는 수동으로).

- 각 인터페이스의 링크-로컬 주소
- 루프백 주소
- All Nodes 멀티캐스트 주소
- 각 유니캐스트 또는 애니캐스트 주소의 Solicited-Node 멀티캐스트 주소

IPv6 라우터에는 최소 다음과 같은 주소를 구성해야 합니다(자동 또는 수동으로).

- 필수 호스트 주소
- 라우터 역할을 수행하도록 구성된 모든 인터페이스의 Subnet-Router 애니캐스트 주소
- All-Routers 멀티캐스트 주소

IPv6 주소 접두사

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. 표 43-5에는 각 IPv6 주소 유형의 접두사가 나와 있습니다.

표 43-5 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

표 43-6에는 프로토콜 리터럴 값 및 포트 번호가 나와 있으며, 이를 ASA 명령에 입력할 수 있습니다.

표 43-6 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)
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. pptp 프로토콜 리터럴을 입력할 경우 gre 프로토콜 리터럴을 입력하는 것에 상응합니다.
snp	109	Sitara Networks Protocol

표 43-6 프로토콜 리터럴 값(계속)

리터럴	값	설명
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

표 43-7에는 프로토콜 리터럴 값 및 포트 번호가 나와 있으며, 이를 ASA 명령에 입력할 수 있습니다. 다음 주의 사항을 참조하십시오.

- ASA에서는 SQL*Net에 포트 1521를 사용합니다. 이는 SQL*Net용 Oracle에서 사용되는 기본 포트입니다. 그러나 이 값은 IANA 포트 할당과 일치하지 않습니다.
- ASA에서는 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 온라인으로 볼 수 있습니다.

http://www.iana.org/assignments/port-numbers

표 43-7 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
bootps	UDP	67	Bootstrap Protocol Server
chargen	TCP	19	Character Generator
citrix-ica	TCP	1494	Citrix Independent Computing Architecture(ICA) 프로토콜
cmd	TCP	514	**cmd**의 경우 자동 인증이 있다는 점을 제외하고 **exec**과 유사함
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time, RFC 867
discard	TCP, UDP	9	Discard
domain	TCP, UDP	53	DNS

표 43-7 포트 리터럴 값(계속)

리터럴	TCP 또는 UDP?	값	설명
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
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
https	TCP	443	HTTP over SSL
h323	TCP	1720	H.323 호출 신호
hostname	TCP	101	NIC Host Name Server
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
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	Lightweight Directory Access Protocol
ldaps	TCP	636	Lightweight Directory Access Protocol(SSL)
lpd	TCP	515	Line Printer Daemon - printer spooler
login	TCP	513	Remote login
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	Mobile IP-Agent
nameserver	UDP	42	Host Name Server
netbios-ns	UDP	137	NetBIOS Name Service
netbios-dgm	UDP	138	NetBIOS Datagram Service
NetBIOS ssn	TCP	139	NetBIOS Session Service
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	Network Time Protocol
pcanywhere-status	UDP	5632	pcAnywhere 상태
pcanywhere-data	TCP	5631	pcAnywhere 데이터
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

표 43-7 포트 리터럴 값(계속)

리터럴	TCP 또는 UDP?	값	설명
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
secureid-udp	UDP	5510	SecureID over UDP
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	Secure Shell
sunrpc (rpc)	TCP, UDP	111	Sun Remote Procedure Call
시스템 로그	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
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP	80	World Wide Web
xdmcp	UDP	177	X Display Manager Control Protocol

로컬 포트 및 프로토콜

표 43-8에는 ASA에 지정된 트래픽을 처리하기 위해 ASA에서 열 수 있는 프로토콜, TCP 포트, UDP 포트가 나와 있습니다. 표 43-8에 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 43-8 기능 및 서비스를 통해 연 프로토콜 및 포트

기능 또는 서비스	프로토콜	포트 번호	코멘트
DHCP	UDP	67,68	—
장애 조치 제어	105	N/A	—
HTTP	TCP	80	—

표 43-8 기능 및 서비스를 통해 연 프로토콜 및 포트(계속)

기능 또는 서비스	프로토콜	포트 번호	코멘트
HTTPS	TCP	443	—
ICMP	1	N/A	—
IGMP	2	N/A	목적지 IP 주소 224.0.0.1에서만 열리는 프로토콜
ISAKMP/IKE	UDP	500	구성 가능합니다.
IPsec(ESP)	50	N/A	—
IPsec over UDP(NAT-T)	UDP	4500	—
IPsec over UDP(Cisco VPN 3000 Series 호환 가능)	UDP	10000	구성 가능합니다.
IPsec over TCP(CTCP)	TCP	—	기본 포트는 사용되지 않습니다. IPsec over TCP를 구성할 경우 포트 번호를 지정해야 합니다.
NTP	UDP	123	—
OSPF	89	N/A	목적지 IP 주소 224.0.0.5 및 224.0.0.6에서만 열리는 프로토콜
PIM	103	N/A	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)	N/A	—
텔넷	TCP	23	—
VPN 로드 밸런싱	UDP	9023	구성 가능합니다.
VPN 개별 사용자 인증 프록시	UDP	1645, 1646	VPN 터널을 통해서만 액세스할 수 있는 포트입니다.

ICMP 유형

표 43-9에는 ASA 명령에 입력할 수 있는 ICMP 유형의 번호 및 이름이 나와 있습니다.

표 43-9 ICMP 유형

ICMP 번호	ICMP 이름
0	echo-reply
3	unreachable
4	source-quench

표 43-9 ICMP 유형(계속)

ICMP 번호	ICMP 이름
5	redirect
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
31	conversion-error
32	mobile-redirect