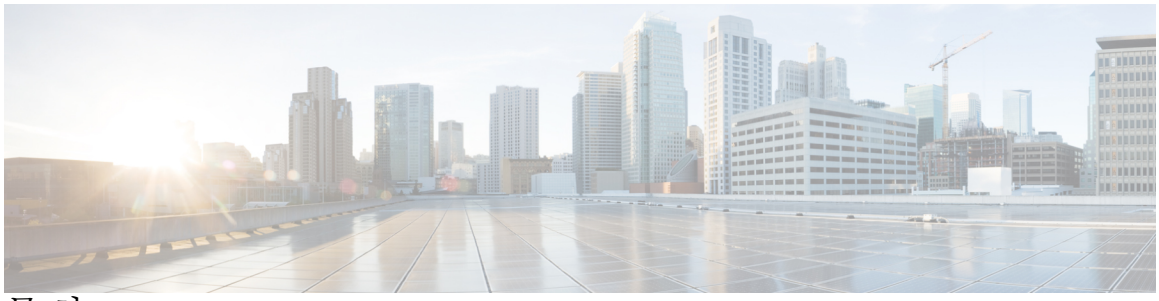
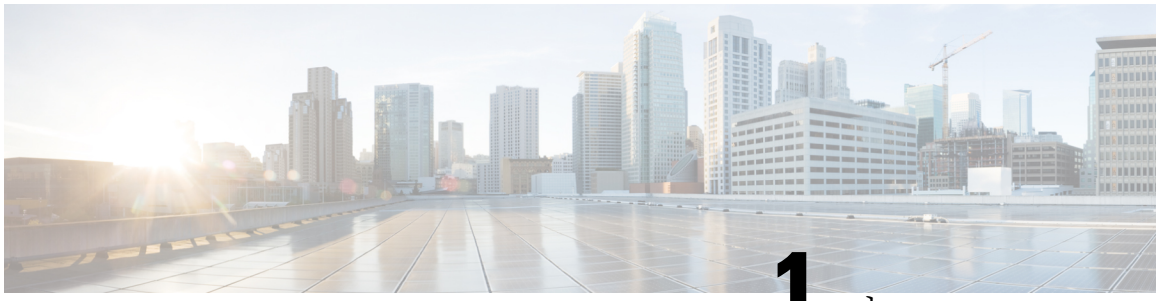
AsyncOS 12.0 for Cisco Content Security Management Appliance 사용자 가이드 - GD(일반 구축)

초판: 2019년 2월 18일

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



목 차



1 장

소개

이 장에는 다음 섹션이 포함되어 있습니다.

이 릴리스의 새로운 기능

여기서는 이번 AsyncOS for Cisco Content Security Management 릴리스의 새로운 기능 및 향상된 점을 소개합니다. 릴리스에 대한 자세한 내용은 다음 URL에 있는 제품 릴리즈 노트를 참조하십시오.

http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

업그레이드하는 경우 이전 릴리스와 이번 릴리스의 중간 단계에 있는 버전의 릴리즈 노트도 검토하여 최신 버전에서 추가된 기능 및 향상된 점을 확인해야 합니다.

표 ***1: AsyncOS 12.0***의 새로운 기능

기능	설명
보고, 격리 및 추적을 위한 새로운 웹 인터페이스	

기능	설명

	이제 이 어플라이언스에는 검색하고 볼 수 있는 새로운 웹 인터페이스가 있습니다.
	• 이메일 보고서. 이제 보고서 드롭다운 목록에서 다음 카테고리에 따라 이메일 보고서를 볼 수 있습니다.
	  • 이메일 위협 보고서
	  • 파일 및 악성코드 보고서
	  • 연결 및 플로우 보고서
	  • 사용자 리포트
	  • 필터 보고서
	  자세한 내용은 중앙 이메일 보안 보고 사용, 61 페이지장을 참조하십시오.
	• 스팸 격리
	  • 이제 웹 인터페이스의 **Quarantine(**격리**) > Spam Quarantine(**스팸 격리**) > Search(**검색**)** 페이지에서 스팸 및 의심스러운 스팸 메시지를 보고 검색할 수 있습니다.
	  • 웹 인터페이스의 **Quarantine(**격리**) > Spam Quarantine(**스팸 격리**) > Safelist(**허용 목록**)** 또는 **Blocklist(**차단 목록**)** 페이지에서 허용 목록 및 차단 목록에 추가된 도메인을 보고, 추가하고, 검색할 수 있습니다.
	  자세한 내용은 스팸 격리, 279 페이지장을 참조하십시오.
	• 정책, 바이러스 및 보안 침해 격리. 웹 인터페이스의 **Quarantine(**격리**) > Other Quarantine(**기타 격리**) > Search(**검색**)** 페이지에서 정책, 바이러스 및 보안 침해 격리를 보고 검색할 수 있습니다. 자세한 내용은 중앙 정책, 바이러스, 보안 침해 격리, 311 페이지장을 참조하십시오.
	• **Message Tracking(**메시지 추적**)**. 웹 인터페이스의 **Tracking(**추적**) > Search(**검색**)** 페이지에서 검색 기준에 따라 메시지 또는 메시지 그룹을 검색할 수 있습니다. 자세한 내용은 메시지 추적, 263 페이지장을 참조하십시오.
	중요 • 어플라이언스에서 AsyncOS API를 활성화했는지 확인합니다.
	• 어플라이언스의 레거시 웹 인터페이스에 로그인해야 합니다.
	• `trailblazerconfig`가 활성화된 경우 방화벽에서 구성된 HTTPS 포트를 열어야 합니다. 기본 HTTPS 포트는 4431입

기능	설명
	니다. 또한 어플라이언스에 액세스하기 위해 지정한 호스트 이름을 DNS 서버에서 확인할 수 있는지 확인합니다. • `trailblazerconfig`가 비활성화된 경우 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)**에서 구성된 AsycnOS API가 방화벽에서 열립니다. 기본 AsyncOS API HTTP/HTTPS 포트는 6080/6443입니다.
`trailblazerconfig` CLI 명령	`trailblazerconfig` 명령을 사용하여 새로운 웹 인터페이스의 HTTP 및 HTTPS 포트를 통해 수신 및 발신 연결을 라우팅할 수 있습니다. 참고 기본적으로 `trailblazerconfig` CLI 명령은 어플라이언스에서 활성화됩니다. 자세한 내용은 `help trailblazerconfig` 명령을 입력하여 인라인 도움말을 참고하십시오. 자세한 내용은 trailblazerconfig 명령, 485 페이지의 내용을 참고하십시오.
어플라이언스에서 민감한 정보 암호화	CLI에서 `adminaccessconfig > encryptconfig` sub 명령을 사용하여 어플라이언스에서 민감한 정보에 대한 암호화를 구성할 수 있습니다. 참고 기본적으로 어플라이언스에서는 암호화가 비활성화됩니다.
메시지 추적 향상 기능	이제 메시지의 "`Reply-To`" 헤더를 기준으로 메시지를 검색할 수 있습니다. 자세한 내용은 메시지 추적, 263 페이지의 내용을 참고하십시오.

기능	설명
AsyncOS 12.0 for Cisco Email Security Appliances의 새로운 기능 지원	이제 Security Management Appliances의 Reporting(보고) 페이지에서 다음 보고서를 볼 수 있습니다. • 외부 위협 피드 • 발신인 도메인 평판 자세한 내용은 새 웹 인터페이스의 Email Reporting(이메일 보고) 페이지 이해, 109 페이지을 참고하십시오. 이제 DANE 성공 및 DANE 실패 시나리오에 대한 발송 TLS 연결 요약을 볼 수 있습니다. 자세한 내용은 *AsyncOS 12.0 for Cisco Email Security Appliances*에 대한 사용 설명서 또는 온라인 도움말에서 명명된 엔티티의 SMTP DNS 기반 인증 섹션을 참조하십시오. 이제 다음 메시지 이벤트를 사용하여 Security Management Appliance의 Message Tracking(메시지 추적) 페이지에서 메시지를 검색할 수 있습니다. • 외부 위협 피드 • 발신인 도메인 평판 • **DANE** 오류

기능	설명
Advanced Malware Protection 보고서 향상	Advanced Malware Protection 보고서 페이지가 다음과 같이 향상되었습니다. • 새 섹션 **Incoming Malware Files by Category(**카테고리별 수신 악성코드 파일**)**에서는 카테고리가 **Custom Detection(**맞춤형 탐지**)**으로 지정되어 있고 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율을 볼 수 있습니다. AMP for Endpoints Console에서 가져온 블랙리스트에 있는 파일 SHA의 위협 이름이 보고서의 Incoming Malware Threat Files(수신 악성코드 위협 파일) 섹션에서 **Simple Custom Detection(**단순 맞춤형 탐색**)**으로 표시됩니다. • 새 섹션 - **Incoming Malware Files by Category(**카테고리별 수신 악성코드 파일**)**라는 새 섹션에서, 카테고리가 **Custom Threshold(**맞춤형 임계값**)**로 지정된 임계값 설정에 따라 블랙리스트에 있는 파일 SHA의 백분율을 볼 수 있습니다. • 보고서의 More Details(추가 세부 정보) 섹션에 있는 링크를 클릭하여 AMP for Endpoints Console에서 블랙리스트에 있는 파일 SHA의 파일 경로 분석 세부 정보를 볼 수 있습니다. • 새로운 판정 - 파일 분석 후 파일에 동적 콘텐츠가 없는 경우 **Low Risk(**낮은 위험**)**이라는 새로운 판정이 도입되었습니다. 보고서의 Incoming Files Handed by AMP(AMP를 통해 전달된 수신 파일) 섹션에서 판정 세부 정보를 볼 수 있습니다. Advanced Malware Protection 페이지 , 123 페이지를 참조하십시오.

기능	설명
웹 보고 및 추적을 위한 새로운 웹 인터페이스	이제 이 어플라이언스에는 검색하고 볼 수 있는 새로운 웹 인터페이스가 있습니다. • 웹 보고서 이제 보고서 드롭다운 목록에서 다음 카테고리에 따라 웹 기반 보고서를 볼 수 있습니다. • 일반 보고서 • 위협 보고서 • 웹 추적 검색 기준에 따라 웹 트랜잭션을 검색할 수 있습니다. Security Management Appliance에서 **Web(**웹**)** 드롭다운을 클릭하고 **Tracking(**추적**) > Web Tracking Search(**웹 추적 검색**)** 페이지를 선택합니다. 중요 • 어플라이언스에서 AsyncOS API를 활성화했는지 확인합니다. • 어플라이언스의 레거시 웹 인터페이스에 로그인해야 합니다. • `trailblazerconfig`가 활성화된 경우 방화벽에서 구성된 HTTPS 포트를 열어야 합니다. 기본 HTTPS 포트는 4431입니다. 또한 어플라이언스에 액세스하기 위해 지정한 호스트 이름을 DNS 서버에서 확인할 수 있는지 확인합니다. • `trailblazerconfig`가 비활성화된 경우 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)**에서 구성된 AsycnOS API가 방화벽에서 열립니다. 기본 AsyncOS API HTTP/HTTPS 포트는 6080/6443입니다. 자세한 내용은 중앙 웹 보고 및 추적 사용, 177 페이지장을 참조하십시오.
메트릭 표시줄 위젯	Metrics Bar(메트릭 표시줄) 위젯을 사용하면 Advanced Malware Protection 보고서 페이지에서 Cisco Threat Grid 어플라이언스가 수행한 파일 분석의 실시간 데이터를 볼 수 있습니다. 자세한 내용은 Advanced Malware Protection 페이지 , 123 페이지의 내용을 참고하십시오.

기능	설명
HTTPS 보고서 페이지	이제 HTTPS Reports(HTTPS 보고서) 보고서 페이지에서 HTTP/HTTPS 트래픽의 전체 집계 및 각 HTTP/HTTPS 트래픽에 대한 클라이언트 및 서버 측 연결 기반 암호 요약을 볼 수 있습니다. 자세한 내용은 중앙 웹 보고 및 추적 사용, 177 페이지을 참고하십시오.
Cisco Threat Response 포털에 어플라이언스 통합	Cisco Threat Response 포털에 어플라이언스를 통합하고 Cisco Threat Response 포털에서 다음 작업을 수행할 수 있습니다. • 조직의 여러 어플라이언스에서 메시지 추적 데이터를 확인합니다. • 메시지 추적에서 관찰된 위협을 식별하고 조사하고 치료합니다. • 식별된 위협을 신속하게 해결하고 식별된 위협에 대해 수행할 권장 조치를 제공합니다. • 포털에서 위협에 대해 문서화하여 조사를 저장하고, 포털의 다른 디바이스 간에 정보 협업을 활성화합니다. 자세한 내용은 네트워크 및 IP 주소 할당, 555 페이지의 내용을 참고하십시오.
웹 트래픽 TAP 정책	이제 Cisco Content Security Management Appliance를 사용하여 웹 트래픽 탭 정책을 설정할 수 있습니다. Web Security Appliance를 통과하는 웹 트래픽 중 태핑되는 웹 트래픽을 기준으로 웹 트래픽 탭 정책을 정의할 수 있습니다. Security Management Appliance의 웹 트래픽 탭 정책을 설정하려면 Web Security Appliance에서 웹 트래픽 탭 기능을 활성화해야 합니다. 이제 **Web Overview(**웹 개요**)** 보고서 페이지에 Web Traffic Tap Status(웹 트래픽 탭 상태), Web Traffic Tap Summary(웹 트래픽 탭 요약), Tapped HTTP/HTTPS Traffic(태핑된 HTTP/HTTPS 트래픽), Tapped Traffic Summary(태핑된 트래픽 요약) 섹션이 있습니다. 웹 보고 개요 , 186 페이지의 내용을 참조하십시오.
AsyncOS for Cisco Web Security Appliance의 Office 365 웹 서비스 외부 URL 카테고리 기능 지원	이 릴리스는 AsyncOS for Cisco Web Security Appliance의 Office 365 웹 서비스 외부 URL 카테고리 기능을 지원합니다. 자세한 내용은 중앙 웹 보고 및 추적 사용, 177 페이지의 내용을 참고하십시오.

동작의 변경 사항

보고서 페이지의 변경 사항	이 릴리스의 새로운 웹 인터페이스에서 다음 보고서가 변경되었습니다. • Overview(개요) 보고서 페이지 이름이 Mail Flow Summary(메일 플로우 요약)로 변경되었습니다. • Outbreak Filters(보안 침해 필터) 보고서 페이지 이름이 Outbreak Filtering(보안 침해 필터링)(신종 바이러스 필터링)으로 변경되었습니다. • Virus Types(바이러스 유형) 보고서 페이지 이름이 Virus Filtering(바이러스 필터링)으로 변경되었습니다. • Advanced Malware Protection, AMP File Analysis(AMP 파일 분석), AMP Verdict Updates(AMP 판정 업데이트) 및 Mailbox Auto Remediation(사서함 자동 교정) 보고서 페이지가 Advanced Malware Protection으로 병합되었습니다. • Incoming Mail(수신 메일) 및 Outgoing Senders(발신 발신자) 보고서 페이지가 Mail Flow Details(메일 플로우 세부 정보)로 병합되었습니다. • TLS Connections(TLS 연결) 보고서 페이지 이름이 TLS Encryption(TLS 암호화)로 변경되었습니다. • Geo-Distribution(지리적 분산) 보고서 페이지 이름이 Connection by Country(국가별 연결 수)로 변경되었습니다. • Internal Users(내부 사용자) 보고서 페이지 이름이 User Mail Summary(사용자 메일 요약)로 변경되었습니다. • Web Interaction Tracking(웹 상호 작용 추적) 보고서 페이지 이름이 Web Interaction(웹 상호 작용)으로 변경되었습니다. 자세한 내용은 새 웹 인터페이스의 Email Reporting(이메일 보고) 페이지 이해, 109 페이지을 참고하십시오.

스팸 격리의 변경 사항	이제 관리 사용자가 어플라이언스의 새로운 웹 인터페이스에서 Spam Quarantine(스팸 격리) 페이지에 액세스할 수 있습니다. **Quarantine(격리) > Spam Quarantine(스팸 격리) > Search(검색)** 페이지를 클릭하여 Spam Quarantine(스팸 격리) 페이지에 액세스할 수 있습니다. 엔드 유저는 이제 새로운 웹 인터페이스의 스팸 격리 포털에 액세스할 수 있습니다. 자세한 내용은 웹 인터페이스 액세스 , 23 페이지를 참고하십시오. 참고 로컬 및 외부 인증 사용자는 엔드 유저 스팸 격리 포털에 로그인할 수 없습니다. 이제 새로운 웹 인터페이스에 대한 링크가 포함된 스팸 알림이 수신됩니다. 어플라이언스에서 AsyncOS API HTTP/HTTPS 포트 및 HTTP/HTTPS 서비스를 활성화했는지 확인합니다. 다른 인터페이스(데이터 1)에서 스팸 격리를 사용하는 경우에는 이를 기본 인터페이스로 설정해야 합니다. `trailblazerconfig`가 활성화된 경우 (데이터 1) 인터페이스에서 AsyncOS API 포트(HTTP/HTTPS) 및 HTTP/HTTPS 서비스를 활성화해야 합니다. `trailblazerconfig`가 비활성화된 경우 (데이터 1) 인터페이스에서 AsyncOS API 포트(HTTP/HTTPS)를 활성화해야 합니다. 자세한 내용은 trailblazerconfig 명령, 485 페이지의 내용을 참고하십시오.
암호 암호화	이 릴리스로 업그레이드한 후에는 어플라이언스에서 구성 파일을 업데이트할 때 사용자의 암호를 암호화할 수 있습니다. 암호를 암호화하려면 다음 중 하나를 수행합니다. • **System Administration(시스템 관리) > Configuration File(구성 파일)** 페이지에서 **Encrypt passphrases in the Configuration Files(구성 파일에서 암호 암호화)** 확인란을 선택합니다. • CLI에서 `saveconfig` 명령을 사용하여 암호를 암호화합니다.
만료 후 사용자의 암호 변경	사용자 계정이 만료되면 암호를 변경하라는 메시지가 표시됩니다. 자세한 내용은 만료 후 사용자의 암호 변경, 412 페이지을 참고하십시오.

데모 인증서 변경 사항	이 릴리스 이전에는 어플라이언스가 사전 구성된 데모 인증서로 TLS 연결을 활성화했습니다. 이 릴리스로 업그레이드한 후에는 어플라이언스가 고유 인증서를 생성하여 TLS 연결을 활성화합니다. 다음 구성에서 사용된 기존 데모 인증서는 새 인증서로 대체됩니다. • 메일 전달 • LDAP • 네트워킹 • URL 필터링 • SMTP 서비스

웹 인터페이스 비교 - 과 이전 릴리스, 11 페이지도 참고하십시오.

웹 인터페이스 비교 - 과 이전 릴리스

다음 표에서는 새로운 웹 인터페이스와 이전 버전을 비교하여 보여 줍니다.

표 *2:* 새로운 웹 인터페이스와 이전 릴리스의 비교

웹 인터페이스 페이지 또는 요소	새로운 웹 인터페이스	레거시 웹 인터페이스
랜딩 페이지	Cloud Email Security Management Console에 로그인하면 Mail Flow Summary(메일 플로우 요약) 페이지가 표시됩니다.	어플라이언스에 로그인하면 System Status(시스템 상태) 페이지가 표시됩니다.
Product(제품) 드롭다운	Product(제품) 드롭다운에서 Email Security Appliance와 Web Security Appliance 간에 전환할 수 있습니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.	Email(이메일) 또는 Web(웹) 탭을 사용하여 Email Security Appliance와 Web Security Appliance 간에 전환할 수 있습니다.
Reports(보고서) 드롭다운	Reports(보고서) 드롭다운에서 Email Security Appliance와 Web Security Appliance에 대한 보고서를 볼 수 있습니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.	Reporting(보고) 드롭다운 메뉴에서 Email Security Appliance와 Web Security Appliance에 대한 보고서를 볼 수 있습니다.

웹 인터페이스 페이지 또는 요소	새로운 웹 인터페이스	레거시 웹 인터페이스
Management Appliance(관리 어플라이언스) 탭	Management Appliance(관리 어플라이언스) 탭에 액세스하려면 Cloud Email Security Management Console에서 ⚙을 클릭합니다.	네트워크 액세스 구성 및 시스템 상태 모니터링 외에 보고, 메시지 추적 및 격리를 활성화하고 구성할 수 있습니다.
내 보고서 페이지	My Reports(내 보고서) 페이지에 액세스하려면 Cloud Email Security Management Console에서 ⚙을 클릭하고 **Email(**이메일**) > Reporting(**보고**) > My Reports(**내 보고서**)**를 선택합니다.	기존 보고서 페이지의 차트(그래프)와 테이블을 조합하여 보고서 대시보드를 맞춤화할 수 있습니다.
보고 데이터 가용성 페이지	Reporting Data Availability(보고 데이터 가용성) 페이지에 액세스하려면 Cloud Email Security Management Console에서 ⚙을 클릭하고 **Email(**이메일**) > Reporting(**보고**) > Reporting Data Availability(**보고 데이터 가용성**)**를 선택합니다.	데이터를 보고 업데이트하고 정렬하면서 리소스 사용 및 이메일 트래픽 문제 지점을 실시간으로 파악할 수 있습니다.
보고서 예약 및 보관	보고서를 예약하려면 Cloud Email Security Management Console에서 ⚙을 클릭하고 **Email(**이메일**) > Reporting(**보고**) > Scheduled Reports(**예약 보고서**)**를 선택합니다. 보고서를 보관하려면 Cloud Email Security Management Console에서 ⚙을 클릭하고 **Email(**이메일**) > Reporting(**보고**) > Archive Reports(**보고서 보관**)**를 선택합니다.	Security Management Appliance의 **Email(**이메일**) > Reporting(**보고**) > Scheduled Reports(**예약 보고서**)** 페이지를 사용하여 보고서를 예약하고, **Email(**이메일**) > Reporting(**보고**) > Archive Reports(**보고서 보관**)** 페이지를 사용하여 보고서를 보관할 수 있습니다.

웹 인터페이스 페이지 또는 요소	새로운 웹 인터페이스	레거시 웹 인터페이스
Reporting Overview(보고 개요) 페이지	Security Management Appliance의 Email Reporting Overview(이메일 보고 개요) 페이지가 새 웹 인터페이스에서 Mail Flow Summary(메일 플로우 요약) 페이지로 변경되었습니다. Mail Flow Summary(메일 플로우 요약) 페이지에는 수신 및 발신 메시지에 대한 트렌드 그래프와 요약 테이블이 포함되어 있습니다.	Security Management Appliance의 Email Reporting Overview(이메일 보고 개요) 페이지는 Email Security Appliance에서 발생한 이메일 메시지 활동의 개요를 제공합니다. Overview(개요) 페이지에는 수신 및 발신 메시지에 대한 그래프와 요약 테이블이 포함되어 있습니다.
Advanced Malware Protection 보고서 페이지	Reports(보고서) 메뉴의 **Advanced Malware Protection** 보고서 페이지에서는 다음 섹션을 사용할 수 있습니다. • Summary(요약) • AMP 파일 평판 • 파일 분석 • 파일 회귀 분석 • 사서함 자동 치료	Security Management Appliance의 **Email(**이메일**) > Reporting(**보고**)** 드롭다운 메뉴에는 다음 Advanced Malware Protection 보고서 페이지가 있습니다. • AMP(Advanced Malware Protection) • AMP 파일 분석 • AMP 판정 업데이트 • 사서함 자동 치료
Outbreak Filters 페이지	새 웹 인터페이스의 Outbreak Filtering(보안 침해 필터링) 보고서 페이지에서는 Past Year Virus Outbreaks(지난해 바이러스 보안 침해) 및 Past Year Virus Outbreak Summary(지난해 바이러스 보안 침해 요약)를 사용할 수 없습니다.	**Email(**이메일**) > Reporting Outbreak Filters(Outbreak Filter** 보고**)** 페이지에 Past Year Virus Outbreaks(지난해 바이러스 보안 침해)와 Past Year Virus Outbreak Summary(지난해 바이러스 보안 침해 요약)가 표시됩니다.

웹 인터페이스 페이지 또는 요소	새로운 웹 인터페이스	레거시 웹 인터페이스
스팸 격리(관리 사용자 및 엔드 유저)	새 웹 인터페이스에서 **Quarantine(**격리**) > Spam Quarantine(**스팸 격리**) > Search(**검색**)**를 클릭합니다. 엔드 유저는 https://example.com:<https-api-port>/euq-login URL을 사용하여 스팸 격리에 액세스할 수 있습니다. 여기서 example.com은 어플라이언스 호스트 이름이고, <https-api-port>는 방화벽에서 열린 AsyncOS API HTTPS 포트입니다.	-
정책, 바이러스 및 신종 바이러스 격리	새 웹 인터페이스에서 **Quarantine(**격리**) > Other Quarantine(**기타 격리**)**을 클릭합니다. 새로운 웹 인터페이스에서는 Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(보안 침해 격리)만 볼 수 있습니다.	어플라이언스에서 Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(보안 침해 격리)를 보고, 구성하고, 수정할 수 있습니다.
격리의 메시지에 대해 모든 작업 선택	여러(또는 모든) 메시지를 선택하여 삭제, 지연, 릴리스, 이동 등과 같은 메시지 작업을 수행할 수 있습니다.	여러 메시지를 선택하여 메시지 작업을 수행할 수 없습니다.
첨부 파일에 대한 최대 다운로드 제한	격리된 메시지의 첨부 파일에 대한 최대 다운로드 제한이 25MB로 제한되어 있습니다.	-
거부된 연결	거부된 연결을 검색하려면 Cloud Email Security Management Console에서 **Tracking(**추적**) > Search(**검색**) > Rejected Connection(**거부된 연결**)** 탭을 클릭합니다.	-
쿼리 설정	Message Tracking(메시지 추적) 기능의 Query Settings(쿼리 설정) 필드는 Cloud Email Security Management Console에서 사용할 수 없습니다.	Message Tracking(메시지 추적) 기능의 Query Settings(쿼리 설정) 필드에 쿼리 시간 초과를 설정할 수 있습니다.

웹 인터페이스 페이지 또는 요소	새로운 웹 인터페이스	레거시 웹 인터페이스
메시지 추적 데이터 가용성	Message Tracking Data Availability(메시지 추적 데이터 가용성) 페이지에 액세스하려면 Cloud Email Security Management Console에서 ⚙을 클릭하고 **Email(**이메일**) > Message Tracking(**메시지 추적**) > Message Tracking Data Availability(**메시지 추적 데이터 가용성**)**를 선택합니다.	어플라이언스의 누락된 데이터 간격을 볼 수 있습니다.
메시지의 추가 세부 정보 표시	Verdict Charts(판정 차트), Last State(마지막 상태), Sender Groups(발신자 그룹), Sender IP(발신자 IP), SBRS Score(SBRS 점수) 및 Policy Match(정책 일치) 세부 정보 같은 메시지의 추가적인 세부 정보를 볼 수 있습니다.	-
Verdict Charts(판정 차트) 및 Last State Verdicts(마지막 상태 판정)	Verdict Charts(판정 차트)에는 어플라이언스의 각 엔진에 의해 트리거되는 가능한 여러 가지 판정에 대한 정보가 표시됩니다. 메시지의 Last State(마지막 상태)에 따라 엔진의 가능한 모든 판정 후에 트리거되는 최종 판정이 결정됩니다.	메시지의 Verdict Charts(판정 차트) 및 Last State Verdicts(마지막 상태 판정)는 사용할 수 없습니다.
Message Details(메시지 세부 정보)의 메시지 첨부 파일 및 호스트 이름	Cloud Email Security Management Console에서 메시지의 Message Details(메시지 세부 정보) 섹션에 메시지 첨부 파일 및 호스트 이름이 표시되지 않습니다.	메시지의 Message Details(메시지 세부 정보) 섹션에 메시지 첨부 파일 및 호스트 이름이 표시됩니다.
Message Details(메시지 세부 정보)의 Sender Groups(발신자 그룹), Sender IP(발신자 IP), SBRS Score(SBRS 점수) 및 Policy Match(정책 일치)	Cloud Email Security Management Console의 Message Details(메시지 세부 정보) 섹션에 메시지의 Sender Groups(발신자 그룹), Sender IP(발신자 IP), SBRS Score(SBRS 점수) 및 Policy Match(정책 일치) 세부 정보가 표시됩니다.	메시지의 Message Details(메시지 세부 정보) 섹션에서 Sender Groups(발신자 그룹), Sender IP(발신자 IP), SBRS Score(SBRS 점수) 및 Policy Match(정책 일치)를 사용할 수 없습니다.

웹 인터페이스 페이지 또는 요소	새로운 웹 인터페이스	레거시 웹 인터페이스
메시지의 방향(수신 또는 발신)	Cloud Email Security Management Console의 메시지 추적 결과 페이지에 메시지의 방향(수신 또는 발신)이 표시됩니다.	메시지 추적 결과 페이지에 메시지의 방향(수신 또는 발신)이 표시되지 않습니다.

Cisco Content Security Management 개요

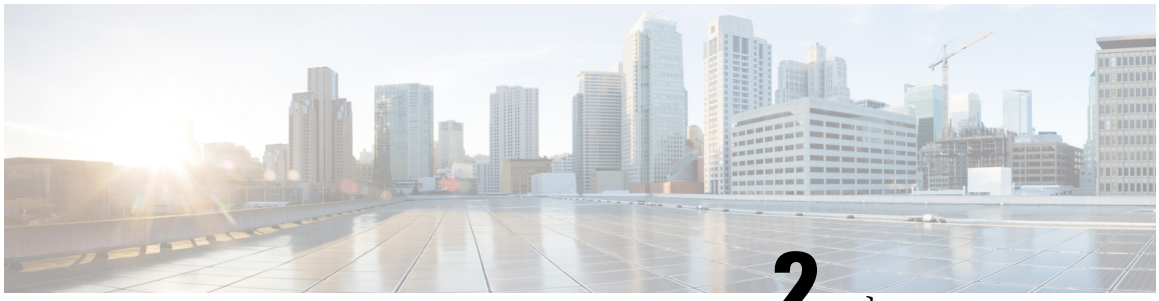
AsyncOS for Cisco Content Security Management는 다음 기능을 제공합니다.

- 외부 스팸 격리**:** 엔드 유저를 위해 스팸 및 의심스러운 스팸 메시지를 보관하며, 엔드 유저 및 관리자는 최종 결정을 내리기 전에 스팸으로 플래그가 지정된 메시지를 검토할 수 있습니다.
- 중앙 집중식 정책**,** 바이러스 및 보안 침해 격리**:** 이러한 격리 및 여러 Email Security Appliance에서 와서 이곳에 격리된 메시지를 관리하기 위한 단일 인터페이스를 제공합니다. 격리된 메시지를 방화벽 뒤에 저장할 수 있습니다.
- 중앙 집중식 보고**:** 여러 Email/Web Security Appliance에서 온 집계된 데이터에 대한 보고서를 실행합니다. 개별 어플라이언스에서 사용할 수 있는 동일한 보고 기능을 Security Management Appliance에서도 사용할 수 있습니다.
- 중앙 집중식 추적**:** 예전에는 여러 Email Security Appliance 및 Web Security Appliance에서 처리하던 이메일 메시지 및 웹 트랜잭션을 단일 인터페이스에서 추적합니다.
- **Web Security Appliance**를 위한 중앙 집중식 구성 관리**:**간소화 및 일관성을 위해 여러 Web Security Appliance의 정책 정의 및 정책 구축을 관리합니다.

  참고 Security Management Appliance는 중앙 집중식 이메일 관리 또는 Email Security Appliance의 '클러스터링'에 관여하지 않습니다.

- 데이터 백업**:** Security Management Appliance에서 보고 및 추적 데이터, 격리된 메시지, 안전한/차단된 발신자 목록 등의 데이터를 백업합니다.

보안 작업을 Security Management Appliance 하나만 사용하여 조율하거나 로드를 여러 개의 어플라이언스로 분산할 수 있습니다.



2 장

설정, 설치, 기본 구성

이 장에는 다음 섹션이 포함되어 있습니다.

솔루션 구축 개요

Cisco Content Security Management Appliance에서 Cisco Content Security 솔루션에 서비스를 제공하도록 구성하려면

	어플라이언스	수행해야 할 작업	추가 정보
1단계	모든 어플라이언스	어플라이언스가 사용할 기능에 대한 시스템 요구 사항을 충족함을 확인합니다. 필요하다면 어플라이언스를 업그레이드합니다.	
2단계	Email Security Appliance	중앙 집중식 서비스를 환경에 도입하기 전, 원하는 보안 기능을 제공하도록 모든 Email Security Appliance를 구성하고 각 어플라이언스에서 모든 기능이 예상대로 작동하는지 확인합니다.	Cisco Email Security 릴리스에 대한 문서를 참조하십시오.
3단계	Web Security Appliance	중앙 집중식 서비스를 환경에 도입하기 전, 원하는 보안 기능을 제공하도록 Web Security Appliance를 하나 이상 구성하고 모든 기능이 예상대로 작동하는지 확인합니다.	AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

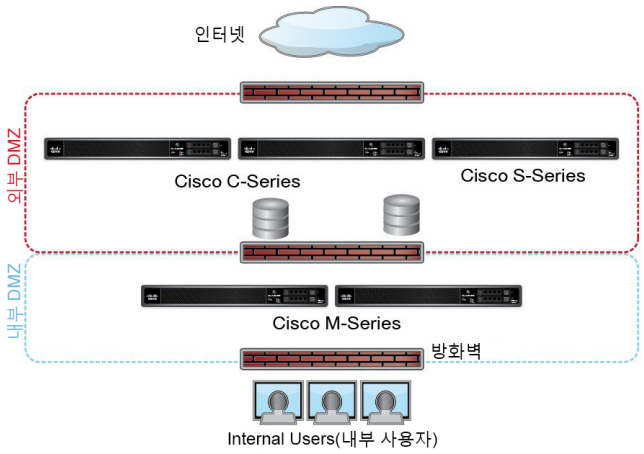
	어플라이언스	수행해야 할 작업	추가 정보
4단계	Security Management Appliance	어플라이언스를 설정하고 시스템 설정 마법사를 실행합니다.	설치 계획 , 18 페이지, 설정 준비 , 19 페이지, 시스템 설정 마법사 실행, 25 페이지를 참조하십시오.
5단계	모든 어플라이언스	구축하려는 각 중앙 서비스를 구성합니다.	Security Management Appliance의 서비스 구성, 30 페이지로 시작합니다.

설치 계획

네트워크 계획

Security Management Appliance에서는 최종 사용자 애플리케이션을 DMZ에 상주하는 좀 더 안전한 게이트웨이 시스템과 분리할 수 있습니다. 2-레이어 방화벽을 사용하면 엔드 유저가 외부 DMZ에 직접 연결하지 않도록 유연하게 네트워크를 계획할 수 있습니다.

그림 ***1: Security Management Appliance***를 통합하는 일반적인 네트워크 구성



다음 그림은 Security Management Appliance 및 여러 DMZ를 통합하는 일반적인 네트워크 구성을 보여줍니다. Security Management Appliance를 내부 네트워크에서 DMZ 외부에 구축합니다. 모든 연결은 Security Management Appliance(M-Series)에서 시작되어, 관리되는 Email Security Appliance(C-Series) 및 관리되는 Web Security Appliance(S-Series)로 이어집니다.

회사 데이터 센터는 Security Management Appliance를 공유하여 Web 및 Email Security Appliance에 대한 중앙 집중식 보고와 메시지 추적을 수행하고, 여러 Web Security Appliance에 대한 중앙 집중식 정

책 구성을 수행할 수 있습니다. Security Management Appliance를 외부 스팸 격리로 사용할 수도 있습니다.

Email Security Appliance 및 Web Security Appliance를 Security Management Appliance에 연결하고 모든 어플라이언스를 적절히 구성하면, AsyncOS는 관리되는 어플라이언스에서 데이터를 수집 및 집계합니다. 집계된 데이터에서 보고서를 생성할 수 있으며, 이메일 및 웹 사용의 전체적인 보기를 확인할 수 있습니다.

Security Management Appliance와 Email Security Appliance의 통합 정보

Security Management Appliance와 Email Security Appliance의 통합에 대한 자세한 내용은 Email Security Appliance용 사용 설명서 또는 온라인 도움말의 "Cisco Content Security Management Appliance에서 서비스 중앙 집중화" 장을 참조하십시오.

클러스터링된 Email Security Appliance와의 구축

Security Management Appliance는 이메일 어플라이언스의 중앙 집중식 관리 기능을 사용하는 Email Security Appliance의 클러스터에 둘 수 없습니다. 그러나 클러스터링된 Email Security Appliance는 중앙 집중식 보고와 추적을 위해 그리고 메시지 격리를 위해 Security Management Appliance에 메시지를 전달할 수 있습니다.

설정 준비

시스템 설정 마법사를 실행하기 전에

단계 **1** 해당 제품의 최신 릴리즈 노트를 검토합니다. 네트워크 계획 , 18 페이지를 참조하십시오.

단계 **2** 보안 솔루션 구성 요소의 호환성을 확인합니다. 를 참조하십시오.

단계 **3** 네트워크 및 물리적 공간에서 이 구축을 지원할 준비가 되었음을 확인합니다. 설치 계획 , 18 페이지를 참조하십시오.

단계 **4** Security Management Appliance를 물리적으로 설치하고 연결합니다. 어플라이언스의 물리적 설정 및 연결 , 19 페이지를 참조하십시오.

단계 **5** 네트워크 및 IP 주소 할당을 확인합니다. 네트워크 및 IP 주소 지정 확인, 20 페이지를 참조하십시오.

단계 **6** 시스템 설정에 대한 정보를 수집합니다. 설정 정보 수집, 20 페이지를 참조하십시오.

어플라이언스의 물리적 설정 및 연결

이 장의 절차를 따르기 전에 어플라이언스와 함께 제공된 빠른 시작 설명서에 나온 단계를 완료합니다. 이 가이드에서는 어플라이언스의 포장을 풀고 랙에 물리적으로 설치한 후 전원을 켠 것으로 가정합니다.

GUI에 로그인하려면 우선 PC와 Security Management Appliance 간 프라이빗 연결을 설정해야 합니다. 예를 들어, 포함된 크로스오버 케이블을 사용하여 어플라이언스의 Management 포트에서 랩톱으로 직접 연결할 수 있습니다. 선택적으로, PC와 네트워크(예: 이더넷 허브) 간 그리고 네트워크와 Security Management Appliance의 Management 포트 간에 이더넷을 통해 연결할 수 있습니다.

네트워크 및 IP 주소 지정 확인

참고 어플라이언스를 이미 네트워크에 연결한 경우 Content Security Appliance의 기본 IP 주소가 네트워크의 다른 IP 주소와 충돌하지 않는지 확인합니다. 각 어플라이언스의 Management 포트에 사전 구성된 IP 주소는 192.168.42.42입니다.

설정 후 Security Management Appliance의 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)** 페이지로 이동하여 Security Management Appliance가 사용하는 인터페이스를 변경합니다.

사용하기 위해 선택하는 각 이더넷 포트에 대한 다음 네트워크 정보가 필요합니다.

- IP 주소
- Netmask

또한 전체 네트워크에 대한 다음 정보가 필요합니다.

- 네트워크에서 기본 라우터의 IP 주소(게이트웨이)
- DNS 서버의 IP 주소 및 호스트 이름(인터넷 루트 서버를 사용하려는 경우 필요하지 않음)
- NTP 서버의 호스트 이름 또는 IP 주소(수동으로 시스템 시간을 설정하는 경우에는 필요 없음)

자세한 내용은 네트워크 및 IP 주소 할당, 555 페이지을 참고하십시오.

참고 인터넷과 Content Security Appliance 간의 네트워크에서 방화벽을 실행하는 중이라면 어플라이언스가 제대로 작동하기 위해서는 특정 포트를 열어야 하는 경우도 있습니다. 방화벽에 대한 자세한 내용은 방화벽 정보, 563 페이지를 참조하십시오.

Email Security Appliance로 이메일 메시지를 보내고 받는 데 Security Management Appliance에서 항상 동일한 IP 주소를 사용하십시오. 자세한 내용은 Email Security Appliance용 문서에서 메일 플로우에 대한 정보를 참조하십시오.

Cisco Content Security Management Appliance와 여기에서 관리하는 어플라이언스 간 통신에는 IPv6이 지원되지 않습니다.

설정 정보 수집

다음 표를 참조하여 시스템 설정에 대한 정보를 수집합니다. 시스템 설정 마법사를 실행할 때 이 정보가 있어야 합니다.

참고 네트워크 및 IP 주소에 대한 자세한 내용은 네트워크 및 IP 주소 할당, 555 페이지을 참조하십시오.

다음 표 시스템 설정 워크시트 표시

1	알림		시스템 알림이 전송되는 이메일 주소:
2	시스템 시간		NTP 서버(IP 주소 또는 호스트 이름):
3	관리자 암호		“admin” 계정의 새 암호를 선택합니다.
4	AutoSupport		AutoSupport 활성화 여부? ___ 예 ___ 아니요
5	호스트 이름		Security Management Appliance의 인증된 호스트 이름:
6	인터페이스/IP 주소		IP 주소:
			넷마스크:
7	네트워크	게이트웨이	기본 게이트웨이(라우터) IP 주소:
		DNS	___ 인터넷 루트 DNS 서버 사용
			___ 이 DNS 서버 사용:

Security Management Appliance 액세스

Security Management Appliance에는 표준 웹 기반 GUI, 스팸 격리 관리를 위한 별도의 웹 기반 인터페이스, CLI, 특정 기능에 대한 액세스 권한이 부여된 관리 사용자용 특수 또는 제한된 웹 인터페이스가 있습니다.

- 브라우저 요구 사항, 21 페이지
- 웹 인터페이스 액세스 정보 , 22 페이지
- 웹 인터페이스 액세스 , 23 페이지
- CLI(Command Line Interface) 액세스, 24 페이지
- 지원되는 언어, 24 페이지

브라우저 요구 사항

GUI에 액세스하려면 브라우저가 JavaScript 및 쿠키를 지원하고 허용해야 하며, CSS(Cascading Style Sheets)가 포함된 HTML 페이지를 렌더링할 수 있어야 합니다.

표 *3:* 지원되는 브라우저 및 릴리스

브라우저	**Windows 7**	**MacOS 10.6**
Safari	—	7.0 이상
Google Chrome	안정적인 최신 버전	안정적인 최신 버전
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	안정적인 최신 버전	안정적인 최신 버전

- Internet Explorer 11.0(Windows 7에만 해당)
- Safari(7 이상)
- Firefox(최신 안정적인 버전)
- Google Chrome(안정적인 최신 버전)

브라우저는 브라우저에서 공식적으로 지원되는 운영 체제에서만 지원됩니다.

인터페이스의 일부 버튼 또는 링크를 사용하면 창이 추가로 열리므로 GUI를 사용하려면 브라우저의 팝업 차단 설정을 구성해야 합니다.

참고 모든 브라우저에서 AsyncOS(11.4 이상) 웹 인터페이스에 가장 적합한 해상도는 1366x786입니다.

웹 인터페이스 액세스 정보

Security Management Appliance에는 포트 80에서 기본적으로 사용할 수 있는 표준 관리자 인터페이스 및 포트 82에서 기본적으로 사용할 수 있는 스팸 격리 최종 사용자 인터페이스, 이렇게 두 개의 웹 인터페이스가 있습니다. 스팸 격리 HTTPS 인터페이스는 기본적으로 포트 83을 사용합니다(활성화된 경우).

각 웹 인터페이스를 구성할 때(Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)**로 이동) HTTP 또는 HTTPS를 지정할 수 있으므로, 세션 중 두 인터페이스 간에 전환하는 경우 재인증이 필요할 수 있습니다. 예를 들어 포트 80에서 HTTP를 통해 관리자 웹 인터페이스에 액세스하다가 동일한 브라우저를 사용하여 포트 83에서 HTTPS를 통해 스팸 격리 최종 사용자 웹 인터페이스에 액세스하는 경우, 관리자 웹 인터페이스로 돌아갈 때 재인증 요청 메시지가 표시될 수 있습니다.

참고 - GUI에 액세스할 때, Security Management Appliance를 변경하기 위해 여러 브라우저 창 또는 탭을 동시에 사용하면 안 됩니다. 동시 GUI 및 CLI 세션도 사용하지 마십시오. 그러한 사용 방식은 지원되지 않으며 예기치 않은 동작의 원인이 될 수 있습니다.

- 기본적으로 30분 넘게 유휴 상태이거나 로그아웃하지 않고 브라우저를 닫으면 세션이 시간 초과됩니다. 그러한 경우 사용자 이름과 암호를 재입력해야 합니다. 시간 초과 한도를 변경하려면 웹 UI 세션 시간 초과 구성, 425 페이지를 참조하십시오.

웹 인터페이스 액세스

단계 **1** 웹 브라우저를 열고 IP 주소 텍스트 필드에 `192.168.42.42`를 입력합니다.

단계 **2** [새로운 웹 인터페이스에만 해당] 다음 방법 중 하나를 사용하여 새로운 웹 인터페이스에 액세스할 수 있습니다.

- `trailblazerconfig` CLI 명령이 활성화된 경우 다음 URL 사용 - `https://example.com:<trailblazer-https-port>/ng-login`

  여기서 `example.com`은 어플라이언스 호스트 이름이고, `<trailblazer-https-port>`는 어플라이언스에 구성된 trailblazer HTTPS 포트입니다.

  trailblazerconfig CLI 명령에 대한 자세한 내용은 trailblazerconfig 명령, 485 페이지을 참고하십시오.

- `trailblazerconfig` CLI 명령이 비활성화된 경우 다음 URL 사용 - `https://example.com:<https-port>/ng-login`

  여기서 example.com은 어플라이언스 호스트 이름이고, `<https-port>`는 어플라이언스에 구성된 HTTPS 포트입니다.

- 레거시 웹 인터페이스에 로그인하여 **Cloud Email Security**를 클릭하면 의 모양이 바뀝니다**. Try It!!(**시도**)** 링크를 클릭하면 새로운 웹 인터페이스에 액세스됩니다.

중요
- 어플라이언스에서 AsyncOS API를 활성화했는지 확인합니다.
- 어플라이언스의 레거시 웹 인터페이스에 로그인해야 합니다.
- `trailblazerconfig`가 활성화된 경우 방화벽에서 구성된 HTTPS 포트를 열어야 합니다. 기본 HTTPS 포트는 4431입니다.

  또한 어플라이언스에 액세스하기 위해 지정한 호스트 이름을 DNS 서버에서 확인할 수 있는지 확인합니다.
- `trailblazerconfig`가 비활성화된 경우 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)**에서 구성된 AsycnOS API가 방화벽에서 열립니다. 기본 AsyncOS API HTTP/HTTPS 포트는 6080/6443입니다.

단계 **3** 다음 기본값을 입력합니다.

- 사용자 이름: **admin**

- 암호: **ironport**

참고 웹 인터페이스 또는 명령행 인터페이스를 사용하여 시스템 설정 마법사를 완료하면 이 passphrase는 유효하지 않습니다.

레거시 웹 인터페이스 액세스

참고 레거시 웹 인터페이스에 액세스하려면 Security Management Appliance에 로그인해야 합니다. 자세한 내용은 웹 인터페이스 액세스 , 23 페이지을 참조해 주십시오.

보고, 메시지 추적, 격리, 네트워크 액세스 및 시스템 상태 모니터링을 활성화하고 구성하려면, 레거시 웹 인터페이스에 액세스해야 합니다.

새로운 웹 인터페이스에서 레거시 웹 인터페이스에 액세스하려면 다음 그림에서 보듯이 기어 아이콘 을 클릭합니다.

그림 *2:* 다음 위치에서 레거시 웹 인터페이스 액세스

새 브라우저 창에 레거시 웹 인터페이스가 열립니다. 여기에 액세스하려면 다시 로그인해야 합니다.

어플라이언스에서 완전히 로그아웃하려면 어플라이언스의 신규 및 레거시 웹 인터페이스에서 모두 로그아웃해야 합니다.

CLI(Command Line Interface) 액세스

모든 Cisco Content Security Appliance에서와 같은 방법으로 Security Management Appliance에서 CLI에 액세스할 수 있습니다. 그러나 몇 가지 차이점이 있습니다.

- 시스템 설정은 반드시 GUI를 통해 수행해야 합니다.
- 일부 CLI 명령은 Security Management Appliance에서 사용할 수 없습니다. 지원되지 않는 명령 목록은 Cisco Content Security Appliance용 IronPort AsyncOS CLI 참조 설명서를 참조하십시오.

프로덕션 구축의 경우 SSH를 사용하여 CLI에 액세스해야 합니다. 포트 22에서 어플라이언스에 액세스하려면 표준 SSH 클라이언트를 사용합니다. 랩 구축의 경우 텔넷도 사용할 수 있습니다. 그러나 이 프로토콜은 암호화되지 않습니다.

지원되는 언어

알맞은 라이센스 키가 있으면 AsyncOS에서 GUI 및 CLI를 다음 언어로 표시할 수 있습니다.

- 영어

- 프랑스어
- 스페인어
- 독일어
- 이탈리아어
- 한국어
- 일본어
- 포르투갈어(브라질)
- 중국어(번체 및 간체)
- 러시아어

GUI 및 기본 보고 언어를 선택하려면 다음 중 하나를 수행합니다.

- 언어 기본 설정을 수행합니다. 기본 설정 , 500 페이지를 참조하십시오.
- GUI 창 오른쪽 위의 Options(옵션) 메뉴를 사용하여 세션을 위한 언어를 선택합니다.

그 방법은 로그인 자격 증명 인증에 쓰인 방법에 따라 달라집니다.

시스템 설정 마법사 실행

AsyncOS에서는 브라우저 기반 시스템 설정 마법사를 제공하여 시스템 구성 프로세스를 안내합니다. 나중에 이 마법사에서 제공하지 않은 맞춤 구성 옵션을 활용해야 하는 경우도 있습니다. 그러나 완전한 구성을 보장하기 위해 초기 설정에는 반드시 마법사를 사용해야 합니다.

Security Management Appliance는 GUI를 통해서만 이 마법사를 지원합니다. CLI를 통한 시스템 설정은 지원하지 않습니다.

- 시작하기 전에 , 25 페이지
- 시스템 설정 마법사 개요 , 26 페이지

시작하기 전에

설정 준비 , 19 페이지의 모든 작업을 완료합니다.

⚠

주의 시스템 설정 마법사는 어플라이언스를 완전히 재구성합니다. 어플라이언스를 처음 설치할 때 또는 기존 구성을 완전히 덮어쓰고자 할 때만 마법사를 사용하십시오.

Management 포트를 통해 Security Management Appliance를 네트워크에 연결해야 합니다.

⚠

주의 Security Management Appliance는 관리 포트의 기본 IP 주소가 192.168.42.42입니다. Security Management Appliance를 네트워크에 연결하기 전에 이 공장 기본 설정과 충돌하는 다른 장비의 IP 주소가 없는지 확인해 주십시오.

참고 기본적으로 30분 넘게 유휴 상태이거나 로그아웃하지 않고 브라우저를 닫으면 세션이 시간 초과됩니다. 그러한 경우 사용자 이름과 암호를 재입력해야 합니다. 시스템 설정 마법사를 실행하는 동안 세션이 시간 초과되면 처음부터 다시 시작해야 합니다. 시간 초과 한도를 변경하려면 웹 UI 세션 시간 초과 구성, 425 페이지를 참조하십시오.

시스템 설정 마법사 개요

단계 **1** 시스템 설정 마법사 구동 , 26 페이지

단계 **2** 최종 사용자 라이센스 계약 검토, 27 페이지

단계 **3** 시스템 설정 구성, 27 페이지

- 알림 설정 및 AutoSupport
- 시스템 시간 설정
- 관리자 암호

단계 **4** 네트워크 설정 구성, 27 페이지

- 어플라이언스의 호스트 이름
- 어플라이언스의 IP 주소, 네트워크 마스크, 게이트웨이
- 기본 라우터 및 DNS 설정

단계 **5** 구성 검토, 28 페이지

마법사 페이지를 진행하고 4단계에서 구성을 면밀하게 검토합니다. **Previous(**이전**)**를 클릭하여 1단계 전으로 돌아갈 수 있습니다. 프로세스가 끝나면 마법사는 변경사항을 커밋하라는 메시지를 표시합니다. 대부분의 변경사항은 커밋해야 적용됩니다.

단계 **6** 다음 단계로 진행, 28 페이지

시스템 설정 마법사 구동

마법사를 구동하려면 웹 인터페이스 액세스 , 23 페이지의 설명대로 GUI에 로그인합니다. 처음으로 GUI에 로그인하면 시스템 설정 마법사의 첫 페이지가 기본적으로 나타납니다. System Administration(시스템 관리) 메뉴(Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > System Setup Wizard(시스템 설정 마법사))에서도 시스템 설정 마법사에 액세스할 수 있습니다.

최종 사용자 라이센스 계약 검토

라이선스 계약을 읽는 것으로 시작합니다. 라이센스 계약을 읽고 내용에 동의하면 동의를 나타내는 확인란을 선택하고 Begin Setup(설정 시작)을 클릭하여 계속 진행합니다.

시스템 설정 구성

시스템 알림을 위한 이메일 주소 입력

사용자 개입이 필요한 시스템 오류가 발생하면 AsyncOS는 이메일을 통해 알림 메시지를 전송합니다. 알림을 수신할 이메일 주소를 하나 이상 입력합니다.

시스템 알림을 위한 이메일 주소를 하나 이상 추가해야 합니다. 주소가 여러 개인 경우 쉼표로 구분해 주십시오. 입력한 이메일 주소에서 처음에는 모든 레벨, 모든 유형의 알림을 수신합니다. 알림구성은 나중에 맞춤 설정할 수 있습니다. 자세한 내용은 경고 관리, 464 페이지를 참조하십시오.

시간 설정

보고서, 메시지 헤더, 로그 파일의 타임스탬프가 정확하도록 Security Management Appliance의 표준 시간대를 설정합니다. 드롭다운 메뉴를 사용하여 표준 시간대를 찾거나 GMT 차감 시간으로 표준 시간대를 정의합니다.

나중에 시스템 시계 시간을 수동으로 설정할 수 있지만, NTP(Network Time Protocol)를 사용하여 네트워크의 다른 서버 또는 인터넷과 시간을 동기화하는 것이 좋습니다. 기본적으로 Cisco NTP 서버(time.sco.cisco.com) 항목이 추가되어 Content Security Appliance의 시간을 동기화합니다. NTP 서버의 호스트 이름을 입력하고 Add Entry(항목 추가)를 클릭하여 추가 NTP 서버를 구성합니다. 자세한 내용은 시스템 시간 구성, 477 페이지를 참조하십시오.

암호 설정

AsyncOS admin 계정의 암호: 관리자 암호를 변경해야 합니다. 암호는 안전한 장소에 보관합니다. 암호 변경은 즉시 적용됩니다.

참고 암호를 재설정한 다음 시스템 설정을 취소하더라도 암호 변경은 실행 취소되지 않습니다.

AutoSupport 활성화

AutoSupport(기본적으로 활성화됨)는 최적의 지원이 이루어지도록 Security Management Appliance 관련 문제를 고객 지원 팀에 알려주는 기능입니다. 자세한 내용은 Cisco AutoSupport, 467 페이지를 참조하십시오.

네트워크 설정 구성

시스템의 호스트 이름을 정의한 다음 게이트웨이와 DNS 설정을 구성합니다.

참고 Management 포트를 통해 Security Management Appliance를 네트워크에 연결했는지 확인하십시오.

네트워크 설정

Security Management Appliance의 정규화된 호스트 이름을 입력합니다. 네트워크 관리자가 지정한 이름이어야 합니다.

Security Management Appliance의 IP 주소를 입력합니다.

네트워크에서 기본 deerrouter(게이트웨이)의 네트워크 마스크 및 IP 주소를 입력합니다.

그다음에는 DNS(Domain Name Service) 설정을 구성합니다. AsyncOS는 인터넷의 루트 서버에 직접 쿼리할 수 있는 고성능 내부 DNS 확인자/캐시를 포함하거나, 사용자가 지정하는 DNS 서버를 사용할 수 있습니다. 자체 서버를 사용하려는 경우 각 DNS 서버의 IP 주소를 제공해야 합니다. 시스템 설정 마법사를 통해 최대 4개의 DNS 서버를 입력할 수 있습니다.

참고 사용자가 지정하는 DNS 서버는 초기 우선 순위가 0입니다. 자세한 내용은 DNS(Domain Name System) 설정 구성, 473 페이지를 참조하십시오.

참고 어플라이언스는 수신 연결에 대한 DNS 조회를 수행하기 위해 작동 중인 DNS 서버에 액세스해야 합니다. 어플라이언스 설정 중에 어플라이언스에서 도달할 수 있는 작동 중인 DNS 서버를 지정할 수 없는 경우 해결책은 "Use Internet Root DNS Servers(인터넷 루트 DNS 서버 사용)"를 선택하거나, 시스템 설정 마법사를 완료할 수 있도록 일시적으로 Management 인터페이스의 IP 주소를 지정하는 것입니다.

구성 검토

이제 시스템 설정 마법사에서 사용자가 입력한 설정 정보의 요약을 표시합니다. 변경하려면 페이지 맨 아래의 **Previous**(이전)를 클릭하고 정보를 수정합니다.

정보를 검토한 다음 **Install This Configuration**(이 구성 설치)을 클릭합니다. 확인 대화 상자가 나타나면 **Install**(설치)을 클릭합니다.

Install This Configuration(이 구성 설치)을 클릭했는데 페이지가 응답하지 않는 것처럼 보인다면 이제 어플라이언스가 마법사에서 지정한 새 IP 주소를 현재 사용하고 있는 것입니다. 어플라이언스를 계속 사용하려면 새 IP 주소를 사용합니다. 빠른 시작 설명서의 지침대로 새 하드웨어 어플라이언스에 액세스하는 데 쓰이는 컴퓨터의 IP 주소를 임시로 변경한 경우 먼저 컴퓨터의 IP 주소를 원래의 설정으로 되돌립니다.

다음 단계로 진행

Security Management Appliance를 설치하고 시스템 설정 마법사를 실행한 후, 어플라이언스에서 다른 설정을 수정하고 모니터링 서비스를 구성할 수 있습니다.

시스템 설정 마법사를 실행하기 위해 어플라이언스에 액세스하는 데 적용한 프로세스에 따라 **System Setup Next Steps**(시스템 설정 다음 단계) 페이지가 나타납니다. 페이지가 자동으로 나타나지 않을 경우 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Next Steps**(다음 단계)를 선택하여 액세스할 수 있습니다.

Cisco Content Security Appliance의 구성을 계속 진행하려면 System Setup Next Steps(시스템 설정 다음 단계) 페이지에서 링크를 클릭합니다.

관리 대상 어플라이언스 추가 정보

각 어플라이언스에 대해 첫 번째 중앙 집중식 서비스를 구성할 때, 관리되는 Email 및 Web Security Appliance를 Security Management Appliance에 추가하게 됩니다.

원격 어플라이언스를 추가하면 Security Management Appliance는 원격 어플라이언스의 제품 이름을 추가 중인 어플라이언스의 유형과 비교합니다. 예를 들어 Add Web Security appliance(Web Security Appliance 추가) 페이지를 사용하여 어플라이언스를 추가하면, Security Management Appliance는 원격 어플라이언스의 제품 이름을 검토하여 제품이 Web Security Appliance이며 Email Security Appliance가 아닌지 확인합니다. Security Management Appliance는 원격 어플라이언스에서 모니터링 서비스를 검토하여, 서비스가 올바르게 구성되었으며 호환되는지를 확인합니다.

Security Appliances(보안 어플라이언스) 페이지에는 사용자가 추가한 관리되는 어플라이언스가 표시됩니다. Connection Established?(연결 여부) 열은 모니터링 서비스의 연결이 제대로 구성되었는지 여부를 보여줍니다.

관리 대상 어플라이언스 추가에 대한 지침이 다음 절차에 나와 있습니다.

- 관리 대상 ESA 각각에 중앙 이메일 보고 서비스 추가 , 63 페이지
- 관리되는 각 Email Security Appliance에 중앙 집중식 메시지 추적 서비스 추가 , 265 페이지
- 관리되는 각 Email Security Appliance에 중앙 집중식 스팸 격리 서비스 추가 , 283 페이지
- 중앙 집중식 정책, 바이러스 및 Outbreak 격리 서비스를 관리되는 각 Email Security Appliance에 추가, 316 페이지
- 관리 대상 WSA 각각에 중앙 웹 보고 서비스 추가 , 180 페이지
- WSA 추가 및 구성 마스터 버전과 연결 , 345 페이지

관리 대상 어플라이언스 구성 수정

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 보안 어플라이언스 섹션에서 수정할 어플라이언스의 이름을 클릭합니다.

단계 **4** 필요에 따라 어플라이언스 구성을 변경합니다.

예를 들어 모니터링 서비스 확인란을 선택하거나 지우고 파일 전송 액세스를 재구성하고 IP 주소를 변경합니다.

참고 관리되는 어플라이언스의 IP 주소를 변경하면 여러 가지 문제가 발생할 수 있습니다. Web Security Appliance의 IP 주소를 변경하면 어플라이언스의 게시 기록이 손실되며, Web Security Appliance가 예약된 게시 작업에 대해 현재 선택된 경우 게시 오류가 발생합니다. (할당된 모든 어플라이언스를 사용하도록 설정된 예약된 게시 작업에는 영향이 미치지 않습니다.) Email Security Appliance의 IP 주소를 변경하면 어플라이언스의 추적 가용성 데이터가 손실됩니다.

단계 **5** **Submit(**제출**)**을 클릭하여 페이지의 변경 사항을 제출한 다음 Commit Changes(변경 사항 적용)를 클릭하여 변경 사항을 적용합니다.

관리 대상 어플라이언스 목록에서 어플라이언스 삭제

시작하기 전에

Security Management Appliance에서 원격 어플라이언스를 제거하려면 먼저 해당 어플라이언스에서 활성화된 중앙 집중식 서비스를 비활성화해야 할 수 있습니다. 예를 들어 중앙 집중식 정책, 바이러스 및 보안 침해 격리 서비스가 활성화된 경우 Email Security Appliance에서 우선 해당 서비스를 비활성화해야 합니다. Email 또는 Web Security Appliance용 문서를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 보안 어플라이언스 섹션에서 삭제할 관리 대상 어플라이언스의 행에 있는 휴지통 아이콘을 클릭합니다.

단계 **4** 확인 대화상자에서 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

Security Management Appliance의 서비스 구성

이메일 보안 서비스:

- 중앙 이메일 보안 보고 사용, 61 페이지
- 메시지 추적, 263 페이지
- 스팸 격리, 279 페이지
- 중앙 정책, 바이러스, 보안 침해 격리, 311 페이지

웹 보안 서비스:

- 중앙 정책, 바이러스, 보안 침해 격리, 311 페이지
- Web Security Appliance 관리, 341 페이지

구성 변경사항 커밋 및 취소

Cisco Content Security Appliance GUI에서 구성을 변경한 경우에는 대부분 명시적으로 변경 사항을 커밋해야 합니다.

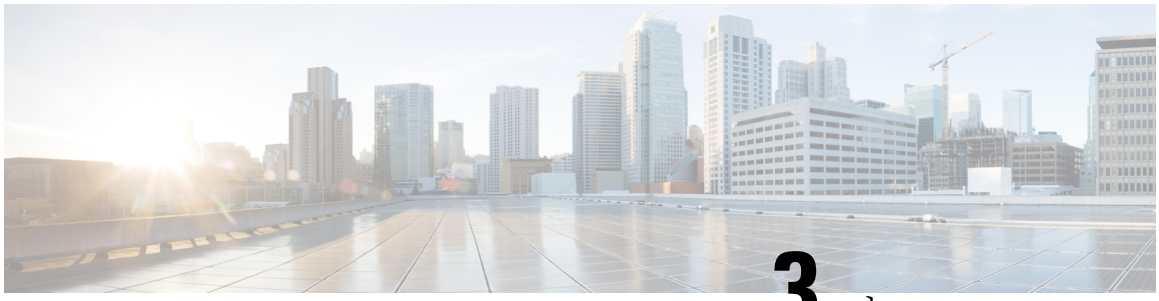
그림 ***3: Commit Changes(***변경사항 커밋***)*** 버튼

변경 후	수행해야 할 작업
모든 보류 중인 변경사항 커밋	창 오른쪽 위에서 오렌지색 Commit Changes(변경사항 커밋) 버튼을 클릭합니다. 변경사항에 대한 설명을 추가하고 커밋을 클릭합니다. 커밋이 필요한 변경사항이 없을 경우 Commit Changes(변경사항 커밋) 대신 회색 No Changes Pending(보류 중 변경사항 없음) 버튼이 나타납니다.
모든 보류 중인 변경사항 취소	창 오른쪽 위에서 오렌지색 Commit Changes(변경사항 커밋) 버튼을 클릭한 다음 Abandon Changes(변경사항 취소)를 클릭합니다.

참고 이전 웹 인터페이스의 구성 변경 사항은 로그아웃하고 새로운 Cisco Content Security Management 웹 인터페이스에 로그인한 후에 새 웹 인터페이스에서 업데이트됩니다.

관련 항목

- 이전에 커밋한 구성으로 롤백 , 483 페이지



3 장

레거시 웹 인터페이스에서 보고서 작업

이 장에는 다음 섹션이 포함되어 있습니다.

보고 데이터를 보는 방법

표 *4:* 보고 데이터를 보는 방법

변경 후	확인
웹 기반 인터랙티브 보고서 페이지 보기 및 맞춤화	• 보고 데이터 보기 맞춤화 , 35 페이지 • 중앙 이메일 보안 보고 사용, 61 페이지 • 중앙 정책, 바이러스, 보안 침해 격리, 311 페이지
반복 PDF 또는 CSV 보고서 자동 생성	• 이메일 보고서 예약, 169 페이지 • 웹 보고서 예약 , 239 페이지
PDF 또는 CSV 보고서 온디맨드 생성	• 온디맨드 이메일 보고서 생성 , 170 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지

변경 후	확인
CSV(Comma-separated values) 파일로 원시 데이터 내보내기	• 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지 • CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기 , 44 페이지
보고서 데이터의 PDF 생성	보고/추적 데이터 인쇄 및 내보내기 , 41 페이지
자신 및 다른 사람에게 보고서 정보 이메일 전송	• 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지 • 웹 보고서 예약 , 239 페이지
특정 트랜잭션에 대한 정보 찾기	보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기 , 40 페이지

참고 로깅과 보고의 차이점은 로깅 대 보고, 503 페이지에서 확인하십시오.

Security Management Appliance에서 보고서를 위한 데이터를 수집하는 방법

Security Management Appliance는 약 15분마다 관리되는 모든 어플라이언스에서 모든 보고서에 대한 데이터를 가져오고 이러한 어플라이언스의 데이터를 집계합니다. 어플라이언스에 따라 특정 메시지가 Security Management Appliance에서 보고 데이터에 포함될 때까지 다소 시간이 걸릴 수 있습니다. 데이터에 대한 정보는 **System Status**(시스템 상태) 페이지에서 확인할 수 있습니다.

보고 데이터는 IPv4 및 IPv6 모두와 관련된 트랜잭션을 포함합니다.

참고 Security Management Appliance는 보고서용 데이터를 수집할 때, Security Management Appliance에서 시간 설정을 구성할 때 지정된 정보에서 타임스탬프를 가져와 적용합니다. Security Management Appliance에서 시간을 설정하는 방법에 대한 자세한 내용은 시스템 시간 구성, 477 페이지를 참조하십시오.

보고 데이터가 저장되는 방법

모든 어플라이언스는 보고 데이터를 저장합니다. 다음 표에는 각 어플라이언스에서 데이터를 저장할 기간이 표시되어 있습니다.

표 *5: Email Security Appliance* 및 *Web Security Appliance*의 데이터 스토리지 보고

	분	**Hourly**(시간당)	**Daily**(매일)	**Weekly**(매주)	**Monthly**(매월)	매년
Email Security Appliance 또는 Web Security Appliance 에 대한 로컬 보고	•	•	•	•	•	
Email Security Appliance 또는 Web Security Appliance에 대한 중앙 집중식 보고	•	•	•	•		
Security Management Appliance		•	•	•	•	•

보고 및 업데이트 정보

새로운 보고 기능이 업그레이드 전에 실행된 트랜잭션에는 적용되지 않을 수 있습니다. 해당 트랜잭션에 대해 필요한 데이터가 보존되지 않았을 가능성도 있기 때문입니다. 보고 데이터 및 업그레이드와 관련되어 나타날 수 있는 제한 사항은 해당 릴리스의 릴리스 정보를 참조해 주십시오.

보고 데이터 보기 맞춤화

웹 인터페이스에서 보고서 데이터를 볼 때 보기를 맞춤화할 수 있습니다.

변경 후	수행해야 할 작업
어플라이언스 또는 보고 그룹별 데이터 보기	어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지
시간 범위 지정	보고서의 시간 범위를 선택 , 36 페이지
(웹 보고서) 차트에 표시할 데이터 선택	(웹 보고서만) 차트에 표시할 데이터 선택 , 37 페이지
테이블 맞춤화	보고서 페이지의 테이블 맞춤화 , 37 페이지를 참조하십시오.
표시할 특정 정보 또는 데이터 하위 집합 검색	• 이메일 보고서의 경우 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오. • 웹 보고서의 경우 대부분의 테이블에서 맨 아래에 있는 Find(찾기) 또는 Filter(필터) 옵션을 찾으십시오. • 일부 테이블은 집계 데이터의 세부사항에 대한 링크(파란색 텍스트)를 포함합니다.
보고서 관련 기본 설정 지정	기본 설정 , 500 페이지를 참조하십시오.

변경 후	수행해야 할 작업
원하는 차트 및 테이블로만 맞춤형 보고서 생성	맞춤 설정 리포트 , 38 페이지를 참조하십시오.

참고 일부 맞춤 설정 기능을 사용할 수 없는 보고서도 있습니다.

어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기

이메일에 대한 Mail Flow Summary(메일 플로우 요약) 보고서와 System Capacity(시스템 용량) 보고서에 대한 시스템 용량 보고서의 경우 모든 어플라이언스의 데이터를 보거나 어느 한 중앙 관리형 어플라이언스의 데이터를 볼 수 있습니다.

이메일 보고서의 경우 이메일 보고 그룹 생성, 64 페이지에서 설명한 대로 Email Security Appliance의 그룹을 생성한 경우 각 보고 그룹에 대한 데이터를 볼 수 있습니다.

보기를 지정하려면 지원되는 페이지에 있는 **View Data For(**데이터 보기**)** 목록에서 어플라이언스 또는 그룹을 선택합니다.

최근에 다른 Security Management Appliance에서 백업을 가져온 Cloud Email Security Management Console에서 보고서 데이터를 보려는 경우, > **Management Appliance(**관리 어플라이언스**)** > **Centralized Services(**중앙 집중식 서비스**)** > **Security Appliances(**보안 어플라이언스**)**에서 각 어플라이언스를 추가해야 합니다(그러나 연결은 설정하지 않음).

보고서의 시간 범위를 선택

대부분의 사전 정의 보고서 페이지에서는 포함할 데이터의 시간 범위를 선택할 수 있습니다. 선택한 시간 범위는 Time Range(시간 범위) 메뉴에서 다른 값을 선택할 때까지 모든 보고서 페이지에 사용됩니다.

사용 가능한 시간 범위 옵션은 어플라이언스에 따라 다르며, Security Management Appliance의 이메일 및 웹 보고에 대해 다릅니다.

참고 보고서 페이지의 시간 범위는 GMT(Greenwich Mean Time) 차감 시간으로 표시됩니다. 예를 들어 태평양 시간은 GMT + 7시간(GMT + 07:00)입니다.

참고 모든 보고서에서 GMT(Greenwich Mean Time) 차감 시간으로 나타나는 시스템 구성 표준 시간대를 사용하여 날짜 및 시간 정보를 표시합니다. 그러나 내보낸 데이터에서는 세계 여러 표준 시간대의 여러 시스템을 수용하기 위해 GMT로 시간이 표시됩니다.

팁 로그인할 때마다 항상 표시될 기본 시간 범위를 지정할 수 있습니다. 자세한 내용은 기본 설정 , 500 페이지 섹션을 참조하십시오.

(웹 보고서만) 차트에 표시할 데이터 선택

각 웹 보고 페이지의 기본 차트에는 자주 참조되는 데이터가 표시되지만 대신 다른 데이터를 차트에 표시하도록 선택할 수 있습니다. 한 페이지에 여러 차트가 있는 경우 각 차트를 변경할 수 있습니다.

일반적으로 차트 옵션은 보고서에 있는 테이블의 열과 동일합니다. 그러나 일부 열은 차트에 추가할 수 없습니다.

연결된 테이블에 표시하도록 선택하는 항목(행) 수와 상관없이 차트는 테이블 열에 있는 모든 사용 가능한 데이터를 나타냅니다.

단계 **1** 차트 아래에 있는 **Chart Options**(차트 옵션) 링크를 클릭합니다.

단계 **2** 표시할 데이터를 선택합니다.

단계 **3** **Done**(완료)을 클릭합니다.

보고서 페이지의 테이블 맞춤화

표 ***6:*** 웹 보고서 페이지의 표 맞춤화

변경 후	수행해야 할 작업	추가 정보
• 추가 열 표시 • 표시된 열 숨기기 • 테이블에 대해 사용 가능한 열 확인	테이블 아래에 있는 **Columns**(열) 링크를 클릭하고 표시할 열을 선택한 다음 **Done**(완료)을 클릭합니다.	대부분의 테이블에서는 일부 열이 기본적으로 숨겨져 있습니다. 각 보고서 페이지에서는 서로 다른 열을 제공합니다. 이메일 보고 페이지의 테이블 열 설명, 71 페이지도 참조하십시오.
테이블 열 순서 재지정	열 제목을 원하는 새 위치로 끌어다 놓습니다.	—
선택한 제목을 기준으로 테이블 정렬	열 제목을 클릭합니다.	—
더 많은 또는 더 적은 수의 데이터 행 표시	테이블 상단 오른쪽의 **Items Displayed**(표시할 행) 드롭다운 목록에서 표시할 행의 수를 선택합니다.	웹 보고서의 경우 기본적으로 표시할 행 수도 설정할 수 있습니다. 기본 설정 , 500 페이지를 참조하십시오.

변경 후	수행해야 할 작업	추가 정보
테이블 항목에 대한 세부사항 보기(가능한 경우)	테이블의 파란색 항목을 클릭합니다.	보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기 , 40 페이지도 참조하십시오.
데이터 풀을 특정 하위 집합으로 좁히기	가능한 경우 테이블 아래의 필터 설정에서 값을 선택하거나 입력합니다.	웹 보고서의 경우 개별 보고서 페이지 설명에 사용 가능한 필터가 나와 있습니다. 웹 보고 페이지 설명, 182 페이지를 참조하십시오.

맞춤 설정 리포트

기존 보고서 페이지의 차트(그래프)와 테이블을 조합하여 맞춤형 이메일 보안 보고서 페이지를 생성할 수 있습니다.

참고 Email Security Appliance는 릴리스 9.6부터 “My Reports(내 보고서)”가 “My Dashboard(내 대시보드)”로 바뀌었습니다.

변경 후	수행해야 할 작업
맞춤형 보고서 페이지에 모듈 추가	참조: • 맞춤형 보고서에 추가될 수 없는 모듈 , 39 페이지 • 맞춤형 보고서 페이지 생성 , 39 페이지
맞춤형 보고서 페이지 보기	1. Email(이메일) > Reporting(보고) > My Reports(내 보고서)를 선택합니다. 2. 보려는 시간 범위를 선택합니다선택한 시간 범위는 My Reports(내 보고서) 페이지의 모든 모듈을 포함한 모든 보고서에 적용됩니다. 새로 추가된 모듈은맞춤형 보고서의 상단에 나타납니다.
맞춤형 보고서 페이지에서 모듈 정돈	모듈을 원하는 위치로 끌어다 놓습니다.
맞춤형 보고서 페이지에서 모듈 삭제	모듈의 상단 우측에 있는 [X]를 클릭합니다.
CSV 버전의 맞춤형 보고서 생성	참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지

변경 후	수행해야 할 작업
주기적으로 CSV 버전의 맞춤형 보고서 생성	참조: • 이메일 보고서 예약, 169 페이지 • 웹 보고서 예약 , 239 페이지

맞춤형 보고서에 추가될 수 없는 모듈

- **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 집중식 서비스) > **System Status**(시스템 상태) 페이지의 모든 모듈
- **Email**(이메일) > **Reporting**(보고) > **Reporting Data Availability**(보고 데이터 가용성) 페이지의 모든 모듈
- **Email**(이메일) > **Message Tracking**(메시지 추적) > **Message Tracking Data Availability**(메시지 추적 데이터 가용성) 페이지에 있는 모든 모듈
- Sender Profile detail report(발신자 프로필 세부사항 보고서) 페이지에 있는 다음과 같은 도메인 단위 모듈: Current Information from SenderBase(SenderBase의 현재 정보), Sender Group Information(발신자 그룹 정보) 및 Network Information(네트워크 정보)
- Outbreak Filters report(보안 침해 필터 보고서) 페이지에 있는 **Past Year Virus Outbreak Summary**(지난해 바이러스 보안 침해 요약) 차트 및 **Past Year Virus Outbreaks**(지난해 바이러스 보안 침해) 테이블

맞춤형 보고서 페이지 생성

시작하기 전에

- 추가하려는 모듈이 추가될 수 있는지 확인합니다. 맞춤형 보고서에 추가될 수 없는 모듈 , 39 페이지를 참조하십시오.
- 필요 없는 기본 모듈은 모듈 오른쪽 위의 [X]를 클릭하여 삭제합니다.

단계 **1** 다음 방법 중 하나로 맞춤형 보고서 페이지에 모듈을 추가합니다.

참고 일부 모듈은 다음 방법 중 하나로만 사용할 수 있습니다. 한 가지 방법을 사용하여 모듈을 추가할 수 없는 경우 다른 방법을 시도하십시오.

-
- 추가하려는 모듈이 있는 Email(이메일) 아래의 보고서 페이지로 이동한 다음 모듈 상단에서 [+] 버튼을 클릭합니다.
- Email(이메일) > Reporting(보고) > My Reports(내 보고서)로 이동하여 섹션 중 하나의 상단에 있는 [+] Report Module(보고서 모듈) 버튼을 클릭한 후 추가할 보고서 모듈을 선택합니다 검색 중인 모듈을 찾기 위해 My Reports(내 보고서) 페이지의 각 섹션에서 + 버튼을 클릭해야 할 수 있습니다.

각 모듈을 한 번만 추가할 수 있습니다. 보고서에 특정 모듈을 이미 추가한 경우, 해당 추가 옵션은 사용할 수 없는 상태가 됩니다.

단계 **2** 열을 추가, 삭제, 재배치하거나 차트에 기본이 아닌 데이터를 표시하는 등의 방법으로 맞춤화한 모듈을 추가하는 경우 My Reports(내 보고서) 페이지에서 모듈을 맞춤화합니다.

모듈이 기본 설정으로 추가됩니다. 원래 모듈의 시간 범위는 유지되지 않습니다.

단계 **3** 별도의 범례가 포함된 차트를 추가하는 경우(예: Overview(개요) 페이지의 그래프) 범례를 따로 추가합니다. 필요한 경우, 설명하는 데이터 옆으로 끌어다 놓습니다.

보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기

단계 **1** 보고서 페이지 테이블에서 파란색 숫자를 클릭합니다.

(모든 테이블이 이러한 링크가 있는 것은 아닙니다.)

해당 숫자에 포함된 메시지 또는 트랜잭션이 각각 Message Tracking(메시지 추적) 또는 Web Tracking(웹 추적)에 표시됩니다.

단계 **2** 메시지 또는 트랜잭션의 목록을 보려면 아래로 스크롤합니다.

다음에 수행할 작업

- 메시지 추적, 263 페이지

이메일 보고서의 성능 향상

1개월간 고유 항목의 수가 많아 집계 보고의 성능이 저하될 경우 보고 필터를 사용하여 전년도를 다루는 보고서(전년도 보고서)에 데이터를 집계하는 것으로 제한합니다. 이 필터로 보고서에서 세부, 개별 IP, 도메인 또는 사용자 데이터를 제한할 수 있습니다. 개요 보고서 및 요약 정보는 모든 보고서에서 계속 사용 가능합니다.

CLI에서 **reportingconfig > filters** 메뉴를 사용하여 보고 필터 하나 이상을 활성화할 수 있습니다. 변경 사항을 적용하려면 커밋해야 합니다.

- **IP Connection Level Detail(IP** 연결 레벨 세부사항**)**. 이 필터를 활성화하면 Security Management Appliance는 개별 IP 주소에 대한 정보를 기록하지 않습니다. 이 필터는 공격 때문에 대규모 수신 IP 주소를 처리하는 시스템에 적절합니다.

  이 필터는 다음 지난해 보고서에 적용됩니다.

  - 수신 메일의 발신자 프로필
  - 수신 메일의 IP 주소
  - IP Addresses for Outgoing Senders(발신 발신자에 대한 IP 주소)

- **User Detail(**사용자 세부사항**)**. 이 필터를 활성화하면 Security Management Appliance는 메일을 주고받은 개별 사용자 및 사용자 메일에 적용된 콘텐츠 필터에 대한 정보를 기록하지 않습니다. 이 필터는 수백만의 내부 사용자 메일을 처리하는 어플라이언스에 또는 시스템이 수신자 주소를 검증하지 않는 경우에 적절합니다.

  이 필터는 다음 지난해 보고서에 적용됩니다.

  - Internal Users(내부 사용자)
  - 내부 사용자 세부사항
  - 발신자 IP 주소
  - 콘텐츠 필터

- **Mail Traffic Detail(**메일 트래픽 세부사항**)**. 이 필터를 활성화하면 Security Management Appliance는 어플라이언스가 모니터링하는 개별 도메인 및 네트워크에 대한 정보를 기록하지 않습니다. 이 필터는 유효한 수신 또는 발신 도메인 수가 수천만에 달할 경우 적절합니다.

  이 필터는 다음 지난해 보고서에 적용됩니다.

  - 수신 메일의 도메인
  - 수신 메일의 발신자 프로필
  - 내부 사용자 세부사항
  - 발신자 도메인

참고 이전 시간의 최신 보고 데이터를 보려면 개별 어플라이언스에 로그인하고 거기서 데이터를 봐야 합니다.

보고/추적 데이터 인쇄 및 내보내기

표 *7:* 보고/추적 데이터 인쇄 및 내보내기

필요한 것	PDF	CSV	수행해야 할 작업	참고
인터랙티브 보고서 페이지의 PDF	•		인터랙티브 보고서 페이지의 상단 오른쪽에서 **Printable (PDF)** 링크를 클릭합니다.	PDF는 현재 보고 있는 맞춤 설정을 반영합니다. PDF는 인쇄용 형식으로 지정됩니다.

필요한 것	PDF	CSV	수행해야 할 작업	참고
보고서 데이터의 PDF	•		예약 또는 온디맨드 보고서를 생성합니다. 참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지 • 웹 보고서 예약 , 239 페이지	—
원시 데이터 CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기 , 44 페이지도 참조하십시오.		•	차트 또는 테이블 아래에 있는 **Export**(내보내기) 링크를 클릭합니다.	CSV 파일은 차트 또는 테이블에 표시되는 데이터뿐 아니라 해당되는 모든 데이터를 포함하고 있습니다.
		•	예약 또는 온디맨드 보고서를 생성합니다. 참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지 • 웹 보고서 예약 , 239 페이지	각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다. 일부 확장 보고서는 CSV 형식으로 사용할 수 없습니다.
다국어 보고서	•		보고서를 예약하거나 온디맨드 보고서를 생성할 때 원하는 보고서 언어를 선택합니다.	Windows 컴퓨터에서 중국어, 일본어 또는 한국어로 PDF를 생성하려면 Adobe.com에서 해당 글꼴 팩을 다운로드하여 로컬 컴퓨터에 설치해야 합니다.
(Web Security) 보고서 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).	•	•	웹 추적에서 검색을 수행하고 Web Tracking(웹 추적) 페이지에서 Printable Download(인쇄용 버전 다운로드) 링크를 클릭합니다. PDF 또는 CSV 형식을 선택합니다.	PDF는 웹 페이지에 있는 정보 중 일부를 포함하지 않을 수도 있습니다. 즉 PDF는 다음 항목을 포함합니다. • 최대 1,000개의 트랜잭션. • 세부사항을 표시할 경우 최대 100개의 관련 트랜잭션. • 관련 트랜잭션당 최대 3,000자. CSV 파일은 검색 조건과 매칭하는 모든 원시 데이터를 포함합니다.

필요한 것	PDF	CSV	수행해야 할 작업	참고
(Email Security) 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).		•	메시지 추적에서 검색을 수행하고 검색 결과 위에 있는 Export(내보내기) 링크 또는 Export All(모두 내보내기) 링크를 클릭합니다.	Export(내보내기) 링크는 검색 조건에 지정한 한도에서 표시된 검색 결과의 CSV 파일을 다운로드합니다. Export All(모두 내보내기) 링크는 검색 조건과 매칭하는 최대 50,000개의 메시지를 포함하는 CSV 파일을 다운로드합니다. 팁: 내보내야 할 메시지가 50,000개를 초과할 경우 더 짧은 시간 범위 집합에 대해 연속적으로 내보내기를 수행합니다.

표 *8:* 새 웹 인터페이스에서 보고/추적 데이터 인쇄 및 내보내기

필요한 것	CSV	수행해야 할 작업	참고
원시 데이터 CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기 , 44 페이지 섹션도 참조해 주십시오.	•	차트 또는 테이블 아래의 Export(내보내기) 링크를 클릭합니다.	CSV 파일은 차트 또는 테이블에 표시되는 데이터는 물론, 해당되는 모든 데이터를 포함하고 있습니다.
	•	예약 또는 온디맨드 보고서를 생성합니다. 참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지	각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 둘 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다. 일부 확장 보고서는 CSV 형식으로 사용할 수 없습니다.
(Web Security) 보고서 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).	•	웹 추적에서 검색을 수행하고 Web Tracking(웹 추적) 페이지에서 Printable Download(인쇄용 버전 다운로드) 링크를 클릭합니다. PDF 또는 CSV 형식을 선택합니다.	CSV 파일은 검색 조건과 매칭하는 모든 원시 데이터를 포함합니다.

필요한 것	CSV	수행해야 할 작업	참고
(Email Security) 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).	•	메시지 추적에서 검색을 수행하고 검색 결과 위에 있는 Export(내보내기) 링크 또는 Export All(모두 내보내기) 링크를 클릭합니다.	Export(내보내기) 링크는 검색 조건에 지정한 한도에서 표시된 검색 결과의 CSV 파일을 다운로드합니다. Export All(모두 내보내기) 링크는 검색 조건과 매칭하는 최대 50,000개의 메시지를 포함하는 CSV 파일을 다운로드합니다. 팁: 내보내야 할 메시지가 50,000개를 초과할 경우 더 짧은 시간 범위 집합에 대해 연속적으로 내보내기를 수행합니다.

CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기

원시 데이터를 CSV(comma-separated values) 파일로 내보낼 수 있습니다. 이 파일은 Microsoft Excel과 같은 데이터베이스 애플리케이션을 사용하여 액세스하고 다룰 수 있습니다. 데이터를 내보내는 여러 가지 방법에 대해서는 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

CSV 내보내기에는 원시 데이터만 포함되므로, 백분율 같은 계산된 데이터가 웹 기반 보고서에는 나타나더라도 웹 기반 보고서 페이지에서 내보낸 데이터에는 포함되지 않을 수 있습니다.

Security Management Appliance에 설정된 내용과 상관없이, 이메일 메시지 추적 및 보고 데이터의 경우 내보낸 CSV 데이터는 GMT로 모든 데이터를 표시합니다. 이렇게 하면 특히 여러 표준 시간대의 어플라이언스에 있는 데이터를 참조할 때, 해당 어플라이언스의 데이터를 독립적으로 사용할 수 있습니다.

다음 예는 악성코드 차단 범주 보고서의 원시 데이터 내보내기에 있는 항목입니다. 여기서 PDT(Pacific Daylight Time)가 GMT - 7시간으로 표시됩니다.

Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100, 2625

표 ***9:*** 원시 데이터 항목 보기

카테고리 헤더	Value	설명
Begin Timestamp	1159772400.0	쿼리 시작 시간입니다(epoch 이후 초 수).
End Timestamp	1159858799.0	쿼리 종료 시간입니다(epoch 이후 초 수).

카테고리 헤더	**Value**	설명
Begin Date	2006-10-02 07:00 GMT	쿼리가 시작된 날짜입니다.
End Date	2006-10-03 오전 6:59 GMT	쿼리가 종료된 날짜입니다.
Name	Adware	악성코드 카테고리의 이름입니다.
Transactions Monitored	525	모니터링되는 트랜잭션 수입니다.
Transactions Blocked	2100	차단된 트랜잭션 수입니다.
Transactions Detected	2625	총 트랜잭션 수. 탐지된 트랜잭션 수 + 차단된 트랜잭션 수

참고 카테고리 헤더는 보고서 유형마다 서로 다릅니다. 현지화된 CSV 데이터를 내보낼 경우 일부 브라우저에서 제목이 제대로 표시되지 않을 수 있습니다. 이 문제는 일부 브라우저에서 현지화된 텍스트의 적절한 문자 집합을 사용하지 않았기 때문에 발생할 수 있습니다. 이 문제를 해결하려면 파일을 로컬 시스템에 저장하고, **File(파일) > Open(열기)**을 사용하여 브라우저에서 열 수 있습니다. 파일을 열 때 현지화된 텍스트를 표시하기 위한 문자 집합을 선택합니다.

보고 및 추적의 하위 도메인과 두 번째 레벨 도메인 비교

두 도메인 유형이 동일하게 나타나더라도, 보고 및 추적 검색에서 2-레벨 도메인 (http://george.surbl.org/two-level-tlds에 나열된 지역 도메인)은 하위 도메인과 다르게 취급됩니다. 예를 들면 다음과 같습니다.

- 보고서에 2-레벨 도메인(예: co.uk)에 대한 결과가 포함되지 않지만 foo.co.uk에 대한 결과는 포함됩니다. 보고서에 기본 회사 도메인(예: cisco.com) 아래의 하위 도메인이 포함됩니다.
- 지역 도메인 co.uk의 추적 검색 결과에는 foo.co.uk와 같은 도메인이 포함되지 않지만 cisco.com의 검색 결과에는 subdomain.cisco.com과 같은 하위 도메인이 포함됩니다.

모든 보고서 트러블슈팅

- 백업 Security Management Appliance에서 보고서 데이터를 볼 수 없음 , 45 페이지
- 보고가 비활성화됨, 46 페이지

백업 **Security Management Appliance**에서 보고서 데이터를 볼 수 없음

문제

보고서 데이터를 볼 단일 Email Security Appliance를 선택할 수 없습니다. **View Data For(데이터 보기)** 옵션은 보고서 페이지에서 나타나지 않습니다.

솔루션

백업 중 서비스 가용성 , 442 페이지도 참고하십시오.

보고가 비활성화됨

문제

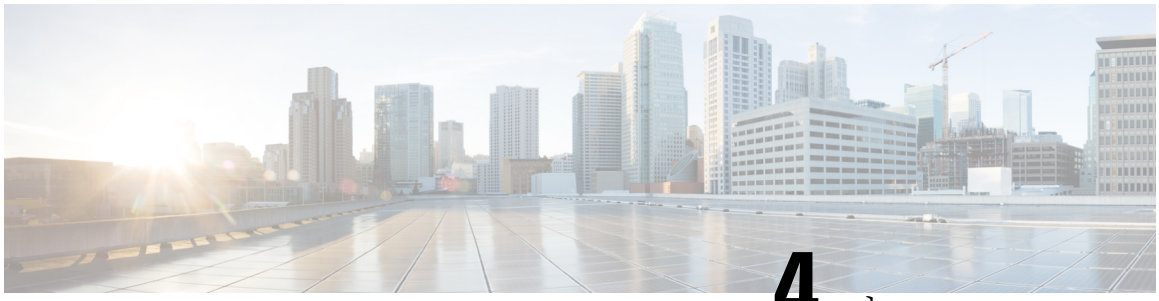
진행 중인 백업을 취소하면 보고가 비활성화될 수 있습니다.

솔루션

백업이 완료되면 보고 기능이 복원됩니다.

이메일 및 웹 보고서

이메일 보고서에 대한 자세한 내용은 중앙 이메일 보안 보고 사용, 61 페이지를 참조하십시오.
웹 보고서에 대한 자세한 내용은 중앙 웹 보고 및 추적 사용, 177 페이지를 참조하십시오.



4 장

새로운 웹 인터페이스에서 보고서 사용

이 장에는 다음 섹션이 포함되어 있습니다.

보고 데이터를 보는 방법

다음 표에는 보고 데이터를 보는 다양한 방법이 나와 있습니다.

표 ***10:*** 보고 데이터를 보는 방법

변경 후	확인
웹 기반 인터랙티브 보고서 페이지 보기 및 맞춤화	• 인터랙티브 보고서 페이지 사용, 49 페이지 • 보고 데이터 보기 맞춤화 , 50 페이지 • 중앙 이메일 보안 보고 사용, 61 페이지
반복 CSV 보고서 자동 생성	이메일 보고서 예약, 169 페이지
온디맨드 CSV 보고서 생성	온디맨드 이메일 보고서 생성 , 170 페이지
CSV(Comma-separated values) 파일로 원시 데이터 내보내기	보고/추적 데이터 인쇄 및 내보내기 , 41 페이지 CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기 , 44 페이지

변경 후	확인
자신 및 다른 사람에게 보고서 정보 이메일 전송	이메일 보고서 예약, 169 페이지 온디맨드 이메일 보고서 생성 , 170 페이지
특정 트랜잭션에 대한 정보 찾기	보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기 , 40 페이지

참고 로깅과 보고의 차이점은 로깅 대 보고, 503 페이지에서 확인하십시오.

Security Management Appliance에서 보고서를 위한 데이터를 수집하는 방법

Security Management Appliance는 약 15분마다 관리되는 모든 어플라이언스에서 모든 보고서에 대한 데이터를 가져오고 이러한 어플라이언스의 데이터를 집계합니다. 어플라이언스에 따라 특정 메시지가 Security Management Appliance에서 보고 데이터에 포함될 때까지 다소 시간이 걸릴 수 있습니다. 데이터에 대한 정보는 **System Status**(시스템 상태) 페이지에서 확인할 수 있습니다.

보고 데이터는 IPv4 및 IPv6 모두와 관련된 트랜잭션을 포함합니다.

참고 Security Management Appliance는 보고서용 데이터를 수집할 때, Security Management Appliance에서 시간 설정을 구성할 때 지정된 정보에서 타임스탬프를 가져와 적용합니다. Security Management Appliance에서 시간을 설정하는 방법에 대한 자세한 내용은 시스템 시간 구성, 477 페이지를 참조하십시오.

보고 데이터가 저장되는 방법

모든 어플라이언스는 보고 데이터를 저장합니다. 다음 표에는 각 어플라이언스에서 데이터를 저장할 기간이 표시되어 있습니다.

표 ***11: Email Security Appliance***의 데이터 스토리지 보고

	분	**Hourly**(시간당)	**Daily**(매일)	**Weekly**(매주)	**Monthly**(매월)	매년
Email Security Appliance에 대한 로컬 보고	•	•	•	•	•	
Email Security Appliance에 대한 중앙 집중식 보고	•	•	•	•		

	분	**Hourly(**시간당**)**	**Daily(**매일**)**	**Weekly(**매주**)**	**Monthly(**매월**)**	매년
Security Management Appliance		•	•	•	•	•

보고 및 업데이트 정보

새로운 보고 기능이 업그레이드 전에 실행된 트랜잭션에는 적용되지 않을 수 있습니다. 해당 트랜잭션에 대해 필요한 데이터가 보존되지 않았을 가능성도 있기 때문입니다. 보고 데이터 및 업그레이드와 관련되어 나타날 수 있는 제한 사항은 해당 릴리스의 릴리스 정보를 참조해 주십시오.

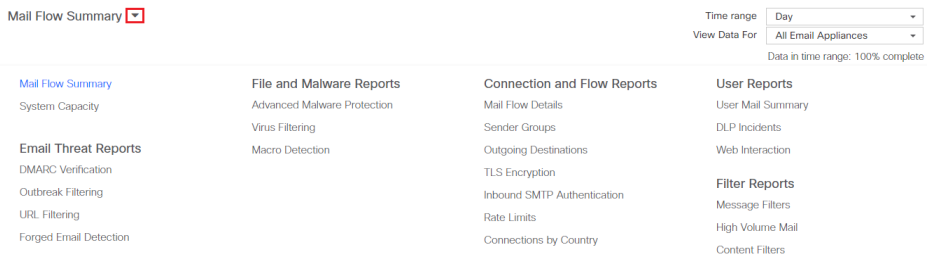
인터랙티브 보고서 페이지 사용

웹 인터페이스 상단에 있는 **Product(**제품**)** 드롭다운을 사용하여 Email Security Appliance와 Web Security Appliance 간에 전환할 수 있습니다.

다음 그림에 표시된 것처럼 **Reports(**보고서**)** 드롭다운을 사용하여 Email Security Appliance와 Web Security Appliance에 대한 보고서를 볼 수 있습니다.

참고 Mail Flow Summary(메일 플로우 요약) 보고서 페이지는 랜딩 페이지(로그인 후에 표시되는 페이지)입니다.

그림 ***4: Reports(***보고서***)*** 드롭다운



Reports(보고서**)** 드롭다운을 사용하여 다음 표에 분류된 이메일 및 웹 보고서를 볼 수 있습니다.

Email Security Appliance	**Web Security Appliance**
• 이메일 위협 보고서 • 파일 및 악성코드 보고서 • 연결 및 플로우 보고서 • 사용자 리포트 • 필터 보고서	• 일반 보고서 • 위협 보고서

관련 주제

- 보고 데이터 보기 맞춤화 , 50 페이지
- 보고서 페이지의 테이블 맞춤화 , 52 페이지
- (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지

보고 데이터 보기 맞춤화

웹 인터페이스에서 보고서 데이터를 볼 때 보기를 맞춤화할 수 있습니다.

변경 후	수행해야 할 작업
시간 범위 지정	보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
어플라이언스 또는 보고 그룹별 데이터 보기	어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지를 참조하십시오.
(웹 보고서) 차트에 표시할 데이터 선택	(웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지를 참조하십시오.
테이블 맞춤화	보고서 페이지의 테이블 맞춤화 , 52 페이지를 참조하십시오.
(이메일 보고서에만 해당) 보기 맞춤화	(이메일 보고서에만 해당) 보고서 페이지의 보기 맞춤화, 52 페이지를 참조하십시오.
카운터를 사용하여 트렌드 그래프에서 데이터 필터링	카운터를 사용하여 트렌드 그래프에서 데이터 필터링, 53 페이지를 참조하십시오.
보고서 관련 기본 설정 지정	기본 설정 , 500 페이지를 참조하십시오.
표시할 특정 정보 또는 데이터 하위 집합 검색	• 이메일 보고서는 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지 섹션을 참조하십시오. • 웹 보고서의 경우 대부분의 테이블에서 맨 아래에 있는 Find(찾기) 또는 Filter(필터) 옵션을 찾으십시오. • 일부 테이블은 집계 데이터의 세부사항에 대한 링크(파란색 텍스트)를 포함합니다. 자세한 내용은 보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기 , 40 페이지을 참고하십시오.

참고 일부 맞춤 설정 기능을 사용할 수 없는 보고서도 있습니다.

어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기

이메일에 대한 Mail Flow Summary(메일 플로우 요약) 보고서와 System Capacity(시스템 용량) 보고서에 대한 시스템 용량 보고서의 경우 모든 어플라이언스의 데이터를 보거나 어느 한 중앙 관리형 어플라이언스의 데이터를 볼 수 있습니다.

이메일 보고서의 경우 이메일 보고 그룹 생성, 64 페이지에서 설명한 대로 Email Security Appliance의 그룹을 생성한 경우 각 보고 그룹에 대한 데이터를 볼 수 있습니다.

보기를 지정하려면 지원되는 페이지에 있는 **View Data For(**데이터 보기**)** 목록에서 어플라이언스 또는 그룹을 선택합니다.

최근에 다른 Security Management Appliance에서 백업을 가져온 Cloud Email Security Management Console에서 보고서 데이터를 보려는 경우, > **Management Appliance(**관리 어플라이언스**)** > **Centralized Services(**중앙 집중식 서비스**)** > **Security Appliances(**보안 어플라이언스**)**에서 각 어플라이언스를 추가해야 합니다(그러나 연결은 설정하지 않음).

보고서의 시간 범위를 선택

대부분의 사전 정의 보고서 페이지에서는 포함할 데이터의 시간 범위를 선택할 수 있습니다. 선택한 시간 범위는 Time Range(시간 범위) 메뉴에서 다른 값을 선택할 때까지 모든 보고서 페이지에 사용됩니다.

사용 가능한 시간 범위 옵션은 어플라이언스에 따라 다르며, Security Management Appliance의 이메일 및 웹 보고에 대해 다릅니다.

참고 보고서 페이지의 시간 범위는 GMT(Greenwich Mean Time) 차감 시간으로 표시됩니다. 예를 들어 태평양 시간은 GMT + 7시간(GMT + 07:00)입니다.

참고 모든 보고서에서 GMT(Greenwich Mean Time) 차감 시간으로 나타나는 시스템 구성 표준 시간대를 사용하여 날짜 및 시간 정보를 표시합니다. 그러나 내보낸 데이터에서는 세계 여러 표준 시간대의 여러 시스템을 수용하기 위해 GMT로 시간이 표시됩니다.

팁 로그인할 때마다 항상 표시될 기본 시간 범위를 지정할 수 있습니다. 자세한 내용은 기본 설정 , 500 페이지 섹션을 참조하십시오.

(웹 보고서만) 차트에 표시할 데이터 선택

각 웹 보고 페이지의 기본 차트에는 자주 참조되는 데이터가 표시되지만 대신 다른 데이터를 차트에 표시하도록 선택할 수 있습니다. 한 페이지에 여러 차트가 있는 경우 각 차트를 변경할 수 있습니다.

일반적으로 차트 옵션은 보고서에 있는 테이블의 열과 동일합니다. 그러나 일부 열은 차트에 추가할 수 없습니다.

연결된 테이블에 표시하도록 선택하는 항목(행) 수와 상관없이 차트는 테이블 열에 있는 모든 사용 가능한 데이터를 나타냅니다.

단계 **1** 특정 차트에서 ✓ 을 클릭합니다.

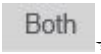
단계 **2** 표시할 필수 데이터를 선택합니다. 선택한 옵션에 따라 차트의 미리보기가 표시됩니다.

단계 **3** **Apply**(적용)를 클릭합니다.

(이메일 보고서에만 해당) 보고서 페이지의 보기 맞춤화

대부분의 보고서 페이지에서는 그래픽 보기, 표 보기 또는 통합 보기 중 하나를 선택할 수 있습니다. 선택하는 보기는 보고서 페이지의 데이터를 표시하는 데 사용됩니다.

표 ***12:*** 이메일 보고 페이지의 보기 맞춤화

변경 후	수행해야 할 작업
데이터를 그래프 보기로 표시합니다.	데이터를 그래프 보기로 보려면  을 클릭합니다.
데이터를 표 보기로 표시합니다.	데이터를 표 보기로 보려면  을 클릭합니다.
테이블 항목에 대한 세부사항 보기(가능한 경우)	테이블의 파란색 항목을 클릭합니다.
데이터를 통합 보기로 표시합니다.	데이터를 그래프 및 표 형식으로 보려면  을 클릭합니다.

보고서 페이지의 테이블 맞춤화

보고서 페이지 내에서 인터랙티브 테이블에 대한 정보를 보고, 맞춤화하고, 정렬할 수 있습니다. 선택하는 보기는 보고서 페이지의 데이터를 표시하는 데 사용됩니다.

표 ***13:*** 보고서 페이지의 테이블 맞춤화

변경 후	수행해야 할 작업	추가 정보
• 추가 열 표시 • 표시된 열 숨기기 • 테이블에 대해 사용 가능한 열 확인	1.  버튼을 클릭합니다. 2. 표시할 열을 선택하고 **Close(**닫기**)**를 클릭합니다.	대부분의 테이블에서는 일부 열이 기본적으로 숨겨져 있습니다. 각 보고서 페이지에서는 서로 다른 열을 제공합니다. 각 테이블에 대한 테이블 열 설명을 참조하십시오.
선택한 제목을 기준으로 테이블 정렬	열 제목을 클릭합니다.	-
테이블 열 순서 재지정	열 제목을 원하는 새 위치로 끌어다 놓습니다.	-
테이블 항목에 대한 세부사항 보기(가능한 경우)	테이블의 파란색 항목을 클릭합니다.	보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기 , 40 페이지도 참조하십시오.
추가 행의 세부 정보를 봅니다.	테이블에서 아래로 스크롤하여 추가 행의 세부 정보를 표시할 수 있습니다.	-
특정 하위 집합으로 데이터 필터링	가능한 경우 특정 테이블 아래의 필터 설정에 값을 입력합니다.	웹 보고서의 경우 개별 보고서 페이지 설명에 사용 가능한 필터가 나와 있습니다. 새 웹 인터페이스의 Web Reporting(웹 보고) 페이지 이해, 212 페이지를 참조하십시오.

카운터를 사용하여 트렌드 그래프에서 데이터 필터링

트렌드 그래프에서 필요한 시간 범위 및 사용 가능한 카운터를 기준으로 데이터를 필터링할 수 있습니다.

Time Range(시간 범위) 드롭다운에서 선택하는 시간 범위는 다른 값을 선택할 때까지 트렌드 그래프에 사용 됩니다.

Mail Flow Summary(메일 플로우 요약) 보고서 페이지의 트렌드 그래프에서 카운터는 여러 필터별로 데이터를 보는 데 사용됩니다. 데이터를 필터링하려면 사용 가능한 카운터를 클릭합니다.

보고서에 포함된 메시지 또는 트랜잭션의 세부사항 보기

단계 **1** 보고서 페이지 테이블에서 파란색 숫자를 클릭합니다.

(모든 테이블이 이러한 링크가 있는 것은 아닙니다.)

해당 숫자에 포함된 메시지 또는 트랜잭션이 각각 Message Tracking(메시지 추적) 또는 Web Tracking(웹 추적)에 표시됩니다.

단계 **2** 메시지 또는 트랜잭션의 목록을 보려면 아래로 스크롤합니다.

다음에 수행할 작업

• 메시지 추적, 263 페이지

이메일 보고서의 성능 향상

1개월간 고유 항목의 수가 많아 집계 보고의 성능이 저하될 경우 보고 필터를 사용하여 전년도를 다루는 보고서(전년도 보고서)에 데이터를 집계하는 것으로 제한합니다. 이 필터로 보고서에서 세부, 개별 IP, 도메인 또는 사용자 데이터를 제한할 수 있습니다. 개요 보고서 및 요약 정보는 모든 보고서에서 계속 사용 가능합니다.

CLI에서 **reportingconfig > filters** 메뉴를 사용하여 보고 필터 하나 이상을 활성화할 수 있습니다. 변경 사항을 적용하려면 커밋해야 합니다.

- **IP Connection Level Detail(IP** 연결 레벨 세부사항**)**. 이 필터를 활성화하면 Security Management Appliance는 개별 IP 주소에 대한 정보를 기록하지 않습니다. 이 필터는 공격 때문에 대규모 수신 IP 주소를 처리하는 시스템에 적절합니다.

  이 필터는 다음 지난해 보고서에 적용됩니다.

  - 수신 메일의 발신자 프로필
  - 수신 메일의 IP 주소
  - IP Addresses for Outgoing Senders(발신 발신자에 대한 IP 주소)

- **User Detail(**사용자 세부사항**)**. 이 필터를 활성화하면 Security Management Appliance는 메일을 주고받은 개별 사용자 및 사용자 메일에 적용된 콘텐츠 필터에 대한 정보를 기록하지 않습니다. 이 필터는 수백만의 내부 사용자 메일을 처리하는 어플라이언스에 또는 시스템이 수신자 주소를 검증하지 않는 경우에 적절합니다.

  이 필터는 다음 지난해 보고서에 적용됩니다.

  - Internal Users(내부 사용자)
  - 내부 사용자 세부사항
  - 발신자 IP 주소

- 콘텐츠 필터

- **Mail Traffic Detail**(메일 트래픽 세부사항). 이 필터를 활성화하면 Security Management Appliance는 어플라이언스가 모니터링하는 개별 도메인 및 네트워크에 대한 정보를 기록하지 않습니다. 이 필터는 유효한 수신 또는 발신 도메인 수가 수천만에 달할 경우 적절합니다.

  이 필터는 다음 지난해 보고서에 적용됩니다.

  - 수신 메일의 도메인
  - 수신 메일의 발신자 프로필
  - 내부 사용자 세부사항
  - 발신자 도메인

참고 이전 시간의 최신 보고 데이터를 보려면 개별 어플라이언스에 로그인하고 거기서 데이터를 봐야 합니다.

보고/추적 데이터 인쇄 및 내보내기

표 *14:* 보고/추적 데이터 인쇄 및 내보내기

필요한 것	PDF	CSV	수행해야 할 작업	참고
인터랙티브 보고서 페이지의 PDF	•		인터랙티브 보고서 페이지의 상단 오른쪽에서 **Printable (PDF)** 링크를 클릭합니다.	PDF는 현재 보고 있는 맞춤 설정을 반영합니다. PDF는 인쇄용 형식으로 지정됩니다.
보고서 데이터의 PDF	•		예약 또는 온디맨드 보고서를 생성합니다. 참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지 • 웹 보고서 예약 , 239 페이지	—

필요한 것	PDF	CSV	수행해야 할 작업	참고
원시 데이터 CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기 , 44 페이지도 참조하십시오.		•	차트 또는 테이블 아래에 있는 **Export**(내보내기) 링크를 클릭합니다.	CSV 파일은 차트 또는 테이블에 표시되는 데이터뿐 아니라 해당되는 모든 데이터를 포함하고 있습니다.
		•	예약 또는 온디맨드 보고서를 생성합니다. 참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지 • 온디맨드 웹 보고서 생성 , 243 페이지 • 웹 보고서 예약 , 239 페이지	각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다. 일부 확장 보고서는 CSV 형식으로 사용할 수 없습니다.
다국어 보고서	•		보고서를 예약하거나 온디맨드 보고서를 생성할 때 원하는 보고서 언어를 선택합니다.	Windows 컴퓨터에서 중국어, 일본어 또는 한국어로 PDF를 생성하려면 Adobe.com에서 해당 글꼴 팩을 다운로드하여 로컬 컴퓨터에 설치해야 합니다.
(Web Security) 보고서 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).	•	•	웹 추적에서 검색을 수행하고 Web Tracking(웹 추적) 페이지에서 Printable Download(인쇄용 버전 다운로드) 링크를 클릭합니다. PDF 또는 CSV 형식을 선택합니다.	PDF는 웹 페이지에 있는 정보 중 일부를 포함하지 않을 수도 있습니다. 즉 PDF는 다음 항목을 포함합니다. • 최대 1,000개의 트랜잭션. • 세부사항을 표시할 경우 최대 100개의 관련 트랜잭션. • 관련 트랜잭션당 최대 3,000자. CSV 파일은 검색 조건과 매칭하는 모든 원시 데이터를 포함합니다.
(Email Security) 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).		•	메시지 추적에서 검색을 수행하고 검색 결과 위에 있는 Export(내보내기) 링크 또는 Export All(모두 내보내기) 링크를 클릭합니다.	Export(내보내기) 링크는 검색 조건에 지정한 한도에서 표시된 검색 결과의 CSV 파일을 다운로드합니다. Export All(모두 내보내기) 링크는 검색 조건과 매칭하는 최대 50,000개의 메시지를 포함하는 CSV 파일을 다운로드합니다. 팁: 내보내야 할 메시지가 50,000개를 초과할 경우 더 짧은 시간 범위 집합에 대해 연속적으로 내보내기를 수행합니다.

표 *15:* 새 웹 인터페이스에서 보고/추적 데이터 인쇄 및 내보내기

필요한 것	CSV	수행해야 할 작업	참고
원시 데이터 CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기 , 44 페이지 섹션도 참조해 주십시오.	•	차트 또는 테이블 아래의 Export(내보내기) 링크를 클릭합니다.	CSV 파일은 차트 또는 테이블에 표시되는 데이터는 물론, 해당되는 모든 데이터를 포함하고 있습니다.
	•	예약 또는 온디맨드 보고서를 생성합니다. 참조: • 온디맨드 이메일 보고서 생성 , 170 페이지 • 이메일 보고서 예약, 169 페이지	각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 둘 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다. 일부 확장 보고서는 CSV 형식으로 사용할 수 없습니다.
(Web Security) 보고서 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).	•	웹 추적에서 검색을 수행하고 Web Tracking(웹 추적) 페이지에서 Printable Download(인쇄용 버전 다운로드) 링크를 클릭합니다. PDF 또는 CSV 형식을 선택합니다.	CSV 파일은 검색 조건과 매칭하는 모든 원시 데이터를 포함합니다.

필요한 것	CSV	수행해야 할 작업	참고
(Email Security) 데이터의 맞춤 하위 집합(예: 특정 사용자의 데이터).	•	메시지 추적에서 검색을 수행하고 검색 결과 위에 있는 Export(내보내기) 링크 또는 Export All(모두 내보내기) 링크를 클릭합니다.	Export(내보내기) 링크는 검색 조건에 지정한 한도에서 표시된 검색 결과의 CSV 파일을 다운로드합니다. Export All(모두 내보내기) 링크는 검색 조건과 매칭하는 최대 50,000개의 메시지를 포함하는 CSV 파일을 다운로드합니다. 팁: 내보내야 할 메시지가 50,000개를 초과할 경우 더 짧은 시간 범위 집합에 대해 연속적으로 내보내기를 수행합니다.

CSV(Comma-Separated Values) 파일로 보고서 데이터 내보내기

원시 데이터를 CSV(comma-separated values) 파일로 내보낼 수 있습니다. 이 파일은 Microsoft Excel과 같은 데이터베이스 애플리케이션을 사용하여 액세스하고 다룰 수 있습니다. 데이터를 내보내는 여러 가지 방법에 대해서는 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

CSV 내보내기에는 원시 데이터만 포함되므로, 백분율 같은 계산된 데이터가 웹 기반 보고서에는 나타나더라도 웹 기반 보고서 페이지에서 내보낸 데이터에는 포함되지 않을 수 있습니다.

Security Management Appliance에 설정된 내용과 상관없이, 이메일 메시지 추적 및 보고 데이터의 경우 내보낸 CSV 데이터는 GMT로 모든 데이터를 표시합니다. 이렇게 하면 특히 여러 표준 시간대의 어플라이언스에 있는 데이터를 참조할 때, 해당 어플라이언스의 데이터를 독립적으로 사용할 수 있습니다.

다음 예는 악성코드 차단 범주 보고서의 원시 데이터 내보내기에 있는 항목입니다. 여기서 PDT(Pacific Daylight Time)가 GMT - 7시간으로 표시됩니다.

Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100, 2625

표 ***16:*** 원시 데이터 항목 보기

카테고리 헤더	Value	설명
Begin Timestamp	1159772400.0	쿼리 시작 시간입니다(epoch 이후 초 수).
End Timestamp	1159858799.0	쿼리 종료 시간입니다(epoch 이후 초 수).

카테고리 헤더	**Value**	설명
Begin Date	2006-10-02 07:00 GMT	쿼리가 시작된 날짜입니다.
End Date	2006-10-03 오전 6:59 GMT	쿼리가 종료된 날짜입니다.
Name	Adware	악성코드 카테고리의 이름입니다.
Transactions Monitored	525	모니터링되는 트랜잭션 수입니다.
Transactions Blocked	2100	차단된 트랜잭션 수입니다.
Transactions Detected	2625	총 트랜잭션 수. 탐지된 트랜잭션 수 + 차단된 트랜잭션 수

참고 카테고리 헤더는 보고서 유형마다 서로 다릅니다. 현지화된 CSV 데이터를 내보낼 경우 일부 브라우저에서 제목이 제대로 표시되지 않을 수 있습니다. 이 문제는 일부 브라우저에서 현지화된 텍스트의 적절한 문자 집합을 사용하지 않았기 때문에 발생할 수 있습니다. 이 문제를 해결하려면 파일을 로컬 시스템에 저장하고, **File(**파일**) > Open(**열기**)**을 사용하여 브라우저에서 열 수 있습니다. 파일을 열 때 현지화된 텍스트를 표시하기 위한 문자 집합을 선택합니다.

모든 보고서 트러블슈팅

백업 **Security Management Appliance**에서 보고서 데이터를 볼 수 없음

문제

보고서 데이터를 볼 단일 Email Security Appliance를 선택할 수 없습니다. **View Data For(**데이터 보기**)** 옵션은 보고서 페이지에서 나타나지 않습니다.

솔루션

백업 중 서비스 가용성 , 442 페이지도 참고하십시오.

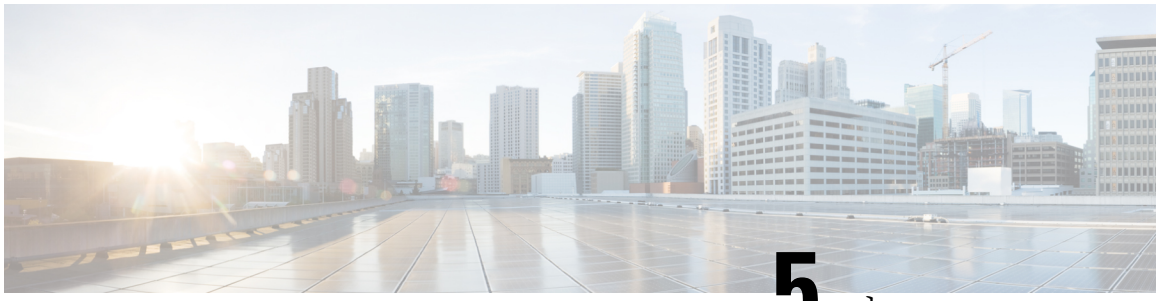
보고가 비활성화됨

문제

진행 중인 백업을 취소하면 보고가 비활성화될 수 있습니다.

솔루션

백업이 완료되면 보고 기능이 복원됩니다.



5 장

중앙 이메일 보안 보고 사용

이 장에는 다음 섹션이 포함되어 있습니다.

중앙 이메일 보고 개요

Cisco Content Security Management Appliance는 이메일 트래픽 패턴 및 보안 위험을 모니터링할 수 있도록 개별 또는 다중 Email Security Appliance에서 수집된 정보를 보여줍니다. 보고서를 실시간으로 실행하여 지정된 기간에 시스템 활동을 상호 작용 방식으로 표시할 수도 있고, 보고서를 예약하여 정기적으로 실행할 수도 있습니다. 보고 기능을 사용하여 원시 데이터를 파일로 내보낼 수도 있습니다.

이 기능은 Email Security Appliance의 Monitor(모니터) 메뉴에 나열되는 보고서를 한데 모아 표시합니다.

중앙 집중식 이메일 보고 기능은 요약 보고서를 생성하여 네트워크의 상황을 파악하는 데 도움을 주는 것은 물론 특정 도메인, 사용자 또는 범주로 드릴다운하여 트래픽 세부사항을 확인하도록 지원합니다.

중앙 집중식 추적 기능을 사용하면 여러 Email Security Appliance에서 이동하는 이메일 메시지를 추적할 수 있습니다.

참고 Email Security Appliance는 로컬 보고가 사용되는 경우에만 데이터를 저장합니다. 중앙 집중식 보고가 Email Security Appliance에 대해 활성화된 경우, Email Security Appliance는 System Capacity(시스템 용량) 및 System Status(시스템 상태) 이외의 어떤 보고 데이터도 유지하지 않습니다. 중앙 집중식 이메일 보고가 활성화되지 않은 경우 System Capacity(시스템 용량) 및 System Status(시스템 상태) 보고서만 생성됩니다.

중앙 집중식 보고로 전환하는 동안과 그 이후의 보고 데이터 가용성에 대한 자세한 내용은 Email Security Appliance에 대한 문서나 온라인 도움말의 "중앙 집중식 보고 모드" 섹션을 참조하십시오.

중앙 이메일 보고 설정

중앙 이메일 보고를 설정하려면 다음 절차를 순서대로 완료합니다.

- Security Management Appliance에서 중앙 이메일 보고 활성화 , 62 페이지
- 관리 대상 ESA 각각에 중앙 이메일 보고 서비스 추가 , 63 페이지
- ESA에서 중앙 이메일 보고 활성화 , 64 페이지

참고 보고 및 추적이 일관성이 없고 동시에 활성화되지 않고 제대로 작동하지 않는 경우 또는 각 Email Security Appliance에서 일관성 있게 동시에 중앙 집중화되거나 로컬에 저장되지 않는 경우, 보고서에서 드릴다운할 때 메시지 추적 결과가 예상과 일치하지 않게 됩니다. 각 기능(보고, 추적)에 대한 데이터는 기능이 활성화된 동안에만 캡처되기 때문입니다.

Security Management Appliance에서 중앙 이메일 보고 활성화

시작하기 전에

- 중앙 집중식 보고를 활성화하려면 우선 모든 Email Security Appliance를 구성하고 예상대로 작동하는지 확인해야 합니다.
- 중앙 집중식 이메일 보고를 활성화하기 전에 이 서비스를 위한 디스크 공간이 충분히 할당되었는지 확인하십시오. 디스크 공간 관리 , 487 페이지를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 집중식 서비스) > **Email**(이메일) > **Centralized Reporting**(중앙 집중식 보고)을 선택합니다.

단계 **3** **Enable**(활성화)을 클릭합니다.

단계 **4** 시스템 설정 마법사를 실행한 후 처음 중앙 이메일 보고를 활성화하는 경우 최종 사용자 라이센스 계약을 읽고 **Accept**(동의)를 클릭합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

참고 어플라이언스에서 이메일 보고를 활성화한 경우 이 작업에 대한 디스크 공간이 할당되지 않았으면 중앙 이메일 보고는 디스크 공간이 할당될 때까지 작동하지 않습니다. 이메일 보고 및 추적을 위한 할당량이 현재 사용된 디스크 공간보다 크다면 보고 및 추적 데이터를 잃을 염려가 없습니다. 자세한 내용은 디스크 공간 관리 , 487 페이지 섹션을 참조하십시오.

관리 대상 **ESA** 각각에 중앙 이메일 보고 서비스 추가

수행하는 단계는 또 다른 중앙 관리 기능을 구성할 때 어플라이언스를 이미 추가했는지 여부에 따라 달라집니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 이 페이지의 목록에 Email Security Appliance를 이미 추가한 경우

a) Email Security Appliance의 이름을 클릭합니다.

b) **Centralized Reporting(**중앙 보고**)** 서비스를 선택합니다.

단계 **4** Email Security Appliance를 아직 추가하지 않은 경우

a) Add Email Appliance(이메일 어플라이언스 추가)를 클릭합니다.

b) Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 Security Management Appliance의 Management 인터페이스에 대한 IP 주소를 입력합니다.

참고 IP Address(IP 주소) 텍스트 필드에 DNS 이름을 입력하는 경우 **Submit(**제출**)**을 클릭하면 즉시 IP 주소로 해석됩니다.

c) 중앙 보고 서비스가 미리 선택되어 있습니다.

d) **Establish Connection(**연결 설정**)**을 클릭합니다.

e) 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다..

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

f) 페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.

g) **Test Connection(**테스트 연결**)**을 클릭합니다..

h) 테이블 위의 테스트 결과를 읽습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** Centralized Reporting(중앙 집중식 보고)을 활성화할 각 Email Security Appliance에 대해 이 절차를 반복합니다.

단계 **7** 변경사항을 커밋합니다.

이메일 보고 그룹 생성

Security Management Appliance의 보고 데이터를 보기 위한 Email Security Appliance의 그룹을 만들 수 있습니다.

그룹에는 하나 이상의 어플라이언스를 포함할 수 있으며, 어플라이언스는 둘 이상의 그룹에 속할 수 있습니다.

시작하기 전에

각 어플라이언스에서 중앙 보고가 활성화되어 있어야 합니다. 관리 대상 ESA 각각에 중앙 이메일 보고 서비스 추가 , 63 페이지를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Centralized Reporting(**중앙 집중식 보고**)**을 선택합니다.

단계 **3** **Add Group(**그룹 추가**)**을 클릭합니다.

단계 **4** 그룹의 고유한 이름을 입력합니다.

Security Management Appliance에 추가한 Email Security Appliance가 Email Security Appliance 목록에 표시됩니다. 그룹에 추가할 어플라이언스를 선택합니다.

추가할 수 있는 최대 그룹 수는 연결 가능한 최대 이메일 어플라이언스의 수보다 작거나 같습니다.

참고 Email Security Appliance를 Security Management Appliance에 추가했지만 목록에 표시되지 않는 경우, Security Management Appliance가 보고 데이터를 수집할 수 있도록 Email Security Appliance의 구성을 수정하십시오.

단계 **5** **Add(**추가**)**를 클릭하여 Group Members(그룹 구성원) 목록에 어플라이언스를 추가합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

ESA에서 중앙 이메일 보고 활성화

각각의 매니지드 Email Security Appliance에서 중앙 집중식 이메일 보고를 활성화해야 합니다.

자세한 내용은 Email Security Appliance에 대한 문서 또는 온라인 도움말의 "중앙 집중식 보고를 사용하도록 Email Security Appliance 구성" 섹션을 참조하십시오.

이메일 보고서 데이터 사용

- 보고서 데이터 액세스 및 보기 옵션에 대해서는 보고 데이터를 보는 방법 , 33 페이지를 참조하십시오.
- 보고서 데이터의 보기를 맞춤 설정하려면 보고 데이터 보기 맞춤화 , 35 페이지를 참조하십시오.
- 데이터 내에서 특정 정보를 검색하려면 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.
- 보고서 정보를 인쇄하거나 내보내려면 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.
- 다양한 인터랙티브 보고서 페이지를 이해하려면 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.
- 온디맨드 보고서를 생성하려면 온디맨드 이메일 보고서 생성 , 170 페이지를 참조하십시오.
- 일정한 간격으로 또한 사용자가 지정한 시간에 자동으로 보고서가 실행되게 예약하려면 이메일 보고서 예약, 169 페이지를 참조하십시오.
- 온디맨드 및 예약 보고서를 보려면 아카이브 이메일 보고서 보기 및 관리 , 172 페이지를 참조하십시오.
- 배경 정보는 Security Management Appliance에서 보고서를 위한 데이터를 수집하는 방법, 34 페이지를 참조하십시오.
- 방대한 양의 데이터를 다룰 때 성능을 향상시키려면 이메일 보고서의 성능 향상 , 40 페이지를 참조하십시오.
- 차트 또는 테이블에서 파란색 링크로 나타나는 개체 또는 수치의 세부사항을 보려면 해당 개체 또는 수치를 클릭합니다.

  예를 들어 권한상 허용된다면 이 기능을 사용하여 콘텐츠 필터링 또는 DLP 정책을 위반하는 메시지의 세부사항을 볼 수 있습니다. 그러면 메시지 추적에서 관련 검색을 수행합니다. 아래로 스크롤하여 결과를 봅니다.

새로운 웹 인터페이스에서 이메일 보고서 사용

- 보고서 데이터 액세스 및 보기 옵션에 대해서는 보고 데이터를 보는 방법 , 47 페이지를 참조하십시오.
- 보고서 데이터의 보기를 맞춤 설정하려면 보고 데이터 보기 맞춤화 , 50 페이지을 참고하십시오.
- 보고서 정보를 인쇄하거나 내보내려면 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참고하십시오.
- 다양한 인터랙티브 보고서 페이지를 이해하려면 인터랙티브 보고서 페이지 사용, 49 페이지를 참조하십시오.

- 온디맨드 보고서를 생성하려면 온디맨드 이메일 보고서 생성 , 170 페이지를 참조하십시오.
- 일정한 간격으로 또한 사용자가 지정한 시간에 자동으로 보고서가 실행되게 예약하려면 이메일 보고서 예약, 169 페이지를 참조하십시오.
- 온디맨드 및 예약 보고서를 보려면 아카이브 이메일 보고서 보기 및 관리 , 172 페이지를 참조하십시오.
- 배경 정보는 Security Management Appliance에서 보고서를 위한 데이터를 수집하는 방법, 34 페이지를 참조하십시오.
- 방대한 양의 데이터를 다룰 때 성능을 향상시키려면 이메일 보고서의 성능 향상 , 40 페이지를 참조하십시오.
- 차트 또는 테이블에서 파란색 링크로 나타나는 개체 또는 수치의 세부사항을 보려면 해당 개체 또는 수치를 클릭합니다.

  예를 들어 권한상 허용된다면 이 기능을 사용하여 콘텐츠 필터링 또는 DLP 정책을 위반하는 메시지의 세부사항을 볼 수 있습니다. 그러면 메시지 추적에서 관련 검색을 수행합니다. 아래로 스크롤하여 결과를 봅니다.

검색 및 인터랙티브 이메일 보고서 페이지

인터랙티브 이메일 보고 페이지 중 상당수는 페이지 맨 아래에 **'Search For(검색):'** 드롭다운 메뉴가 있습니다.

드롭다운 메뉴에서 다음을 비롯한 여러 유형의 조건으로 검색할 수 있습니다.

- IP 주소
- 도메인
- 네트워크 소유자
- 내부 사용자
- 목적지 도메인
- 내부 발신자 도메인
- 내부 발신자 IP 주소
- 수신 TLS 도메인
- 발신 TLS 도메인
- SHA-256

대부분의 검색에서는 검색 텍스트와 정확한 매치를 찾을지 아니면 입력한 텍스트로 시작하는 항목을 찾을지(예: "ex"로 시작하면 "example.com"이 검색됨) 선택합니다.

IPv4 검색의 경우, 입력한 텍스트는 점 십진수 형식에서 최대 4개의 IP 옥텟으로 시작하는 것으로 해석됩니다. 예를 들어 '17.*'은 17.0.0.0~17.255.255.255 범위에서 검색하므로, 17.0.0.1은 매치하지만 172.0.0.1은 매치하지 않습니다. 정확하게 매치하는 것을 찾으려면 네 개의 옥텟을 모두 입력하면 됩니다. IP 주소 검색은 CIDR(Classless Inter-Domain Routing) 형식(17.16.0.0/12)도 지원합니다.

IPv6 검색에서는 다음 예의 형식을 사용하여 주소를 입력할 수 있습니다.

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

이메일 보고 페이지 이해

참고 이 목록에는 지원되는 최신 Email Security Appliance용 AsyncOS 릴리스에서 사용 가능한 보고서가 나와 있습니다. Email Security Appliance에서 이전 AsyncOS 릴리스를 실행 중인 경우 이러한 보고서 중 일부를 사용할 수 없습니다.

표 ***17: Email Reporting(***이메일 보고***)*** 탭 옵션

이메일 보고 메뉴	작업
이메일 보고 개요 페이지	Overview(개요) 페이지는 Email Security Appliance에 대한 활동 개요를 제공합니다. 이 페이지에는 수신 및 발신 메시지에 대한 그래프와 요약 테이블이 포함되어 있습니다. 자세한 내용은 이메일 보고 개요 페이지, 74 페이지를 참조하십시오.
Incoming Mail(수신 메일) 페이지	Incoming Mail(수신 메일) 페이지는 관리되는 Email Security Appliance에 연결된 모든 원격 호스트의 실시간 정보에 대한 인터랙티브 보고를 제공합니다. IP 주소, 도메인, 시스템에 메일을 전송하는 네트워크 소유자(조직)에 대한 정보를 수집할 수 있습니다. 자세한 내용은 Incoming Mail(수신 메일) 페이지, 78 페이지를 참조하십시오.
발신자 그룹 보고서 페이지	Sender Groups(발신자 그룹) 보고서 페이지는 발신자 그룹 및 메일 플로우 정책 작업별로 연결 요약을 제공하므로, SMTP 연결 및 메일 플로우 정책 추세를 검토할 수 있습니다. 자세한 내용은 발신자 그룹 보고서 페이지, 82 페이지를 참조하십시오.
Sender Domain Reputation(발신인 도메인 평판) 페이지	이 보고서 페이지를 사용하면 SDR 서비스에서 받은 판정과 위협 카테고리를 기반으로 수신 메시지를 볼 수 있습니다. 자세한 내용은 Sender Domain Reputation(발신인 도메인 평판) 페이지, 82 페이지를 참조하십시오.

이메일 보고 메뉴	작업
Outgoing Destinations(발신 대상) 페이지	Outgoing Destinations(발신 목적지) 페이지는 여기서 보내는 메일의 도메인에 대한 정보를 제공합니다. 페이지 맨 위에는 위협 메시지의 상위 목적지 및 정상 메시지의 상위 목적지를 보여주는 그래프가 있습니다. 맨 아래에는 전체 수신자를 기준으로 정렬된 열과 함께 차트를 표시합니다(기본 설정). 자세한 내용은 Outgoing Destinations(발신 대상) 페이지, 83 페이지를 참조하십시오.
발신자 페이지	Outgoing Senders(발신 발신자) 페이지는 네트워크의 IP 주소 및 도메인에서 전송되는 메일의 양과 유형에 대한 정보를 제공합니다. 자세한 내용은 발신자 페이지, 84 페이지를 참조하십시오.
Internal Users(내부 사용자) 페이지	Internal Users(내부 사용자)는 내부 사용자가 보내고 받는 메일에 대한 정보를 이메일 주소별로 제공합니다 단일 사용자가 여러 개의 이메일 주소를 가질 수 있습니다. 이메일 주소는 보고서에서 결합되지 않습니다. 자세한 내용은 Internal Users(내부 사용자) 페이지, 85 페이지를 참조하십시오.
DLP Incidents(DLP 인시던트)	DLP Incident Summary(DLP 인시던트 요약) 페이지는 발신 메일에서 발생하는 DLP(data loss prevention) 정책 위반에 대한 정보를 보여줍니다. 자세한 내용은 DLP Incidents(DLP 인시던트) , 86 페이지를 참조하십시오.
메시지 필터	Message Filters(메시지 필터) 페이지는 수신 및 발신 메시지에 대한 상위 메시지 필터 매칭 결과(매칭하는 메시지 수가 가장 많은 메시지 필터)를 보여줍니다. 자세한 내용은 메시지 필터 , 88 페이지을(를) 참고하십시오.
지리적 분포	Geo Distribution(지리적 분포) 페이지에 다음 내용이 표시됩니다. • 그래픽 형식의 발신지 국가별 상위 수신 메일 연결입니다. • 표 형식의 발신지 국가별 상위 수신 메일 연결입니다. 자세한 내용은 지리적 분포, 88 페이지를 참조하십시오.
대량 메일	High Volume Mail(대량 메일) 페이지는 가변적인 1시간 동안 단일 발신자가 보낸 또는 동일한 제목으로 된 최다 메시지 수의 공격을 보여줍니다. 자세한 내용은 대량 메일 , 88 페이지를 참조하십시오.

이메일 보고 메뉴	작업
Content Filters(콘텐츠 필터) 페이지	Content Filters(콘텐츠 필터) 페이지는 상위 수신 및 발신 콘텐츠 필터 매칭 결과(매칭하는 메시지가 가장 많은 콘텐츠 필터)에 대한 정보를 제공합니다. 또한 이 페이지에서는 데이터가 막대 차트 및 목록으로 표시됩니다. Content Filters(콘텐츠 필터) 페이지를 사용하면 콘텐츠 필터 또는 사용자 단위로 회사 정책을 검토할 수 있습니다. 자세한 내용은 Content Filters(콘텐츠 필터) 페이지, 89 페이지를 참조하십시오.
DMARC 확인	DMARC Verification(DMARC 검증) 페이지는 DMARC(Domain-based Message Authentication, Reporting and Conformance) 검증에 실패한 상위 발신자 도메인 및 그 도메인으로부터 수신한 메시지에 대해 수행한 조치의 요약을 표시합니다. 자세한 내용은 DMARC 확인 , 89 페이지를 참조하십시오.
매크로 탐지	Macro Detection Report(매크로 탐지 보고서) 페이지에는 상위 수신 및 발신 매크로가 활성화된 첨부 파일이 콘텐츠 또는 메시지 필터로 탐지된 파일 형식으로 표시됩니다. 자세한 내용은 매크로 탐지, 90 페이지을(를) 참고하십시오.
External Threat Feeds(외부 위협 피드) 페이지	External Threat Feeds(외부 위협 피드) 페이지에는 다음 보고서가 표시됩니다. • 메시지에서 위협을 탐지하는 데 사용되는 상위 ETF 소스입니다. • 메시지에서 탐지된 위협과 일치하는 상위 IOC입니다. • 악의적인 수신 메일 연결을 필터링하는 데 사용되는 상위 ETF 소스입니다. 자세한 내용은 External Threat Feeds(외부 위협 피드) 페이지, 90 페이지를 참조하십시오.
Virus Types(바이러스 유형) 페이지	Virus Types(바이러스 유형) 페이지는 네트워크로/네트워크에서 전송되는 바이러스의 개요를 제공합니다. Virus Types(바이러스 유형) 페이지는 Email Security Appliance에서 실행 중인 바이러스 검사 엔진에 의해 탐지되고 Security Management Appliance에 표시되는 바이러스를 보여줍니다. 특정 바이러스에 대해 작업을 수행하려면 이 보고서를 사용합니다. 자세한 내용은 Virus Types(바이러스 유형) 페이지, 91 페이지를 참조하십시오.

이메일 보고 메뉴	작업
URL Filtering(URL 필터링) 페이지	메시지에서 가장 자주 발생하는 URL 카테고리, 스팸 메시지에 가장 많이 포함된 URL, 메시지에 나타난 악성 및 일반 URL 수를 확인할 때 이 페이지를 활용합니다. 자세한 내용은 URL Filtering(URL 필터링) 페이지 , 92 페이지를 참조하십시오.
Web Interaction Tracking(웹 상호 작용 추적) 페이지	정책 또는 Outbreak Filter에 의해 재작성된 URL을 클릭한 엔드유저 및 및 각 사용자의 클릭과 연결된 조치를 나타냅니다. 자세한 내용은 Web Interaction Tracking(웹 상호 작용 추적) 페이지, 92 페이지를 참조하십시오.
Forged Email Detection(위조 이메일 탐지) 페이지	Forged Email Detection(위조 이메일 탐지) 페이지에는 다음 보고서가 포함됩니다. • **Top Forged Email Detection**(상위 위조 이메일 탐지). 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 사용자 상위 10명이 표시됩니다. • **Forged Email Detection: Details**(위조 이메일 탐지**:** 세부 정보**)**. 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 모든 사용자 목록과, 지정한 사용자에 대해 일치하는 메시지 수가 표시됩니다. Forged Email Detection(위조 이메일 탐지) 페이지, 93 페이지를 참조하십시오.
Advanced Malware Protection(파일 평판 및 파일 분석) 보고 페이지	3가지 보고 페이지에서 파일 평판 및 분석 데이터를 제시합니다. 자세한 내용은 Advanced Malware Protection(파일 평판 및 파일 분석) 보고 페이지 , 94 페이지를 참조하십시오.
사서함 자동 치료	이 페이지를 사용하여 사서함 치료 결과의 세부 정보를 표시합니다. 사서함 자동 치료, 100 페이지를 참조하십시오.
TLS Connections(TLS 연결) 페이지	TLS Connections(TLS 연결) 페이지는 주고받은 메일에 대한 TLS 연결의 전체 사용량을 보여줍니다. 보고서에서는 또한 TLS 연결을 사용하여 메일을 전송하는 각 도메인에 대한 세부사항도 보여줍니다. 자세한 내용은 TLS Connections(TLS 연결) 페이지, 100 페이지를 참조하십시오.

이메일 보고 메뉴	작업
Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지	Inbound SMTP authentication(인바운드 SMTP 인증) 페이지는 클라이언트 인증서의 사용 및 ESA와 사용자 메일 클라이언트 간 SMTP 세션 인증을 위한 SMTP AUTH 명령을 보여줍니다. 자세한 내용은 Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지, 101 페이지를 참고하십시오.
Outbreak Filters 페이지	Outbreak Filters 페이지는 Outbreak Filter에서 격리한 최근 보안 침해 및 메시지에 대한 정보를 제공합니다. 바이러스 공격에 대한 방어 체계를 모니터링할 때 이 보고서를 활용합니다. 자세한 내용은 Outbreak Filters 페이지, 103 페이지를 참조하십시오.
Rate Limits(속도 제한) 페이지	Rate Limits(속도 제한) 페이지는 설정된 발신자별 메일 수신자 수 한도를 초과하는 메일 발신자(MAIL-FROM 주소 기준)를 표시합니다. 자세한 내용은 Rate Limits(속도 제한) 페이지 , 102 페이지를 참조하십시오.
System Capacity(시스템 용량) 페이지	Security Management Appliance에 보고 데이터를 전송하는 전체적인 워크로드를 볼 수 있습니다. 자세한 내용은 System Capacity(시스템 용량) 페이지, 105 페이지를 참조하십시오.
보고 데이터 가용성 페이지	보고 데이터가 Security Management Appliance에 미치는 영향을 각 어플라이언스에 대해 간략하게 볼 수 있습니다. 자세한 내용은 보고 데이터 가용성 페이지, 109 페이지를 참조하십시오.
이메일 보고서 예약	지정된 시간 범위에 대해 보고서를 예약할 수 있습니다. 자세한 내용은 이메일 보고서 예약, 169 페이지을 참조하십시오.
아카이브 이메일 보고서 보기 및 관리	아카이브 보고서를 보고 관리할 수 있습니다. 자세한 내용은 아카이브 이메일 보고서 보기 및 관리 , 172 페이지를 참조하십시오. 온디맨드 보고서를 생성할 수 있습니다. 온디맨드 이메일 보고서 생성 , 170 페이지를 참조하십시오.

이메일 보고 페이지의 테이블 열 설명

표 ***18:*** 이메일 보고 페이지의 테이블 열 설명

열 이름	
수신 메일 정보	

열 이름	
거부된 연결	HAT 정책에 의해 차단된 모든 연결. 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다.
허용된 연결	허용된 모든 연결.
총 시도 수	시도하여 수락된 또는 차단된 모든 연결.
수신자 제한에 의한 차단	Stopped by Reputation Filtering(평판 필터링에 의해 차단됨) 구성 요소입니다. 시간당 최대 수신자 수, 메시지당 최대 수신자 수 또는 연결당 최대 메시지 수 등 HAT 제한 중 하나가 초과되어 차단된 수신자 메시지 수를 나타냅니다. 이 수는 거부된 또는 TCP 거절된 연결과 관련이 있는 수신자 메시지의 추정치와 합산되어 Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)을 산출합니다.
평판 필터링에 따른 차단	Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)에 대한 값은 여러 요인을 기반으로 계산됩니다. • 해당 발신자가 보낸 "제한된(throttled)" 메시지의 수 • 거부된 또는 TCP 거절된 연결의 수(부분 개수일 수 있음) • 연결당 메시지 수에 대한 보수적 승수 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다. 이 상황에서는 표시된 값을 "바닥(floor)"으로 해석할 수 있습니다. 즉 최소한 이 개수의 메시지가 차단된 것입니다. 참고 Overview(개요) 페이지의 Stopped by Reputation Filtering(평판 필터링에 의해 차단됨) 합계는 항상 거부된 모든 연결의 전체 개수를 기반으로 합니다. 발신자 기준 연결 개수만 부하 때문에 제한됩니다.

열 이름	
올바르지 않은 수신자로 차단됨	대화형 LDAP 거부에 의해 거부된 모든 수신자와 모든 RAT 거부를 더한 수
탐지된 스팸	탐지된 모든 스팸.
탐지된 바이러스	탐지된 모든 바이러스
콘텐츠 필터에 의해 차단됨	콘텐츠 필터에 의해 차단된 총 메시지 수.
총 위협	총 위협 메시지 수(평판에 의해 차단됨, 잘못된 수신자, 스팸 및 바이러스로 분류되어 차단됨).
마케팅	원치 않은 마케팅 메시지로 탐지된 메시지 수.
정상	모든 정상 메시지. 그레이메일 기능이 활성화되지 않은 어플라이언스에서 처리된 메시지는 정상으로 분류됩니다.
사용자 메일 흐름 세부사항**(**내부 사용자 페이지**)**	
탐지된 수신 스팸	탐지된 모든 수신 스팸
탐지된 수신 바이러스	탐지된 수신 바이러스.
수신 콘텐츠 필터 매치	탐지된 수신 콘텐츠 필터 매치.
콘텐츠 필터에 의해 차단된 수신 메시지	설정된 콘텐츠 필터에 의해 차단된 수신 메시지.
수신 정상	모든 수신 정상 메시지.
탐지된 발신 스팸	탐지된 발신 스팸.
탐지된 발신 바이러스	탐지된 발신 바이러스.
발신 콘텐츠 필터 매치	탐지된 발신 콘텐츠 필터 매치.
콘텐츠 필터에 의해 차단된 발신 메시지	설정된 콘텐츠 필터에 의해 차단된 발신 메시지.
발신 정상	모든 발신 정상 메시지.
수신 및 발신 **TLS** 연결**: TLS** 연결 페이지	
필수 TLS: 실패	실패한 모든 필수 TLS 연결.
필수 TLS: 성공	성공한 모든 필수 TLS 연결.
선호 TLS: 실패	실패한 모든 선호 TLS 연결.
선호 TLS: 성공	성공한 모든 선호 TLS 연결.

열 이름	
전체 연결 수	총 TLS 연결 수.
총 메시지 수	총 TLS 메시지 수.
Outbreak Filter	
보안 침해 이름	보안 침해 이름.
보안 침해 ID	보안 침해 ID.
전역 최초 확인	전역에서 바이러스가 처음 확인되었을 때.
보호 시간	바이러스에 대한 보호가 이루어진 시간.
격리된 메시지	격리 관련 메시지.

이메일 보고 개요 페이지

Security Management Appliance의 **Email(**이메일**) Reporting(**보고**) Overview(**개요**)** 페이지는 Email Security Appliance에서 발생한 이메일 메시지 활동의 개요를 제공합니다. Overview(개요) 페이지에는 수신 및 발신 메시지에 대한 그래프와 요약 테이블이 포함되어 있습니다.

상위 레벨에서 **Overview(**개요**)** 페이지는 수발신 메일 그래프 및 수발신 메일 요약도 표시합니다.

메일 추세 그래프는 메일 플로우를 시각적으로 나타냅니다. 메일 추세 그래프를 사용하여 어플라이언스를 드나드는 모든 메일의 플로우를 모니터링할 수 있습니다.

참고 도메인 기반 총괄 요약 보고서 및 총괄 개요 보고서는 이메일 보고 개요 페이지, 74 페이지를 기반으로 합니다. 자세한 내용은 도메인 기반 총괄 요약 보고서, 165 페이지 및 총괄 요약 보고서 , 168 페이지를 참조하십시오

표 ***19: Email Reporting Overview(***이메일 보고 개요***)*** 페이지 세부 정보

섹션	설명
시간 범위	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
View Data for(데이터 보기)	Overview(개요) 데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참고하십시오.

수신 메일 메시지 카운트 방법

수신 메시지 카운트는 메시지당 수신자 수를 기준으로 합니다. 예를 들어 example.com에서 오는 하나의 수신 메시지가 세 명의 수신자에게 전송되면 해당 발신자로부터 3개의 메시지가 오는 것으로 계산됩니다.

발신자 평판 필터링에 의해 차단된 메시지는 실제로 작업 대기열에 들어가지 못하므로, 어플라이언스는 수신 메시지에 대한 수신자 목록에 액세스하지 못합니다. 이 경우 수신자 수를 추적하기 위해 승수가 사용됩니다. 승수는 기존 고객 데이터의 대규모 샘플링을 조사하여 결정합니다.

어플라이언스에서 이메일 메시지를 분류하는 방법

이메일 파이프라인을 통해 진행되는 동안 메시지는 여러 범주에 적용될 수 있습니다. 예를 들어 한 메시지가 스팸 또는 바이러스 양성으로 표시될 수 있으며, 콘텐츠 필터와 매치할 수도 있습니다. 각종 필터 및 검사 활동의 우선순위가 메시지 처리 결과에 큰 영향을 미칩니다.

위의 예에서 다양한 판정이 이 우선순위 규칙을 따릅니다.

- 스팸 양성
- 바이러스 양성
- 콘텐츠 필터 일치

이 규칙에 따라, 메시지가 스팸 양성으로 표시되고 안티스팸 설정이 스팸 양성 메시지를 삭제하도록 설정된 경우 메시지가 삭제되고 스팸 카운터가 늘어납니다.

스팸 양성 메시지가 이메일 파이프라인에서 계속 진행되도록 안티스팸 설정이 구성되었으며 후속 콘텐츠 필터가 메시지를 삭제, 반송 또는 격리하는 경우에도 스팸 수가 증가합니다. 메시지가 스팸 또는 바이러스 양성이 아닌 경우에만 콘텐츠 필터 수가 증가합니다.

또는 메시지가 보안 침해 필터에 의해 격리된 경우, 격리에서 해제되어 작업 대기열을 통해 다시 처리될 때까지 계산되지 않습니다.

메시지 처리 우선 순위에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말이나 사용 설명서에 있는 이메일 파이프라인에 대한 장을 참조하십시오.

Overview(개요**)** 페이지의 이메일 메시지 분류

개요 보고서 페이지의 수신 메일 요약에서 보고되는 메시지는 다음과 같이 분류됩니다.

표 *20: Overview(개요)* 페이지의 이메일 범주

카테고리	설명
평판 필터링에 따른 차단	HAT 정책에 의해 차단된 모든 연결을 고정 승수로 곱하고(수신 메일 메시지 카운트 방법, 75 페이지 참조) 여기에 수신자 제한에 의해 차단된 모든 수신자를 더한 값. Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)에 대한 값은 여러 요인을 기반으로 계산됩니다. • 해당 발신자가 보낸 "제한된(throttled)" 메시지의 수 • 거부된 또는 TCP 거절된 연결의 수(부분 개수일 수 있음) • 연결당 메시지 수에 대한 보수적 승수 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다. 이 상황에서는 표시된 값을 "바닥(floor)"으로 해석할 수 있습니다. 즉 최소한 이 개수의 메시지가 차단된 것입니다. Overview(개요) 페이지의 Stopped by Reputation Filtering(평판 필터링에 의해 차단됨) 합계는 항상 거부된 모든 연결의 전체 개수를 기반으로 합니다. 발신자 기준 연결 개수만 부하 때문에 제한됩니다.
올바르지 않은 수신인	대화형 LDAP 거부에 의해 거부된 모든 수신자와 모든 RAT 거부를 더한 수
스팸 메시지 감지됨	안티스팸 검사 엔진에 의해 양성 또는 의심으로 탐지된 총 메시지 수. 또는 스팸이면서 동시에 바이러스 양성인 메시지.
탐지된 바이러스 메시지	바이러스 양성이며 스팸은 아닌 것으로 탐지된 메시지의 총 개수 및 비율. 다음 메시지는 "탐지된 바이러스" 범주에 포함됩니다. • 바이러스 검사 결과가 "손상" 또는 "감염"인 메시지. • 암호화 메시지를 바이러스 포함으로 간주하는 옵션이 선택된 경우 바이러스 검사 결과가 "암호화"인 메시지. • 검사 불가 메시지에 대한 조치가 "전달"이 아닐 경우 바이러스 검사 결과가 "검사 불가"인 메시지. • 대체 메일 호스트 또는 대체 수신자에게 전달하는 옵션이 선택된 경우 바이러스 검사 결과가 "검사 불가" 또는 "암호화"인 메시지. • 보안 침해 격리에서 수동으로 또는 시간 초과로 인해 삭제된 메시지.
AMP에서 탐지	메시지 첨부 파일이 파일 평판 필터링에서 악성으로 확인되었습니다. 이 값에는 파일 분석에 의해 악성으로 확인된 판정 업데이트 또는 파일이 포함되어 있지 않습니다.
악성 **URL**이 있는 메시지	메시지의 URL 중 하나 이상이 URL 필터링에서 악성으로 확인되었습니다.
콘텐츠 필터에 의해 차단됨	콘텐츠 필터에 의해 차단된 총 메시지 수. 사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 콘텐츠 필터 위반에 대한 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

카테고리	설명
DMARC에 의해 차단됨	DMARC 검증을 통과하지 못한 총 메시지 수.
S/MIME 확인/암호 해독 실패	S/MIME 검증 및/또는 해독에 실패한 총 메시지 수.
마케팅 메시지	확인된 마케팅 그룹(예: Amazon.com)에서 보낸 총 광고 메시지 수. 이 항목은 마케팅 데이터가 시스템에 있는 경우에만 나타납니다. 그레이메일 기능이 활성화된 Email Security Appliance 및 안티 스팸 설정의 마케팅 이메일 검사가 활성화된 어플라이언스 모두에서 식별한 마케팅 메시지도 여기에 포함됩니다.
소셜 네트워킹 메시지	소셜 네트워크, 데이트 웹사이트, 포럼 등에서 보낸 총 알림 메시지 수. 예를 들면 LinkedIn 및 CNET 포럼이 있습니다. 그레이메일 기능에서 이 정보를 결정합니다.
대량 메시지	미확인 마케팅 그룹(예: 기술 미디어 회사인 TechTarget)에서 보낸 총 광고 메시지 수. 그레이메일 기능에서 이 정보를 결정합니다.
그레이메일 메시지	그레이메일 기능에서 탐지한 마케팅 메시지, 소셜 네트워킹 메시지, 대량 메일이 포함됩니다. 그레이메일 기능이 활성화되지 않은 어플라이언스에서 식별한 마케팅 메시지는 그 합계가 마케팅 메시지 값에 포함되더라도 여기에 포함되지 않습니다. 메시지 추적을 사용하여 해당 범주에 속한 메시지 목록을 보려면 그레이메일 범주 중 하나에 해당하는 번호를 클릭합니다. 그레이메일 보고 , 104 페이지도 참조하십시오.
S/MIME 확인/암호 해독 성공	S/MIME을 사용하여 성공적으로 확인, 해독 또는 해독 및 확인된 총 메시지 수.
수락된 메시지 삭제	바이러스 및 스팸이 없는 것으로 확인되어 수락된 메일입니다. 수신자별 검사 작업을 고려하여 수락되는 정상 메시지(예: 별도의 메일 정책으로 처리되는 분할 메시지)를 가장 정확하게 나타냅니다. 그러나 스팸 또는 바이러스 양성으로 표시되지만 전달되는 메시지는 포함되지 않으므로 전달되는 실제 메시지 수는 정상 메시지 수와 다를 수 있습니다. 메시지 필터와 매치하며 필터에 의해 삭제되거나 반송되지 않은 메시지는 정상으로 간주됩니다. 메시지 필터에 의해 삭제 또는 반송된 메시지는 합계에 포함되지 않습니다. 그레이메일 기능이 활성화되지 않은 어플라이언스에서 처리된 메시지는 정상으로 분류됩니다.
총 시도 메시지	스팸, 마케팅 메시지(그레이메일 기능에서 발견했거나 안티스팸 기능의 마케팅 이메일 검사 기능에서 발견한 것), 소셜 네트워킹 메시지, 대량 메일, 정상 메시지가 포함됩니다.

참고 검사할 수 없는 메시지 또는 암호화된 메시지를 전달하도록 안티바이러스 설정을 구성한 경우 이러한 메시지는 바이러스 양성이 아닌 정상 메시지로 계산됩니다. 그렇지 않은 경우 메시지는 바이러스 양성으로 계산됩니다. 또한 메시지 필터와 매치하며 필터에 의해 삭제되거나 반송되지 않은 메시지는 정상으로 간주됩니다. 메시지 필터에 의해 삭제 또는 반송된 메시지는 합계에 포함되지 않습니다.

Incoming Mail(수신 메일) 페이지

Security Management Appliance의 **Email(이메일) > Reporting(보고) > Incoming Mail(수신 메일)** 페이지는 관리되는 Security Management Appliance에 연결된 모든 원격 호스트의 실시간 정보에 대한 인터랙티브 보고를 제공합니다. IP 주소, 도메인, 시스템에 메일을 전송하는 네트워크 소유자(조직)에 대한 정보를 수집할 수 있습니다. 또한 메일을 보낸 IP 주소, 도메인 또는 조직에 대해 발신자 프로필 검색을 수행할 수 있습니다.

수신 메일 세부사항 인터랙티브 테이블에서는 특정 IP 주소, 도메인, 네트워크 소유자(조직)에 대한 세부 정보를 표시합니다. 임의의 IP 주소, 도메인, 네트워크 소유자에 대한 발신자 프로필 페이지는 **Incoming Mail(수신 메일)** 페이지 또는 다른 발신자 프로필 페이지의 맨 위에 있는 해당 링크를 클릭하여 액세스할 수 있습니다.

Incoming Mail(수신 메일) 페이지에서 다음을 할 수 있습니다.

- Security Management Appliance로 메일을 보낸 IP 주소, 도메인 또는 네트워크 소유자(조직)에 대한 검색 수행. 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.
- 특정 발신자 그룹 및 메일 플로우 정책 작업에 따라 연결을 모니터링할 발신자 그룹 보고서 보기. 자세한 내용은 발신자 그룹 보고서 페이지, 82 페이지을 참조하십시오.
- 어플라이언스로 메일을 보낸 발신자에 대한 자세한 통계 보기. 통계에는 시도된 메시지 수를 발신자 평판 필터링, 안티스팸, 안티바이러스 등의 보안 서비스별로 구분한 내용이 포함됩니다.
- 안티스팸 또는 안티바이러스 보안 서비스에 의해 확인된 대용량 스팸 또는 바이러스 이메일을 보낸 발신자별로 정렬할 수 있습니다.
- SenderBase Reputation Service를 통해 특정 IP 주소, 도메인 및 조직 사이의 관계를 점검하여 발신자에 대한 더 많은 정보 얻기.
- SenderBase Reputation Service에서 발신자의 SBRS(SenderBase Reputation Score) 및 가장 최근에 도메인과 매치한 발신자 그룹 등 발신자에 대한 추가 정보를 얻습니다. 발신자를 발신자 그룹에 추가할 수 있습니다.
- 안티스팸 또는 안티바이러스 보안 서비스에 의해 확인된 대용량 스팸 또는 바이러스 이메일을 보낸 특정 발신자에 대해 자세히 알아보기.

수신 메일 페이지의 보기

Incoming Mail(수신 메일) 페이지에는 3가지 보기가 있습니다.

- IP 주소
- 도메인
- 네트워크 소유자

시스템에 연결된 원격 호스트를 해당 보기의 관점에서 조명합니다.

또한 수신 메일 페이지의 수신 메일 세부사항 섹션에서는 발신자 IP 주소, 도메인 이름, 네트워크 소유자 정보를 클릭하여 구체적인 발신자 프로필 정보를 얻을 수도 있습니다. 발신자 프로필에 대한 자세한 내용은 발신자 프로필 페이지, 80 페이지를 참조하십시오.

참고 *Network owners(*네트워크 소유자*)*는 도메인을 보유한 엔티티입니다. *Domains(*도메인*)*은 IP 주소를 보유한 엔티티입니다.

선택한 보기에 따라 Incoming Mail Details(수신 메일 세부사항) 인터랙티브 테이블에는 Email Security Appliance에 구성된 모든 퍼블릭 리스너에 메일을 전송한 상위 IP 주소, 도메인 또는 네트워크 소유자가 표시됩니다. 어플라이언스로 가는 모든 메일의 플로우를 모니터링할 수 있습니다.

Sender Profile(발신자 프로필) 페이지에서 발신자에 대한 세부사항에 액세스하려면 IP 주소, 도메인 또는 네트워크 소유자를 클릭합니다. 발신자 프로필 페이지는 특정 IP 주소, 도메인, 네트워크 소유자에 한정된 수신 메일 페이지입니다.

발신자 그룹별로 메일 플로우 정보에 액세스하려면 수신 메일 페이지의 맨 아래에서 **Sender Groups Report(**발신자 그룹 보고서**)** 링크를 클릭합니다. 발신자 프로필 페이지, 80 페이지를 참조하십시오.

일부 보고서 페이지는 여러 고유 하위 보고서를 포함하는데, 이는 최상위 페이지에서 액세스할 수 있습니다. 예를 들어 Security Management Appliance의 Incoming Mail report(수신 메일 보고서) 페이지에서는 개별 IP 주소, 도메인 및 네트워크 소유자에 대한 정보를 볼 수 있습니다. 이들은 각각 Incoming Mail report(수신 메일 보고서) 페이지에서 액세스할 수 있는 하위 페이지입니다.

페이지 오른쪽 위의 인쇄용 PDF 링크를 클릭하면 각 하위 보고서 페이지의 결과가 단일 통합 보고서에 생성됩니다. 여기서는 수신 메일 보고서 페이지입니다. 이메일 보고 페이지 이해, 67 페이지의 중요 내용을 참조하십시오.

Email(이메일**) > Reporting(**보고**) > Incoming Mail(**수신 메일**)** 페이지에서는 **IP Addresses(IP** 주소**)**, **Domains(**도메인**)**, **Network Owners(**네트워크 소유자**)** 보기를 제공합니다.

Incoming Mail Details(수신 메일 세부사항) 인터랙티브 테이블에 포함된 데이터에 대한 설명은 수신 메일 세부사항 테이블, 80 페이지 섹션을 참조하십시오.

Incoming Mail(수신 메일**)** 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지 섹션을 참조하십시오.

참고 수신 메일 보고서 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

"No Domain Information(도메인 정보 없음)" 링크

Security Management Appliance와 연결되어 있으며 이중 DNS 조회로 확인할 수 없는 도메인은 자동으로 특수 도메인인 "No Domain Information(도메인 정보 없음)"으로 그룹화됩니다. Sender Verification(발신자 확인)을 통해 이런 유형의 확인되지 않은 호스트를 관리하는 방법을 제어할 수 있습니다. Sender

Verification(발신자 확인)에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

Items Displayed(표시 항목) 메뉴를 사용하여 목록에 표시할 발신자 수를 선택할 수 있습니다.

메일 추세 그래프의 시간 범위

다양한 세부 수준을 선택하여 메일 그래프로 데이터를 표시할 수 있습니다. 동일한 데이터에 대해 일, 주, 월, 연도 보기를 선택할 수 있습니다. 데이터는 실시간으로 모니터링되므로, 데이터베이스에서 주기적으로 정보가 업데이트 및 요약됩니다.

시간 범위에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.

수신 메일 세부사항 테이블

Incoming Mail(수신 메일**)** 페이지 하단에 있는 Incoming Mail Details(수신 메일 세부사항) 인터랙티브 테이블에는 Email Security Appliance의 퍼블릭 리스너에 연결된 상위 발신자가 나열됩니다. 선택한 보기에 따라 도메인, IP 주소 또는 네트워크 소유자가 테이블에 표시됩니다. 데이터를 정렬하려면 열 머리글을 클릭합니다.

시스템은 이중 *DNS* 조회를 수행하여 원격 호스트 IP 주소의 유효성을 확보하고 확인합니다. 이중 DNS 조회 및 발신자 확인에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

발신자의 경우 수신 메일 세부사항 테이블의 첫 열에 나열된 네트워크 소유자, IP 주소 또는 도메인입니다. 또는 Top Senders by Total Threat Message(총 위협 메시지별 상위 발신자)에서는 **Sender(**발신자**)** 또는 **No Domain Information(**도메인 정보 없음**)** 링크를 클릭하여 발신자에 대한 추가 정보를 표시합니다. 그 결과는 **Sender Profile(**발신자 프로필**)** 페이지에 나타납니다. 여기에는 SenderBase Reputation Service의 실시간 정보도 포함되어 있습니다. 발신자 프로필 페이지에서 특정 IP 주소 또는 네트워크 소유자에 대한 추가 정보를 볼 수 있습니다. 자세한 내용은 발신자 프로필 페이지, 80 페이지을 참조하십시오.

수신 메일 페이지의 맨 아래에서 **Sender Groups report(**발신자 그룹 보고서**)**를 클릭하여 발신자 그룹 보고서를 표시할 수도 있습니다. 발신자 그룹 보고서 페이지에 대한 자세한 내용은 발신자 그룹 보고서 페이지, 82 페이지를 참조하십시오.

사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 콘텐츠 필터 위반에 대한 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

발신자 프로필 페이지

Mail Flow Details(메일 흐름 상세정보**)**[새로운 웹 인터페이스] 또는 **Incoming Mail(**수신 메일**)** 페이지의 Incoming Mail 인터랙티브 테이블에서 발신자를 클릭하면 Sender Profile(발신자 프로파일) 페이지가 나타납니다. 특정 IP 주소, 도메인, 네트워크 소유자(조직)에 대한 세부 정보를 표시합니다. 임의의 IP 주소, 도메인, 네트워크 소유자에 대한 발신자 프로필 페이지는 Mail Flow Details(메일 플로우 세부 정보) 페이지 또는 다른 발신자 프로필 페이지의 맨 위에 있는 해당 링크를 클릭하여 액세스할 수 있습니다.

*Network owners(*네트워크 소유자*)*는 도메인을 보유한 엔티티입니다. *Domains(*도메인*)*은 IP 주소를 보유한 엔티티입니다.

IP 주소, 네트워크 소유자, 도메인에 대해 표시되는 발신자 프로필 페이지는 약간 다릅니다. 각 페이지에는 해당 발신자가 보낸 수신 메일에 대한 그래프 및 요약 테이블이 포함됩니다. 그래프 아래의 테이블에는 발신자와 연결된 도메인 또는 IP 주소가 나열되어 있습니다. 개별 IP 주소에 대한 발신자 프로필 페이지는 더 세부적인 목록이 없습니다. 발신자 프로필 페이지에는 현재 SenderBase, 발신자 그룹, 네트워크 정보와 관련된 정보 섹션도 있습니다.

- 네트워크 소유자 프로필 페이지에는 네트워크 소유자는 물론 네트워크 소유자와 연결된 도메인 및 IP 주소에 대한 정보가 포함됩니다.
- 도메인 프로필 페이지에는 도메인 및 해당 도메인과 연결된 IP 주소에 대한 정보가 포함됩니다.
- IP 주소 프로필 페이지에는 IP 주소에 대한 정보만 포함되어 있습니다.

각 발신자 프로필 페이지의 하단에 있는 Current Information(현재 정보) 테이블에는 다음 데이터가 포함됩니다.

- SenderBase Reputation Service에서 제공하는 전역 정보:
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자
  - 네트워크 소유자 범주(네트워크 소유자만)
  - CIDR 범위(IP 주소만)
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자에 대한 일일 규모 및 월간 규모
  - 해당 발신자로부터 첫 메시지를 수신한 후 경과일
  - 마지막 발신자 그룹 및 DNS 확인 여부(IP 주소 발신자 프로필 페이지만)

  일일 규모는 지난 24시간 동안 도메인이 보낸 메시지 수 측정값입니다. 리히터 지진계가 지진을 측정하는 것과 마찬가지로 SenderBase 규모는 10을 기준으로 로그 스케일을 사용하여 계산된 메시지 볼륨 측정치입니다. 이론상 최대 스케일 값은 10으로 설정되며, 이는 세계 이메일 메시지 볼륨의 100%와 같습니다. 로그 스케일을 사용할 경우, 규모가 1 증가하는 것은 실제 볼륨이 10배 증가하는 것과 같습니다.

  월간 규모는 일일 규모와 동일한 접근법을 사용하여 계산되지만, 비율이 지난 30일 동안 전송된 이메일의 볼륨을 기반으로 계산된다는 점만 다릅니다.

  - 평균 규모(IP 주소만)
  - 수명 주기 볼륨/30일 볼륨(IP 주소 프로필 페이지만)
  - Bonded Sender 상태(IP 주소 프로필 페이지만)
  - SenderBase Reputation Score(IP 주소 프로필 페이지만)
  - 첫 메시지 이후 경과일(네트워크 소유자 및 도메인 프로필 페이지만)
  - 이 네트워크 소유자와 연결된 도메인의 수(네트워크 소유자 및 도메인 프로필 페이지만)
  - 이 네트워크 소유자의 IP 주소 수(네트워크 소유자 및 도메인 프로필 페이지만)
  - 이메일 전송에 사용된 IP 주소 수(네트워크 소유자 페이지만)

SenderBase Reputation Service에서 제공하는 모든 정보가 포함된 페이지를 보려면 **More from SenderBase(SenderBase**에서 더 보기**)**를 클릭합니다.

- 이 네트워크 소유자가 제어하는 도메인 및 IP 주소에 대한 세부사항은 네트워크 소유자 프로필 페이지에 표시됩니다. 도메인의 IP 주소에 대한 세부사항은 도메인 페이지에 표시됩니다.

도메인 프로필 페이지에서 특정 IP 주소를 클릭하여 특정 정보를 보거나 조직 프로필 페이지를 볼 수 있습니다.

발신자 그룹 보고서 페이지

Sender Groups(발신자 그룹**)** 보고서 페이지는 발신자 그룹 및 메일 플로우 정책 작업별로 연결 요약을 제공하므로, SMTP 연결 및 메일 플로우 정책 추세를 검토할 수 있습니다. Mail Flow by Sender Group(발신자 그룹별 메일 플로우) 목록은 각 발신자 그룹에 대한 연결 비율과 수를 보여줍니다. Connections by Mail Flow Policy Action(메일 플로우 정책 작업별 연결) 차트는 각 메일 플로우 정책 작업에 대한 연결의 비율을 보여줍니다. 이 페이지는 HAT(Host Access Table) 정책 효과의 개요를 제공합니다. HAT에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

Sender Groups report(발신자 그룹 보고서) 페이지를 보려면 **Email(**이메일**) > Reporting(**보고**) > Sender Groups(**발신자 그룹**)**를 선택합니다.

Sender Groups(발신자 그룹**)** 보고서 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.

참고 발신자 그룹 보고서 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Sender Domain Reputation(발신인 도메인 평판) 페이지

Sender Domain Reputation(발신자 도메인 평판 보고서) 페이지를 사용하여 다음을 볼 수 있습니다.

- SDR 서비스에서 받은 판정에 기반한 수신 메시지를 그래픽 형식으로 봅니다.
- SDR 서비스에서 받은 위협 카테고리 및 판정에 기반한 수신 메시지를 표 형식으로 봅니다.
- SDR 서비스에서 받은 위협 카테고리에 기반한 수신 메시지를 그래픽 형식으로 봅니다.

참고 SDR 판정이 '매우 나쁨' 또는 '나쁨'인 메시지만 '스팸', '악성' 등과 같은 SDR 위협 카테고리에 따라 분류됩니다.

- SDR 서비스에서 받은 위협 카테고리에 기반한 수신 메시지를 표 형식으로 봅니다.

SDR 섹션에서 처리된 수신 메시지의 요약에서는, 특정 판정에 해당하는 메시지의 수를 클릭하여 메시지 추적의 관련 메시지를 볼 수 있습니다.

Outgoing Destinations(발신 대상) 페이지

Email(이메일) > Reporting(보고) > Outgoing Destinations(발신 대상) 페이지는 여기서 보내는 메일의 도메인에 대한 정보를 제공합니다.

다음 유형의 질문에 답하려면 Outgoing Destinations(발신 대상) 페이지를 사용합니다.

- Email Security Appliance가 어떤 도메인으로 메일을 전송합니까?
- 각 도메인으로 얼마나 많은 메일이 전송됩니까?
- 이 메일 중에 콘텐츠 필터에 의해 중단된 메일, 악성코드, 바이러스 양성, 스팸 양성 또는 정상 메일은 얼마나 됩니까?
- 전달된 메시지는 몇 개이며 목적지 서버에 의해 하드 반송된 메시지는 몇 개입니까?

다음 목록은 **Outgoing Destinations(발신 대상)** 페이지의 여러 섹션을 설명합니다.

표 ***21: Email Reporting Outgoing Destinations(이메일 보고 발신 대상)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
총 위협 메시지별 상위 목적지	이 조직에서 보낸 발신 위협 메시지(스팸, 안티바이러스 등)의 상위 목적지 도메인. 총 위협에는 스팸 또는 바이러스 양성이거나 콘텐츠 필터를 트리거한 메시지가 포함됩니다.
정상 메시지별 상위 목적지	이 조직에서 보낸 발신 정상 메시지의 상위 목적지 도메인.
발신 목적지 세부사항	이 조직에서 보낸 모든 발신 메시지의 목적지 도메인 관련 세부사항을 총 수신자 기준으로 정렬한 것. 탐지된 스팸, 바이러스, 정상 메시지 등이 포함됩니다. 사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 콘텐츠 필터 위반에 대한 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

Outgoing Destinations(발신 대상) 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.

참고 발신 목적지 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

발신자 페이지

Email(이메일**) > Reporting(**보고**) > Outgoing Senders(**발신자**)** 페이지는 네트워크의 IP 주소 및 도메인에서 전송되는 메일의 양과 유형에 대한 정보를 제공합니다.

다음 유형의 질문에 답하는 데 발신자 페이지를 사용할 수 있습니다.

- 대부분의 바이러스 양성 또는 스팸 양성 또는 악성코드 이메일을 전송하는 IP 주소는 무엇입니까?
- 가장 자주 콘텐츠 필터를 트리거하는 IP 주소는 무엇입니까?
- 대부분의 메일을 전송하는 도메인은 무엇입니까?
- 전달을 시도했을 때 처리 중인 수신자는 총 몇 명입니까?

Outgoing Sender(발신자**)** 페이지를 보려면 다음을 수행합니다.

발신자 결과는 2가지 유형의 보기로 확인할 수 있습니다.

- **Domain(**도메인**)**: 각 도메인에서 보내는 메일의 볼륨을 볼 수 있습니다.
- **IP address(IP** 주소**)**: 어떤 IP 주소에서 가장 많은 바이러스 메시지를 보내거나 콘텐츠 필터를 실행하는지 볼 수 있습니다.

다음 목록은 **Outgoing Senders(**발신자**)** 페이지의 두 보기를 구성하는 여러 섹션을 설명합니다.

표 ***22: Email Reporting Outgoing Sender(***이메일 보고 발신자***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
총 위협 메시지별 상위 발신자	이 조직에서 보낸 발신 위협 메시지(스팸, 안티바이러스 등)의 상위 발신자(IP 주소 또는 도메인 기준).
정상 메시지별 상위 발신자	이 조직에서 보낸 정상 발신 메시지의 상위 발신자(IP 주소 또는 도메인 기준).
발신자 세부사항	이 조직에서 보낸 모든 발신 메시지의 발신자 세부사항(IP 주소 또는 도메인 기준). 탐지된 스팸, 바이러스, 정상 메시지 등이 포함됩니다. 사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 DLP 및 콘텐츠 필터 위반에 대한 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

참고 이 페이지에는 메시지 전달에 대한 정보가 표시되지 않습니다. 특정 도메인에서 반송된 메시지 수와 같은 전달 정보를 추적하려면 해당 Email Security Appliance에 로그인하고 **Monitor(**모니터**) > Delivery Status(**전달 상태**)**를 선택합니다.

Outgoing Senders(발신자**)** 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.

참고 **Outgoing Senders(**발신자**)**에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Internal Users(내부 사용자) 페이지

Email(이메일**) > Reporting(**보고**) > Internal Users(**내부 사용자**)** 페이지는 내부 사용자가 보내고 받는 메일에 대한 정보를 이메일 주소별로 제공합니다. 단일 사용자가 여러 개의 이메일 주소를 가질 수 있습니다. 이메일 주소는 보고서에서 결합되지 않습니다.

내부 사용자 인터랙티브 보고서를 사용하면 다음과 같은 종류의 질문에 답할 수 있습니다.

- 외부 이메일을 가장 많이 보내는 사람은?
- 정상 이메일을 가장 많이 받는 사람은?
- 그레이메일 메시지를 가장 많이 받는 사람은?
- 스팸을 가장 많이 받는 사람은?
- 누가 어떤 콘텐츠 필터를 트리거하나?
- 누구의 이메일이 콘텐츠 필터에서 가장 많이 포착되는가?

표 ***23: Email Reporting Internal Users(***이메일 보고 내부 사용자***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
정상 수신 메시지별 상위 사용자	이 조직에서 보낸 정상 수신 메시지의 상위 사용자(IP 주소 또는 도메인 기준).
정상 발신 메시지별 상위 사용자	이 조직에서 보낸 정상 발신 메시지의 상위 사용자(IP 주소 또는 도메인 기준).
사용자 메일 흐름 정보	사용자 메일 흐름 세부사항 인터랙티브 섹션은 각 메일 주소에서 보내고 받는 메일을 분류합니다. 열 제목을 클릭하여 목록을 정렬할 수 있습니다. 어떤 사용자의 세부사항을 보려면 내부 사용자 열에서 이름을 클릭합니다. 자세한 내용은 내부 사용자 세부사항 페이지, 86 페이지을 참조하십시오. 사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 콘텐츠 필터 위반에 대한 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

Internal Users(내부 사용자**)** 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.

참고 내부 사용자 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

내부 사용자 세부사항 페이지

Internal User detail(내부 사용자 세부 정보) 페이지는 각 카테고리(스팸 탐지됨, 바이러스 탐지됨, Advanced Malware Protection에 의해 탐지됨, 콘텐츠 필터에 의해 중단됨 등)의 메시지 수를 보여주는 수신 및 발신 메시지 분류를 포함하여, 사용자에 대한 자세한 정보를 보여줍니다. 수신 및 발신 콘텐츠 필터 매치도 표시됩니다.

Inbound Internal Users(인바운드 내부 사용자)란 Rcpt To: 주소를 기반으로 이메일을 수신한 사용자입니다. Outbound Internal Users(아웃바운드 내부 사용자)는 Mail From: 주소를 기반으로 하며 내부 네트워크의 발신자가 전송하는 이메일 유형을 추적할 때 유용합니다.

해당 콘텐츠 필터 정보 페이지에서 해당 필터에 대한 자세한 정보를 보려면 콘텐츠 필터 이름을 클릭합니다(Content Filters(콘텐츠 필터) 페이지, 89 페이지 참조). 특정 콘텐츠 필터와 일치한 메일을 보내거나 받은 사용자 목록을 표시하려면 이 방법을 사용할 수 있습니다.

참고 일부 아웃바운드 메일(예: 반송)에는 null 발신자가 있습니다. 이러한 메일은 아웃바운드 "unknown(알 수 없음)"으로 계산됩니다.

특정 내부 사용자 검색

User Mail Summary(사용자 메일 요약) 페이지 및 User Mail Flow Details(사용자 메일 플로우 세부 정보) 페이지 하단에 있는 검색 양식에서 특정 내부 사용자(이메일 주소)를 검색할 수 있습니다. 검색 텍스트와 정확한 매치를 찾을지 아니면 입력한 텍스트로 시작하는 항목을 찾을지(예: "ex"로 시작하면 "example.com"이 검색됨) 선택합니다.

DLP Incidents(DLP 인시던트)

Email(이메일) > Reporting(보고) > DLP Incidents (DLP Incident Summary)(DLP 인시던트 - DLP 인시던트 요약) 페이지는 발신 메일에서 발생하는 DLP(data loss prevention) 정책 위반에 대한 정보를 보여줍니다. Email Security Appliance는 사용자가 전송한 민감한 데이터를 탐지하기 위해 Outgoing Mail Policies(발신 메일 정책) 테이블에서 활성화된 DLP 이메일 정책을 사용합니다. DLP 정책을 위반하는 모든 발신 메시지는 인시던트로 보고됩니다.

DLP 인시던트 요약 보고서를 사용하면 다음과 같은 종류의 질문에 답할 수 있습니다.

- 사용자들이 어떤 유형의 민감한 데이터를 전송합니까?
- 이러한 DLP 인시던트가 얼마나 심각합니까?
- 이러한 메시지 중 몇 개가 전달되었습니까?
- 이러한 메시지 중 몇 개가 삭제되었습니까?
- 누가 이러한 메시지를 전송합니까?

DLP Incident 요약 페이지는 크게 2개 섹션으로 구성됩니다.

- 심각도(Low, Medium, High, Critical) 및 정책 매치 기준으로 상위 DLP 인시던트를 요약한 DLP 인시던트 추세 그래프
- DLP 인시던트 세부사항 목록

표 ***24: Email Reporting DLP Incident Summary(***이메일 보고 ***DLP*** 인시던트 요약***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
심각도별 상위 인시던트	심각도 기준 상위 DLP 인시던트입니다.
인시던트 요약	각 이메일 어플라이언스의 발신 메일 정책에 대해 현재 활성화된 DLP 정책은 **DLP Incident Summary(DLP** 인시던트 요약**)** 페이지 맨 아래의 DLP 인시던트 세부사항 인터랙티브 테이블에 나열됩니다. 자세한 정보를 표시하려면 DLP 정책의 이름을 클릭합니다.
상위 DLP 정책 매치	매치한 상위 DLP 정책.
DLP 인시던트 세부사항	DLP Incident Details(DLP 인시던트 세부사항) 테이블에는 심각도 레벨로 구분된 정책당 총 DLP 인시던트 수와 일반 텍스트로 전달되거나 암호화되어 전달되거나 삭제된 메시지의 수가 표시됩니다. DLP 인시던트 세부사항 테이블에 대한 자세한 내용은 DLP 인시던트 세부사항 테이블, 87 페이지를 참조하십시오.

정책에 의해 탐지된 DLP 인시던트에 대한 자세한 정보를 보려면 DLP 정책의 이름을 클릭합니다. 정책에서 탐지한 민감한 데이터가 포함된 메일을 전송한 사용자 목록을 표시하려면 이 방법을 사용할 수 있습니다.

DLP 인시던트 세부사항 테이블

DLP Incident Details(DLP 인시던트 세부사항) 테이블에는 심각도 레벨로 구분된 정책당 총 DLP 인시던트 수와 일반 텍스트로 전달되거나 암호화되어 전달되거나 삭제된 메시지의 수가 표시됩니다. 데이터를 정렬하려면 열 머리글을 클릭합니다.

이 테이블에 있는 DLP 정책에 대한 추가 정보를 보려면 DLP 정책의 이름을 클릭하면 DLP 정책 페이지가 나타납니다. 자세한 내용은 DLP 정책 세부사항 페이지, 87 페이지를 참조하십시오.

사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

DLP 정책 세부사항 페이지

DLP Incident Details(DLP 인시던트 세부사항) 테이블에서 DLP 정책의 이름을 클릭하면 DLP Policy Detail(DLP 정책 세부사항) 페이지에 정책에 대한 DLP 세부사항 데이터가 표시됩니다. 이 페이지는 심각도를 기반으로 DLP 인시던트에 대한 그래프를 표시합니다.

또한 DLP 정책을 위반한 메시지를 전송한 각 내부 사용자가 나열된 Incidents by Sender(발신자별 인시던트) 테이블이 페이지 하단에 포함되어 있습니다. 이 목록에는 또한 심각도 레벨로 구분된 정책의 사용자당 총 DLP 인시던트 수와 메시지가 일반 텍스트로 전달되었는지, 암호화되어 전달되었는지 또는 삭제되었는지가 표시됩니다. 어떤 사용자가 조직의 민감한 데이터를 네트워크 외부의 사람들에게 전송하는지를 알아내려면 Incidents by Sender(발신자별 인시던트) 테이블을 사용할 수 있습니다.

발신자 이름을 클릭하면 Internal Users(내부 사용자) 페이지가 열립니다. 자세한 내용은 Internal Users(내부 사용자) 페이지, 85 페이지를 참조하십시오.

메시지 필터

Message Filters(메시지 필터) 페이지는 수신 및 발신 메시지에 대한 상위 메시지 필터 매칭 결과(매칭하는 메시지 수가 가장 많은 메시지 필터)를 보여줍니다.

지리적 분포

Geo Distribution(지리적 분포) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 그래픽 형식의 발신지 국가별 상위 수신 메일 연결입니다.
- 표 형식의 발신지 국가별 상위 수신 메일 연결입니다.

다음은 상위 및 총 수신 메일 연결에 대해 국가 정보가 표시되지 않는 시나리오입니다.

- 발신자 IP 주소는 프라이빗 IP 주소에 속합니다.
- 발신자 IP 주소는 유효한 SBRS를 얻을 수 없습니다.

대량 메일

이 페이지의 보고서로 다음을 수행할 수 있습니다.

- 가변적인 1시간 동안 단일 발신자가 보낸 또는 동일한 제목으로 된 최다 메시지 수의 공격을 확인합니다.
- 상위 도메인을 모니터링하여 해당 공격이 자체 도메인에서 발생하지 않았음을 확인합니다. 자체 도메인에서 발생했다면 하나 이상의 계정이 감염되었을 가능성이 있습니다.
- 오탐지를 확인하여 필터를 조정할 수 있습니다.

이 페이지의 보고서는 헤더 반복 규칙을 사용하고 이 규칙에서 설정한 메시지 수 임계값을 통과한 메시지 필터의 데이터만 표시합니다. 다른 규칙과 연계할 경우 헤더 반복 규칙이 마지막으로 평가됩니다. 이전의 조건에서 메시지 특성이 확인된 경우 평가되지 않습니다. 또한 속도 제한에 걸린 메시지는 헤더 반복 메시지 필터에 오지 않습니다. 따라서 대량 메일로 간주되었을 메시지가 이 보고서에 포함되지 않을 수도 있습니다. 특정 메시지를 화이트리스트에 포함하도록 필터를 구성한 경우 그러한 메시지도 보고서에서 제외될 수 있습니다.

메시지 필터 및 Header Repeats(헤더 반복) 규칙에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서를 참조하십시오.

관련 주제

- Rate Limits(속도 제한) 페이지 , 102 페이지

Content Filters(콘텐츠 필터) 페이지

Email(이메일) > Reporting(보고) > Content Filters(콘텐츠 필터) 페이지는 상위 수신 및 발신 콘텐츠 필터 매칭 결과(매칭하는 메시지가 가장 많은 콘텐츠 필터)에 대한 정보를 제공합니다. 이 페이지에서는 데이터가 막대 차트 및 목록으로 표시됩니다. Content Filters(콘텐츠 필터) 페이지를 사용하면 콘텐츠 필터 또는 사용자 단위로 회사 정책을 검토하고 다음과 같은 유형의 질문에 답할 수 있습니다.

- 수신 또는 발신 메일에 의해 가장 많이 트리거되는 콘텐츠 필터는 무엇입니까?
- 특정 콘텐츠 필터를 트리거하는 메일을 보내거나 받는 상위 사용자는 누구입니까?

특정 필터에 대한 추가 정보를 보려면 해당 필터의 이름을 클릭합니다. 콘텐츠 필터 세부사항 페이지가 나타납니다. 콘텐츠 필터 세부사항 페이지에 대한 자세한 내용은 Content Filter Details(콘텐츠 필터 세부사항) 페이지, 89 페이지를 참조하십시오.

사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

Content Filters(콘텐츠 필터) 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.

참고 콘텐츠 필터 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Content Filter Details(콘텐츠 필터 세부사항) 페이지

Content Filter Detail(콘텐츠 필터 세부사항) 페이지에는 시간별 해당 필터에 대한 일치 및 내부 사용자별 일치가 표시됩니다.

Matches by Internal User(내부 사용자별 매치) 섹션에서 내부 사용자(이메일 주소)의 세부사항 페이지를 보려면 해당 사용자의 이름을 클릭합니다. 자세한 내용은 내부 사용자 세부사항 페이지, 86 페이지을(를) 참고하십시오.

사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

DMARC 확인

DMARC Verification(DMARC 검증) 페이지는 DMARC(Domain-based Message Authentication, Reporting and Conformance) 검증에 실패한 상위 발신자 도메인 및 그 도메인으로부터 수신한 메시지에 대해 수행한 조치의 요약을 표시합니다. 이 보고서를 사용하면 DMARC 설정을 세부적으로 조정하고 다음과 같은 종류의 질문에 답할 수 있습니다.

- DMARC 검증을 통과하지 못한 메시지가 가장 많은 도메인은 무엇입니까?
- 각 도메인에서, DMARC 확인에 실패한 메시지에 대해 수행된 작업은 무엇입니까?

DMARC 확인에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서의 이메일 인증 장을 참조하십시오.

매크로 탐지

Macro Detection(매크로 탐지) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 파일 형식별 상위 수신 매크로 사용 첨부 파일을 그래픽 형식과 표 형식으로 봅니다.
- 파일 형식별 상위 발신 매크로 사용 첨부 파일을 그래픽 형식과 표 형식으로 봅니다.

매크로 사용 첨부 파일의 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.

참고 보고서 생성 시:

- 아카이브 파일 내에서 하나 이상의 매크로가 탐지되면 아카이브 파일 파일 형식이 1씩 증가합니다. 아카이브 파일 내 매크로 사용 첨부 파일의 수는 계산되지 않습니다.
- 내장 파일 내에서 하나 이상의 매크로가 탐지되면 상위 파일 형식이 1씩 증가합니다. 내장 파일 내 매크로 사용 첨부 파일의 수는 계산되지 않습니다.

External Threat Feeds(외부 위협 피드) 페이지

External Threat Feeds(외부 위협 피드) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 메시지에서 위협을 탐지하는 데 사용되는 그래픽 형식의 상위 ETF 소스
- 메시지에서 위협을 탐지하는 데 사용되는 표 형식의 ETF 소스 요약
- 메시지에서 탐지된 위협과 일치하는 그래픽 형식의 상위 IOC
- 악의적인 수신 메일 연결을 필터링하는 데 사용되는 그래픽 형식의 상위 ETF 소스
- 악의적인 수신 메일 연결을 필터링하는 데 사용되는 표 형식의 ETF 소스 요약

'Summary of External Threat Feed Sources(외부 위협 피드 소스 요약)' 섹션에서 다음 작업을 수행할 수 있습니다.

- 특정 ETF 소스에 대한 메시지 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.
- 특정 위협 피드 소스를 클릭하여 IOC를 기준으로 ETF 소스의 배포를 볼 수 있습니다.

'Summary of Indicator of Compromise (IOC) Matches(IOC(Indicator of Compromise) 매치 요약)' 섹션에서 다음 작업을 수행할 수 있습니다.

- 특정 ETF 소스에 대한 IOC 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.

• 특정 IOC를 클릭하여 ETF 소스를 기준으로 IOC 배포를 볼 수 있습니다.

Virus Types(바이러스 유형) 페이지

Email(이메일) > Reporting(보고) > Virus Types(바이러스 유형) 페이지는 네트워크에 유입되고 네트워크에서 전송되는 바이러스의 개요를 제공합니다. Virus Types(바이러스 유형) 페이지는 Email Security Appliance에서 실행 중인 바이러스 검사 엔진에 의해 탐지되고 Security Management Appliance에 표시되는 바이러스를 보여줍니다. 특정 바이러스에 대해 작업을 수행하려면 이 보고서를 사용합니다. 예를 들어 PDF 파일에 포함된 것으로 알려진 대량의 바이러스를 수신하고 있다면 PDF 첨부 파일이 있는 메시지를 격리하는 필터 작업을 만들 수 있습니다.

참고 Outbreak Filter에서 사용자 개입 없이 이 바이러스 감염 메시지 유형을 격리할 수 있습니다.

여러 바이러스 검사 엔진을 실행 중인 경우 Virus Types(바이러스 유형) 페이지에는 활성화된 모든 바이러스 검사 엔진에서 온 결과가 포함됩니다. 페이지에 표시되는 바이러스의 이름은 바이러스 검사 엔진에서 확인한 이름입니다. 둘 이상의 검사 엔진에서 바이러스를 탐지하는 경우 동일한 바이러스에 대한 항목이 둘 이상 있을 수 있습니다.

표 ***25: Email Reporting Virus Types(***이메일 보고 바이러스 유형***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
탐지된 상위 수신 바이러스 유형	네트워크로 전송된 바이러스의 차트 보기를 표시합니다.
탐지된 상위 발신 바이러스 유형	네트워크에서 전송된 바이러스의 차트 보기를 표시합니다.
바이러스 유형 세부사항	각 바이러스 유형의 세부사항을 표시하는 인터랙티브 테이블입니다.

참고 어떤 호스트에서 바이러스에 감염된 메시지를 네트워크로 전송했는지를 보려면 Incoming Mail(수신 메일) 페이지로 이동하고, 동일한 보고 기간을 지정하고, 바이러스 양성으로 정렬합니다. 마찬가지로, 어떤 IP 주소가 네트워크 내에서 바이러스 양성 이메일을 전송했는지 알아보려면 Outgoing Senders(발신 발신자) 페이지로 이동하여 바이러스 양성 메시지로 정렬할 수 있습니다.

Virus Types(바이러스 유형) 페이지에서 PDF를 생성하거나 원시 데이터를 CSV 파일로 내보낼 수도 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 이메일 보고 페이지 이해, 67 페이지를 참조하십시오.

참고 **Virus Types(**바이러스 유형**)** 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

URL Filtering(URL 필터링) 페이지

- URL Filtering(URL 필터링) 보고서 모듈은 URL 필터링이 활성화된 경우에만 채워집니다.
- URL Filtering(URL 필터링) 보고서는 수신 및 발신 메시지에 대해 사용 가능합니다.
- URL 필터링 엔진으로 검사된(안티스팸/Outbreak Filter 검사의 일환으로 또는 메시지/콘텐츠 필터를 통해) 메시지만 이러한 모듈에 포함됩니다. 그러나 모든 결과가 URL 필터링 기능으로 인한 것이라 할 수는 없습니다.
- Top URL Categories(상위 URL 범주) 모듈은 검사된 메시지에서 발견된 모든 범주(콘텐츠 또는 메시지 필터와의 매치 여부와 상관없이)를 포함합니다.
- 각 메시지는 오로지 평판 레벨 하나와 연결할 수 있습니다. 여러 URL이 포함된 메시지의 경우 통계는 메시지에 있는 URL의 최하 평판을 반영합니다.
- Security Services(보안 서비스) > URL Filtering(URL 필터링)에 구성된 전역 화이트리스트의 URL은 보고서에 포함되지 않습니다.

  개별 필터에서 사용되는 화이트리스트의 URL은 보고서에 포함됩니다.
- 악성 URL은 Outbreak Filter가 평판이 좋지 않다고 판단한 URL입니다. 일반 URL은 Outbreak Filter에서 클릭 시 보호가 필요하다고 결정한 URL입니다. 따라서 일반 URL은 Cisco Web Security 프록시로 리디렉션하도록 재작성되었습니다.
- URL 범주 기반 필터의 결과는 콘텐츠 및 메시지 필터 보고서에서 반영됩니다.
- Cisco Web Security 프록시에 의한 클릭 시 URL 평가의 결과는 보고서에 반영되지 않습니다.

Web Interaction Tracking(웹 상호 작용 추적) 페이지

- Web Interaction Tracking(웹 상호 작용 추적) 보고서 모듈은 관리 Email Security Appliance에서 웹 인터랙티브 추적 기능이 활성화된 경우에만 채워집니다.
- Web Interaction Tracking(웹 상호 작용 추적) 보고서는 수신 및 발신 메시지에 대해 사용 가능합니다.
- 최종 사용자가 클릭하여 재작성된 URL만(정책에 의해서든 Outbreak Filter에 의해서든) 이러한 모듈에 포함됩니다.
- Web Interaction Tracking(웹 상호 작용 추적) 페이지에는 다음과 같은 보고서가 포함되어 있습니다.

  Top Rewritten Malicious URLs clicked by End Users(최종 사용자가 클릭한 재작성된 악의적인 상위 **URL)**. 다음 정보가 포함된 자세한 보고서를 보려면 URL을 클릭합니다.

  - 재작성된 악의적인 URL을 클릭한 최종 사용자 목록.
  - URL을 클릭한 날짜 및 시간.
  - URL이 정책 또는 Outbreak Filter에 의해 재작성되었는지 여부.

- 재작성된 URL을 클릭했을 때 수행된 작업(허용, 차단 또는 알 수 없음). URL이 Outbreak Filter에 의해 재작성되었거나 최종 판정을 사용할 수 없는 경우 상태는 unknown(알 수 없음)으로 표시됩니다.

참고 기능 제한 때문에 모든 보안 침해 재작성 URL의 상태는 unknown(알 수 없음)으로 표시됩니다.

Top End Users who clicked on Rewritten Malicious URLs(재작성된 악의적인 **URL**을 클릭한 상위 최종 사용자**)**

Tracking Web Interaction(웹 상호 작용 추적**)** 세부 정보. 다음 정보가 포함됩니다.

- 모든 재작성된 URL(악의적인 URL 또는 악의적이지 않은 URL)의 목록. 자세한 보고서를 보려면 URL을 클릭합니다.
- 재작성된 URL을 클릭했을 때 수행된 작업(허용, 차단 또는 알 수 없음).

  최종 사용자가 클릭했을 때 URL(정상 또는 악성)의 판정을 알 수 없는 경우 상태는 unknown(알 수 없음)으로 표시됩니다. 이는 사용자가 클릭한 시점에 URL이 추가 정밀 조사 중이었거나 웹 서버가 다운되었거나 도달할 수 없는 상태였기 때문에 발생할 수 있습니다.

- 최종 사용자가 재작성된 URL에서 클릭한 횟수. 클릭된 URL을 포함하는 모든 메시지의 목록을 보려면 번호를 클릭합니다.

- 다음에 유의하십시오.
  - 악성 URL을 재작성한 후 메시지를 전달하고 다른 사용자(예: 관리자)에게 알리도록 콘텐츠 또는 메시지 필터를 구성한 경우, 알림을 받은 사용자가 재작성된 URL을 클릭하더라도 원래 수신자의 웹 상호 작용 추적 데이터가 증가합니다.
  - 재작성된 URL을 포함하는 격리된 메시지의 복사본을 웹 인터페이스를 통해 원래 수신자가 아닌 사용자(예: 관리자)에게 전송하는 경우, 이 사용자가 재작성된 URL을 클릭하더라도 원래 수신자의 웹 상호 작용 추적 데이터가 증가합니다.

Forged Email Detection(위조 이메일 탐지) 페이지

- Forged Email Detection(위조 이메일 탐지) 페이지에는 다음 보고서가 포함됩니다.
  - **Top Forged Email Detection(**상위 위조 이메일 탐지**)**. 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 사용자 상위 10명이 표시됩니다.
  - **Forged Email Detection(**위조 이메일 탐지**)** 세부 정보. 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 모든 사용자 목록과, 지정한 사용자에 대해 일치하는 메시지 수가 표시됩니다.

- Forged Email Detection(위조 이메일 탐지) 보고서는 Forged Email Detection(위조 이메일 탐지) 콘텐츠 필터 또는 forged-email-detection 메시지 필터를 사용하는 경우에만 채워집니다.

Advanced Malware Protection(파일 평판 및 파일 분석) 보고 페이지

파일 분석 보고서 요구 사항 정보

(클라우드 파일 분석) 관리 어플라이언스에서 파일 분석 서버와 연결할 수 있음을 확인

파일 분석 보고서 세부사항을 얻으려면 어플라이언스가 포트 443을 통해 파일 분석 서버에 연결할 수 있습니다. 자세한 내용은 방화벽 정보, 563 페이지를 참조하십시오.

Cisco Content Security Management Appliance가 인터넷에 직접 연결되지 않은 경우 이 트래픽용 프록시 서버를 구성합니다(업그레이드 및 업데이트 설정, 453 페이지 참조). 프록시를 사용하여 업그레이드와 서비스 업데이트를 가져오도록 어플라이언스를 이미 구성한 경우 기존 설정이 사용됩니다.

HTTPS 프록시를 사용할 경우 프록시가 트래픽을 해독해서는 안 됩니다. 파일 분석 서버와의 통신에는 pass-through 메커니즘을 사용합니다. 프록시 서버가 파일 분석 서버의 인증서를 신뢰해야 하지만 파일 분석 서버에 자신의 인증서를 제공할 필요는 없습니다.

(클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성

조직의 모든 콘텐츠 보안 어플라이언스가 Cisco Email Security Appliance 또는 Cisco Web Security Appliance에서 분석을 위해 전송한 파일에 대해 클라우드에서 파일 분석 결과 세부 정보를 볼 수 있게 하려면 모든 어플라이언스를 동일한 어플라이언스 그룹으로 묶어야 합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 파일 분석 섹션으로 스크롤합니다.

단계 **4** 관리 대상 어플라이언스가 다른 파일 분석 클라우드 서버에 지정된 경우 결과 세부사항을 표시할 서버를 선택합니다.

다른 클라우드 서버에서 처리하는 파일에 대해서는 결과 세부사항이 제공되지 않습니다.

단계 **5** 분석 그룹 ID를 입력합니다.

- 그룹 ID를 잘못 입력하거나 어떠한 이유로 인해 이를 변경해야 할 경우 Cisco TAC에서 케이스를 열어야 합니다.
- 이 변경사항은 즉시 적용되므로 커밋이 필요하지 않습니다.
- 이 값에 CCOID를 사용하는 것이 좋습니다.
- 이 값은 대/소문자를 구분합니다.
- 이 값은 분석을 위해 업로드된 파일에 대한 데이터를 공유하는 모든 어플라이언스에서 동일해야 합니다.
- 어플라이언스는 단 하나의 그룹에만 속할 수 있습니다.
- 언제든지 그룹에 머신을 추가할 수 있지만 한 번만 추가할 수 있습니다.

단계 **6** **Group Now**(지금 그룹화)를 클릭합니다.

단계 **7** 이 어플라이언스와 데이터를 공유할 각 Email Security Appliance에서 동일한 그룹을 구성합니다.

다음에 수행할 작업

관련 주제

클라우드에서 세부 파일 분석 결과를 볼 수 있는 파일은? , 99 페이지

(온프레미스 파일 분석) 파일 분석 계정 활성화

온프레미스 Cisco AMP Threat Grid 어플라이언스를 구축한 경우 Cisco Content Security Management Appliance에 대해 파일 분석 계정을 활성화해야 AMP Threat Grid 어플라이언스에서 제공하는 보고서 세부 정보를 볼 수 있습니다. 일반적으로 한 번만 하면 됩니다.

시작하기 전에

중대 레벨의 시스템 알림을 받아야 합니다.

단계 **1** 처음으로 Threat Grid 어플라이언스에서 파일 분석 보고서 세부사항에 액세스할 때 몇 분 기다리면 링크가 포함된 알림을 수신하게 됩니다.

이 링크를 받지 못한 경우 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Alerts**(알림)에서 **View Top Alerts**(상위 알림 보기)를 클릭합니다.

단계 **2** 알림 메시지에서 링크를 클릭합니다.

단계 **3** 관리 어플라이언스 계정을 활성화합니다.

추가 요구 사항

추가 요건은 다음에서 Security Management Appliance 릴리스용 릴리스 정보를 참조하십시오.
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

SHA-256 해시로 파일 식별

파일 이름을 쉽게 변경할 수 있으므로 어플라이언스가 보안 해시 알고리즘(SHA-256)을 사용하여 각 파일에 대해 식별자를 생성합니다. 어플라이언스가 이름이 다른 동일한 파일을 처리할 경우 모든 인스턴스가 동일한 SHA-256으로 인식됩니다. 여러 어플라이언스가 동일한 파일을 처리하는 경우 해당 파일의 모든 인스턴스에 동일한 SHA-256 식별자가 있습니다.

대부분의 보고서에서는 파일이 SHA-256 값(단축 형식)으로 나열됩니다.

파일 평판 및 파일 분석 보고서 페이지

보고서	설명
AMP(Advanced Malware Protection)	파일 평판 서비스에서 찾은 파일 기반 위협을 보여줍니다. 판정이 변경된 파일은 AMP 판정 업데이트 보고서를 참조하십시오. 그러한 판정은 Advanced Malware Protection 보고서에 적용되지 않습니다. 압축 또는 아카이브 파일에서 추출된 파일 중 하나가 악성인 경우 압축 또는 아카이브 파일의 SHA 값만 Advanced Malware Protection 보고서에 포함됩니다. 참고 AsyncOS 9.6.5부터는 Advanced Malware Protection 보고서가 향상되어 추가 필드, 그래프 등이 표시됩니다. 업그레이드 후에 표시되는 보고서에는 업그레이드 전의 보고 데이터가 포함되지 않습니다. 9.6.5 AsyncOS 업그레이드 전에 Advanced Malware Protection 보고서를 보려면 페이지의 맨 아래에서 하이퍼링크를 클릭합니다. **Incoming Malware Files by Category(**카테고리별 수신 악성코드 파일**)** 섹션에는 다음 내용이 표시됩니다. • 카테고리가 악성 코드로 지정된 AMP 평판 서버에서 수신한 블랙리스트에 있는 파일 SHA의 백분율입니다. • 카테고리가 **Custom Detection(**맞춤형 탐지**)**으로 지정된 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율이 표시됩니다. AMP for Endpoints Console에서 가져온 블랙리스트에 있는 파일의 위협 이름이 보고서의 Incoming Malware Threat Files(수신 악성코드 위협 파일) 섹션에서 **Simple Custom Detection(**단순 맞춤형 탐색**)**으로 표시됩니다. • 카테고리가 **Custom Threshold(**맞춤형 임계값**)**으로 지정된 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율이 표시됩니다. 보고서의 More Details(추가 세부 정보) 섹션에 있는 링크를 클릭하여 AMP for Endpoints Console에서 블랙리스트에 있는 파일 SHA의 파일 경로 분석 세부 정보를 볼 수 있습니다. 보고서의 AMP 섹션에서 수신 파일 전달에 낮은 위험 판정 세부 정보를 볼 수 있습니다.

보고서	설명
Advanced Malware Protection 파일 분석	분석을 위해 전송된 각 파일의 시간 및 판정(또는 임시 판정)을 표시합니다. 어플라이언스는 30분마다 분석 결과를 확인합니다. 1,000개가 넘는 파일 분석 결과를 보려면 데이터를 .csv 파일로 내보냅니다. 온프레미스 Cisco AMP Threat Grid 어플라이언스 구축: 화이트리스트에 나열된 파일은 "정상"으로 표시됩니다. 화이트리스트에 대한 내용은 AMP Threat Grid 설명서 또는 온라인 도움말을 참조하십시오. 각 파일의 위협 특성을 포함한 자세한 분석 결과를 보려면 드릴다운합니다. SHA에 대한 추가 정보를 검색하거나 파일 분석 세부사항 페이지 맨 아래의 링크를 클릭하여 파일을 분석한 서버에 대한 세부사항을 볼 수 있습니다. 파일을 분석한 서버의 세부사항을 보려면 파일 분석 보고서 요구 사항 정보 , 94 페이지를 참조하십시오. 압축 또는 아카이브 파일에서 추출된 파일이 분석을 위해 전송된 경우 이러한 추출된 파일의 SHA 값만 파일 분석 보고서에 포함됩니다. 참고 AsyncOS 9.6.5부터는 File Analysis(파일 분석) 보고서가 향상되어 추가 필드, 그래프 등이 표시됩니다. 업그레이드 후에 표시되는 보고서에는 업그레이드 전의 보고 데이터가 포함되지 않습니다. 9.6.5 AsyncOS 업그레이드 전에 File Analysis(파일 분석) 보고서를 보려면 페이지의 맨 아래에서 하이퍼링크를 클릭합니다.

보고서	설명
Advanced Malware Protection 판정 업데이트	Advanced Malware Protection는 표적 및 제로데이 위협에 중점을 두므로 집계된 데이터에서 추가 정보를 제공하면 위협 판정이 바뀔 수 있습니다. AMP Verdict Updates(AMP 판정 업데이트) 보고서에는 메시지 수신 이후 판정이 변경된 어플라이언스에 의해 처리된 파일이 나열됩니다. 자세한 내용은 Email Security Appliance용 문서를 참조하십시오. 1,000개가 넘는 판정 업데이트를 보려면 데이터를 .csv 파일로 내보냅니다. 단일 SHA-256에 대해 여러 판정이 변경된 경우 이 보고서에 판정 기록이 아닌 최신 판정만 표시됩니다. 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 특정 SHA-256의 영향을 받는 모든 메시지를 보려면 SHA-256 링크를 클릭합니다.

다른 보고서의 파일 평판 필터링 데이터 보기

파일 평판 및 분석 데이터는 관련이 있는 경우 다른 보고서에서도 볼 수 있습니다. "Advanced Malware Protection에 의해 탐지됨" 열이 해당 보고서에서 기본적으로 숨겨질 수 있습니다. 추가 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

클라우드에서 세부 파일 분석 결과를 볼 수 있는 파일은?

퍼블릭 클라우드 파일 분석을 구축한 경우 파일 분석을 위해 어플라이언스 그룹에 추가된 모든 관리 대상 어플라이언스에서 업로드된 모든 파일의 세부 결과를 볼 수 있습니다.

관리 어플라이언스를 그룹에 추가했다면 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)** 페이지에서 버튼을 클릭하여 그룹에 속한 관리 대상 어플라이언스의 목록을 볼 수 있습니다.

분석 그룹의 어플라이언스는 파일 분석 클라이언트 ID로 식별됩니다. 특정 어플라이언스의 파일 분석 클라이언트 ID를 보려면 다음 위치에서 찾으십시오.

어플라이언스	파일 분석 클라이언트 **ID**의 위치
Email Security Appliance	**Security Services(**보안 서비스**) > File Reputation and Analysis(**파일 평판 및 분석**)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Web Security Appliance	**Security Services(**보안 서비스**) > Anti-Malware and Reputation(**악성코드 차단 및 평판**)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션

어플라이언스	파일 분석 클라이언트 ID의 위치
Cisco Content Security Management Appliance	**Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 서비스) > **Security Appliances**(보안 어플라이언스) 페이지의 하단

관련 주제

- (클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성 , 94 페이지

사서함 자동 치료

Mailbox Auto Remediation(사서함 자동 치료) 보고서 페이지를 사용하여 사서함 치료 결과의 세부 정보를 볼 수 있습니다. 이 보고서를 사용하여 다음과 같은 세부 정보를 봅니다.

- 사서함 치료에 성공했거나 실패한 수신자 목록
- 메시지에 수행된 교정 조치
- SHA-256 해시와 관련된 파일 이름

Recipients for whom remediation was unsuccessful(교정에 실패한 수신자) 필드는 다음과 같은 시나리오에서 업데이트됩니다.

- 수신자가 유효한 Office 365 사용자가 아니거나 수신자가 어플라이언스에 구성된 Office 365 도메인 계정에 속하지 않습니다.
- 사서함에서 첨부 파일이 포함된 메시지를 더 이상 사용할 수 없습니다. 예를 들어, 엔드 유저가 메시지를 삭제했습니다.
- 어플라이언스에 구성된 교정 조치를 수행하려 했을 때 어플라이언스와 Office 365 서비스 간의 연결 문제가 있었습니다.

메시지 추적에서 관련된 메시지를 보려면 SHA-256 해시를 클릭합니다.

TLS Connections(TLS 연결) 페이지

Email(이메일) > **Reporting**(보고) > **TLS Connections**(TLS 연결) 페이지는 주고받은 메일에 대한 TLS 연결의 전체 사용량을 보여줍니다. 보고서에서는 또한 TLS 연결을 사용하여 메일을 전송하는 각 도메인에 대한 세부사항도 보여줍니다.

TLS Connections(TLS 연결) 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- 전반적으로 어떤 수신 및 발신 연결 부분에서 TLS를 사용합니까?
- 어떤 파트너와의 TLS 연결에 성공했습니까?
- 어떤 파트너와의 TLS 연결에 실패했습니까?
- 어떤 파트너가 TLS 인증서에 문제가 있습니까?
- 파트너별 TLS를 사용하는 전체 메일 비율은 어떻게 됩니까?

표 *26: Email Reporting TLS Connections(*이메일 보고 *TLS* 연결*)* 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
수신 TLS 연결 그래프	선택한 기간에 따라 지난 시간, 전날, 전주의 수신 TLS 암호화 및 비암호화 연결을 보여줍니다.
수신 TLS 연결 요약	총 메시지 볼륨, 암호화된/암호화되지 않은 메시지의 볼륨, 성공한/실패한 TLS 암호화 메시지 볼륨이 표시됩니다.
수신 TLS 메시지 요약	수신 메시지의 총 볼륨을 요약하여 표시합니다.
수신 TLS 연결 정보	암호화된 메시지를 보내거나 받는 도메인에 대한 세부사항이 테이블에 표시됩니다. 각 도메인에 대해 총연결 수, 전송한 메시지 수, 성공하거나 실패한 TLS 연결 수를 볼 수 있습니다. 각 도메인에서 성공한 연결 및 실패한 연결의 비율도 볼 수 있습니다.
발신 TLS 연결 그래프	선택한 기간에 따라 지난 시간, 전날, 전주의 수신 TLS 암호화 및 비암호화 연결을 보여줍니다.
발신 TLS 연결 요약	총 메시지 볼륨, 암호화된/암호화되지 않은 메시지의 볼륨, 성공한/실패한 TLS 암호화 메시지 볼륨이 표시됩니다.
발신 TLS 메시지 요약	발신 메시지의 총 볼륨을 요약하여 표시합니다.
발신 TLS 연결 정보	암호화된 메시지를 보내거나 받는 도메인에 대한 세부사항이 테이블에 표시됩니다. 각 도메인에 대해 총연결 수, 전송한 메시지 수, 성공하거나 실패한 TLS 연결 수, 마지막 TLS 상태를 볼 수 있습니다. 각 도메인에서 성공한 연결 및 실패한 연결의 비율도 볼 수 있습니다.

Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지

Inbound SMTP authentication(인바운드 SMTP 인증) 페이지는 클라이언트 인증서의 사용 및 ESA와 사용자 메일 클라이언트 간 SMTP 세션 인증을 위한 SMTP AUTH 명령을 보여줍니다. 어플라이언스는 인증서 및 SMTP AUTH 명령을 수락하는 경우 메일 클라이언트에 대한 TLS 연결을 설정합니다. 클라이언트는 메시지를 전송하는 데 이 연결을 사용합니다. 어플라이언스는 사용자 단위로 이러한 시도를 추적할 수 없으므로, 보고서는 도메인 이름 및 도메인 IP 주소를 기반으로 SMTP 인증에 대한 세부사항을 표시합니다.

이 보고서를 사용하면 다음 정보를 확인할 수 있습니다.

- 전체적으로 SMTP 인증을 사용하는 수신 연결은 몇 개입니까?
- 인증된 클라이언트를 사용하는 연결은 몇 개입니까?
- SMTP AUTH를 사용하는 연결은 몇 개입니까?
- SMTP 인증을 사용하려고 시도할 때 어떤 도메인이 연결에 실패합니까?

- SMTP 인증에 실패할 때 대안을 사용하여 성공한 연결은 몇 개입니까?

Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지에는 수신된 연결에 대한 그래프, SMTP 인증 연결을 시도한 메일 수신자에 대한 그래프, 그리고 연결 인증 시도에 대한 세부사항을 보여주는 테이블이 포함되어 있습니다.

Received Connections(수신된 연결) 그래프는 지정한 시간 범위 동안 SMTP 인증을 사용하여 연결을 인증하려고 시도한 메일 클라이언트로부터의 수신 연결을 보여줍니다. 이 그래프에는 어플라이언스가 수신한 총 연결 수, SMTP 인증을 사용하여 인증하려고 시도하지 않은 횟수, 클라이언트 인증서를 사용하여 연결을 인증하는 데 실패한/성공한 횟수, 그리고 SMTP AUTH 명령을 사용하여 인증하는 데 실패한/성공한 횟수가 표시됩니다.

Received Recipients(수신된 수신자) 그래프는 해당 메일 클라이언트가 SMTP 인증을 사용하여 메시지를 전송하기 위해 ESA에 대한 연결을 인증하려고 시도한 수신자 수를 보여줍니다. 또한 연결이 인증된 수신자 수 및 연결이 인증되지 않은 수신자 수도 보여줍니다.

SMTP Authentication details(SMTP 인증 세부사항 테이블)는 해당 사용자가 메시지를 전송하기 위해 ESA에 대한 연결을 인증하려고 시도한 도메인에 대한 세부사항을 표시합니다. 각 도메인에 대해 클라이언트 인증서를 사용하여 성공 또는 실패한 연결 시도 횟수, SMTP AUTH 명령을 사용하여 성공 또는 실패한 연결 시도 횟수, 그리고 클라이언트 인증서 연결 시도 실패 후 SMTP AUTH로 전환한 횟수를 볼 수 있습니다. 도메인 이름 또는 도메인 IP 주소로 이 정보를 표시하려면 페이지 상단에 있는 링크를 사용할 수 있습니다.

Rate Limits(속도 제한) 페이지

봉투 발신자에 의한 속도 제한 기능을 사용하면 mail-from 주소를 기반으로 개별 발신자의 시간 간격당 이메일 메시지 수신자의 수를 제한할 수 있습니다. Rate Limits(속도 제한) 보고서는 가장 눈에 띄게 이 제한을 초과한 발신자를 보여줍니다.

이 보고서를 사용하면 다음을 식별할 수 있습니다.

- 대량 스팸 발신에 사용되었을 수 있는 손상된 사용자 계정.
- 알림, 자동화된 발표 등에 이메일을 사용하는 조직의 제어 불가능한 애플리케이션.
- 내부 결제 또는 리소스 관리 목적으로 조직에서 이메일 활동이 과중한 소스.
- 달리 스팸으로 간주되지 않을 수 있는 대량 인바운드 이메일 트래픽의 소스.

Internal Users(내부 사용자) 또는 Outgoing Senders(외부 발신자) 등 내부 발신자에 대한 통계를 포함하는 기타 보고서는 전송된 메시지의 수만 측정합니다. 소수의 메시지를 다수의 수신자에게 보내는 발신자는 식별하지 않습니다.

Top Offenders by Incident(인시던트별 상위 위반자) 차트는 구성된 제한보다 더 많은 수신자에게 메시지를 보내려고 가장 자주 시도한 봉투 발신자를 보여줍니다. 각 시도가 하나의 인시던트입니다. 이 차트는 모든 리스너로부터 인시던트 수를 집계합니다.

Top Offenders by Rejected Recipients(거부된 수신자별 상위 위반자) 차트는 구성된 제한을 넘어 최대 수신자에게 메시지를 보낸 봉투 전송자를 보여줍니다. 이 차트는 모든 리스너로부터 수신자 수를 집계합니다.

"Rate Limit for Envelope Senders(봉투 발신자에 대한 속도 제한)" 설정을 비롯한 속도 제한 설정이 Email Security Appliance의 Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책)에 구성되

어 있습니다. 속도 제한에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

관련 주제

- 대량 메일 , 88 페이지

Outbreak Filters 페이지

Email(이메일) > Reporting(보고) > Outbreak Filters 페이지는 Outbreak Filters에서 격리한 최근 보안 침해 및 메시지에 대한 정보를 제공합니다. 이 페이지를 사용하면 대상이 지정된 바이러스, 스캠 및 피싱 공격에 대한 방어를 모니터링할 수 있습니다.

다음 유형의 질문에 답하는 데 Outbreak Filters 페이지를 사용할 수 있습니다.

- 어떤 Outbreak Filters 규칙에 의해 몇 개의 메시지가 격리되어 있습니까?
- Outbreak Filter 기능이 바이러스 전파 확산에 제공한 리드 타임은 얼마입니까?
- 로컬 보안 침해를 전역 보안 침해와 비교하면 어떻습니까?
- 메시지가 보안 침해 격리에 얼마나 머뭅니까?
- 어떤 잠재적 악성 URL이 가장 많이 나타납니까?

Threats By Type(유형별 위협) 섹션에는 어플라이언스에서 수신한 두 가지 유형의 위협 메시지가 표시됩니다. Threat Summary(위협 요약) 섹션에서는 바이러스, 피싱, 스캠별로 메시지를 구분합니다.

Past Year Outbreak Summary(지난해 Outbreak 요약)에는 지난해의 로컬 및 전역 전파 확산 정보가 나열되어 있으므로, 로컬 네트워크 추세를 전역 추세와 비교할 수 있습니다. 전역 전파 확산의 목록은 모든 전파 확산(바이러스 및 비 바이러스)의 상위 집합인 반면, 로컬 전파 확산은 어플라이언스에 영향을 미친 바이러스 전파 확산으로 제한됩니다. 로컬 전파 확산 데이터에는 비 바이러스 위협이 포함되어 있지 않습니다. 전역 전파 확산 데이터는 Outbreak 격리에 대해 현재 구성된 임계값을 초과한, Threat Operations Center에 의해 탐지된 모든 전파 확산을 나타냅니다. 로컬 전파 확산 데이터는 Outbreak 격리에 대해 현재 구성된 임계값을 초과한, 이 어플라이언스에서 탐지된 모든 바이러스 전파 확산을 나타냅니다. Total Local Protection Time(총 로컬 보호 시간)은 항상 Threat Operations Center에서 탐지된 각 바이러스 전파 확산과 주요 공급업체의 안티바이러스 서명 릴리스 사이의 차이를 기반으로 합니다. 모든 전역 전파 확산이 어플라이언스에 영향을 미치는 것은 아닙니다. 값 "--"는 보호 시간이 없음을 나타내거나, 안티바이러스 공급업체에서 사용 가능한 서명 시간이 없었음을 나타냅니다(일부 공급업체는 서명 시간을 보고하지 않을 수 있음). 보호 시간이 영(0)임을 나타낸다기보다는, 보호 시간 계산에 필요한 정보를 사용할 수 없음을 나타냅니다.

Outbreak Filter 격리가 요약되어 있는 Quarantined Messages(격리된 메시지) 섹션은 Outbreak Filter가 파악하는 잠재적 위협 메시지의 수를 측정하는 데 유용합니다. 격리된 메시지는 릴리스될 때 계산됩니다. 일반적으로 메시지는 안티바이러스 및 안티스팸 규칙을 사용할 수 있기 전에 격리됩니다. 메시지가 릴리스되면 안티바이러스 및 안티스팸 소프트웨어로 검사되고 양성 또는 깨끗한 메시지로 확인됩니다. Outbreak 추적의 동적 속성 때문에 메시지를 격리하는 규칙(및 관련 전파 확산)은 메시지가 격리에 있는 동안 변경될 수 있습니다. 릴리스될 때(격리에 들어갈 때보다) 메시지를 계산하면 숫자가 늘고 주는 데서 오는 혼동을 피할 수 있습니다.

Threat Details(위협 세부사항) 목록에는 위협 범주(바이러스, 스캠 또는 피싱), 위협 이름, 위협 설명, 식별된 메시지 수를 포함하여 특정 전파 확산에 대한 정보가 표시됩니다. 바이러스 전파 확산의 경우,

Past Year Virus Outbreaks(지난해 바이러스 Outbreaks)에는 Outbreak 이름과 ID, 바이러스 전파 확산이 처음 전역적으로 발견된 시간과 날짜, Outbreak Filter가 제공한 보안 시간 및 격리된 메시지의 수가 포함됩니다. 전역 또는 로컬 보안 침해를 표시하도록 선택할 수 있습니다.

First Seen Globally(처음 전역적으로 발견) 시간은 세계 최대 이메일 및 웹 트래픽 모니터링 네트워크인 SenderBase에서 제공하는 데이터를 기반으로 Threat Operations Center에 의해 결정됩니다. 보호 시간은 Threat Operations Center에서 탐지된 각 위협과 주요 공급업체의 안티바이러스 서명 릴리스 사이의 차이를 기반으로 합니다.

값 "--"는 보호 시간이 없음을 나타내거나, 안티바이러스 공급업체에서 사용 가능한 서명 시간이 없었음을 나타냅니다(일부 공급업체는 서명 시간을 보고하지 않을 수 있음). 보호 시간이 영(0)임을 나타내지는 않습니다. 오히려 보호 시간 계산에 필요한 정보를 사용할 수 없음을 나타냅니다.

이 페이지의 다른 모듈은 다음 항목을 제공합니다.

- 선택한 기간에 Outbreak Filter에서 처리한 수신 메시지 수.

바이러스 외 위협 - 피싱 이메일, 스캠, 외부 웹 사이트 링크를 사용한 악성코드 배포.

- Outbreak Filter에서 탐지한 위협의 심각도.

레벨 5는 심각하거나 영향이 있는 위협인 반면, 레벨 1은 낮은 위협을 나타냅니다. 위협 레벨에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서를 참조하십시오.

- 메시지가 보안 침해 격리에 머무는 시간.

시스템이 그 안정성에 대한 판정을 내리기 위해 잠재적 위협에 대한 충분한 데이터를 수집할 때까지 걸리는 시간으로 결정됩니다. 바이러스 위협 메시지는 격리 시간이 더 긴 편입니다. 안티바이러스 프로그램 업데이트를 기다려야 하기 때문입니다. 각 메일 정책에 대해 지정한 최대 보존 시간도 반영됩니다.

- 수신자가 잠재적 악성 링크를 클릭할 경우 클릭 시간 평가를 위해 메시지 수신자를 Cisco Web Security Proxy로 리디렉션하고자 자주 재작성되는 URL .

이 목록은 악성이 아닌 URL을 포함할 수도 있습니다. 메시지의 어떤 URL이 악성으로 간주되면 모든 URL이 재작성되기 때문입니다.

참고 Outbreak Filters 보고서 페이지의 테이블을 정확하게 작성하려면 어플라이언스에서 에 지정된 Cisco 업데이트 서버와 통신할 수 있어야 합니다. Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Update Settings(업데이트 설정)

자세한 내용은 의 보안 침해 필터 장을 참조하십시오.

그레이메일 보고

그레이메일 통계는 다음 보고서에 반영됩니다.

보고서	다음 그레이메일 데이터 포함
Mail Flow Summary(메일 플로우 요약) 페이지 > Incoming(수신) 탭	각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.
Mail Flow Details(메일 플로우 세부 정보) 페이지 > Outgoing Senders(발신 발신자) 탭	상위 그레이메일 발신자.
Mail Flow Details(메일 플로우 세부 정보) 페이지 > Incoming Mails(수신 메일) 탭	모든 IP 주소, 도메인 이름 또는 네트워크 소유자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.
User Mail Summary(사용자 메일 요약) 페이지 > Top Users by Graymail(그레이메일별 상위 사용자)	그레이메일을 수신하는 상위 최종 사용자.
User Mail Summary(사용자 메일 요약) 페이지 > User Mail Details(사용자 메일 세부 정보)	모든 사용자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.

관련 주제

• AsyncOS 9.5 업그레이드 후 마케팅 메시지 보고 , 105 페이지

AsyncOS 9.5 업그레이드 후 마케팅 메시지 보고

AsyncOS 9.5로 업그레이드하면

- 마케팅 메시지 수는 업그레이드 전후에 탐지된 마케팅 메시지의 합계입니다.
- 총 그레이메일 메시지 수에는 업그레이드 이전에 탐지된 마케팅 메시지의 수가 포함되지 않습니다.
- 총 시도된 메시지 수에는 또한 업그레이드 전에 탐지된 마케팅 메시지의 수가 포함됩니다.
- 관리 Email Security Appliance에서 그레이메일 기능이 활성화되지 않은 경우 마케팅 메시지는 정상 메시지로 간주됩니다.

System Capacity(시스템 용량) 페이지

Email(이메일) > Reporting(보고) > System Capacity(시스템 용량) 페이지는 작업 대기열에 있는 메시지, 수신/발신 메시지(볼륨, 크기 및 수), 전체 CPU 사용량, 기능별 CPU 사용량, 메모리 페이지 스와핑 정보 등 시스템 로드에 대한 자세한 내용을 제공합니다.

System Capacity(시스템 용량) 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- Email Security Appliance가 권장 용량을 초과하는 시기를 식별합니다. 이를 통해 구성 최적화 또는 추가 어플라이언스가 필요한 시기를 결정할 수 있습니다.

- 앞으로의 용량 문제를 보여주는 시스템 동작의 기록 추세를 식별합니다.
- 문제 해결을 위해, 시스템의 어떤 부분이 가장 많은 리소스를 사용하는지를 식별합니다.

용량이 메시지 볼륨에 적절한지 확인하려면 Email Security Appliance를 모니터링해야 합니다. 시간이 지나면 볼륨이 불가피하게 증가하므로, 적절한 모니터링을 통해 추가 용량 또는 구성 변경을 사전에 적용해야 합니다. 시스템 용량을 모니터링하는 가장 효과적인 방법은 전체적인 볼륨, 작업 대기열의 메시지 수 및 리소스 절약 모드의 인시던트 수를 추적하는 것입니다.

- **Volume(볼륨):** 현재 환경에서 "정상" 메시지 볼륨 및 "일상적인" 급증을 이해하는 것이 중요합니다. 시간의 경과에 따라 이 데이터를 추적하여 볼륨 증가를 측정하십시오. 시간의 경과에 따른 볼륨을 추적하려면 Incoming Mail(수신 메일) 및 Outgoing Mail(발신 메일) 페이지를 사용할 수 있습니다. 자세한 내용은 시스템 용량 - 수신 메일, 107 페이지 및 시스템 용량 - 발신 메일, 107 페이지를 참조하십시오.
- **Work Queue(작업 대기열):** 작업 대기열은 스팸 공격을 흡수 및 필터링하고 비 스팸 메시지의 증가를 처리하는 "충격 흡수자" 역할을 하도록 설계되었습니다. 그러나 작업 대기열도 부하 상태의 시스템을 나타내는 지표가 될 수 있습니다. 작업 대기열 백업을 길게 자주 수행할 경우 용량 문제가 발생할 수 있습니다. System Capacity - Workqueue(시스템 용량 - 작업 대기열) 페이지에서 작업 대기열의 활동을 추적할 수 있습니다. 자세한 내용은 시스템 용량 - 작업 대기열, 106 페이지을(를) 참고하십시오.
- **Resource Conservation Mode(리소스 절약 모드):** 어플라이언스는 과부하 상태가 되면 RCM(Resource Conservation Mode) 모드로 들어가며 CRITICAL 시스템 알림을 전송합니다. 이 기능은 디바이스를 보호하고 메시지의 백로그를 처리하도록 설계되었습니다. 어플라이언스가 RCM에 들어가는 경우는 매우 드물게, 메일 볼륨이 매우 크거나 비정상적으로 증가하는 동안에만 발생해야 합니다. 빈번한 RCM 알림은 시스템이 과부하 상태임을 나타내는 것일 수 있습니다. 리소스 절약 활동 , 108 페이지를 참조하십시오.

시스템 용량 페이지의 데이터를 해석하는 방법

시스템 용량 보고서의 데이터를 조회할 시간 범위를 선택할 때 다음 사항에 유의하십시오.

- 일일 보고서 - 시간 테이블을 쿼리하고 24시간 동안 어플라이언스가 수신한 쿼리 수를 시간별로 정확하게 표시합니다. 이 정보는 시간 테이블에서 수신합니다. 이는 정확한 수치입니다.
- 월간 보고서 - 30일 또는 31일(해당 월의 일수에 따라)의 일일 테이블을 쿼리하여 30일 또는 31일의 쿼리 수를 정확하게 보고합니다. 이 역시 정확한 수치입니다.

시스템 용량 페이지의 '최대값' 표시는 지정된 기간에 나타난 최고치를 의미합니다. '평균값'은 지정된 기간의 모든 값의 평균치입니다. 집계 기간은 보고서에서 선택한 간격에 따라 다릅니다. 예를 들어 차트가 1개월분이라면 일별 평균값 및 최대값을 표시할 수 있습니다.

개별 Email Security Appliance에 대한 데이터 및 Security Management Appliance에 연결된 어플라이언스에 대한 전체 데이터를 보려면 특정 그래프에 대한 View Details(세부사항 보기) 링크를 클릭할 수 있습니다.

시스템 용량 - 작업 대기열

Workqueue(작업 대기열) 페이지는 메시지가 작업 대기열에 머무는 평균 시간을 보여줍니다(스팸 대기열 또는 정책, 바이러스, 전파 확산 대기열에 머무는 시간 제외). 1시간에서 1개월 사이의 기간을 볼

수 있습니다. 이러한 평균은 메일 전달을 지연시키는 단기 이벤트와 시스템 워크로드의 장기 추세를 모두 파악하는 데 도움이 될 수 있습니다.

참고 메시지가 격리에서 작업 대기열로 릴리스되면 "작업 대기열의 평균 시간" 메트릭이 이 시간을 무시합니다. 이렇게 되면 격리에서 사용되는 시간이 연장되어 이중 계산 및 왜곡된 통계가 방지됩니다.

보고서에는 또한 지정된 기간에 작업 대기열에 포함된 메시지의 볼륨과, 동일한 기간 전체에서 작업 대기열의 최대 메시지 수가 표시됩니다. 작업 대기열에 포함된 최대 메시지 수가 그래픽으로 표시되어 작업 대기열 임계값 레벨도 보여줍니다.

작업 대기열에 더러 나타나는 급증은 예상되는 정상적인 현상입니다. 작업 대기열의 메시지 수가 구성된 임계값보다 장시간 높게 유지되면 이는 용량 문제를 나타낼 수 있습니다. 이 시나리오에서는 임계값 조정을 고려해보거나 시스템 구성을 검토하십시오.

작업 대기열 임계값 레벨을 변경하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오.

팁 작업 대기열 페이지를 검토할 때 작업 대기열 백업의 빈도를 측정하고 메시지 10,000개를 초과하는 작업 대기열 백업을 메모해둘 수 있습니다.

시스템 용량 - 수신 메일

System Capacity(시스템 용량) – Incoming Mail(수신 메일) 페이지는 수신 연결, 총수신 메시지 수, 평균 메시지 크기 및 총수신 메시지 크기를 보여줍니다. 일, 주, 월, 연도의 결과를 볼 수 있습니다. 현재 환경에서 정상적인 메시지 볼륨 및 급증의 추세를 이해하는 것이 중요합니다. 시간에 따른 볼륨 증가를 추적하고 시스템 용량을 계획하려면 Incoming Mail(수신 메일) 페이지를 사용할 수 있습니다. 특정 도메인에서 현재 네트워크로 전송되는 이메일 볼륨의 추세를 보려면 Incoming Mail(수신 메일) 데이터를 Sender Profile(발신자 프로필) 데이터와 비교할 수도 있습니다.

참고 수신 연결 수의 증가가 반드시 시스템 로드에 영향을 미치는 것은 아닙니다.

시스템 용량 - 발신 메일

System Capacity(시스템 용량) – Outgoing Mail(발신 메일) 페이지는 발신 연결, 총발신 메시지 수, 평균 메시지 크기 및 총 발신 메시지 크기를 보여줍니다. 일, 주, 월, 연도의 결과를 볼 수 있습니다. 현재 환경에서 정상적인 메시지 볼륨 및 급증의 추세를 이해하는 것이 중요합니다. 시간에 따른 볼륨 증가를 추적하고 시스템 용량을 계획하려면 Outgoing Mail(발신 메일) 페이지를 사용할 수 있습니다. 특정 도메인 또는 IP 주소에서 전송되는 이메일 볼륨의 추세를 보려면 Outgoing Mail(발신 메일) 데이터를 Outgoing Destinations(발신 목적지) 데이터와 비교할 수도 있습니다.

시스템 용량 - 시스템 로드

시스템 로드 보고서는 다음을 보여줍니다.

전체 **CPU** 사용

Email Security Appliance는 메시지 처리량 개선을 위해 유휴 CPU 리소스를 사용하도록 최적화됩니다. 높은 CPU 사용량은 시스템 용량 문제를 나타내지 않을 수 있습니다. 높은 CPU 사용량이 지속적인 높은 볼륨의 메모리 페이지 스와핑과 결합되면 이는 용량 문제일 수 있습니다.

참고 이 그래프는 CPU 사용량 임계값도 보여주는데, 이는 시각적 참조일 뿐입니다. 이 선의 위치를 조정하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오. Email Security Appliance에서 용량 문제 해결을 위한 권장 조치를 알림으로 전달하도록 구성할 수 있습니다.

메일 처리, 스팸 및 바이러스 엔진, 보고, 격리 등의 여러 기능에 사용된 CPU의 양을 보여주는 그래프도 이 페이지에 표시됩니다. 기능별 CPU 그래프는 제품의 어떤 영역에서 시스템의 리소스를 가장 많이 사용하는지를 보여주는 훌륭한 지표입니다. 어플라이언스를 최적화해야 하는 경우 어떤 기능을 조정 또는 비활성화해야 할지를 결정하는 데 이 그래프가 도움이 될 수 있습니다.

메시지 페이지 스와핑

메모리 페이지 스와핑 그래프는 시스템이 디스크에 페이징해야 하는 빈도를 초당 킬로바이트 단위로 보여줍니다.

시스템은 메모리를 정기적으로 스와핑하도록 설계되었으므로, 어느 정도의 메모리 스와핑은 발생할 수 있으며 이것이 어플라이언스의 문제를 나타내지는 않습니다. 시스템이 일관되게 대량의 메모리를 서로 바꾸지 않는 한 메모리 스와핑은 정상이며 예상된 동작입니다(특히 C170어플라이언스에서). 성능을 높이려면 네트워크에 Email Security Appliance를 추가하거나 최대 처리량이 보장되도록 구성을 조정해야 할 수 있습니다.

참고 이 그래프는 메모리 페이지 스와핑 임계값도 보여주는데, 이는 시각적 참조일 뿐입니다. 이 선의 위치를 조정하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오. Email Security Appliance에서 용량 문제 해결을 위한 권장 조치를 알림으로 전달하도록 구성할 수 있습니다.

리소스 절약 활동

리소스 절약 활동 그래프는 Email Security Appliance가 RCM(Resource Conservation Mode)으로 들어간 횟수를 보여줍니다. 예를 들어 그래프에 n번이 표시되면 이는 어플라이언스가 RCM에 n번 들어갔으며 적어도 n-1번 RCM에서 빠져나왔음을 의미합니다.

어플라이언스가 RCM에 들어가는 경우는 매우 드물게, 메일 볼륨이 매우 크거나 비정상적으로 증가하는 동안에만 발생해야 합니다. 리소스 절약 활동 그래프에 어플라이언스가 RCS에 자주 들어가는 것으로 표시되면, 이는 시스템이 과부화되고 있음을 나타내는 것일 수 있습니다.

시스템 용량 - 전체

All(전체**)** 페이지는 서로 다른 보고서 사이의 관계를 파악할 수 있도록 모든 이전 시스템 용량 보고서를 단일 페이지로 통합합니다. 예를 들면, 과도한 메모리 스와핑이 발생할 때 메시지 대기열의 볼륨이 동시에 높아지는 것을 볼 수 있습니다. 이는 용량 문제를 나타내는 것일 수 있습니다. 이 페이지를 PDF로 저장하여 나중에 참조하도록(또는 지원 담당자와 공유하기 위해) 시스템 성능의 스냅샷을 보관할 수 있습니다.

시스템 용량 그래프의 임계값 표시

일부 그래프에서는 자주 또는 계속 넘을 경우 문제가 생길 수 있는 기본값을 선으로 나타냅니다. 이 시각적 표시를 조정하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오.

보고 데이터 가용성 페이지

Email(이메일**) > Reporting(**보고**) > Reporting Data Availability(**보고 데이터 가용성**)** 페이지는 데이터를 보고 업데이트하고 정렬하여, 리소스 사용률 및 이메일 트래픽 문제 지점에 대한 실시간 가시성을 제공할 수 있습니다.

Security Management Appliance에서 관리하는 전체 어플라이언스의 데이터 가용성을 포함하여, 모든 데이터 리소스 사용률 및 이메일 트래픽 문제 지점은 이 페이지에 표시됩니다.

또한 이 보고서 페이지에서 특정 어플라이언스 및 시간 범위에 대한 데이터 가용성을 볼 수 있습니다.

새 웹 인터페이스의 **Email Reporting(**이메일 보고**)** 페이지 이해

참고 이 목록에는 웹 인터페이스의 **Reports(**보고서**)** 드롭다운 아래에서 지원되는 최신 Email Security Appliance용 AsyncOS 릴리스에 사용 가능한 보고서가 나와 있습니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오. Email Security Appliance에서 이전 AsyncOS 릴리스를 실행 중인 경우 이러한 보고서 중 일부를 사용할 수 없습니다.

표 ***27: Email Reports***(이메일 보고서)**:** 드롭다운 옵션

Reports(보고서) 드롭다운 옵션	작업
Mail Flow Summary(메일 플로우 요약) 페이지	Mail Flow Summary(메일 플로우 요약) 보고서 페이지는 Email Security Appliance에 대한 활동 개요를 제공합니다. 이 페이지에는 수신 및 발신 메시지에 대한 그래프와 요약 테이블이 포함되어 있습니다. 자세한 내용은 Mail Flow Summary(메일 플로우 요약) 페이지, 114 페이지를 참조하십시오.
System Capacity(시스템 용량) 페이지	System Capacity(시스템 용량) 보고서 페이지에는 Security Management Appliance로 전송된 보고 데이터의 전체 워크로드에 대한 세부 정보가 표시됩니다. 자세한 내용은 System Capacity(시스템 용량) 페이지, 119 페이지를 참조하십시오.
파일 및 악성코드 보고서	
Advanced Malware Protection 페이지(파일 평판 및 파일 분석)	Advanced Malware Protection 보고서 페이지에서는 수신 및 발신 파일 기반 위협에 대한 요약, 파일 평판, 파일 분석, 파일 회귀 분석 및 사서함 자동 치료의 세부 정보를 표시하는 보고 보기가 표시됩니다. 자세한 내용은 Advanced Malware Protection 페이지 , 123 페이지를 참조하십시오.
Virus Filtering(바이러스 필터링) 페이지	Filtering(바이러스 필터링) 보고서 페이지는 네트워크에 유입되고 네트워크에서 전송되는 바이러스의 개요를 제공합니다. 이 페이지는 Email Security Appliance에서 실행 중인 바이러스 검사 엔진에 의해 탐지되고 Security Management Appliance에 표시되는 바이러스를 보여줍니다. 특정 바이러스에 대해 작업을 수행하려면 이 보고서를 사용합니다. 자세한 내용은 Virus Filtering(바이러스 필터링) 페이지, 130 페이지를 참조하십시오.
Macro Detection(매크로 탐지) 페이지	Macro Detection(매크로 탐지) 보고서 페이지에는 상위 수신 및 발신 매크로가 활성화된 첨부 파일이 콘텐츠 필터 및 메시지 필터로 탐지된 파일 형식으로 표시됩니다. 자세한 내용은 Macro Detection(매크로 탐지) 페이지, 132 페이지를 참조하십시오.
이메일 위협 보고서	

Reports(보고서) 드롭다운 옵션	작업
DMARC Verification(DMARC 확인) 페이지	DMARC Verification(DMARC 확인) 보고서 페이지는 DMARC(Domain-based Message Authentication, Reporting and Conformance) 확인에 실패한 상위 발신자 도메인 및 그 도메인으로부터 수신한 메시지에 대해 수행한 조치의 요약을 표시합니다. 자세한 내용은 DMARC Verification(DMARC 확인) 페이지, 132 페이지를 참조하십시오.
Outbreak Filtering(보안 침해 필터링) 페이지	Outbreak Filters 페이지는 Outbreak Filter에서 격리한 최근 보안 침해 및 메시지에 대한 정보를 제공합니다. 피싱, 스캠, 바이러스 및 악성 코드 공격에 대한 방어 체계를 모니터링할 때 이 보고서를 활용합니다. 자세한 내용은 Outbreak Filtering(보안 침해 필터링) 페이지, 133 페이지를 참조하십시오.
URL Filtering(URL 필터링) 페이지	메시지에서 가장 자주 발생하는 URL 범주, 스팸 메시지에 가장 많이 포함된 URL, 메시지에 나타난 악성 및 일반 URL 수를 확인할 때 이 페이지를 활용합니다. 자세한 내용은 URL Filtering(URL 필터링) 페이지, 135 페이지를 참조하십시오.
Forged Email Detection(위조 이메일 탐지) 페이지	Forged Email Detection(위조 이메일 탐지) 보고서 페이지에는 다음 보고서가 포함됩니다. • **Top Forged Email Detection**(상위 위조 이메일 탐지). 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 사용자 상위 10명이 표시됩니다. • **Forged Email Detection: Details**(위조 이메일 탐지: 세부 정보). 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 모든 사용자 목록과, 지정한 사용자에 대해 일치하는 메시지 수가 표시됩니다. 자세한 내용은 Forged Email Detection(위조 이메일 탐지) 페이지, 137 페이지를 참조하십시오.
Sender Domain Reputation(발신인 도메인 평판) 페이지	이 보고서 페이지를 사용하면 SDR 서비스에서 받은 판정과 위협 카테고리를 기반으로 수신 메시지를 볼 수 있습니다. 자세한 내용은 Sender Domain Reputation(발신인 도메인 평판) 페이지, 138 페이지를 참조하십시오.

Reports(보고서) 드롭다운 옵션	작업
External Threat Feeds(외부 위협 피드) 페이지	External Threat Feeds(외부 위협 피드) 페이지에는 다음 보고서가 표시됩니다. • 메시지에서 위협을 탐지하는 데 사용되는 상위 ETF 소스입니다. • 메시지에서 탐지된 위협과 일치하는 상위 IOC입니다. • 악의적인 수신 메일 연결을 필터링하는 데 사용되는 상위 ETF 소스입니다. 자세한 내용은 External Threat Feeds(외부 위협 피드) 페이지, 137 페이지를 참조하십시오.
연결 및 플로우 보고서	
Mail Flow Details(메일 플로우 세부 정보) 페이지	Mail Flow Details(메일 플로우 세부 정보) 페이지는 관리되는 Email Security Appliance에 연결된 모든 원격 호스트의 실시간 정보에 대한 인터랙티브 보고를 제공합니다. IP 주소, 도메인, 시스템에 메일을 전송하는 네트워크 소유자(조직)에 대한 정보를 수집할 수 있습니다. 자세한 내용은 Mail Flow Details(메일 플로우 세부 정보) 페이지, 138 페이지를 참조하십시오.
Sender Groups(발신자 그룹) 페이지	Sender Groups(발신자 그룹) 보고서 페이지는 발신자 그룹 및 메일 플로우 정책 작업별로 연결 요약을 제공하므로, SMTP 연결 및 메일 플로우 정책 추세를 검토할 수 있습니다. 자세한 내용은 Sender Groups(발신자 그룹) 페이지, 146 페이지를 참조하십시오.
Outgoing Destinations(발신 대상) 페이지	Outgoing Destinations(발신 목적지) 보고서 페이지는 여기서 보내는 메일의 도메인에 대한 정보를 제공합니다. 페이지 맨 위에는 위협 메시지의 상위 목적지 및 정상 메시지의 상위 목적지를 보여주는 그래프가 있습니다. 맨 아래에는 전체 수신자를 기준으로 정렬된 열과 함께 차트를 표시합니다(기본 설정). 자세한 내용은 Outgoing Destinations(발신 대상) 페이지, 147 페이지를 참조하십시오.
TLS Encryption(TLS 암호화) 페이지	TLS Encryption(TLS 암호화) 보고서 페이지는 주고받은 메일에 대한 TLS 연결의 전체 사용량을 보여줍니다. 보고서에서는 또한 TLS 연결을 사용하여 메일을 전송하는 각 도메인에 대한 세부사항도 보여줍니다. 자세한 내용은 TLS Encryption(TLS 암호화) 페이지, 149 페이지를 참조하십시오.

Reports(보고서) 드롭다운 옵션	작업
Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지	Inbound SMTP authentication(인바운드 SMTP 인증) 보고서 페이지는 클라이언트 인증서의 사용 및 ESA와 사용자 메일 클라이언트 간 SMTP 세션 인증을 위한 SMTP AUTH 명령을 보여줍니다. 자세한 내용은 Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지, 152 페이지를 참조하십시오.
Rate Limits(속도 제한) 페이지	Rate Limits(속도 제한) 보고서 페이지는 설정된 발신자별 메일 수신자 수 한도를 초과하는 메일 발신자(MAIL-FROM 주소 기준)를 표시합니다. 자세한 내용은 Rate Limits(속도 제한) 페이지, 153 페이지를 참조하십시오.
Connections by Country(국가별 연결 수) 페이지	Connections by Country(국가별 연결 수) 페이지에는 다음 내용이 표시됩니다. • 그래픽 형식의 발신지 국가별 상위 수신 메일 연결. • 표 형식의 총 수신 연결 및 발신지 국가별 메시지 수. 자세한 내용은 Connections by Country(국가별 연결 수) 페이지, 154 페이지를 참조하십시오.
사용자 리포트	
User Mail Summary(사용자 메일 요약) 페이지	User Mail Summary(사용자 메일 요약) 페이지는 내부 사용자가 보내고 받는 메일에 대한 정보를 이메일 주소별로 제공합니다 한 사용자가 여러 이메일 주소를 가질 수 있습니다. 이메일 주소는 보고서에서 결합되지 않습니다. 자세한 내용은 사용자 메일 요약, 155 페이지를 참조하십시오.
DLP Incident Summary(DLP 인시던트 요약) 페이지	DLP Incident Summary(DLP 인시던트 요약) 보고서 페이지는 발신 메일에서 발생하는 DLP(data loss prevention) 정책 위반에 대한 정보를 보여줍니다. 자세한 내용은 DLP Incident Summary(DLP 인시던트 요약) 페이지, 157 페이지를 참조하십시오.
Web Interaction Tracking(웹 상호 작용) 페이지	Web Interaction Tracking(웹 상호 작용) 보고서 페이지는 정책 또는 Outbreak Filter에 의해 재작성된 URL을 클릭한 엔드유저 및 각 사용자의 클릭과 연결된 조치를 나타냅니다. 자세한 내용은 Web Interaction Tracking(웹 상호 작용) 페이지, 159 페이지를 참조하십시오.
필터 보고서	

Reports(보고서) 드롭다운 옵션	작업
Message Filters(메시지 필터) 페이지	Message Filters(메시지 필터) 보고서 페이지는 수신 및 발신 메시지에 대한 상위 메시지 필터 매칭 결과(매칭하는 메시지 수가 가장 많은 메시지 필터)를 보여줍니다. 자세한 내용은 Message Filters(메시지 필터) 페이지, 161 페이지를 참조하십시오.
High Volume Mail(대용량 메일) 페이지	High Volume Mail(대량 메일) 보고서 페이지는 가변적인 1시간 동안 단일 발신자가 보낸 또는 동일한 제목으로 된 최다 메시지 수의 공격을 보여줍니다. 자세한 내용은 High Volume Mail(대용량 메일) 페이지, 161 페이지를 참조하십시오.
Content Filters(콘텐츠 필터) 페이지	Content Filters(콘텐츠 필터) 보고서 페이지는 상위 수신 및 발신 콘텐츠 필터 매칭 결과(매칭하는 메시지가 가장 많은 콘텐츠 필터)에 대한 정보를 제공합니다. 이 페이지는 데이터를 막대그래프 및 목록 형태로도 표시합니다. 자세한 내용은 Content Filters(콘텐츠 필터) 페이지, 162 페이지를 참조하십시오.

Mail Flow Summary(메일 플로우 요약) 페이지

Security Management Appliance의 Mail Flow Summary(메일 플로우 요약) 보고서 페이지는 Email Security Appliance에서 발생한 이메일 메시지 활동의 개요를 제공합니다. Mail Flow Summary(메일 플로우 요약) 보고서 페이지에는 수신 및 발신 메시지에 대한 그래프와 요약 테이블이 포함되어 있습니다.

Mail Flow Summary(메일 플로우 요약): Incoming(수신) 보고서 페이지에는 어플라이언스에서 처리하고 차단한 총 메시지 수에 대한 수신 메일 그래프와 수신 메일의 요약이 표시됩니다.

이 페이지의 메일 트렌드 그래프를 사용하면 어플라이언스에서 처리하고 차단한 모든 수신 메시지의 플로우를 선택한 시간 범위에 따라 모니터링할 수 있습니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.

데이터 내에서 특정 정보를 검색하려면 다음 섹션을 참조하십시오. 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지

다음 메일 트렌드 그래프는 수신 메일 플로우를 시각적으로 나타냅니다.

- 위협 탐지 요약
- 콘텐츠 요약

각 카테고리에 대한 필수 카운터에 따라 수신 메시지의 메일 트렌드를 볼 수 있습니다. 자세한 내용은 카운터를 사용하여 트렌드 그래프에서 데이터 필터링, 53 페이지을 참고하십시오.

Mail Flow Summary(메일 플로우 요약): Outgoing(발신) 보고서 페이지에는 어플라이언스에서 처리하고 차단한 총 메시지 수에 대한 발신 메일 그래프와 발신 메일의 요약이 표시됩니다.

이 페이지의 메일 트렌드 그래프를 사용하면 어플라이언스에서 처리하고 전송한 모든 발신 메시지의 플로우를 선택한 시간 범위에 따라 모니터링할 수 있습니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.

다음 메일 트렌드 그래프는 발신 메일의 메일 플로우를 시각적으로 나타냅니다.

처리된 메시지의 필수 카운터에 따라 발신 메시지의 메일 트렌드를 볼 수 있습니다. 자세한 내용은 카운터를 사용하여 트렌드 그래프에서 데이터 필터링, 53 페이지을 참고하십시오.

다음 목록은 Mail Flow Summary(메일 플로우 요약) 보고서 페이지의 여러 섹션을 설명합니다.

표 ***28: Mail Flow Summary(***메일 플로우 요약***)*** 페이지 세부 정보

섹션	설명
Mail Flow Summary(메일 플로우 요약**): Incoming(**수신**)**	
메시지 수	Number of Messages(메시지 수) 그래프는 위협 메시지로 처리된 메시지를 포함하여 처리된 총 메시지 수를 시각적으로 나타냅니다.
위협 메시지	Threat Messages(위협 메시지) 그래프는 Email Security Appliance에 의해 차단된 메시지의 총 수를 시각적으로 나타냅니다.
위협 탐지 요약	Threat Detection Summary(위협 탐지 요약) 메일 트렌드 그래프는 다음 카테고리를 기반으로 시각적으로 나타냅니다. • **Connection and Reputation Filtering(**연결 및 평판 필터링**)**: Reputation Filtering(평판 필터링) 및 Invalid Recipients(잘못된 수신자)를 기준으로 위협으로 분류되는 메시지입니다. • **Spam Detection(**스팸 탐지**)**: 안티 스팸 검사 엔진에 의해 위협으로 분류되는 메시지입니다. • **Email Spoofing(**이메일 스푸핑**)**: DMARC 확인 실패로 인해 위협으로 분류되는 메시지입니다. • **Outbreak Threat Summary(**보안 침해 위협 요약**)**: Outbreak Filtering(보안 침해 필터링) 엔진에 의해 피싱, 스캠, 바이러스 또는 악성코드로 분류되는 메시지입니다. • **Attachment and Malware Detection(**첨부 파일 및 악성코드 탐지**)**: 안티바이러스 및 AMP 엔진에 의해 위협으로 분류되는 메시지입니다. • **All Categories(**모든 카테고리**)**: 위협으로 분류되는 모든 메시지입니다.

섹션	설명
콘텐츠 요약	Content Summary(콘텐츠 요약) 메일 트렌드 그래프는 다음 카테고리를 기반으로 시각적으로 나타냅니다. • **Graymail(**그레이메일**)**: 마케팅, 대량 또는 소셜 네트워킹으로 분류되는 메시지입니다. • **Content Filters(**콘텐츠 필터**)**: 콘텐츠 필터에 의해 분류되는 메시지입니다. • **All Categories(**모든 카테고리**)**: 그레이메일 엔진 및 콘텐츠 필터로 분류되는 모든 메시지입니다.
Mail Flow Summary(메일 플로우 요약**): Outgoing(**발신**)**	
메시지 수	Number of Messages(메시지 수) 그래프는 정상으로 처리된 메시지를 포함하여 처리된 총 메시지 수를 시각적으로 나타냅니다.
메시지 전송	Message Delivery(메시지 전송) 그래프는 하드 반송을 포함하여 전송되는 메시지의 총 수를 시각적으로 나타냅니다.
발신 메일	Outgoing Mails(발신 메일) 트렌드 그래프는 다음 카테고리를 기반으로 시각적으로 나타냅니다. • 탐지된 스팸 • 탐지된 바이러스 • AMP에서 탐지됨 • 콘텐츠 필터에 의해 중지됨 • DLP에 의해 중지됨

관련 주제

- 어플라이언스에서 이메일 메시지를 분류하는 방법, 75 페이지
- 수신 메일 메시지 카운트 방법, 75 페이지
- Mail Flow Summary(메일 플로우 요약) 페이지의 이메일 메시지 분류, 117 페이지

수신 메일 메시지 카운트 방법

수신 메시지 카운트는 메시지당 수신자 수를 기준으로 합니다. 예를 들어 example.com에서 오는 하나의 수신 메시지가 세 명의 수신자에게 전송되면 해당 발신자로부터 3개의 메시지가 오는 것으로 계산됩니다.

발신자 평판 필터링에 의해 차단된 메시지는 실제로 작업 대기열에 들어가지 못하므로, 어플라이언스는 수신 메시지에 대한 수신자 목록에 액세스하지 못합니다. 이 경우 수신자 수를 추적하기 위해 승수가 사용됩니다. 승수는 기존 고객 데이터의 대규모 샘플링을 조사하여 결정합니다.

어플라이언스에서 이메일 메시지를 분류하는 방법

이메일 파이프라인을 통해 진행되는 동안 메시지는 여러 범주에 적용될 수 있습니다. 예를 들어 한 메시지가 스팸 또는 바이러스 양성으로 표시될 수 있으며, 콘텐츠 필터와 매치할 수도 있습니다. 각종 필터 및 검사 활동의 우선순위가 메시지 처리 결과에 큰 영향을 미칩니다.

위의 예에서 다양한 판정이 이 우선순위 규칙을 따릅니다.

- 스팸 양성
- 바이러스 양성
- 콘텐츠 필터 일치

이 규칙에 따라, 메시지가 스팸 양성으로 표시되고 안티스팸 설정이 스팸 양성 메시지를 삭제하도록 설정된 경우 메시지가 삭제되고 스팸 카운터가 늘어납니다.

스팸 양성 메시지가 이메일 파이프라인에서 계속 진행되도록 안티스팸 설정이 구성되었으며 후속 콘텐츠 필터가 메시지를 삭제, 반송 또는 격리하는 경우에도 스팸 수가 증가합니다. 메시지가 스팸 또는 바이러스 양성이 아닌 경우에만 콘텐츠 필터 수가 증가합니다.

또는 메시지가 보안 침해 필터에 의해 격리된 경우, 격리에서 해제되어 작업 대기열을 통해 다시 처리될 때까지 계산되지 않습니다.

메시지 처리 우선 순위에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말이나 사용 설명서에 있는 이메일 파이프라인에 대한 장을 참조하십시오.

Mail Flow Summary(메일 플로우 요약**)** 페이지의 이메일 메시지 분류

위협으로 간주되는 수신 메시지 및 Mail Flow Summary(메일 플로우 요약) 보고서 페이지에서 제공되는 발신 메시지는 다음과 같이 분류됩니다.

표 ***29: Mail Flow Summary(***메일 플로우 요약***)*** 페이지의 이메일 카테고리

카테고리	설명
Mail Flow Summary(메일 플로우 요약**): Incoming(**수신**)**	

카테고리	설명
평판 필터링	HAT 정책에 의해 차단된 모든 연결을 고정 승수로 곱하고(수신 메일 메시지 카운트 방법, 75 페이지 참조) 여기에 수신자 제한에 의해 차단된 모든 수신자를 더한 값. Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)에 대한 값은 다음 요인을 기반으로 계산됩니다. • 해당 발신자가 보낸 "조절된(throttled)" 메시지의 수 • 거부된 또는 TCP 거절된 연결의 수(부분 개수일 수 있음) • 연결당 메시지 수에 대한 보수적 승수 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다. 이 상황에서 표시된 값은 최소 메시지 수를 나타내는 값이 중지된 것으로 해석할 수 있습니다. Mail Flow Summary(메일 플로우 요약) 보고서 페이지의 Reputation Filtering(평판 필터링) 총 수와 백분율은 항상 거부된 모든 연결의 전체 개수를 기반으로 합니다. 발신자 기준 연결 개수만 부하 때문에 제한됩니다.
올바르지 않은 수신인	대화형 LDAP 거부에 의해 거부된 모든 메일 수신자와 모든 RAT 거부를 더한 총 수와 백분율.
Anti-Spam	안티 스팸 검사 엔진에 의해 양성이거나 의심스러운 것으로 탐지된 수신 메시지의 총 수와 백분율. 스팸이자 바이러스 양성인 메시지도 해당됩니다.
Anti-Virus	바이러스 양성이며 스팸은 아닌 것으로 탐지된 수신 메시지의 총 수와 백분율. 다음 메시지는 "탐지된 바이러스" 범주에 포함됩니다. • 바이러스 검사 결과가 "손상" 또는 "감염"인 메시지. • 암호화 메시지를 바이러스 포함으로 간주하는 옵션이 선택된 경우 바이러스 검사 결과가 "암호화"인 메시지. • 검사 불가 메시지에 대한 조치가 "전달"이 아닐 경우 바이러스 검사 결과가 "검사 불가"인 메시지. • 대체 메일 호스트 또는 대체 수신자에게 전달하는 옵션이 선택된 경우 바이러스 검사 결과가 "검사 불가" 또는 "암호화"인 메시지. • 보안 침해 격리에서 수동으로 또는 시간 초과로 인해 삭제된 메시지.

카테고리	설명
AMP(Advanced Malware Protection)	파일 분석 서비스에 의해 차단된 수신 메시지의 총 수와 백분율. 메시지 첨부 파일이 파일 평판 필터링에서 악성으로 확인되었습니다. 이 값에는 파일 분석에 의해 악성으로 확인된 판정 업데이트 또는 파일이 포함되어 있지 않습니다.
콘텐츠 필터	메시지 및 콘텐츠 필터에 의해 중지된 총 수신 메시지 수와 백분율.
DMARC 정책	DMARC 확인, 해독 또는 둘 다에 실패한 수신 메시지의 총 수와 백분율.
S/MIME 확인/암호 해독 실패	S/MIME 검증 및/또는 해독에 실패한 수신 메시지의 총 수와 백분율.
Mail Flow Summary(메일 플로우 요약): Outgoing(발신)	
하드 바운스됨	영구적으로 전달할 수 없는 발신 메시지의 총 수와 백분율.
배달됨	전달되는 발신 메시지의 총 수와 백분율.

참고 검사할 수 없는 메시지 또는 암호화된 메시지를 전달하도록 안티바이러스 설정을 구성한 경우 이러한 메시지는 바이러스 양성이 아닌 정상 메시지로 계산됩니다. 그렇지 않은 경우 메시지는 바이러스 양성으로 계산됩니다.

또한 메시지 필터와 매치하며 필터에 의해 삭제되거나 반송되지 않은 메시지는 정상으로 간주됩니다. 메시지 필터에 의해 삭제 또는 반송된 메시지는 합계에 포함되지 않습니다.

관련 주제

Mail Flow Details(메일 플로우 세부 정보) 페이지, 138 페이지

System Capacity(시스템 용량) 페이지

System Capacity(시스템 용량) 보고서 페이지는 작업 대기열에 있는 메시지, 수신/발신 메시지(볼륨, 크기 및 수), 전체 CPU 사용량, 기능별 CPU 사용량, 메모리 페이지 스와핑 정보 등 시스템 로드에 대한 자세한 내용을 제공합니다.

System Capacity(시스템 용량) 보고서 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- Email Security Appliance가 권장 용량을 초과하는 시기를 식별합니다. 이를 통해 구성 최적화 또는 추가 어플라이언스가 필요한 시기를 결정할 수 있습니다.
- 앞으로의 용량 문제를 보여주는 시스템 동작의 기록 추세를 식별합니다.
- 문제 해결을 위해, 시스템의 어떤 부분이 가장 많은 리소스를 사용하는지를 식별합니다.

Security Management Appliance에서 System Capacity(시스템 용량) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) >**

System Capacity(시스템 용량)를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

용량이 메시지 볼륨에 적절한지 확인하려면 Email Security Appliance를 모니터링할 수 있습니다. 시간이 지나면 볼륨이 불가피하게 증가하므로, 적절한 모니터링을 통해 추가 용량 또는 구성 변경을 사전에 적용해야 합니다. 시스템 용량을 모니터링하는 가장 효과적인 방법은 전체적인 볼륨, 작업 대기열의 메시지 수 및 리소스 절약 모드의 인시던트 수를 추적하는 것입니다.

- **Volume**(볼륨): 현재 환경에서 "정상" 메시지 볼륨 및 "일상적인" 급증을 이해하는 것이 중요합니다. 시간의 경과에 따라 이 데이터를 추적하여 볼륨 증가를 측정하십시오. 시간의 경과에 따른 볼륨을 추적하려면 Incoming Mail(수신 메일) 및 Outgoing Mail(발신 메일) 페이지를 사용할 수 있습니다. 자세한 내용은 시스템 용량 - 수신 메일, 107 페이지 및 시스템 용량 - 발신 메일, 107 페이지를 참조하십시오.
- **Work Queue**(작업 대기열): 작업 대기열은 스팸 공격을 흡수 및 필터링하고 비 스팸 메시지의 증가를 처리하는 "충격 흡수자" 역할을 하도록 설계되었습니다. 그러나 작업 대기열도 부하 상태의 시스템을 나타내는 지표가 될 수 있습니다. 작업 대기열 백업을 길게 자주 수행할 경우 용량 문제가 발생할 수 있습니다. System Capacity - Workqueue(시스템 용량 - 작업 대기열) 페이지에서 작업 대기열의 활동을 추적할 수 있습니다. 자세한 내용은 시스템 용량 - 작업 대기열, 106 페이지을(를) 참고하십시오.
- **Resource Conservation Mode**(리소스 절약 모드): 어플라이언스는 과부하 상태가 되면 RCM(Resource Conservation Mode) 모드로 들어가며 CRITICAL 시스템 알림을 전송합니다. 이 기능은 디바이스를 보호하고 메시지의 백로그를 처리하도록 설계되었습니다. 어플라이언스가 RCM에 들어가는 경우는 매우 드물게, 메일 볼륨이 매우 크거나 비정상적으로 증가하는 동안에만 발생해야 합니다. 빈번한 RCM 알림은 시스템이 과부하 상태임을 나타내는 것일 수 있습니다. 리소스 절약 활동 , 108 페이지를 참조하십시오.

관련 주제

- 시스템 용량 페이지의 데이터를 해석하는 방법, 106 페이지
- 시스템 용량 - 작업 대기열, 106 페이지
- 시스템 용량 - 수신 메일, 107 페이지
- 시스템 용량 - 발신 메일, 107 페이지
- 시스템 용량 - 전체, 109 페이지
- 시스템 용량 그래프의 임계값 표시 , 109 페이지

시스템 용량 페이지의 데이터를 해석하는 방법

시스템 용량 보고서의 데이터를 조회할 시간 범위를 선택할 때 다음 사항에 유의하십시오.

- 일일 보고서 - 시간 테이블을 쿼리하고 24시간 동안 어플라이언스가 수신한 쿼리 수를 시간별로 정확하게 표시합니다. 이 정보는 시간 테이블에서 수신합니다. 이는 정확한 수치입니다.
- 월간 보고서 - 30일 또는 31일(해당 월의 일수에 따라)의 일일 테이블을 쿼리하여 30일 또는 31일의 쿼리 수를 정확하게 보고합니다. 이 역시 정확한 수치입니다.

시스템 용량 페이지의 '최대값' 표시는 지정된 기간에 나타난 최고치를 의미합니다. '평균값'은 지정된 기간의 모든 값의 평균치입니다. 집계 기간은 보고서에서 선택한 간격에 따라 다릅니다. 예를 들어 차트가 1개월분이라면 일별 평균값 및 최대값을 표시할 수 있습니다.

개별 Email Security Appliance에 대한 데이터 및 Security Management Appliance에 연결된 어플라이언스에 대한 전체 데이터를 보려면 특정 그래프에 대한 View Details(세부사항 보기) 링크를 클릭할 수 있습니다.

시스템 용량 - 작업 대기열

Workqueue(작업 대기열) 페이지는 메시지가 작업 대기열에 머무는 평균 시간을 보여줍니다(스팸 대기열 또는 정책, 바이러스, 전파 확산 대기열에 머무는 시간 제외). 1시간에서 1개월 사이의 기간을 볼 수 있습니다. 이러한 평균은 메일 전달을 지연시키는 단기 이벤트와 시스템 워크로드의 장기 추세를 모두 파악하는 데 도움이 될 수 있습니다.

참고 메시지가 격리에서 작업 대기열로 릴리스되면 "작업 대기열의 평균 시간" 메트릭이 이 시간을 무시합니다. 이렇게 되면 격리에서 사용되는 시간이 연장되어 이중 계산 및 왜곡된 통계가 방지됩니다.

보고서에는 또한 지정된 기간에 작업 대기열에 포함된 메시지의 볼륨과, 동일한 기간 전체에서 작업 대기열의 최대 메시지 수가 표시됩니다. 작업 대기열에 포함된 최대 메시지 수가 그래픽으로 표시되어 작업 대기열 임계값 레벨도 보여줍니다.

작업 대기열에 더러 나타나는 급증은 예상되는 정상적인 현상입니다. 작업 대기열의 메시지 수가 구성된 임계값보다 장시간 높게 유지되면 이는 용량 문제를 나타낼 수 있습니다. 이 시나리오에서는 임계값 조정을 고려해보거나 시스템 구성을 검토하십시오.

작업 대기열 임계값 레벨을 변경하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오.

팁 작업 대기열 페이지를 검토할 때 작업 대기열 백업의 빈도를 측정하고 메시지 10,000개를 초과하는 작업 대기열 백업을 메모해둘 수 있습니다.

시스템 용량 - 수신 메일

System Capacity(시스템 용량) – Incoming Mail(수신 메일) 페이지는 수신 연결, 총수신 메시지 수, 평균 메시지 크기 및 총수신 메시지 크기를 보여줍니다. 일, 주, 월, 연도의 결과를 볼 수 있습니다. 현재 환경에서 정상적인 메시지 볼륨 및 급증의 추세를 이해하는 것이 중요합니다. 시간에 따른 볼륨 증가를 추적하고 시스템 용량을 계획하려면 Incoming Mail(수신 메일) 페이지를 사용할 수 있습니다. 특정 도메인에서 현재 네트워크로 전송되는 이메일 볼륨의 추세를 보려면 Incoming Mail(수신 메일) 데이터를 Sender Profile(발신자 프로필) 데이터와 비교할 수도 있습니다.

참고 수신 연결 수의 증가가 반드시 시스템 로드에 영향을 미치는 것은 아닙니다.

시스템 용량 - 발신 메일

System Capacity(시스템 용량) – Outgoing Mail(발신 메일) 페이지는 발신 연결, 총발신 메시지 수, 평균 메시지 크기 및 총 발신 메시지 크기를 보여줍니다. 일, 주, 월, 연도의 결과를 볼 수 있습니다. 현재 환경에서 정상적인 메시지 볼륨 및 급증의 추세를 이해하는 것이 중요합니다. 시간에 따른 볼륨 증가를 추적하고 시스템 용량을 계획하려면 Outgoing Mail(발신 메일) 페이지를 사용할 수 있습니다. 특정 도메인 또는 IP 주소에서 전송되는 이메일 볼륨의 추세를 보려면 Outgoing Mail(발신 메일) 데이터를 Outgoing Destinations(발신 목적지) 데이터와 비교할 수도 있습니다.

시스템 용량 - 시스템 로드

시스템 로드 보고서는 다음을 보여줍니다.

- 전체 CPU 사용, 108 페이지
- 메시지 페이지 스와핑, 108 페이지
- 리소스 절약 활동 , 108 페이지

전체 **CPU** 사용

Email Security Appliance는 메시지 처리량 개선을 위해 유휴 CPU 리소스를 사용하도록 최적화됩니다. 높은 CPU 사용량은 시스템 용량 문제를 나타내지 않을 수 있습니다. 높은 CPU 사용량이 지속적인 높은 볼륨의 메모리 페이지 스와핑과 결합되면 이는 용량 문제일 수 있습니다.

참고 이 그래프는 CPU 사용량 임계값도 보여주는데, 이는 시각적 참조일 뿐입니다. 이 선의 위치를 조정하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오. Email Security Appliance에서 용량 문제 해결을 위한 권장 조치를 알림으로 전달하도록 구성할 수 있습니다.

메일 처리, 스팸 및 바이러스 엔진, 보고, 격리 등의 여러 기능에 사용된 CPU의 양을 보여주는 그래프도 이 페이지에 표시됩니다. 기능별 CPU 그래프는 제품의 어떤 영역에서 시스템의 리소스를 가장 많이 사용하는지를 보여주는 훌륭한 지표입니다. 어플라이언스를 최적화해야 하는 경우 어떤 기능을 조정 또는 비활성화해야 할지를 결정하는 데 이 그래프가 도움이 될 수 있습니다.

메시지 페이지 스와핑

메모리 페이지 스와핑 그래프는 시스템이 디스크에 페이징해야 하는 빈도를 초당 킬로바이트 단위로 보여줍니다.

시스템은 메모리를 정기적으로 스와핑하도록 설계되었으므로, 어느 정도의 메모리 스와핑은 발생할 수 있으며 이것이 어플라이언스의 문제를 나타내지는 않습니다. 시스템이 일관되게 대량의 메모리를 서로 바꾸지 않는 한 메모리 스와핑은 정상이며 예상된 동작입니다(특히 C170어플라이언스에서). 성능을 높이려면 네트워크에 Email Security Appliance를 추가하거나 최대 처리량이 보장되도록 구성을 조정해야 할 수 있습니다.

참고 이 그래프는 메모리 페이지 스와핑 임계값도 보여주는데, 이는 시각적 참조일 뿐입니다. 이 선의 위치를 조정하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오. Email Security Appliance에서 용량 문제 해결을 위한 권장 조치를 알림으로 전달하도록 구성할 수 있습니다.

리소스 절약 활동

리소스 절약 활동 그래프는 Email Security Appliance가 RCM(Resource Conservation Mode)으로 들어간 횟수를 보여줍니다. 예를 들어 그래프에 n번이 표시되면 이는 어플라이언스가 RCM에 n번 들어갔으며 적어도 n-1번 RCM에서 빠져나왔음을 의미합니다.

어플라이언스가 RCM에 들어가는 경우는 매우 드물게, 메일 볼륨이 매우 크거나 비정상적으로 증가하는 동안에만 발생해야 합니다. 리소스 절약 활동 그래프에 어플라이언스가 RCS에 자주 들어가는 것으로 표시되면, 이는 시스템이 과부화되고 있음을 나타내는 것일 수 있습니다.

시스템 용량 - 전체

All(전체**)** 페이지는 서로 다른 보고서 사이의 관계를 파악할 수 있도록 모든 이전 시스템 용량 보고서를 단일 페이지로 통합합니다. 예를 들면, 과도한 메모리 스와핑이 발생할 때 메시지 대기열의 볼륨이 동시에 높아지는 것을 볼 수 있습니다. 이는 용량 문제를 나타내는 것일 수 있습니다. 이 페이지를 PDF로 저장하여 나중에 참조하도록(또는 지원 담당자와 공유하기 위해) 시스템 성능의 스냅샷을 보관할 수 있습니다.

시스템 용량 그래프의 임계값 표시

일부 그래프에서는 자주 또는 계속 넘을 경우 문제가 생길 수 있는 기본값을 선으로 나타냅니다. 이 시각적 표시를 조정하려면 ESA 시스템 상태 그래프의 참조 임계값 조정, 491 페이지를 참조하십시오.

Advanced Malware Protection 페이지

Advanced Malware Protection은 다음을 통해 이메일 첨부 파일의 제로 데이 및 표적 파일 기반 위협으로부터 보호합니다.

- 알려진 파일의 평판 가져오기
- 아직 평판 서비스에 알려지지 특정 파일의 동작 분석
- 새로운 정보가 사용 가능하게 될 때 새로 발생하는 위협을 평가하고 네트워크에 들어온 후 위협으로 확인된 파일에 대해 알림

이 기능은 수신 및 발신 메시지에 사용할 수 있습니다.

파일 평판 필터링 및 파일 분석에 대한 자세한 내용은 *AsyncOS for Email Security Appliance*에 대한 온라인 도움말 또는 사용 설명서를 참조하십시오.

보고서 페이지를 보려면 Reports(보고서) 드롭다운의 Filter and Malware Reports(필터 및 악성코드 보고서) 섹션에서 **Advanced Malware Protection**을 선택합니다.

Advanced Malware Protection 보고서 페이지에는 다음 보고 보기가 표시됩니다.

- Advanced Malware Protection - Summary(요약), 124 페이지
- Advanced Malware Protection – AMP Reputation(AMP 평판), 124 페이지
- Advanced Malware Protection – File Analysis(파일 분석), 126 페이지
- Advanced Malware Protection – File Retrospection(파일 회귀 분석), 126 페이지
- Advanced Malware Protection – Mailbox Auto Remediation(사서함 자동 치료), 127 페이지

Security Management Appliance에서 Advanced Malware Protection 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Advanced Malware Protection**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지를 참고해 주십시오.

Advanced Malware Protection 보고서 페이지에는 Cisco Threat Grid 어플라이언스에 연결된 모든 관리 대상 어플라이언스의 실시간 데이터를 제공하는 메트릭 표시줄이 표시됩니다.

참고
- 메트릭 표시줄에 데이터를 채우려면 CLI에서 `trailblazerconfig > enable` 명령을 사용해야 합니다. 자세한 내용은 trailblazerconfig 명령, 485 페이지의 내용을 참고하십시오.
- 일, 주, 월에 대한 Cisco Threat Grid 어플라이언스의 데이터만 볼 수 있습니다.

관련 주제
- SHA-256 해시로 파일 식별 , 96 페이지
- 파일 분석 보고서 요구 사항 정보 , 94 페이지
- 다른 보고서의 파일 평판 필터링 데이터 보기 , 99 페이지

Advanced Malware Protection - Summary(요약)

Advanced Malware Protection - Summary(요약) 페이지에는 파일 평판 및 파일 분석 서비스에 의해 식별되는 수신 및 발신 파일 기반 위협의 전체 요약을 표시합니다.

자세한 내용은 Advanced Malware Protection – AMP Reputation(AMP 평판), 124 페이지 및 Advanced Malware Protection – File Analysis(파일 분석), 126 페이지를 참조하십시오.

Advanced Malware Protection – AMP Reputation(AMP 평판)

Advanced Malware Protection – AMP Reputation(AMP 평판) 페이지에는 파일 평판 서비스에 의해 식별된 수신 및 발신 파일 기반 위협을 표시합니다.

판정이 변경된 파일은 AMP 판정 업데이트 보고서를 참조하십시오. 그러한 판정은 Advanced Malware Protection 보고서에 적용되지 않습니다.

압축 또는 아카이브 파일에서 추출된 파일 중 하나가 악성인 경우 압축 또는 아카이브 파일의 SHA 값만 Advanced Malware Protection 보고서에 포함됩니다.

AMP에 의해 처리되는 수신 파일 섹션에는 악성, 정상, 알 수 없음, 검사 불가, 낮은 위험 등 다양 한 카테고리별 수신 악성코드 파일이 표시됩니다.

수신 악성 파일은 다음과 같이 분류됩니다.

- 카테고리가 악성 코드로 지정된 AMP 평판 서버에서 수신한 블랙리스트에 있는 파일 SHA의 백분율입니다.
- 카테고리가 **Custom Detection(**맞춤형 탐지**)**으로 지정된 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율이 표시됩니다. AMP for Endpoints Console에서 가져온 블랙리스트에 있는 파일의 위협 이름이 보고서의 Incoming Malware Threat Files(수신 악성코드 위협 파일) 섹션에서 **Simple Custom Detection(**단순 맞춤형 탐색**)**으로 표시됩니다.
- 카테고리가 **Custom Threshold(**맞춤형 임계값**)**로 지정된 임계값 설정에 따라 블랙리스트에 있는 파일 SHA의 백분율

보고서의 More Details(추가 세부 정보) 섹션에 있는 링크를 클릭하여 AMP for Endpoints Console에서 블랙리스트에 있는 파일 SHA의 파일 경로 분석 세부 정보를 볼 수 있습니다.

보고서의 AMP 섹션에서 수신 파일 전달에 낮은 위험 판정 세부사항을 볼 수 있습니다.

Advanced Malware Protection: Incoming(Advanced Malware Protection: 수신) 보고서 페이지의 AMP Reputation(AMP 평판) 보기를 사용하면 다음 정보를 볼 수 있습니다.

- Advanced Malware Protection 엔진의 파일 평판 서비스에 의해 식별되는 수신 파일의 요약(그래픽 형식)
- 선택한 시간 범위에 따른 모든 수신 악성코드 위협 파일의 트렌드 그래프
- 상위 수신 악성코드 위협 파일
- 파일 유형에 따른 상위 수신 위협 파일
- 상위 수신 악성코드 위협 파일을 나열하는 Incoming Malware Threat Files(수신 악성코드 위협 파일) 인터랙티브 테이블

  각 파일의 위협 특성을 포함한 자세한 분석 결과를 보려면 드릴다운합니다.

  사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 파란색 숫자 링크를 클릭합니다.

Advanced Malware Protection: Outgoing(Advanced Malware Protection: 발신) 보고서 페이지의 AMP Reputation(AMP 평판) 보기를 사용하면 다음 정보를 볼 수 있습니다.

- Advanced Malware Protection 엔진의 파일 평판 서비스에 의해 식별되는 발신 파일의 요약(그래픽 형식)
- 선택한 시간 범위에 따른 모든 발신 악성코드 위협 파일의 트렌드 그래프
- 상위 발신 악성코드 위협 파일

- 파일 유형에 따른 상위 발신 위협 파일
- 파일 평판 서비스에 의해 식별되는 상위 발신 악성코드 위협 파일이 나열되는 Outgoing Malware Threat Files(발신 악성코드 위협 파일) 인터랙티브 테이블

  각 파일의 위협 특성을 포함한 자세한 분석 결과를 보려면 드릴다운합니다.

  사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 파란색 숫자 링크를 클릭합니다.

Advanced Malware Protection – File Analysis(파일 분석)

Advanced Malware Protection – File Analysis(파일 분석) 페이지는 분석을 위해 전송된 각 파일에 대한 시간 및 판정(또는 임시 판정)을 보여줍니다. 어플라이언스는 30분마다 분석 결과를 확인합니다.

1,000개가 넘는 파일 분석 결과를 보려면 데이터를 .csv 파일로 내보냅니다.

온프레미스 Cisco AMP Threat Grid 어플라이언스 구축: 화이트리스트에 나열된 파일은 "정상"으로 표시됩니다. 화이트리스트에 대한 내용은 AMP Threat Grid 설명서 또는 온라인 도움말을 참조하십시오.

각 파일의 위협 특성을 포함한 자세한 분석 결과를 보려면 드릴다운합니다.

SHA에 대한 추가 정보를 검색하거나 파일 분석 세부사항 페이지 맨 아래의 링크를 클릭하여 파일을 분석한 서버에 대한 세부사항을 볼 수 있습니다. 자세한 내용은 SHA-256 해시로 파일 식별 , 96 페이지을 참고하십시오.

사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 세부 정보 링크를 클릭합니다.

파일을 분석한 서버의 세부사항을 보려면 파일 분석 보고서 요구 사항 정보 , 94 페이지를 참조하십시오.

압축 또는 아카이브 파일에서 추출된 파일이 분석을 위해 전송된 경우 이러한 추출된 파일의 SHA 값만 파일 분석 보고서에 포함됩니다.

Advanced Malware Protection 보고서 페이지의 File Analysis(파일 분석) 보기를 사용하면 다음 정보를 볼 수 있습니다.

- Advanced Malware Protection 엔진 파일 분석 서비스로 파일 분석을 수행하기 위해 업로드되는 수신 및 발신 파일의 수
- 파일 분석 요청이 완료된 수신 및 발신 파일 목록
- 파일 분석 요청이 보류 중인 수신 및 발신 파일 목록

Advanced Malware Protection – File Retrospection(파일 회귀 분석)

Advanced Malware Protection – Retrospection(파일 회귀 분석) 페이지는 메시지가 수신된 이후에 판정이 변경되어 이 어플라이언스에서 처리한 파일을 표시합니다. 이 시나리오에 대한 자세한 내용은 Email Security Appliance용 설명서를 참조하십시오.

Advanced Malware Protection은 표적 및 제로데이 위협에 중점을 두므로 집계된 데이터에서 추가 정보를 표시하면 위협 판정이 바뀔 수 있습니다.

1,000개가 넘는 판정 업데이트를 보려면 데이터를 .csv 파일로 내보냅니다.

단일 SHA-256에 대해 여러 판정이 변경된 경우 이 보고서에 판정 기록이 아닌 최신 판정만 표시됩니다.

보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 특정 SHA-256의 영향을 받는 모든 메시지를 보려면 SHA-256 링크를 클릭합니다.

Advanced Malware Protection: Outgoing(Advanced Malware Protection: 발신) 보고서 페이지의 File Retrospection(파일 회귀 분석) 보기를 사용하면 다음 정보를 볼 수 있습니다.

- 회귀 판정 변경 사항이 있는 수신 및 발신 파일의 목록.

Advanced Malware Protection – Mailbox Auto Remediation(사서함 자동 치료)

Advanced Malware Protection - Mailbox Auto Remediation(사서함 자동 치료) 보고서 페이지에는 수신 파일에 대한 사서함 치료 결과에 대한 세부 정보가 표시됩니다.

Advanced Malware Protection - Mailbox Auto Remediation(사서함 자동 치료) 페이지를 사용하여 다음과 같은 회귀적 보안 세부 정보를 볼 수 있습니다.

- SHA-256 해시와 관련된 파일 이름
- 메시지에 수행된 교정 조치
- 사서함 치료에 성공했거나 실패한 수신자 목록

Recipients for whom remediation was unsuccessful(교정에 실패한 수신자) 필드는 다음과 같은 시나리오에서 업데이트됩니다.

- 어플라이언스에 구성된 교정 조치를 수행하려 했을 때 어플라이언스와 Office 365 서비스 간의 연결 문제가 있었습니다.

메시지 추적에서 관련된 메시지를 보려면 SHA-256 해시를 클릭합니다.

파일 분석 보고서 요구 사항 정보

- (클라우드 파일 분석) 관리 어플라이언스에서 파일 분석 서버와 연결할 수 있음을 확인 , 94 페이지
- (클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성 , 94 페이지
- (온프레미스 파일 분석) 파일 분석 계정 활성화 , 95 페이지
- 추가 요구 사항 , 95 페이지

(클라우드 파일 분석) 관리 어플라이언스에서 파일 분석 서버와 연결할 수 있음을 확인

파일 분석 보고서 세부사항을 얻으려면 어플라이언스가 포트 443을 통해 파일 분석 서버에 연결할 수 있습니다. 자세한 내용은 방화벽 정보, 563 페이지를 참조하십시오.

Cisco Content Security Management Appliance가 인터넷에 직접 연결되지 않은 경우 이 트래픽용 프록시 서버를 구성합니다(업그레이드 및 업데이트 설정, 453 페이지 참조). 프록시를 사용하여 업그레이드와 서비스 업데이트를 가져오도록 어플라이언스를 이미 구성한 경우 기존 설정이 사용됩니다.

HTTPS 프록시를 사용할 경우 프록시가 트래픽을 해독해서는 안 됩니다. 파일 분석 서버와의 통신에는 pass-through 메커니즘을 사용합니다. 프록시 서버가 파일 분석 서버의 인증서를 신뢰해야 하지만 파일 분석 서버에 자신의 인증서를 제공할 필요는 없습니다.

(클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성

조직의 모든 콘텐츠 보안 어플라이언스가 Cisco Email Security Appliance 또는 Cisco Web Security Appliance에서 분석을 위해 전송한 파일에 대해 클라우드에서 파일 분석 결과 세부 정보를 볼 수 있게 하려면 모든 어플라이언스를 동일한 어플라이언스 그룹으로 묶어야 합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) **> Centralized Services**(중앙 서비스) **> Security Appliances**(보안 어플라이언스)를 선택합니다.

단계 **3** 파일 분석 섹션으로 스크롤합니다.

단계 **4** 관리 대상 어플라이언스가 다른 파일 분석 클라우드 서버에 지정된 경우 결과 세부사항을 표시할 서버를 선택합니다.

다른 클라우드 서버에서 처리하는 파일에 대해서는 결과 세부사항이 제공되지 않습니다.

단계 **5** 분석 그룹 ID를 입력합니다.

- 그룹 ID를 잘못 입력하거나 어떠한 이유로 인해 이를 변경해야 할 경우 Cisco TAC에서 케이스를 열어야 합니다.
- 이 변경사항은 즉시 적용되므로 커밋이 필요하지 않습니다.
- 이 값에 CCOID를 사용하는 것이 좋습니다.
- 이 값은 대/소문자를 구분합니다.
- 이 값은 분석을 위해 업로드된 파일에 대한 데이터를 공유하는 모든 어플라이언스에서 동일해야 합니다.
- 어플라이언스는 단 하나의 그룹에만 속할 수 있습니다.
- 언제든지 그룹에 머신을 추가할 수 있지만 한 번만 추가할 수 있습니다.

단계 **6** **Group Now**(지금 그룹화)를 클릭합니다.

단계 **7** 이 어플라이언스와 데이터를 공유할 각 Email Security Appliance에서 동일한 그룹을 구성합니다.

다음에 수행할 작업

관련 주제

클라우드에서 세부 파일 분석 결과를 볼 수 있는 파일은? , 99 페이지

(온프레미스 파일 분석) 파일 분석 계정 활성화

온프레미스 Cisco AMP Threat Grid 어플라이언스를 구축한 경우 Cisco Content Security Management Appliance에 대해 파일 분석 계정을 활성화해야 AMP Threat Grid 어플라이언스에서 제공하는 보고서 세부 정보를 볼 수 있습니다. 일반적으로 한 번만 하면 됩니다.

시작하기 전에

중대 레벨의 시스템 알림을 받아야 합니다.

단계 **1** 처음으로 Threat Grid 어플라이언스에서 파일 분석 보고서 세부사항에 액세스할 때 몇 분 기다리면 링크가 포함된 알림을 수신하게 됩니다.

이 링크를 받지 못한 경우 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Alerts**(알림)에서 **View Top Alerts**(상위 알림 보기)를 클릭합니다.

단계 **2** 알림 메시지에서 링크를 클릭합니다.

단계 **3** 관리 어플라이언스 계정을 활성화합니다.

추가 요구 사항

추가 요건은 다음에서 Security Management Appliance 릴리스용 릴리스 정보를 참조하십시오.
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

SHA-256 해시로 파일 식별

파일 이름을 쉽게 변경할 수 있으므로 어플라이언스가 보안 해시 알고리즘(SHA-256)을 사용하여 각 파일에 대해 식별자를 생성합니다. 어플라이언스가 이름이 다른 동일한 파일을 처리할 경우 모든 인스턴스가 동일한 SHA-256으로 인식됩니다. 여러 어플라이언스가 동일한 파일을 처리하는 경우 해당 파일의 모든 인스턴스에 동일한 SHA-256 식별자가 있습니다.

대부분의 보고서에서는 파일이 SHA-256 값(단축 형식)으로 나열됩니다.

다른 보고서의 파일 평판 필터링 데이터 보기

파일 평판 및 분석 데이터는 관련이 있는 경우 다른 보고서에서도 볼 수 있습니다. "Advanced Malware Protection에 의해 탐지됨" 열이 해당 보고서에서 기본적으로 숨겨질 수 있습니다. 추가 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

클라우드에서 세부 파일 분석 결과를 볼 수 있는 파일은?

퍼블릭 클라우드 파일 분석을 구축한 경우 파일 분석을 위해 어플라이언스 그룹에 추가된 모든 관리 대상 어플라이언스에서 업로드된 모든 파일의 세부 결과를 볼 수 있습니다.

관리 어플라이언스를 그룹에 추가했다면 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)** 페이지에서 버튼을 클릭하여 그룹에 속한 관리 대상 어플라이언스의 목록을 볼 수 있습니다.

분석 그룹의 어플라이언스는 파일 분석 클라이언트 ID로 식별됩니다. 특정 어플라이언스의 파일 분석 클라이언트 ID를 보려면 다음 위치에서 찾으십시오.

어플라이언스	파일 분석 클라이언트 **ID**의 위치
Email Security Appliance	**Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Web Security Appliance	**Security Services(보안 서비스) > Anti-Malware and Reputation(악성코드 차단 및 평판)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Cisco Content Security Management Appliance	**Management Appliance(관리 어플라이언스) > Centralized Services(중앙 서비스) > Security Appliances(보안 어플라이언스)** 페이지의 하단

관련 주제

- (클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성 , 94 페이지

Virus Filtering(바이러스 필터링) 페이지

Filtering(바이러스 필터링) 보고서 페이지는 네트워크에 유입되고 네트워크에서 전송되는 바이러스의 개요를 제공합니다. Virus Types(바이러스 유형) 페이지는 Email Security Appliance에서 실행 중인 바이러스 검사 엔진에 의해 탐지되고 Security Management Appliance에 표시되는 바이러스를 보여줍니다. 특정 바이러스에 대해 작업을 수행하려면 이 보고서를 사용합니다. 예를 들어 PDF 파일에 포함된 것으로 알려진 대량의 바이러스를 수신하고 있다면 PDF 첨부 파일이 있는 메시지를 격리하는 필터 작업을 만들 수 있습니다.

Security Management Appliance에서 Virus Filtering(바이러스 필터링) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Virus Filtering(바이러스 필터링)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

여러 바이러스 검사 엔진을 실행 중인 경우 Virus Filtering(바이러스 필터링) 보고서 페이지에는 활성화된 모든 바이러스 검사 엔진에서 온 결과가 포함됩니다. 페이지에 표시되는 바이러스의 이름은 바이러스 검사 엔진에서 확인한 이름입니다. 둘 이상의 검사 엔진에서 바이러스를 탐지하는 경우 동일한 바이러스에 대한 항목이 둘 이상 있을 수 있습니다.

다음 목록은 Virus Filtering(바이러스 필터링) 보고서 페이지의 여러 섹션을 설명합니다.

표 *30: Virus Filtering(*바이러스 필터링*)* 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
탐지된 상위 수신 바이러스 유형	이 섹션에는 네트워크로 전송된 메시지에서 탐지된 바이러스의 차트 보기가 표시됩니다.
탐지된 상위 발신 바이러스 유형	이 섹션에는 네트워크에서 전송된 메시지에서 탐지된 바이러스의 차트 보기가 표시됩니다.
바이러스 유형 세부사항	각 바이러스 유형의 세부사항을 표시하는 인터랙티브 테이블입니다. 자세한 내용은 Virus Types Detail(바이러스 유형 세부 정보) 테이블, 131 페이지을 참조해 주십시오.

참고 어떤 호스트에서 바이러스에 감염된 메시지를 네트워크로 전송했는지를 보려면 Incoming Mail(수신 메일) 페이지로 이동하고, 동일한 보고 기간을 지정하고, 바이러스 양성 메시지로 정렬합니다. 마찬가지로, 어떤 IP 주소가 네트워크 내에서 바이러스 양성 이메일을 전송했는지 알아보려면 Outgoing Senders(발신 발신자) 페이지로 이동하여 바이러스 양성 메시지를 기준으로 정렬할 수 있습니다.

Virus Filtering(바이러스 필터링) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

Virus Filtering(바이러스 필터링) 보고서 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Virus Types Detail(바이러스 유형 세부 정보) 테이블

Virus Types Detail(바이러스 유형 세부 정보) 테이블은 바이러스에 감염된 메시지의 총 수를 수신 및 발신 메시지별로 분류하여 표시하는 인터랙티브 테이블입니다. 데이터를 정렬하려면 열 머리글을 클릭합니다.

다음 표에는 Virus Types Detail(바이러스 유형 세부 정보) 테이블의 테이블 열 설명이 나와 있습니다.

표 *31: Virus Types Detail(*바이러스 유형 세부 정보*)* 테이블의 테이블 열 설명

열 이름	설명
바이러스 유형	바이러스 유형의 이름입니다.
수신 메시지	바이러스로 탐지된 수신 메시지의 수입니다.
발송 메시지	바이러스로 탐지된 발신 메시지의 수입니다.
감염된 총 메시지 수	감염된 메시지(수신 및 발신)의 총 수입니다.

Macro Detection(매크로 탐지) 페이지

Macro Detection(매크로 탐지) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 파일 형식별 상위 수신 매크로 사용 첨부 파일을 그래픽 형식과 표 형식으로 봅니다.
- 파일 형식별 총 수신 매크로 사용 첨부 파일을 표 형식으로 봅니다.
- 파일 형식별 상위 발신 매크로 사용 첨부 파일을 그래픽 형식과 표 형식으로 봅니다.
- 파일 형식별 총 발신 매크로 사용 첨부 파일을 표 형식으로 봅니다.

Security Management Appliance에서 Macro Detection(매크로 탐지) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Macro Detection(**매크로 탐지**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Macro Detection(매크로 탐지) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

매크로 사용 첨부 파일의 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.

참고 보고서 생성 시:

- 아카이브 파일 내에서 하나 이상의 매크로가 탐지되면 아카이브 파일 파일 형식이 1씩 증가합니다. 아카이브 파일 내 매크로 사용 첨부 파일의 수는 계산되지 않습니다.
- 내장 파일 내에서 하나 이상의 매크로가 탐지되면 상위 파일 형식이 1씩 증가합니다. 내장 파일 내 매크로 사용 첨부 파일의 수는 계산되지 않습니다.

DMARC Verification(DMARC 확인) 페이지

DMARC Verification(DMARC 확인) 보고서 페이지는 DMARC(Domain-based Message Authentication, Reporting and Conformance) 확인에 실패한 상위 발신자 도메인 및 그 도메인으로부터 수신한 메시지

에 대해 수행한 조치의 요약을 표시합니다. 이 보고서를 사용하면 DMARC 설정을 세부적으로 조정하고 다음과 같은 종류의 질문에 답할 수 있습니다.

- DMARC 검증을 통과하지 못한 메시지가 가장 많은 도메인은 무엇입니까?
- 각 도메인에서 DMARC 확인을 통과하지 못한 메시지에 대해 수행한 작업은 무엇입니까?

DMARC Verification(DMARC 확인) 보고서 페이지를 사용하면 다음 내용을 볼 수 있습니다.

- DMARC 확인 실패별 상위 도메인(그래픽 형식)
- DMARC 확인 세부 정보별 총 도메인(표 형식) 자세한 내용은 Domains by DMARC Verification Details(DMARC 확인 세부 정보별 도메인) 테이블, 133 페이지을 참고하십시오.

Security Management Appliance에서 DMARC Verification(DMARC 확인) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > DMARC Verification(DMARC** 확인**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 파란색 숫자 링크를 클릭합니다.

DMARC Verification(DMARC 확인) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

DMARC 확인에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서의 이메일 인증 장을 참조하십시오.

Domains by DMARC Verification Details(DMARC 확인 세부 정보별 도메인) 테이블

Domains by DMARC Verification Details(DMARC 확인 세부 정보별 도메인) 테이블은 DMARC(Domain-based Message Authentication, Reporting and Conformance) 확인에 실패(거부되거나, 격리되거나, 작업 없음), 시도, 통과한 발신자 도메인의 세부 정보를 표시하는 인터랙티브 테이블입니다.

테이블에 대한 정보를 맞춤화하고 정렬하려면 보고서 페이지의 테이블 맞춤화 , 52 페이지 섹션을 참조하십시오.

이 보고서에 기록되는 메시지 추적 세부 정보를 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

Outbreak Filtering(보안 침해 필터링) 페이지

Outbreak Filtering(보안 침해 필터링) 보고서 페이지는 Outbreak Filter에서 격리한 최근 보안 침해 및 메시지에 대한 정보를 제공합니다. 이 페이지를 사용하면 대상이 지정된 바이러스, 스캠 및 피싱 공격에 대한 방어를 모니터링할 수 있습니다.

다음 유형의 질문에 답하는 데 Outbreak Filtering(보안 침해 필터링) 보고서 페이지를 사용할 수 있습니다.

- 어떤 Outbreak Filters 규칙에 의해 몇 개의 메시지가 격리되어 있습니까?
- 메시지가 보안 침해 격리에 얼마나 머뭅니까?
- 어떤 잠재적 악성 URL이 가장 많이 나타납니까?

Security Management Appliance에서 Outbreak Filtering(보안 침해 필터링) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Outbreak Filtering(**보안 침해 필터링**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

다음 표에서 Outbreak Filtering(보안 침해 필터링) 보고서 페이지에서 여러 섹션을 설명합니다.

표 ***32: Outbreak Filtering(***보안 침해 필터링***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
Threats by Type(유형별 위협)	Threats by Type(유형별 위협) 섹션에는 어플라이언스에서 수신한 두 가지 유형의 위협 메시지가 표시됩니다.
위협 요약	Threat Summary(위협 요약) 섹션에는 Malware(악성코드), Phish(피싱), Scam(스캠) 및 Virus(바이러스)별로 구분된 메시지가 표시됩니다. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.
위협 세부 정보	Threat Details(위협 세부 정보) 인터랙티브 테이블에는 위협 카테고리(바이러스, 스캠 또는 피싱), 위협 이름, 위협 설명, 식별된 메시지 수를 포함하여 특정 보안 침해에 대한 정보가 표시됩니다. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.
Hit Messages from Incoming Messages(수신 메시지에서 적중된 메시지)	Hit Messages from Incoming Messages(수신 메시지에서 적중된 메시지) 섹션에는 선택한 기간에 Outbreak Filter로 처리한 수신 메시지 수의 차트 및 요약이 표시됩니다. 바이러스 외 위협 - 피싱 이메일, 스캠, 외부 웹 사이트 링크를 사용한 악성코드 배포.

섹션	설명
Hit Messages by Threat Level(위협 레벨별 적중 메시지)	Hit Messages by Threat Level(위협 레벨별 적중 메시지) 섹션에는 Outbreak Filter에 걸린 위협의 심각도의 차트와 요약이 표시됩니다. 레벨 5는 심각하거나 영향이 있는 위협인 반면, 레벨 1은 낮은 위협을 나타냅니다. 위협 레벨에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서를 참조하십시오.
Messages resided in Outbreak Quarantine(보안 침해 격리에 있는 메시지)	Messages resided in Outbreak Quarantine(보안 침해 격리에 있는 메시지)에는 보안 침해 격리에 소요된 시간 메시지의 길이가 표시됩니다. 시스템이 그 안정성에 대한 판정을 내리기 위해 잠재적 위협에 대한 충분한 데이터를 수집할 때까지 걸리는 시간으로 결정됩니다. 바이러스 위협 메시지는 격리 시간이 더 긴 편입니다. 안티바이러스 프로그램 업데이트를 기다려야 하기 때문입니다. 각 메일 정책에 대해 지정한 최대 보존 시간도 반영됩니다.
Top URL's Rewritten(상위 URL 재작성)	Top URL's Rewritten(상위 URL 재작성) 섹션에는 수신자가 메시지에서 잠재적 악성 링크를 클릭할 경우 클릭 시간 평가를 위해 메시지 수신자를 Cisco Web Security Proxy로 리디렉션하고자 가장 자주 재작성되는 URL이 표시됩니다. 이 목록은 악성이 아닌 URL을 포함할 수도 있습니다. 메시지의 어떤 URL이 악성으로 간주되면 모든 URL이 재작성되기 때문입니다. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

참고 Outbreak Filtering(보안 침해 필터링) 보고서 페이지의 테이블을 정확하게 작성하려면 어플라이언스에서 Cisco 업데이트 서버와 통신할 수 있어야 합니다.

자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서의 보안 침해 필터 장을 참조하십시오.

URL Filtering(URL 필터링) 페이지

URL Filtering(URL 필터링) 보고서는 수신 및 발신 메시지에 대해 사용 가능합니다.

URL 필터링 엔진으로 검사된(안티스팸/Outbreak Filter 검사의 일환으로 또는 메시지/콘텐츠 필터를 통해) 메시지만 이러한 모듈에 포함됩니다. 그러나 모든 결과가 URL 필터링 기능으로 인한 것이라 할 수는 없습니다.

참고 URL Filtering(URL 필터링) 보고서 모듈은 URL 필터링이 활성화된 경우에만 채워집니다.

URL Filtering(URL 필터링) 보고서 페이지에서 다음을 볼 수 있습니다.

- Top URL Categories(상위 URL 범주) 모듈은 검사된 메시지에서 발견된 모든 범주(콘텐츠 또는 메시지 필터와의 매치 여부와 상관없이)를 포함합니다.

  각 메시지는 오로지 평판 레벨 하나와 연결할 수 있습니다. 여러 URL이 포함된 메시지의 경우 통계는 메시지에 있는 URL의 최하 평판을 반영합니다.

- 상위 URL 스팸 메시지

  Email Security Appliance의 **Security Services(**보안 서비스**) > URL Filtering(URL** 필터링**)** 페이지에 구성된 전역 화이트리스트의 URL은 보고서에 포함되지 않습니다.

  개별 필터에서 사용되는 화이트리스트의 URL은 보고서에 포함됩니다.

- 악성 URL은 Outbreak Filter가 평판이 좋지 않다고 판단한 URL입니다. 일반 URL은 Outbreak Filter에서 클릭 시 보호가 필요하다고 결정한 URL입니다. 따라서 일반 URL은 Cisco Web Security 프록시로 리디렉션하도록 재작성되었습니다.

  URL 범주 기반 필터의 결과는 콘텐츠 및 메시지 필터 보고서에서 반영됩니다.

  Cisco Web Security 프록시에 의한 클릭 시 URL 평가의 결과는 보고서에 반영되지 않습니다.

Security Management Appliance에서 URL Filtering(URL 필터링) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > URL Filtering(URL** 필터링**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

다음 표에서 URL Filtering(URL 필터링) 보고서 페이지에서 여러 섹션을 설명합니다.

표 ***33: URL Filtering(URL*** 필터링***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
상위 URL 범주	이 섹션에는 수신 및 발신 메시지의 상위 URL 카테고리의 그래픽 보기와 요약이 표시됩니다. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

섹션	설명
상위 URL 스팸 메시지	이 섹션에는 상위 수신 및 발신 URL 스팸 메시지의 그래픽 보기와 요약이 표시됩니다.
악의적/중립 URL	이 섹션에는 수신 및 발신 메시지의 악의적 URL 및 중립 URL의 차트 보기와 요약이 표시됩니다. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

URL Filtering(URL 필터링) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

Forged Email Detection(위조 이메일 탐지) 페이지

Forged Email Detection(위조 이메일 탐지) 페이지에는 다음 보고서가 포함됩니다.

- **Top Forged Email Detection(**상위 위조 이메일 탐지**).** 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 사용자 상위 10명이 표시됩니다.
- **Forged Email Detection Details(**위조 이메일 탐지 세부 정보**).** 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 모든 사용자 목록과, 지정한 사용자에 대해 일치하는 메시지 수가 표시됩니다.

Security Management Appliance에서 Forged Email Detection(위조 이메일 탐지) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Forged Email Detection(**위조 이메일 탐지**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Forged Email Detection(위조 이메일 탐지) 보고서는 Forged Email Detection(위조 이메일 탐지) 콘텐츠 필터 또는 `forged-email-detection` 메시지 필터를 사용하는 경우에만 채워집니다.

Forged Email Detection(위조 이메일 탐지) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

External Threat Feeds(외부 위협 피드) 페이지

External Threat Feeds(외부 위협 피드) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 메시지에서 위협을 탐지하는 데 사용되는 그래픽 형식의 상위 ETF 소스
- 메시지에서 위협을 탐지하는 데 사용되는 표 형식의 ETF 소스 요약
- 메시지에서 탐지된 위협과 일치하는 그래픽 형식의 상위 IOC
- 악의적인 수신 메일 연결을 필터링하는 데 사용되는 그래픽 형식의 상위 ETF 소스

- 악의적인 수신 메일 연결을 필터링하는 데 사용되는 표 형식의 ETF 소스 요약

'Summary of External Threat Feed Sources(외부 위협 피드 소스 요약)' 섹션에서 다음 작업을 수행할 수 있습니다.

- 특정 ETF 소스에 대한 메시지 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.
- 특정 위협 피드 소스를 클릭하여 IOC를 기준으로 ETF 소스의 배포를 볼 수 있습니다.

'Summary of Indicator of Compromise (IOC) Matches(IOC(Indicator of Compromise) 매치 요약)' 섹션에서 다음 작업을 수행할 수 있습니다.

- 특정 ETF 소스에 대한 IOC 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.
- 특정 IOC를 클릭하여 ETF 소스를 기준으로 IOC 배포를 볼 수 있습니다.

Security Management Appliance에서 External Threat Feeds(외부 위협 피드) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > External Threat Feeds(외부 위협 피드)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지를 참고하십시오.

Sender Domain Reputation(발신인 도메인 평판) 페이지

Sender Domain Reputation(발신자 도메인 평판 보고서) 페이지를 사용하여 다음을 볼 수 있습니다.

- SDR 서비스에서 받은 판정에 기반한 수신 메시지를 그래픽 형식으로 봅니다.
- SDR 서비스에서 받은 위협 카테고리 및 판정에 기반한 수신 메시지를 표 형식으로 봅니다.
- SDR 서비스에서 받은 위협 카테고리에 기반한 수신 메시지를 그래픽 형식으로 봅니다.

참고 SDR 판정이 '매우 나쁨' 또는 '나쁨'인 메시지만 '스팸', '악성' 등과 같은 SDR 위협 카테고리에 따라 분류됩니다.

- SDR 서비스에서 받은 위협 카테고리에 기반한 수신 메시지를 표 형식으로 봅니다.

Security Management Appliance에서 Sender Domain Reputation(발신인 도메인 평판) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Sender Domain Reputation(발신인 도메인 평판)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지를 참고하십시오.

Mail Flow Details(메일 플로우 세부 정보) 페이지

Security Management Appliance의 Mail Flow Details(메일 플로우 세부 정보) 페이지는 관리되는 Security Management Appliance에 연결된 모든 원격 호스트의 실시간 정보에 대한 인터랙티브 보고를 제공합니다. IP 주소, 도메인, 시스템에 메일을 전송하는 네트워크 소유자(조직)에 대한 정보를 수집할 수 있습니다. 발신 발신자의 IP 주소 및 도메인에 대한 정보도 수집할 수 있습니다.

Security Management Appliance에서 Mail Flow Details(메일 플로우 세부 정보) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email**(이메일)을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring**(모니터링) **> Mail Flow Details**(메일 플로우 세부 정보)를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Mail Flow Details(메일 플로우 세부 정보) 보고서 페이지에는 다음 탭이 있습니다.

- 수신 메일
- Outgoing Senders(발신 발신자)

데이터 내에서 특정 정보를 검색하려면 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.

Incoming Mails(수신 메일) 탭에서는 다음 작업을 수행할 수 있습니다.

- 총 위협 메시지별 상위 발신자를 그래픽 형식으로 봅니다.
- 정상 메시지별 상위 발신자를 그래픽 형식으로 봅니다.
- 그래픽 형식으로 그레이메일 메시지별 상위 발신자를 그래픽 형식으로 봅니다.
- Security Management Appliance로 메일을 보낸 IP 주소, 도메인 또는 네트워크 소유자(조직)를 봅니다.
- 어플라이언스에 메일을 보낸 발신자에 대한 세부 통계를 확인합니다. 이 통계에는 연결 수(수락된 연결 또는 거부된 연결), 시도된 메시지 수를 보안 서비스(발신자 평판 필터링, 안티 스팸, 안티바이러스 등)별로 구분한 수, 총 위협 메시지 수, 총 그레이메일 수 및 정상 메시지 수가 포함됩니다.
- 특정 IP 주소, 도메인 또는 네트워크 소유자(조직)에 대한 자세한 정보는 Incoming Mail Details(수신 메일 세부 정보) 인터랙티브 테이블에서 확인하십시오. 자세한 내용은 수신 메일 테이블, 141 페이지을 참고하십시오.

  사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 숫자 하이퍼링크를 클릭합니다.

Outgoing Senders(발신 발신자) 탭에서는 다음 작업을 수행할 수 있습니다.

- 총 위협 메시지별 상위 발신자를 그래픽 형식으로 봅니다.
- 정상 메시지별 상위 발신자를 그래픽 형식으로 봅니다.
- 이 조직에서 보낸 발신 위협 메시지(스팸, 안티바이러스 등)의 상위 발신자(IP 주소 또는 도메인 기준)를 봅니다.
- 어플라이언스에서 메일을 보낸 발신자에 대한 세부 통계를 봅니다. 이 통계에는 총 위협 메시지 보안 서비스(수를 발신자 평판 필터링, 안티 스팸, 안티바이러스 등)별로 구분한 수와 정상 메시지 수가 포함됩니다.
- 특정 IP 주소 또는 도메인에 대한 자세한 정보는 Sender Details(발신자 세부 정보) 인터랙티브 테이블에서 확인하십시오. 자세한 내용은 Sender Details(발신자 세부 정보) 테이블, 145 페이지을 참고하십시오.

사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 숫자 하이퍼링크를 클릭합니다.

관련 주제

- "No Domain Information(도메인 정보 없음)" 링크, 79 페이지
- 메일 추세 그래프의 시간 범위, 80 페이지
- Mail Flow Details(메일 플로우 세부 정보) 페이지에서 보기, 140 페이지
- 수신 메일 테이블, 141 페이지
- Sender Details(발신자 세부 정보) 테이블, 145 페이지

Mail Flow Details(메일 플로우 세부 정보) 페이지에서 보기

Mail Flow Details(메일 플로우 세부 정보): Incoming(수신) 보고서 페이지에는 다음 3가지 보기가 있습니다.

- IP 주소
- 도메인
- 네트워크 소유자

시스템에 연결된 원격 호스트를 해당 보기의 관점에서 조명합니다.

또한 Mail Flow Details(메일 플로우 세부 정보) 페이지의 Incoming Mail(수신 메일) 테이블에서 발신자 IP 주소, 도메인 이름, 네트워크 소유자 정보를 클릭하여 구체적인 발신자 프로필 정보를 얻을 수도 있습니다. 발신자 프로필에 대한 자세한 내용은 발신자 프로필 페이지, 80 페이지를 참조하십시오.

참고 Network owners(네트워크 소유자)는 도메인을 보유한 엔티티입니다. 도메인은 IP 주소를 포함하는 엔티티입니다.

선택한 보기에 따라 Incoming Mail Details(수신 메일 세부사항) 인터랙티브 테이블에는 Email Security Appliance에 구성된 모든 퍼블릭 리스너에 메일을 전송한 상위 IP 주소, 도메인 또는 네트워크 소유자가 표시됩니다. 어플라이언스로 가는 모든 메일의 플로우를 모니터링할 수 있습니다.

Sender Profile(발신자 프로필) 페이지에서 발신자에 대한 세부사항에 액세스하려면 IP 주소, 도메인 또는 네트워크 소유자를 클릭합니다. 발신자 프로필 페이지는 특정 IP 주소, 도메인, 네트워크 소유자에 한정된 Mail Flow Details(메일 플로우 세부 정보) 페이지입니다.

Incoming Mail(수신 메일) 인터랙티브 테이블에 포함된 데이터에 대한 설명은 수신 메일 테이블, 141 페이지 섹션을 참조하십시오.

Mail Flow Details(메일 플로우 세부 정보) 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

참고 Mail Flow Details(메일 플로우 세부 정보) 보고서 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Mail Flow Details(메일 플로우 세부 정보): Outgoing(발신) 보고서 페이지에는 다음 2가지 보기가 있습니다.

- IP 주소
- 도메인

시스템에 연결된 원격 호스트를 해당 보기의 관점에서 조명합니다.

선택한 보기에 따라 Sender Details(발신자 세부 정보) 인터랙티브 테이블에는 Email Security Appliance에 구성된 퍼블릭 리스너에서 메일을 전송한 발신자의 상위 IP 주소 또는 도메인이 표시됩니다. 어플라이언스에서 받은 모든 메일의 플로우를 모니터링할 수 있습니다.

Sender Details(발신자 세부 정보) 인터랙티브 테이블에 포함된 데이터에 대한 설명은 Sender Details(발신자 세부 정보) 테이블, 145 페이지를 참조하십시오.

"No Domain Information(도메인 정보 없음)" 링크

Security Management Appliance와 연결되어 있으며 이중 DNS 조회로 확인할 수 없는 도메인은 자동으로 특수 도메인인 "No Domain Information(도메인 정보 없음)"으로 그룹화됩니다. Sender Verification(발신자 확인)을 통해 이런 유형의 확인되지 않은 호스트를 관리하는 방법을 제어할 수 있습니다. Sender Verification(발신자 확인)에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

Items Displayed(표시 항목) 메뉴를 사용하여 목록에 표시할 발신자 수를 선택할 수 있습니다.

메일 추세 그래프의 시간 범위

다양한 세부 수준을 선택하여 메일 그래프로 데이터를 표시할 수 있습니다. 동일한 데이터에 대해 일, 주, 월, 연도 보기를 선택할 수 있습니다. 데이터는 실시간으로 모니터링되므로, 데이터베이스에서 주기적으로 정보가 업데이트 및 요약됩니다.

시간 범위에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.

수신 메일 테이블

Mail FLow Details(메일 플로우 세부 정보): Incoming Mail(수신 메일) 페이지 하단에 있는 인터랙티브 Incoming Mail Details(수신 메일 세부 정보) 테이블에는 Email Security Appliance의 퍼블릭 리스너에 연결된 상위 발신자가 나열됩니다. 선택한 보기에 따라 도메인, IP 주소 또는 네트워크 소유자가 테이블에 표시됩니다.

이중 DNS 조회를 통해 원격 호스트의 IP 주소를 확보하고 그 유효성을 확인합니다. 이중 *DNS* 조회 및 발신자 확인에 대한 자세한 내용은 AsyncOS Email Security Appliance 사용 설명서 또는 온라인 도움말을 참조하십시오.

발신자의 경우 수신 메일 테이블의 첫 열에 나열된 네트워크 소유자, IP 주소 또는 도메인입니다. 또는 Top Senders by Total Threat Message(총 위협 메시지별 상위 발신자)에서는 Sender(발신자) 또는 No Domain Information(도메인 정보 없음) 링크를 클릭하여 발신자에 대한 추가 정보를 표시합니다. 그 결과는 Sender Profile(발신자 프로필) 페이지에 나타납니다. 여기에는 SenderBase Reputation Service의 실시간 정보도 포함되어 있습니다. 발신자 프로필 페이지에서 특정 IP 주소 또는 네트워크 소유자에 대한 추가 정보를 볼 수 있습니다. 자세한 내용은 발신자 프로필 페이지, 80 페이지을 참조하십시오.

Mail FLow Details(메일 플로우 세부 정보) 페이지의 맨 아래에서 Sender Groups(발신자 그룹) 보고서를 클릭하여 발신자 그룹 보고서를 표시할 수도 있습니다. 발신자 그룹 보고서 페이지에 대한 자세한 내용은 Sender Groups(발신자 그룹) 페이지, 146 페이지를 참조하십시오.

이 보고서에서 메시지 추적 세부 정보를 보려면 테이블에서 숫자 하이퍼링크를 클릭합니다.

다음 표는 수신 메일 테이블에 대한 테이블 열 설명을 보여줍니다.

표 ***34:*** 수신 메일 테이블에 대한 테이블 열 설명

열 이름	설명
발신자 도메인(도메인)	발신자의 도메인 이름입니다.
발신자 IP 주소(IP 주소)	발신자의 IP 주소입니다.
호스트 이름(IP 주소)	발신자의 호스트 이름입니다.
DNS 확인됨(IP 주소)	DNS가 확인하는 IP 주소입니다.
SBRS(IP 주소)	발신자의 SenderBase 평판 점수입니다.
마지막 발신자 그룹(IP 주소)	마지막 발신자 그룹의 세부사항이 있습니다.
마지막 발신자 그룹(IP 주소)	마지막 발신자 그룹의 세부사항이 있습니다.
네트워크 소유자(네트워크 소유자)	발신자의 네트워크 소유자입니다.
거부된 연결(도메인 및 네트워크 소유자)	HAT 정책에 의해 차단된 모든 연결. 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다.
수락된 연결(도메인 및 네트워크 소유자)	허용된 모든 연결.

열 이름	설명
총 시도 수	시도하여 수락된 또는 차단된 모든 연결.
수신자 제한에 의한 차단(도메인 및 네트워크 소유자)	Stopped by Reputation Filtering(평판 필터링에 의해 차단됨) 구성 요소입니다. 시간당 최대 수신자 수, 메시지당 최대 수신자 수 또는 연결당 최대 메시지 수 등 HAT 제한 중 하나가 초과되어 차단된 수신자 메시지 수를 나타냅니다. 이 수는 거부된 또는 TCP 거절된 연결과 관련이 있는 수신자 메시지의 추정치와 합산되어 Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)을 산출합니다.
평판 필터링에 따른 차단	Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)에 대한 값은 여러 요인을 기반으로 계산됩니다. • 해당 발신자가 보낸 "제한된(throttled)" 메시지의 수 • 거부된 또는 TCP 거절된 연결의 수(부분 개수일 수 있음) • 연결당 메시지 수에 대한 보수적 승수 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다. 이 상황에서는 표시된 값을 "바닥(floor)"으로 해석할 수 있습니다. 즉 최소한 이 개수의 메시지가 차단된 것입니다. 참고 Mail Flow Summary(메일 플로우 요약) 페이지의 Reputation Filtering(평판 필터링) 합계는 항상 거부된 모든 연결의 전체 개수를 기반으로 합니다. 발신자 기준 연결 개수만 부하 때문에 제한됩니다.
올바르지 않은 수신자로 차단됨	대화형 LDAP 거부에 의해 거부된 모든 수신자와 모든 RAT 거부를 더한 수
탐지된 스팸	탐지된 모든 스팸.
탐지된 바이러스	탐지된 모든 바이러스
AMP에서 탐지	Advanced Malware Protection 엔진에서 탐지된 메시지의 총 수입니다.
콘텐츠 필터에 의해 차단됨	콘텐츠 필터에 의해 차단된 총 메시지 수입니다.
DMARC에 의해 차단됨	DMARC(Domain-Based Message Authentication, Reporting, and Conformance) 확인에 실패한 총 메시지 수입니다.
총 위협	총 위협 메시지 수(평판에 의해 차단됨, 잘못된 수신자, 스팸 및 바이러스로 분류되어 차단됨).
마케팅	원치 않은 마케팅 메시지로 탐지된 메시지 수.

열 이름	설명
소셜	소셜 메시지로 탐지된 메시지 수입니다.
대량	벌크로 탐지된 메시지의 수입니다.
총 그레이메일	그레이메일로 탐지된 메시지의 수입니다.
정상	모든 정상 메시지. 그레이메일 기능이 활성화되지 않은 어플라이언스에서 처리된 메시지는 정상으로 분류됩니다.

발신자 프로필 페이지

Mail Flow Details(메일 흐름 상세정보**)**[새로운 웹 인터페이스] 또는 **Incoming Mail(**수신 메일**)** 페이지의 Incoming Mail 인터랙티브 테이블에서 발신자를 클릭하면 Sender Profile(발신자 프로파일) 페이지가 나타납니다. 특정 IP 주소, 도메인, 네트워크 소유자(조직)에 대한 세부 정보를 표시합니다. 임의의 IP 주소, 도메인, 네트워크 소유자에 대한 발신자 프로필 페이지는 Mail Flow Details(메일 플로우 세부 정보) 페이지 또는 다른 발신자 프로필 페이지의 맨 위에 있는 해당 링크를 클릭하여 액세스할 수 있습니다.

*Network owners(*네트워크 소유자*)*는 도메인을 보유한 엔티티입니다. *Domains(*도메인*)*은 IP 주소를 보유한 엔티티입니다.

IP 주소, 네트워크 소유자, 도메인에 대해 표시되는 발신자 프로필 페이지는 약간 다릅니다. 각 페이지에는 해당 발신자가 보낸 수신 메일에 대한 그래프 및 요약 테이블이 포함됩니다. 그래프 아래의 테이블에는 발신자와 연결된 도메인 또는 IP 주소가 나열되어 있습니다. 개별 IP 주소에 대한 발신자 프로필 페이지는 더 세부적인 목록이 없습니다. 발신자 프로필 페이지에는 현재 SenderBase, 발신자 그룹, 네트워크 정보와 관련된 정보 섹션도 있습니다.

- 네트워크 소유자 프로필 페이지에는 네트워크 소유자는 물론 네트워크 소유자와 연결된 도메인 및 IP 주소에 대한 정보가 포함됩니다.
- 도메인 프로필 페이지에는 도메인 및 해당 도메인과 연결된 IP 주소에 대한 정보가 포함됩니다.
- IP 주소 프로필 페이지에는 IP 주소에 대한 정보만 포함되어 있습니다.

각 발신자 프로필 페이지의 하단에 있는 Current Information(현재 정보) 테이블에는 다음 데이터가 포함됩니다.

- SenderBase Reputation Service에서 제공하는 전역 정보:
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자
  - 네트워크 소유자 범주(네트워크 소유자만)
  - CIDR 범위(IP 주소만)
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자에 대한 일일 규모 및 월간 규모
  - 해당 발신자로부터 첫 메시지를 수신한 후 경과일

- 마지막 발신자 그룹 및 DNS 확인 여부(IP 주소 발신자 프로필 페이지만)

일일 규모는 지난 24시간 동안 도메인이 보낸 메시지 수 측정값입니다. 리히터 지진계가 지진을 측정하는 것과 마찬가지로 SenderBase 규모는 10을 기준으로 로그 스케일을 사용하여 계산된 메시지 볼륨 측정치입니다. 이론상 최대 스케일 값은 10으로 설정되며, 이는 세계 이메일 메시지 볼륨의 100%와 같습니다. 로그 스케일을 사용할 경우, 규모가 1 증가하는 것은 실제 볼륨이 10배 증가하는 것과 같습니다.

월간 규모는 일일 규모와 동일한 접근법을 사용하여 계산되지만, 비율이 지난 30일 동안 전송된 이메일의 볼륨을 기반으로 계산된다는 점만 다릅니다.

- 평균 규모(IP 주소만)
- 수명 주기 볼륨/30일 볼륨(IP 주소 프로필 페이지만)
- Bonded Sender 상태(IP 주소 프로필 페이지만)
- SenderBase Reputation Score(IP 주소 프로필 페이지만)
- 첫 메시지 이후 경과일(네트워크 소유자 및 도메인 프로필 페이지만)
- 이 네트워크 소유자와 연결된 도메인의 수(네트워크 소유자 및 도메인 프로필 페이지만)
- 이 네트워크 소유자의 IP 주소 수(네트워크 소유자 및 도메인 프로필 페이지만)
- 이메일 전송에 사용된 IP 주소 수(네트워크 소유자 페이지만)

SenderBase Reputation Service에서 제공하는 모든 정보가 포함된 페이지를 보려면 **More from SenderBase(SenderBase**에서 더 보기**)**를 클릭합니다.

- 이 네트워크 소유자가 제어하는 도메인 및 IP 주소에 대한 세부사항은 네트워크 소유자 프로필 페이지에 표시됩니다. 도메인의 IP 주소에 대한 세부사항은 도메인 페이지에 표시됩니다.

도메인 프로필 페이지에서 특정 IP 주소를 클릭하여 특정 정보를 보거나 조직 프로필 페이지를 볼 수 있습니다.

Sender Details(발신자 세부 정보) 테이블

Mail FLow Details(메일 플로우 세부 정보): Outgoing(발신) 페이지 하단에 있는 인터랙티브 Sender Details(발신자 세부 정보) 테이블에는 Email Security Appliance의 퍼블릭 리스너에 연결된 상위 발신자가 나열됩니다. 선택한 보기에 따라 도메인 또는 IP 주소가 테이블에 표시됩니다.

이 보고서에서 메시지 추적 세부사항을 보려면 테이블에서 숫자 하이퍼링크를 클릭합니다.

다음 표에는 Sender Details(발신자 세부 정보) 테이블의 테이블 열 설명이 나와 있습니다.

표 ***35: Sender Details(***발신자 세부 정보***)*** 테이블의 테이블 열 설명

열 이름	설명
발신자 도메인(도메인)	발신자의 도메인 이름입니다.
발신자 IP 주소(IP 주소)	발신자의 IP 주소입니다.

열 이름	설명
호스트 이름(IP 주소)	발신자의 호스트 이름입니다.
탐지된 스팸	탐지된 모든 스팸.
탐지된 바이러스	탐지된 모든 바이러스입니다.
AMP에서 탐지	Advanced Malware Protection 엔진에서 탐지된 메시지의 총 수입니다.
콘텐츠 필터에 의해 차단됨	콘텐츠 필터에 의해 차단된 총 메시지 수입니다.
DLP에 의해 중지됨	DLP 엔진에 의해 중단된 총 메시지 수입니다.
총 위협	위협 메시지(스팸, 바이러스)의 총 수입니다.
정상	모든 정상 메시지. 그레이메일 기능이 활성화되지 않은 어플라이언스에서 처리된 메시지는 정상으로 분류됩니다.
총 메시지 수	모든 메시지의 총 수입니다.

Sender Groups(발신자 그룹) 페이지

Sender Groups(발신자 그룹) 보고서 페이지는 발신자 그룹 및 메일 플로우 정책 작업별로 연결 요약을 제공하므로, SMTP 연결 및 메일 플로우 정책 추세를 검토할 수 있습니다. Mail Flow by Sender Group(발신자 그룹별 메일 플로우) 목록은 각 발신자 그룹에 대한 연결 비율과 수를 보여줍니다. Connections by Mail Flow Policy Action(메일 플로우 정책 작업별 연결) 차트는 각 메일 플로우 정책 작업에 대한 연결의 비율을 보여줍니다. 이 페이지는 HAT(Host Access Table) 정책 효과의 개요를 제공합니다. HAT에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

Security Management Appliance에서 Sender Groups(발신자 그룹) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Sender Groups(발신자 그룹)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Sender Groups(발신자 그룹) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

참고 발신자 그룹 보고서 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Outgoing Destinations(발신 대상) 페이지

Outgoing Destinations(발신 목적지) 보고서 페이지는 여기서 보내는 메일의 도메인에 대한 정보를 제공합니다.

Outgoing Destinations(발신 대상) 페이지를 사용하면 다음 정보를 볼 수 있습니다.

- Email Security Appliance가 어떤 도메인으로 메시지를 전송합니까?
- 각 도메인에 전송되는 메시지 수가 얼마나 많습니까?
- 이 메시지 중에 콘텐츠 필터에 의해 중단된 메일, 악성코드, 바이러스 양성, 스팸 양성 또는 정상 메일은 얼마나 됩니까?
- 전달된 메시지는 몇 개이며 목적지 서버에 의해 하드 반송된 메시지는 몇 개입니까?

Security Management Appliance에서 Outgoing Destinations(발신 대상) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Outgoing Destinations(발신 대상)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

데이터 내에서 특정 정보를 검색하려면 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.

다음 목록은 Outgoing Destinations(발신 대상) 보고서 페이지의 여러 섹션을 설명합니다.

표 ***36: Outgoing Destinations(***발신 대상***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
총 위협 메시지별 상위 대상	이 조직에서 보낸 발신 위협 메시지(스팸, 안티바이러스 등)의 상위 목적지 도메인. 위협 메시지 합계에는 스팸 또는 바이러스 양성이거나 콘텐츠 필터에서 트리거한 메시지가 포함됩니다.
정상 메시지별 상위 대상	이 조직에서 보낸 발신 정상 메시지의 상위 목적지 도메인.

섹션	설명
Outgoing Destinations Details(발신 대상 세부 정보)	이 조직에서 보낸 모든 발신 메시지의 목적지 도메인 관련 세부사항을 총 수신자 기준으로 정렬한 것. 탐지된 스팸, 바이러스, 정상 메시지 등이 포함됩니다. 자세한 내용은 Outgoing Destinations Detail(발신 대상 세부 정보) 테이블, 148 페이지을 참고하십시오. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

Outgoing Destinations(발신 대상) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

발신 목적지 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

관련 주제

Outgoing Destinations Detail(발신 대상 세부 정보) 테이블, 148 페이지

Outgoing Destinations Detail(발신 대상 세부 정보) 테이블

Outgoing Destinations Detail(발신 대상 세부 정보) 테이블은 처리되고 전달되는 메시지의 총 수와 함께 위협(스팸, 바이러스 등) 또는 정상으로 처리되는 메시지와 하드 반송되거나 전달되는 메시지를 분류하여 표시하는 인터랙티브 테이블입니다. 데이터를 정렬하려면 열 머리글을 클릭합니다.

이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

다음 표에는 Outgoing Destinations Detail(발신 대상 세부 정보) 테이블의 테이블 열 설명이 나와 있습니다.

표 ***37: Outgoing Destinations Detail(***발신 대상 세부 정보***)*** 테이블의 테이블 열 설명

열 이름	설명
대상 도메인	대상 도메인의 이름입니다.
탐지된 스팸	스팸으로 탐지된 메시지의 수입니다.
탐지된 바이러스	스팸으로 탐지된 메시지의 수입니다.
콘텐츠 필터에 의해 차단됨	콘텐츠 필터에 의해 중단된 메시지의 수입니다.
총 위협	위협(스팸, 바이러스 등)으로 탐지된 메시지의 총 수
정상	정상으로 탐지된 메시지의 수입니다.

열 이름	설명
처리된 총 메시지 수	위협 또는 정상으로 처리된 메시지의 총 수입니다.
하드 바운스됨	영구적으로 전달할 수 없는 것으로 표시되는 메시지의 수입니다.
배달됨	전달되는 메시지의 수입니다.
배달된 총 메시지 수	전달(하드 반송 포함)되는 메시지의 총 수입니다.

TLS Encryption(TLS 암호화) 페이지

TLS Encryption(TLS 암호화) 페이지는 주고받은 메일에 대한 TLS 연결의 전체 사용량을 보여줍니다. 보고서에서는 또한 TLS 연결을 사용하여 메일을 전송하는 각 도메인에 대한 세부사항도 보여줍니다.

TLS Connections(TLS 연결) 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- 전반적으로 어떤 수신 및 발신 연결 부분에서 TLS를 사용합니까?
- 어떤 파트너와의 TLS 연결에 성공했습니까?
- 어떤 파트너와의 TLS 연결에 실패했습니까?
- DANE 지원을 사용하여 어떤 파트너와의 발신 TLS 연결에 성공했습니까?
- DANE 지원을 사용하여 어떤 파트너와의 TLS 연결에 실패했습니까?
- 어떤 파트너가 TLS 인증서에 문제가 있습니까?
- 파트너별 TLS를 사용하는 전체 메일 비율은 어떻게 됩니까?

Security Management Appliance에서 TLS Encryption(TLS 암호화) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > TLS Encryption(TLS 암호화)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

TLS Encryption(TLS 암호화) 보고서 페이지에는 다음 탭이 있습니다.

- Incoming
- Outgoing

데이터 내에서 특정 정보를 검색하려면 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.

다음 목록은 TLS Encryption(TLS 암호화) 보고서 페이지의 여러 섹션을 설명합니다.

표 ***38: TLS Encryption(TLS 암호화) 페이지의 세부 정보***

시간 범위(드롭다운 목록)	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.

(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
TLS 연결 그래프	TLS Encryption(TLS 암호화): 수신 페이지에는 선택한 기간에 따라 지난 시간, 전날, 전주, 전달의 암호화된/암호화되지 않은 수신 TLS 연결이 그래프 보기로 표시됩니다. TLS Encryption(TLS 암호화): 발신 페이지에는 선택한 기간에 따라 지난 시간, 전날, 전주, 전달의 암호화된/암호화되지 않은 발신 TLS 연결이 그래프 보기로 표시됩니다.
TLS 연결 요약	TLS Encryption(TLS 암호화): 수신 페이지에는 총 메시지 볼륨, 암호화된/암호화되지 않은 메시지의 볼륨, 성공한/실패한 TLS 암호화 메시지 볼륨이 표시됩니다. TLS Encryption(TLS 암호화): 발신 페이지에는 발신 메시지의 총 볼륨, 암호화된/암호화되지 않은 메시지의 볼륨, 성공한/실패한 발신 TLS 암호화 메시지의 볼륨, DANE 지원을 사용하여 성공한/실패한 발신 TLS 연결의 볼륨이 표시됩니다.
TLS 메시지	TLS Encryption(TLS 암호화): 수신 페이지에는 암호화된/암호화되지 않은 수신 TLS 메시지의 총 수와 백분율이 차트 보기로 표시됩니다. TLS Encryption(TLS 암호화): 발신 페이지에는 암호화된/암호화되지 않은 발신 TLS 메시지의 총 수와 백분율이 차트 보기로 표시됩니다.
TLS 메시지 요약	이 테이블에는 암호화된/암호화되지 않은 수신 및 발신 TLS 메시지의 총 수와 백분율의 요약이 표시됩니다.
TLS 연결 세부 정보	암호화된 메시지를 보내거나 받는 도메인에 대한 세부 정보가 이 테이블에 표시됩니다. 각 도메인에 대해 총연결 수, 전송한 메시지 수, 성공하거나 실패한 TLS 연결 수를 볼 수 있습니다. 각 도메인에서 성공한 연결 및 실패한 연결의 비율도 볼 수 있습니다. 자세한 내용은 TLS Connections Details(TLS 연결 세부 정보) 테이블, 151 페이지를 참고하십시오.

관련 주제

TLS Connections Details(TLS 연결 세부 정보) 테이블, 151 페이지

TLS Connections Details(TLS 연결 세부 정보) 테이블

TLS Connections Details(TLS 연결 세부 정보) 테이블은 총 연결 수, 전송된 메시지, 성공 또는 실패한 TLS 연결 수, 수신 및 발신 메시지의 마지막 TLS 상태를 보여주는 인터랙티브 테이블입니다. 각 도메인에서 성공한 연결 및 실패한 연결의 비율도 볼 수 있습니다.

다음 표에는 TLS Connections Details(TLS 연결 세부 정보) 테이블의 테이블 열 설명이 나와 있습니다.

표 ***39: TLS Connections Details(TLS*** 연결 세부 정보***)*** 테이블의 테이블 열 설명

열 이름	설명
도메인	발신자의 도메인 이름.
TLS Req. Failed(TLS 필수 실패)	실패한 모든 필수 TLS 연결.
TLS Req. Success(TLS 필수 성공)	성공한 모든 필수 TLS 연결.
TLS Pref. Failed(TLS 기본 설정 실패)	실패한 모든 선호 TLS 연결.
TLS Pref. Success(TLS 기본 설정 성공)	성공한 모든 선호 TLS 연결.
최근 TLS 상태	다음 기준으로 매핑된 TLS 연결의 상태. • 0: 해당 사항 없음 • 1: 필수 - 실패 • 2: 권장 - 실패 • 3: 필수 - 성공 • 4: 권장 - 성공
DANE 오류	DANE 지원을 사용하여 실패한 총 발신 TLS 연결 수.
DANE 성공	DANE 지원을 사용하여 성공한 총 발신 TLS 연결 수.
Total TLS Connections(총 TLS 연결)	총 TLS 연결 수.
암호화되지 않은 연결	암호화되지 않은 총 TLS 연결 수.
% TLS of all Connections(모든 연결의 % TLS)	모든 TLS 연결에 대 한 TLS 암호화의 비율.

열 이름	설명
Messages by TLS(TLS별 메시지)	총 TLS 메시지 수.

Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지

Inbound SMTP authentication(인바운드 SMTP 인증) 보고서 페이지는 클라이언트 인증서의 사용 및 ESA와 사용자 메일 클라이언트 간 SMTP 세션 인증을 위한 SMTP AUTH 명령을 보여줍니다. 어플라이언스는 인증서 및 SMTP AUTH 명령을 수락하는 경우 메일 클라이언트에 대한 TLS 연결을 설정합니다. 클라이언트는 메시지를 전송하는 데 이 연결을 사용합니다. 어플라이언스는 사용자 단위로 이러한 시도를 추적할 수 없으므로, 보고서는 도메인 이름 및 도메인 IP 주소를 기반으로 SMTP 인증에 대한 세부사항을 표시합니다.

이 보고서를 사용하면 다음 정보를 확인할 수 있습니다.

- 전체적으로 SMTP 인증을 사용하는 수신 연결은 몇 개입니까?
- 인증된 클라이언트를 사용하는 연결은 몇 개입니까?
- SMTP AUTH를 사용하는 연결은 몇 개입니까?
- SMTP 인증을 사용하려고 시도할 때 어떤 도메인이 연결에 실패합니까?
- SMTP 인증에 실패할 때 대안을 사용하여 성공한 연결은 몇 개입니까?

Security Management Appliance에서 Inbound SMTP Authentication(인바운드 SMTP 인증) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Inbound SMTP Authentication(인바운드 SMTP 인증)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

인바운드 SMTP 인증에는 다음 두 가지 보기가 있습니다.

- 도메인
- IP 주소

SMTP 인증을 선택한 보기의 관점에서 조명합니다.

Inbound SMTP Authentication(인바운드 SMTP 인증) 보고서 페이지에는 수신된 연결에 대한 그래프, SMTP 인증 연결을 시도하여 수신된 수신자에 대한 그래프, 그리고 연결 인증 시도에 대한 세부 정보를 보여주는 테이블이 포함되어 있습니다.

다음 목록은 Inbound SMTP Authentication(인바운드 SMTP 인증) 보고서 페이지의 여러 섹션을 설명합니다.

표 *40: Inbound SMTP Authentication(*인바운드 *SMTP* 인증*)* 페이지에 대한 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
수신된 연결 그래프	Received Connections(수신된 연결) 그래프는 지정한 시간 범위 동안 SMTP 인증을 사용하여 연결을 인증하려고 시도한 메일 클라이언트로부터의 수신 연결을 보여줍니다. 이 그래프에는 어플라이언스가 수신한 총 연결 수, SMTP 인증을 사용하여 인증하려고 시도하지 않은 횟수, 클라이언트 인증서를 사용하여 연결을 인증하는 데 실패한/성공한 횟수, 그리고 SMTP AUTH 명령을 사용하여 인증하는 데 실패한/성공한 횟수가 표시됩니다.
수신된 수신자 그래프	Received Recipients(수신된 수신자) 그래프는 해당 메일 클라이언트가 SMTP 인증을 사용하여 메시지를 전송하기 위해 ESA에 대한 연결을 인증하려고 시도한 수신자 수를 보여줍니다. 또한 연결이 인증된 수신자 수 및 연결이 인증되지 않은 수신자 수도 보여줍니다.
SMTP 인증 세부 정보(도메인 이름 또는 IP 주소 기준)	SMTP Authentication Details(SMTP 인증 세부 정보)(도메인 이름 또는 IP 주소 기준) 테이블은 메시지를 전송하기 위해 ESA에 대한 연결을 인증하려고 시도한 사용자에 대한 세부 정보를 표시합니다. 각 도메인에 대해 클라이언트 인증서를 사용하여 성공 또는 실패한 연결 시도 횟수, SMTP AUTH 명령을 사용하여 성공 또는 실패한 연결 시도 횟수, 그리고 클라이언트 인증서 연결 시도 실패 후 SMTP AUTH로 전환한 횟수를 볼 수 있습니다.

Rate Limits(속도 제한) 페이지

봉투 발신자에 의한 속도 제한 기능을 사용하면 mail-from 주소를 기반으로 개별 발신자의 시간 간격당 이메일 메시지 수신자의 수를 제한할 수 있습니다. Rate Limits(속도 제한) 보고서는 가장 눈에 띄게 이 제한을 초과한 발신자를 보여줍니다.

이 보고서를 사용하면 다음을 식별할 수 있습니다.

- 대량 스팸 발신에 사용되었을 수 있는 손상된 사용자 계정.
- 알림, 자동화된 발표 등에 이메일을 사용하는 조직의 제어 불가능한 애플리케이션.

- 내부 결제 또는 리소스 관리 목적으로 조직에서 이메일 활동이 과중한 소스.
- 달리 스팸으로 간주되지 않을 수 있는 대량 인바운드 이메일 트래픽의 소스.

Security Management Appliance에서 Rate Limits(속도 제한) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Rate Limits(**속도 제한**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Internal Users(내부 사용자) 또는 Outgoing Senders(외부 발신자) 등 내부 발신자에 대한 통계를 포함하는 기타 보고서는 전송된 메시지의 수만 측정합니다. 소수의 메시지를 다수의 수신자에게 보내는 발신자는 식별하지 않습니다.

Top Offenders by Incident(인시던트별 상위 위반자) 차트는 구성된 제한보다 더 많은 수신자에게 메시지를 보내려고 가장 자주 시도한 봉투 발신자를 보여줍니다. 각 시도가 하나의 인시던트입니다. 이 차트는 모든 리스너로부터 인시던트 수를 집계합니다.

Top Offenders by Rejected Recipients(거부된 수신자별 상위 위반자) 차트는 구성된 제한을 넘어 최대 수신자에게 메시지를 보낸 봉투 전송자를 보여줍니다. 이 차트는 모든 리스너로부터 수신자 수를 집계합니다.

"Rate Limit for Envelope Senders(봉투 발신자에 대한 속도 제한)" 설정을 비롯한 속도 제한 설정이 Email Security Appliance의 Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책)에 구성되어 있습니다. 속도 제한에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

관련 주제

High Volume Mail(대용량 메일) 페이지, 161 페이지

Connections by Country(국가별 연결 수) 페이지

보려는 Connections by Country(국가별 연결 수) 페이지에서 연결을 사용할 수 있습니다.

- 그래픽 형식의 발신지 국가별 상위 수신 메일 연결.
- 표 형식의 총 수신 연결 및 발신지 국가별 메시지 수.

Security Management Appliance에서 Connections by Country(국가별 연결 수) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Connections by Country(**국가별 연결 수**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

다음은 상위 및 총 수신 메일 연결에 대해 국가 정보가 표시되지 않는 시나리오입니다.

- 발신자 IP 주소는 프라이빗 IP 주소에 속합니다.
- 발신자 IP 주소는 유효한 SBRS를 얻을 수 없습니다.

사용자의 액세스 권한을 통해 이 보고서를 채우는 메시지에 대한 메시지 추적 데이터를 볼 수 있는 경우 테이블에서 파란색 숫자 링크를 클릭합니다.

Connections by Country(국가별 연결 수) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

사용자 메일 요약

User Mail Summary(사용자 메일 요약) 보고서 페이지는 내부 사용자가 보내고 받는 메일에 대한 정보를 이메일 주소별로 제공합니다 한 사용자가 여러 이메일 주소를 가질 수 있습니다. 이메일 주소는 보고서에서 결합되지 않습니다.

User Mail Summary(사용자 메일 요약) 보고서 페이지를 사용하면 다음 정보를 볼 수 있습니다.

- 외부 이메일을 가장 많이 보내는 사람은?
- 정상 이메일을 가장 많이 받는 사람은?
- 그레이메일 메시지를 가장 많이 받는 사람은?
- 스팸을 가장 많이 받는 사람은?
- 누가 어떤 콘텐츠 필터를 트리거하나?
- 누구의 이메일이 콘텐츠 필터에서 가장 많이 포착되는가?

Security Management Appliance에서 User Mail Summary(사용자 메일 요약) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > User Mail Summary(**사용자 메일 요약**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

데이터 내에서 특정 정보를 검색하려면 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.

다음 목록은 User Mail Summary(사용자 메일 요약) 보고서 페이지의 여러 섹션을 설명합니다.

표 ***41: User Mail Summary(***사용자 메일 요약***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
정상 수신 메시지별 상위 사용자	조직에서 받은 정상 수신 메시지의 상위 사용자(도메인 기준)입니다.
정상 발신 메시지별 상위 사용자	조직에서 보낸 정상 발신 메시지의 상위 사용자(도메인 기준)입니다.

섹션	설명
그레이메일별 상위 사용자	그레이메일 메시지의 상위 사용자(도메인 기준)입니다.
사용자 메일 흐름 정보	User Mail Flow Details(사용자 메일 플로우 세부 정보) 인터랙티브 테이블에서는 각 이메일 주소에서 보내고 받는 메일을 분류합니다. 열 제목을 클릭하여 목록을 정렬할 수 있습니다. 자세한 내용은 User Mail Flow Details(사용자 메일 플로우 세부 정보) 테이블, 156 페이지를 참조하십시오. 이 보고서에 기록되는 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

User Mail Summary(사용자 메일 요약) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

참고 User Mail Summary(사용자 메일 요약) 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

관련 주제

- User Mail Flow Details(사용자 메일 플로우 세부 정보) 테이블, 156 페이지
- 특정 내부 사용자 검색, 86 페이지

User Mail Flow Details(사용자 메일 플로우 세부 정보) 테이블

User Mail Flow Details(사용자 메일 플로우 세부 정보) 페이지에는 수신 및 발신 메시지의 분류 및 각 카테고리(탐지된 스팸, 바이러스로 탐지된 메시지, 콘텐츠 필터에 의해 차단된 메시지, 정상 메시지)의 메시지 수를 포함하여 사용자에 대한 자세한 정보가 표시됩니다. 수신 및 발신 콘텐츠 필터 매치도 표시됩니다.

Inbound Internal Users(인바운드 내부 사용자)란 Rcpt To: 주소를 기반으로 이메일을 수신한 사용자입니다. Outbound Internal Users(아웃바운드 내부 사용자)는 Mail From: 주소를 기반으로 하며 내부 네트워크의 발신자가 전송하는 이메일 유형을 추적할 때 유용합니다.

일부 아웃바운드 메일(예: 반송)에는 null 발신자가 있습니다. 이러한 메일은 아웃바운드 "unknown(알 수 없음)"으로 계산됩니다.

이 보고서에서 메시지 추적 세부사항을 보려면 테이블에서 숫자 하이퍼링크를 클릭합니다.

다음 표에는 User Mail Flow Details(사용자 메일 플로우 세부 정보) 테이블의 테이블 열 설명이 나와 있습니다.

표 ***42: User Mail Flow Details(***사용자 메일 플로우 세부 정보***)*** 테이블의 테이블 열 설명

열 이름	설명
내부 사용자	내부 사용자의 도메인 이름입니다.
탐지된 수신 스팸	탐지된 모든 수신 스팸입니다.
탐지된 수신 바이러스	탐지된 수신 바이러스입니다.
Advanced Malware Protection에서 탐지된 수신 메시지	Advanced Malware Protection(파일 분석 및 파일 평판)에서 탐지한 수신 메시지입니다.
수신 콘텐츠 필터 매치	탐지된 수신 콘텐츠 필터 매치입니다.
콘텐츠 필터에 의해 차단된 수신 메시지	설정된 콘텐츠 필터에 의해 차단된 수신 메시지입니다.
수신 마케팅	마케팅으로 탐지된 수신 메시지입니다.
수신 소셜 네트워킹	소셜 네트워킹으로 탐지된 수신 메시지입니다.
수신 대량	대량으로 탐지된 수신 메시지입니다.
수신 그레이메일	그레이메일로 탐지된 수신 메시지입니다.
수신 정상	모든 수신 정상 메시지.
탐지된 발신 스팸	탐지된 발신 스팸.
탐지된 발신 바이러스	탐지된 발신 바이러스입니다.
발신 콘텐츠 필터 매치	탐지된 발신 콘텐츠 필터 매치입니다.
콘텐츠 필터에 의해 차단된 발신 메시지	설정된 콘텐츠 필터에 의해 차단된 발신 메시지.
발신 정상	모든 발신 정상 메시지.

특정 내부 사용자 검색

User Mail Summary(사용자 메일 요약) 페이지 및 User Mail Flow Details(사용자 메일 플로우 세부 정보) 페이지 하단에 있는 검색 양식에서 특정 내부 사용자(이메일 주소)를 검색할 수 있습니다. 검색 텍스트와 정확한 매치를 찾을지 아니면 입력한 텍스트로 시작하는 항목을 찾을지(예: "ex"로 시작하면 "example.com"이 검색됨) 선택합니다.

DLP Incident Summary(DLP 인시던트 요약) 페이지

DLP Incidents (DLP Incident Summary)(DLP 인시던트 - DLP 인시던트 요약) 페이지는 발신 메일에서 발생하는 DLP(data loss prevention) 정책 위반에 대한 정보를 보여줍니다. Email Security Appliance는

사용자가 전송한 민감한 데이터를 탐지하기 위해 Outgoing Mail Policies(발신 메일 정책) 테이블에서 활성화된 DLP 이메일 정책을 사용합니다. DLP 정책을 위반하는 모든 발신 메시지는 인시던트로 보고됩니다.

DLP 인시던트 요약 보고서를 사용하면 다음과 같은 종류의 질문에 답할 수 있습니다.

- 사용자들이 어떤 유형의 민감한 데이터를 전송합니까?
- 이러한 DLP 인시던트가 얼마나 심각합니까?
- 이러한 메시지 중 몇 개가 전달되었습니까?
- 이러한 메시지 중 몇 개가 삭제되었습니까?
- 누가 이러한 메시지를 전송합니까?

DLP Incident 요약 페이지는 크게 2개 섹션으로 구성됩니다.

- 심각도(Low, Medium, High, Critical) 및 정책 매치 기준으로 상위 DLP 인시던트를 요약한 DLP 인시던트 추세 그래프
- DLP 인시던트 세부 정보 목록

Security Management Appliance에서 DLP Incident Summary(DLP 인시던트 요약) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > DLP Incident Summary(DLP** 인시던트 요약**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

DLP Incidents(DLP 인시던트) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

데이터 내에서 특정 정보를 검색하려면 검색 및 인터랙티브 이메일 보고서 페이지 , 66 페이지를 참조하십시오.

다음 목록은 DLP Incident Summary(DLP 인시던트 요약) 보고서 페이지의 여러 섹션을 설명합니다.

표 ***43: DLP Incident Summary(DLP*** 인시던트 요약***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
심각도별 상위 인시던트	심각도 기준 상위 DLP 인시던트입니다.

섹션	설명
인시던트 요약	각 이메일 어플라이언스의 발신 메일 정책에 대해 현재 활성화된 DLP 정책은 DLP Incident Summary(DLP 인시던트 요약) 페이지 맨 아래의 DLP 인시던트 세부사항 인터랙티브 테이블에 나열됩니다. 자세한 정보를 표시하려면 DLP 정책의 이름을 클릭합니다.
상위 DLP 정책 매치	매치한 상위 DLP 정책.
DLP 인시던트 세부사항	DLP Incident Details(DLP 인시던트 세부 정보) 테이블에는 심각도 레벨로 구분된 정책당 총 DLP 인시던트 수와 일반 텍스트로 전달되거나 암호화되어 전달되거나 삭제된 메시지의 수가 표시됩니다. 이 보고서에 기록되는 메시지 추적 세부 정보를 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

Web Interaction Tracking(웹 상호 작용) 페이지

Web Interaction Tracking(웹 상호 작용 추적) 보고서 페이지를 사용하면 다음 정보를 볼 수 있습니다.

- 엔드 유저가 클릭한 상위 악성 URL
- 재작성된 악의적인 URL을 클릭한 상위 엔드 유저
- Web Interaction Tracking Details(웹 상호 작용 추적 세부사항).

참고 Web Interaction(웹 상호 작용) 보고서 모듈은 매니지드 Email Security Appliance에서 웹 인터랙티브 추적 기능이 활성화된 경우에만 채워집니다.

Web Interaction(웹 상호 작용) 보고서는 수신 및 발신 메시지에 대해 사용 가능합니다. 최종 사용자가 클릭하여 재작성된 URL만(정책에 의해서든 Outbreak Filter에 의해서든) 이러한 모듈에 포함됩니다.

Security Management Appliance에서 Web Interaction(웹 상호 작용) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Web Interaction(**웹 상호 작용**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Web Interaction(웹 상호 작용) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

다음 목록은 Web Interaction(웹 상호 작용) 보고서 페이지의 여러 섹션을 설명합니다.

표 *44: Web Interaction(웹 상호 작용)* 페이지의 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	표시할 시간 범위를 선택하는 옵션이 있는 드롭다운 목록. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참고하십시오.
(드롭다운 목록)의 데이터 보기	데이터를 볼 Email Security Appliance를 선택하거나 All Email Appliances(모든 이메일 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
최종 사용자가 클릭한 상위 악성 URL	이 섹션에는 수신 및 발신 메시지에 대해 엔드 유저가 클릭한 상위 악의적 URL의 요약이 표시됩니다.
악의적 URL을 클릭한 상위 사용자	이 섹션에는 수신 및 발신 메시지에 대해 엔드 유저가 클릭한 재작성된 악의적 URL의 요약이 표시됩니다.
Web Interaction Tracking Details(웹 상호 작용 추적 세부 정보)	이 섹션에는 수신 및 발신 메시지의 악의적 URL 및 중립 URL의 차트 보기와 요약이 표시됩니다. 이 보고서에 기록되는 메시지 추적 세부 정보를 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

Web Interaction Tracking Details(웹 상호 작용 추적 세부 정보)

Web Interaction Tracking Details(웹 상호 작용 추적 세부 정보) 테이블은 다음 정보를 포함하는 인터랙티브 테이블입니다.

- 모든 재작성된 URL(악의적인 URL 또는 악의적이지 않은 URL)의 목록.
- 재작성된 URL을 클릭했을 때 수행된 작업(허용, 차단 또는 알 수 없음).
- 최종 사용자가 클릭했을 때 URL(정상 또는 악성)의 판정을 알 수 없는 경우 상태는 unknown(알 수 없음)으로 표시됩니다. 이는 사용자가 클릭한 시점에 URL이 추가 정밀 조사 중이었거나 웹 서버가 다운되었거나 도달할 수 없는 상태였기 때문에 발생할 수 있습니다.
- 최종 사용자가 재작성된 URL에서 클릭한 횟수.
- 다음에 유의하십시오.
  - 악성 URL을 재작성한 후 메시지를 전달하고 다른 사용자(예: 관리자)에게 알리도록 콘텐츠 또는 메시지 필터를 구성한 경우, 알림을 받은 사용자가 재작성된 URL을 클릭하더라도 원래 수신자의 웹 상호 작용 추적 데이터가 증가합니다.
  - 재작성된 URL을 포함하는 격리된 메시지의 복사본을 웹 인터페이스를 통해 원래 수신자가 아닌 사용자(예: 관리자)에게 전송하는 경우, 이 사용자가 재작성된 URL을 클릭하더라도 원래 수신자의 웹 상호 작용 추적 데이터가 증가합니다.

이 보고서에 기록되는 메시지 추적 세부 정보를 보려면 테이블에서 파란색 숫자 하이퍼링크를 클릭합니다.

Message Filters(메시지 필터) 페이지

Message Filters(메시지 필터) 보고서 페이지는 수신 및 발신 메시지에 대한 상위 메시지 필터 매칭 결과(매칭하는 메시지 수가 가장 많은 메시지 필터)를 보여줍니다.

Message Filters(메시지 필터) 보고서 페이지를 사용하면 다음 정보를 볼 수 있습니다.

- 일치 수 기준 상위 메시지 필터(그래픽 형식)
- 일치 수 기준 총 메시지 필터(표 형식)

Security Management Appliance에서 Message Filters(메시지 필터) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Message Filters(**메시지 필터**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Message Filters(메시지 필터) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

High Volume Mail(대용량 메일) 페이지

High Volume Mail(대용량 메일) 보고서 페이지를 사용할 수 있습니다.

- 가변적인 1시간 동안 단일 발신자가 보낸 또는 동일한 제목으로 된 최다 메시지 수의 공격을 확인합니다.
- 상위 도메인을 모니터링하여 해당 공격이 자체 도메인에서 발생하지 않았음을 확인합니다. 자체 도메인에서 발생했다면 하나 이상의 계정이 감염되었을 가능성이 있습니다.
- 오탐지를 확인하여 필터를 조정할 수 있습니다.

High Volume Mail(대용량 메일) 보고서 페이지를 사용하면 다음 정보를 볼 수 있습니다.

- 상위 제목 포함된 메시지(그래픽 형식)
- 봉투 발신자의 메시지(그래픽 형식)
- 일치 수 기준 상위 메시지 필터(그래픽 형식)
- 일치 수 기준 총 메시지 필터(표 형식)

Security Management Appliance에서 High Volume Mail(대용량 메일) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(**이메일**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > High Volume Mail(**대용량 메일**)**을 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

High Volume Mail(대용량 메일) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

이 페이지의 보고서는 헤더 반복 규칙을 사용하고 이 규칙에서 설정한 메시지 수 임계값을 통과한 메시지 필터의 데이터만 표시합니다. 다른 규칙과 연계할 경우 헤더 반복 규칙이 마지막으로 평가됩니다. 이전의 조건에서 메시지 특성이 확인된 경우 평가되지 않습니다. 또한 속도 제한에 걸린 메시지는 헤더 반복 메시지 필터에 오지 않습니다. 따라서 대량 메일로 간주되었을 메시지가 이 보고서에 포함되지 않을 수도 있습니다. 특정 메시지를 화이트리스트에 포함하도록 필터를 구성한 경우 그러한 메시지도 보고서에서 제외될 수 있습니다.

메시지 필터 및 Header Repeats(헤더 반복) 규칙에 대한 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서를 참조하십시오.

Content Filters(콘텐츠 필터) 페이지

Content Filters(콘텐츠 필터) 보고서 페이지는 상위 수신 및 발신 콘텐츠 필터 매칭 결과(매칭하는 메시지가 가장 많은 콘텐츠 필터)에 대한 정보를 제공합니다. 이 페이지는 데이터를 막대그래프 및 목록 형태로도 표시합니다. Content Filters(콘텐츠 필터) 보고서 페이지를 사용하면 다음 유형의 질문에 답할 수 있습니다.

- 수신 또는 발신 메일에 의해 가장 많이 트리거되는 콘텐츠 필터는 무엇입니까?
- 특정 콘텐츠 필터를 트리거하는 메일을 보내거나 받는 상위 사용자는 누구입니까?

Content Filters(콘텐츠 필터) 보고서 페이지를 사용하면 다음 정보를 볼 수 있습니다.

- 상위 수신 및 발신 콘텐츠 필터 매치(그래픽 형식)
- 상위 수신 및 발신 콘텐츠 필터 매치(표 형식)

Security Management Appliance에서 Content Filters(콘텐츠 필터) 보고서 페이지를 보려면, Product(제품) 드롭다운에서 **Email(이메일)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > Content Filters(콘텐츠 필터)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Content Filters(콘텐츠 필터) 보고서 페이지에서 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 파일 인쇄 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지를 참조하십시오.

참고 콘텐츠 필터 페이지에 대한 예약 보고서를 생성할 수 있습니다. 이메일 보고서 예약, 169 페이지를 참조하십시오.

Content Filter Details(콘텐츠 필터 세부사항) 페이지

Content Filter Detail(콘텐츠 필터 세부사항) 페이지에는 시간별 해당 필터에 대한 일치 및 내부 사용자별 일치가 표시됩니다.

Matches by Internal User(내부 사용자별 매치) 섹션에서 내부 사용자(이메일 주소)의 세부사항 페이지를 보려면 해당 사용자의 이름을 클릭합니다. 자세한 내용은 사용자 메일 요약, 155 페이지을(를) 참고하십시오.

사용자의 액세스 권한상 메시지 추적 데이터를 볼 수 있는 경우: 이 보고서에서 메시지 추적 세부사항을 보려면 테이블에서 파란색 숫자 링크를 클릭합니다.

보고 데이터 가용성 페이지

Email(이메일) > Reporting(보고) > Reporting Data Availability(보고 데이터 가용성) 페이지는 데이터를 보고 업데이트하고 정렬하여, 리소스 사용률 및 이메일 트래픽 문제 지점에 대한 실시간 가시성을 제공할 수 있습니다.

Security Management Appliance에서 관리하는 전체 어플라이언스의 데이터 가용성을 포함하여, 모든 데이터 리소스 사용률 및 이메일 트래픽 문제 지점은 이 페이지에 표시됩니다.

또한 이 보고서 페이지에서 특정 어플라이언스 및 시간 범위에 대한 데이터 가용성을 볼 수 있습니다.

그레이메일 보고

그레이메일 통계는 다음 보고서에 반영됩니다.

보고서	다음 그레이메일 데이터 포함
Mail Flow Summary(메일 플로우 요약) 페이지 > Incoming(수신) 탭	각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.
Mail Flow Details(메일 플로우 세부 정보) 페이지 > Outgoing Senders(발신 발신자) 탭	상위 그레이메일 발신자.
Mail Flow Details(메일 플로우 세부 정보) 페이지 > Incoming Mails(수신 메일) 탭	모든 IP 주소, 도메인 이름 또는 네트워크 소유자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.
User Mail Summary(사용자 메일 요약) 페이지 > Top Users by Graymail(그레이메일별 상위 사용자)	그레이메일을 수신하는 상위 최종 사용자.
User Mail Summary(사용자 메일 요약) 페이지 > User Mail Details(사용자 메일 세부 정보)	모든 사용자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.

관련 주제

- AsyncOS 9.5 업그레이드 후 마케팅 메시지 보고 , 105 페이지

AsyncOS 9.5 업그레이드 후 마케팅 메시지 보고

AsyncOS 9.5로 업그레이드하면

- 마케팅 메시지 수는 업그레이드 전후에 탐지된 마케팅 메시지의 합계입니다.
- 총 그레이메일 메시지 수에는 업그레이드 이전에 탐지된 마케팅 메시지의 수가 포함되지 않습니다.
- 총 시도된 메시지 수에는 또한 업그레이드 전에 탐지된 마케팅 메시지의 수가 포함됩니다.
- 관리 Email Security Appliance에서 그레이메일 기능이 활성화되지 않은 경우 마케팅 메시지는 정상 메시지로 간주됩니다.

예약 및 온디맨드 이메일 보고서 정보

사용 가능한 보고서 유형

달리 명시되지 않는 한 다음 이메일 보안 보고서 유형은 예약 및 온디맨드 버전으로 이용할 수 있습니다.

- 콘텐츠 필터 - 최대 40개의 콘텐츠 필터를 포함합니다. 이 페이지의 내용에 대해서는 Content Filters(콘텐츠 필터) 페이지, 162 페이지를 참조하십시오.
- DLP 인시던트 요약 - 이 페이지의 내용에 대해서는 DLP Incident Summary(DLP 인시던트 요약) 페이지, 157 페이지를 참조하십시오.
- 전달 상태 - 특정 수신자 도메인 또는 가상 게이트웨이 주소에 대한 전달 문제에 대한 정보를 표시합니다. 지난 3시간 내에 시스템에서 전달한 메시지에 대한 상위 수신자 도메인 20, 50 또는 100개 목록을 표시합니다. 각 통계의 열 머리글에 있는 링크를 클릭하여 최신 호스트 상태, 활성 수신자(기본값), 외부 연결, 전달된 수신자, 소프트 바운스된 이벤트, 하드 바운스된 수신자 등을 기준으로 정렬할 수 있습니다. Email Security Appliance에서 Delivery Status(전달 상태) 페이지의 역할에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.
- Domain-Based Executive Summary(도메인 기반 개요 요약) - 이 보고서는 Mail Flow Summary(메일 플로우 요약) 페이지, 114 페이지를 기반으로 하며, 지정된 도메인 그룹으로 제한됩니다. 그 내용에 대해서는 도메인 기반 총괄 요약 보고서, 165 페이지를 참조하십시오.
- 총괄 요약 - Mail Flow Summary(메일 플로우 요약) 페이지, 114 페이지의 정보를 기반으로 합니다. 그 내용에 대해서는 도메인 기반 총괄 요약 보고서, 165 페이지를 참조하십시오.
- Mail Flow Details(메일 플로우 세부 정보) - 이 페이지의 내용에 대해서는 Mail Flow Details(메일 플로우 세부 정보) 페이지, 138 페이지를 참조하십시오.
- User Mail Summary(사용자 메일 요약) - 이 페이지의 내용에 대해서는 사용자 메일 요약, 155 페이지를 참조하십시오.
- 발신 목적지 - 이 페이지의 내용에 대해서는 Outgoing Destinations(발신 대상) 페이지, 147 페이지를 참조하십시오.
- 발신자 그룹 - 이 페이지의 내용에 대해서는 Sender Groups(발신자 그룹) 페이지, 146 페이지를 참조하십시오.
- TLS Encryptions(TLS 암호화) - 이 페이지의 내용에 대해서는 TLS Encryption(TLS 암호화) 페이지, 149 페이지를 참조하십시오.

- 바이러스 유형 - 이 페이지의 내용에 대해서는 Virus Filtering(바이러스 필터링) 페이지, 130 페이지를 참조하십시오.

시간 범위

보고서에 따라 전날, 지난 7일, 지난달, 지난해(최대 250일), 지난해 월(최대 12개월)의 데이터를 포함하도록 구성할 수 있습니다. 또는 맞춤 일수(2일 ~ 100일(또는 맞춤 월수(2개월 ~ 12개월)의 데이터를 포함할 수 있습니다.

보고서 실행 시점과 상관없이 데이터는 이전 시간 간격(시간, 일, 주, 월)에서 반환됩니다. 예를 들어 오전 1시에 일일 보고서를 실행하도록 예약할 경우 전날 자정부터 자정까지(00:00 ~ 23:59)의 데이터가 포함됩니다.

언어 및 로케일

참고 개별 보고서에 특정 로케일로 PDF 보고서를 예약하거나 원시 데이터를 CSV 파일로 내보낼 수 있습니다. 예약 보고서 페이지의 언어 드롭다운 메뉴를 통해 현재 선택한 로케일 및 언어로 PDF 보고서를 보거나 예약할 수 있습니다. 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지의 중요 내용을 참조하십시오.

아카이브 보고서 저장

보고서 저장 기간 및 아카이브 보고서가 시스템에서 삭제되는 시점에 대해서는 아카이브 이메일 보고서 보기 및 관리 , 172 페이지를 참조하십시오.

추가 보고서 유형

Security Management Appliance의 **Email(이메일) > Reporting(보고)** 섹션에서 두 가지 특수 보고서를 생성할 수 있습니다.

- 도메인 기반 총괄 요약 보고서, 165 페이지
- 총괄 요약 보고서 , 168 페이지

도메인 기반 총괄 요약 보고서

네트워크에 있는 하나 이상의 도메인에 대해 수발신 메시지 활동을 요약하여 표시합니다. 총괄 요약 보고서와 비슷하지만 지정된 도메인의 수발신 메시지에 대한 데이터로 한정합니다. 발신 메일 요약은 발신 서버의 PTR이 지정된 도메인과 매치할 경우에만 데이터를 표시합니다. 여러 도메인이 지정된 경우 어플라이언스는 모든 해당 도메인의 데이터를 단일 보고서로 집계합니다.

하위 도메인용 보고서를 생성하려면 Email Security Appliance 및 Security Management Appliance의 보고 시스템에서 부모 도메인을 두 번째 레벨 도메인으로 추가해야 합니다. 예를 들어 example.com을 두 번째 레벨 도메인으로 추가하면 해당 하위 도메인(예: subdomain.example.com)을 보고에 사용할 수 있습니다. 두 번째 레벨 도메인을 추가하려면 Email Security Appliance CLI에서 **reportingconfig -> mailsetup -> tld**를 사용하고 Security Management Appliance CLI에서 **reportingconfig -> domain -> tld**를 사용합니다.

다른 예약 보고서와 달리 도메인 기반 총괄 요약 보고서는 아카이빙되지 않습니다.

도메인 기반 총괄 요약 보고서 및 발신자 평판 필터링 차단 메시지

발신자 평판 필터링에 의해 차단된 메시지는 실제로 작업 대기열에 들어가지 못하므로, AsyncOS는 도메인 목적지를 확인하기 위해 이 메시지를 처리하지 못합니다. 알고리즘이 도메인당 거부된 메시지 수를 예측합니다. 도메인당 차단된 메시지의 정확한 수를 확인하려면 메시지가 수신자 레벨(RCPT TO)에 도달할 때까지 Security Management Appliance에서 HAT 거부를 지연할 수 있습니다. 그러면 AsyncOS는 수신 메시지에서 수신자 데이터를 수집할 수 있습니다. Email Security Appliance에서 **listenerconfig -> setup** 명령을 사용하여 거부를 지연할 수 있습니다. 그러나 이 옵션은 시스템 성능에 영향을 미칠 수 있습니다. 지연된 HAT 거부에 대한 자세한 내용은 Email Security Appliance용 문서를 참조하십시오.

참고 Security Management Appliance에서 Domain-Based Executive Summary(도메인 기반 개요 요약) 보고서의 Stopped by Reputation Filtering(평판 필터링에 의해 중단됨) 결과를 보려면 Email Security Appliance 및 Security Management Appliance에서 모두 **hat_reject_info**를 활성화해야 합니다. Security Management Appliance에서 **hat_reject_info**를 활성화하려면 **reportingconfig > domain > hat_reject_info** 명령을 실행합니다.

도메인 기반 총괄 요약 보고서의 도메인 및 수신자 목록 관리

구성 파일을 사용하여 도메인 기반 총괄 요약 보고서의 도메인 및 수신자를 관리할 수 있습니다. 구성 파일은 어플라이언스의 구성 디렉터리에 저장되는 텍스트 파일입니다. 파일의 각 행이 별도의 보고서를 생성합니다. 그러면 다수의 도메인 및 수신자를 단일 보고서에 포함할 뿐 아니라 단일 구성 파일에서 여러 도메인 보고서를 정의할 수 있습니다.

구성 파일의 각 행은 공백으로 구분된 도메인 이름 목록 및 공백으로 구분된 보고서 수신자 이메일 주소의 목록을 포함합니다. 도메인 이름 목록과 이메일 수신자 목록은 쉼표로 구분됩니다. ubdomain.example.com과 같이 상위 도메인 이름의 서두에 하위 도메인 이름과 마침표를 추가하여 하위 도메인을 포함할 수 있습니다.

다음은 3개의 보고서를 생성하는 단일 보고서 구성 파일입니다.

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```

참고 구성 파일 및 단일 명명 보고서에 대해 정의된 설정을 사용하여 여러 보고서를 동시에 생성할 수 있습니다. 예를 들어 Bigfish라는 회사가 Redfish와 Bluefish라는 회사를 인수하고 그 도메인을 유지하려 합니다. Bigfish는 각 도메인 보고서에 해당하는 3개의 행으로 구성된 구성 파일을 사용하여 도메인 기반 총괄 요약 보고서를 생성합니다. 어플라이언스에서 도메인 기반 총괄 요약 보고서를 생성할 때 Bigfish 관리자는 Bigfish.com, Redfish.com, Bluefish.com 도메인에 대한 보고서를 수신하지만 Redfish 관리자는 Redfish.com 도메인에 대한 보고서를, Bluefish 관리자는 Bluefish.com 도메인에 대한 보고서를 수신합니다.

각 명명된 보고서에 대해 다른 구성 파일을 어플라이언스에 업로드할 수 있습니다. 동일한 구성 파일을 여러 보고서에 사용할 수도 있습니다. 동일한 도메인에 대해 서로 다른 시간의 데이터를 제공하는 개별 보고서를 생성할 수 있습니다. 어플라이언스에서 구성 파일을 업데이트할 경우, 파일 이름을 변경하지 않는 한 GUI에서 보고서 설정을 업데이트할 필요 없습니다.

도메인 기반 총괄 요약 보고서 생성

단계 **1** Security Management Appliance에서 보고서를 예약하거나 즉시 생성할 수 있습니다.

보고서를 예약하려면

a) [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.
b) **Email**(이메일) **> Reporting**(보고) **> Scheduled Reports**(예약 보고서)를 선택합니다.
c) **Add Scheduled Report**(예약 보고서 추가)를 클릭합니다.

온디맨드 보고서를 생성하려면

- [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.
- **Email**(이메일) **> Reporting**(보고) **> Archived Reports**(아카이브 보고서)를 선택합니다.
- **Generate Report Now**(지금 보고서 생성)를 클릭합니다.

단계 **2** **Report Type**(보고서 유형) 드롭다운 목록에서 **Domain-Based Executive Summary**(도메인 기반 총괄 요약) 보고서 유형을 선택합니다.

단계 **3** 보고서에 포함할 도메인을 선택하고 보고서 수신자의 이메일 주소를 지정합니다. 다음 옵션 중 하나를 선택하여 보고서를 생성할 수 있습니다.

- 개별 도메인을 지정하여 보고서를 생성합니다. 보고서에 포함할 도메인을 입력하고 보고서 수신자의 이메일 주소를 지정합니다. 여러 항목을 구분하려면 쉼표를 사용합니다. subdomain.yourdomain.com과 같은 하위 도메인을 사용할 수도 있습니다. 자주 바뀌지 않을 소수의 도메인에 대한 보고서를 생성할 경우 개별 도메인을 지정하는 것이 좋습니다.
- 파일을 업로드하여 보고서를 생성합니다. 보고서를 위한 도메인 및 수신자 이메일 주소의 목록이 포함된 구성 파일을 가져옵니다. 어플라이언스의 구성 디렉터리에서 구성 파일을 선택하거나 로컬 컴퓨터에서 업로드할 수 있습니다. 자주 바뀌는 다수의 도메인에 대한 보고서를 생성할 경우 구성 파일을 사용하는 것이 좋습니다. 도메인 기반 보고서의 구성 파일에 대한 자세한 내용은 도메인 기반 총괄 요약 보고서의 도메인 및 수신자 목록 관리 , 166 페이지를 참조하십시오.

참고 외부 계정에 보고서를 보낼 경우(예: Yahoo! Mail, Gmail) , 보고서 이메일이 스팸으로 잘못 분류되지 않도록 하려면 외부 계정의 화이트리스트에 보고 반환 주소를 추가해야 할 수 있습니다.

단계 **4** 제목 텍스트 필드에 보고서 제목의 이름을 입력합니다.

AsyncOS는 보고서 이름의 고유성을 확인하지 않습니다. 혼동을 피하려면 동일한 이름의 여러 보고서를 만들지 마십시오.

단계 **5** 발신 도메인 섹션에서 발신 메일 요약의 도메인 유형을 선택합니다. By Server 또는 By Email Address 중에서 선택합니다.

단계 **6** 포함할 시간 범위 드롭다운 목록에서는 보고서 데이터의 시간 범위를 선택합니다.

단계 **7** 형식에서는 보고서의 형식을 선택합니다.

선택 사항은 다음과 같습니다.

- PDF. 전달용, 보관용 또는 둘 모두를 위한 형식이 지정된 PDF 문서를 만듭니다. Preview PDF Report(PDF 보고서 미리 보기)를 클릭하여 보고서를 PDF 파일로 즉시 볼 수 있습니다.
- CSV. 표 형식의 데이터 및 쉼표로 구분된 값을 포함하는 ASCII 텍스트 파일을 만듭니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다.

단계 **8** 일정에서 보고서 생성 일정을 선택합니다.

Daily, Weekly(요일 드롭다운 목록 포함), Monthly 중에서 선택합니다.

단계 **9** (선택 사항) 보고서를 위한 맞춤 로고를 업로드합니다. 로고가 보고서 맨 위에 나타납니다.

- .jpg, .gif, or .png 파일이고 최대 550 x 50픽셀이어야 합니다.
- 로고 파일이 지원되지 않으면 기본 Cisco 로고가 사용됩니다.

단계 **10** 이 보고서의 언어를 선택합니다. 아시아 언어로 PDF를 생성하려면 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지의 중요 내용을 참조하십시오.

단계 **11** **Submit**(제출)을 클릭하여 페이지의 변경 사항을 제출한 다음 **Commit Changes**(변경 사항 적용)를 클릭하여 변경 사항을 적용합니다.

총괄 요약 보고서

Executive Summary(개요 요약) 보고서는 Security Management Appliance에서 볼 수 있는 Email Security Appliance의 수신 및 발신 이메일 메시지 활동을 요약하여 보여주는 보고서입니다.

이 보고서 페이지에는 Mail Flow Summary(메일 플로우 요약) 페이지, 114 페이지에서 볼 수 있는 내용이 요약되어 있습니다. 이메일 보고 개요 페이지에 대한 자세한 내용은 Mail Flow Summary(메일 플로우 요약) 페이지, 114 페이지를 참조하십시오.

Scheduled Reports(예약된 보고서) 페이지

- 이메일 보고서 예약, 169 페이지
- 웹 보고서 예약 , 239 페이지

이메일 보고서 예약

예약 및 온디맨드 이메일 보고서 정보 , 164 페이지에 나열된 모든 보고서를 예약할 수 있습니다.

보고서 예약을 관리하려면 다음을 참조하십시오.

- 예약 보고서 추가, 169 페이지
- 예약된 보고서 편집, 170 페이지
- 예약 보고서 삭제 , 170 페이지

예약 보고서 추가

예약 이메일 보고서를 추가하려면 다음 단계를 수행합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email**(이메일) > **Reporting**(보고) > **Scheduled Reports**(예약 보고서)를 선택합니다.

단계 **3** **Add Scheduled Report**(예약 보고서 추가)를 클릭합니다.

단계 **4** 보고서 유형을 선택합니다.

보고서 유형에 대해서는 예약 및 온디맨드 이메일 보고서 정보 , 164 페이지를 참조하십시오.

참고 - 도메인 기반 총괄 요약 보고서의 설정에 대해서는 도메인 기반 총괄 요약 보고서, 165 페이지를 참조하십시오.

- 예약 보고서에 사용 가능한 옵션은 보고서 유형에 따라 다릅니다. 이 절차의 나머지 부분에서 설명하는 옵션이 모든 보고서에 적용되는 것은 아닙니다.

단계 **5** **Title**(제목) 필드에 보고서의 제목을 입력합니다.

같은 이름으로 여러 보고서가 생성되지 않도록 설명적 제목을 사용하는 것이 좋습니다.

단계 **6** **Time Range to Include**(포함할 시간 범위) 드롭다운 목록에서 보고서의 시간 범위를 선택합니다.

단계 **7** 생성된 보고서의 형식을 선택합니다.

기본 형식은 PDF입니다. 또한 대부분의 보고서에서는 원시 데이터를 CSV 파일로 저장할 수 있습니다.

단계 **8** 보고서에 따라 Number of Rows(행 수)에서 포함할 데이터의 양을 선택합니다.

단계 **9** 보고서에 따라 데이터를 정렬할 열을 선택합니다.

단계 **10** **Schedule**(일정) 영역에서는 예약 보고서를 위해 일, 주, 월 옆에 있는 라디오 버튼을 선택합니다. 또한 보고서 예약 시간을 포함합니다. 시간은 자정부터 자정까지(00:00 ~ 23:59)입니다.

단계 **11** **Email**(이메일) 텍스트 필드에는 생성된 보고서를 받을 이메일 주소를 입력합니다.

이메일 수신자를 지정하지 않더라도 시스템에서는 여전히 보고서를 보관합니다.

0명을 포함하여 원하는 만큼 보고서의 수신자를 추가할 수 있습니다. 그러나 보고서를 대량의 주소로 전송하려면 수신자를 개별적으로 나열하는 것보다 메일 목록을 작성하는 것이 더 쉬울 수 있습니다.

단계 **12** 보고서의 언어를 선택합니다.

아시아 언어의 경우 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지의 중요 내용을 참조하십시오.

단계 **13** 제출을 클릭합니다.

예약된 보고서 편집

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email(이메일) > Reporting(보고) > Scheduled Reports(예약 보고서)**를 선택합니다.

단계 **3** 보고서 제목 열에서 수정할 보고서 이름 링크를 클릭합니다.

단계 **4** 보고서 설정을 수정합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

예약 보고서 삭제

예약 보고서가 더 이상 생성되지 않게 하려면 다음 단계를 수행합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email(이메일) > Reporting(보고) > Scheduled Reports(예약 보고서)**를 선택합니다.

단계 **3** 더 이상 생성하지 않을 보고서의 확인란을 선택합니다. 모든 예약 보고서를 삭제하려면 **All(모두)** 확인란을 선택합니다.

단계 **4** **Delete(삭제)**를 클릭합니다.

참고 삭제된 보고서의 보관된 버전은 자동으로 삭제되지 않습니다. 이전에 생성한 보고서를 삭제하려면 아카이브 보고서 삭제, 173 페이지를 참조하십시오.

온디맨드 이메일 보고서 생성

새 웹 인터페이스의 Email Reporting(이메일 보고) 페이지 이해, 109 페이지에서 설명한 인터랙티브 보고서 페이지를 사용하여 조회하고 PDF를 생성할 수 있는 보고서 외에도 언제라도 사용자 지정 기간

에 대해 예약 및 온디맨드 이메일 보고서 정보 , 164 페이지에 나열된 보고서의 PDF 또는 원시 데이터 CSV 파일을 저장할 수 있습니다.

온디맨드 보고서를 생성하려면 다음을 수행합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email**(이메일) **> Reporting**(보고) **> Archived Reports**(아카이브 보고서)를 선택합니다.

단계 **3** **Generate Report Now**(지금 보고서 생성)를 클릭합니다.

단계 **4** 보고서 유형을 선택합니다.

보고서 유형에 대해서는 예약 및 온디맨드 이메일 보고서 정보 , 164 페이지를 참조하십시오.

단계 **5** 제목 텍스트 필드에 보고서 제목의 이름을 입력합니다.

AsyncOS는 보고서 이름의 고유성을 확인하지 않습니다. 혼동을 피하려면 동일한 이름의 여러 보고서를 만들지 마십시오.

참고 도메인 기반 총괄 요약 보고서의 설정에 대해서는 도메인 기반 총괄 요약 보고서, 165 페이지를 참조하십시오.

예약 보고서에 사용 가능한 옵션은 보고서 유형에 따라 다릅니다. 이 절차의 나머지 부분에서 설명하는 옵션이 모든 보고서에 적용되는 것은 아닙니다.

단계 **6** 포함할 시간 범위 드롭다운 목록에서는 보고서 데이터의 시간 범위를 선택합니다.

맞춤 시간 범위 옵션에 주의하십시오.

단계 **7** 형식에서는 보고서의 형식을 선택합니다.

선택 사항은 다음과 같습니다.

- PDF. 전달용, 보관용 또는 둘 모두를 위한 형식이 지정된 PDF 문서를 만듭니다. Preview PDF Report(PDF 보고서 미리 보기)를 클릭하여 보고서를 PDF 파일로 즉시 볼 수 있습니다.
- CSV. 표 형식의 데이터 및 쉼표로 구분된 값을 포함하는 ASCII 텍스트 파일을 만듭니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다.

단계 **8** 보고서를 실행할 어플라이언스 또는 어플라이언스 그룹을 선택합니다. 어플라이언스 그룹을 생성하지 않았다면 이 옵션은 나타나지 않습니다.

단계 **9** 전달 옵션에서 다음을 선택합니다.

- **Archive Report**(보고서 아카이빙) 확인란을 선택하여 보고서를 아카이빙합니다.

그러면 아카이브 보고서 페이지에 나타납니다.

참고 도메인 기반 총괄 요약 보고서는 아카이빙할 수 없습니다.

- **Email now to recipients**(지금 수신자에게 이메일 보내기) 확인란을 선택하여 이메일로 보냅니다.

텍스트 필드에 수신자 이메일 주소를 입력합니다.

단계 **10** 이 보고서의 언어를 선택합니다. 아시아 언어로 PDF를 생성하려면 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지의 중요 내용을 참조하십시오.

단계 **11** **Deliver This Report(**이 보고서 전달**)**를 클릭하여 보고서를 생성합니다.

Archived Email Reports(보관된 이메일 보고서) 페이지

- 예약 및 온디맨드 이메일 보고서 정보 , 164 페이지
- 온디맨드 이메일 보고서 생성 , 170 페이지
- 아카이브 이메일 보고서 보기 및 관리 , 172 페이지

아카이브 이메일 보고서 보기 및 관리

예약된 보고서 및 온디맨드 보고서는 일정 기간 보관됩니다.

Security Management Appliance는 각 예약된 보고서 최대 30개 인스턴스, 모든 보고서 최대 총 1000개 버전까지 최신 보고서를 유지합니다. 30개 인스턴스 제한은 동일한 이름과 기간의 각 예약된 보고서에 적용됩니다.

아카이브 보고서는 자동으로 삭제됩니다. 새 보고서가 추가되면 1000개 개수를 유지하기 위해 이전 보고서가 제거됩니다.

아카이브 보고서는 어플라이언스의 /periodic_reports 디렉터리에 저장됩니다. (자세한 내용은 IP 인터페이스 및 어플라이언스 액세스, 547 페이지를 참조해 주십시오.)

아카이브 보고서 액세스

Email(이메일**) > Reporting(**보고**) > Archived Reports(**아카이브 보고서**)** 페이지에는 보관하기로 결정한, 즉 생성한 후 아직 삭제하지 않은 예약 및 온디맨드 보고서가 나열됩니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email(**이메일**) > Reporting(**보고**) > Archived Reports(**보관된 보고서**)**를 선택합니다.

단계 **3** 이 목록이 길 때 특정 보고서를 찾으려면 **Show(**표시**)** 메뉴에서 보고서 유형을 선택하여 필터링하거나 열 제목을 클릭하여 정렬합니다.

단계 **4** Report Title(보고서 제목)을 클릭하여 보고서를 봅니다.

아카이브 보고서 삭제

아카이브 이메일 보고서 보기 및 관리 , 172 페이지에 설명된 규칙에 따라 자동으로 보고서가 삭제됩니다. 그러나 불필요한 보고서를 수동으로 삭제할 수 있습니다.

아카이브 보고서를 수동으로 삭제하려면 다음을 수행합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email**(이메일) > **Reporting**(보고) > **Archived Reports**(아카이브 보고서)를 선택합니다.

사용 가능한 아카이브 보고서가 표시됩니다.

단계 **3** 삭제할 하나 이상의 보고서에 대해 확인란을 선택합니다.

단계 **4** **Delete**(삭제)를 클릭합니다.

단계 **5** 예약 보고서가 다시 생성되지 않도록 예약 보고서 삭제 , 170 페이지를 참조하십시오.

이메일 보고서 문제 해결

- Outbreak Filters 보고서에서 정보가 올바르게 표시되지 않음 , 173 페이지
- 메시지 추적 결과가 보고서의 링크를 클릭한 후 나타나는 결과와 매치하지 않음 , 173 페이지
- Advanced Malware Protection 판정 업데이트 보고서 결과가 다름 , 174 페이지
- 파일 분석 보고서 세부사항 보기 문제 , 174 페이지

모든 보고서 트러블슈팅 , 45 페이지도 참고하십시오.

Outbreak Filters 보고서에서 정보가 올바르게 표시되지 않음

문제

Outbreak Filters 보고서에서 위협 정보를 올바르게 표시하지 않습니다.

솔루션

어플라이언스가 Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Update Settings(업데이트 설정)에 지정된 Cisco 업데이트 서버와 통신할 수 있음을 확인합니다.

메시지 추적 결과가 보고서의 링크를 클릭한 후 나타나는 결과와 매치하지 않음

문제

보고서에서 드릴다운한 메시지 추적 결과가 예상과 다릅니다.

솔루션

이 문제는 보고 및 추적이 일관성이 없고 동시에 활성화되지 않고 제대로 작동하지 않는 경우 또는 각 Email Security Appliance에서 일관성 있게 동시에 중앙 집중화되거나 로컬에 저장되지 않는 경우 발생할 수 있습니다. 각 기능(보고, 추적)에 대한 데이터는 기능이 활성화된 동안에만 캡처됩니다.

관련 주제

- 메시지 추적 데이터 가용성 확인 , 266 페이지

Advanced Malware Protection 판정 업데이트 보고서 결과가 다름

문제

Web Security Appliance 및 Email Security Appliance에서 분석을 위해 동일한 파일을 전송하면 웹 및 이메일에 대한 AMP 판정 업데이트 보고서에 해당 파일에 대한 서로 다른 판정이 표시됩니다.

솔루션

이 상황은 일시적입니다. 모든 판정 업데이트가 다운로드되면 결과가 매치합니다. 이 과정이 완료될 때까지 최대 30분이 걸릴 수 있습니다.

파일 분석 보고서 세부사항 보기 문제

- 파일 분석 보고서 세부사항이 제공되지 않음 , 174 페이지
- 파일 분석 보고서 세부사항 보기 오류, 174 페이지
- 프라이빗 클라우드 Cisco AMP Threat Grid Appliance에서 파일 분석 보고서 세부사항 보기 오류 , 175 페이지
- 파일 분석 관련 오류 로깅 , 175 페이지

파일 분석 보고서 세부사항이 제공되지 않음

문제

파일 분석 보고서 세부사항을 사용할 수 없습니다.

솔루션

파일 분석 보고서 요구 사항 정보 , 94 페이지를 참조하십시오.

파일 분석 보고서 세부사항 보기 오류

문제

파일 분석 보고서 세부사항을 보려고 할 때 No cloud server configuration is available 오류가 나타납니다.

솔루션

Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)로 이동하여, 파일 분석 기능이 활성화된 Email Security Appliance를 하나 이상 추가합니다.

프라이빗 클라우드 **Cisco AMP Threat Grid Appliance**에서 파일 분석 보고서 세부사항 보기 오류

문제

파일 분석 보고서 세부사항을 보려고 할 때 API 키, 등록 또는 활성화 오류가 나타납니다.

솔루션

프라이빗 클라우드(온프레미스) Cisco AMP Threat Grid 어플라이언스를 파일 분석에 사용하는 경우 (온프레미스 파일 분석) 파일 분석 계정 활성화 , 95 페이지를 참조하십시오.

Threat Grid 어플라이언스 호스트 이름이 바뀌면 참조된 절차의 프로세스를 반복해야 합니다.

파일 분석 관련 오류 로깅

등록 및 기타 파일 분석 관련 오류는 GUI 로그에 기록됩니다.

전체 그레이메일 또는 마케팅 메시지 정보가 올바르지 않음

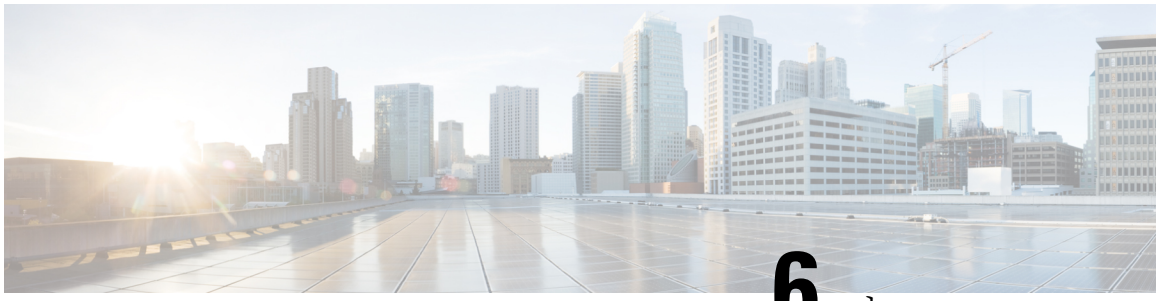
문제

마케팅, 소셜, 대량 메일의 수가 총 그레이메일 메시지 수를 초과합니다.

솔루션

총마케팅 메시지 수는 AsyncOS 9.5 업그레이드 전후에 받은 마케팅 메시지를 포함하지만, 총그레이메일 메시지 수는 업그레이드 후에 받은 것만 포함합니다. AsyncOS 9.5 업그레이드 후 마케팅 메시지 보고 , 105 페이지를 참조하십시오.

전체 그레이메일 또는 마케팅 메시지 정보가 올바르지 않음



6 장

중앙 웹 보고 및 추적 사용

이 장에는 다음 섹션이 포함되어 있습니다.

중앙 웹 보고 및 추적 개요

Cisco Content Security Management Appliance는 여러 Web Security Appliance의 보안 기능에서 오는 정보를 집계하고, 웹 트래픽 패턴과 보안 위험을 모니터링하는 데 사용할 수 있는 데이터를 기록합니다. 보고서를 실시간으로 실행하여 지정된 기간에 시스템 활동을 상호 작용 방식으로 표시할 수도 있고, 보고서를 예약하여 정기적으로 실행할 수도 있습니다. 보고 기능을 사용하여 원시 데이터를 파일로 내보낼 수도 있습니다.

중앙 웹 보고 기능은 네트워크 현황을 이해할 수 있도록 종합 보고서를 생성할 뿐 아니라 드릴다운 기능을 통해 특정 도메인, 사용자, 범주의 트래픽 세부사항을 이해할 수 있도록 지원합니다.

도메인

웹 보고 기능은 도메인에 대해 다음 데이터 요소를 생성하여 도메인 보고서에 수록할 수 있습니다. 예를 들어 Facebook.com 도메인에 대한 보고서를 생성할 때 다음 내용을 포함할 수 있습니다.

- Facebook.com에 액세스한 상위 사용자의 목록
- Facebook.com 내에서 액세스된 상위 URL의 목록

사용자

웹 보고 기능은 사용자에 대해 데이터 요소를 생성하여 사용자 보고서에 수록할 수 있습니다. 예를 들어 'Jamie'라는 제목의 사용자 보고서는 다음 내용을 포함할 수 있습니다.

- 사용자 'Jamie'가 액세스한 상위 도메인의 목록
- 악성코드 또는 바이러스 양성이었던 상위 URL의 목록
- 사용자 'Jamie'가 액세스한 상위 범주의 목록

URL 범주

웹 보고 기능은 URL 범주에 대해 범주 보고서에 수록할 데이터를 생성할 수 있습니다. 예를 들어 범주 '스포츠'에 대한 보고서는 다음 내용을 포함할 수 있습니다.

- '스포츠' 범주에 속한 상위 도메인의 목록
- '스포츠' 범주에 액세스한 상위 사용자의 목록

이 모든 예에서 보고서의 목적은 네트워크의 특정 항목에 대한 종합적인 관점을 제시하여 관리자가 조치를 취할 수 있게 하는 것입니다.

일반

로깅 페이지와 보고 페이지를 비교하는 설명은 로깅 대 보고, 503 페이지를 참조하십시오.

참고 웹 보고에서는 사용자가 이동한 모든 도메인 정보를 검색할 수 있습니다. 즉 액세스한 특정 URL이 아닐 수도 있습니다. URL을 방문한 시간, URL 허용 여부 등 사용자가 액세스한 특정 URL에 대한 정보를 알아보려면 Web Tracking(웹 추적) 페이지의 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지 섹션을 사용할 수 있습니다.

참고 Web Security Appliance는 로컬 보고가 사용되는 경우에만 데이터를 저장합니다. 중앙 집중식 보고가 Web Security Appliance에 대해 활성화된 경우, Web Security Appliance는 System Capacity(시스템 용량) 및 System Status(시스템 상태) 데이터만 유지합니다. 중앙 집중식 웹 보고가 활성화되지 않은 경우 System Capacity(시스템 용량) 및 System Status(시스템 상태) 보고서만 생성됩니다.

Security Management Appliance에서 웹 보고 데이터를 볼 수 있는 여러 방법이 있습니다.

- 인터랙티브 보고서 페이지를 보려면 웹 보고 페이지 설명, 182 페이지 섹션을 참조하십시오.

- 온디맨드 보고서를 생성하려면 온디맨드 웹 보고서 생성 , 243 페이지를 참조하십시오.
- 정기적으로 보고서를 생성하도록 예약하려면 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.
- 전에 실행한 보고서(예약 및 온디맨드)의 아카이브 버전을 보려면 아카이브 웹 보고서 보기 및 관리, 244 페이지를 참조하십시오.
- 개별 트랜잭션에 대한 정보를 보려면 웹 추적 , 245 페이지를 참조하십시오.

중앙 웹 보고 및 추적 설정

중앙 웹 보고 및 추적을 설정하려면 다음 단계를 순서대로 수행합니다.

- Security Management Appliance에서 중앙 웹 보고 활성화 , 179 페이지
  - 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지
- WSA에서 중앙 웹 보고 활성화 , 180 페이지
- 관리 대상 WSA 각각에 중앙 웹 보고 서비스 추가 , 180 페이지
- 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지

Security Management Appliance에서 중앙 웹 보고 활성화

단계 **1** 중앙 웹 보고 기능을 활성화하기에 앞서 이 서비스에 충분한 디스크 공간이 지정되었음을 확인합니다. 디스크 공간 관리 , 487 페이지를 참조하십시오.

단계 **2** [새 웹 인터페이스에만 해당] 레거시 웹 인터페이스를 로드하려면 Security Management Appliance에서 ⚙ 을 클릭합니다.

단계 **3** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Web(**웹**) > Centralized Reporting(**중앙 집중식 보고**)**을 선택합니다.

단계 **4** 시스템 설정 마법사를 실행한 후 처음으로 중앙 보고 기능을 활성화하는 경우

a) **Enable(**활성화**)**을 클릭합니다.

b) 최종 사용자 라이센스 계약을 검토한 후 **Accept(**동의**)**를 클릭합니다.

단계 **5** 중앙 보고 기능을 비활성화했다가 활성화하는 경우

a) **Edit Settings(**설정 수정**)**를 클릭합니다.

b) **Enable Centralized Web Report Services(**중앙 웹 보고서 서비스 활성화**)** 확인란을 선택합니다.

c) 지금 또는 나중에 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지를 처리할 수 있습니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

WSA에서 중앙 웹 보고 활성화

중앙 집중식 보고를 활성화하려면 우선 모든 Web Security Appliance를 구성하고 예상대로 작동하는지 확인해야 합니다.

중앙 집중식 보고를 사용하는 각 Web Security Appliance에서 중앙 집중식 보고를 활성화해야 합니다.

AsyncOS for Cisco Web Security Appliances 사용 설명서의 "중앙 집중식 보고 활성화" 섹션을 참조하십시오.

관리 대상 WSA 각각에 중앙 웹 보고 서비스 추가

수행하는 단계는 또 다른 중앙 관리 기능을 구성할 때 어플라이언스를 이미 추가했는지 여부에 따라 달라집니다.

단계 **1** [새 웹 인터페이스에만 해당] 레거시 웹 인터페이스를 로드하려면 Security Management Appliance에서 ⚙ 을 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 목록에 Web Security Appliance를 이미 추가한 경우

a) Web Security Appliance의 이름을 클릭합니다.

b) **Centralized Reporting(**중앙 집중식 보고**)** 서비스를 선택합니다.

단계 **4** Web Security Appliance를 아직 추가하지 않은 경우

a) Add Web Appliance(웹 어플라이언스 추가)를 클릭합니다.

b) Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 Web Security Appliance의 Management 인터페이스에 대한 IP 주소를 입력합니다.

참고 DNS 이름은 IP Address(IP 주소) 텍스트 필드에 입력해야 합니다. 그러나 **Submit(**제출**)**을 클릭하면 즉시 IP 주소로 해석됩니다.

c) 중앙 보고 서비스가 미리 선택되어 있습니다.

d) **Establish Connection(**연결 설정**)**을 클릭합니다.

e) 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다.

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

f) 페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.

g) **Test Connection(**테스트 연결**)**을 클릭합니다.

h) 테이블 위의 테스트 결과를 읽습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** 중앙 보고를 활성화하려는 WSA 각각에서 이 절차를 반복합니다.

단계 **7** 변경사항을 커밋합니다.

웹 보고서에서 사용자 이름 익명 처리

기본적으로 사용자 이름은 보고 페이지와 PDF에 나타납니다. 그러나 개인 정보 보호를 위해 웹 보고서에서 사용자 이름을 알 수 없게 하는 경우도 있습니다.

참고 이 어플라이언스에 대한 관리자 권한이 있는 사용자는 인터랙티브 보고서를 볼 때 항상 사용자 이름을 볼 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] 레거시 웹 인터페이스를 로드하려면 Security Management Appliance에서 ⚙을 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Web(**웹**) > Centralized Reporting(**중앙 보고**)**를 선택합니다.

단계 **3** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **4** **Anonymize usernames in reports(**보고서에서 사용자 이름 익명 처리**)** 확인란을 선택합니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

웹 보안 보고서 사용

웹 보고 페이지에서는 시스템에 있는 관리되는 Web Security Appliance 하나 또는 전체에 대한 정보를 모니터링할 수 있습니다.

변경 후	확인
보고서 데이터 액세스 및 조회 옵션 보기	보고 데이터를 보는 방법 , 33 페이지
인터랙티브 보고서 페이지의 보기 맞춤 설정	보고 데이터 보기 맞춤화 , 35 페이지
데이터 내에서 특정 트랜잭션에 대한 정보 찾기	웹 추적 , 245 페이지
보고서 정보 인쇄 또는 내보내기	보고/추적 데이터 인쇄 및 내보내기 , 41 페이지
다양한 인터랙티브 보고서 페이지 이해	웹 보고 페이지 설명, 182 페이지
온디맨드 보고서 생성	새 웹 인터페이스의 Web Reporting(웹 보고) 페이지 이해, 212 페이지
일정한 간격으로 또한 사용자가 지정한 시간에 자동으로 보고서가 실행되게 예약	예약 및 온디맨드 웹 보고서 정보, 239 페이지

변경 후	확인
아카이브 온디맨드 및 예약 보고서 보기	아카이브 웹 보고서 보기 및 관리, 244 페이지
데이터 수집 방식 이해	Security Management Appliance에서 보고서를 위한 데이터를 수집하는 방법, 34 페이지

새로운 웹 인터페이스에서 웹 보안 보고서 사용

웹 보고 페이지에서는 시스템에 있는 관리되는 Web Security Appliance 하나 또는 전체에 대한 정보를 모니터링할 수 있습니다.

변경 후	확인
보고서 데이터 액세스 및 조회 옵션 보기	보고 데이터를 보는 방법 , 47 페이지
인터랙티브 보고서 페이지의 보기 맞춤 설정	보고 데이터 보기 맞춤화 , 50 페이지
데이터 내에서 특정 트랜잭션에 대한 정보 찾기	새 웹 인터페이스의 웹 추적, 251 페이지
보고서 정보 인쇄 또는 내보내기	보고/추적 데이터 인쇄 및 내보내기 , 41 페이지
다양한 인터랙티브 보고서 페이지 이해	새 웹 인터페이스의 Web Reporting(웹 보고) 페이지 이해, 212 페이지

웹 보고 페이지 설명

참고 Web Reporting(웹 보고) 탭의 어떤 옵션이 온디맨드 보고서 또는 예약 보고서의 형태로 제공되는지에 대해서는 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.

표 ***45:*** 웹 보고 탭 세부사항

웹 보고 메뉴	작업
웹 보고 개요 , 186 페이지	Overview(개요) 페이지는 Web Security Appliance에 대한 활동 개요를 제공합니다. 이 페이지에는 수신 및 발신 트랜잭션에 대한 그래프와 요약 테이블이 포함되어 있습니다. 자세한 내용은 웹 보고 개요 , 186 페이지를 참조하십시오.

웹 보고 메뉴	작업
사용자 보고서(웹) , 187 페이지	Users(사용자) 페이지는 개별 사용자에 대한 웹 추적 정보를 볼 수 있는 여러 웹 추적 링크를 제공합니다. **Users(**사용자**)** 페이지에서 시스템의 사용자가 인터넷, 특정 사이트 또는 URL에서 보낸 시간 및 대역폭 사용량을 확인할 수 있습니다. **Users(**사용자**)** 페이지의 인터랙티브 사용자 테이블에서 개별 사용자를 클릭하면 그 사용자에 대한 세부사항이 사용자 세부사항 페이지에 나타납니다. **User Details(**사용자 세부사항**)** 페이지에서는 **Web(**웹**) > Reporting(**보고**) > Users(**사용자**)** 페이지의 Users(사용자) 테이블에서 확인한 사용자에 대한 정보를 확인할 수 있습니다. 이 페이지에서는 개별 사용자가 시스템에서 수행한 활동을 조사할 수 있습니다. 사용자 레벨 조사를 진행 중인데 사용자가 어떤 사이트를 방문하는지, 어떤 악성코드 위협을 겪는지, 어떤 URL 범주에 액세스하는지, 이 사이트에서 얼마나 많은 시간을 보내는지 등을 알아야 할 경우 이 페이지가 특히 유용합니다. 자세한 내용은 사용자 보고서(웹) , 187 페이지을 참조하십시오. 시스템의 특정 사용자에 대해서는 사용자 세부사항(웹 보고) , 189 페이지를 참조하십시오.
사용자 수 보고서(웹)	User Count(사용자 수) 페이지는 Centralized Reporting(중앙 집중식 보고)이 활성화된 Web Security Appliance의 인증된 사용자 및 인증되지 않은 사용자의 총 수에 대해 집계된 정보를 제공합니다. 이 페이지에는 지난 30일, 90일, 180일 동안의 고유한 사용자 수가 나열됩니다. 참고 시스템에서 인증된 사용자 및 인증되지 않은 사용자의 총 사용자 수를 1시간마다 계산합니다.
웹 사이트 보고서 , 190 페이지	웹 사이트 페이지에서는 관리 대상 어플라이언스에서 일어나는 활동을 종합적으로 살펴볼 수 있습니다. 이 페이지에서는 특정 시간 범위에 액세스한 고위험 웹 사이트를 모니터링할 수 있습니다. 자세한 내용은 웹 사이트 보고서 , 190 페이지을 참조하십시오.
URL 범주 보고서 , 191 페이지	URL 범주 페이지에서는 다음을 포함하여 방문 중인 상위 URL 범주를 볼 수 있습니다. • 트랜잭션별로 차단 또는 경고 작업을 유발한 상위 URL. • 완료된 트랜잭션, 경고된 트랜잭션, 차단된 트랜잭션을 대상으로 한 지정된 시간 범위의 모든 URL 범주. 인터랙티브 열 제목을 포함한 인터랙티브 테이블이며, 필요에 따라 데이터를 정렬할 수 있습니다. 자세한 내용은 URL 범주 보고서 , 191 페이지을 참조하십시오.

웹 보고 메뉴	작업
애플리케이션 가시성 보고서 , 194 페이지	Application Visibility(애플리케이션 가시성) 페이지에서는 Security Management Appliance 및 Web Security Appliance 내에서 특정 애플리케이션 유형에 적용된 컨트롤을 보고 적용할 수 있습니다. 자세한 내용은 애플리케이션 가시성 보고서 , 194 페이지를 참조하십시오.
악성코드 차단 보고서 , 195 페이지	악성코드 차단 페이지에서는 악성코드 차단 검사 엔진이 지정된 시간 범위에 탐지한 악성코드 포트 및 악성코드 사이트에 대한 정보를 볼 수 있습니다. 보고서의 상단에는 상위 악성코드 포트 및 웹 사이트 각각의 연결 수가 표시됩니다. 하단에는 탐지된 악성코드 포트 및 사이트가 표시됩니다. 자세한 내용은 악성코드 차단 보고서 , 195 페이지을 참조하십시오.
Advanced Malware Protection(파일 평판 및 파일 분석) 보고서 , 199 페이지	3가지 보고 페이지에서 파일 평판 및 분석 데이터를 제시합니다. 자세한 내용은 Advanced Malware Protection(파일 평판 및 파일 분석) 보고서 , 199 페이지를 참조하십시오.
클라이언트 악성코드 위험 보고서 , 203 페이지	클라이언트 악성코드 리스크 페이지는 보안 관련 보고 페이지이며, 비정상적으로 악성코드 사이트에 자주 연결하는 개별 클라이언트 컴퓨터를 파악하는 데 사용할 수 있습니다. 자세한 내용은 클라이언트 악성코드 위험 보고서 , 203 페이지을 참조하십시오.
웹 평판 필터 보고서 , 204 페이지	지정된 시간 범위의 트랜잭션에 대한 웹 평판 필터링 보고를 볼 수 있습니다. 자세한 내용은 웹 평판 필터 보고서 , 204 페이지를 참조하십시오.
L4 Traffic Monitor 보고서 , 206 페이지	지정된 시간 범위에 L4 Traffic Monitor에서 탐지한 악성코드 포트 및 악성코드 사이트에 대한 정보를 볼 수 있습니다. 자세한 내용은 L4 Traffic Monitor 보고서 , 206 페이지을 참조하십시오.
SOCKS 프록시 보고서 , 208 페이지	목적지 및 사용자를 포함하여 SOCKS 프록시 트랜잭션에 대한 데이터를 볼 수 있습니다. 자세한 내용은 SOCKS 프록시 보고서 , 208 페이지을 참조하십시오.
사용자 위치별 보고서 , 208 페이지	사용자 위치별 보고서 페이지에서는 모바일 사용자가 로컬 또는 원격 시스템에서 어떤 활동을 하는지 확인할 수 있습니다. 자세한 내용은 사용자 위치별 보고서 , 208 페이지을 참조하십시오.

웹 보고 메뉴	작업
웹 추적 , 245 페이지	웹 추적 페이지에서는 다음 유형의 질문에 답할 수 있습니다. • 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지에서는 어플라이언스에서 처리 중인 웹 트래픽의 유형 등 웹과 관련된 기본적인 정보를 추적하고 확인할 수 있습니다. 여기에는 시간 범위, 사용자 ID 및 클라이언트 IP 주소와 같은 정보뿐 아니라 특정 URL 유형, 각 연결에서 소모하는 대역폭의 양 등을 확인하고 특정 사용자의 웹 사용량을 추적할 수도 있습니다. • L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지에서는 악성코드 전송 활동과 관련된 사이트, 포트, 클라이언트 IP 주소에 대한 L4TM 데이터를 검색할 수 있습니다. • SOCKS 프록시에서 처리되는 트랜잭션 검색 , 250 페이지에서는 SOCKS 프록시에서 처리하는 트랜잭션을 검색할 수 있습니다. 자세한 내용은 웹 추적 , 245 페이지를 참조하십시오.
System Capacity(시스템 용량) 페이지, 210 페이지	Security Management Appliance에 보고 데이터를 전송하는 전체적인 워크로드를 볼 수 있습니다. 자세한 내용은 System Capacity(시스템 용량) 페이지, 210 페이지를 참조하십시오.
데이터 가용성 페이지, 211 페이지	보고 데이터가 Security Management Appliance에 미치는 영향을 각 어플라이언스에 대해 간략하게 볼 수 있습니다. 자세한 내용은 데이터 가용성 페이지, 211 페이지를 참조하십시오.
예약 보고서	지정된 시간 범위에 대해 보고서를 예약할 수 있습니다. 자세한 내용은 예약 및 온디맨드 웹 보고서 정보, 239 페이지을 참조하십시오.
Archived Reports(보관된 보고서)	지정된 시간 범위에 대해 보고서를 아카이빙할 수 있습니다. 자세한 내용은 아카이브 웹 보고서 보기 및 관리, 244 페이지을 참조하십시오.

참고 확장 상위 URL 범주 및 상위 애플리케이션 유형에 대한 추가 보고서를 비롯하여 웹 보고 범주 대부분에 대한 보고서를 예약할 수 있습니다. 보고서 예약에 대한 자세한 내용은 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.

소요 시간 정보

여러 테이블의 Time Spent(소요 시간) 열은 사용자가 웹 페이지에 보낸 시간을 나타냅니다. 사용자 조사에서는 사용자가 각 URL 범주에서 보낸 시간입니다. URL 추적에서는 각 사용자가 해당 URL에서 보낸 시간입니다.

트랜잭션 이벤트가 'viewed' 태그를 갖게 되면, 즉 사용자가 특정 URL을 방문하면 'Time Spent' 값이 계산되기 시작하고 웹 보고 테이블의 필드로 추가됩니다.

AsyncOS는 소요 시간을 계산하기 위해 각 활성 사용자에게 1분간의 활동에 대해 60초를 부여합니다. 1분이 끝나면 각 사용자의 소요 시간은 그 사용자가 방문한 여러 도메인에 고르게 분배됩니다. 예를 들어 사용자가 활성 상태의 1분간 서로 다른 도메인 4개를 방문할 경우 각 도메인에서 15초를 보낸 것으로 간주합니다.

소요 시간의 값에서는 다음 사항을 고려합니다.

- 활성 사용자란 애플리케이션을 통해 HTTP 트래픽을 보내고 AsyncOS에서 "페이지 뷰"로 간주하는 웹 사이트를 방문한 사용자 이름 또는 IP 주소로 정의됩니다.
- AsyncOS는 페이지 뷰를 사용자가 시작하는 HTTP 요청으로 정의합니다. 클라이언트 애플리케이션에서 시작한 요청이 아닙니다. AsyncOS에서는 휴리스틱 알고리즘을 사용하여 최선 노력 추측으로 사용자 페이지 뷰를 파악합니다.

단위는 시간:분 형식으로 표시됩니다.

웹 보고 개요

Web(웹) > Reporting(보고) > Overview(개요) 페이지에서는 Web Security Appliance에 대한 활동 개요를 제공합니다. 이 페이지에는 수신 및 발신 트랜잭션에 대한 그래프와 요약 테이블이 포함되어 있습니다.

상위 레벨에서 **Overview(개요)** 페이지는 URL 및 사용자 사용량, 웹 프록시 활동, 각종 트랜잭션 요약에 대한 통계를 제공합니다. 트랜잭션 요약에서는 이를테면 의심스러운 트랜잭션의 추세를 더 면밀하게 파악할 수 있습니다. 또한 그래프를 통해 이 의심스러운 트랜잭션 중 몇 개가 차단되었고 어떤 식으로 차단되고 있는지 알 수 있습니다.

Overview(개요) 페이지의 하단에서는 사용량을 다룹니다. 즉 조회 중인 상위 URL 범주, 차단 중인 상위 애플리케이션 유형 및 범주, 이 차단 또는 경고를 발생시키는 상위 사용자 등입니다.

표 ***46: Web Reporting Overview(***웹 보고 개요***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
데이터 보기	Overview(개요) 데이터를 볼 Web Security Appliance를 선택하거나 All Web Appliances(모든 웹 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지도 참조하십시오.
총 웹 프록시 작업	이 섹션에서는 현재 Security Management Appliance에 의해 관리되고 있는 Web Security Appliance가 보고하는 웹 프록시 활동을 볼 수 있습니다. 이 섹션은 실제 트랜잭션 수(세로 크기) 및 활동이 발생한 대략적인 날짜(가로 타임라인)를 표시합니다.

섹션	설명
웹 프록시 요약	의심스러운 웹 프록시 활동 또는 정상 프록시 활동의 비율을 볼 수 있습니다. 총트랜잭션 수도 포함됩니다.
L4 Traffic Monitor 요약	이 섹션은 현재 Security Management Appliance에 의해 관리되고 있는 Web Security Appliance가 보고하는 L4 트래픽을 보고합니다.
의심되는 트랜잭션	관리자가 의심스러운 것으로 표시한 웹 트랜잭션을 볼 수 있습니다. 실제 트랜잭션 수(세로축)와 그 활동이 일어난 대략적인 날짜(가로축 타임라인)를 표시합니다.
의심되는 트랜잭션 요약	의심되는 트랜잭션 중 차단되었거나 경고된 것의 비율을 볼 수 있습니다. 탐지 및 차단된 트랜잭션의 유형 그리고 트랜잭션이 차단된 실제 횟수도 확인할 수 있습니다.
전체 트랜잭션별 상위 URL 범주	차단된 상위 10개 URL 범주를 표시합니다. URL 범주 유형(세로축) 및 이 범주 유형이 실제로 차단된 횟수(가로축)도 보여줍니다. 사전 정의 URL 범주의 집합은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.
전체 트랜잭션별 상위 애플리케이션 유형	차단된 상위 애플리케이션 범주를 표시합니다. 실제 애플리케이션 유형(세로축) 및 이 애플리케이션 유형이 실제로 차단된 횟수(가로축)도 보여줍니다.
탐지된 상위 악성코드 범주	탐지된 모든 악성코드 범주를 표시합니다.
상위 사용자 차단 또는 경고 트랜잭션	차단되었거나 경고된 트랜잭션을 생성하는 실제 사용자를 표시합니다. IP 주소 또는 사용자 이름으로 표시할 수 있습니다. 사용자 이름을 식별 불가능하게 하려면 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지를 참조하십시오.
웹 트래픽 탭 상태	태핑되지 않은 트래픽 트랜잭션 및 태핑된 트래픽 트랜잭션을 그래프 형식으로 표시합니다.
웹 트래픽 탭 요약	태핑된 트래픽 트랜잭션 및 태핑되지 않은 트래픽 트랜잭션의 요약을 총 트래픽 트랜잭션과 함께 표시합니다.
태핑된 HTTP/HTTPS 트래픽	태핑된 HTTP 및 HTTPS 트래픽 트랜잭션을 그래프 형식으로 표시합니다.
태핑된 트래픽 요약	HTTP 및 HTTPS 트래픽 트랜잭션의 요약을 총 HTTP/HTTPS 트래픽 트랜잭션과 함께 표시합니다.

사용자 보고서(웹)

Web(웹) > Reporting(보고) > Users(사용자) 페이지에서 제공하는 여러 링크를 통해 개별 사용자에 대한 웹 보고 정보를 볼 수 있습니다.

Users(사용자) 페이지에서는 시스템의 한 명 이상의 사용자가 인터넷, 특정 사이트 또는 URL에서 얼마나 시간을 보냈는지, 그리고 해당 사용자가 사용하는 대역폭이 얼마인지를 볼 수 있습니다.

Users(사용자) 페이지에서 시스템의 사용자에 대한 다음과 같은 정보를 볼 수 있습니다.

표 ***47: Web Reporting Users***(웹 보고 사용자) 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
차단된 트랜잭션별 상위 사용자	상위 사용자를 IP 주소 또는 사용자 이름으로 나열하며(세로축) 이 사용자의 차단된 트랜잭션 수(가로축)를 보여줍니다. 보고서에서는 사용자 이름 또는 IP를 식별 불가능하게 만들 수 있습니다. 이 페이지 또는 예약 보고서에서 사용자 이름을 식별 불가능하게 만드는 방법에 대해서는 Security Management Appliance에서 중앙 웹 보고 활성화 , 179 페이지섹션을 참조하십시오. 기본 설정은 모든 사용자 이름이 나타나는 것입니다. 사용자 이름을 숨기려면 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지를 참조하십시오.
사용된 대역폭별 상위 사용자	시스템에서 가장 많은 대역폭(가로축, 사용량 기가바이트 단위)을 사용하는 상위 사용자(세로축)를 IP 주소 또는 사용자 이름으로 표시합니다.
사용자 테이블	특정 사용자 ID 또는 클라이언트 IP 주소를 찾을 수 있습니다. 사용자 섹션 맨 아래의 텍스트 필드에 특정 사용자 ID 또는 클라이언트 IP 주소를 입력하고 **Find User ID or Client IP Address**(사용자 **ID** 또는 클라이언트 **IP** 주소 찾기)를 클릭합니다. IP 주소가 정확하게 일치하지 않아도 결과를 얻을 수 있습니다. 사용자 테이블에서 특정 사용자를 클릭하여 더 구체적인 정보를 얻을 수 있습니다. 이 정보는 User Details(사용자 세부사항) 페이지에 나타납니다. User Details(사용자 세부사항) 페이지에 대한 자세한 내용은 사용자 세부사항(웹 보고) , 189 페이지를 참조하십시오.

참고 클라이언트 IP 주소 대신 사용자 ID를 보려면, LDAP 서버에서 사용자 정보를 가져오도록 Security Management Appliance를 설정해야 합니다. 자세한 내용은 LDAP와의 통합, 377 페이지장의 LDAP 서버 프로필 생성, 378 페이지를 참조하십시오.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

Users(사용자) 페이지를 활용하는 예를 보려면 예 1: 사용자 조사 , 567 페이지를 참조하십시오.

참고 사용자 페이지에 대한 보고서를 생성하거나 예약할 수 있습니다. 자세한 내용은 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.

사용자 세부사항(웹 보고)

User Details(사용자 세부사항) 페이지에서는 **Web**(웹) > **Reporting**(보고) > **Users**(사용자) 페이지의 인터랙티브 Users(사용자) 테이블에서 확인한 사용자에 대한 정보를 확인할 수 있습니다.

User Details(사용자 세부사항) 페이지에서는 개별 사용자가 시스템에서 수행한 활동을 조사할 수 있습니다. 사용자 레벨 조사를 진행 중인데 사용자가 어떤 사이트를 방문하는지, 어떤 악성코드 위협을 겪는지, 어떤 URL 범주에 액세스하는지, 이 사이트에서 얼마나 많은 시간을 보내는지 등을 알아야 할 경우 이 페이지가 특히 유용합니다.

특정 사용자에 대한 **User Details**(사용자 세부사항) 페이지를 표시하려면 **Web**(웹) > **Users**(사용자) 페이지의 사용자 테이블에서 해당 사용자를 클릭합니다.

User Details(사용자 세부사항) 페이지에서 시스템의 개별 사용자에 대한 다음 정보를 볼 수 있습니다.

표 ***48: Web Reporting User Details***(웹 보고 사용자 세부 정보)*:* 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 포함되는 데이터의 시간 범위를 선택할 수 있는 메뉴. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
전체 트랜잭션별 URL 범주	특정 사용자가 이용 중인 URL 범주를 나열합니다. 사전 정의 URL 범주의 집합은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.
전체 트랜잭션별 추세	이 그래프는 사용자가 웹에 액세스한 시간을 표시합니다. 이를테면 하루 중 특정 시간대에 웹 트래픽이 급증했는지 여부 및 그 시각을 보여줍니다. 시간 범위 드롭다운 목록으로 이 그래프를 확장하여 해당 사용자가 웹에 있던 시간 범위를 더 면밀하게 또는 더 간략하게 표시할 수 있습니다.
매치하는 URL 범주	완료된 트랜잭션 및 차단된 트랜잭션 모두에 대해 매치된 범주를 표시합니다. 여기서는 특정 URL 범주를 찾을 수도 있습니다. 맨 아래의 텍스트 필드에 URL 범주를 입력하고 **Find URL Category**(URL 범주 찾기)를 클릭합니다. 범주가 정확하게 일치하지 않아도 됩니다. 사전 정의 URL 범주의 집합은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.
매치하는 도메인	여기서는 이 사용자가 액세스한 특정 도메인 또는 IP 주소에 대해 알아낼 수 있습니다. 또한 이 범주에서 보낸 시간 및 열 보기에서 설정한 기타 다양한 정보도 볼 수 있습니다. 맨 아래의 텍스트 필드에 도메인 또는 IP 주소를 입력하고 **Find Domain or IP**(도메인 또는 **IP** 찾기)를 클릭합니다. 도메인 또는 IP 주소가 정확하게 일치하지 않아도 됩니다.

섹션	설명
매치하는 애플리케이션	특정 사용자가 이용 중인 애플리케이션을 찾을 수 있습니다. 예를 들어 사용자가 많은 플래시 비디오를 사용해야 하는 웹 사이트에 액세스하고 있다면 애플리케이션 열에서 해당 애플리케이션 유형을 확인합니다. 맨 아래의 텍스트 필드에 애플리케이션 이름을 입력하고 **Find Application**(애플리케이션 찾기)을 클릭합니다. 애플리케이션 이름이 정확하게 일치하지 않아도 됩니다.
탐지된 악성코드 위협	이 테이블에서는 특정 사용자가 유발하는 상위 악성코드 위협을 확인할 수 있습니다. Find Malware Threat(악성코드 위협 찾기) 필드에서 특정 악성코드 위협 이름에 대한 데이터를 검색할 수 있습니다. 악성코드 위협 이름을 입력하고 Find Malware Threat(악성코드 위협 찾기)를 클릭합니다. 악성코드 위협의 이름이 정확하게 일치하지 않아도 됩니다.
매치하는 정책	이 사용자가 웹에 액세스할 때 적용되는 정책 그룹을 찾을 수 있습니다. 맨 아래의 텍스트 필드에 정책 이름을 입력하고 **Find Policy**(정책 찾기)를 클릭합니다. 정책 이름이 정확하게 일치하지 않아도 됩니다.

참고 클라이언트 악성코드 위험 세부사항 테이블: 클라이언트 보고서에서는 사용자 이름 끝에 별표(*)를 표시할 때가 있습니다. 예를 들어 “jsmith” 및 “jsmith*” 모두에 한 항목을 표시합니다. 별표(*)가 있는 사용자 이름은 그 사용자가 부여한 이름이며, 인증 서버에서 확인하지 않았습니다. 해당 시점에 인증 서버를 사용할 수 없었고 애플리케이션 서비스가 제공되지 않을 때 트래픽을 허용하도록 어플라이언스가 구성된 경우 이렇게 됩니다.

사용자 세부사항 페이지를 활용하는 예를 보려면 예 1: 사용자 조사 , 567 페이지를 참조하십시오.

사용자 수 보고서(웹)

Web(웹) >**Reporting**(보고) > **User Count**(사용자 수) 페이지에는 Centralized Reporting(중앙 집중식 보고)이 활성화된 Web Security Appliance의 인증된 사용자 및 인증되지 않은 사용자의 총 수에 대해 집계된 정보가 표시됩니다. 이 페이지에는 지난 30일, 90일, 180일 동안의 고유한 사용자 수가 나열됩니다.

참고 시스템에서 인증된 사용자 및 인증되지 않은 사용자의 총 사용자 수를 1시간마다 계산합니다.

웹 사이트 보고서

Web(웹) > **Reporting**(보고) > **Web Sites**(웹 사이트) 페이지에서는 관리 대상 어플라이언스에서 일어나는 활동을 종합적으로 살펴볼 수 있습니다. 이 페이지에서는 특정 시간 범위에 액세스한 고위험 웹 사이트를 모니터링할 수 있습니다.

Web Sites(웹사이트**)** 페이지에서 다음 정보를 볼 수 있습니다.

표 ***49: Web Reporting Web Sites(***웹 보고 웹 사이트***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
전체 트랜잭션별 상위 도메인	사이트에서 방문하고 있는 상위 도메인을 그래프 형식으로 보여줍니다.
차단된 트랜잭션별 상위 도메인	트랜잭션별로 차단 조치를 유발한 상위 도메인을 그래프 형식으로 보여줍니다. 예를 들어 어떤 사용자가 특정 도메인을 방문했고, 설정된 어떤 정책 때문에 차단 조치가 실행되었습니다. 이 도메인은 이 그래프에서 차단된 트랜잭션으로 표시되고 차단 조치를 유발한 도메인 사이트가 목록에 포함됩니다.
매치하는 도메인	사이트에서 방문하고 있는 도메인을 인터랙티브 테이블로 보여줍니다. 이 테이블에서 특정 도메인을 클릭하여 더 세부적인 정보에 액세스할 수 있습니다. 웹 추적 페이지의 프록시 서비스 탭이 나타나고 추적 정보 및 특정 도메인이 차단된 이유를 확인할 수 있습니다. 특정 도메인을 클릭하면 그 도메인의 상위 사용자, 상위 트랜잭션, 매치한 URL 범주, 탐지된 악성코드 위협을 볼 수 있습니다. 웹 추적을 활용하는 예를 보려면 예 2: URL 추적, 569 페이지를 참조하십시오. 참고 이 데이터를 CSV 파일로 내보낼 경우 처음 30만 개 항목만 내보내집니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

참고 웹 사이트 페이지의 정보에 대한 보고서를 생성하거나 예약할 수 있습니다. 자세한 내용은 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.

URL 범주 보고서

Web(웹**) > Reporting(**보고**) > URL Categories(URL** 카테고리**)** 페이지에서는 시스템의 사용자가 방문 중인 사이트의 URL 카테고리를 볼 수 있습니다.

URL Categories(URL 카테고리**)** 페이지에서 다음 정보를 볼 수 있습니다.

표 *50: Web Reporting URL Categories*(웹 보고 *URL* 카테고리) 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
전체 트랜잭션별 상위 URL 범주	사이트에서 방문 중인 상위 URL 범주를 그래프 형식으로 보여줍니다.
차단 및 경고된 트랜잭션별 상위 URL 범주	트랜잭션별로 차단 또는 경고 조치를 유발한 상위 URL을 그래프 형식으로 보여줍니다. 예를 들어 어떤 사용자가 특정 URL을 방문했고, 설정된 어떤 정책 때문에 차단 또는 경고 조치가 실행되었습니다. 그러면 이 URL은 그래프에서 차단된 또는 경고된 트랜잭션으로 표시됩니다.
매치하는 URL 범주	지정된 시간 범위의 트랜잭션 특성을 URL 범주별로 보여줍니다. 각 범주의 대역폭 사용량 및 소요 시간도 나타납니다. 미분류 URL이 많을 경우 미분류 URL 줄이기 , 192 페이지를 참조하십시오.
바이패스한 URL 필터링	URL 필터링 이전에 일어난 정책, 포트, admin 사용자 에이전트 차단을 나타냅니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

참고 이 페이지보다 세부적인 보고서를 생성하려면 상위 URL 범주 - 확장, 241 페이지를 참조하십시오.

- 데이터 가용성이 URL 카테고리에 대한 예약 보고서에 사용된 경우 어플라이언스 중 하나에서 데이터 공백이 있으면 페이지의 맨 아래에 “Some data in this time range was unavailable.(이 시간 범위의 일부 데이터를 사용할 수 없습니다).”이라는 메시지가 표시됩니다. 공백이 없으면 아무것도 표시되지 않습니다.

미분류 URL 줄이기

범주화되지 않은 URL의 비율이 15-20%보다 높으면 다음 옵션을 고려해볼 수 있습니다.

- 특정 현지화된 URL에 대해 맞춤 URL 범주를 생성하고 특정 사용자 또는 그룹 정책에 적용할 수 있습니다. 그러면 이 트랜잭션은 "바이패스한 URL 필터링" 통계에 포함됩니다. 이렇게 하려면 AsyncOS for Cisco Web Security Appliances 사용 설명서에서 맞춤형 URL 카테고리에 대한 정보를 참조하십시오.
- 기존 또는 다른 범주에 포함해야 하는 사이트에 대해서는 오분류 및 미분류 URL 보고 , 193 페이지를 참조하십시오.

URL 카테고리 집합 업데이트 및 보고

URL 범주 집합 업데이트 준비 및 관리 , 365 페이지에 설명된 대로, 사전 정의된 URL 범주 집합은 Security Management Appliance에서 주기적으로 업데이트될 수 있습니다.

이러한 업데이트가 발생하면, 데이터가 너무 오래되어 포함될 수 없을 때까지 이전 범주에 대한 데이터가 보고서 및 웹 추적 결과에 계속 나타납니다. 범주 집합 업데이트 이후에 생성된 보고서 데이터는 새 범주를 사용하므로 기존 범주와 새 범주가 동일한 보고서에 나타날 수 있습니다.

기존 범주와 새 범주 간에 콘텐츠 중복이 있을 경우 유효한 통계를 얻으려면 더 면밀하게 보고서 결과를 검토해야 합니다. 예를 들어 지금 보고 있는 시간 범위에서 "Instant Messaging" 및 "Web-based Chat" 범주가 "Chat and Instant Messaging" 범주로 병합된 경우, 병합 전에 "Instant Messaging" 및 "Web-based Chat" 범주의 사이트에 방문한 것은 "Chat and Instant Messaging" 합계에 포함되지 않습니다. 또한 병합 이후에 "Instant Messaging" 또는 "Web-based Chat" 사이트에 방문한 것은 "Instant Messaging" 또는 "Web-based Chat" 범주의 합계에 포함되지 않습니다.

URL 범주와 다른 보고 페이지 연계 사용

URL 범주 페이지를 Application Visibility(애플리케이션 가시성) 페이지, 216 페이지 및 Users(사용자) 페이지, 225 페이지와 함께 사용하여 특정 사용자, 특정 사용자가 액세스를 시도하는 애플리케이션 또는 웹 사이트 유형을 조사할 수 있습니다.

예를 들어 URL 범주 페이지, 222 페이지에서는 인사부에 대한 상위 레벨 보고서를 생성합니다. 여기서는 사이트에서 방문한 모든 URL 범주를 자세히 보여줍니다. 동일한 페이지에서 URL 범주 'Streaming Media'에 대한 세부 사항을 URL 범주 인터랙티브 테이블에서 수집할 수 있습니다. 스트리밍 미디어 범주 링크를 클릭하면 특정 URL 범주 보고서 페이지를 볼 수 있습니다. 이 페이지에서는 스트리밍 미디어 사이트를 방문 중인 상위 사용자를 표시할 뿐 아니라(전체 트랜잭션의 카테고리별 상위 사용자 섹션) YouTube.com 또는 QuickPlay.com과 같은 방문한 도메인(매치하는 도메인 인터랙티브 테이블)도 표시합니다.

여기서는 특정 사용자에 대한 더 자세한 정보를 수집하게 됩니다. 이 사용자의 사용량이 이례적이라면 과연 무엇에 액세스하고 있는지 정확히 알아보고 싶습니다. 사용자 인터랙티브 테이블에서 그 사용자를 클릭할 수 있습니다. 그러면 Users(사용자) 페이지, 225 페이지로 이동합니다. 여기서 이 사용자의 추세를 확인하고 웹에서 정확히 무슨 일을 했는지 알 수 있습니다.

더 나아가 인터랙티브 테이블에서 완료된 트랜잭션 링크를 클릭하면 웹 추적 세부 사항까지 볼 수 있습니다. 이는 웹 추적 페이지에 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지을 표시하는데, 여기서는 사용자가 사이트에 액세스한 날짜, 전체 URL, 그 URL에서 보낸 시간 등의 실제 세부사항을 확인할 수 있습니다.

URL 범주 페이지를 활용하는 또 다른 예를 보려면 예 3: 최다 방문 URL 범주 조사, 569 페이지를 참조하십시오.

오분류 및 미분류 URL 보고

다음 URL에서 오분류 및 미분류 URL을 보고할 수 있습니다.

https://securityhub.cisco.com/web/submit_urls

제출한 자료를 평가하여 후속 규칙 업데이트에 포함합니다.

제출된 URL의 상태를 확인하려면 이 페이지에 있는 **Status on Submitted URLs(**제출된 **URL**의 상태**)** 탭을 클릭합니다.

애플리케이션 가시성 보고서

참고 애플리케이션 가시성에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 '애플리케이션 가시성 및 컨트롤 이해' 장을 참조하십시오.

Web(웹**) > Reporting(**보고**) > Application Visibility(**애플리케이션 가시성**)** 페이지에서는 Security Management Appliance 및 Web Security Appliance 내 특정 애플리케이션 유형에 컨트롤을 적용할 수 있습니다.

애플리케이션 컨트롤은 URL 필터링만 사용하는 것보다 웹 트래픽을 더 세부적으로 제어할 수 있습니다. 예를 들어 다음 유형의 애플리케이션 및 애플리케이션 유형을 더 잘 제어할 수 있습니다.

- 회피성 애플리케이션 - 익명 서비스, 암호화 터널 등
- 협업 애플리케이션 - Cisco WebEx, Facebook, 인스턴트 메시징 등
- 리소스 집약적인 애플리케이션 - 스트리밍 미디어

애플리케이션과 애플리케이션 유형의 차이점 이해

보고서를 위해 관련 애플리케이션을 제어할 수 있도록 애플리케이션과 애플리케이션 유형의 차이점을 이해하는 것이 중요합니다.

- 애플리케이션 유형 하나 이상의 애플리케이션을 포함하는 범주. 예를 들어 검색 엔진은 Google Search, Craigslist와 같은 검색 엔진을 포함할 수 있는 애플리케이션 유형입니다. 인스턴트 메시징 역시 Yahoo Instant Messenger, Cisco WebEx 등을 포함할 수 있는 애플리케이션 유형 범주입니다. Facebook도 애플리케이션 유형입니다.
- 애플리케이션**.** 애플리케이션 유형에 속하는 특정 애플리케이션. YouTube는 미디어 애플리케이션 유형에 속하는 애플리케이션입니다.
- 애플리케이션 동작**.** 사용자가 어떤 애플리케이션 내에서 수행할 수 있는 특정 작업 또는 동작. 예를 들어 사용자가 Yahoo Messenger와 같은 애플리케이션을 사용하면서 파일을 전송할 수 있습니다. 모든 애플리케이션의 애플리케이션 동작이 구성 가능한 것은 아닙니다.

참고 AVC(Application Visibility and Control) 엔진을 사용하여 Facebook 활동을 제어하는 방법에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 '애플리케이션 가시성 및 컨트롤 이해' 장을 참조하십시오.

Application Visibility(애플리케이션 가시성**)** 페이지에서 다음 정보를 볼 수 있습니다.

표 ***51: Web Reporting Application Visibility(***웹 보고 애플리케이션 가시성***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
전체 트랜잭션별 상위 애플리케이션 유형	사이트에서 방문 중인 애플리케이션 유형을 그래프 형식으로 보여줍니다. 예를 들어 Yahoo Instant Messenger와 같은 인스턴트 메시징 툴, Facebook, 프레젠테이션 애플리케이션 유형이 있습니다.
차단된 트랜잭션별 상위 애플리케이션	트랜잭션별로 차단 조치를 유발한 상위 애플리케이션 유형을 그래프 형식으로 보여줍니다. 예를 들어 어떤 사용자가 특정 애플리케이션 유형, 이를테면 Google Talk 또는 Yahoo Instant Messenger를 시작하려 했습니다. 설정된 어떤 정책 때문에 차단 조치가 실행되었습니다. 그러면 이 애플리케이션은 그래프에서 차단된 또는 경고된 트랜잭션으로 표시됩니다.
매치하는 애플리케이션 유형	이 인터랙티브 테이블에서는 전체 트랜잭션의 상위 애플리케이션 유형 테이블에 나열된 애플리케이션 유형에 대한 자세한 정보를 볼 수 있습니다. 애플리케이션 열에서 세부사항을 표시할 애플리케이션을 클릭할 수 있습니다.
매치하는 애플리케이션	지정된 시간 범위의 모든 애플리케이션을 표시합니다. 인터랙티브 열 제목을 포함한 인터랙티브 테이블이며, 필요에 따라 데이터를 정렬할 수 있습니다. 매치하는 애플리케이션 섹션에 표시할 열을 구성할 수 있습니다. 이 섹션에서 열을 구성하는 것에 대한 자세한 내용은 웹 보안 보고서 사용, 181 페이지를 참조하십시오. 애플리케이션 테이블에 표시할 항목을 선택한 다음 **Items Displayed(**표시 항목**)** 드롭다운 메뉴에서는 몇 개의 항목을 표시할지 선택할 수 있습니다. 10, 20, 50, 100 중에서 선택합니다. 또한 매치하는 애플리케이션 섹션 내에서 특정 애플리케이션을 찾을 수 있습니다. 맨 아래의 텍스트 필드에 애플리케이션 이름을 입력하고 **Find Application(**애플리케이션 찾기**)**을 클릭합니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

참고 애플리케이션 가시성 페이지의 정보에 대한 예약 보고서를 생성할 수 있습니다. 보고서 예약에 대해서는 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.

악성코드 차단 보고서

Web(웹**) > Reporting(**보고**) > Anti-Malware(**악성코드 차단**)** 페이지는 보안 관련 보고서 페이지이며, 활성화된 검사 엔진(Webroot, Sophos, McAfee, Adaptive Scanning)의 검사 결과를 반영합니다.

이 페이지를 사용하여 웹 기반 악성코드 위협을 식별하고 모니터링할 수 있습니다.

참고 L4 Traffic Monitor에서 찾은 악성코드에 대한 데이터를 보려면 L4 Traffic Monitor 보고서 , 206 페이지를 참조하십시오.

Anti-Malware(악성코드 차단**)** 페이지에서 다음 정보를 볼 수 있습니다.

표 ***52: Web Reporting Anti-Malware(***웹 보고 악성코드 차단***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
상위 악성코드 범주: 모니터링 또는 차단	지정된 범주 유형으로 탐지된 상위 악성코드 범주를 표시합니다. 이 정보는 그래프 형식으로 표시됩니다. 유효한 악성코드 범주에 대해서는 악성코드 카테고리 설명, 197 페이지를 참조하십시오.
상위 악성코드 위협: 모니터링 또는 차단	상위 악성코드 위협을 표시합니다. 이 정보는 그래프 형식으로 표시됩니다.
악성코드 범주	이 인터랙티브 테이블에서는 상위 악성코드 범주 차트에 표시된 특정 악성코드 범주에 대한 자세한 정보를 제공합니다. 악성코드 범주 인터랙티브 테이블에서 어떤 링크를 클릭하면 개별 악성코드 범주 및 네트워크에서의 위치에 대한 자세한 정보를 볼 수 있습니다. 예외: 보안 침해 휴리스틱 링크를 클릭하면 이 범주의 트랜잭션이 발생한 시점을 보여주는 차트가 나타납니다. 유효한 악성코드 범주에 대해서는 악성코드 카테고리 설명, 197 페이지를 참조하십시오.
악성코드 위협	이 인터랙티브 테이블에서는 상위 악성코드 위협 섹션에 표시된 특정 악성코드 위협에 대한 자세한 정보를 제공합니다. “Outbreak(보안 침해)” 레이블과 숫자가 표시된 위협은 다른 검사 엔진과 상관없이 Adaptive Scanning 기능에서 식별한 위협입니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

악성코드 범주 보고서

이 페이지에서는 개별 악성코드 범주 및 네트워크에서 수행하는 활동에 대한 자세한 정보를 볼 수 있습니다.

악성코드 범주 보고서 페이지에 액세스하려면 다음을 수행합니다.

단계 **1** Security Management Appliance의 드롭다운 목록에서 **Web(웹)**을 선택합니다.

단계 **2** **Monitoring(모니터링) > Anti-Malware(악성코드 차단)** 페이지를 선택합니다.

단계 **3** Malware Categories(악성코드 범주) 인터랙티브 테이블의 Malware Category(악성코드 범주) 열에서 범주를 클릭합니다.

단계 **4** 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

악성코드 위협 보고서

특정 위협에 대해 위험한 상태인 클라이언트를 보여줍니다. 감염되었을 가능성이 있는 클라이언트의 목록 및 클라이언트 세부사항 페이지 링크를 표시합니다. 보고서 맨 위의 추세 그래프는 지정된 시간 범위에 어떤 위협에 대해 모니터링되고 차단된 트랜잭션을 표시합니다. 맨 아래의 테이블은 지정된 시간 범위에 어떤 위협에 대해 모니터링되고 차단된 트랜잭션의 실제 개수를 표시합니다.

이 보고서를 보려면 악성코드 차단 보고서 페이지의 악성코드 범주 열에 있는 범주를 클릭합니다.

자세한 내용은 테이블 아래의 **Support Portal Malware Details(지원 포털 악성코드 세부사항)**를 클릭하여 확인하십시오.

악성코드 카테고리 설명

Web Security Appliance는 다음의 악성코드 유형을 차단할 수 있습니다.

악성코드 유형	설명
애드웨어	사용자를 판매할 제품으로 연결하는 모든 소프트웨어 실행 파일 및 플러그인을 포함합니다. 일부 애드웨어 애플리케이션은 별도의 프로세스가 동시에 실행되어 서로 모니터링하면서 영구적인 수정을 보장합니다. 시스템이 시작할 때마다 자동으로 실행되게 하는 변형도 있습니다. 보안 설정을 변경하여 사용자가 브라우저 검색 옵션, 바탕화면, 기타 시스템 설정을 변경하지 못하게 하는 프로그램도 있습니다.
브라우저 헬퍼 개체	브라우저 플러그인이며 광고 서비스 또는 사용자 설정 하이재킹과 관련된 다양한 기능을 수행할 수 있습니다.
상업용 시스템 모니터	상업용 시스템 모니터는 법적인 수단을 통해 적법한 라이센스로 확보할 수 있는 시스템 모니터 특성이 포함된 소프트웨어 부분입니다.
다이얼러	사용자의 모뎀 또는 기타 인터넷 액세스 유형을 이용하여 어떤 전화선 또는 사이트에 연결함으로써 완전한 사전 고지에 의한 사용자 동의 없이 장거리 통화 요금이 부과되게 하는 프로그램입니다.
일반 스파이웨어	스파이웨어는 컴퓨터에 설치되는 일종의 악성코드이며, 사용자가 모르는 사이에 사용자에 대한 작은 정보 조각을 수집합니다.

악성코드 유형	설명
하이잭커	시스템 설정을 수정하거나 사용자가 원치 않는 시스템 변경을 수행하는 수법으로 완전한 사전 고지에 의한 사용자 동의 없이 어떤 웹 사이트로 연결하거나 프로그램을 실행하기도 합니다.
기타 악성코드	이 카테고리는 정의된 다른 카테고리 중 하나에 정확하게 맞지 않는 기타 모든 악성코드와 의심스러운 동작을 포착하는 데 사용됩니다.
보안 침해 휴리스틱	이 범주는 다른 악성코드 차단 엔진과 관계없이 Adaptive Scanning에서 찾아낸 악성코드입니다.
피싱 URL	피싱 URL은 브라우저 주소 창에 표시됩니다. 도메인 이름을 사용하고 합법적 도메인을 모방하는 경우도 있습니다. 온라인 신원 도용 형태 중 하나로서 사회공학 및 기술적 속임수를 모두 구사하면서 개인 신원 데이터 및 금융 계정 자격 증명을 훔칩니다.
PUA	Potentially Unwanted Application. PUA는 악성이 아니지만 원치 않는 것으로 간주할 수 있는 애플리케이션입니다.
시스템 모니터	다음 작업 중 하나를 수행하는 모든 소프트웨어를 포괄합니다. 명시적으로 또는 은밀하게 시스템 프로세스 또는 사용자 작업을 기록합니다. 나중에 이러한 레코드를 검색 및 검토할 수 있도록 합니다.
트로이 목마 다운로더	설치되면 원격 호스트/사이트에 접속하고 원격 호스트로부터 패키지 또는 연관 프로그램을 설치하는 트로이 목마입니다. 이러한 설치는 대개 사용자 모르게 이루어집니다. 또한 트로이 목마 다운로더의 페이로드는 설치마다 달라질 수 있습니다. 원격 호스트/사이트로부터 다운로드 명령을 받기 때문입니다.
트로이 목마	트로이 목마는 무해한 애플리케이션으로 위장한 파괴적인 프로그램입니다. 바이러스와 달리 트로이 목마는 자체적으로 복제하지 않습니다.
트로이 피셔	감염된 컴퓨터에 상주하면서 특정 웹 페이지에 방문할 때까지 기다리거나 감염된 시스템을 검사하여 은행 사이트, 옥션 사이트, 온라인 결제 사이트용 사용자 이름 및 암호를 찾아낼 수 있습니다.
바이러스	사용자 모르게 컴퓨터에 로드되어 사용자의 의사와 상관없이 실행되는 프로그램 또는 코드입니다.
웜	컴퓨터 네트워크를 통해 자가 복제하는 프로그램 또는 알고리즘이며 대개 악성 활동을 수행합니다.

Advanced Malware Protection(파일 평판 및 파일 분석) 보고서

파일 분석 보고서 요구 사항 정보

(클라우드 파일 분석) 관리 어플라이언스에서 파일 분석 서버와 연결할 수 있음을 확인

파일 분석 보고서 세부사항을 얻으려면 어플라이언스가 포트 443을 통해 파일 분석 서버에 연결할 수 있습니다. 방화벽 정보, 563 페이지에서 세부 정보를 참조하십시오.

Cisco Content Security Management Appliance가 인터넷에 직접 연결되지 않은 경우 이 트래픽용 프록시 서버를 구성합니다(업그레이드 및 업데이트 설정, 453 페이지 참조). 프록시를 사용하여 업그레이드와 서비스 업데이트를 가져오도록 어플라이언스를 이미 구성한 경우 기존 설정이 사용됩니다.

HTTPS 프록시를 사용할 경우 프록시가 트래픽을 해독해서는 안 됩니다. 파일 분석 서버와의 통신에는 pass-through 메커니즘을 사용합니다. 프록시 서버가 파일 분석 서버의 인증서를 신뢰해야 하지만 파일 분석 서버에 자신의 인증서를 제공할 필요는 없습니다.

(클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성

조직의 모든 콘텐츠 보안 어플라이언스가 Cisco Email Security Appliance 또는 Cisco Web Security Appliance에서 분석을 위해 전송한 파일에 대해 클라우드에서 파일 분석 결과 세부 정보를 볼 수 있게 하려면 모든 어플라이언스를 동일한 어플라이언스 그룹으로 묶어야 합니다.

단계 **1** [새 웹 인터페이스에만 해당] 레거시 웹 인터페이스를 로드하려면 Security Management Appliance에서 ⚙ 을 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 파일 분석 섹션으로 스크롤합니다.

단계 **4** 관리 대상 어플라이언스가 다른 파일 분석 클라우드 서버에 지정된 경우 결과 세부사항을 표시할 서버를 선택합니다.

다른 클라우드 서버에서 처리하는 파일에 대해서는 결과 세부사항이 제공되지 않습니다.

단계 **5** 분석 그룹 ID를 입력합니다.

- 그룹 ID를 잘못 입력하거나 어떠한 이유로 인해 이를 변경해야 할 경우 Cisco TAC에서 케이스를 열어야 합니다.
- 이 변경사항은 즉시 적용되므로 커밋이 필요하지 않습니다.
- 이 값에 CCOID를 사용하는 것이 좋습니다.
- 이 값은 대/소문자를 구분합니다.
- 이 값은 분석을 위해 업로드된 파일에 대한 데이터를 공유하는 모든 어플라이언스에서 동일해야 합니다.
- 어플라이언스는 단 하나의 그룹에만 속할 수 있습니다.
- 언제든지 그룹에 머신을 추가할 수 있지만 한 번만 추가할 수 있습니다.

단계 **6** **Group Now**(지금 그룹화)를 클릭합니다.

단계 **7** 이 어플라이언스와 데이터를 공유할 각 Web Security Appliance에서 동일한 그룹을 구성합니다.

다음에 수행할 작업

관련 주제

클라우드에서 세부 파일 분석 결과를 볼 수 있는 파일은? , 202 페이지

(온프레미스 파일 분석) 파일 분석 계정 활성화

온프레미스 Cisco AMP Threat Grid 어플라이언스를 구축한 경우 Cisco Content Security Management Appliance에 대해 파일 분석 계정을 활성화해야 AMP Threat Grid 어플라이언스에서 제공하는 보고서 세부 정보를 볼 수 있습니다. 일반적으로 한 번만 하면 됩니다.

시작하기 전에

중대 레벨의 시스템 알림을 받아야 합니다.

단계 **1** 처음으로 Threat Grid 어플라이언스에서 파일 분석 보고서 세부사항에 액세스할 때 몇 분 기다리면 링크가 포함된 알림을 수신하게 됩니다.

이 링크를 받지 못한 경우 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 로드하고 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Alerts**(알림)를 선택하여 **View Top Alerts**(상위 알림 보기)를 클릭합니다.

단계 **2** 알림 메시지에서 링크를 클릭합니다.

단계 **3** 필요하다면 Cisco AMP Threat Grid Appliance에 로그인합니다.

단계 **4** 관리 어플라이언스 계정을 활성화합니다.

추가 요구 사항

추가 요건은 다음에서 Security Management Appliance 릴리스용 릴리스 정보를 참조하십시오.
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

SHA-256 해시로 파일 식별

파일 이름을 쉽게 변경할 수 있으므로 어플라이언스가 보안 해시 알고리즘(SHA-256)을 사용하여 각 파일에 대해 식별자를 생성합니다. 어플라이언스가 이름이 다른 동일한 파일을 처리할 경우 모든 인스턴스가 동일한 SHA-256으로 인식됩니다. 여러 어플라이언스가 동일한 파일을 처리하는 경우 해당 파일의 모든 인스턴스에 동일한 SHA-256 식별자가 있습니다.

대부분의 보고서에서는 파일이 SHA-256 값(단축 형식)으로 나열됩니다. 조직에서 악성코드 인스턴스와 관련된 파일 이름을 식별하려면 Advanced Malware Protection 보고서 페이지를 선택하고 표에서 SHA-256 링크를 클릭합니다. 세부사항 페이지에 관련 파일 이름이 표시됩니다.

Advanced Malware Protection(파일 평판 및 파일 분석) 보고서 페이지

보고서	설명
AMP(Advanced Malware Protection)	파일 평판 서비스에서 찾은 파일 기반 위협을 보여줍니다. 각 SHA에 액세스를 시도한 사용자와 해당 SHA-256과 관련된 파일 이름을 보려면 표에서 SHA-256을 클릭합니다. 악성코드 위협 파일 세부사항 보고서 페이지의 하단에 있는 링크를 클릭하면 보고서에 대해 선택한 시간 범위와 관계없이 최대 가용 시간 범위 내에서 발생한 웹 추적의 파일의 모든 인스턴스가 표시됩니다. 판정이 변경된 파일은 AMP 판정 업데이트 보고서를 참조하십시오. 그러한 판정은 Advanced Malware Protection 보고서에 적용되지 않습니다. 압축 또는 아카이브 파일에서 추출된 파일 중 하나가 악성인 경우 압축 또는 아카이브 파일의 SHA 값만 Advanced Malware Protection 보고서에 포함됩니다. **Malware Files by Category(**카테고리별 악성코드 파일**)** 섹션에는 카테고리가 **Custom Detection(**맞춤형 탐지**)**으로 지정된 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율이 표시됩니다. AMP for Endpoints Console에서 가져온 블랙리스트에 있는 파일의 위협 이름이 보고서의 Malware Threat Files(악성코드 위협 파일) 섹션에서 **Simple Custom Detection(**단순 맞춤형 탐색**)**으로 표시됩니다. AMP for Endpoints Console에서 블랙리스트에 있는 파일 SHA의 파일 경로 세부 정보를 보려면 다음 단계를 수행합니다. 1. **Reporting(**보고**)** > **Advanced Malware Protection**을 선택합니다. 2. 경로 분석 세부 정보를 보려는 파일 SHA 링크를 클릭합니다. 3. 추가 세부 정보 섹션에서 AMP 콘솔 링크를 클릭합니다.

보고서	설명
파일 분석	분석을 위해 전송된 각 파일의 시간 및 판정(또는 임시 판정)을 표시합니다. 어플라이언스는 30분마다 분석 결과를 확인합니다. 1,000개가 넘는 파일 분석 결과를 보려면 데이터를 .csv 파일로 내보냅니다. 온프레미스 Cisco AMP Threat Grid 어플라이언스 구축: 화이트리스트에 나열된 파일은 "정상"으로 표시됩니다. 허용 목록에 대한 내용은 AMP Threat Grid 온라인 도움말을 참조하십시오. 각 파일의 위협 특성 및 점수를 포함한 자세한 분석 결과를 보려면 드릴다운합니다. SHA를 검색하거나 파일 분석 세부사항 페이지의 하단에서 Cisco AMP Threat Grid 링크를 클릭하여 분석을 수행한 서버에서 직접 SHA에 대한 추가 세부사항을 볼 수도 있습니다. 파일을 분석한 서버의 세부사항을 보려면 파일 분석 보고서 요구 사항 정보 , 199 페이지를 참조하십시오. 압축 또는 아카이브 파일에서 추출된 파일이 분석을 위해 전송된 경우 이러한 추출된 파일의 SHA 값만 파일 분석 보고서에 포함됩니다.
AMP 판정 업데이트	트랜잭션이 처리된 이후에 판정이 변경되어 이 어플라이언스에서 처리한 파일을 표시합니다. 자세한 내용은 Web Security Appliance용 문서를 참조하십시오. 1,000개가 넘는 판정 업데이트를 보려면 데이터를 .csv 파일로 내보냅니다. 단일 SHA-256에 대해 여러 판정이 변경된 경우 이 보고서에 판정 기록이 아닌 최신 판정만 표시됩니다. 동일한 파일에 대한 여러 WSA의 판정 업데이트가 서로 다를 경우 최신 타임스탬프가 포함된 결과가 표시됩니다. SHA-256 링크를 클릭하면 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 이 SHA-256이 포함된 모든 트랜잭션의 웹 추적 결과가 표시됩니다. 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 특정 SHA-256의 영향을 받는 모든 트랜잭션을 보려면 악성코드 위협 파일 페이지의 하단에 있는 링크를 클릭합니다.

다른 보고서의 파일 평판 필터링 데이터 보기

파일 평판 및 분석 데이터는 관련이 있는 경우 다른 보고서에서도 볼 수 있습니다. "Advanced Malware Protection에 의해 차단됨" 열이 해당 보고서에서 기본적으로 숨겨질 수 있습니다. 추가 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

클라우드에서 세부 파일 분석 결과를 볼 수 있는 파일은?

퍼블릭 클라우드 파일 분석을 구축한 경우 파일 분석을 위해 어플라이언스 그룹에 추가된 모든 관리 대상 어플라이언스에서 업로드된 모든 파일의 세부 결과를 볼 수 있습니다.

관리 어플라이언스를 그룹에 추가했다면 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)** 페이지에서 버튼을 클릭하여 그룹에 속한 관리 대상 어플라이언스의 목록을 볼 수 있습니다.

분석 그룹의 어플라이언스는 파일 분석 클라이언트 ID로 식별됩니다. 특정 어플라이언스의 파일 분석 클라이언트 ID를 보려면 다음 위치에서 찾으십시오.

어플라이언스	파일 분석 클라이언트 **ID**의 위치
Email Security Appliance	**Security Services(**보안 서비스**) > File Reputation and Analysis(**파일 평판 및 분석**)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Web Security Appliance	**Security Services(**보안 서비스**) > Anti-Malware and Reputation(**악성코드 차단 및 평판**)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Cisco Content Security Management Appliance	**Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)** 페이지의 하단

관련 주제

(클라우드 파일 분석) 파일 분석 세부 결과를 표시하도록 관리 어플라이언스 구성 , 199 페이지

클라이언트 악성코드 위험 보고서

Web(웹**) > Reporting(**보고**) > Client Malware Risk(**클라이언트 악성코드 위험**)** 페이지는 보안 관련 보고 페이지로서 클라이언트 악성코드 위험 활동을 모니터링하는 데 사용할 수 있습니다.

시스템 관리자는 Client Malware Risk(클라이언트 악성코드 위험) 페이지에서 사용자 중 누가 가장 많은 차단 또는 경고를 겪고 있는지 확인할 수 있습니다. 관리자는 이 페이지에서 수집한 정보를 토대로 사용자 링크를 클릭하여 이 사용자가 웹에서 무슨 활동을 하여 그토록 많은 차단 또는 경고를 받았는지 또한 네트워크의 다른 사용자보다 더 많은 탐지를 유발했는지 파악할 수 있습니다.

또한 클라이언트 악성코드 위험 페이지에서는 L4TM(L4 Traffic Monitor)에서 찾아낸 자주 발생하는 악성코드 연결과 관련된 클라이언트 IP 주소를 나열합니다. 악성코드 사이트에 자주 연결되는 컴퓨터는 중앙 C&C(command and control) 서버와의 연결을 시도하는 악성코드에 감염되었을 가능성이 있으며 따라서 치료해야 합니다.

다음 표에서는 Client Malware Risk(클라이언트 악성코드 위험) 페이지의 정보를 설명합니다.

표 ***53:*** 클라이언트 악성코드 위험 보고서 페이지 구성 요소

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 포함되는 데이터의 시간 범위를 선택할 수 있는 메뉴. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참고하십시오.

섹션	설명
웹 프록시: 모니터링 또는 차단된 상위 클라이언트	악성코드 위험을 겪은 상위 10대 사용자를 표시합니다.
L4 Traffic Monitor: 탐지된 악성코드 연결	사내에서 가장 자주 악성코드 사이트에 연결되는 10대 컴퓨터의 IP 주소를 표시합니다. L4 Traffic Monitor 보고서 , 206 페이지의 "상위 클라이언트 IP" 차트와 동일합니다. 자세한 내용 및 차트 옵션은 이 섹션에서 확인하십시오.
웹 프록시: 클라이언트 악성코드 위험	이 테이블에서는 웹 프록시: 악성코드 위험별 상위 클라이언트 섹션에 표시된 특정 클라이언트에 대한 세부 정보를 표시합니다. 이 테이블에서 각 사용자를 클릭하여 그 클라이언트의 사용자 세부사항 페이지를 표시할 수 있습니다. 그 페이지에 대해서는 사용자 세부사항(웹 보고) , 189 페이지를 참조하십시오. 테이블의 어떤 링크를 클릭하면 개별 사용자 및 악성코드 위험을 유발하는 그 사용자의 활동을 더 자세히 알아볼 수 있습니다. 예를 들어 "사용자 ID/클라이언트 ID 주소" 열의 링크를 클릭하면 그 사용자의 페이지로 이동합니다.
L4 Traffic Monitor: 악성코드 위험별 클라이언트	이 테이블에서는 사내에서 악성코드 사이트에 자주 연결하는 컴퓨터의 IP 주소를 표시합니다. L4 Traffic Monitor 보고서 , 206 페이지의 "클라이언트 IP" 테이블과 동일합니다. 이 테이블의 사용에 대해서는 그 섹션을 참조하십시오.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

웹 평판 필터 보고서

Web(웹) > Reporting(보고) > Web Reputation Filters(웹 평판 필터)에서는 지정된 시간 범위의 트랜잭션에 대해 설정한 웹 평판 필터의 결과를 볼 수 있습니다.

웹 평판 필터란?

웹 서버 동작을 분석하고 URL에 평판 점수를 부여하여 URL 기반 악성코드를 포함하고 있을 가능성을 나타냅니다. 따라서 최종 사용자 개인 정보 및 민감한 기업 정보를 위협하는 URL 기반 악성코드 차단에 도움이 됩니다. Web Security Appliance는 URL 평판 점수를 사용하여 의심스러운 활동을 식별하고 악성코드 공격을 사전에 방지합니다. 웹 평판 필터는 액세스 정책 및 해독 정책 모두와 함께 사용할 수 있습니다.

웹 평판 필터에서는 통계 데이터를 사용하여 인터넷 도메인의 신뢰도를 평가하고 URL 평판 점수를 산정합니다. 특정 도메인이 등록된 기간, 웹 사이트가 호스팅되는 위치, 웹 서버에서 동적 IP 주소를 사용하는지 여부 등의 데이터를 참조하여 URL의 신뢰도를 평가합니다.

웹 평판 계산 시 URL을 네트워크 매개변수와 연계하여 악성코드가 있을 가능성을 판단합니다. 그런 다음, 악성코드가 존재할 확률 합계가 -10에서 +10 사이의 웹 평판 점수에 매핑됩니다. +10이 악성코드를 포함할 가능성이 가장 낮은 경우입니다.

예를 들어, 매개변수는 다음과 같습니다.

- URL 분류 데이터
- 다운로드 가능한 코드 있음
- 길고 애매한 EULA(End-User License Agreements)의 존재 여부
- 전역 볼륨 및 볼륨 변경
- 네트워크 소유자 정보
- URL 이력
- URL 유효 기간
- 차단 목록에 있는지 여부
- 허용 목록에 있는지 여부
- 인기 있는 도메인의 URL 오자
- 도메인 등록자 정보
- IP 주소 정보

웹 평판 필터링에 대한 자세한 내용은 IronPort AsyncOS for Web 사용 설명서의 "웹 평판 필터"를 참조하십시오.

Web Reputation Filters(웹 평판 필터**)** 페이지에서 다음 정보를 볼 수 있습니다.

표 ***54: Web Reporting Web Reputation Filters(***웹 보고 웹 평판 필터***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
웹 평판 작업(추세)	지정된 시간(가로축 타임라인)에서 총웹 평판 작업 수(세로축)를 그래프 형식으로 표시합니다. 여기서 웹 평판 작업의 장기 추세를 예상할 수 있습니다.
웹 평판 작업(볼륨)	웹 평판 작업의 볼륨을 트랜잭션별로 백분율 표시합니다.
웹 평판: WBRS에서 차단한 위협 유형	웹 평판 필터링에서 차단한 트랜잭션에서 발견된 위협 유형을 표시합니다. 참고: WBRS에서 위협 유형을 식별하지 못할 때도 있습니다.

섹션	설명
다른 트랜잭션에서 탐지된 위협 유형	웹 평판 필터링에서 차단하지 못한 트랜잭션에서 발견된 위협 유형을 표시합니다. 이 위협이 차단되지 않은 이유로는 • 모든 위협의 점수가 차단 임계값에 도달하는 것은 아닙니다. 그러나 어플라이언스의 다른 기능에서 이 위협을 잡아낼 수도 있습니다. • 위협의 통과를 허용하도록 정책이 구성될 수도 있습니다. 참고: WBRS에서 위협 유형을 식별하지 못할 때도 있습니다.
웹 신뢰도 작업(점수별 분석)	Adaptive Scanning이 활성화되지 않은 경우 이 인터랙티브 테이블은 각 작업에 대한 웹 평판 점수를 분류하여 표시합니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

웹 평판 설정 조정

보고서 결과에 따라 구성된 웹 평판 설정을 조정할 수도 있습니다. 이를테면 임계 점수를 조정하거나 Adaptive Scanning을 활성화/비활성화합니다. 웹 평판 설정 구성에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

L4 Traffic Monitor 보고서

Web(웹) > Reporting(보고) > L4 Traffic Monitor(L4 트래픽 모니터) 페이지에는 지정된 시간 범위 중에 Web Security Appliance에서 L4 트래픽 모니터가 탐지한 악성코드 포트 및 사이트에 대한 정보가 표시됩니다. 악성코드 사이트에 자주 연결하는 클라이언트의 IP 주소도 표시됩니다.

L4 트래픽 모니터는 각 Web Security Appliance의 모든 포트에서 오는 네트워크 트래픽을 수신 대기하고 자체 데이터베이스 테이블의 항목을 기준으로 도메인 이름과 IP 주소가 일치하는지 확인하여 수신 및 발신 트래픽의 허용 여부를 결정합니다.

이 보고서의 데이터를 사용하여 포트나 사이트의 차단 여부를 결정할 수 있습니다. 또는 특정 클라이언트 IP 주소가 악성코드 사이트에 비정상적으로 자주 연결되는 이유를 조사할 수 있습니다. 예를 들면, 해당 IP 주소와 연결된 컴퓨터가 중앙 제어 시스템에 연결하여 서버를 제어하려고 시도하는 악성코드에 감염되었기 때문일 수 있습니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

표 ***55: L4 Traffic Monitor*** 보고서 페이지 구성 요소

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고할 시간 범위를 선택할 수 있는 메뉴. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참고하십시오.
상위 클라이언트 IP	사내에서 악성코드 사이트에 가장 자주 연결하는 컴퓨터의 IP 주소를 그래프 형식으로 표시합니다. 차트 아래의 차트 옵션 링크를 클릭하면 탐지된 전체 악성코드 연결을 모니터링된 악성코드 연결 또는 차단된 악성코드 연결로 변경할 수 있습니다. 이 차트는 클라이언트 악성코드 위험 보고서 , 203 페이지의 "L4 Traffic Monitor: 탐지된 악성코드 연결" 차트와 동일합니다.
상위 악성코드 사이트	L4 Traffic Monitor에서 탐지한 상위 악성코드 도메인을 그래프 형식으로 표시합니다. 차트 아래의 차트 옵션 링크를 클릭하면 탐지된 전체 악성코드 연결을 모니터링된 악성코드 연결 또는 차단된 악성코드 연결로 변경할 수 있습니다.
클라이언트 소스 IP	이 테이블에서는 사내에서 악성코드 사이트에 자주 연결하는 컴퓨터의 IP 주소를 표시합니다. 특정 포트에 대한 데이터만 포함하려면 테이블 맨 아래의 상자에 포트 번호를 입력하고 Filter by Port(포트 기준 필터링)를 클릭합니다. 악성코드 사이트에 "콜홈"하는 악성코드에 의해 이용되는 포트를 결정하는 데 이 기능을 사용할 수 있습니다. 각 연결의 포트 및 목적지 도메인과 같은 세부사항을 보려면 테이블에서 항목을 클릭합니다. 예를 들어 어떤 클라이언트 IP 주소에서 차단된 악성코드 연결 건수가 많을 경우 열에서 그 숫자를 클릭하면 차단된 각 연결의 목록이 표시됩니다. 이 목록은 Web(웹) > Reporting(보고) > Web Tracking(웹 추적) 페이지의 L4 Traffic Monitor 탭에 검색 결과로 표시됩니다. 이 목록에 대한 자세한 내용은 L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지를 참조하십시오. 클라이언트 악성코드 위험 보고서 , 203 페이지의 "L4 Traffic Monitor - 악성코드 위험별 클라이언트" 테이블과 동일합니다.
악성코드 포트	L4 Traffic Monitor가 가장 자주 악성코드를 탐지한 포트를 표시합니다. 세부사항을 보려면 테이블의 항목을 클릭합니다. 예를 들어 탐지된 총악성코드 연결의 숫자를 클릭하면 해당 포트에서 각 연결의 세부사항이 표시됩니다. 이 목록은 Web(웹) > Reporting(보고) > Web Tracking(웹 추적) 페이지의 L4 Traffic Monitor 탭에 검색 결과로 표시됩니다. 이 목록에 대한 자세한 내용은 L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지를 참조하십시오.

섹션	설명
탐지된 악성코드 사이트	L4 Traffic Monitor가 가장 자주 악성코드를 탐지한 도메인을 표시합니다. 특정 포트에 대한 데이터만 포함하려면 테이블 맨 아래의 상자에 포트 번호를 입력하고 Filter by Port(포트 기준 필터링)를 클릭합니다. 어떤 사이트 또는 포트를 차단할지 여부를 결정할 때 이 기능을 사용할 수 있습니다. 세부사항을 보려면 테이블의 항목을 클릭합니다. 예를 들어 탐지된 악성코드 연결의 숫자를 클릭하면 해당 사이트에 대해 차단된 각 연결의 목록이 표시됩니다. 이 목록은 Web(웹) > Reporting(보고) > Web Tracking(웹 추적) 페이지의 L4 Traffic Monitor 탭에 검색 결과로 표시됩니다. 이 목록에 대한 자세한 내용은 L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지를 참조하십시오.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

관련 주제

- L4 Traffic Monitor 보고서 트러블슈팅 , 261 페이지

SOCKS 프록시 보고서

Web(웹) > Reporting(보고) > SOCKS Proxy(SOCKS 프록시) 페이지에서는 SOCKS 프록시를 통해 처리된 트랜잭션에 대한 데이터 및 추세를 볼 수 있습니다. 목적지 및 사용자에 대한 정보도 포함됩니다.

참고 보고서에 표시된 목적지는 SOCKS 클라이언트(주로 브라우저)가 SOCKS 프록시에 보내는 주소입니다.

SOCKS 프록시 설정을 변경하려면 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

관련 주제

- SOCKS 프록시에서 처리되는 트랜잭션 검색 , 250 페이지

사용자 위치별 보고서

Web(웹) > Reporting(보고) > Reports by User Location(사용자 위치별 보고서) 페이지에서는 모바일 사용자가 로컬 또는 원격 시스템에서 어떤 활동을 하는지 확인할 수 있습니다.

예를 들면

- 로컬 및 원격 사용자가 액세스하고 있는 URL 범주.

- 로컬 및 원격 사용자가 액세스하고 있는 사이트에서 유발하는 악성코드 차단 활동.
- 로컬 및 원격 사용자가 액세스하는 사이트의 웹 평판
- 로컬 및 원격 사용자가 액세스하는 애플리케이션
- 사용자(로컬 및 원격)
- 로컬 및 원격 사용자가 액세스하는 도메인

Reports by User Location(사용자 위치별 보고서) 페이지에서 다음 정보를 볼 수 있습니다.

표 ***56: Web Reporting Reports by User Location***(웹 보고 사용자 위치별 보고서) 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	90일부터 맞춤 범위까지 가능한 드롭다운 목록. 시간 범위 및 맞춤 설정에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
총웹 프록시 작업 - 원격 사용자	지정된 시간(가로축 타임라인)에서 원격 사용자의 활동(세로축)을 그래프 형식으로 표시합니다.
웹 프록시 요약	시스템에서 로컬 및 원격 사용자의 활동을 요약하여 표시합니다.
총웹 프록시 작업 - 로컬 사용자	지정된 시간(가로축 타임라인)에서 원격 사용자의 활동(세로축)을 그래프 형식으로 표시합니다.
탐지된 의심스러운 트랜잭션: 원격 사용자	지정된 시간(가로축 타임라인)에 원격 사용자에 대해 정의된 액세스 정책 때문에 탐지된 의심스러운 트랜잭션의 활동(세로축)을 그래프 형식으로 표시합니다.
의심되는 트랜잭션 요약	시스템에서 원격 사용자의 의심스러운 활동을 요약하여 표시합니다.
탐지된 의심스러운 트랜잭션: 로컬 사용자	지정된 시간(가로축 타임라인)에 원격 사용자에 대해 정의된 액세스 정책 때문에 탐지된 의심스러운 트랜잭션의 활동(세로축)을 그래프 형식으로 표시합니다.
의심되는 트랜잭션 요약	시스템의 로컬 사용자에 대해 의심스러운 트랜잭션의 요약을 표시합니다.

Reports by User Location(사용자 위치별 보고서) 페이지에서 로컬 및 원격 사용자의 활동을 보여주는 보고서를 생성할 수 있습니다. 그러면 사용자의 로컬 및 원격 활동을 쉽게 비교할 수 있습니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

참고 사용자 위치별 보고서 페이지의 정보에 대한 예약 보고서를 생성할 수 있습니다. 보고서 예약에 대해서는 예약 및 온디맨드 웹 보고서 정보, 239 페이지를 참조하십시오.

System Capacity(시스템 용량) 페이지

Web(웹) > Reporting(보고) > System Capacity(시스템 용량) 페이지에서는 Web Security Appliance에 의해 Security Management Appliance에 부과된 전체적인 워크로드를 볼 수 있습니다. System Capacity(시스템 용량) 페이지에서는 시간에 따른 증가를 추적하고 시스템 용량을 계획할 수 있다는 점이 가장 중요합니다. WSA를 모니터링하면서 볼륨에 적합한 용량임을 확인합니다. 시간이 지나면 볼륨이 불가피하게 증가하므로, 적절한 모니터링을 통해 추가 용량 또는 구성 변경을 사전에 적용해야 합니다.

System Capacity(시스템 용량) 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- WSA가 권장 CPU 용량을 초과할 때를 파악합니다. 그러면 구성 최적화 또는 추가 어플라이언스가 필요한 시점을 결정할 수 있습니다.
- 트러블슈팅을 위해 시스템의 어떤 부분이 가장 많은 리소스를 사용하는지를 식별합니다.
- 응답 시간 및 프록시 버퍼 메모리를 식별합니다.
- 초당 트랜잭션 및 보류 중인 연결을 나타냅니다.

시스템 용량 보고서 보기

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > System Capacity(시스템 용량)**를 선택합니다.

단계 **2** 서로 다른 데이터 유형을 보려면 **Columns(열)**를 클릭하고 볼 데이터를 선택합니다.

단계 **3** 단일 어플라이언스의 시스템 용량을 보려면 Overview of Averaged Usage and Performance(평균 사용량 및 성능 개요) 테이블의 Web Security Appliance 열에서 어플라이언스를 클릭합니다.

해당 어플라이언스에 대한 System Capacity(시스템 용량) 그래프가 나타납니다. 페이지의 그래프는 2가지 집합으로 나뉩니다.

- 시스템 용량 - 시스템 로드 , 211 페이지
- 시스템 용량 - 네트워크 로드 , 211 페이지

시스템 용량 페이지의 데이터를 해석하는 방법

시스템 용량 보고서의 데이터를 조회할 시간 범위를 선택할 때 다음 사항에 유의하십시오.

- 일일 보고서 - 시간 테이블을 쿼리하고 24시간 동안 어플라이언스가 수신한 쿼리 수를 시간별로 정확하게 표시합니다. 이 정보는 시간 테이블에서 수신합니다.
- 월간 보고서 - 30일 또는 31일(해당 월의 일수에 따라)의 일일 테이블을 쿼리하여 30일 또는 31일의 쿼리 수를 정확하게 보고합니다. 이 역시 정확한 수치입니다.

시스템 용량 페이지의 '최대값' 표시는 지정된 기간에 나타난 최고치를 의미합니다. '평균값'은 지정된 기간의 모든 값의 평균치입니다. 집계 기간은 보고서에서 선택한 간격에 따라 다릅니다. 예를 들어 차트가 1개월분이라면 일별 평균값 및 최대값을 표시할 수 있습니다.

참고 다른 보고서에서 시간 범위로 **Year(**년**)**를 선택했다면 가장 큰 시간 범위, 즉 90일을 선택하는 것이 좋습니다.

시스템 용량 - 시스템 로드

시스템 용량 창에서 처음 4개 그래프는 시스템 로드 보고서입니다. 이 보고서에서는 어플라이언스의 전체 CPU 사용량을 보여줍니다. AsyncOS는 유휴 CPU 리소스를 사용하여 트랜잭션 처리량을 개선할 수 있도록 최적화되었습니다. 높은 CPU 사용량은 시스템 용량 문제를 나타내지 않을 수 있습니다. 높은 CPU 사용량이 지속적인 높은 볼륨의 메모리 페이지 스와핑과 결합되면 이는 용량 문제일 수 있습니다. 여러 기능의 CPU 사용량도 표시하는데, 여기에는 WSA 보고를 위한 처리도 포함되어 있습니다. 기능별 CPU 그래프는 제품의 어떤 영역에서 시스템의 리소스를 가장 많이 사용하는지 보여주는 훌륭한 지표입니다. 어플라이언스를 최적화해야 하는 경우 어떤 기능을 조정 또는 비활성화해야 할지를 결정하는 데 이 그래프가 도움이 될 수 있습니다.

또한 응답 시간/레이턴시 및 초당 트랜잭션 그래프는 전체 응답 시간(밀리초) 및 시간 범위 드롭다운 메뉴에서 지정한 날짜 범위의 초당 트랜잭션 수를 표시합니다.

시스템 용량 - 네트워크 로드

시스템 용량 창의 다음 그래프는 발신 연결, 대역폭 출력, 프록시 버퍼 메모리 통계를 표시합니다. 일, 주, 월, 연도의 결과를 볼 수 있습니다. 현재 환경에서 정상적인 볼륨 및 급증의 추세를 이해하는 것이 중요합니다.

Proxy Buffer Memory(프록시 버퍼 메모리)는 정상 작동 중에 네트워크 트래픽 급증을 나타낼 수 있지만, 그래프가 최대치를 향해 계속해서 올라가는 경우 어플라이언스가 최대 용량에 도달한 것일 수 있으므로 용량 추가를 고려해야 합니다.

이러한 차트는 시스템 용량 - 시스템 로드 , 211 페이지에서 설명한 차트와 같은 페이지, 해당 차트 아래에 있습니다.

프록시 버퍼 메모리 스와핑에 대한 참고 사항

시스템은 프록시 버퍼 메모리를 정기적으로 스와핑하도록 설계되었으므로, 어느 정도의 프록시 버퍼 메모리 스와핑은 발생할 수 있으며 이것이 어플라이언스의 문제를 나타내지는 않습니다. 시스템이 일관되게 대량의 프록시 버퍼 메모리를 교체하지 않는 한 프록시 버퍼 메모리 스와핑은 정상이며 예상된 동작입니다. 시스템이 매우 많은 볼륨으로 운영되며 이러한 많은 볼륨 때문에 일관되게 프록시 버퍼 메모리를 교체하는 경우, 성능을 높이려면 네트워크에 Web Security Appliance를 추가하거나 최대 처리량이 보장되도록 구성을 조정해야 할 수 있습니다.

데이터 가용성 페이지

Web(웹**) > Reporting(**보고**) > Data Availability(**데이터 가용성**)** 페이지는 각각의 관리되는 Web Security Appliance에 대해 Security Management Appliance에서 사용 가능한 보고 및 웹 추적 데이터에 대한 데이터 범위의 개요를 제공합니다.

참고 Web Reporting(웹 보고)이 비활성화된 경우 Security Management Appliance는 Web Security Appliance에서 새 데이터를 가져오지 않지만, 전에 검색된 데이터는 여전히 Security Management Appliance에 있습니다.

웹 보고 'From' 및 'To' 열의 상태와 웹 보고 및 추적 'From' 및 'To' 열의 상태가 서로 다를 경우 가장 심각한 결과가 Status 열에 나타납니다.

데이터 지우기에 대해서는 디스크 공간 관리 , 487 페이지를 참조하십시오.

참고 데이터 가용성이 URL 범주에 대한 예약 보고서에 사용된 경우 어플라이언스 중 하나에서 데이터 공백이 있으면 페이지의 맨 아래에 "이 시간 범위의 일부 데이터를 사용할 수 없습니다"라는 메시지가 표시됩니다. 공백이 없으면 아무 것도 표시되지 않습니다.

새 웹 인터페이스의 **Web Reporting(**웹 보고**)** 페이지 이해

다음 표에는 웹 인터페이스의 **Reports(**보고서**)** 드롭다운 아래에서 지원되는 최신 Web Security Appliance용 AsyncOS 릴리스에 사용 가능한 보고서가 나와 있습니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오. Web Security Appliance에서 이전 AsyncOS 릴리스를 실행 중인 경우 이러한 보고서 중 일부를 사용할 수 없습니다.

표 ***57: Web Reports(***웹 보고서***)*** 드롭다운 옵션

Reports(보고서**)** 드롭다운 옵션	작업
일반 보고서	
Overview(개요) 페이지	Overview(개요) 페이지는 Web Security Appliance에 대한 활동 개요를 제공합니다. 이 페이지에는 수신 및 발신 트랜잭션에 대한 그래프와 요약 테이블이 포함되어 있습니다. 자세한 내용은 Overview(개요) 페이지, 215 페이지를 참조하십시오.
Application Visibility(애플리케이션 가시성) 페이지	Application Visibility(애플리케이션 가시성) 페이지에서는 Security Management Appliance 및 Web Security Appliance 내에서 특정 애플리케이션 유형에 적용된 컨트롤을 보고 적용할 수 있습니다. 자세한 내용은 Application Visibility(애플리케이션 가시성) 페이지, 216 페이지를 참조하십시오.
Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지	지정된 시간 범위에 L4 Traffic Monitor에서 탐지한 악성코드 포트 및 악성코드 사이트에 대한 정보를 볼 수 있습니다. 자세한 내용은 Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지, 219 페이지을 참조하십시오.

Reports(보고서) 드롭다운 옵션	작업
SOCKS Proxy(SOCKS 프록시) 페이지	목적지 및 사용자를 포함하여 SOCKS 프록시 트랜잭션에 대한 데이터를 볼 수 있습니다. 자세한 내용은 SOCKS Proxy(SOCKS 프록시) 페이지, 221 페이지을 참조하십시오.
URL 범주 페이지	URL 범주 페이지에서는 다음을 포함하여 방문 중인 상위 URL 범주를 볼 수 있습니다. • 트랜잭션별로 차단 또는 경고 작업을 유발한 상위 URL. • 완료된 트랜잭션, 경고된 트랜잭션, 차단된 트랜잭션을 대상으로 한 지정된 시간 범위의 모든 URL 카테고리. 인터랙티브 열 제목을 포함한 인터랙티브 테이블이며, 필요에 따라 데이터를 정렬할 수 있습니다. 자세한 내용은 URL 범주 페이지, 222 페이지을 참조하십시오.
Users(사용자) 페이지	Users(사용자) 페이지는 개별 사용자에 대한 웹 추적 정보를 볼 수 있는 여러 웹 추적 링크를 제공합니다. Users(사용자) 페이지에서는 시스템의 한 명 이상의 사용자가 인터넷, 특정 사이트 또는 URL에서 얼마나 시간을 보냈는지, 그리고 해당 사용자가 사용하는 대역폭이 얼마인지를 볼 수 있습니다. Users(사용자) 페이지의 인터랙티브 Users(사용자) 테이블에서 개별 사용자를 클릭하면 User Details(사용자 세부사항) 페이지에서 해당 특정 사용자에 대한 자세한 정보를 볼 수 있습니다. User Details(사용자 세부 정보) 페이지에서는 Users(사용자) 페이지의 Users(사용자) 테이블에서 확인한 사용자에 대한 정보를 확인할 수 있습니다. 이 페이지에서는 개별 사용자가 시스템에서 수행한 활동을 조사할 수 있습니다. 사용자 레벨 조사를 진행 중인데 사용자가 어떤 사이트를 방문하는지, 어떤 악성코드 위협을 겪는지, 어떤 URL 범주에 액세스하는지, 이 사이트에서 얼마나 많은 시간을 보내는지 등을 알아야 할 경우 이 페이지가 특히 유용합니다. 자세한 내용은 Users(사용자) 페이지, 225 페이지을 참조하십시오. 시스템의 특정 사용자에 대해서는 User Details(사용자 세부 정보) 페이지(웹 보고) , 227 페이지 섹션을 참조하십시오.
웹 사이트 페이지	웹 사이트 페이지에서는 관리 대상 어플라이언스에서 일어나는 활동을 종합적으로 살펴볼 수 있습니다. 이 페이지에서는 특정 시간 범위에 액세스한 고위험 웹 사이트를 모니터링할 수 있습니다. 자세한 내용은 웹 사이트 페이지, 229 페이지을 참조하십시오.

Reports(보고서) 드롭다운 옵션	작업
HTTPS 보고서	HTTPS Reports(HTTPS 보고서) 보고서 페이지는 매니지드 어플라이언스의 HTTP/HTTPS 트래픽 요약에 대한 전체 집계입니다. 자세한 내용은 HTTPS 보고서 페이지, 230 페이지을(를) 참고하십시오.
위협 보고서	
Anti-Malware(악성코드 차단) 페이지	악성코드 차단 페이지에서는 악성코드 차단 검사 엔진이 지정된 시간 범위에 탐지한 악성코드 포트 및 악성코드 사이트에 대한 정보를 볼 수 있습니다. 보고서의 상단에는 상위 악성코드 포트 및 웹 사이트 각각의 연결 수가 표시됩니다. 하단에는 탐지된 악성코드 포트 및 사이트가 표시됩니다. 자세한 내용은 Anti-Malware(악성코드 차단) 페이지 , 232 페이지을 참조하십시오.
Client Malware Risk(클라이언트 악성코드 위험) 페이지	클라이언트 악성코드 리스크 페이지는 보안 관련 보고 페이지이며, 비정상적으로 악성코드 사이트에 자주 연결하는 개별 클라이언트 컴퓨터를 파악하는 데 사용할 수 있습니다. 자세한 내용은 클라이언트 악성코드 위험 보고서 , 235 페이지을 참조하십시오.
Web Reputation Filters(웹 평판 필터) 페이지	지정된 시간 범위의 트랜잭션에 대한 웹 평판 필터링 보고를 볼 수 있습니다. 자세한 내용은 Web Reputation Filters(웹 평판 필터) 페이지 , 237 페이지를 참조하십시오.

소요 시간 정보

여러 테이블의 Time Spent(소요 시간) 열은 사용자가 웹 페이지에 보낸 시간을 나타냅니다. 사용자 조사에서는 사용자가 각 URL 범주에서 보낸 시간입니다. URL 추적에서는 각 사용자가 해당 URL에서 보낸 시간입니다.

트랜잭션 이벤트가 'viewed' 태그를 갖게 되면, 즉 사용자가 특정 URL을 방문하면 'Time Spent' 값이 계산되기 시작하고 웹 보고 테이블의 필드로 추가됩니다.

AsyncOS는 소요 시간을 계산하기 위해 각 활성 사용자에게 1분간의 활동에 대해 60초를 부여합니다. 1분이 끝나면 각 사용자의 소요 시간은 그 사용자가 방문한 여러 도메인에 고르게 분배됩니다. 예를 들어 사용자가 활성 상태의 1분간 서로 다른 도메인 4개를 방문할 경우 각 도메인에서 15초를 보낸 것으로 간주합니다.

소요 시간의 값에서는 다음 사항을 고려합니다.

- 활성 사용자란 애플리케이션을 통해 HTTP 트래픽을 보내고 AsyncOS에서 "페이지 뷰"로 간주하는 웹 사이트를 방문한 사용자 이름 또는 IP 주소로 정의됩니다.

- AsyncOS는 페이지 뷰를 사용자가 시작하는 HTTP 요청으로 정의합니다. 클라이언트 애플리케이션에서 시작한 요청이 아닙니다. AsyncOS에서는 휴리스틱 알고리즘을 사용하여 최선 노력 추측으로 사용자 페이지 뷰를 파악합니다.

단위는 시간:분 형식으로 표시됩니다.

Overview(개요) 페이지

Overview(개요**)** 보고서 페이지는 Web Security Appliance에 대한 활동 개요를 제공합니다. 이 페이지에는 수신 및 발신 트랜잭션에 대한 그래프와 요약 테이블이 포함되어 있습니다.

Overview(개요) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 **Monitoring(**모니터링**) > Overview(**개요**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

상위 레벨에서 **Overview(**개요**)** 보고서 페이지는 URL 및 사용자 사용량, 웹 프록시 활동, 각종 트랜잭션 요약에 대한 통계를 제공합니다. 트랜잭션 요약에서는 이를테면 의심스러운 트랜잭션의 추세를 더 면밀하게 파악할 수 있습니다. 또한 그래프를 통해 이 의심스러운 트랜잭션 중 몇 개가 차단되었고 어떤 식으로 차단되고 있는지 알 수 있습니다.

Overview(개요) 보고서 페이지의 하단에서는 사용량을 다룹니다. 즉 조회 중인 상위 URL 범주, 차단 중인 상위 애플리케이션 유형 및 범주, 이 차단 또는 경고를 발생시키는 상위 사용자 등입니다.

표 ***58: Overview(***개요***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
(드롭다운 목록)의 데이터 보기	Overview(개요) 데이터를 볼 Web Security Appliance를 선택하거나 All Web Appliances(모든 웹 어플라이언스)를 선택합니다. 어플라이언스 또는 보고 그룹에 대한 보고 데이터 보기, 36 페이지 섹션도 참조해 주십시오.
총 웹 프록시 작업	현재 Security Management Appliance에 의해 관리되고 있는 Web Security Appliance가 보고하는 웹 프록시 활동을 볼 수 있습니다. 이 섹션에는 활동이 발생한 대략적인 날짜와 실제 트랜잭션 수가 그래픽 형식으로 표시됩니다. 의심스러운 웹 프록시 활동 또는 정상 프록시 활동의 비율을 볼 수 있습니다. 총 트랜잭션 수도 포함됩니다.

섹션	설명
의심되는 트랜잭션	관리자가 의심스러운 것으로 지정한 웹 트랜잭션을 그래픽 형식으로 볼 수 있습니다. 이 섹션에는 활동이 발생한 대략적인 날짜와 실제 트랜잭션 수가 그래픽 형식으로 표시됩니다. 의심되어 차단되거나 경고가 표시된 트랜잭션의 백분율도 볼 수 있습니다. 탐지 및 차단된 트랜잭션의 유형 그리고 트랜잭션이 차단된 실제 횟수도 확인할 수 있습니다.
L4 Traffic Monitor 요약	현재 Security Management Appliance에 의해 관리되는 Web Security Appliance가 보고하는 L4 트래픽을 그래픽 형식으로 볼 수 있습니다.
상위 URL 카테고리: 총 트랜잭션 수	차단된 상위 URL 카테고리를 표시합니다. URL 카테고리 유형 및 이 카테고리 유형이 실제로 차단된 횟수도 그래픽 형식으로 볼 수 있습니다. 사전 정의 URL 범주의 집합은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.
상위 애플리케이션 유형: 총 트랜잭션 수	차단된 상위 애플리케이션 카테고리를 표시합니다. 실제 애플리케이션 유형 및 이 애플리케이션 유형이 실제로 차단된 횟수도 그래픽 형식으로 볼 수 있습니다.
상위 악성코드 카테고리: 모니터링됨 또는 차단됨	탐지된 모든 악성코드 카테고리를 그래픽 형식으로 볼 수 있습니다.
상위 사용자: 차단 또는 경고를 받은 트랜잭션	차단 또는 경고를 받은 트랜잭션을 생성하는 실제 사용자를 그래픽 형식으로 볼 수 있습니다. IP 주소 또는 사용자 이름으로 표시할 수 있습니다. 사용자 이름을 식별 불가능하게 하려면 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지를 참조하십시오.

Application Visibility(애플리케이션 가시성) 페이지

참고 애플리케이션 가시성에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 '애플리케이션 가시성 및 컨트롤 이해' 장을 참조하십시오.

Application Visibility(애플리케이션 가시성) 보고서 페이지에서는 Security Management Appliance 및 Web Security Appliance 내 특정 애플리케이션 유형에 컨트롤을 적용할 수 있습니다.

Application Visibility(애플리케이션 가시성) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web**(웹)을 선택하고 **Monitoring**(모니터링) > **Application Visibility**(애플리케이션 가시성)를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

애플리케이션 제어는 웹 트래픽에 대해 예컨대 URL 필터링보다 세부적인 제어가 가능할 뿐 아니라 다음 애플리케이션 유형에 대한 더 강력한 제어를 지원합니다.

- 회피성 애플리케이션 - 익명 서비스, 암호화 터널 등
- 협업 애플리케이션 - Cisco WebEx, Facebook, 인스턴트 메시징 등
- 리소스 집약적인 애플리케이션 - 스트리밍 미디어

애플리케이션과 애플리케이션 유형의 차이점 이해

보고서를 위해 관련 애플리케이션을 제어할 수 있도록 애플리케이션과 애플리케이션 유형의 차이점을 이해하는 것이 중요합니다.

- 애플리케이션 유형. 하나 이상의 애플리케이션을 포함하는 범주. 예를 들어 검색 엔진은 Google Search, Craigslist와 같은 검색 엔진을 포함할 수 있는 애플리케이션 유형입니다. 인스턴트 메시징 역시 Yahoo Instant Messenger, Cisco WebEx 등을 포함할 수 있는 애플리케이션 유형 범주입니다. Facebook도 애플리케이션 유형입니다.
- 애플리케이션. 애플리케이션 유형에 속하는 특정 애플리케이션. YouTube는 미디어 애플리케이션 유형에 속하는 애플리케이션입니다.
- 애플리케이션 동작. 사용자가 어떤 애플리케이션 내에서 수행할 수 있는 특정 작업 또는 동작. 예를 들어 사용자가 Yahoo Messenger와 같은 애플리케이션을 사용하면서 파일을 전송할 수 있습니다. 모든 애플리케이션의 애플리케이션 동작이 구성 가능한 것은 아닙니다.

참고 AVC(Application Visibility and Control) 엔진을 사용하여 Facebook 활동을 제어하는 방법에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 '애플리케이션 가시성 및 컨트롤 이해' 장을 참조하십시오.

Application Visibility(애플리케이션 가시성) 페이지에서 다음 정보를 볼 수 있습니다.

표 ***59: Application Visibility***(애플리케이션 가시성)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.

섹션	설명
전체 트랜잭션별 상위 애플리케이션 유형	웹 사이트에서 방문하는 상위 애플리케이션 유형을 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오. 예를 들어 Yahoo Instant Messenger와 같은 인스턴트 메시징 툴, Facebook, 프레젠테이션 애플리케이션 유형이 있습니다.
차단된 트랜잭션별 상위 애플리케이션	트랜잭션별로 차단 조치가 발생하도록 트리거한 상위 애플리케이션 유형을 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오. 예를 들어 어떤 사용자가 특정 애플리케이션 유형, 이를테면 Google Talk 또는 Yahoo Instant Messenger를 시작하려 했습니다. 설정된 어떤 정책 때문에 차단 조치가 실행되었습니다. 그러면 이 애플리케이션은 그래프에서 차단된 또는 경고된 트랜잭션으로 표시됩니다.
매치하는 애플리케이션 유형	이 인터랙티브 테이블에서는 전체 트랜잭션의 상위 애플리케이션 유형 테이블에 나열된 애플리케이션 유형에 대한 자세한 정보를 볼 수 있습니다. Applications(애플리케이션) 열에서 세부 정보를 표시할 애플리케이션을 클릭할 수 있습니다.
매치하는 애플리케이션	Applications Matched(매치하는 애플리케이션) 인터랙티브 테이블은 지정된 시간 범위의 모든 애플리케이션을 표시합니다. 또한 매치하는 애플리케이션 섹션 내에서 특정 애플리케이션을 찾을 수 있습니다. 맨 아래의 텍스트 필드에 애플리케이션 이름을 입력하고 Find Application(애플리케이션 찾기)을 클릭합니다.

참고 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지

Layer 4 Traffic Monitor(레이어 **4** 트래픽 모니터**)** 보고서 페이지에는 지정된 시간 범위 중에 Web Security Appliance에서 Layer 4 Traffic Monitors(레이어 4 트래픽 모니터)가 탐지한 악성코드 포트 및 사이트에 대한 정보가 표시됩니다. 또한 악성코드 사이트를 자주 발견하는 클라이언트의 IP 주소를 표시합니다.

Web Sites(웹 사이트) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Web Sites(**웹 사이트**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

레이어 4 트래픽 모니터는 각 Web Security Appliance의 모든 포트에서 오는 네트워크 트래픽을 수신 대기하고 자체 데이터베이스 테이블의 항목을 기준으로 도메인 이름과 IP 주소가 일치하는지 확인하여 수신 및 발신 트래픽의 허용 여부를 결정합니다.

이 보고서의 데이터를 활용하여 어떤 포트 또는 사이트의 차단 여부를 결정하거나 특정 클라이언트 IP 주소가 비정상적으로 자주 악성코드 사이트에 연결되는 이유를 조사할 수 있습니다(예: 해당 IP 주소의 컴퓨터가 중앙 C&C 서버와의 연결을 시도하는 악성코드에 감염됨).

표 ***60: Layer 4 Traffic Monitor(***레이어 ***4*** 트래픽 모니터***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
상위 클라이언트 IP: 악성코드 연결 탐지됨	악성코드 사이트에 가장 자주 연결하는 사용자 조직에 있는 컴퓨터의 상위 IP 주소를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오. 이 차트는 클라이언트 악성코드 위험 보고서 , 235 페이지의 "Layer 4 Traffic Monitor: Malware Connections Detected(레이어 4 트래픽 모니터: 탐지된 악성코드 연결)" 차트와 동일합니다.
상위 악성코드 사이트: 악성코드 연결 탐지됨	레이어 4 트래픽 모니터에서 탐지된 상위 악성코드 도메인을 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.

섹션	설명
클라이언트 소스 IP	이 인터랙티브 테이블을 사용하면 사내에서 악성코드 사이트에 자주 연결하는 컴퓨터의 IP 주소를 볼 수 있습니다. 특정 포트에 대한 데이터만 포함하려면 테이블 맨 아래의 상자에 포트 번호를 입력하고 Filter by Client IP(클라이언트 IP 기준 필터링)를 클릭합니다. 악성코드 사이트에 "콜홈"하는 악성코드에 의해 이용되는 포트를 결정하는 데 이 기능을 사용할 수 있습니다. 각 연결의 포트 및 목적지 도메인과 같은 세부사항을 보려면 테이블에서 항목을 클릭합니다. 예를 들어 어떤 클라이언트 IP 주소에서 차단된 악성코드 연결 건수가 많을 경우 열에서 그 숫자를 클릭하면 차단된 각 연결의 목록이 표시됩니다. 이 목록은 Web Tracking Search(웹 추적 검색) 페이지의 Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 탭에 검색 결과로 표시됩니다. 이 목록에 대한 자세한 내용은 L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지를 참조하십시오. 이 차트는 클라이언트 악성코드 위험 보고서 , 235 페이지의 "Layer 4 Traffic Monitor: Malware Connections Detected(레이어 4 트래픽 모니터: 탐지된 악성코드 연결)" 차트와 동일합니다.
악성코드 포트	이 인터랙티브 테이블을 사용하면 레이어 4 트래픽 모니터에서 악성코드가 가장 자주 탐지된 포트를 볼 수 있습니다. 세부사항을 보려면 테이블의 항목을 클릭합니다. 예를 들어 탐지된 총악성코드 연결의 숫자를 클릭하면 해당 포트에서 각 연결의 세부사항이 표시됩니다. 이 목록은 Web Tracking Search(웹 추적 검색) 페이지의 Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 탭에 검색 결과로 표시됩니다. 이 목록에 대한 자세한 내용은 L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지를 참조하십시오.

섹션	설명
탐지된 악성코드 사이트	이 인터랙티브 테이블을 사용하면 레이어 4 트래픽 모니터에서 악성코드가 가장 자주 탐지된 도메인을 볼 수 있습니다. 특정 포트에 대한 데이터만 포함하려면 테이블 맨 아래의 상자에 포트 번호를 입력하고 Filter by Port(포트 기준 필터링)를 클릭합니다. 어떤 사이트 또는 포트를 차단할지 여부를 결정할 때 이 기능을 사용할 수 있습니다. 세부사항을 보려면 테이블의 항목을 클릭합니다. 예를 들어 탐지된 악성코드 연결의 숫자를 클릭하면 해당 사이트에 대해 차단된 각 연결의 목록이 표시됩니다. 이 목록은 Web Tracking Search(웹 추적 검색) 페이지의 Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 탭에 검색 결과로 표시됩니다. 이 목록에 대한 자세한 내용은 L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지를 참조하십시오.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

관련 주제

L4 Traffic Monitor 보고서 트러블슈팅 , 261 페이지

SOCKS Proxy(SOCKS 프록시) 페이지

SOCKS Proxy(SOCKS 프록시) 보고서 페이지에서는 SOCKS 프록시를 통해 처리된 트랜잭션을 그래픽 형식과 표 형식으로 볼 수 있습니다. 목적지 및 사용자에 대한 정보도 포함됩니다.

SOCKS Proxy(SOCKS 프록시) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(웹)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > SOCKS Proxy(SOCKS 프록시)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

참고 보고서에 표시된 목적지는 SOCKS 클라이언트(주로 브라우저)가 SOCKS 프록시에 보내는 주소입니다.

SOCKS 프록시 설정을 변경하려면 *AsyncOS for Cisco Web Security Appliances* 사용 설명서를 참조하십시오.

표 *61: SOCKS Proxy(SOCKS* 프록시*)* 페이지의 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
SOCKS에 대한 상위 대상: 총 트랜잭션 수	SOCKS 프록시에서 탐지한 상위 목적지를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
SOCKS에 대한 상위 사용자: 악성코드 트랜잭션	SOCKS 프록시에서 탐지한 상위 사용자를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
대상	이 인터랙티브 테이블을 사용하여 SOCKS 프록시를 통해 처리되는 대상 도메인 또는 IP 주소의 목록을 볼 수 있습니다. 특정 대상에 대한 데이터만 포함하려면 테이블의 맨 아래에 있는 상자에 도메인 이름 또는 IP 주소를 입력하고 **Find Domain or IP**(도메인 또는 **IP** 찾기)를 클릭합니다.
사용자	이 인터랙티브 테이블을 사용하여 SOCKS 프록시를 통해 처리되는 사용자 또는 IP 주소의 목록을 볼 수 있습니다. 특정 사용자에 대한 데이터만 포함하려면 테이블의 맨 아래에 있는 상자에 사용자 이름 또는 IP 주소를 입력하고 **Find User ID / Client IP Address**(사용자 **ID** / 클라이언트 **IP** 주소 찾기)를 클릭합니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

관련 주제

SOCKS 프록시에서 처리되는 트랜잭션 검색 , 250 페이지

URL 범주 페이지

URL Categories(URL 카테고리**)** 보고서 페이지에서는 시스템의 사용자가 방문 중인 사이트의 URL 카테고리를 볼 수 있습니다.

URL Categories(URL 카테고리) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(웹)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(모니터링) > URL Categories(URL** 카테고리**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

URL Categories(URL 범주) 페이지에서 다음 정보를 볼 수 있습니다.

표 ***62: URL Categories(URL*** 카테고리***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
상위 URL 카테고리: 총 트랜잭션 수	웹 사이트에서 방문하는 상위 URL 카테고리를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
상위 URL 카테고리: 차단 및 경고받은 트랜잭션	트랜잭션별로 차단 또는 경고 조치가 발생하도록 트리거한 상위 URL을 그래픽 형식으로 볼 수 있습니다. 예를 들어 어떤 사용자가 특정 URL을 방문했고, 설정된 어떤 정책 때문에 차단 또는 경고 조치가 실행되었습니다. 그러면 이 URL은 그래프에서 차단된 또는 경고된 트랜잭션으로 표시됩니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
매치하는 URL 범주	URL Categories Matched(일치하는 URL 카테고리) 인터랙티브 테이블은 지정된 시간 범위의 트랜잭션 특성을 URL 카테고리별로 보여줍니다. 각 카테고리의 대역폭 사용량 및 소요 시간도 나타납니다. 미분류 URL이 많을 경우 미분류 URL 줄이기 , 192 페이지를 참조하십시오.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

미분류 URL 줄이기

범주화되지 않은 URL의 비율이 15-20%보다 높으면 다음 옵션을 고려해볼 수 있습니다.

- 특정 현지화된 URL에 대해 맞춤 URL 범주를 생성하고 특정 사용자 또는 그룹 정책에 적용할 수 있습니다. 그러면 이 트랜잭션은 "바이패스한 URL 필터링" 통계에 포함됩니다. 이렇게 하려면

AsyncOS for Cisco Web Security Appliances 사용 설명서에서 맞춤형 URL 카테고리에 대한 정보를 참조하십시오.

- 기존 또는 다른 범주에 포함해야 하는 사이트에 대해서는 오분류 및 미분류 URL 보고 , 193 페이지를 참조하십시오.

URL 카테고리 집합 업데이트 및 보고

URL 범주 집합 업데이트 준비 및 관리 , 365 페이지에 설명된 대로, 사전 정의된 URL 범주 집합은 Security Management Appliance에서 주기적으로 업데이트될 수 있습니다.

이러한 업데이트가 발생하면, 데이터가 너무 오래되어 포함될 수 없을 때까지 이전 범주에 대한 데이터가 보고서 및 웹 추적 결과에 계속 나타납니다. 범주 집합 업데이트 이후에 생성된 보고서 데이터는 새 범주를 사용하므로 기존 범주와 새 범주가 동일한 보고서에 나타날 수 있습니다.

기존 범주와 새 범주 간에 콘텐츠 중복이 있을 경우 유효한 통계를 얻으려면 더 면밀하게 보고서 결과를 검토해야 합니다. 예를 들어 지금 보고 있는 시간 범위에서 “Instant Messaging” 및 “Web-based Chat” 범주가 “Chat and Instant Messaging” 범주로 병합된 경우, 병합 전에 “Instant Messaging” 및 “Web-based Chat” 범주의 사이트에 방문한 것은 “Chat and Instant Messaging” 합계에 포함되지 않습니다. 또한 병합 이후에 “Instant Messaging” 또는 “Web-based Chat” 사이트에 방문한 것은 “Instant Messaging” 또는 “Web-based Chat” 범주의 합계에 포함되지 않습니다.

URL 범주와 다른 보고 페이지 연계 사용

URL 범주 페이지를 Application Visibility(애플리케이션 가시성) 페이지, 216 페이지 및 Users(사용자) 페이지, 225 페이지와 함께 사용하여 특정 사용자, 특정 사용자가 액세스를 시도하는 애플리케이션 또는 웹 사이트 유형을 조사할 수 있습니다.

예를 들어 URL 범주 페이지, 222 페이지에서는 인사부에 대한 상위 레벨 보고서를 생성합니다. 여기서는 사이트에서 방문한 모든 URL 범주를 자세히 보여줍니다. 동일한 페이지에서 URL 범주 ‘Streaming Media’에 대한 세부 사항을 URL 범주 인터랙티브 테이블에서 수집할 수 있습니다. 스트리밍 미디어 범주 링크를 클릭하면 특정 URL 범주 보고서 페이지를 볼 수 있습니다. 이 페이지에서는 스트리밍 미디어 사이트를 방문 중인 상위 사용자를 표시할 뿐 아니라(전체 트랜잭션의 카테고리별 상위 사용자 섹션) YouTube.com 또는 QuickPlay.com과 같은 방문한 도메인(매치하는 도메인 인터랙티브 테이블)도 표시합니다.

여기서는 특정 사용자에 대한 더 자세한 정보를 수집하게 됩니다. 이 사용자의 사용량이 이례적이라면 과연 무엇에 액세스하고 있는지 정확히 알아보고 싶습니다. 사용자 인터랙티브 테이블에서 그 사용자를 클릭할 수 있습니다. 그러면 Users(사용자) 페이지, 225 페이지로 이동합니다. 여기서 이 사용자의 추세를 확인하고 웹에서 정확히 무슨 일을 했는지 알 수 있습니다.

더 나아가 인터랙티브 테이블에서 완료된 트랜잭션 링크를 클릭하면 웹 추적 세부 사항까지 볼 수 있습니다. 이는 웹 추적 페이지에 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지을 표시하는데, 여기서는 사용자가 사이트에 액세스한 날짜, 전체 URL, 그 URL에서 보낸 시간 등의 실제 세부사항을 확인할 수 있습니다.

URL 범주 페이지를 활용하는 또 다른 예를 보려면 예 3: 최다 방문 URL 범주 조사, 569 페이지를 참조하십시오.

오분류 및 미분류 URL 보고

다음 URL에서 오분류 및 미분류 URL을 보고할 수 있습니다.

https://securityhub.cisco.com/web/submit_urls

제출한 자료를 평가하여 후속 규칙 업데이트에 포함합니다.

제출된 URL의 상태를 확인하려면 이 페이지에 있는 **Status on Submitted URLs(**제출된 **URL**의 상태**)** 탭을 클릭합니다.

Users(사용자) 페이지

Users(사용자**)** 보고서 페이지에서 제공하는 여러 링크를 통해 개별 사용자에 대한 웹 보고 정보를 볼 수 있습니다.

Users(사용자) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Users(**사용자**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Users(사용자**)** 페이지에서는 시스템의 한 명 이상의 사용자가 인터넷, 특정 사이트 또는 URL에서 얼마나 시간을 보냈는지, 그리고 해당 사용자가 사용하는 대역폭이 얼마인지를 볼 수 있습니다.

참고 Security Management Appliance가 지원할 수 있는 Web Security Appliance 최대 사용자 수는 500명입니다.

Users(사용자**)** 페이지에서 시스템의 사용자에 대한 다음과 같은 정보를 볼 수 있습니다.

표 ***63: Users(***사용자***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.

섹션	설명
상위 사용자: 차단된 트랜잭션	상위 사용자를 IP 주소 또는 사용자 이름별로 볼 수 있으며, 해당 사용자에 대해 차단된 트랜잭션 수를 그래픽 형식으로 볼 수 있습니다. 보고서에서는 사용자 이름 또는 IP를 식별 불가능하게 만들 수 있습니다. 이 페이지 또는 예약 보고서에서 사용자 이름을 식별 불가능하게 만드는 방법에 대해서는 Security Management Appliance에서 중앙 웹 보고 활성화 , 179 페이지 섹션을 참조하십시오. 기본 설정은 모든 사용자 이름이 나타나는 것입니다. 사용자 이름을 숨기려면 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지를 참조하십시오. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
상위 사용자: 사용된 대역폭	시스템에서 가장 많은 대역폭을 사용하고 있는 상위 사용자를 IP 주소나 사용자 이름별로 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
사용자	특정 사용자 ID 또는 클라이언트 IP 주소를 검색하려면 이 인터랙티브 테이블을 사용할 수 있습니다. User(사용자) 테이블 맨 아래의 텍스트 필드에 특정 사용자 ID 또는 클라이언트 IP 주소를 입력하고 Find User ID or Client IP Address(사용자 ID 또는 클라이언트 IP 주소 찾기)를 클릭합니다. IP 주소가 정확하게 일치하지 않아도 결과를 얻을 수 있습니다. 특정 사용자를 클릭하여 더 구체적인 정보를 얻을 수 있습니다. 자세한 내용은 User Details(사용자 세부 정보) 페이지(웹 보고) , 227 페이지을(를) 참고하십시오.

참고 클라이언트 IP 주소 대신 사용자 ID를 보려면, LDAP 서버에서 사용자 정보를 가져오도록 Security Management Appliance를 설정해야 합니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

User Details(사용자 세부 정보) 페이지(웹 보고)

User Details(사용자 세부 정보**)** 페이지에서는 Users(사용자) 보고서 페이지의 인터랙티브 테이블에서 확인한 사용자에 대한 정보를 확인할 수 있습니다.

User Details(사용자 세부사항) 페이지에서는 개별 사용자가 시스템에서 수행한 활동을 조사할 수 있습니다. 사용자 레벨 조사를 진행 중인데 사용자가 어떤 사이트를 방문하는지, 어떤 악성코드 위협을 겪는지, 어떤 URL 범주에 액세스하는지, 이 사이트에서 얼마나 많은 시간을 보내는지 등을 알아야 할 경우 이 페이지가 특히 유용합니다.

특정 사용자에 대한 User Details(사용자 세부 정보) 페이지를 표시하려면 **Users(**사용자**)** 보고서 페이지의 User(사용자) 인터랙티브 테이블에서 해당 사용자를 클릭합니다.

User Details(사용자 세부사항) 페이지에서 시스템의 개별 사용자에 대한 다음 정보를 볼 수 있습니다.

표 ***64: User Details(***사용자 세부 정보***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
URL 카테고리: 총 트랜잭션 수	특정 사용자가 사용 중인 특정 URL 카테고리를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 사전 정의 URL 범주의 집합은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.
추세: 총 트랜잭션 수	이 트렌드 그래프를 사용하여 특정 사용자의 모든 웹 트랜잭션을 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 이를테면 하루 중 특정 시간대에 웹 트래픽이 급증했는지 여부 및 그 시각을 보여줍니다. 시간 범위 드롭다운 목록으로 이 그래프를 확장하여 해당 사용자가 웹에 있던 시간 범위를 더 면밀하게 또는 더 간략하게 표시할 수 있습니다.

섹션	설명
매치하는 URL 범주	URL Categories Matched(일치하는 URL 카테고리) 섹션에는 완료된 트랜잭션 및 차단된 트랜잭션 모두에 대해 일치하는 카테고리가 표시됩니다. 테이블 맨 아래의 텍스트 필드에 특정 URL 카테고리를 입력하고 **Find URL Category(URL** 카테고리 찾기**)**를 클릭하여 검색할 수 있습니다. 범주가 정확하게 일치하지 않아도 됩니다. 사전 정의 URL 범주의 집합은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.
매치하는 도메인	Domains Matched(매치하는 도메인) 인터랙티브 테이블에는 사용자가 액세스한 도메인 또는 IP 주소가 표시됩니다. 또한 이 카테고리에서 보낸 시간 및 열 보기에서 설정한 기타 다양한 정보도 볼 수 있습니다. 테이블 맨 아래의 텍스트 필드에 특정 도메인 또는 IP 주소를 입력하고 **Find Domain or IP(**도메인 또는 **IP** 찾기**)**를 클릭하여 검색할 수 있습니다. 도메인 또는 IP 주소가 정확하게 일치하지 않아도 됩니다.
매치하는 애플리케이션	Applications Matched(매치하는 애플리케이션) 인터랙티브 테이블에는 특정 사용자가 사용하는 애플리케이션이 표시됩니다. 예를 들어 사용자가 많은 플래시 비디오를 사용해야 하는 웹 사이트에 액세스하고 있다면 애플리케이션 열에서 해당 애플리케이션 유형을 확인합니다. 이 섹션 맨 아래의 텍스트 필드에 특정 애플리케이션 이름을 입력하고 **Find Application(**애플리케이션 찾기**)**을 클릭하여 검색할 수 있습니다. 애플리케이션 이름이 정확하게 일치하지 않아도 됩니다.
Advanced Malware Protection 위협 탐지됨	Advanced Malware Protection Threats Detected(Advanced Malware Protection 위협 탐지됨) 인터랙티브 테이블에는 Advanced Malware Protection 엔진에서 탐지한 악성코드 위협 파일이 표시됩니다. 테이블의 맨 아래에 있는 텍스트 필드에서 악성코드 위협 파일의 특정 SHA 값에 대한 데이터를 입력하고 **Find malware Threat File SHA 256(**악성코드 위협 파일 **SHA 256** 찾기**)**를 클릭하여 검색할 수 있습니다. 애플리케이션 이름이 정확하게 일치하지 않아도 됩니다.

섹션	설명
탐지된 악성코드 위협	Malware Threats Detected(악성코드 위협 탐지됨) 인터랙티브 테이블에는 특정 사용자가 트리거하는 상위 악성코드 위협이 표시됩니다. 테이블의 맨 아래에 있는 텍스트 필드에서 특정 악성코드 위협 파일에 대한 데이터를 입력하고 **Find Malware Threat(**악성코드 위협 찾기**)**를 클릭하여 검색할 수 있습니다. 악성코드 위협의 이름이 정확하게 일치하지 않아도 됩니다.
매치하는 정책	Policies Matched(매치하는 정책) 인터랙티브 테이블에는 웹에 액세스할 때 이 사용자에게 적용되는 정책 그룹이 표시됩니다. 이 섹션 맨 아래의 텍스트 필드에 특정 정책 이름을 입력하고 **Find Policy(**정책 찾기**)**을 클릭하여 검색할 수 있습니다. 정책 이름이 정확하게 일치하지 않아도 됩니다.

참고 클라이언트 악성코드 위험 세부사항 테이블: 클라이언트 보고서에서는 사용자 이름 끝에 별표(*)를 표시할 때가 있습니다. 예를 들어 “jsmith” 및 “jsmith*” 모두에 한 항목을 표시합니다. 별표(*)가 있는 사용자 이름은 그 사용자가 부여한 이름이며, 인증 서버에서 확인하지 않았습니다. 해당 시점에 인증 서버를 사용할 수 없었고 애플리케이션 서비스가 제공되지 않을 때 트래픽을 허용하도록 어플라이언스가 구성된 경우 이렇게 됩니다.

웹 사이트 페이지

Web Sites(웹 사이트**)** 보고서 페이지에서는 관리 대상 어플라이언스에서 일어나는 활동을 종합적으로 살펴볼 수 있습니다. 이 보고서 페이지를 사용하여 특정 시간 범위에 액세스한 고위험 웹 사이트를 모니터링할 수 있습니다.

Web Sites(웹 사이트) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Web Sites(**웹 사이트**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

Web Sites(웹 사이트) 페이지에서 다음 정보를 볼 수 있습니다.

표 ***65: Web Sites(***웹 사이트***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.

섹션	설명
상위 도메인: 총 트랜잭션 수	웹 사이트에서 방문하는 상위 도메인을 그래프 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
상위 도메인: 차단된 트랜잭션	트랜잭션별로 차단 조치가 발생하도록 트리거한 상위 도메인을 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오. 예를 들어 어떤 사용자가 특정 도메인을 방문했고, 설정된 어떤 정책 때문에 차단 조치가 실행되었습니다. 이 도메인은 이 그래프에서 차단된 트랜잭션으로 표시되고 차단 조치를 유발한 도메인 사이트가 목록에 포함됩니다.
매치하는 도메인	인터랙티브 테이블을 사용하여 웹 사이트에서 방문하는 도메인을 검색할 수 있습니다. 특정 도메인을 클릭하여 더 세부적인 정보에 액세스할 수 있습니다. 웹 추적 페이지의 프록시 서비스 탭이 나타나고 추적 정보 및 특정 도메인이 차단된 이유를 확인할 수 있습니다. 특정 도메인을 클릭하면 그 도메인의 상위 사용자, 상위 트랜잭션, 매치한 URL 범주, 탐지된 악성코드 위협을 볼 수 있습니다. 웹 추적을 활용하는 예를 보려면 예 2: URL 추적, 569 페이지를 참조하십시오.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

HTTPS 보고서 페이지

HTTPS Reports(HTTPS 보고서) 보고서 페이지는 관리 대상 어플라이언스의 HTTP/HTTPS 트래픽 요약에 대한 전체 집계입니다.

또한 매니지드 어플라이언스를 통과하는 개별 HTTP/HTTPS 웹 트래픽에 대해 클라이언트 측 연결 또는 서버 측 연결을 기준으로 지원되는 암호의 요약을 볼 수 있습니다.

HTTPS Reports(HTTPS 보고서) 보고서 페이지를 보려면 **Product(제품)** 드롭다운에서 **Web(웹)**을 선택하고 **Reports(보고서)** 드롭다운에서 **Monitoring(모니터링)> HTTPS Reports(HTTPS 보고서)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지의 내용을 참고하십시오.

표 ***66: HTTPS*** 보고서 페이지의 상세정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
웹 트래픽 요약	다음 방법 중 하나를 사용하여 어플라이언스의 웹 트래픽 요약을 볼 수 있습니다. • **Transactions(**트랜잭션**)**: 그래픽 형식의 HTTP 또는 HTTPS 웹 트랜잭션 수 및 테이블 형식의 HTTP 또는 HTTPS 웹 트랜잭션 백분율을 기반으로 웹 트래픽 요약을 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다. • **Bandwidth Usage(**대역폭 사용량**)**: 그래픽 형식의 HTTP 또는 HTTPS 웹 트래픽에서 사용하는 대역폭 양 및 테이블 형식의 HTTP 또는 HTTPS 대역폭 사용량 백분율을 기반으로 웹 트래픽 요약을 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다.
추세: 웹 트래픽	다음 방법 중 하나를 사용하여 필요한 시간 범위를 기준으로 어플라이언스의 웹 트래픽에 대한 추세 그래프를 볼 수 있습니다. • **Web Traffic Trend(**웹 트래픽 추세**)**: 트랜잭션 또는 대역폭 사용량을 기준으로 HTTP 및 HTTPS 웹 트래픽에 대한 누적 추세를 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다. • **HTTPS Trend(HTTPS** 추세**)**: 트랜잭션 또는 대역폭 사용량을 기준으로 HTTPS 웹 트래픽에 대한 추세를 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다. • **HTTP Trend(HTTPS** 추세**)**: 트랜잭션 또는 대역폭 사용량을 기준으로 HTTP 웹 트래픽에 대한 추세를 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다.
암호화	다음 방법 중 하나를 사용하여 암호의 요약을 볼 수 있습니다. • **By Client Side Connections(**클라이언트 측 연결 기준**)**: HTTP 또는 HTTPS 웹 트래픽의 클라이언트 측에서 사용되는 암호의 요약을 그래픽 형식으로 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다. • **By Server Side Connections(**서버 측 연결 기준**)**: HTTP 또는 HTTPS 웹 트래픽의 서버 측에서 사용되는 암호의 요약을 그래픽 형식으로 표시하려면 드롭다운 목록에서 이 옵션을 선택합니다.

Anti-Malware(악성코드 차단) 페이지

Anti-Malware(악성코드 차단**)** 보고서 페이지는 보안 관련 보고서 페이지이며, 활성화된 검사 엔진(Webroot, Sophos, McAfee, Adaptive Scanning)의 검사 결과를 반영합니다.

Anti-Malware(악성코드 차단) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Anti-Malware(**악성코드 차단**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

이 페이지를 사용하여 웹 기반 악성코드 위협을 식별하고 모니터링할 수 있습니다.

참고 L4 Traffic Monitor에서 찾은 악성코드에 대한 데이터를 보려면 다음 섹션을 참조하십시오. Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지, 219 페이지

Anti-Malware(악성코드 차단) 페이지에서 다음 정보를 볼 수 있습니다.

표 ***67: Anti-Malware(***악성코드 차단***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
주요 멀웨어 종류	지정된 카테고리 유형으로 탐지된 상위 악성코드 카테고리를 그래픽 형식으로 볼 수 있습니다. 유효한 악성코드 범주에 대해서는 악성코드 카테고리 설명, 197 페이지를 참조하십시오. 차트의 보기를 사용자 지정하려면 차트에서 ✓을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
상위 악성코드 위협	상위 악성코드 위협을 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.

섹션	설명
악성코드 범주	이 인터랙티브 테이블에서는 상위 악성코드 범주 차트에 표시된 특정 악성코드 범주에 대한 자세한 정보를 제공합니다. 악성코드 범주 인터랙티브 테이블에서 어떤 링크를 클릭하면 개별 악성코드 범주 및 네트워크에서의 위치에 대한 자세한 정보를 볼 수 있습니다. 예외: 보안 침해 휴리스틱 링크를 클릭하면 이 범주의 트랜잭션이 발생한 시점을 보여주는 차트가 나타납니다. 유효한 악성코드 범주에 대해서는 악성코드 카테고리 설명, 197 페이지를 참조하십시오.
악성코드 위협	이 인터랙티브 테이블에서는 상위 악성코드 위협 섹션에 표시된 특정 악성코드 위협에 대한 자세한 정보를 제공합니다. “Outbreak(보안 침해)” 레이블과 숫자가 표시된 위협은 다른 검사 엔진과 상관없이 Adaptive Scanning 기능에서 식별한 위협입니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

악성코드 범주 보고서

이 페이지에서는 개별 악성코드 범주 및 네트워크에서 수행하는 활동에 대한 자세한 정보를 볼 수 있습니다.

악성코드 범주 보고서 페이지에 액세스하려면 다음을 수행합니다.

단계 **1** Security Management Appliance의 드롭다운 목록에서 **Web(웹)**을 선택합니다.

단계 **2** **Monitoring(모니터링) > Anti-Malware(악성코드 차단)** 페이지를 선택합니다.

단계 **3** Malware Categories(악성코드 범주) 인터랙티브 테이블의 Malware Category(악성코드 범주) 열에서 범주를 클릭합니다.

단계 **4** 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

악성코드 위협 보고서

특정 위협에 대해 위험한 상태인 클라이언트를 보여줍니다. 감염되었을 가능성이 있는 클라이언트의 목록 및 클라이언트 세부사항 페이지 링크를 표시합니다. 보고서 맨 위의 추세 그래프는 지정된 시간 범위에 어떤 위협에 대해 모니터링되고 차단된 트랜잭션을 표시합니다. 맨 아래의 테이블은 지정된 시간 범위에 어떤 위협에 대해 모니터링되고 차단된 트랜잭션의 실제 개수를 표시합니다.

이 보고서를 보려면 악성코드 차단 보고서 페이지의 악성코드 범주 열에 있는 범주를 클릭합니다.

자세한 내용은 테이블 아래의 **Support Portal Malware Details(**지원 포털 악성코드 세부사항**)**를 클릭하여 확인하십시오.

악성코드 카테고리 설명

Web Security Appliance는 다음의 악성코드 유형을 차단할 수 있습니다.

악성코드 유형	설명
애드웨어	사용자를 판매할 제품으로 연결하는 모든 소프트웨어 실행 파일 및 플러그인을 포함합니다. 일부 애드웨어 애플리케이션은 별도의 프로세스가 동시에 실행되어 서로 모니터링하면서 영구적인 수정을 보장합니다. 시스템이 시작할 때마다 자동으로 실행되게 하는 변형도 있습니다. 보안 설정을 변경하여 사용자가 브라우저 검색 옵션, 바탕화면, 기타 시스템 설정을 변경하지 못하게 하는 프로그램도 있습니다.
브라우저 헬퍼 개체	브라우저 플러그인이며 광고 서비스 또는 사용자 설정 하이재킹과 관련된 다양한 기능을 수행할 수 있습니다.
상업용 시스템 모니터	상업용 시스템 모니터는 법적인 수단을 통해 적법한 라이센스로 확보할 수 있는 시스템 모니터 특성이 포함된 소프트웨어 부분입니다.
다이얼러	사용자의 모뎀 또는 기타 인터넷 액세스 유형을 이용하여 어떤 전화선 또는 사이트에 연결함으로써 완전한 사전 고지에 의한 사용자 동의 없이 장거리 통화 요금이 부과되게 하는 프로그램입니다.
일반 스파이웨어	스파이웨어는 컴퓨터에 설치되는 일종의 악성코드이며, 사용자가 모르는 사이에 사용자에 대한 작은 정보 조각을 수집합니다.
하이잭커	시스템 설정을 수정하거나 사용자가 원치 않는 시스템 변경을 수행하는 수법으로 완전한 사전 고지에 의한 사용자 동의 없이 어떤 웹 사이트로 연결하거나 프로그램을 실행하기도 합니다.
기타 악성코드	이 카테고리는 정의된 다른 카테고리 중 하나에 정확하게 맞지 않는 기타 모든 악성코드와 의심스러운 동작을 포착하는 데 사용됩니다.
보안 침해 휴리스틱	이 범주는 다른 악성코드 차단 엔진과 관계없이 Adaptive Scanning에서 찾아낸 악성코드입니다.
피싱 URL	피싱 URL은 브라우저 주소 창에 표시됩니다. 도메인 이름을 사용하고 합법적 도메인을 모방하는 경우도 있습니다. 온라인 신원 도용 형태 중 하나로서 사회공학 및 기술적 속임수를 모두 구사하면서 개인 신원 데이터 및 금융 계정 자격 증명을 훔칩니다.
PUA	Potentially Unwanted Application. PUA는 악성이 아니지만 원치 않는 것으로 간주할 수 있는 애플리케이션입니다.

악성코드 유형	설명
시스템 모니터	다음 작업 중 하나를 수행하는 모든 소프트웨어를 포괄합니다. 명시적으로 또는 은밀하게 시스템 프로세스 또는 사용자 작업을 기록합니다. 나중에 이러한 레코드를 검색 및 검토할 수 있도록 합니다.
트로이 목마 다운로더	설치되면 원격 호스트/사이트에 접속하고 원격 호스트로부터 패키지 또는 연관 프로그램을 설치하는 트로이 목마입니다. 이러한 설치는 대개 사용자 모르게 이루어집니다. 또한 트로이 목마 다운로더의 페이로드는 설치마다 달라질 수 있습니다. 원격 호스트/사이트로부터 다운로드 명령을 받기 때문입니다.
트로이 목마	트로이 목마는 무해한 애플리케이션으로 위장한 파괴적인 프로그램입니다. 바이러스와 달리 트로이 목마는 자체적으로 복제하지 않습니다.
트로이 피셔	감염된 컴퓨터에 상주하면서 특정 웹 페이지에 방문할 때까지 기다리거나 감염된 시스템을 검사하여 은행 사이트, 옥션 사이트, 온라인 결제 사이트용 사용자 이름 및 암호를 찾아낼 수 있습니다.
바이러스	사용자 모르게 컴퓨터에 로드되어 사용자의 의사와 상관없이 실행되는 프로그램 또는 코드입니다.
웜	컴퓨터 네트워크를 통해 자가 복제하는 프로그램 또는 알고리즘이며 대개 악성 활동을 수행합니다.

클라이언트 악성코드 위험 보고서

Client Malware Risk(클라이언트 악성코드 위험**)** 보고서 페이지는 보안 관련 보고 페이지이며 클라이언트 악성코드 위험 활동을 모니터링하는 데 사용할 수 있습니다.

Client Malware Risk(클라이언트 악성코드 위험) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Client Malware Risk(**클라이언트 악성코드 위험**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

시스템 관리자는 Client Malware Risk(클라이언트 악성코드 위험) 보고서 페이지에서 사용자 중 누가 가장 많은 차단 또는 경고를 겪고 있는지 확인할 수 있습니다. 관리자는 이 페이지에서 수집한 정보를 토대로 사용자 링크를 클릭하여 이 사용자가 웹에서 무슨 활동을 하여 그토록 많은 차단 또는 경고를 받았는지 또한 네트워크의 다른 사용자보다 더 많은 탐지를 유발했는지 파악할 수 있습니다.

또한 클라이언트 악성코드 위험 페이지에서는 L4TM(L4 Traffic Monitor)에서 찾아낸 자주 발생하는 악성코드 연결과 관련된 클라이언트 IP 주소를 나열합니다. 악성코드 사이트에 자주 연결되는 컴퓨터는 중앙 C&C(command and control) 서버와의 연결을 시도하는 악성코드에 감염되었을 가능성이 있으며 따라서 치료해야 합니다.

다음 표에서는 Client Malware Risk(클라이언트 악성코드 위험) 페이지의 정보를 설명합니다.

표 ***68: Client Malware Risk(***클라이언트 악성코드 위험***)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
웹 프록시: 모니터링 또는 차단된 상위 클라이언트	악성코드 위험이 발생한 상위 10명의 사용자를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오.
L4 Traffic Monitor: 탐지된 악성코드 연결	악성코드 사이트에 가장 자주 연결하는 사용자 조직에 있는 10대의 컴퓨터의 IP 주소를 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오. Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지, 219 페이지의 "상위 클라이언트 IP" 차트와 동일합니다.
웹 프록시: 클라이언트 악성코드 위험	Web Proxy: Client Malware Risk(웹 프록시: 클라이언트 악성코드 위험) 테이블에는 Web Proxy: Top Clients by Malware Risk(웹 프록시: 악성코드 위험별 상위 클라이언트)에 표시된 특정 클라이언트에 대한 자세한 정보가 표시됩니다. 이 테이블에서 각 사용자를 클릭하여 그 클라이언트의 사용자 세부사항 페이지를 표시할 수 있습니다. 그 페이지에 대해서는 User Details(사용자 세부 정보) 페이지(웹 보고) , 227 페이지를 참조하십시오. 테이블의 링크 중 아무거나 클릭하면 개별 사용자 및 악성코드 위험을 유발하는 그 사용자의 활동을 더 자세히 알아볼 수 있습니다.
L4 Traffic Monitor: 악성코드 위험별 클라이언트	L4 Traffic Monitor: Clients by Malware Risk(L4 트래픽 모니터: 악성코드 위험별 클라이언트) 인터랙티브 테이블에는 사내에서 악성코드 사이트에 자주 연결하는 컴퓨터의 IP 주소가 표시됩니다. Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지, 219 페이지의 "클라이언트 IP" 테이블과 동일합니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

Web Reputation Filters(웹 평판 필터) 페이지

Web Reputation Filters(웹 평판 필터**)** 보고서 페이지를 사용하여 지정된 시간 범위의 트랜잭션에 대해 설정한 웹 평판 필터의 결과를 볼 수 있습니다.

Web Reputation Filters(웹 평판 필터) 보고서 페이지를 보려면 Product(제품) 드롭다운에서 **Web(**웹**)**을 선택하고 Reports(보고서) 드롭다운에서 **Monitoring(**모니터링**) > Web Reputation Filters(**웹 평판 필터**)**를 선택합니다. 자세한 내용은 인터랙티브 보고서 페이지 사용, 49 페이지을 참고하십시오.

웹 평판 필터란**?**

웹 서버 동작을 분석하고 URL에 평판 점수를 부여하여 URL 기반 악성코드를 포함하고 있을 가능성을 나타냅니다. 따라서 최종 사용자 개인 정보 및 민감한 기업 정보를 위협하는 URL 기반 악성코드 차단에 도움이 됩니다. Web Security Appliance는 URL 평판 점수를 사용하여 의심스러운 활동을 식별하고 악성코드 공격을 사전에 방지합니다. 웹 평판 필터는 액세스 정책 및 해독 정책 모두와 함께 사용할 수 있습니다.

웹 평판 필터에서는 통계 데이터를 사용하여 인터넷 도메인의 신뢰도를 평가하고 URL 평판 점수를 산정합니다. 특정 도메인이 등록된 기간, 웹 사이트가 호스팅되는 위치, 웹 서버에서 동적 IP 주소를 사용하는지 여부 등의 데이터를 참조하여 URL의 신뢰도를 평가합니다.

웹 평판 계산 시 URL을 네트워크 매개변수와 연계하여 악성코드가 있을 가능성을 판단합니다. 그런 다음, 악성코드가 존재할 확률 합계가 -10에서 +10 사이의 웹 평판 점수에 매핑됩니다. +10이 악성코드를 포함할 가능성이 가장 낮은 경우입니다.

예를 들어, 매개변수는 다음과 같습니다.

- URL 분류 데이터
- 다운로드 가능한 코드 있음
- 길고 애매한 EULA(End-User License Agreements)의 존재 여부
- 전역 볼륨 및 볼륨 변경
- 네트워크 소유자 정보
- URL 이력
- URL 유효 기간
- 차단 목록에 있는지 여부
- 허용 목록에 있는지 여부
- 인기 있는 도메인의 URL 오자
- 도메인 등록자 정보
- IP 주소 정보

웹 평판 필터링에 대한 자세한 내용은 *AsyncOS for Web Security Appliance* 사용 설명서의 '웹 평판 필터'를 참조하십시오.

Web Reputation Filters(웹 평판 필터) 페이지에서 다음 정보를 볼 수 있습니다.

표 ***69: Web Reputation Filters(웹 평판 필터)*** 페이지 세부 정보

섹션	설명
Time Range (drop-down list)(시간 범위(드롭다운 목록))	보고서에 대한 시간 범위를 선택합니다. 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지을 참조하십시오.
웹 평판 조치(추세)	지정된 시간에 대한 웹 평판 작업의 총 수를 그래픽 형식으로 볼 수 있습니다. 여기서 웹 평판 작업의 장기 추세를 예상할 수 있습니다.
웹 평판 작업(볼륨)	트랜잭션별 웹 평판 조치 볼륨(백분율)을 표시할 수 있습니다.
웹 평판: WBRS에서 차단한 위협 유형	웹 평판 필터링에서 차단한 트랜잭션에서 발견된 위협 유형을 그래픽 형식으로 볼 수 있습니다. 참고 WBRS에서 위협 유형을 식별하지 못할 때도 있습니다.
다른 트랜잭션에서 탐지된 위협 유형	웹 평판 필터링에서 차단되지 않은 트랜잭션에서 발견된 위협 유형을 그래픽 형식으로 볼 수 있습니다. 차트의 보기를 사용자 지정하려면 차트에서 ✓ 을 클릭합니다. 자세한 내용은 (웹 보고서만) 차트에 표시할 데이터 선택, 51 페이지을 참고하십시오. 이 위협이 차단되지 않은 이유로는 • 모든 위협의 점수가 차단 임계값에 도달하는 것은 아닙니다. 그러나 어플라이언스의 다른 기능에서 이 위협을 잡아낼 수도 있습니다. • 위협의 통과를 허용하도록 정책이 구성될 수도 있습니다. 참고 WBRS에서 위협 유형을 식별하지 못할 때도 있습니다.
웹 신뢰도 작업(점수별 분석)	Adaptive Scanning이 활성화되지 않은 경우 이 인터랙티브 테이블은 각 작업에 대한 웹 평판 점수를 분류하여 표시합니다.

팁 이 보고서의 보기를 맞춤 설정하려면 웹 보안 보고서 사용, 181 페이지를 참조하십시오.

웹 평판 설정 조정

보고서 결과에 따라 구성된 웹 평판 설정을 조정할 수도 있습니다. 이를테면 임계 점수를 조정하거나 Adaptive Scanning을 활성화/비활성화합니다. 웹 평판 설정 구성에 대한 자세한 내용은 *AsyncOS for Cisco Web Security Appliances* 사용 설명서를 참조하십시오.

예약 및 온디맨드 웹 보고서 정보

달리 명시되지 않는 한 다음 웹 보안 보고서 유형은 예약 또는 온디맨드 버전으로 생성할 수 있습니다.

- 웹 보고 개요 - 이 페이지의 내용에 대해서는 웹 보고 개요 , 186 페이지를 참조하십시오.
- 사용자 - 이 페이지의 내용에 대해서는 사용자 보고서(웹) , 187 페이지를 참조하십시오.
- 웹 사이트 - 이 페이지의 내용에 대해서는 웹 사이트 보고서 , 190 페이지를 참조하십시오.
- URL 범주 - 이 페이지의 내용에 대해서는 URL 범주 보고서 , 191 페이지를 참조하십시오.
- 상위 URL 범주 - 확장: 상위 URL 범주 - 확장에 대한 보고서를 생성하는 방법은 상위 URL 범주 - 확장, 241 페이지를 참조하십시오.

이 보고서는 온디맨드 보고서로 사용할 수 없습니다.

- 애플리케이션 가시성 - 이 페이지의 내용에 대해서는 애플리케이션 가시성 보고서 , 194 페이지를 참조하십시오.
- 상위 애플리케이션 유형 - 확장: 상위 URL 범주 - 확장에 대한 보고서를 생성하는 방법은 상위 애플리케이션 유형 - 확장, 242 페이지를 참조하십시오.

이 보고서는 온디맨드 보고서로 사용할 수 없습니다.

- 악성코드 차단 - 이 페이지의 내용에 대해서는 악성코드 차단 보고서 , 195 페이지를 참조하십시오.
- 클라이언트 악성코드 위험 - 이 페이지의 내용에 대해서는 클라이언트 악성코드 위험 보고서 , 203 페이지를 참조하십시오.
- 웹 평판 필터 - 이 페이지의 내용에 대해서는 웹 평판 필터 보고서 , 204 페이지를 참조하십시오.
- L4 Traffic Monitor—이 페이지의 내용에 대해서는 L4 Traffic Monitor 보고서 , 206 페이지를 참조하십시오.
- 모바일 보안 솔루션 - 이 페이지의 내용에 대해서는 사용자 위치별 보고서 , 208 페이지를 참조하십시오.
- 시스템 용량 - 이 페이지의 내용에 대해서는 System Capacity(시스템 용량) 페이지, 210 페이지를 참조하십시오.

웹 보고서 예약

이 섹션에서는 다음 주제에 대해 알아봅니다.

- 예약 웹 보고서 추가, 240 페이지
- 예약 웹 보고서 수정, 241 페이지
- 예약 웹 보고서 삭제, 241 페이지
- 추가 확장 웹 보고서, 241 페이지

참고 모든 보고서에서 사용자 이름이 식별 불가능하게 할 수 있습니다. 자세한 내용은 웹 보고서에서 사용자 이름 익명 처리 , 181 페이지를 참조하십시오.

매일, 매주 또는 매달 보고서를 실행하도록 예약할 수 있습니다. 예약 보고서는 전날, 지난 7일, 지난 달, 지난 역일(최대 250일), 지난 역월(최대 12개월)의 데이터를 포함하도록 구성할 수 있습니다. 또는 맞춤 일수(2일 ~ 100일(또는 맞춤 월수(2개월 ~ 12개월)의 데이터를 포함할 수 있습니다.

보고서 실행 시점과 상관없이 데이터는 이전 시간 간격(시간, 일, 주, 월)에서 반환됩니다. 예를 들어 오전 1시에 일일 보고서를 실행하도록 예약할 경우 전날 자정부터 자정까지(00:00 ~ 23:59)의 데이터가 포함됩니다.

0명을 포함하여 원하는 만큼 보고서의 수신자를 정의할 수 있습니다. 이메일 수신자를 지정하지 않더라도 시스템에서는 여전히 보고서를 보관합니다. 그러나 보고서를 대량의 주소로 전송하려면 수신자를 개별적으로 나열하는 것보다 메일 목록을 작성하는 것이 더 쉬울 수 있습니다.

예약 웹 보고서 저장

Security Management Appliance는 각 예약된 최신 보고서 최대 30개 인스턴스, 모든 보고서 최대 총 1000개 버전까지 최신 보고서를 유지합니다.

아카이브 보고서는 자동으로 삭제됩니다. 새 보고서가 추가되면 1000개 개수를 유지하기 위해 이전 보고서가 제거됩니다. 30개 인스턴스 한도는 동일한 이름 및 시간 범위의 예약 보고서 각각에 적용됩니다.

아카이브 보고서는 어플라이언스의 /periodic_reports 디렉터리에 저장됩니다. (자세한 내용은 IP 인터페이스 및 어플라이언스 액세스, 547 페이지를 참조해 주십시오.)

관련 주제

- 아카이브 웹 보고서 보기 및 관리, 244 페이지

예약 웹 보고서 추가

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > Scheduled Reports(예약된 보고서)**를 선택합니다.

단계 **2** **Add Scheduled Report(예약된 보고서 추가)**를 클릭합니다.

단계 **3** **Type(유형)** 옆의 드롭다운 메뉴에서 보고서 유형을 선택합니다.

단계 **4** **Title(제목)** 필드에 보고서의 제목을 입력합니다.

같은 이름으로 여러 보고서가 생성되지 않도록 설명적 제목을 사용하는 것이 좋습니다.

단계 **5** **Time Range(시간 범위)** 드롭다운 메뉴에서 보고서의 시간 범위를 선택합니다.

단계 **6** 생성된 보고서의 형식을 선택합니다.

기본 형식은 PDF입니다. 또한 대부분의 보고서에서는 원시 데이터를 CSV 파일로 저장할 수 있습니다.

단계 **7** **Number of Items(**항목 수**)** 옆의 드롭다운 목록에서 생성된 보고서에 포함할 항목의 수를 선택합니다.

유효한 값은 2 ~ 20입니다. 기본값은 5입니다.

단계 **8** **Charts(**차트**)**에서는 **Data to display(**표시할 데이터**)** 아래서 기본 차트를 클릭하고 보고서에서 각 차트에 표시할 데이터를 선택합니다.

단계 **9** **Sort Column(**열 정렬**)** 옆의 드롭다운 목록에서 이 보고서 데이터의 정렬 기준이 될 열을 선택합니다. 그러면 예약 보고서에서 제공되는 임의의 열을 기준으로 상위 'N'개 항목에 대한 예약 보고서를 생성할 수 있습니다.

단계 **10** **Schedule(**일정**)** 영역에서는 예약 보고서를 위해 일, 주, 월 옆에 있는 라디오 버튼을 선택합니다.

단계 **11** **Email(**이메일**)** 텍스트 필드에는 생성된 보고서를 받을 이메일 주소를 입력합니다.

이메일 주소를 지정하지 않으면 보고서는 보관될 뿐입니다.

단계 **12** 제출을 클릭합니다.

예약 웹 보고서 수정

보고서를 수정하려면 **Web(**웹**) > Reporting(**보고**) > Scheduled Reports(**예약 보고서**)** 페이지로 이동하고 수정할 보고서의 확인란을 선택합니다. 설정을 수정한 다음 **Submit(**제출**)**을 클릭하여 페이지에서 변경사항을 제출하고 **Commit Changes(**변경사항 커밋**)** 버튼을 클릭하여 어플라이언스에서 변경사항을 커밋합니다.

예약 웹 보고서 삭제

보고서를 삭제하려면 **Web(**웹**) > Reporting(**보고**) > Scheduled Reports(**예약 보고서**)** 페이지로 이동하고 삭제할 보고서의 확인란을 선택합니다. 모든 예약 보고서를 삭제하려면 **All(**전체**)** 확인란을 선택하고 **Delete(**삭제**)**를 선택한 다음 변경사항을 **Commit(**커밋**)**합니다. 삭제된 보고서의 아카이브 버전은 삭제되지 않습니다.

추가 확장 웹 보고서

두 가지 추가 보고서는 Security Management Appliance에서 예약된 보고서로서만 사용 가능합니다.

- 상위 URL 범주 - 확장, 241 페이지
- 상위 애플리케이션 유형 - 확장, 242 페이지

상위 **URL** 범주 **-** 확장

URL 범주 보고서보다 자세한 정보를 얻으려는 관리자에게 유용합니다.

예를 들어 일반적인 URL 범주 보고서에서는 더 큰 URL 범주 레벨에서 특정 직원의 대역폭 사용량을 추적하면서 정보를 수집할 수 있습니다. URL 범주별로 상위 10개 URL의 대역폭 사용량 또는 URL 범주별로 상위 5명 사용자의 대역폭 사용량을 모니터링하려면 상위 URL 범주 - 확장 보고서를 사용합니다.

참고 이 보고서 유형으로 생성 가능한 보고서의 최대 개수는 20입니다.

- 사전 정의 URL 범주 목록은 때때로 업데이트됩니다. 이 업데이트가 보고서 결과에 미치는 영향에 대해서는 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오.

상위 URL 범주 - 확장 보고서를 생성하려면 다음을 수행합니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > Scheduled Reports(예약된 보고서)**를 선택합니다.

단계 **2** **Add Scheduled Report(예약 보고서 추가)**를 클릭합니다.

단계 **3** Type(유형) 옆의 드롭다운 메뉴에서 **Top URL Categories - Extended(상위 URL 범주 - 확장)**를 선택합니다.

단계 **4** **Title(제목)** 텍스트 필드에 URL 확장 보고서 제목을 입력합니다.

단계 **5** **Time Range(시간 범위)** 드롭다운 메뉴에서 보고서의 시간 범위를 선택합니다.

단계 **6** 생성된 보고서의 형식을 선택합니다.

기본 형식은 PDF입니다.

단계 **7** **Number of Items(항목 수)** 옆의 드롭다운 목록에서 생성된 보고서에 포함할 URL 범주의 수를 선택합니다.

유효한 값은 2 ~ 20입니다. 기본값은 5입니다.

단계 **8** **Sort Column(열 정렬)** 옆의 드롭다운 목록에서 이 보고서 데이터의 정렬 기준이 될 열을 선택합니다. 그러면 예약 보고서에서 제공되는 임의의 열을 기준으로 상위 'N'개 항목에 대한 예약 보고서를 생성할 수 있습니다.

단계 **9** **Charts(차트)**에서는 **Data to display(표시할 데이터)** 아래서 기본 차트를 클릭하고 보고서에서 각 차트에 표시할 데이터를 선택합니다.

단계 **10** **Schedule(일정)** 영역에서는 예약 보고서를 위해 일, 주, 월 옆에 있는 라디오 버튼을 선택합니다.

단계 **11** **Email(이메일)** 텍스트 필드에는 생성된 보고서를 받을 이메일 주소를 입력합니다.

단계 **12** 제출을 클릭합니다.

상위 애플리케이션 유형 - 확장

상위 애플리케이션 유형 - 확장 보고서를 생성하려면 다음을 수행합니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > Scheduled Reports(예약된 보고서)**를 선택합니다.

단계 **2** **Add Scheduled Report(예약 보고서 추가)**를 클릭합니다.

단계 **3** Type(유형) 옆의 드롭다운 메뉴에서 **Top Application Type — Extended(상위 애플리케이션 유형 - 확장)**를 선택합니다.

페이지의 옵션은 바뀝니다.

단계 **4** **Title**(제목) 텍스트 필드에 보고서의 제목을 입력합니다.

단계 **5** **Time Range**(시간 범위) 드롭다운 메뉴에서 보고서의 시간 범위를 선택합니다.

단계 **6** 생성된 보고서의 형식을 선택합니다.

기본 형식은 PDF입니다.

단계 **7** **Number of Items**(항목 수) 옆의 드롭다운 목록에서 생성된 보고서에 포함할 애플리케이션 유형의 수를 선택합니다.

유효한 값은 2 ~ 20입니다. 기본값은 **5**입니다.

단계 **8** **Sort Column**(열 정렬) 옆의 드롭다운 목록에서 테이블에 표시할 열 수를 선택합니다. Transactions Completed(완료된 트랜잭션), Transactions Blocked(차단된 트랜잭션), Transaction Totals(트랜잭션 총계) 중에서 선택합니다.

단계 **9** **Charts**(차트)에서는 **Data to display**(표시할 데이터) 아래서 기본 차트를 클릭하고 보고서에서 각 차트에 표시할 데이터를 선택합니다.

단계 **10** **Schedule**(일정) 영역에서는 예약 보고서를 위해 일, 주, 월 옆에 있는 라디오 버튼을 선택합니다.

단계 **11** **Email**(이메일) 텍스트 필드에는 생성된 보고서를 받을 이메일 주소를 입력합니다.

단계 **12** 제출을 클릭합니다.

온디맨드 웹 보고서 생성

예약 가능한 보고서 대부분은 온디맨드 생성도 가능합니다.

참고 일부 보고서는 온디맨드가 불가하고 예약 보고서로만 이용 가능합니다. 추가 확장 웹 보고서, 241 페이지를 참조하십시오.

온디맨드 보고서를 생성하려면 다음 단계를 수행합니다.

단계 **1** Security Management Appliance에서 **Web**(웹) > **Reporting**(보고) > **Archived Reports**(보관된 보고서)를 선택합니다.

단계 **2** **Generate Report Now**(지금 보고서 생성)를 클릭합니다.

단계 **3** **Report type**(보고서 유형) 섹션의 드롭다운 목록에서 보고서 유형을 선택합니다.

페이지의 옵션은 바뀝니다.

단계 **4** 제목 텍스트 필드에 보고서 제목의 이름을 입력합니다.

AsyncOS는 보고서 이름의 고유성을 확인하지 않습니다. 혼동을 피하려면 동일한 이름의 여러 보고서를 만들지 마십시오.

단계 **5** **Time Range to Include**(포함할 시간 범위) 드롭다운 목록에서는 보고서 데이터의 시간 범위를 선택합니다.

단계 **6** 형식에서는 보고서의 형식을 선택합니다.

선택 사항은 다음과 같습니다.

- PDF. 전달용, 보관용 또는 둘 모두를 위한 형식이 지정된 PDF 문서를 만듭니다. Preview PDF Report(PDF 보고서 미리 보기)를 클릭하여 보고서를 PDF 파일로 즉시 볼 수 있습니다.
- CSV. 표 형식의 데이터 및 쉼표로 구분된 값을 포함하는 ASCII 텍스트 파일을 만듭니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다.

단계 **7** 보고서에 대해 사용 가능한 옵션에 따라 다음을 선택합니다.

- **Number of rows(**행 수**)**: 테이블에 표시할 데이터 행 수.
- **Charts(**차트**)**: 보고서의 차트에 표시할 데이터.
- 표시할 데이터 아래에서 기본 옵션을 클릭합니다.
- **Sort Column(**열 정렬**)**: 각 테이블의 정렬 기준이 될 열입니다.

단계 **8** 전달 옵션에서 다음을 선택합니다.

- 이 보고서를 Archive Report(아카이브 보고서)를 선택하여 **Archive Report(**아카이브 보고서**)** 확인란을 선택합니다.

참고 도메인 기반 총괄 요약 보고서는 아카이빙할 수 없습니다.

- 보고서를 이메일로 보내려면 **Email now to recipients(**지금 수신자에게 이메일 보내기**)** 확인란을 선택합니다.
- 텍스트 필드에 수신자 이메일 주소를 입력합니다.

단계 **9** **Deliver This Report(**이 보고서 전달**)**를 클릭하여 보고서를 생성합니다.

Archived Web Reports(보관된 웹 보고서) 페이지

- 예약 및 온디맨드 웹 보고서 정보, 239 페이지
- 온디맨드 웹 보고서 생성 , 243 페이지
- 아카이브 웹 보고서 보기 및 관리, 244 페이지

아카이브 웹 보고서 보기 및 관리

이 섹션의 내용을 참조하여 예약 보고서로 생성되는 보고서를 다룹니다.

단계 **1** **Web(**웹**) > Reporting(**보고**) > Archived Reports(**아카이브 보고서**)**로 이동합니다.

단계 **2** 보고서를 보려면 Report Title(보고서 제목) 열에서 보고서 이름을 클릭합니다. Show(표시) 드롭다운 메뉴는 **Archived Reports(**아카이브 보고서**)** 페이지에 나열된 보고서의 유형을 필터링합니다.

단계 **3** 이 목록이 길 때 특정 보고서를 찾으려면 **Show(표시)** 메뉴에서 보고서 유형을 선택하여 필터링하거나 열 제목을 클릭하여 정렬합니다.

다음에 수행할 작업

관련 주제

- 예약 웹 보고서 저장 , 240 페이지
- 예약 웹 보고서 추가, 240 페이지
- 온디맨드 웹 보고서 생성 , 243 페이지

웹 추적

개별 트랜잭션의 세부사항 또는 관심사가 될 트랜잭션 패턴을 검색하고 보려면 웹 추적 페이지를 사용합니다. 구축에서 사용하는 서비스에 따라 관련 탭에서 검색합니다.

- 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지
- L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지
- SOCKS 프록시에서 처리되는 트랜잭션 검색 , 250 페이지
- 웹 추적 검색 결과 작업 , 256 페이지
- 웹 추적 검색 결과에 대한 트랜잭션 세부사항 보기 , 257 페이지

웹 프록시와 L4 트래픽 모니터의 차이에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 "Web Security Appliance 작동 방식" 섹션을 참조하십시오.

관련 주제

- 웹 추적 및 업데이트 정보 , 258 페이지

웹 프록시 서비스에서 처리한 트랜잭션 검색

Web(웹) > Reporting(보고) > Web Tracking(웹 추적) 페이지의 **Proxy Services(프록시 서비스)** 탭을 사용하여 개별 보안 구성 요소뿐 아니라 사용 정책 적용 구성 요소로부터 집계된 데이터를 추적할 수 있습니다. 이 데이터는 L4 Traffic Monitoring 데이터 또는 SOCKS 프록시에서 처리하는 트랜잭션을 포함하지 않습니다.

다음 역할을 지원하는 데 이를 사용할 수도 있습니다.

- **HR** 또는 법적 관리자**.** 특정 기간에 직원에 대한 조사 보고서를 실행합니다.

예를 들어 Proxy Services(프록시 서비스) 탭을 사용하여 어떤 사용자가 액세스하고 있는 특정 URL, 사용자가 그 URL을 방문한 시간, 허용되는 URL인지 여부 등의 정보를 검색할 수 있습니다.

- 네트워크 보안 관리자**.** 회사 네트워크가 직원의 스마트폰에 의해 악성코드 위협에 노출되고 있는지 여부를 조사합니다.

특정 기간에 기록된 트랜잭션(차단된, 모니터링된, 경고받은, 완료된 트랜잭션 포함)에 대한 검색 결과를 볼 수 있습니다. URL 범주, 악성코드 위협, 애플리케이션과 같은 여러 기준을 사용하여 데이터 결과를 필터링할 수도 있습니다.

참고 웹 프록시는 "OTHER-NONE"이 아닌 ACL 결정 태그를 포함한 트랜잭션에 대해서만 보고합니다.

웹 추적 사용의 예는 예 1: 사용자 조사 , 567 페이지를 참조하십시오.

프록시 서비스 탭을 다른 웹 보고 페이지와 함께 사용할 수 있는 방법의 예를 보려면 URL 범주와 다른 보고 페이지 연계 사용, 193 페이지를 참조하십시오.

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > Web Tracking(웹 추적)**을 선택합니다.

단계 **2** **Proxy Services(프록시 서비스)** 탭을 클릭합니다.

단계 **3** 모든 검색 및 필터링 옵션을 보려면 **Advanced(고급)**를 클릭합니다.

단계 **4** 검색 기준을 입력합니다.

표 ***70: Proxy Services(프록시 서비스)*** 탭의 웹 추적 검색 조건

옵션	설명
기본 검색 조건	
시간 범위	보고할 시간 범위를 선택합니다. Security Management Appliance에서 사용 가능한 시간 범위에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
User/Client IPv4 or IPv6(사용자/클라이언트 IPv4 또는 IPv6)	선택 사항으로, 보고서에 나타나는 인증 사용자 이름 또는 추적하려는 클라이언트 IP 주소를 입력합니다. 172.16.0.0/16과 같이 CIDR 형식의 IP 범위를 입력할 수도 있습니다. 이 필드를 비워 두면 모든 사용자에 대한 검색 결과를 반환합니다.
웹사이트	선택 사항으로, 추적하려는 웹 사이트를 입력합니다. 이 필드를 비워 두면 모든 웹 사이트에 대한 검색 결과를 반환합니다.
트랜잭션 유형	추적하려는 트랜잭션의 유형을 선택합니다. 모든 트랜잭션, 완료된 트랜잭션, 차단된 트랜잭션, 모니터링된 트랜잭션, 경고받은 트랜잭션 중에서 선택합니다.

옵션	설명
고급 검색 조건 URL 범주	URL 범주로 필터링하려면 **Filter by URL Category(URL** 범주 기준 필터링**)**를 선택하고 필터링 기준이 될 맞춤 또는 사전 정의 URL 범주의 첫 문자를 입력합니다. 나타나는 목록에서 범주를 선택합니다. . URL 범주의 집합이 업데이트된 경우 일부 범주는 “Deprecated(사용 중단)” 레이블이 지정될 수 있습니다. Deprecated(사용되지 않음) 범주는 에서 새 트랜잭션에 더 이상 사용되지 않습니다. 그러나 범주가 활성 상태인 동안 발생한 최신 트랜잭션은 여전히 검색할 수 있습니다. URL 범주 집합 업데이트에 대한 자세한 내용은 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오. 드롭다운 목록에 표시된 엔진 이름과 상관없이 범주 이름과 매치하는 모든 최신 트랜잭션이 포함됩니다.
애플리케이션	애플리케이션으로 필터링하려면 **Filter by Application(**애플리케이션 기준 필터링**)**을 선택하고 필터링 기준이 될 애플리케이션을 선택합니다. 애플리케이션 유형으로 필터링하려면 **Filter by Application Type(**애플리케이션 유형 기준 필터링**)**을 선택하고 필터링 기준이 될 애플리케이션 유형을 선택합니다.
정책	정책 그룹을 기준으로 필터링하려면 **Filter by Policy(**정책 기준 필터링**)**를 선택하고 필터링할 정책 그룹 이름을 입력합니다. Web Security Appliance에서 정책을 선언했는지 확인합니다.
악성코드 위협	특정 악성코드 위협으로 필터링하려면 **Filter by Malware Threat(**악성코드 위협 기준 필터링**)**를 선택하고 필터링 기준이 될 악성코드 위협 이름을 입력합니다. 악성코드 범주로 필터링하려면 **Filter by Malware Category(**악성코드 범주 기준 필터링**)**를 선택하고 필터링 기준이 될 악성코드 범주를 선택합니다. 자세한 내용은 악성코드 카테고리 설명, 197 페이지를 참조하십시오.
WBRS	WBRS 섹션에서 WBRS(Web-Based Reputation Score) 및 특정 웹 평판 위협으로 필터링할 수 있습니다. • 웹 평판 점수별로 필터링하려면 **Score Range(**점수 범위**)**를 선택하고 필터링 기준이 될 상위 및 하위 값을 선택합니다. 또는 **No Score(**점수 없음**)**를 선택하여 점수가 없는 웹 사이트를 필터링할 수 있습니다. • 웹 평판 위협으로 필터링하려면 **Filter by Reputation Threat(**평판 위협 기준 필터링**)**를 선택하고 필터링 기준이 될 웹 평판 위협을 입력합니다. WBRS 점수에 대한 자세한 내용은 IronPort AsyncOS for Web 사용 설명서를 참조하십시오.
AnyConnect Secure Mobility	원격 또는 로컬 액세스로 필터링하려면 **Filter by User Location(**사용자 위치 기준 필터링**)**을 선택하고 액세스 유형을 선택합니다. 모든 액세스 유형을 포함하려면 **Disable Filter(**필터 비활성화**)**를 선택합니다. 이전 릴리스에서는 이 옵션의 레이블이 Mobile User Security였습니다.

옵션	설명
웹 어플라이언스	특정 웹 어플라이언스로 필터링하려면 **Filter by Web Appliance(**웹 어플라이언스 기준 필터링**)** 옆의 라디오 버튼을 클릭하고 텍스트 필드에 웹 어플라이언스 이름을 입력합니다. **Disable Filter(**필터 비활성화**)**를 선택하면 Web Security Appliance associated with the Security Management Appliance와 연결된 모든 Web Security Appliance가 검색에 포함됩니다.
User Request(사용자 요청)	사용자가 실제로 시작한 트랜잭션으로 필터링하려면 **Filter by Web User-Requested Transactions(**웹 사용자 요청 트랜잭션 기준 필터링**)**를 선택합니다. 참고**:** 이 필터를 활성화할 경우 검색 결과는 “best guess(최선의 추정)” 트랜잭션을 포함합니다.

단계 **5** **Search(**검색**)**를 클릭합니다.

다음에 수행할 작업

관련 주제

- 추가 웹 추적 검색 결과 표시 , 256 페이지
- 웹 추적 검색 결과 이해 , 257 페이지
- 웹 추적 검색 결과에 대한 트랜잭션 세부사항 보기 , 257 페이지
- 웹 추적 및 Advanced Malware Protection 기능 정보 , 257 페이지

악성코드 카테고리 설명

Web Security Appliance는 다음의 악성코드 유형을 차단할 수 있습니다.

악성코드 유형	설명
애드웨어	사용자를 판매할 제품으로 연결하는 모든 소프트웨어 실행 파일 및 플러그인을 포함합니다. 일부 애드웨어 애플리케이션은 별도의 프로세스가 동시에 실행되어 서로 모니터링하면서 영구적인 수정을 보장합니다. 시스템이 시작할 때마다 자동으로 실행되게 하는 변형도 있습니다. 보안 설정을 변경하여 사용자가 브라우저 검색 옵션, 바탕화면, 기타 시스템 설정을 변경하지 못하게 하는 프로그램도 있습니다.
브라우저 헬퍼 개체	브라우저 플러그인이며 광고 서비스 또는 사용자 설정 하이재킹과 관련된 다양한 기능을 수행할 수 있습니다.
상업용 시스템 모니터	상업용 시스템 모니터는 법적인 수단을 통해 적법한 라이센스로 확보할 수 있는 시스템 모니터 특성이 포함된 소프트웨어 부분입니다.
다이얼러	사용자의 모뎀 또는 기타 인터넷 액세스 유형을 이용하여 어떤 전화선 또는 사이트에 연결함으로써 완전한 사전 고지에 의한 사용자 동의 없이 장거리 통화 요금이 부과되게 하는 프로그램입니다.

악성코드 유형	설명
일반 스파이웨어	스파이웨어는 컴퓨터에 설치되는 일종의 악성코드이며, 사용자가 모르는 사이에 사용자에 대한 작은 정보 조각을 수집합니다.
하이잭커	시스템 설정을 수정하거나 사용자가 원치 않는 시스템 변경을 수행하는 수법으로 완전한 사전 고지에 의한 사용자 동의 없이 어떤 웹 사이트로 연결하거나 프로그램을 실행하기도 합니다.
기타 악성코드	이 카테고리는 정의된 다른 카테고리 중 하나에 정확하게 맞지 않는 기타 모든 악성코드와 의심스러운 동작을 포착하는 데 사용됩니다.
보안 침해 휴리스틱	이 범주는 다른 악성코드 차단 엔진과 관계없이 Adaptive Scanning에서 찾아낸 악성코드입니다.
피싱 URL	피싱 URL은 브라우저 주소 창에 표시됩니다. 도메인 이름을 사용하고 합법적 도메인을 모방하는 경우도 있습니다. 온라인 신원 도용 형태 중 하나로서 사회공학 및 기술적 속임수를 모두 구사하면서 개인 신원 데이터 및 금융 계정 자격 증명을 훔칩니다.
PUA	Potentially Unwanted Application. PUA는 악성이 아니지만 원치 않는 것으로 간주할 수 있는 애플리케이션입니다.
시스템 모니터	다음 작업 중 하나를 수행하는 모든 소프트웨어를 포괄합니다. 명시적으로 또는 은밀하게 시스템 프로세스 또는 사용자 작업을 기록합니다. 나중에 이러한 레코드를 검색 및 검토할 수 있도록 합니다.
트로이 목마 다운로더	설치되면 원격 호스트/사이트에 접속하고 원격 호스트로부터 패키지 또는 연관 프로그램을 설치하는 트로이 목마입니다. 이러한 설치는 대개 사용자 모르게 이루어집니다. 또한 트로이 목마 다운로더의 페이로드는 설치마다 달라질 수 있습니다. 원격 호스트/사이트로부터 다운로드 명령을 받기 때문입니다.
트로이 목마	트로이 목마는 무해한 애플리케이션으로 위장한 파괴적인 프로그램입니다. 바이러스와 달리 트로이 목마는 자체적으로 복제하지 않습니다.
트로이 피셔	감염된 컴퓨터에 상주하면서 특정 웹 페이지에 방문할 때까지 기다리거나 감염된 시스템을 검사하여 은행 사이트, 옥션 사이트, 온라인 결제 사이트용 사용자 이름 및 암호를 찾아낼 수 있습니다.
바이러스	사용자 모르게 컴퓨터에 로드되어 사용자의 의사와 상관없이 실행되는 프로그램 또는 코드입니다.
웜	컴퓨터 네트워크를 통해 자가 복제하는 프로그램 또는 알고리즘이며 대개 악성 활동을 수행합니다.

L4 트래픽 모니터에서 처리되는 트랜잭션 검색

Web(웹) > Reporting(보고) > Web Tracking(웹 추적) 페이지의 L4 Traffic Monitor 탭은 악성코드 사이트 및 포트와의 연결에 대한 세부 정보를 제공합니다. 다음 정보 유형으로 악성코드 사이트와의 연결을 검색할 수 있습니다.

- 시간 범위
- 트랜잭션을 시작한 시스템의 IP 주소(IPv4 또는 IPv6)
- 목적지 웹 사이트의 도메인 또는 IP 주소(IPv4 또는 IPv6)
- 포트
- 사내의 어떤 컴퓨터와 연결된 IP 주소
- 연결 유형
- 연결을 처리한 Web Security Appliance

처음 1000개의 일치하는 검색 결과가 표시됩니다.

트랜잭션을 처리한 문제의 사이트 또는 Web Security Appliance에서 호스트 이름을 보려면 Destination IP Address(대상 IP 주소) 열 머리글에서 Display Details(세부사항 표시) 링크를 클릭합니다.

이 정보를 사용하는 방법에 대한 자세한 내용은 L4 Traffic Monitor 보고서 , 206 페이지 섹션을 참조하십시오.

SOCKS 프록시에서 처리되는 트랜잭션 검색

다양한 조건, 이를테면 차단된 또는 완료된 트랜잭션, 트랜잭션을 시작한 클라이언트 시스템의 IP 주소, 목적지 도메인, IP 주소, 포트를 충족하는 트랜잭션을 검색할 수 있습니다. 맞춤 URL 범주, 매치하는 정책, 사용자 위치(로컬 또는 원격)로 결과를 필터링할 수도 있습니다. IPv4 및 IPv6 주소가 지원됩니다.

단계 **1** **Web(웹) > Reporting(보고) > Web Tracking(웹 추적)**을 선택합니다.

단계 **2** **SOCKS Proxy(SOCKS 프록시)** 탭을 클릭합니다.

단계 **3** 결과를 필터링하려면 **Advanced(고급)**를 클릭합니다.

단계 **4** 검색 조건을 입력합니다.

단계 **5** **Search(검색)**를 클릭합니다.

다음에 수행할 작업

관련 주제

SOCKS 프록시 보고서 , 208 페이지

새 웹 인터페이스의 웹 추적

개별 트랜잭션의 세부 정보 또는 관심사가 될 트랜잭션 패턴을 검색하고 보려면 **Web Tracking Search(**웹 추적 검색**)** 페이지를 사용할 수 있습니다. 구축에서 사용하는 서비스에 따라 관련 탭에서 검색합니다.

- 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 251 페이지
- L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지
- SOCKS 프록시에서 처리되는 트랜잭션 검색 , 256 페이지
- 웹 추적 검색 결과 작업 , 256 페이지
- 웹 추적 검색 결과에 대한 트랜잭션 세부사항 보기 , 257 페이지

웹 프록시와 Layer4 트래픽 모니터의 차이에 대한 자세한 내용은 *AsyncOS for Cisco Web Security Appliances* 사용 설명서의 "Web Security Appliance 작동 방식" 섹션을 참조하십시오.

웹 프록시 서비스에서 처리한 트랜잭션 검색

Web Tracking Search(웹 추적 검색**)** 페이지의 **Proxy Services(**프록시 서비스**)** 탭을 사용하여 개별 보안 구성 요소뿐 아니라 사용 정책 적용 구성 요소로부터 집계된 데이터를 추적할 수 있습니다. 이 데이터는 레이어 4 트래픽 모니터링 데이터 또는 SOCKS 프록시에서 처리하는 트랜잭션을 포함하지 않습니다.

다음 역할을 지원하는 데 이를 사용할 수도 있습니다.

- **HR** 또는 법적 관리자**.** 특정 기간에 직원에 대한 조사 보고서를 실행합니다.

  예를 들어 Proxy Services(프록시 서비스) 탭을 사용하여 어떤 사용자가 액세스하고 있는 특정 URL, 사용자가 그 URL을 방문한 시간, 허용되는 URL인지 여부 등의 정보를 검색할 수 있습니다.

- 네트워크 보안 관리자**.** 회사 네트워크가 직원의 스마트폰에 의해 악성코드 위협에 노출되고 있는지 여부를 조사합니다.

특정 기간에 기록된 트랜잭션(차단된, 모니터링된, 경고받은, 완료된 트랜잭션 포함)에 대한 검색 결과를 볼 수 있습니다. URL 범주, 악성코드 위협, 애플리케이션과 같은 여러 기준을 사용하여 데이터 결과를 필터링할 수도 있습니다.

참고 웹 프록시는 "OTHER-NONE"이 아닌 ACL 결정 태그를 포함한 트랜잭션에 대해서만 보고합니다.

웹 추적 사용의 예는 예 1: 사용자 조사 , 567 페이지를 참조하십시오.

프록시 서비스 탭을 다른 웹 보고 페이지와 함께 사용할 수 있는 방법의 예를 보려면 URL 범주와 다른 보고 페이지 연계 사용, 193 페이지를 참조하십시오.

단계 **1** Security Management Appliance의 드롭다운 목록에서 **Web(웹)**을 선택합니다.

단계 **2** **Tracking(추적) > Proxy Services(프록시 서비스)**를 선택합니다.

단계 **3** 모든 검색 및 필터링 옵션을 보려면 **Advanced(고급)**를 클릭합니다.

단계 **4** 검색 기준을 입력합니다.

표 ***71: Proxy Services(프록시 서비스)*** 탭의 웹 추적 검색 조건

옵션	설명
기본 검색 조건	
시간 범위	보고할 시간 범위를 선택합니다. Security Management Appliance에서 사용 가능한 시간 범위에 대한 자세한 내용은 보고서의 시간 범위를 선택 , 36 페이지를 참조하십시오.
User/Client IPv4 or IPv6(사용자/클라이언트 IPv4 또는 IPv6)	선택 사항으로, 보고서에 나타나는 인증 사용자 이름 또는 추적하려는 클라이언트 IP 주소를 입력합니다. 172.16.0.0/16과 같이 CIDR 형식의 IP 범위를 입력할 수도 있습니다. 이 필드를 비워 두면 모든 사용자에 대한 검색 결과를 반환합니다.
웹사이트	선택 사항으로, 추적하려는 웹 사이트를 입력합니다. 이 필드를 비워 두면 모든 웹 사이트에 대한 검색 결과를 반환합니다.
트랜잭션 유형	추적하려는 트랜잭션의 유형을 선택합니다. 모든 트랜잭션, 완료된 트랜잭션, 차단된 트랜잭션, 모니터링된 트랜잭션, 경고받은 트랜잭션 중에서 선택합니다.
고급 검색 조건	
URL 범주	URL 범주로 필터링하려면 **Filter by URL Category(URL** 범주 기준 필터링**)**를 선택하고 필터링 기준이 될 맞춤 또는 사전 정의 URL 범주의 첫 문자를 입력합니다. 나타나는 목록에서 범주를 선택합니다. . URL 범주의 집합이 업데이트된 경우 일부 범주는 “Deprecated(사용 중단)” 레이블이 지정될 수 있습니다. Deprecated(사용되지 않음) 범주는 에서 새 트랜잭션에 더 이상 사용되지 않습니다. 그러나 범주가 활성 상태인 동안 발생한 최신 트랜잭션은 여전히 검색할 수 있습니다. URL 범주 집합 업데이트에 대한 자세한 내용은 URL 카테고리 집합 업데이트 및 보고 , 193 페이지를 참조하십시오. 드롭다운 목록에 표시된 엔진 이름과 상관없이 범주 이름과 매치하는 모든 최신 트랜잭션이 포함됩니다.
애플리케이션	애플리케이션으로 필터링하려면 **Filter by Application(**애플리케이션 기준 필터링**)**을 선택하고 필터링 기준이 될 애플리케이션을 선택합니다. 애플리케이션 유형으로 필터링하려면 **Filter by Application Type(**애플리케이션 유형 기준 필터링**)**을 선택하고 필터링 기준이 될 애플리케이션 유형을 선택합니다.

옵션	설명
정책	정책 그룹을 기준으로 필터링하려면 **Filter by Policy(**정책 기준 필터링**)**를 선택하고 필터링할 정책 그룹 이름을 입력합니다. Web Security Appliance에서 정책을 선언했는지 확인합니다.
악성코드 위협	특정 악성코드 위협으로 필터링하려면 **Filter by Malware Threat(**악성코드 위협 기준 필터링**)**를 선택하고 필터링 기준이 될 악성코드 위협 이름을 입력합니다. 악성코드 범주로 필터링하려면 **Filter by Malware Category(**악성코드 범주 기준 필터링**)**를 선택하고 필터링 기준이 될 악성코드 범주를 선택합니다. 자세한 내용은 악성코드 카테고리 설명, 197 페이지를 참조하십시오.
WBRS	WBRS 섹션에서 WBRS(Web-Based Reputation Score) 및 특정 웹 평판 위협으로 필터링할 수 있습니다. • 웹 평판 점수별로 필터링하려면 **Score Range(**점수 범위**)**를 선택하고 필터링 기준이 될 상위 및 하위 값을 선택합니다. 또는 **No Score(**점수 없음**)**를 선택하여 점수가 없는 웹 사이트를 필터링할 수 있습니다. • 웹 평판 위협으로 필터링하려면 **Filter by Reputation Threat(**평판 위협 기준 필터링**)**를 선택하고 필터링 기준이 될 웹 평판 위협을 입력합니다. WBRS 점수에 대한 자세한 내용은 IronPort AsyncOS for Web 사용 설명서를 참조하십시오.
AnyConnect Secure Mobility	원격 또는 로컬 액세스로 필터링하려면 **Filter by User Location(**사용자 위치 기준 필터링**)**을 선택하고 액세스 유형을 선택합니다. 모든 액세스 유형을 포함하려면 **Disable Filter(**필터 비활성화**)**를 선택합니다. 이전 릴리스에서는 이 옵션의 레이블이 Mobile User Security였습니다.
웹 어플라이언스	특정 웹 어플라이언스로 필터링하려면 **Filter by Web Appliance(**웹 어플라이언스 기준 필터링**)** 옆의 라디오 버튼을 클릭하고 텍스트 필드에 웹 어플라이언스 이름을 입력합니다. **Disable Filter(**필터 비활성화**)**를 선택하면 Web Security Appliance associated with the Security Management Appliance와 연결된 모든 Web Security Appliance가 검색에 포함됩니다.
User Request(사용자 요청)	사용자가 실제로 시작한 트랜잭션으로 필터링하려면 **Filter by Web User-Requested Transactions(**웹 사용자 요청 트랜잭션 기준 필터링**)**를 선택합니다. 참고**:** 이 필터를 활성화할 경우 검색 결과는 “best guess(최선의 추정)” 트랜잭션을 포함합니다.

악성코드 카테고리 설명

Web Security Appliance는 다음의 악성코드 유형을 차단할 수 있습니다.

악성코드 유형	설명
애드웨어	사용자를 판매할 제품으로 연결하는 모든 소프트웨어 실행 파일 및 플러그인을 포함합니다. 일부 애드웨어 애플리케이션은 별도의 프로세스가 동시에 실행되어 서로 모니터링하면서 영구적인 수정을 보장합니다. 시스템이 시작할 때마다 자동으로 실행되게 하는 변형도 있습니다. 보안 설정을 변경하여 사용자가 브라우저 검색 옵션, 바탕화면, 기타 시스템 설정을 변경하지 못하게 하는 프로그램도 있습니다.
브라우저 헬퍼 개체	브라우저 플러그인이며 광고 서비스 또는 사용자 설정 하이재킹과 관련된 다양한 기능을 수행할 수 있습니다.
상업용 시스템 모니터	상업용 시스템 모니터는 법적인 수단을 통해 적법한 라이센스로 확보할 수 있는 시스템 모니터 특성이 포함된 소프트웨어 부분입니다.
다이얼러	사용자의 모뎀 또는 기타 인터넷 액세스 유형을 이용하여 어떤 전화선 또는 사이트에 연결함으로써 완전한 사전 고지에 의한 사용자 동의 없이 장거리 통화 요금이 부과되게 하는 프로그램입니다.
일반 스파이웨어	스파이웨어는 컴퓨터에 설치되는 일종의 악성코드이며, 사용자가 모르는 사이에 사용자에 대한 작은 정보 조각을 수집합니다.
하이잭커	시스템 설정을 수정하거나 사용자가 원치 않는 시스템 변경을 수행하는 수법으로 완전한 사전 고지에 의한 사용자 동의 없이 어떤 웹 사이트로 연결하거나 프로그램을 실행하기도 합니다.
기타 악성코드	이 카테고리는 정의된 다른 카테고리 중 하나에 정확하게 맞지 않는 기타 모든 악성코드와 의심스러운 동작을 포착하는 데 사용됩니다.
보안 침해 휴리스틱	이 범주는 다른 악성코드 차단 엔진과 관계없이 Adaptive Scanning에서 찾아낸 악성코드입니다.
피싱 URL	피싱 URL은 브라우저 주소 창에 표시됩니다. 도메인 이름을 사용하고 합법적 도메인을 모방하는 경우도 있습니다. 온라인 신원 도용 형태 중 하나로서 사회공학 및 기술적 속임수를 모두 구사하면서 개인 신원 데이터 및 금융 계정 자격 증명을 훔칩니다.
PUA	Potentially Unwanted Application. PUA는 악성이 아니지만 원치 않는 것으로 간주할 수 있는 애플리케이션입니다.
시스템 모니터	다음 작업 중 하나를 수행하는 모든 소프트웨어를 포괄합니다. 명시적으로 또는 은밀하게 시스템 프로세스 또는 사용자 작업을 기록합니다. 나중에 이러한 레코드를 검색 및 검토할 수 있도록 합니다.

악성코드 유형	설명
트로이 목마 다운로더	설치되면 원격 호스트/사이트에 접속하고 원격 호스트로부터 패키지 또는 연관 프로그램을 설치하는 트로이 목마입니다. 이러한 설치는 대개 사용자 모르게 이루어집니다. 또한 트로이 목마 다운로더의 페이로드는 설치마다 달라질 수 있습니다. 원격 호스트/사이트로부터 다운로드 명령을 받기 때문입니다.
트로이 목마	트로이 목마는 무해한 애플리케이션으로 위장한 파괴적인 프로그램입니다. 바이러스와 달리 트로이 목마는 자체적으로 복제하지 않습니다.
트로이 피셔	감염된 컴퓨터에 상주하면서 특정 웹 페이지에 방문할 때까지 기다리거나 감염된 시스템을 검사하여 은행 사이트, 옥션 사이트, 온라인 결제 사이트용 사용자 이름 및 암호를 찾아낼 수 있습니다.
바이러스	사용자 모르게 컴퓨터에 로드되어 사용자의 의사와 상관없이 실행되는 프로그램 또는 코드입니다.
웜	컴퓨터 네트워크를 통해 자가 복제하는 프로그램 또는 알고리즘이며 대개 악성 활동을 수행합니다.

Layer 4 트래픽 모니터에서 처리되는 트랜잭션 검색

Web Tracking Search(웹 추적 검색**)** 페이지의 Layer 4 Traffic Monitor(Layer 4 트래픽 모니터) 탭에서는 악성코드 사이트 및 포트에 대한 연결과 관련된 상세정보를 제공합니다. 다음 정보 유형으로 악성코드 사이트와의 연결을 검색할 수 있습니다.

- 시간 범위
- 트랜잭션을 시작한 시스템의 IP 주소(IPv4 또는 IPv6)
- 목적지 웹 사이트의 도메인 또는 IP 주소(IPv4 또는 IPv6)
- 포트
- 사내의 어떤 컴퓨터와 연결된 IP 주소
- 연결 유형
- 연결을 처리한 Web Security Appliance

트랜잭션을 처리한 문제의 사이트 또는 Web Security Appliance에서 호스트 이름을 보려면 Destination IP Address(대상 IP 주소) 열 머리글에서 Display Details(세부사항 표시) 링크를 클릭합니다.

이 정보를 사용하는 방법에 대한 자세한 내용은 Layer 4 Traffic Monitor(레이어 4 트래픽 모니터) 페이지, 219 페이지 섹션을 참조하십시오.

SOCKS 프록시에서 처리되는 트랜잭션 검색

다양한 조건, 이를테면 차단된 또는 완료된 트랜잭션, 트랜잭션을 시작한 클라이언트 시스템의 IP 주소, 목적지 도메인, IP 주소, 포트를 충족하는 트랜잭션을 검색할 수 있습니다. 맞춤 URL 범주, 매치하는 정책, 사용자 위치(로컬 또는 원격)로 결과를 필터링할 수도 있습니다. IPv4 및 IPv6 주소가 지원됩니다.

단계 **1** Security Management Appliance의 드롭다운 목록에서 **Web(웹)**을 선택합니다.

단계 **2** **Tracking(추적) > SOCKS Proxy(SOCKS 프록시)**를 선택합니다.

단계 **3** 모든 검색 및 필터링 옵션을 보려면 **Advanced(고급)**를 클릭합니다.

단계 **4** 검색 조건을 입력합니다.

단계 **5** **Search(검색)**를 클릭합니다.

다음에 수행할 작업

관련 주제

SOCKS 프록시 보고서 , 208 페이지

웹 추적 검색 결과 작업

추가 웹 추적 검색 결과 표시

단계 **1** 반환된 결과의 모든 페이지를 검토해야 합니다.

단계 **2** 표시된 현재 번호가 아닌 추가 결과를 페이지별로 표시하려면 **Items Displayed(표시 항목)** 메뉴에서 옵션을 선택합니다.

단계 **3** Items Displayed(표시 항목) 메뉴에서 지정된 최대 트랜잭션 수보다 많은 트랜잭션이 조건과 매치할 경우 **Printable Download(인쇄용 다운로드)** 링크를 클릭하여 매치하는 모든 트랜잭션을 포함한 CSV 파일을 만들어 전체 결과를 볼 수 있습니다.

이 CSV 파일은 원시 데이터의 전체 집합을 포함하는데, 관련 트랜잭션의 세부사항은 제외합니다.

웹 추적 검색 결과 이해

기본적으로 결과의 정렬 기준은 타임스탬프입니다. 최근 결과가 맨 위에 옵니다.

검색 결과는 다음 항목을 포함합니다.

- URL을 액세스한 시간.
- 사용자가 시작한 트랜잭션에서 파생된 관련 트랜잭션의 수 - 로드한 이미지, 실행한 자바스크립트, 액세스한 보조 사이트 등 관련 트랜잭션의 수는 열 제목에서 Display All Details(모든 세부사항 표시) 링크의 아래에 각 행으로 나타납니다.
- 배치(트랜잭션의 결과. 가능하다면 트랜잭션이 차단되었거나 모니터링되었거나 경고받은 이유 표시)

웹 추적 검색 결과에 대한 트랜잭션 세부사항 보기

보려는 내용	수행해야 할 작업
목록에서 잘린 URL의 전체 URL	어떤 호스트 Web Security Appliance가 트랜잭션을 처리했는지 알아본 다음 해당 어플라이언스의 Accesslog를 확인합니다.
개별 트랜잭션에 대한 세부사항	웹 사이트 열에서 URL을 클릭합니다.
모든 트랜잭션의 세부사항	웹 사이트 열 제목에서 **Display All Details...(**모든 세부사항 표시**...)** 링크를 클릭합니다.
최대 500개의 관련 트랜잭션 목록	검색 결과 목록의 관련 트랜잭션의 수는 열 제목에서 Display Details(세부사항 표시) 링크의 아래에 괄호로 묶여 나타납니다. 트랜잭션의 Details(세부사항 보기)에서 **Related Transactions(**관련 트랜잭션**)** 링크를 클릭합니다.

웹 추적 및 **Advanced Malware Protection** 기능 정보

웹 추적에서 파일 위협 정보를 검색할 때 다음 사항에 유의하십시오.

- 파일 평판 서비스에 의해 발견된 악성 파일을 검색하려면 웹 추적의 Advanced(고급) 섹션 Malware Threat(악성코드 위협) 영역 **Filter by Malware Category(**악성코드 범주 기준 필터링**)** 옵션에서 **Known Malicious and High-Risk Files(**알려진 악성 및 고위험 파일**)**를 선택합니다.
- 웹 추적은 트랜잭션이 처리된 시점에 반환된 파일 평판 처리 및 원래의 파일 평판 판정의 정보만 포함합니다. 예를 들어, 파일이 처음에는 클린으로 확인되었으나 판정 업데이트에서는 파일이 악성으로 확인된 경우 클릭 판정만 추적 결과에 표시됩니다.

  검색 결과의 "차단 - AMP"는 파일의 평판 판정으로 인해 트랙잭션이 차단되었음을 의미합니다.

  추적 세부사항에서 "AMP 위협 점수"는 파일에 대한 정상 판정을 결정할 수 없는 경우 클라우드 평판 서비스가 제공하는 최상의 점수입니다. 이 경우 점수는 1~100입니다. (AMP 판정이 반환되

거나 점수가 0인 경우 AMP 위협 점수를 무시하십시오.) 어플라이언스가 이 점수를 임계값 점수(Security Services(보안 서비스) > Anti-Malware and Reputation(악성코드 차단 및 평판) 페이지에서 구성됨)와 비교하여 수행할 작업을 결정합니다. 기본적으로 점수가 60~100인 파일은 악성으로 간주됩니다. Cisco에서는 기본 임계값 점수 변경을 권장하지 않습니다. WBRS 점수는 파일을 다운로드한 사이트의 평판이므로 이 점수는 파일 평판과 관련이 없습니다.

- 판정 업데이트는 AMP 판정 업데이트 보고서에서만 사용할 수 있습니다. 웹 추적에 있는 원래 트랜잭션 세부사항은 판정 변동 시 업데이트되지 않습니다. 특정 파일이 있는 트랜잭션을 확인하려면 판정 업데이트 보고서에서 SHA-256을 클릭합니다.
- 분석 결과 및 분석을 위해 파일이 전송되었는지 여부를 포함한 파일 분석에 대한 정보는 파일 분석 보고서에서만 사용할 수 있습니다.

  분석한 파일에 대한 추가 정보는 클라우드에서 사용할 수 있습니다. 파일에 대한 사용 가능한 파일 분석 정보를 보려면 **Reporting(보고) > File Analysis(파일 분석)**를 선택하고 SHA-256을 입력하여 해당 파일을 검색합니다. 또는 웹 추적 세부사항에서 SHA-256 링크를 클릭합니다. 파일 분석 서비스가 임의의 소스에서 파일을 분석한 경우 세부사항을 볼 수 있습니다. 결과는 분석된 파일에 대해서만 표시됩니다.

  어플라이언스에서 분석을 위해 보내진 파일의 또 다른 인스턴스를 처리한 경우 이 인스턴스는 웹 추적 검색 결과에 나타납니다.

관련 주제

- SHA-256 해시로 파일 식별 , 201 페이지

웹 추적 및 업데이트 정보

새로운 웹 추적 기능이 업그레이드 전에 실행된 트랜잭션에는 적용되지 않을 수 있습니다. 해당 트랜잭션에 대해 필요한 데이터가 보존되지 않았을 가능성도 있기 때문입니다. 웹 추적 데이터 및 업그레이드와 관련되어 나타날 수 있는 제한 사항은 해당 릴리스의 릴리스 정보를 참조해 주십시오.

웹 보고 및 추적 트러블슈팅

- 중앙 보고가 제대로 활성화되었으나 작동하지 않음 , 259 페이지
- Advanced Malware Protection 판정 업데이트 보고서 결과가 다름 , 259 페이지
- 파일 분석 보고서 세부사항 보기 문제 , 259 페이지
- 보고 또는 추적 결과에서 예상 데이터가 없음, 260 페이지
- PDF에서 웹 추적 데이터의 일부만 표시 , 260 페이지
- L4 Traffic Monitor 보고서 트러블슈팅 , 261 페이지
- 내보낸 CSV 파일이 웹 인터페이스 데이터와 다름 , 261 페이지

모든 보고서 트러블슈팅 , 45 페이지도 참고하십시오.

중앙 보고가 제대로 활성화되었으나 작동하지 않음

문제

지침대로 중앙 웹 보고를 활성화했으나 작동하지 않습니다.

솔루션

보고에 할당된 디스크 공간이 없을 경우 중앙 웹 보고는 디스크 공간이 할당될 때까지 작동하지 않습니다. 웹 보고 및 추적을 위한 할당량이 현재 사용된 디스크 공간보다 크다면 웹 보고 및 추적 데이터를 잃을 염려가 없습니다. 자세한 내용은 디스크 공간 관리 , 487 페이지를 참조하십시오.

Advanced Malware Protection 판정 업데이트 보고서 결과가 다름

문제

Web Security Appliance 및 Email Security Appliance에서 분석을 위해 동일한 파일을 전송하면 웹 및 이메일에 대한 AMP 판정 업데이트 보고서에 해당 파일에 대한 서로 다른 판정이 표시됩니다.

솔루션

이 상황은 일시적입니다. 모든 판정 업데이트가 다운로드되면 결과가 매치합니다. 이 과정이 완료될 때까지 최대 30분이 걸릴 수 있습니다.

파일 분석 보고서 세부사항 보기 문제

파일 분석 보고서 세부사항이 제공되지 않음

문제

파일 분석 보고서 세부사항을 사용할 수 없습니다.

솔루션

파일 분석 보고서 요구 사항 정보 , 199 페이지를 참조하십시오.

파일 분석 보고서 세부사항 보기 오류

문제

파일 분석 보고서 세부 정보를 보려고 할 때 "No cloud server configuration is available(사용할 수 있는 클라우드 서버 구성이 없습니다.)"이라는 오류가 나타납니다.

솔루션

Management Appliance(관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)**로 이동하여, 파일 분석 기능이 활성화된 Web Security Appliance를 하나 이상 추가합니다.

프라이빗 클라우드 Cisco AMP Threat Grid Appliance에서 파일 분석 보고서 세부사항 보기 오류

문제

파일 분석 보고서 세부사항을 보려고 할 때 API 키, 등록 또는 활성화 오류가 나타납니다.

솔루션

프라이빗 클라우드(온프레미스) Cisco AMP Threat Grid 어플라이언스를 파일 분석에 사용하는 경우 (온프레미스 파일 분석) 파일 분석 계정 활성화 , 200 페이지를 참조하십시오.

Threat Grid 어플라이언스 호스트 이름이 바뀌면 참조된 절차의 프로세스를 반복해야 합니다.

보고 또는 추적 결과에서 예상 데이터가 없음

문제

보고 또는 추적 결과에서 예상했던 데이터가 빠져 있습니다.

솔루션

가능한 원인

- 원하는 시간 범위를 선택했음을 확인합니다.
- 추적 결과에서는 매치하는 모든 결과를 표시해야 합니다. 추가 웹 추적 검색 결과 표시 , 256 페이지를 참조하십시오.
- Web Security Appliance와 Cisco Content Security Management Appliance 간의 데이터 전송이 중단되었거나, 데이터가 삭제되었을 수 있습니다. 데이터 가용성 페이지, 211 페이지를 참조하십시오.
- 업그레이드 때문에 정보를 보고하고 추적하는 방식이 바뀔 경우 업그레이드 전에 일어난 트랜잭션이 제대로 나타나지 않을 수 있습니다. 사용하는 릴리스가 이와 같이 변경되었는지 확인하려면 설명서 , 571 페이지에 제시된 위치에서 릴리즈 노트를 참조하십시오.
- 웹 프록시 서비스 추적 검색 결과에서 누락된 결과에 대해서는 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지를 참조하십시오.
- 사용자 요청 트랜잭션으로 필터링할 때 예상치 않은 결과가 나오면 웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지의 테이블에서 User Request(사용자 요청) 행을 참조하십시오.

PDF에서 웹 추적 데이터의 일부만 표시

문제

PDF에서 웹 추적 페이지에 나타나는 데이터 중 일부만 표시합니다.

솔루션

PDF 및 CSV 파일에 포함되는 데이터와 생략되는 데이터에 대해서는 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지의 테이블에서 웹 추적 정보를 참조하십시오.

L4 Traffic Monitor 보고서 트러블슈팅

웹 프록시가 전달 프록시로 구성되었고 L4 Traffic Monitor가 모든 포트를 모니터링하도록 설정된 경우 프록시 데이터 포트의 IP 주소가 기록되어 보고서에 클라이언트 IP 주소로 표시됩니다. 웹 프록시가 투명 프록시로 구성된 경우 IP 스푸핑을 활성화해야 클라이언트 IP 주소를 제대로 기록하고 표시할 수 있습니다. 그렇게 하려면 IronPort AsyncOS for Web 사용 설명서를 참조하십시오.

관련 주제

- 클라이언트 악성코드 위험 보고서 , 203 페이지
- L4 트래픽 모니터에서 처리되는 트랜잭션 검색 , 250 페이지

내보낸 CSV 파일이 웹 인터페이스 데이터와 다름

문제

매치하는 도메인 데이터를 CSV 파일로 내보냈는데 웹 인터페이스에 표시되는 데이터와 다릅니다.

솔루션

성능상의 이유로 첫 30만 개의 항목만 CSV 파일에 내보냅니다.

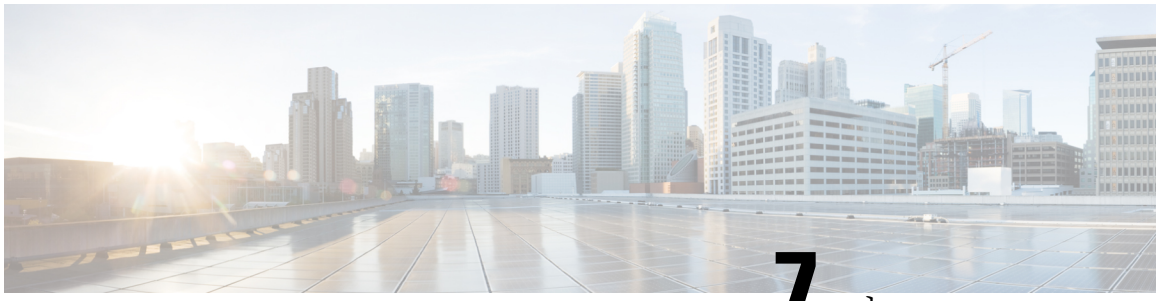
웹 추적 검색 결과 내보내기 문제

문제

여러 대규모 검색 쿼리를 동시에 실행하는 경우 웹 추적 검색 결과에 "Out of Memory(메모리 부족)" 오류가 표시됩니다.

솔루션

하나의 해결 방법으로, 메모리의 힙 크기를 1024MB 이상으로 늘리거나 검색 기준의 시간 범위를 줄일 수 있습니다. 메모리의 힙 크기를 늘리면 메모리 관련 문제가 발생할 수 있습니다.



7 장

메시지 추적

이 장에는 다음 섹션이 포함되어 있습니다.

추적 서비스 개요

Cisco Content Security Management Appliance의 추적 서비스는 Email Security Appliance를 보완합니다. Security Management Appliance에는 Email Security Appliance를 통과하는 메시지의 상태를 이메일 관리자가 추적할 수 있는 단일 장소가 있습니다.

Security Management Appliance에서는 Email Security Appliance가 처리하는 메시지의 상태를 손쉽게 찾을 수 있습니다. 이메일 관리자는 메시지의 정확한 위치를 확인하여 헬프 데스크 문의 사항을 신속하게 해결할 수 있습니다. Security Management Appliance에서 관리자는 특정 메시지가 전달되었는지, 바이러스를 포함한 것으로 발견되었는지, 스팸 격리에 있는지, 아니면 메일 처리 과정에서 다른 곳에 있는지를 확인할 수 있습니다.

Grep 또는 유사 툴을 사용하여 로그를 검색하지 않고도 Security Management Appliance의 유연한 추적 인터페이스를 사용하여 메시지를 찾을 수 있습니다. 다양한 검색 매개변수의 조합을 사용할 수 있습니다.

추적 쿼리는 다음을 포함할 수 있습니다.

- 기간: 지정된 날짜와 시간의 간격에 발송된 메시지를 찾습니다.
- 환경 정보: 매칭할 텍스트 문자열을 입력하여 특정 봉투 발신자 또는 수신자의 메시지를 찾습니다.
- 제목: 제목줄의 텍스트 문자열을 매칭합니다. 경고: 그러한 추적을 금지하는 규정이 있는 환경에서는 이 검색 유형을 사용하지 마십시오.

- 첨부 파일 이름: 첨부 파일 이름에 따라 메시지를 검색할 수 있습니다. 쿼리된 첨부 파일이 하나 이상 포함된 메시지가 검색 결과에 나타납니다.

  성능상의 이유로 첨부 파일 내의 파일 이름(OLE 개체 또는 .ZIP 파일과 같은 아카이브)은 추적되지 않습니다.

  일부 첨부 파일은 추적되지 않을 수 있습니다. 성능상의 이유로, 첨부 파일 이름 검사는 메시지 또는 콘텐츠 필터링, DLP, 면책조항 스탬프 등 다른 검사 운영의 일부로서만 발생합니다. 본문 검사를 통과하고 첨부 파일이 여전히 첨부되어 있는 메시지에 대해서만 첨부 파일 이름을 사용할 수 있습니다. 다음과 같은 여러 경우에 첨부 파일 이름이 나타나지 않습니다.

  - 시스템에서 콘텐츠 필터만 사용하고, 안티스팸 또는 안티바이러스 필터에 의해 메시지가 삭제되거나 첨부 파일이 제거된 경우
  - 메시지 분리 정책에 따라 본문 검사가 발생하기 전에 일부 메시지에서 첨부 파일이 제거된 경우

- 파일 **SHA256**: 메시지 파일의 SHA-256 값으로 메시지 찾기
- **Cisco** 호스트: 특정 Email Security Appliance로 검색 기준을 좁히거나, 모든 관리되는 어플라이언스에서 검색합니다.
- 메시지 **ID** 헤더 및 **Cisco MID**: SMTP “Message-ID:” 헤더 또는 Cisco MID(메시지 ID)를 식별하여 메시지를 찾습니다.
- 발신자 **IP** 주소/도메인/네트워크 소유자: 특정 IP 주소, 도메인 이름 또는 네트워크 소유자가 보낸 메시지를 검색합니다.
- 메시지 이벤트: 지정된 이벤트와 매칭하는 메시지를 찾습니다. 이를테면 바이러스 양성, 스팸 양성 또는 의심스러운 스팸으로 지정된 메시지 및 전달, 하드 반송, 소프트 반송, 바이러스 보안 침해 격리에 보내진 메시지를 찾습니다.
- 거부된 연결: 검색 결과에서 거부된 연결의 특정 IP 주소, 도메인 이름 또는 네트워크 소유자가 보낸 메시지를 검색합니다.

중앙 집중식 메시지 추적 설정

중앙 집중식 메시지 추적을 설정하려면 순서대로 다음 절차를 완료해 주십시오.

- Security Management Appliance에서 중앙 집중식 이메일 추적 활성화, 264 페이지
- ESA의 중앙 메시지 추적 구성 , 265 페이지
- 관리되는 각 Email Security Appliance에 중앙 집중식 메시지 추적 서비스 추가 , 265 페이지

Security Management Appliance에서 중앙 집중식 이메일 추적 활성화

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Email(**이메일**) > Centralized Message Tracking(**중앙 집중식 이메일 추적**)**을 선택합니다.

단계 **3** Message Tracking Service(메시지 추적 서비스) 섹션에서 **Enable(**활성화**)**을 클릭합니다.

단계 **4** 시스템 설정 마법사를 실행한 후 처음 중앙 집중식 이메일 추적을 활성화하는 경우 최종 사용자 라이센스 계약을 읽고 **Accept(**동의**)**를 클릭합니다.

단계 **5** 변경 사항을 **Submit(**제출**)** 및 커밋합니다.

ESA의 중앙 메시지 추적 구성

단계 **1** 메시지 추적이 Email Security Appliance에서 제대로 구성되어 작동하는지 확인합니다.

단계 **2** **Security Services(**보안 서비스**) > Message Tracking(**메시지 추적**)**으로 이동합니다.

단계 **3** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **4** **Centralized Tracking(**중앙 추적**)**을 선택합니다.

단계 **5** **Submit(**제출**)**를 클릭합니다.

단계 **6** 이메일 첨부 파일의 이름을 검색하고 기록하려면:

Email Security Appliance에서 하나 이상의 수신 콘텐츠 필터 또는 기타 본문 검사 기능이 ESA에서 구성 및 활성화되어 있어야 합니다. 콘텐츠 필터 및 본문 검사에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말을 참조하십시오.

단계 **7** 변경 사항을 커밋합니다.

단계 **8** 관리할 각 Email Security Appliance에 대해 반복합니다.

관리되는 각 Email Security Appliance에 중앙 집중식 메시지 추적 서비스 추가

수행하는 단계는 또 다른 중앙 관리 기능을 구성할 때 어플라이언스를 이미 추가했는지 여부에 따라 달라집니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 이 페이지의 목록에 Email Security Appliance를 이미 추가한 경우

a) Email Security Appliance의 이름을 클릭합니다.

b) **Centralized Message Tracking(**중앙 집중식 메시지 추적**)** 서비스를 선택합니다.

단계 **4** Email Security Appliance를 아직 추가하지 않은 경우

a) Add Email Appliance(이메일 어플라이언스 추가)를 클릭합니다.
b) Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 Email Security Appliance의 Management 인터페이스에 대한 IP 주소를 입력합니다.

참고 IP Address(IP 주소) 텍스트 필드에 DNS 이름을 입력하는 경우 **Submit(**제출**)**을 클릭하면 즉시 IP 주소로 해석됩니다.

c) Centralized Message Tracking(중앙 집중식 메시지 추적) 서비스가 미리 선택되어 있습니다.
d) **Establish Connection(**연결 설정**)**을 클릭합니다.
e) 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다.

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

f) 페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.
g) **Test Connection(**테스트 연결**)**을 클릭합니다.
h) 테이블 위의 테스트 결과를 읽습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** Centralized Message Tracking(중앙 집중식 메시지 추적)을 활성화할 각 Security Management Appliance에 대해 이 절차를 반복합니다.

단계 **7** 변경사항을 커밋합니다.

민감 정보에 대한 액세스 관리

관리 작업을 타인에게 분배하는 경우 DLP(Data Loss Prevention) 정책을 위반하는 이메일 메시지에 나타날 수 있는 민감 정보에 대한 액세스를 제한하고 싶다면 메시지 추적 시 중요 정보의 액세스 제어 , 426 페이지를 참조하십시오.

메시지 추적 데이터 가용성 확인

메시지 추적 데이터에 포함되는 날짜 범위를 결정하고, 해당 데이터에서 누락된 간격을 식별할 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email(**이메일**) > Message Tracking(**메시지 추적**) > Message Tracking Data Availability(**메시지 추적 데이터 가용성**)**를 선택합니다.

이메일 메시지 검색

새로운 웹 인터페이스에서 이메일 메시지 검색

어플라이언스의 추적 서비스를 사용하면 메시지 제목 줄, 날짜 및 시간 범위, 봉투 발신자 또는 수신자, 처리 이벤트(예: 메시지 상태가 바이러스 양성, 스팸 양성, 하드 반송, 전달됨 등인지 여부) 등의 지정된 기준과 일치하는 특정 이메일 메시지 또는 메시지 그룹을 검색할 수 있습니다. 메시지 추적은 메시지 플로우의 세부적인 보기를 제공합니다. 특정 이메일 메시지로 드릴다운하여 메시지 세부 사항, 즉 처리 이벤트, 첨부 파일 이름, 봉투 및 헤더 정보 등을 확인할 수도 있습니다.

참고 추적 구성 요소는 개별 이메일 메시지에 대한 세부 정보를 제공하지만 메시지의 내용을 읽는 데 사용할 수는 없습니다.

단계 **1** Cloud Email Security 관리 콘솔에서 **Tracking(**추적**)** > **Search(**검색**)**를 선택합니다.

단계 **2** 검색 범위를 좁히려면 **Messages(**메시지**)** 탭 또는 **Rejected Connections(**거부된 연결**)** 탭을 선택합니다.

참고 발신자 IP 주소, 도메인 또는 네트워크 소유자를 기준으로 거부된 연결을 검색할 수 있습니다.

단계 **3** (선택 사항) **Advanced Search(**고급 검색**)**를 클릭하여 추가 검색 옵션을 표시합니다.

단계 **4** 다음 검색 기준을 입력합니다.

참고 추적 검색에서는 와일드카드 문자나 정규식이 지원되지 않습니다. 추적 검색은 대/소문자를 구분하지 않습니다.

- [메시지 및 거부된 연결] **Message Received(**수신 메시지**)**: "전날", "지난 7일", "맞춤 범위"를 사용하여 쿼리할 날짜 및 시간 범위를 지정합니다. 지난 24시간의 메시지에서 검색하려면 "전날" 옵션을, 지난 7일 및 당일 경과한 시간의 메시지에서 검색하려면 "지난 7일" 옵션을 선택합니다.

  날짜를 지정하지 않으면 모든 날짜의 데이터가 반환됩니다. 시간 범위만 지정하는 경우 사용 가능한 모든 날짜에서 해당 시간 범위의 데이터가 반환됩니다. 현재 날짜와 23:59를 종료 날짜 및 시간으로 지정할 경우 쿼리는 당일의 모든 데이터를 반환합니다.

  날짜 및 시간은 데이터베이스에 저장될 때 GMT 형식으로 변환됩니다. 어플라이언스에서 날짜와 시간을 볼 때는 어플라이언스의 현지 시간으로 표시됩니다.

  Email Security Appliance에 기록되고 Security Management Appliance에 의해 검색된 후에야 비로소 메시지가 결과에 나타납니다. 로그의 크기 및 폴링 빈도에 따라 이메일 메시지가 전송된 시간과 추적 및 보고 결과에 실제로 나타나는 시간 사이에 약간의 차이가 생길 수 있습니다.

- **Envelope Sender(**봉투 발신자**)**: 시작, 일치, 포함을 선택하고 봉투 발신자에서 찾을 텍스트 문자열을 입력합니다. 이메일 주소, 사용자 이름 또는 도메인을 입력할 수 있습니다. 다음 형식을 사용합니다.
  - 이메일 도메인: *example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]*
  - 전체 이메일 주소: *user@example.com, user@[203.0.113.15]* 또는 *user@[ipv6:2001:db8:80:1::5]*.
  - 임의의 문자를 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
- **Subject(**제목**)**: 시작, 일치, 포함 또는 비어 있음을 선택하고 메시지 제목줄에서 검색할 텍스트 문자열을 입력합니다.
- **Envelope Recipient(**봉투 수신자**)**: 시작, 일치, 포함을 선택하고 봉투 수신자에서 찾을 텍스트 문자열을 입력합니다. 이메일 주소, 사용자 이름 또는 도메인을 입력할 수 있습니다.

  구축에서 별칭 확장용 별칭 테이블을 사용하는 경우 원래 봉투 주소보다는 확장된 수신자 주소가 검색됩니다. 다른 모든 경우에는 메시지 추적 조회에서 원래 봉투 수신자 주소가 검색됩니다.

  그렇지 않으면 봉투 수신자에 대한 유효한 검색 조건은 봉투 발신자와 동일합니다.

  임의의 문자를 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
- **Attachment Name(**첨부 파일 이름**)**: 시작, 일치, 포함 중에서 선택하고 검색할 첨부 파일 이름 하나를 ASCII 또는 Unicode 텍스트 문자열로 입력합니다. 입력한 텍스트에서 전후 공백이 제거되지 않습니다.
- **Reply-To(**회신**)**: 시작, 일치, 포함 또는 비어 있음을 선택하고 메시지의 `Reply-To(회신)` 헤더에 따라 검색할 텍스트 문자열을 입력합니다.
- 파일 **SHA256**: 메시지의 파일 SHA-256 값을 입력합니다.

  SHA-256 해시를 기반으로 파일을 식별하는 방법에 대한 자세한 내용은 SHA-256 해시로 파일 식별 , 96 페이지 섹션을 참조하십시오.
- **Cisco Host(Cisco** 호스트**)**: 모든 이메일 보안 어플라이언스에서 검색하려면 모든 호스트를 선택하고, 그렇지 않으면 드롭다운 메뉴에서 필요한 이메일 보안 어플라이언스를 선택합니다.
- **Message ID Header and Cisco MID(**메시지 **ID** 헤더 및 **Cisco MID)**: 메시지 ID 헤더, Cisco IronPort MID(message ID) 또는 둘 다에 대한 텍스트 문자열을 입력합니다.
- [메시지 및 거부된 연결] **Sender IP Address/ Domain/ Network Owner(**발신자 **IP** 주소/도메인/네트워크 소유자**)**: 발신자 IP 주소, 도메인 또는 네트워크 소유자 상세정보를 입력합니다.
  - IPv4 주소는 4개의 숫자가 마침표로 구분되어야 합니다. 각 숫자는 0 ~ 255의 값이어야 합니다. (예: 203.0.113.15)
  - IPv6 주소는 콜론으로 구분되는 16비트의 16진수 값 8개로 구성됩니다.

    2001:db8:80:1::5와 같이 한 위치에서 영 제거를 사용할 수 있습니다.
  - **Message Event(**메시지 이벤트**)**: 추적할 이벤트를 선택합니다. 바이러스 양성, 스팸 양성, 스팸 의심, 억제된 악성 URL, 지정된 범주의 억제된 URL, DLP 위반(DLP 정책의 이름을 입력하고 위반 심각도 또는 이행한 조치를 선택할 수 있음). DMARC 위반, 전달됨, AMP 양성(첨부 파일에서 발견된 악성코드), 하드 반송, 소프트 반송, 현재 정책, 바이러스, 바이러스 격리 중, 메시지 필터 또는 콘텐츠 필터에 의해 차단, 스팸으

로 격리 등의 옵션이 있습니다. 추적 쿼리에 추가하는 여느 조건과 달리 이벤트는 "OR" 연산자와 함께 추가됩니다. 여러 이벤트를 선택하면 검색이 확대됩니다.

모든 필드를 완료할 필요는 없습니다. 메시지 이벤트 옵션을 제외하고 쿼리는 "AND" 검색입니다. 검색 필드에 지정된 “AND” 조건과 매칭하는 메시지를 반환합니다. 예를 들어, 봉투 수신자 및 제목 줄 매개변수에 대한 텍스트 문자열을 지정하는 경우 지정된 봉투 수신자 및(and) 제목 줄과 모두 일치하는 메시지만 반환됩니다.

단계 **5** **Search(**검색**)**를 클릭합니다.

각 행은 하나의 이메일 메시지에 해당합니다. 아래로 스크롤하여 보기에서 추가 메시지를 로드합니다.

필요한 경우 새 검색 기준을 입력하여 검색을 구체화한 후 쿼리를 다시 실행합니다. 또는 다음 섹션의 설명대로 검색 결과를 좁히는 방법으로 검색을 개선할 수 있습니다.

다음에 수행할 작업

- 결과 집합 좁히기, 271 페이지
- 메시지 추적 및 AMP 기능 정보 , 272 페이지
- 추적 쿼리 결과 이해, 273 페이지

레거시 웹 인터페이스에서 이메일 메시지 검색

Security Management Appliance의 추적 서비스를 사용하면 메시지 제목 줄, 날짜 및 시간 범위, 봉투 발신자 또는 수신자, 처리 이벤트(예: 메시지 상태가 바이러스 양성, 스팸 양성, 하드 반송, 전달됨 등인지 여부) 등의 지정된 기준과 일치하는 특정 이메일 메시지 또는 메시지 그룹을 검색할 수 있습니다. 메시지 추적은 메시지 플로우의 세부적인 보기를 제공합니다. 특정 이메일 메시지로 드릴다운하여 메시지 세부 사항, 즉 처리 이벤트, 첨부 파일 이름, 봉투 및 헤더 정보 등을 확인할 수도 있습니다.

참고 추적 구성 요소는 개별 이메일 메시지에 대한 세부 정보를 제공하지만 메시지의 내용을 읽는 데 사용할 수는 없습니다.

단계 **1** **Email(**이메일**) > Message Tracking(**메시지 추적**) > Message Tracking(**메시지 추적**)**을 선택합니다.

단계 **2** (선택 사항) Advanced(고급) 링크를 클릭하여 추가 검색 옵션을 표시합니다.

단계 **3** 검색 기준을 입력합니다.

참고 추적 검색에서는 와일드카드 문자나 정규식이 지원되지 않습니다. 추적 검색은 대/소문자를 구분하지 않습니다.

- 봉투 발신자: 시작, 일치, 포함을 선택하고 봉투 발신자에서 찾을 텍스트 문자열을 입력합니다. 이메일 주소, 사용자 이름 또는 도메인을 입력할 수 있습니다. 다음 형식을 사용합니다.
  - 이메일 도메인: example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]

  - 전체 이메일 주소: user@example.com, user@[203.0.113.15] 또는 user@[ipv6:2001:db8:80:1::5]
  - 임의의 문자를 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
- 봉투 수신자: 시작, 일치, 포함을 선택하고 봉투 수신자에서 찾을 텍스트 문자열을 입력합니다. 이메일 주소, 사용자 이름 또는 도메인을 입력할 수 있습니다.

구축에서 별칭 확장용 별칭 테이블을 사용하는 경우 원래 봉투 주소보다는 확장된 수신자 주소가 검색됩니다. 다른 모든 경우에는 메시지 추적 조회에서 원래 봉투 수신자 주소가 검색됩니다.

그렇지 않으면 봉투 수신자에 대한 유효한 검색 조건은 봉투 발신자와 동일합니다.

임의의 문자를 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.

- 제목: 시작, 일치, 포함 또는 비어 있음을 선택하고 메시지 제목줄에서 검색할 텍스트 문자열을 입력합니다.
- 수신 메시지: "전날", "지난 7일", "맞춤 범위"를 사용하여 쿼리할 날짜 및 시간 범위를 지정합니다. 지난 24시간의 메시지에서 검색하려면 "전날" 옵션을, 지난 7일 및 당일 경과한 시간의 메시지에서 검색하려면 "지난 7일" 옵션을 선택합니다.

날짜를 지정하지 않으면 모든 날짜의 데이터가 반환됩니다. 시간 범위만 지정하는 경우 사용 가능한 모든 날짜에서 해당 시간 범위의 데이터가 반환됩니다. 현재 날짜와 23:59를 종료 날짜 및 시간으로 지정할 경우 쿼리는 당일의 모든 데이터를 반환합니다.

날짜 및 시간은 데이터베이스에 저장될 때 GMT 형식으로 변환됩니다. 어플라이언스에서 날짜와 시간을 볼 때는 어플라이언스의 현지 시간으로 표시됩니다.

Email Security Appliance에 기록되고 Security Management Appliance에 의해 검색된 후에야 비로소 메시지가 결과에 나타납니다. 로그의 크기 및 폴링 빈도에 따라 이메일 메시지가 전송된 시간과 추적 및 보고 결과에 실제로 나타나는 시간 사이에 약간의 차이가 생길 수 있습니다.

- 발신자 IP 주소: 발신자 IP 주소를 입력하고 메시지를 검색할지 아니면 거부된 연결만 검색할지 선택합니다.
  - IPv4 주소는 4개의 숫자가 마침표로 구분되어야 합니다. 각 숫자는 0 ~ 255의 값이어야 합니다. (예: 203.0.113.15)
  - IPv6 주소는 콜론으로 구분되는 16비트의 16진수 값 8개로 구성됩니다. 2001:db8:80:1::5와 같이 한 위치에서 영 제거를 사용할 수 있습니다.
- 메시지 이벤트: 추적할 이벤트를 선택합니다. 옵션으로는 Virus Positive(바이러스 양성), Spam Positive(스팸 양성), Suspect Spam(의심스러운 스팸), contained malicious URLs(포함된 악성 URL), contained URL in specified category(지정된 카테고리에 포함된 URL), DLP Violations(DLP 위반)(DLP 정책의 이름을 입력하고 위반 심각도나 수행된 작업을 선택할 수 있음), DMARC violations(DMARC 위반), Delivered(전달됨), Advanced Malware Protection Positive(Advanced Malware Protection 양성)(첨부 파일에서 발견된 악성코드), Hard Bounced(하드 반송됨), Soft Bounced(소프트 반송됨)(현재 정책, 바이러스 또는 보안 침해 격리에 있으며 메시지 필터 또는 콘텐츠 필터에 걸림), Macro File Types Detected(탐지된 매크로 파일 형식), Geolocation(지리위치), Low Risk(낮은 위험), Quarantined as Spam(스팸으로 격리됨)이 있습니다. 추적 쿼리에 추가하는 여느 조건과 달리 이벤트는 "OR" 연산자와 함께 추가됩니다. 여러 이벤트를 선택하면 검색이 확대됩니다.
- 메시지 ID 헤더 및 Cisco IronPort MID: 메시지 ID 헤더, Cisco IronPort MID(message ID) 또는 둘 다를 위한 텍스트 문자열을 입력합니다.
- 쿼리 설정: 드롭다운 메뉴에서 쿼리가 시간 초과될 때까지 실행될 시간을 선택합니다. "1분", "2분", "5분", "10분", "시간 제한 없음" 옵션이 있습니다. 또한 쿼리에서 반환할 최대 결과 수를 선택합니다(1,000개까지).

- 첨부 파일 이름: 시작, 일치, 포함 중에서 선택하고 검색할 첨부 파일 이름 하나를 ASCII 또는 Unicode 텍스트 문자열로 입력합니다. 입력한 텍스트에서 전후 공백이 제거되지 않습니다.

모든 필드를 완료할 필요는 없습니다. 메시지 이벤트 옵션을 제외하고 쿼리는 "AND" 검색입니다. 검색 필드에 지정된 “AND” 조건과 매칭하는 메시지를 반환합니다. 예를 들어, 봉투 수신자 및 제목 줄 매개변수에 대한 텍스트 문자열을 지정하는 경우 지정된 봉투 수신자 및(and) 제목 줄과 모두 일치하는 메시지만 반환됩니다.

단계 **4** **Search(**검색**)**를 클릭합니다.

쿼리 결과는 페이지의 맨 아래에 나타납니다. 각 행은 하나의 이메일 메시지에 해당합니다.

검색 조건이 각 행에서 강조 표시됩니다.

반환된 행 수가 “Items per page(페이지당 항목)” 필드에 지정된 값보다 클 경우 여러 페이지에 결과가 표시됩니다. 여러 페이지를 탐색하려면 목록 맨 위 또는 아래의 페이지 번호를 클릭합니다.

필요하다면 새 검색 조건을 입력하고 다시 쿼리를 실행하여 검색을 개선합니다. 또는 다음 섹션의 설명대로 검색 결과를 좁히는 방법으로 검색을 개선할 수 있습니다.

다음에 수행할 작업

- 결과 집합 좁히기, 271 페이지
- 메시지 추적 및 AMP 기능 정보 , 272 페이지
- 추적 쿼리 결과 이해, 273 페이지

결과 집합 좁히기

쿼리를 실행한 후 결과 집합에 필요 이상의 정보가 포함된 경우도 있습니다. 새 쿼리를 생성하지 말고 결과의 목록에서 행 내의 어떤 값을 클릭하여 결과 집합을 좁힐 수 있습니다. 값을 클릭하면 그 매개변수 값이 검색 조건으로 추가됩니다. 예를 들어 쿼리 결과가 여러 날짜의 메시지를 포함할 경우 행 내에서 특정 날짜를 클릭하면 그 날짜에 수신한 메시지만 표시됩니다.

단계 **1** 조건으로 추가할 값 위에 커서를 놓습니다. 이 값이 노란색으로 강조 표시됩니다.

다음 매개변수 값을 사용하여 검색을 개선합니다.

- 날짜 및 시간
- 메시지 ID(MID)
- 호스트(Email Security Appliance)
- 발신자
- 수신자
- 메시지의 제목 줄 또는 제목의 시작 단어

단계 **2** [새 웹 인터페이스에만 해당] Message Tracking(메시지 추적) 검색 조건에서 **Modify(**수정**)**를 클릭합니다.

다음 매개변수 값을 사용하여 검색을 개선합니다.

- 날짜 및 시간
- 메시지 ID(MID)
- Cisco 호스트(Email Security Appliance)
- 발신자
- 수신자
- 메시지의 제목 줄 또는 제목의 시작 단어
- 메시지 이벤트
- 추가 세부 정보(메시지 마지막 상태, SBRS, 발신자 IP 및 그룹)

단계 **3** 값을 클릭하여 검색을 개선합니다.

결과 섹션에는 원래의 검색 매개변수 및 새로 추가한 검색 조건과 매칭하는 메시지가 표시됩니다.

단계 **4** 필요하다면 결과에서 또 다른 값을 클릭하여 검색을 더욱 개선합니다.

참고 쿼리 조건을 제거하려면 **Clear(**지우기**)**를 클릭하고 새 추적 쿼리를 실행합니다.

메시지 추적 및 **AMP** 기능 정보

메시지 추적에서 파일 위협 정보를 검색할 때 다음 사항에 유의하십시오.

- 파일 평판 서비스에서 발견한 악성 파일을 검색하려면 메시지 추적의 Advanced(고급) 섹션, Message Event(메시지 이벤트) 옵션에서 **Advanced Malware Protection Positive(AMP** 양성**)**를 선택합니다.
- 메시지 추적은 메시지가 처리된 시점에 반환된 파일 평판 처리 및 원래의 파일 평판 판정의 정보만 포함합니다. 예를 들어, 파일이 처음에는 클린으로 확인되었으나 판정 업데이트에서는 파일이 악성으로 확인된 경우 클릭 판정만 추적 결과에 표시됩니다.

  메시지 추적 세부사항에 처리 세부사항 섹션이 표시됩니다.

  - 메시지의 각 첨부 파일의 SHA-256
  - 전체 메시지에 대한 최종 Advanced Malware Protection 판정
  - 악성코드가 포함된 것으로 확인된 첨부 파일

    클린 또는 검사 불가 첨부 파일에 대해 제공된 정보가 없습니다.

- 판정 업데이트는 AMP 판정 업데이트 보고서에서만 사용할 수 있습니다. 메시지 추적에 있는 원래 메시지 세부사항은 판정 변동 시 업데이트되지 않습니다. 특정 첨부 파일이 있는 메시지를 확인하려면 판정 업데이트 보고서에서 SHA-256을 클릭합니다.
- 분석 결과 및 분석을 위해 파일이 전송되었는지 여부를 포함한 파일 분석에 대한 정보는 파일 분석 보고서에서만 사용할 수 있습니다.

분석한 파일에 대한 추가 정보는 클라우드에서 사용할 수 있습니다. 어떤 파일에 대해 사용 가능한 파일 분석 정보를 보려면 **Monitor(**모니터링**) > File Analysis(**파일 분석**)**를 선택하고 SHA-256을 입력하여 파일을 검색합니다. 파일 분석 서비스가 임의의 소스에서 파일을 분석한 경우 세부사항을 볼 수 있습니다. 결과는 분석된 파일에 대해서만 표시됩니다.

어플라이언스에서 분석을 위해 보내진 파일의 또 다른 인스턴스를 처리한 경우 이 인스턴스는 메시지 추적 검색 결과에 나타납니다.

추적 쿼리 결과 이해

기대한 결과가 아닐 경우 메시지 추적 트러블슈팅, 277 페이지를 참조하십시오.

추적 쿼리 결과에서는 추적 쿼리에 지정된 조건과 매칭하는 모든 메시지를 나열합니다. 메시지 이벤트 옵션을 제외하고 쿼리 조건은 "AND" 연산자가 추가됩니다. 결과 집합의 메시지는 모든 조건을 충족해야 합니다. 예를 들어 봉투 발신자가 J로 시작하고 제목이 T로 시작하도록 지정할 경우 쿼리는 두 조건이 모두 참인 메시지만 반환합니다.

메시지에 대한 자세한 정보를 보려면 새 웹 인터페이스에서 **More Details(**추가 세부 정보**)** 링크를 클릭하거나 해당 메시지에 대한 레거시 웹 인터페이스에서 **Show Details(**세부 정보 표시**)** 링크를 클릭합니다. 자세한 내용은 메시지 세부사항, 274 페이지을 참조하십시오.

참고

- 수신자가 50명 이상인 메시지는 추적 쿼리 결과에 나타나지 않습니다. 이 문제는 향후 릴리스에서 해결될 것입니다.
- [새 웹 인터페이스에만 해당] 쿼리를 지정할 때 아래로 스크롤하여 검색 결과를 표시할 수 있습니다. 아래로 스크롤하면 보기에 더 많은 결과가 표시됩니다.
- 검색 결과 섹션 위의 **Export(**내보내기**)** 링크를 사용하여 검색 결과를 .csv 파일로 내보낼 수 있습니다.

  쿼리를 지정할 때 최대 1,000개의 검색 결과를 표시하도록 선택할 수 있습니다. 조건과 매칭하는 최대 50,000개의 메시지를 표시하려면 검색 결과 섹션 위의 **Export All(**모두 내보내기**)** 링크를 클릭하고 생성되는 CSV 파일을 다른 애플리케이션에서 엽니다.
- 메시지 추적에서 메시지 세부사항을 보기 위해 보고서 페이지의 링크를 클릭했는데 예상했던 것과 다른 결과 집합이 표시되는 경우, 검토 기간 중에 보고와 추적이 동시에 계속해서 활성화되지 않았기 때문일 수 있습니다.
- 메시지 추적 검색 결과의 출력 또는 내보내기에 대한 자세한 내용은 보고/추적 데이터 인쇄 및 내보내기 , 41 페이지 섹션을 참조해 주십시오.

관련 주제

메시지 세부사항, 274 페이지

메시지 세부사항

특정 이메일 메시지에 대한 세부 정보를 보려면(예: 메시지 헤더 정보, 처리 정보) 검색 결과 목록에서 임의의 항목에 대해 **More Details(**추가 세부 정보**)** 링크를 클릭합니다. 새 창이 열리고 메시지 세부사항이 표시됩니다.

메시지 세부사항은 다음 섹션으로 구성됩니다.

- Verdict Charts(판정 차트) 및 Last State Verdicts(마지막 상태 판정), 274 페이지
- 봉투 및 헤더 요약, 275 페이지
- 발송 호스트 요약, 276 페이지
- 처리 정보, 276 페이지

Verdict Charts(판정 차트) 및 Last State Verdicts(마지막 상태 판정)

Verdict Charts(판정 차트)에는 Email Security Appliance의 각 엔진에 의해 트리거되는 가능한 여러 가지 판정에 대한 정보가 표시됩니다.

참고 12.0 이전 AsyncOS에 대한 판정 차트는 표시되지 않으며 마지막 상태 판정은 "Last State Not Available(마지막 상태를 사용할 수 없음)"로 표시됩니다.

다음 표에는 각 엔진의 다양한 판정이 표시됩니다.

표 *72:* 판정 차트

연결 동작	메시지 필터	**Anti-Spam**	**Anti-Virus**	**AMP**	그레이메일	콘텐츠 필터	보안 침해 필터	**DLP**
해당 없음 허용됨 Relayed	평가되지 않음 일치 일치하지 않음	평가되지 않음 부정적 의심스러움 벌크 메일 소셜 메일 마케팅 메일 Positive	평가되지 않음 부정적 Repaired(복구됨) 암호화 Unscanable(스캔할 수 없음) Positive	평가되지 않음 정상 FA 보류 중 알 수 없음 건너뜀 악성 Unscannable(검색할 수 없음) 낮은 위험	평가되지 않음 부정적 Positive	평가되지 않음 일치 No Match(일치하지 않음)	평가되지 않음 일치 No Match(일치하지 않음)	평가되지 않음 트리거 없음 위반 위반 없음

메시지의 Last State(마지막 상태) 판정에 따라 어플라이언스의 각 엔진의 가능한 모든 판정 후에 트리거되는 최종 판정이 결정됩니다.

다음은 마지막 상태 판정의 일부입니다.

- 배달됨: 메시지가 배달되는 경우
- 삭제됨: 메시지가 삭제되는 경우
- 중단됨: 메시지가 중단된 경우 (예: 메일 정책 제한으로 인해)
- 반송됨: 메시지가 반송되는 경우
- 분리됨: 메시지의 MID가 여러 최종 상태를 보유한 여러 MID로 분리되는 경우
- 격리됨: 메시지가 엔진에 의해 격리되는 경우
- 대기열에 있음: 메시지가 최종 수신자 또는 오프박스 스팸 격리나 중앙 집중식 정책, 바이러스 또는 보안 침해 격리로 전달되기 위해 대기열에 있는 경우
- 처리 중: 메시지가 모든 엔진에서 완전히 처리되지 않았거나, 메시지가 특정 엔진의 대기열에서 대기 중인 경우
- 마지막 상태를 사용할 수 없음: 메시지의 마지막 상태를 검색할 수 없는 경우 (예: 메시지가 엔진에서 계속 처리되고 있으며 최종 상태에 도달하지 않은 경우.

봉투 및 헤더 요약

이 섹션은 메시지 봉투 및 헤더의 정보, 즉 봉투 발신자 및 수신자 등을 표시합니다. 여기에는 다음 정보가 포함되어 있습니다.

Received Time(수신 시간**):** Email Security Appliance가 메시지를 수신한 시간입니다.

MID: 메시지 ID.

Subject(제목**):** 메시지의 제목 줄.

메시지에 제목이 없는 경우 또는 로그 파일에 제목 헤더를 기록하도록 Email Security Appliance가 구성되지 않은 경우 추적 결과의 제목 줄에 "(No Subject)" 값이 표시될 수 있습니다.

Envelope Sender(봉투 발신자**):** SMTP 봉투의 발신자 주소입니다.

봉투 수신자**:** SMTP 봉투의 수신자 주소.

메시지 **ID** 헤더**:** 각 이메일 메시지를 고유하게 식별하는 “Message-ID:” 헤더. 메시지를 처음 만들 때 메시지에 삽입됩니다. “Message-ID:” 헤더는 특정 메시지를 검색할 때 유용할 수 있습니다.

Cisco Host(Cisco 호스트**):** 메시지를 처리한 Email Security Appliance입니다.

SMTP Auth User ID(SMTP 인증 사용자 **ID):** 발신자가 SMTP 인증을 사용하여 이메일을 전송한 경우 발신자의 SMTP 인증 사용자 이름. 그렇지 않으면 값은 "N/A"입니다.

첨부 파일: 메시지에 첨부된 파일의 이름.

Sender Group(발신자 그룹**)**: 메시지를 수신한 발신자 그룹입니다.

Message Size(메시지 크기**)**: 메시지의 크기입니다.

Policy Match (Incoming or Outgoing)(정책 일치**(**수신 또는 발신**))**: 메시지를 수신한 정책입니다.

참고 엔진이 세부 정보를 가져올 수 없는 경우 값은 "N/A"로 표시됩니다.

발송 호스트 요약

Reverse DNS Hostname(역방향 **DNS** 호스트 이름**):** 역방향 DNS(PTR) 조회로 확인한 발신 호스트의 호스트 이름입니다.

IP 주소**:** 발신 호스트의 IP 주소.

SBRS Score(SBRS 점수**):** SenderBase 평판 점수입니다. 범위는 10(신뢰할 수 있는 발신자) ~ -10(명백한 스패머)입니다. 점수는 메시지가 처리된 시점에 이 호스트에 대한 정보가 없음을 나타냅니다.

처리 정보

여기서는 메시지 처리 과정에 로깅된 다양한 상태 이벤트를 표시합니다.

메일 정책 처리에 대한 정보(예: 안티스팸 및 안티바이러스 검사)와 기타 이벤트(예: 메시지 분할)가 포함됩니다.

메시지가 전달된 경우 전달 세부사항이 여기에 표시됩니다. 예를 들어 메시지가 전달되었고 그 복사본이 격리되어 있을 수 있습니다.

마지막에 기록된 이벤트가 처리 세부사항에 강조 표시됩니다.

Summary(요약**)** 탭

이 탭에는 메시지 처리 중에 기록된 모든 이벤트의 요약 로그가 표시됩니다.

DLP 매칭 콘텐츠 탭

이 탭에는 데이터 손실 방지(DLP) 정책을 위반하는 콘텐츠가 표시됩니다.

여기에는 일반적으로 민감한 정보(예: 회사 기밀 정보 및 신용카드 번호와 건강 기록 등의 개인 정보)가 포함되므로, Security Management Appliance에 대해 관리자 레벨 액세스 권한이 없는 사용자에 대해서는 액세스를 비활성화할 수 있습니다. 메시지 추적 시 중요 정보의 액세스 제어 , 426 페이지를 참조하십시오.

URL 세부 정보 탭

이 탭은 메시지 필터가 아니라 URL 평판 및 URL 카테고리 콘텐츠 필터와 Outbreak Filter에 걸린 메시지에 대해서만 표시됩니다.

이 탭에는 다음 정보가 표시됩니다.

- 평판 점수 또는 URL과 관련된 카테고리
- URL에서 수행한 작업(재작성, 무해화 또는 리디렉션)

- 메시지에 여러 URL이 포함된 경우 필터 작업을 트리거하는 URL

Email Security Appliance에서 이 정보를 표시하도록 구성한 경우에만 이 탭을 볼 수 있습니다. *AsyncOS for Cisco Email Security Appliances* 사용 설명서를 참조하십시오.

이 탭에 대한 액세스를 제어하려면 다음을 참조하십시오. 메시지 추적 시 중요 정보의 액세스 제어 , 426 페이지

SMTP Log(SMTP 로그) 탭

이 섹션에는 이메일 발신자가 SMTP 인증에 실패한 경우의 메시지 로그가 표시됩니다.

AMP Log(AMP 로그) 탭

이 섹션에는 Advanced Malware Protection 파일 평판 및 파일 분석 서비스에서 포착한 메시지 로그가 표시됩니다.

메시지 추적 트러블슈팅

검색 결과에 예상 메시지가 누락됨

문제

기준을 충족했을 메시지가 검색 결과에 포함되지 않았습니다.

솔루션

- 많은 검색, 특히 메시지 이벤트와 관련된 검색의 결과는 어플라이언스 구성에 따라 달라집니다. 예를 들어 필터링하지 않은 URL 범주를 검색하는 경우, 해당 범주에 URL이 메시지에 포함되었더라도 결과에 아무것도 표시되지 않습니다. 예상한 동작이 수행되도록 Email Security Appliance를 적절히 구성했는지 확인하십시오. 예를 들면 메일 정책, 콘텐츠 및 메시지 필터, 격리 설정을 점검해 주십시오.
- 메시지 추적 데이터 가용성 확인 , 266 페이지를 참조하십시오.

첨부 파일이 검색 결과에 나타나지 않음

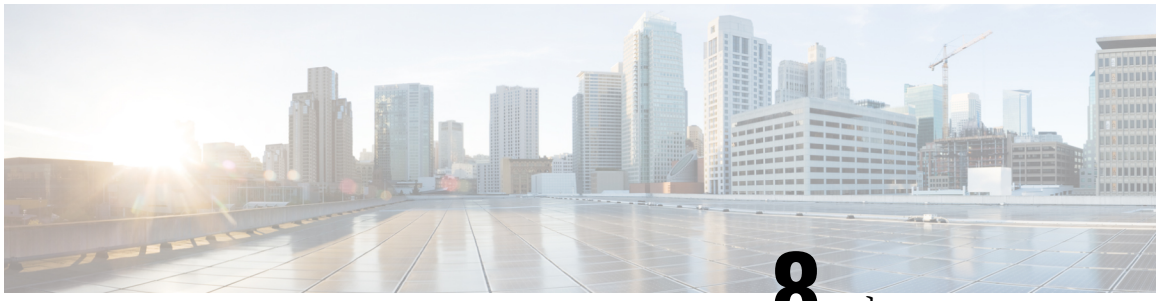
문제

첨부 파일 이름이 검색 결과에 나타나지 않으며 찾을 수 없습니다.

솔루션

하나 이상의 수신 콘텐츠 필터 또는 기타 본문 검사 기능이 ESA에서 구성 및 활성화되었습니다. Security Management Appliance에서 중앙 집중식 이메일 추적 활성화, 264 페이지의 구성 요구 사항 및 추적 서비스 개요, 263 페이지의 첨부 파일 이름 검색에 대한 제한 사항을 참조하십시오.

첨부 파일이 검색 결과에 나타나지 않음



8 장

스팸 격리

이 장에는 다음 섹션이 포함되어 있습니다.

스팸 격리 개요

스팸 격리(ISQ라고도 함) 및 엔드 유저 격리(EUQ라고도 함)는 이메일 메시지가 합법적이지만 어플라이언스에서 스팸으로 간주하는 "오탐"을 우려하는 조직을 위한 안전 메커니즘을 제공합니다. 어플라이언스에서 메시지가 스팸인지 또는 의심스러운 스팸인지를 확인할 때, 메시지를 전달 또는 삭제하기 전에 수신자나 관리자가 검토하도록 할 수 있습니다. 스팸 격리는 이 목적으로 메시지를 저장합니다.

Email Security Appliance의 관리 사용자는 스팸 격리의 모든 메시지를 볼 수 있습니다. 최종 사용자(대개 메시지 수신자)는 약간 다른 웹 인터페이스에서 자신의 격리된 메시지를 볼 수 있습니다.

스팸 격리는 정책, 바이러스 및 보안 침해 격리와 다릅니다.

관련 주제

- 중앙 정책, 바이러스, 보안 침해 격리, 311 페이지

로컬 대 외부 스팸 격리

로컬 스팸 격리는 Email Security Appliance에 스팸 및 의심스러운 스팸을 저장합니다. 외부 스팸 격리는 이러한 메시지를 별도의 Cisco Content Security Management Appliance에 저장할 수 있습니다.

다음과 같은 경우에는 외부 스팸 격리의 사용을 고려해볼 수 있습니다.

- 여러 Email Security Appliance에서 오는 스팸을 저장 및 관리할 중앙 집중식 위치가 필요한 경우.
- Email Security Appliance에 보관할 수 있는 것보다 더 많은 스팸을 저장하려는 경우.
- 스팸 격리 및 해당 메시지를 정기적으로 백업하려는 경우

중앙 집중식 스팸 격리 설정

프로시저

	명령 또는 동작	목적
단계 **1**	Security Management Appliance에서 중앙 집중식 스팸 격리 서비스를 활성화합니다.	스팸 격리 활성화 및 구성 , 281 페이지
단계 **2**	Security Management Appliance에서 중앙 집중식 스팸 격리에 포함할 Email Security Appliance를 지정합니다.	관리되는 각 Email Security Appliance에 중앙 집중식 스팸 격리 서비스 추가 , 283 페이지
단계 **3**	알림 및 릴리스된 스팸 전송에 대해 Security Management Appliance를 설정합니다.	Security Management Appliance에서 아웃바운드 IP 인터페이스 구성 , 283 페이지
단계 **4**	Security Management Appliance에서 스팸 격리 브라우저 인터페이스를 구성합니다.	브라우저가 스팸 격리에 액세스하도록 IP 인터페이스 구성 , 284 페이지
단계 **5**	메일을 스팸 격리로 전송하도록 Email Security Appliance가 구성되어 있는지 확인합니다.	안티 스팸 및 메일 정책을 구성하는 방법에 대한 자세한 내용은 *AysncOS for Email Security Appliances* 사용 설명서의 "안티 스팸" 섹션을 참조하십시오.
단계 **6**	Email Security Appliance에서 외부 스팸 격리를 활성화 및 구성합니다.	자세한 내용은 *AysncOS for Email Security Appliance* 사용 설명서를 참조하십시오.
단계 **7**	Email Security Appliance에서 로컬 격리를 비활성화합니다.	외부 스팸 격리 활성화를 위해 로컬 스팸 격리를 비활성화하는 방법에 대한 자세한 내용은 *AysncOS for Email Security Appliance* 사용 설명서를 참조하십시오.

스팸 격리 활성화 및 구성

참고 외부 스팸 격리를 사용하는 경우 Security Management Appliance의 이 섹션에 설명된 설정을 구성하게 됩니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **3** 시스템 설정 마법사를 실행한 후 처음으로 스팸 격리를 활성화하는 경우

a) **Enable(**활성화**)**을 클릭합니다.

b) 엔드 유저 라이선스 계약을 검토한 후 **Accept(**동의**)**를 클릭합니다.

단계 **4** 스팸 격리 설정을 수정하는 경우 **Edit Settings(**설정 수정**)** 링크를 클릭합니다.

단계 **5** 옵션을 지정합니다.

옵션	설명
Quarantine IP Interface(격리 IP 인터페이스) Quarantine Port(격리 포트)	기본적으로 스팸 격리는 Management 인터페이스 및 포트 6025를 사용합니다. IP 인터페이스는 수신 메일을 대기하도록 구성된 Security Management Appliance의 인터페이스입니다. 격리 포트는 전송 어플라이언스가 외부 격리 설정에서 사용하는 포트 번호입니다. Email Security Appliance가 Security Management Appliance와 동일한 네트워크에 있지 않은 경우 Management 인터페이스를 사용해야 합니다.
Deliver Messages Via(메시지 전달 경로)	모든 발신 격리 관련 이메일(예: 스팸 알림 및 스팸 격리에서 릴리스된 메시지)은 메시지를 전송하도록 구성된 서버 또는 다른 어플라이언스를 통해 전달해야 합니다. SMTP 또는 그룹웨어 서버를 통해 이러한 메시지를 라우팅하거나, Email Security Appliance의 아웃바운드 리스너 인터페이스(일반적으로 Data 2 인터페이스)를 지정할 수 있습니다. 로드 밸런싱 및 장애 조치에 대체 주소가 사용됩니다. 여러 Email Security Appliance가 있는 경우, 기본 및 대체 주소에 대해 관리되는 Email Security Appliance의 아웃바운드 리스너 인터페이스를 사용할 수 있습니다. 아웃바운드 리스너로 동일한 인터페이스(Data 1 또는 Data 2)를 사용해야 합니다. 이러한 주소에 대한 추가 주의 사항은 화면의 지침을 참조하십시오.

옵션	설명
쿼런틴 크기	**When storage space is full, automatically delete oldest messages first**(스토리지 공간이 꽉 차면 가장 오래된 메시지부터 자동으로 삭제)의 선택을 취소하면 꽉 찬 격리에 새 메시지가 추가되지 않습니다. 꽉 찬 격리 때문에 메시지가 어플라이언스에서 대기열에 추가(백업)되지 않도록 하려면 이 옵션을 활성화하는 것이 좋습니다. 격리에 대한 디스크 공간 관리는 디스크 공간 관리 , 487 페이지 섹션을 참조하십시오.
Schedule Delete After(삭제 기준 일정)	삭제 전에 메시지를 유지할 일수를 지정합니다. 격리의 용량이 꽉 차는 것을 방지하기 위해 오래된 메시지를 삭제하도록 격리를 구성하는 것이 좋지만, 자동 삭제를 예약하지 않을 수도 있습니다.
Notify Cisco Upon Message Release(메시지 릴리스 시 Cisco에 알림)	—
Spam Quarantine Appearance(스팸 격리 모양)	로고 기본적으로 사용자가 격리된 메시지를 보기 위해 로그인하면 스팸 격리 페이지 상단에 Cisco 로고가 표시됩니다. 두 신규 및 레거시 웹 인터페이스에서 로고를 볼 수 있습니다. 대신 맞춤형 로고를 사용하려면 해당 로그를 업로드합니다. 로고는 최대 50픽셀(세로) X 500픽셀(가로)의 .jpg, .gif 또는 .png 파일이어야 합니다.
	로그인 페이지 메시지 (선택 사항) 로그인 페이지 메시지를 지정합니다. 이 메시지는 격리를 보기 위해 로그인하는 관리자 및 최종 사용자에게 표시됩니다. 메시지를 지정하지 않으면 다음 메시지가 나타납니다. Enter your login information below. If you are unsure what to enter, please contact your administrator.(아래에 로그인 정보를 입력하십시오. 입력할 정보를 모르면 관리자에게 문의하십시오.)
관리자	스팸 격리에 대한 관리 사용자 액세스 구성 , 285 페이지를 참조하십시오.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

- 다음으로 돌아갑니다. 중앙 집중식 스팸 격리 설정 , 280 페이지

관리되는 각 **Email Security Appliance**에 중앙 집중식 스팸 격리 서비스 추가

수행하는 단계는 또 다른 중앙 집중식 관리 기능을 구성할 때 어플라이언스를 이미 추가했는지 여부에 따라 달라집니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 이 페이지의 목록에 Email Security Appliance를 이미 추가한 경우

a) Email Security Appliance의 이름을 클릭합니다.

b) **Spam Quarantine(**스팸 격리**)** 서비스를 선택합니다.

단계 **4** Email Security Appliance를 아직 추가하지 않은 경우

a) Add Email Appliance(이메일 어플라이언스 추가)를 클릭합니다.

b) Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 어플라이언스 Management 인터페이스의 IP 주소를 입력합니다.

참고 DNS 이름은 IP Address(IP 주소) 텍스트 필드에 입력해야 합니다. 그러나 **Submit(**제출**)**을 클릭하면 즉시 IP 주소로 해석됩니다.

c) Spam Quarantine(스팸 격리) 서비스가 미리 선택되어 있습니다.

d) **Establish Connection(**연결 설정**)**을 클릭합니다.

e) 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다.

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

f) 페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.

g) **Test Connection(**테스트 연결**)**을 클릭합니다.

h) 테이블 위의 테스트 결과를 읽습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** 스팸 격리를 활성화할 각 Email Security Appliance에 대해 이 절차를 반복합니다.

단계 **7** 변경사항을 커밋합니다.

Security Management Appliance에서 아웃바운드 **IP** 인터페이스 구성

격리 관련 메시지(알림 및 릴리스된 이메일 포함)를 전달용 Email Security Appliance로 전송하도록 Security Management Appliance에서 인터페이스를 구성합니다.

시작하기 전에

아웃바운드 인터페이스에 사용할 IP 주소를 가져오거나 식별합니다. 일반적으로 Security Management Appliance의 Data 2 인터페이스입니다. 네트워크 요구 사항에 대한 자세한 내용은 네트워크 및 IP 주소 할당, 555 페이지을 참조하십시오.

단계 **1** 다음 페이지의 정보를 참조하여 이 절차를 수행합니다. IP 인터페이스 구성, 548 페이지

단계 **2** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **3** **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 주소**)**를 선택합니다.

단계 **4** **Add IP Interface(IP** 인터페이스 추가**)**를 클릭합니다.

단계 **5** 다음 설정을 입력합니다.

- 이름
- 이더넷 포트

  일반적으로 Data 2입니다. 특히, 이는 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**의 Spam Quarantine Settings(스팸 격리 설정) 페이지에서 **Deliver Messages Via(**메시지 전달 경로**)** 섹션의 **Primary Server(**기본 서버**)**에 대해 지정한 Email Security Appliance의 데이터 인터페이스와 일치해야 합니다.
- IP 주소

  방금 지정한 인터페이스의 IP 주소.
- Netmask
- 호스트 이름

  예를 들어 호스트 이름이 Data 2 인터페이스이면 data2.sma.example.com을 사용합니다.

이 인터페이스에 대한 Spam Quarantine(스팸 격리) 섹션에 정보를 입력하지 마십시오.

단계 **6** 변경 사항을 제출 및 커밋합니다.

브라우저가 스팸 격리에 액세스하도록 IP 인터페이스 구성

관리자와 최종 사용자가 스팸 격리에 액세스하면 별도의 브라우저 창이 열립니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)**를 선택합니다.

단계 **3** **Management** 인터페이스의 이름을 클릭합니다.

단계 **4** Spam Quarantine(스팸 격리) 섹션에서 스팸 격리에 액세스하기 위한 설정을 구성합니다.

- 기본적으로 HTTP는 포트 82를 사용하고 HTTPS는 포트 83을 사용합니다.
- 알림 및 스팸 격리 브라우저 창에 나타나는 URL을 지정합니다.

  Security Management Appliance의 호스트 이름을 최종 사용자에게 노출하지 않으려면 대체 호스트 이름을 지정할 수 있습니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

스팸 격리 액세스를 위해 지정한 호스트 이름을 DNS 서버가 인식할 수 있는지 확인합니다.

스팸 격리에 대한 관리 사용자 액세스 구성

관리자 권한이 있는 모든 사용자는 스팸 격리 설정을 변경하고 스팸 격리의 메시지를 보고 관리할 수 있습니다. 관리자 사용자에 대해서는 스팸 격리 액세스를 구성할 필요가 없습니다.

다음 역할의 사용자에 대해 스팸 격리에 대한 액세스를 구성하는 경우 해당 사용자는 스팸 격리의 메시지를 보고 릴리스하고 삭제할 수 있습니다.

- Email administrator
- 운영자
- Read-only operator
- Help desk user
- 게스트
- 스팸 격리 권한을 가진 맞춤형 사용자 역할

이러한 사용자는 스팸 격리 설정에 액세스할 수 없습니다.

시작하기 전에

스팸 격리에 액세스할 수 있는 사용자 또는 맞춤형 사용자 역할을 만듭니다. 자세한 내용은 에서 맞춤 사용자 역할의 격리 액세스 , 406 페이지에 대한 관리 작업 배포, 401 페이지 정보를 참조하십시오.

단계 **1** 아직 스팸 격리 설정 페이지를 수정하고 있지 않은 경우

a) [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.
b) **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**을 선택합니다.
c) **Edit Settings(**설정 수정**)**Spam Quarantine(스팸 격리) 섹션의 Quarantine Name(격리 이름) 열에서 **Spam Quarantine(**스팸 격리**)** 링크를 클릭합니다.

단계 **2** 추가할 사용자 유형(로컬, 외부 인증 또는 맞춤형 역할)에 대한 링크를 클릭합니다.

사용자 또는 역할을 이미 추가한 경우 모든 해당 사용자 또는 역할을 보려면 사용자 이름이나 역할을 클릭합니다.

단계 **3** 추가할 사용자 또는 역할을 선택합니다.

관리자 권한을 가진 사용자(이메일 관리자 포함)는 스팸 격리에 자동으로 전체 액세스 권한을 가지므로 나열되지 않습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지

메일을 격리할 수신자 제한

메일을 격리하지 않을 수신자 주소 목록을 지정하려면에서 여러 메일 정책(Mail Policies(메일 정책) > Incoming Mail Policy(수신 메일 정책))을 사용할 수 있습니다. 메일 정책의 안티스팸 설정을 구성할 때 격리 대신 'Deliver(전달)' 또는 'Drop(삭제)'을 선택합니다.

스팸 격리 언어

최종 사용자는 창 오른쪽 상단에 있는 Options(옵션) 메뉴에서 스팸 격리의 언어를 선택합니다.

Spam Quarantine(스팸 격리) 페이지 수정

- 스팸 격리 활성화 및 구성 , 281 페이지
- 로컬 대 외부 스팸 격리 , 280 페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지
- 최종 사용자에게 격리된 메시지에 대해 알리기 , 303 페이지

허용 목록 및 차단 목록을 사용하여 발신자 기준으로 이메일 전달 제어

관리자 및 최종 사용자는 스팸 메시지를 식별하는 데 허용 목록과 차단 목록을 사용할 수 있습니다. 허용 목록은 스팸으로 취급되지 않을 발신자 및 도메인을 지정합니다. 차단 목록은 항상 스팸으로 취급될 발신자 및 도메인을 지정합니다.

최종 사용자(이메일 사용자)가 각자의 이메일 계정에 대해 허용 목록과 차단 목록을 관리하도록 허용할 수 있습니다. 예를 들어, 최종 사용자가 더 이상 관심이 없는 메일 목록에서 이메일을 수신할 수 있습니다. 이 발신자의 이메일이 메일 목록에서 자신의 받은 편지함으로 전송되지 않도록 하려면 해당 발신자를 차단 목록에 추가할 수 있습니다. 반면, 스팸으로 취급하고 싶지 않은 특정 발신자의 이메

일이 스팸 격리로 전송되는 경우를 발견할 수 있습니다. 이러한 발신자의 메시지가 격리되지 않도록 하려면 해당 발신자를 허용 목록에 추가할 수 있습니다.

최종 사용자 및 관리자는 설정을 변경할 수 있으며 이러한 변경 사항을 볼 수 있습니다.

관련 주제

- 허용 목록 및 차단 목록의 메시지 처리 , 287 페이지
- 허용 목록 및 차단 목록 활성화 , 288 페이지
- 외부 스팸 격리 및 허용 목록/차단 목록 , 288 페이지
- 허용 목록 및 차단 목록에 발신자 및 도메인 추가(관리자) , 288 페이지
- 허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보 , 294 페이지
- 허용 목록/차단 목록 백업 및 복원 , 296 페이지
- 허용 목록 및 차단 목록 문제 해결, 296 페이지

허용 목록 및 차단 목록의 메시지 처리

허용 목록 또는 차단 목록에 있는 발신자에 대해서도 어플라이언스는 메시지에서 바이러스를 검사하며, 메시지가 콘텐츠 관련 메일 정책의 기준을 충족하는지 확인합니다. 메시지 발신자가 수신자의 허용 목록에 있더라도 검사 설정 및 결과에 따라 메시지가 최종 사용자에게 전달되지 않을 수 있습니다.

허용 목록 및 차단 목록을 활성화하면 어플라이언스는 안티스팸 검사 직전에 허용 목록/차단 목록 데이터베이스를 기준으로 메시지를 검사합니다. 어플라이언스가 허용 목록 또는 차단 목록과 일치하는 발신자나 도메인을 검색하면, 다중 수신자인 경우(그리고 수신자의 허용 목록/차단 목록 설정이 다른 경우) 메시지가 분리됩니다. 예를 들어 메시지가 수신자 A 및 수신자 B에게 전송되는데, 수신자 A는 해당 발신자를 허용 목록에 추가한 반면 수신자 B는 허용 목록이나 차단 목록에 해당 발신자의 항목이 없습니다. 이 경우 메시지는 두 개의 메시지 ID와 함께 둘로 분리됩니다. 수신자 A에게 전송되는 메시지는 *X-SLBL-Result-Safelist* 헤더와 함께 허용 목록 항목으로 표시되는 반면, 수신자 B에 대한 메시지는 안티 스팸 검사 엔진의 검사를 받게 됩니다. 두 메시지는 계속해서 파이프라인을 따라 이동하며(안티바이러스 검사, 콘텐츠 정책 등) 구성된 설정에 따라 처리됩니다.

메시지 발신자 또는 도메인이 차단 목록에 있으면, 허용 목록/차단 목록 기능을 활성화할 때 지정한 차단 목록 작업을 기반으로 전달 동작이 수행됩니다. 허용 목록 전달과 마찬가지로, 서로 다른 허용 목록/차단 목록 설정의 서로 다른 수신자가 있는 경우 메시지가 분리됩니다. 차단 목록에 따라 분리된 메시지는 차단 목록 작업 설정에 따라 격리되거나 삭제됩니다. 차단 목록 작업이 격리로 구성된 경우 메시지가 검사되고 결국 격리됩니다. 차단 목록 작업이 삭제로 구성된 경우 허용 목록/차단 목록 검사 직후 메시지가 삭제됩니다.

허용 목록 및 차단 목록은 스팸 격리에서 유지 관리되므로 전달 동작도 다른 안티스팸 설정에 따라 달라집니다. 예를 들어 안티스팸 검사를 건너뛰도록 HAT(Host Access Table)의 "Accept(수락)" 메일 플로우 정책을 구성한 경우, 해당 리스너에서 메일을 수신하는 사용자는 수신한 메일에 허용 목록 및 차단 목록 설정을 적용할 수 없습니다. 마찬가지로, 특정 메시지 수신자에 대해 안티스팸 검사를 건너뛰는 메일 플로우 정책을 만들면 해당 수신자에게는 허용 목록 및 차단 목록 설정이 적용되지 않습니다.

관련 주제

- 허용 목록 및 차단 목록 활성화 , 288 페이지
- 외부 스팸 격리 및 허용 목록/차단 목록 , 288 페이지

허용 목록 및 차단 목록 활성화

시작하기 전에

- 스팸 격리를 활성화해야 합니다. 중앙 집중식 스팸 격리 설정 , 280 페이지를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **3** **End-User Safelist/Blocklist (Spam Quarantine)(**최종 사용자 허용 목록/차단 목록**(**스팸 격리**))** 섹션에서 **Enable(**활성화**)**을 선택합니다.

단계 **4** **Enable End User Safelist/Blocklist Feature(**최종 사용자 허용 목록/차단 목록 기능 활성화**)**를 선택합니다.

단계 **5** **Maximum List Items Per User(**사용자당 최대 목록 항목**)**를 지정합니다.

이 값은 각 목록에서 각 수신자별 최대 주소 또는 도메인 수입니다. 사용자당 다수의 목록 항목을 허용하면 시스템 성능이 저하될 수 있습니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

외부 스팸 격리 및 허용 목록/차단 목록

Email Security Appliance는 수신 메일을 처리할 때 허용 목록 및 차단 목록의 발신자를 평가하므로, 수신 메일에 적용하려면 Security Management Appliance에 저장된 허용 목록 및 차단 목록을 Email Security Appliance로 전송해야 합니다. Security Management Appliance에서 허용 목록/차단 목록 기능을 구성할 때 이러한 업데이트의 빈도를 구성합니다.

허용 목록 및 차단 목록에 발신자 및 도메인 추가(관리자)

허용 목록 및 차단 목록은 스팸 격리 인터페이스를 통해 관리합니다.

많은 수신자(조직의 최종 사용자)가 특정 발신자 또는 도메인을 화이트리스트 또는 블랙리스트에 추가했는지도 확인할 수 있습니다.

관리자는 각 최종 사용자가 보고 작업하는 동일한 항목의 상위 집합을 보고 관리합니다.

시작하기 전에

- 스팸 격리에 액세스할 수 있는지 확인합니다. 스팸 격리에 액세스(관리 사용자), 306 페이지를 참조하십시오.
- 허용 목록/차단 목록에 대한 액세스를 활성화합니다. 허용 목록 및 차단 목록 활성화 , 288 페이지를 참조하십시오.
- (선택 사항) 이 섹션의 절차를 사용하여 이러한 목록을 작성하는 대신 허용 목록/차단 목록을 가져오려면 허용 목록/차단 목록 백업 및 복원 , 296 페이지에 설명된 프로세스를 사용합니다.
- 허용 목록 및 차단 목록 항목의 필수 형식을 이해합니다. 허용 목록 및 차단 목록 항목의 구문 , 293 페이지를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 **Quarantine(격리) > Spam Quarantine(스팸 격리) > Search(검색)**를 클릭합니다.

또는

Email(이메일) > Message Quarantine(메시지 격리) > Spam Quarantine(스팸 격리)를 선택하고 페이지의 오른쪽 상단에서 **Options(옵션)** 드롭다운 메뉴를 선택합니다.

단계 **2** **Safelist(허용 목록)** 또는 **Blocklist(차단 목록)**를 선택합니다.

단계 **3** (선택 사항) 발신자 또는 수신자를 검색합니다.

단계 **4** 다음 중 하나를 수행합니다.

변경 후	수행해야 할 작업
한 명의 수신자에 대해 여러 발신자 추가	새로운 웹 인터페이스에서 수신자에 대해 여러 발신자를 추가하려면 다음을 수행합니다. 1. **Recipient(**수신자**)** 탭을 선택합니다. 2. 수신자 주소 및 발신자 목록을 추가하려면 + 아이콘을 클릭합니다. 3. 수신자의 이메일 주소를 입력합니다. 4. 발신자 이메일 주소 및 도메인을 입력합니다. 각 항목을 별도의 줄에 입력하거나, 쉼표로 각 항목을 구분합니다. 5. ✓을 클릭하여 항목을 저장합니다. 기존 발신자 주소를 수정하려면 필요한 수신자 주소 옆의 확인란을 선택하고 편집 아이콘을 클릭하여 발신자 주소를 수정하고 ✓을 클릭하여 항목을 저장합니다. 레거시 웹 인터페이스에서 수신자에 대해 여러 발신자를 추가하려면 다음을 수행합니다. 1. **View by: Recipient(**보기 기준**:** 수신자**)**를 선택합니다. 2. **Add(**추가**)**를 클릭하거나, 수신자에 대해 **Edit(**수정**)**을 클릭합니다. 3. 수신자 이메일 주소를 입력하거나 수정합니다. 4. 발신자 이메일 주소 및 도메인을 입력합니다. 각 항목을 별도의 줄에 입력하거나, 쉼표로 각 항목을 구분합니다. 5. **Submit(**제출**)**을 클릭합니다.

변경 후	수행해야 할 작업
한 명의 발신자에 대해 여러 수신자 추가	새로운 웹 인터페이스에서 발신자에 대해 여러 수신자를 추가하려면 다음을 수행합니다. 1. **Sender(**발신자**)** 탭을 선택합니다. 2. 발신자 주소 및 수신자 목록을 추가하려면 + 아이콘을 클릭합니다. 3. 발신자 주소 또는 도메인을 입력합니다. 4. 수신자의 이메일 주소를 입력합니다. 각 항목을 별도의 줄에 입력하거나, 쉼표로 각 항목을 구분합니다. 5. ✓을 클릭하여 항목을 저장합니다. 기존 수신자 주소를 수정하려면 필요한 발신자 주소 옆의 확인란을 선택하고 편집 아이콘을 클릭하여 수신자 주소를 수정하고 ✓을 클릭하여 항목을 저장합니다. 레거시 웹 인터페이스에서 발신자에 대해 여러 수신자를 추가하려면 다음을 수행합니다. 1. **View by: Sender(**보기 기준**:** 발신자**)**를 선택합니다. 2. **Add(**추가**)**를 클릭하거나, 발신자에 대해 **Edit(**수정**)**을 클릭합니다. 3. 발신자 주소 또는 도메인을 입력하거나 수정합니다. 4. 수신자 이메일 주소를 입력합니다. 각 항목을 별도의 줄에 입력하거나, 쉼표로 각 항목을 구분합니다. 5. **Submit(**제출**)**을 클릭합니다.
한 명의 수신자와 관련된 모든 발신자 삭제	새로운 웹 인터페이스에서 한 명의 수신자와 관련된 모든 발신자를 삭제하려면 다음을 수행합니다. 1. 수신자 또는 발신자 주소 옆에 있는 확인란을 선택하여 항목을 선택합니다. 모든 항목을 선택하고 삭제할 수 있습니다. 2. 테이블 행 전체를 삭제하려면 휴지통 아이콘을 클릭합니다. 레거시 웹 인터페이스에서 한 명의 수신자와 관련된 모든 발신자를 삭제하려면 다음을 수행합니다. 1. **View by(**보기 기준**)** 옵션을 선택합니다. 2. 테이블 행 전체를 삭제하려면 휴지통 아이콘을 클릭합니다.

변경 후	수행해야 할 작업
한 명의 발신자와 관련된 모든 수신자 삭제	새로운 웹 인터페이스에서 한 명의 발신자와 관련된 모든 수신자를 삭제하려면 다음을 수행합니다. 1. 수신자 또는 발신자 주소 옆에 있는 확인란을 선택하여 항목을 선택합니다. 모든 항목을 선택하고 삭제할 수 있습니다. 2. 테이블 행 전체를 삭제하려면 휴지통 아이콘을 클릭합니다. 레거시 웹 인터페이스에서 한 명의 발신자와 관련된 모든 수신자를 삭제하려면 다음을 수행합니다. 1. **View by**(보기 기준) 옵션을 선택합니다. 2. 테이블 행 전체를 삭제하려면 휴지통 아이콘을 클릭합니다.
한 명의 수신자에 대해 개별 발신자 삭제	새로운 웹 인터페이스에서 수신자에 대해 개별 발신자를 삭제하려면 다음을 수행합니다. 1. 수신자 또는 발신자 주소 옆에 있는 확인란을 선택하여 항목을 선택합니다. 여러 항목을 선택하고 삭제할 수 있습니다. 2. 편집 아이콘을 클릭하여 개별 수신자 또는 발신자를 수정합니다. 3. 텍스트 상자에서 항목을 추가 또는 제거합니다. 항목을 적어도 하나는 남겨두어야 합니다. 4. ✓을 클릭하여 항목을 저장합니다. 레거시 웹 인터페이스에서 수신자에 대해 개별 발신자를 삭제하려면 다음을 수행합니다. 1. **View by**(보기 기준) 옵션을 선택합니다. 2. 개별 수신자 또는 발신자에 대해 **Edit**(수정)을 클릭합니다. 3. 텍스트 상자에서 항목을 추가 또는 제거합니다. 항목을 적어도 하나는 남겨두어야 합니다. 4. **Submit**(제출)을 클릭합니다.

변경 후	수행해야 할 작업
한 명의 발신자에 대해 개별 수신자 삭제	새로운 웹 인터페이스에서 발신자에 대해 개별 수신자를 삭제하려면 다음을 수행합니다. 1. 수신자 또는 발신자 주소 옆에 있는 확인란을 선택하여 항목을 선택합니다. 여러 항목을 선택하고 삭제할 수 있습니다. 2. 편집 아이콘을 클릭하여 개별 수신자 또는 발신자를 수정합니다. 3. 텍스트 상자에서 항목을 추가 또는 제거합니다. 항목을 적어도 하나는 남겨두어야 합니다. 4. ✓을 클릭하여 항목을 저장합니다. 레거시 웹 인터페이스에서 수신자에 대해 개별 발신자를 삭제하려면 다음을 수행합니다. 1. **View by**(보기 기준) 옵션을 선택합니다. 2. 개별 수신자 또는 발신자에 대해 **Edit**(수정)을 클릭합니다. 3. 텍스트 상자에서 항목을 추가 또는 제거합니다. 항목을 적어도 하나는 남겨두어야 합니다. 4. **Submit**(제출)을 클릭합니다.

다음에 수행할 작업

관련 주제

- 허용 목록 및 차단 목록 항목의 구문 , 293 페이지
- 모든 허용 목록 및 차단 목록 지우기 , 294 페이지

허용 목록 및 차단 목록 항목의 구문

다음 형식을 사용하여 허용 목록 및 차단 목록에 발신자를 추가할 수 있습니다.

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

동일한 항목(예: 발신자 주소 또는 도메인)을 동시에 허용 목록과 차단 목록에 모두 포함할 수는 없습니다. 그러나 어떤 도메인이 허용 목록에 있고 그 도메인에 속한 발신자 이메일 주소가 차단 목록에 포함되는 것은(또는 그 반대의 경우도) 가능하며, 두 규칙 모두 적용됩니다. 예를 들어 *example.com*이 허용 목록에 있더라도 *george@example.com*을 차단 목록에 추가할 수 있습니다. 이 경우 어플라이언스는 *example.com*에서 오는 모든 메일을 스팸 검사 없이 전달하되, *george@example.com*의 메일만 스팸으로 처리합니다.

.domain.com 구문을 사용하여 하위 도메인의 범위를 허용하거나 차단할 수는 없습니다. 그러나 *server.domain.com* 구문을 사용하여 특정 도메인을 차단하는 것은 가능합니다.

모든 허용 목록 및 차단 목록 지우기

모든 발신자와 모든 수신자를 포함하여 모든 허용 목록 및 차단 목록 항목을 삭제해야 하는 경우 허용 목록/차단 목록 백업 및 복원 , 296 페이지의 절차를 사용하여 항목이 없는 파일을 가져옵니다.

허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보

최종 사용자는 스팸 격리를 통해 허용 목록 및 차단 목록에 액세스합니다. 스팸 격리에 대한 최종 사용자 액세스를 구성하려면 최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정 , 300 페이지 섹션을 참조하십시오.

최종 사용자에게 스팸 격리의 URL과 그 아래에 설명(해당되는 경우)을 제공할 수 있습니다.

관련 주제

- 허용 목록에 항목 추가(최종 사용자) , 294 페이지
- 차단 목록에 발신자 추가(최종 사용자) , 295 페이지

허용 목록에 항목 추가(최종 사용자)

참고 허용 목록에 있는 발신자가 보낸 메시지 전달은 시스템에 구성된 설정에 따라 다릅니다. 허용 목록 및 차단 목록의 메시지 처리 , 287 페이지를 참조하십시오.

두 가지 방법으로 허용 목록에 발신자를 추가할 수 있습니다.

- 격리된 메시지의 발신자를 허용 목록에 추가 , 294 페이지
- 격리된 메시지 없는 허용 목록에 발신자 추가 , 295 페이지

격리된 메시지의 발신자를 허용 목록에 추가

메시지가 스팸 격리로 전송된 경우 최종 사용자는 허용 목록에 발신자를 추가할 수 있습니다.

단계 **1** Spam Quarantine(스팸 격리)을 선택합니다.

단계 **2** [새 웹 인터페이스에만 해당] **Safelist(**허용 목록**)**를 선택하고 메시지 옆에 있는 확인란을 선택합니다.

단계 **3** [새 웹 인터페이스에만 해당] 메시지를 릴리스하고 허용 목록에 추가하려면 **Release and Add to Safelist(**릴리스한 후 허용 목록에 추가**)** 아이콘을 클릭합니다.

단계 **4** 드롭다운 메뉴에서 **Safelist(**허용 목록**)**를 선택하고 **Release and Add to Safelist(**릴리스한 후 허용 목록에 추가**)**를 선택합니다.

지정된 메일의 봉투 발신자 및 from 헤더 모두 허용 목록에 추가되고 릴리스된 메시지는 대상 대기열로 직접 이동하며, 이메일 파이프라인에서 추가 작업 대기열 처리를 건너뜁니다.

격리된 메시지 없는 허용 목록에 발신자 추가

단계 **1** 브라우저를 통해 스팸 격리에 액세스합니다.

단계 **2** [새 웹 인터페이스에만 해당] **Safelist(**허용 목록**)**를 선택합니다.

단계 **3** [새 웹 인터페이스에만 해당] 이메일 주소 또는 도메인을 입력합니다. 쉼표로 구분하여 여러 도메인 및 이메일 주소를 입력할 수 있습니다.

단계 **4** [새 웹 인터페이스에만 해당] ✓ 을 클릭하여 항목을 저장합니다.

단계 **5** 페이지의 오른쪽 상단에 있는 **Options(**옵션**)** 드롭다운 메뉴를 선택합니다.

단계 **6** **Safelist(**허용 목록**)**를 선택합니다.

단계 **7** Safelist(허용 목록) 대화 상자에서 이메일 주소 또는 도메인을 입력합니다. 쉼표로 구분하여 여러 도메인 및 이메일 주소를 입력할 수 있습니다.

단계 **8** **Add to List(**목록에 추가**)**를 클릭합니다.

차단 목록에 발신자 추가(최종 사용자)

차단 목록의 발신자가 보낸 메시지는 관리자가 정의한 허용 목록/차단 목록 작업 설정에 따라 거부되거나 격리됩니다.

참고 차단 목록 항목은 이 절차를 사용해서만 추가할 수 있습니다.

단계 **1** 스팸 격리에 로그인합니다.

단계 **2** [새 웹 인터페이스에만 해당] **Blocklist(**차단 목록**)**를 선택하고 차단 목록에 추가할 도메인 또는 이메일 주소를 입력합니다. 쉼표로 구분하여 여러 도메인 및 이메일 주소를 입력할 수 있습니다.

단계 **3** [새 웹 인터페이스에만 해당] 항목을 저장하려면 ✓ 을 클릭합니다.

단계 **4** 페이지의 오른쪽 상단에 있는 **Options(**옵션**)** 드롭다운 메뉴에서 **Blocklist(**차단 목록**)**를 선택합니다.

단계 **5** 차단 목록에 추가할 도메인 또는 이메일 주소를 입력합니다. 쉼표로 구분하여 여러 도메인 및 이메일 주소를 입력할 수 있습니다.

단계 **6** **Add to List**(목록에 추가)를 클릭합니다.

허용 목록/차단 목록 백업 및 복원

어플라이언스를 업그레이드하거나 설치 마법사를 실행하기 전에 허용 목록/차단 목록 데이터베이스를 백업해야 합니다. 허용 목록/차단 목록 정보는 어플라이언스 구성 설정을 포함하는 기본 XML 구성 파일에 포함되지 않습니다.

허용 목록/차단 목록 항목은 또한 Security Management Appliance의 다른 데이터와 함께 백업할 수 있습니다. Security Management Appliance 데이터 백업 , 440 페이지를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Configuration File**(구성 파일)을 선택합니다.

단계 **3** **End-User Safelist/Blocklist Database (Spam Quarantine)**(최종 사용자 허용 목록/차단 목록 데이터베이스(스팸 격리)) 섹션으로 스크롤합니다.

변경 후	수행해야 할 작업
허용 목록/차단 목록 내보내기	.csv 파일의 경로 및 파일 이름을 확인하고 필요한 대로 수정합니다. **Backup Now**(지금 백업)를 클릭합니다. 어플라이언스에서는 다음 명명 규칙을 사용하여 .csv 파일을 /configuration 디렉터리에 저장합니다. *slbl<serial number><timestamp>.csv*
허용 목록/차단 목록 가져오기	주의 이 프로세스는 모든 사용자에 대한 허용 목록 및 차단 목록에 있는 모든 기존 항목을 덮어씁니다. **Select File to Restore**(복원할 파일 선택)를 클릭합니다. configuration 디렉터리의 파일 목록에서 원하는 파일을 선택합니다. 복원할 허용 목록/차단 목록 백업 파일을 선택합니다. **Restore**(복원)를 클릭합니다.

허용 목록 및 차단 목록 문제 해결

허용 목록 및 차단 목록의 문제를 해결하려면 로그 파일 또는 시스템 알림을 볼 수 있습니다.

허용 목록/차단 목록 설정 때문에 이메일이 차단되면 ISQ_log 파일 또는 antispam 로그 파일에 작업이 기록됩니다. 허용 목록에 있는 이메일은 *X-SLBL-Result-Safelist* 헤더와 함께 허용 목록 항목으로 표시됩니다. 차단 목록에 있는 이메일은 *X-SLBL-Result-Blocklist* 헤더와 함께 차단 목록 항목으로 표시됩니다.

데이터베이스가 생성되거나 업데이트될 때 또는 데이터베이스를 수정하거나 허용 목록/차단 목록 프로세스를 실행하는 동안 오류가 발생하는 경우 알림이 전송됩니다.

알림에 대한 자세한 내용은 경고 관리, 464 페이지 섹션을 참조하십시오.

로그 파일에 대한 자세한 내용은 로깅, 503 페이지 를 참조하십시오.

관련 주제

- 허용 목록 발신자의 메시지가 전달되지 않음 , 297 페이지

허용 목록 발신자의 메시지가 전달되지 않음

문제

허용 목록 발신자의 메시지가 전달되지 않았습니다.

솔루션

가능한 원인

- 악성코드 또는 콘텐츠 위반 때문에 메시지가 삭제되었습니다. 허용 목록 및 차단 목록의 메시지 처리 , 287 페이지를 참조하십시오.
- 여러 어플라이언스가 있고 발신자가 최근에 허용 목록에 추가된 경우, 메시지가 처리된 시점에 허용 목록/차단 목록이 동기화되지 않았을 수 있습니다. 외부 스팸 격리 및 허용 목록/차단 목록 , 288 페이지 를 참조하십시오.

최종 사용자에 대한 스팸 관리 기능 구성

변경 후	확인
최종 사용자의 스팸 관리 기능 액세스에 대한 여러 인증 방법의 이점과 한계를 이해합니다.	스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지 및 하위 섹션
최종 사용자가 브라우저를 통해 직접 스팸 격리에 액세스하도록 허용합니다.	스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 298 페이지
사용자에게 주소가 지정된 메시지가 스팸 격리로 라우팅될 때 해당 사용자에게 알림을 전송합니다. 스팸 격리에 액세스하기 위한 링크를 알림에 포함할 수 있습니다.	최종 사용자에게 격리된 메시지에 대해 알리기 , 303 페이지

변경 후	확인
사용자가 안전하다고 생각하는 발신자 및 스팸이나 기타 원치 않는 메일을 전송한다고 생각하는 발신자의 이메일 주소와 도메인을 지정하도록 허용합니다.	허용 목록 및 차단 목록을 사용하여 발신자 기준으로 이메일 전달 제어 , 286 페이지

관련 주제

- 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 298 페이지
- 최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정 , 300 페이지
- 최종 사용자에게 격리된 메시지에 대해 알리기 , 303 페이지

스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션

참고 사서함 인증을 사용하는 경우 사용자는 이메일 별칭으로 주소가 지정된 메시지를 볼 수 없습니다.

엔드 유저 스팸 격리 액세스의 경우	수행해야 할 작업
웹 브라우저를 통해 직접, 인증 필요 및 알림의 링크를 통해, 인증 필요	1. End User Quarantine Access(엔드 유저 격리 액세스) 설정에서 **LDAP, SAML 2.0** 또는 **Mailbox (IMAP/POP)(**사서함 **(IMAP/POP))**를 선택합니다. 2. Spam Notifications(스팸 알림) 설정에서 **Enable login without credentials for quarantine access(**격리 액세스를 위한 자격 증명 없이 로그인 활성화**)**의 선택을 취소합니다.
웹 브라우저를 통해 직접, 인증 필요 및 알림의 링크를 통해, 인증 필요 없음	1. End User Quarantine Access(엔드 유저 격리 액세스) 설정에서 **LDAP, SAML 2.0** 또는 **Mailbox (IMAP/POP)(**사서함 **(IMAP/POP))**를 선택합니다. 2. Spam Notifications(스팸 알림) 설정에서 **Enable login without credentials for quarantine access(**격리 액세스를 위한 자격 증명 없이 로그인 활성화**)**를 선택합니다.
알림의 링크를 통해서만, 인증 필요 없음	End User Quarantine Access(최종 사용자 격리 액세스) 설정에서 인증 방법으로 **None(**없음**)**을 선택합니다.
액세스 없음	End User Quarantine Access(최종 사용자 격리 액세스) 설정에서 **Enable End-User Quarantine Access(**최종 사용자 격리 액세스 활성화**)**의 선택을 취소합니다.

관련 주제

- LDAP 인증 프로세스 , 299 페이지
- IMAP/POP 인증 프로세스 , 299 페이지

- SAML 2.0 인증 프로세스, 300 페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지
- 최종 사용자에게 격리된 메시지에 대해 알리기 , 303 페이지
- 스팸 격리를 사용하도록 LDAP 구성, 378 페이지
- 허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보 , 294 페이지

LDAP 인증 프로세스

1. 사용자가 웹 UI 로그인 페이지에 자신의 사용자 이름 및 암호를 입력합니다.
2. 익명 검색을 수행하여 또는 지정된 "서버 로그인" DN 및 암호가 있는 인증된 사용자로서 스팸 격리가 지정된 LDAP 서버에 연결합니다. Active Directory의 경우 일반적으로 "전역 카탈로그 포트"(6000s에 있음)에서 서버를 연결하거나, 검색을 수행하기 위해 스팸 격리가 바인딩할 수 있는 권한이 낮은 LDAP 사용자를 만들어야 합니다.
3. 그러면 스팸 격리는 지정된 BaseDN 및 쿼리 문자열을 사용하여 사용자를 검색합니다. 사용자의 LDAP 레코드가 발견되면 스팸 격리는 해당 레코드의 DN을 추출하고, 사용자가 원래 입력한 사용자 레코드의 DN 및 암호를 사용하여 디렉터리에 바인딩하려고 시도합니다. 암호 확인이 성공하면 사용자가 적절하게 인증되지만, 스팸 격리는 여전히 해당 사용자에게 어떤 사서함의 내용을 보여줄지를 결정해야 합니다.
4. 메시지는 수신자의 봉투 주소를 사용하여 스팸 격리에 저장됩니다. LDAP에 대해 사용자의 암호가 검증되면 스팸 격리는 LDAP 레코드에서 "기본 메일 특성"을 검색하여 사용자에게 어떤 격리 메시지를 보여줄지를 결정합니다. "기본 이메일 특성"은 여러 이메일 주소를 포함할 수 있으며, 이러한 주소는 인증된 사용자에 대해 격리에서 어떤 봉투 주소를 표시해야 할지를 결정하는 데 사용됩니다.

관련 주제

- 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 298 페이지
- LDAP와의 통합, 377 페이지

IMAP/POP 인증 프로세스

1. 메일 서버 구성에 따라 사용자는 웹 UI 로그인 페이지에 사용자 이름(joe) 또는 이메일 주소(joe@example.com) 및 암호를 입력합니다. 전체 이메일 주소를 입력해야 할지 사용자 이름만 입력하면 될지를 사용자에게 알려주기 위해 로그인 페이지 메시지를 수정할 수 있습니다(스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지 참조).
2. 스팸 격리는 IMAP 또는 POP 서버에 연결하고, 입력된 로그인(사용자 이름 또는 이메일 주소) 및 암호를 사용하여 IMAP/POP 서버에 로그인하려고 시도합니다. 암호가 수락되면 사용자는 인증된 것으로 간주되며, IMAP/POP 서버에서 스팸 격리가 즉시 로그아웃됩니다.
3. 사용자가 인증되면 스팸 격리는 이메일 주소를 기반으로 사용자의 이메일을 나열합니다.
    - 베어(bare) 사용자 이름(예: joe)에 추가할 도메인을 지정하도록 스팸 격리를 구성한 경우 해당 도메인이 추가되며 격리에서 일치하는 봉투를 검색하는 데 인증된 이메일 주소가 사용됩니다.
    - 그렇지 않은 경우 스팸 격리는 입력된 이메일 주소를 사용하여 일치하는 봉투를 검색합니다.

IMAP에 대한 자세한 내용은 University of Washington 웹사이트를 참조하십시오.

http://www.washington.edu/imap/

SAML 2.0 인증 프로세스

Cisco Content Security Management Appliance 설명서에서 *SAML 2.0*을 사용하는 *SSO* 섹션을 참조하십시오.

최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정

프로시저

	명령 또는 동작	목적
단계 **1**	최종 사용자의 스팸 관리 기능 액세스에 대한 여러 인증 방법의 이점과 한계를 이해합니다.	*Cisco Content Security Management Appliance* 설명서에서 *SAML 2.0*을 사용하는 *SSO* 섹션을 참조하십시오.
단계 **2**	LDAP를 사용하여 엔드 유저를 인증하려면 **System Administration(**시스템 관리**) > LDAP > LDAP Server Profile(LDAP** 서버 프로필**)** 페이지의 **Spam Quarantine End-User Authentication Query(**스팸 격리 엔드 유저 인증 쿼리**)** 설정을 비롯한 LDAP 서버 프로필을 구성합니다. 예제: `If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the` **`System Administration`** `>` **`SAML`** `page.`	LDAP와의 통합, 377 페이지 및 하위 섹션 SAML 2.0을 사용하는 SSO, 491 페이지
단계 **3**	스팸 격리에 대한 최종 사용자 액세스를 구성합니다.	스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지
단계 **4**	스팸 격리에 대한 최종 사용자 액세스용 URL을 결정합니다.	스팸 격리에 대한 최종 사용자 액세스용 URL 결정, 302 페이지

다음에 수행할 작업

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지
- 스팸 격리에 대한 최종 사용자 액세스용 URL 결정, 302 페이지
- 최종 사용자에게 표시할 메시지 , 302 페이지

스팸 격리에 대한 최종 사용자 액세스 구성

최종 사용자 액세스의 활성화 여부와 상관없이 관리 사용자는 스팸 격리에 액세스할 수 있습니다.

시작하기 전에

스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 298 페이지의 요구 사항을 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **3** **Edit Settings(**설정 수정**)** 링크를 클릭합니다.

단계 **4** **End-User Quarantine Access(**최종 사용자 격리 액세스**)** 섹션으로 스크롤합니다.

단계 **5** **Enable End-User Quarantine Access(**최종 사용자 격리 액세스 활성화**)**를 선택합니다.

단계 **6** 최종 사용자가 격리된 메시지를 보려고 할 때 이들을 인증하는 데 사용할 방법을 지정합니다.

선택 옵션	추가 정보
None	—
Mailbox(IMAP/POP)	인증에 사용할 LDAP 디렉터리가 없는 사이트의 경우 격리는 사서함이 있는 표준 기반 IMAP 또는 POP 서버에 대해 이메일 주소와 암호를 검증할 수 있습니다. 스팸 격리에 로그인할 때 엔드 유저는 전체 이메일 주소 및 사서함 암호를 입력합니다. POP 서버가 배너에서 APOP 지원을 광고하는 경우 보안상의 이유로(즉, 암호를 암호화 없이 전송하지 않도록) Cisco 어플라이언스는 APOP만 사용합니다. APOP가 일부 또는 전체 사용자에 대해 지원되지 않으면 APOP를 광고하지 않도록 POP 서버를 다시 구성해야 합니다. SSL을 사용하도록 서버를 구성한 경우 SSL을 선택합니다. 사용자가 사용자 이름만 입력하는 경우 자동으로 이메일 주소를 완성하기 위해 추가할 도메인을 지정할 수 있습니다. "인증되지 않은 사용자 이름에 도메인 추가"에 로그인하는 사용자를 위한 봉투의 도메인을 입력합니다.
LDAP	이 항목의 '시작하기 전에' 섹션에서 참조하는 섹션에 설명된 대로 LDAP 설정을 구성합니다.
SAML 2.0	스팸 격리에 대해 Single Sign-On을 활성화합니다. 이 옵션을 사용하기 전에 Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > SAML 페이지에서 모든 설정을 구성했는지 확인입니다. *Cisco Content Security Management Appliance* 설명서에서 *SAML 2.0*을 사용하는 *SSO* 섹션을 참조하십시오.

단계 **7** 메시지가 릴리스되기 전에 메시지 본문을 표시할지 여부를 지정합니다.

이 확인란을 선택하면 사용자는 스팸 격리 페이지를 통해 메시지 본문을 볼 수 없습니다. 격리된 메시지의 본문을 보려면 사용자는 메시지를 릴리스하고 각자의 메일 애플리케이션(예: Microsoft Outlook)을 이용해야 합니다. 정책 및 규정 준수에 이 기능을 사용할 수 있습니다(예: 규정에서 모든 검토한 이메일을 보관하도록 요구하는 경우).

단계 **8** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

(선택 사항) 아직 하지 않은 경우, 사용자가 스팸 격리에 액세스할 때 표시되는 페이지를 맞춤화합니다. 스팸 격리 활성화 및 구성 , 281 페이지의 설정 설명을 참조하십시오.

스팸 격리에 대한 최종 사용자 액세스용 URL 결정

최종 사용자가 스팸 격리에 직접 액세스하기 위해 사용할 수 있는 URL은 시스템의 호스트 이름 및 격리가 활성화된 IP 인터페이스에 구성된 설정(HTTP/S 및 포트 번호)으로 만들어집니다. 예: `HTTP://mail3.example.com:82`

엔드 유저는 이제 다음 방법 중 하나를 사용하여 새로운 웹 인터페이스의 스팸 격리에 액세스할 수 있습니다.

- `trailblazerconfig` CLI 명령이 활성화된 경우 다음 URL 사용 - `https://example.com:<trailblazer-https-port>/euq-login`

  여기서 `example.com`은 어플라이언스 호스트 이름이고, `<trailblazer-https-port>`는 어플라이언스에 구성된 trailblazer HTTPS 포트입니다.

- `trailblazerconfig` CLI 명령이 비활성화된 경우 다음 URL 사용 - `https://example.com:<https-port>/euq-login`

  여기서 `example.com`은 어플라이언스 호스트 이름이고, `<https-port>`는 어플라이언스에 구성된 HTTPS 포트입니다.

참고 로컬 및 외부에서 인증된 사용자는 엔드 유저 Spam Qurantine(스팸 격리) 포털에 로그인할 수 없습니다.

최종 사용자에게 표시할 메시지

일반적으로 최종 사용자는 스팸 격리에서 자신의 메시지만 볼 수 있습니다.

액세스 방법(알림을 통해 또는 웹 브라우저를 통해 직접) 및 인증 방법(LDAP 또는 IMAP/POP)에 따라 사용자는 스팸 격리에서 여러 이메일 주소의 메일을 볼 수 있습니다.

LDAP 인증이 사용될 때 Primary Email(기본 이메일) 특성에 LDAP 디렉터리의 여러 값이 포함되어 있으면 그러한 모든 값(주소)이 사용자와 연결됩니다. 따라서 LDAP 디렉터리의 최종 사용자와 연결된 모든 이메일 주소로 지정된 격리된 메시지가 격리에 표시됩니다.

인증 방법이 IMAP/POP인 경우 또는 사용자가 알림을 통해 직접 격리에 액세스하는 경우 격리에는 해당 사용자의 이메일 주소(또는 알림이 전송된 주소)에 대한 메시지만 표시됩니다.

사용자가 구성원으로 속해 있는 별칭으로 전송되는 메시지에 대한 자세한 내용은 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 304 페이지 섹션을 참조하십시오.

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지
- 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 304 페이지

최종 사용자에게 격리된 메시지에 대해 알리기

스팸 격리에 스팸 메시지 및 의심스런 스팸 메시지가 있는 일부 또는 전체 사용자에게 알림 이메일을 전송하도록 시스템을 구성할 수 있습니다.

기본적으로 스팸 알림은 사용자의 격리된 메시지를 나열합니다. 또한 알림에 스팸 격리에서 격리된 메시지를 보기 위해 사용자가 클릭할 수 있는 링크를 포함할 수 있습니다. 이러한 링크는 만료되지 않습니다. 사용자는 격리된 메시지를 보고 이를 받은 편지함으로 전달할지 아니면 삭제할지를 결정할 수 있습니다.

참고 클러스터 구성에서, 시스템 레벨에서만 알림을 수신할 사용자를 선택할 수 있습니다.

시작하기 전에

- 최종 사용자는 알림에 나열된 메시지를 관리하려면 스팸 격리에 액세스할 수 있어야 합니다. 스팸 격리에 대한 최종 사용자 액세스 구성 , 300 페이지를 참조하십시오.
- 알림을 사용하여 스팸을 관리하기 위한 인증 옵션을 이해합니다. 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 298 페이지를 참조하십시오.
- 최종 사용자가 여러 별칭으로 이메일을 받는 경우 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 304 페이지 섹션을 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 집중식 서비스) > **Spam Quarantine**(스팸 격리)을 선택합니다.

단계 **3** **Edit Settings**(설정 수정) 링크를 클릭합니다.

단계 **4** **Spam Notifications**(스팸 알림) 섹션으로 스크롤합니다.

단계 **5** **Enable Spam Notification**(스팸 알림 활성화)을 선택합니다.

단계 **6** 옵션을 지정합니다.

메시지 본문을 맞춤화하려면

a) (선택 사항) 기본 텍스트 및 변수를 맞춤화합니다.

변수를 삽입하려면 삽입할 위치에 커서를 두고 오른쪽의 Message Variables(메시지 변수) 목록에서 변수의 이름을 클릭합니다. 또는 변수를 입력합니다.

다음 메시지 변수는 특정 최종 사용자에 대한 실제 값으로 확장됩니다.

- 새 메시지 개수(%new_message_count%) - 사용자가 마지막으로 로그인한 이후 새 메시지 수입니다.

- 총 메시지 개수(%total_message_count%) - 사용자에 대한 스팸 격리에 있는 메시지 수입니다.
- 메시지 만료까지 남은 일수(%days_until_expire%)
- 격리 **URL**(%quarantine_url%) - 격리에 로그인하여 메시지를 보기 위한 URL입니다.
- 사용자 이름(%username%)
- 새 메시지 테이블(%new_quarantine_messages%) - 사용자의 새로 격리된 메시지 목록으로, 발신자, 메시지 제목, 날짜 및 메시지를 릴리스할 링크를 보여줍니다. 사용자가 메시지 제목을 클릭하여 스팸 격리의 메시지를 봅니다.
- 제목이 없는 새 메시지 테이블(%new_quarantine_messages_no_subject%) - 새 메시지 테이블과 유사하지만 각 메시지의 제목 대신 "View Message(메시지 보기)" 링크만 표시됩니다.

b) 이 페이지의 End User Quarantine Access(최종 사용자 격리 액세스) 섹션에서 인증 방법을 활성화한 경우

- 사용자가 알림의 링크를 클릭하여 액세스할 때 자동으로 스팸 격리에 로그인되도록 하려면 **Enable login without credentials for quarantine access(**격리 액세스를 위한 자격 증명 없이 로그인 활성화**)**를 선택합니다. 최종 사용자는 알림의 "Release" 링크를 클릭하여 간단하게 메시지를 릴리스할 수 있습니다.
- 사용자가 알림의 링크를 클릭하여 액세스할 때 스팸 격리에 로그인하도록 요구하려면 이 옵션의 선택을 취소합니다. 최종 사용자는 알림의 "Release" 링크를 클릭하여 간단하게 메시지를 릴리스할 수 없습니다.

c) 메시지가 원하는 모습인지 확인하려면 **Preview Message(**메시지 미리 보기**)**를 클릭합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

최종 사용자가 이러한 알림을 받는지 확인하려면, 메일 애플리케이션(예: Microsoft Outlook 또는 Mozilla Thunderbird)의 정크 메일 설정에서 "화이트리스트"에 스팸 격리 알림 이메일에 대한 From: 주소를 추가하도록 권장할 수 있습니다.

관련 주제

- 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 304 페이지
- 알림 테스트, 305 페이지
- 스팸 알림 문제 해결 , 305 페이지

수신자 이메일 메일 목록 별칭 및 스팸 알림

메일 목록 및 기타 별칭을 포함하여 격리된 이메일이 있는 각 봉투 수신자에게 알림이 전송됩니다. 각 메일 목록은 단일 digest를 수신합니다. 메일 목록으로 알림을 전송하면 해당 목록의 모든 구독자가 알림을 수신합니다. 여러 이메일 별칭에 속한 사용자, 알림을 수신하는 LDAP 그룹에 속한 사용자 또는 여러 이메일 주소를 사용하는 사용자는 여러 스팸 알림을 받을 수 있습니다. 다음 표에서는 사용자가 여러 알림을 받을 수 있는 상황의 예를 보여줍니다.

표 ***73:*** 주소/별칭당 알림 수

사용자	이메일 주소	별명	알림
Sam	sam@example.com	—	1

사용자	이메일 주소	별명	알림
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com, admin@example.com	hr@example.com	3

LDAP 인증을 사용하는 경우 메일 목록 별칭으로 알림을 전송하지 않도록 선택할 수 있습니다. 메일 목록 별칭에 스팸 알림을 전송하도록 선택하는 경우 여러 알림의 발생을 어느 정도 막을 수 있습니다.
.

어플라이언스가 이메일 알림에 대해 스팸 격리 별칭 통합을 사용하지 않는 한, 알림의 링크를 클릭하여 스팸 격리에 액세스하는 사용자는 자신이 가지고 있을 수 있는 다른 별칭에 대한 격리된 메시지를 볼 수 없습니다. 어플라이언스에 의한 처리 이후 확장되는 배포 목록으로 알림이 전송된 경우 여러 수신자가 해당 목록에 대한 동일한 격리에 액세스할 수 있습니다.

즉, 모든 메일 목록 구독자가 알림을 수신하며 격리에 로그인하여 메시지를 릴리스 또는 삭제할 수 있습니다. 이 경우 알림에 나와 있는 메시지를 보기 위해 격리를 방문하는 최종 사용자는 해당 메시지가 이미 다른 사용자에 의해 삭제된 것을 발견할 수 있습니다.

참고 LDAP를 사용하지 않으며 최종 사용자가 여러 이메일 알림을 받지 않도록 하려면, 알림을 비활성화하고 대신 최종 사용자가 격리에 직접 액세스하여 LDAP 또는 POP/IMAP를 통해 인증을 받도록 할 수 있습니다.

알림 테스트

테스트 메일 정책을 구성하고 단일 사용자에 대해서만 스팸을 격리하여 알림을 테스트할 수 있습니다. 그런 다음 스팸 격리 알림 설정을 구성합니다. **Enable Spam Notification(**스팸 알림 활성화**)** 확인란을 선택하고 **Enable End-User Quarantine Access(**최종 사용자 격리 액세스 활성화**)**를 선택하지 않습니다. 그러면 **Deliver Bounced Messages To(**반송 메시지 전달**)** 필드에 구성된 관리자에게만 격리의 새 스팸에 대한 알림이 제공됩니다.

스팸 알림 문제 해결

관련 주제

- 사용자가 여러 알림 수신 , 306 페이지
- 수신자가 알림을 수신하지 못함 , 306 페이지
- 사용자가 여러 알림 수신 , 306 페이지
- 수신자가 알림을 수신하지 못함 , 306 페이지

사용자가 여러 알림 수신

문제

한 사용자가 단일 메시지에 대해 여러 스팸 알림을 수신합니다.

솔루션

가능한 원인

- 사용자가 여러 이메일 주소를 가지고 있고 스팸 메시지가 그러한 주소 중 둘 이상으로 전송되었습니다.
- 사용자가 스팸 메시지를 수신한 둘 이상의 이메일 별칭에 속한 구성원입니다. 중복을 최소화하는 방법에 대한 자세한 내용은 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 304 페이지 섹션을 참조하십시오.

수신자가 알림을 수신하지 못함

문제

수신자가 알림을 수신하지 못합니다.

솔루션

- 알림이 스팸 수신자 대신 "Deliver Bounce Messages To(반송 메시지 전달):" 주소로 전송되고 있다면, 이는 스팸 알림은 활성화되었지만 스팸 격리 액세스는 활성화되지 않았음을 나타냅니다. 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 298 페이지를 참조하십시오.
- 사용자에게 이메일 클라이언트의 정크 메일 설정을 확인하도록 안내합니다.
- 스팸 격리 활성화 및 구성 , 281 페이지에서 **Deliver Messages Via(**메시지 전달 경로**)**에 대해 지정한 어플라이언스 또는 서버의 문제를 확인합니다.

스팸 격리의 메시지 관리

이 섹션에서는 로컬 또는 외부 스팸 격리의 메시지로 작업하는 방법에 대해 설명합니다.

관리 사용자는 스팸 격리의 모든 메시지를 보고 관리할 수 있습니다.

관련 주제

- 스팸 격리에 액세스(관리 사용자), 306 페이지
- 스팸 격리에서 메시지 검색, 307 페이지
- 스팸 격리의 메시지 보기, 308 페이지
- 스팸 격리의 메시지 전달, 308 페이지
- 스팸 격리에서 메시지 삭제, 308 페이지

스팸 격리에 액세스(관리 사용자)

관리 사용자는 스팸 격리의 모든 메시지를 보고 관리할 수 있습니다.

스팸 격리에 액세스(관리 사용자)

관리 사용자는 스팸 격리의 모든 메시지를 보고 관리할 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 **Quarantine**(격리) > **Spam Quarantine**(스팸 격리) > **Search**(검색)를 선택합니다.

단계 **2** **Email**(이메일) > **Message Quarantine**(메시지 격리) > **Spam Quarantine**(스팸 격리)을 선택한 다음 **Spam Quarantine**(스팸 격리) 링크를 클릭합니다.

별도의 브라우저 창에 스팸 격리가 열립니다.

스팸 격리에서 메시지 검색

단계 **1** 봉투 수신자를 지정합니다.

참고 부분 주소를 입력할 수 있습니다.

단계 **2** 검색 결과가 입력한 수신자와 정확히 일치해야 하는지, 또는 검색 결과가 입력한 항목을 포함해야 하는지, 입력한 항목으로 시작해야 하는지 또는 끝나야 하는지를 선택합니다.

단계 **3** 검색할 날짜 범위를 입력합니다. 날짜를 선택할 달력 아이콘을 클릭합니다.

단계 **4** From: 주소를 지정하고, 검색 결과가 입력한 항목을 포함해야 하는지, 입력한 항목으로 시작해야 하는지 또는 끝나야 하는지를 선택합니다.

단계 **5** **Search**(검색)를 클릭합니다. 검색 기준과 일치하는 메시지가 페이지의 Search(검색) 섹션 아래에 표시됩니다.

다음에 수행할 작업

관련 주제

매우 큰 메시지 컬렉션 검색, 307 페이지

매우 큰 메시지 컬렉션 검색

스팸 격리에 매우 큰 메시지 컬렉션이 있는 경우 그리고 검색 조건이 좁게 정의되지 않은 경우, 쿼리에서 정보를 반환하는 데 시간이 오래 걸리거나 시간 초과가 발생할 수도 있습니다.

검색을 다시 제출할지를 확인하는 프롬프트가 표시됩니다. 큰 규모의 검색을 여러 개 동시에 실행하면 성능이 저하될 수 있습니다.

스팸 격리의 메시지 보기

메시지 목록은 스팸 격리의 메시지를 보여줍니다. 한 번에 표시할 메시지 수를 선택할 수 있습니다. 열 제목을 클릭하여 표시를 정렬할 수 있습니다. 정렬 순서를 반대로 하려면 동일한 열을 다시 클릭합니다.

본문과 헤더를 포함하여 메시지를 보려면 메시지의 제목을 클릭합니다. Message Details(메시지 세부사항) 페이지에 메시지가 표시됩니다. 메시지의 처음 20K가 표시됩니다. 메시지가 더 길면 20K에서 잘리며, 메시지 하단에 있는 링크를 통해 메시지를 다운로드할 수 있습니다.

Message Details(메시지 세부사항) 페이지에서 메시지를 삭제하거나(**Delete** 선택) 릴리스할 수 있습니다(**Release** 선택). 메시지를 릴리스하면 메시지가 전달됩니다.

메시지에 대한 추가 세부사항을 보려면 **Message Tracking(**메시지 추적**)** 링크를 클릭합니다.

다음에 유의하십시오.

- 첨부 파일이 있는 메시지 보기

  첨부 파일이 포함된 메시지를 볼 경우 메시지 본문이 표시되고 그 뒤에 첨부 파일 목록이 표시됩니다.

  새 웹 인터페이스에서 메시지에 첨부 파일을 포함하는 경우 메시지의 Attachments(첨부 파일) 섹션에서 첨부 파일의 세부 정보를 볼 수 있습니다.

- **HTML** 메시지 보기

  스팸 격리는 HTML 기반 메시지에 가깝게 렌더링하려고 시도합니다. 이미지는 표시되지 않습니다.

- 인코딩된 메시지 보기

  Base64 인코딩 메시지는 해독된 후 표시됩니다.

스팸 격리의 메시지 전달

메시지를 릴리스하여 전달하려면, 릴리스할 메시지 옆에 있는 확인란을 클릭하고 드롭다운 메뉴에서 **Release(**릴리스**)**를 선택합니다. 그런 후 **Submit(**제출**)**을 클릭합니다.

페이지에 현재 표시된 모든 메시지를 자동으로 선택하려면 머리글 행의 확인란을 클릭합니다.

릴리스된 메시지는 대상 대기열로 직접 이동하며, 이메일 파이프라인에서 추가 작업 대기열 처리를 건너뜁니다.

스팸 격리에서 메시지 삭제

일정한 시간이 지난 후 메시지를 자동으로 삭제하도록 스팸 격리를 구성할 수 있습니다. 격리가 최대 크기에 도달하면 가장 오래된 메시지를 자동으로 삭제하도록 스팸 격리를 구성할 수 있습니다. 스팸 격리에서 메시지를 수동으로 삭제할 수도 있습니다.

특정 메시지를 삭제하려면 삭제할 메시지 옆에 있는 확인란을 클릭하고 드롭다운 메뉴에서 **Delete(**삭제**)**를 선택합니다. 그런 후 **Submit(**제출**)**을 클릭합니다. 페이지에 현재 표시된 모든 메시지를 자동으로 선택하려면 머리글 행의 확인란을 클릭합니다.

스팸 격리의 모든 메시지를 삭제하려면 격리를 비활성화하고(외부 스팸 격리 비활성화 소개 , 309 페이지 참조) **Delete All Messages(**모든 메시지 삭제**)** 링크를 클릭합니다. 링크의 끝에 있는 괄호의 숫자는 스팸 격리에 있는 메시지의 수입니다.

스팸 격리에 대한 디스크 공간

격리에 사용할 수 있는 디스크 공간은 어플라이언스 모델에 따라 다릅니다. 디스크 공간, 할당량 및 사용률 보기 , 488 페이지를 참조하십시오.

기본적으로 스팸 격리의 메시지는 지정된 시간이 지나면 자동으로 삭제됩니다. 격리가 꽉 차면 오래된 스팸이 삭제됩니다. 이 설정을 변경하려면 스팸 격리 활성화 및 구성 , 281 페이지 섹션을 참조하십시오.

관련 주제

외부 스팸 격리 비활성화 소개

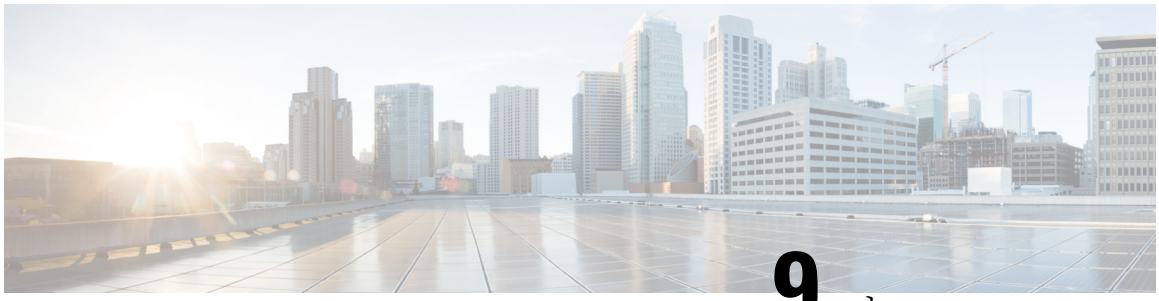
스팸 격리를 비활성화하려면

- 비활성화된 스팸 격리에 메시지가 있으면 메시지를 모두 삭제할 수 있습니다.
- 스팸 또는 의심스런 스팸을 격리하도록 설정된 메일 정책이 메시지를 전달하도록 설정됩니다. Email Security Appliance에서 메일 정책을 조정해야 할 수 있습니다.
- 외부 스팸 격리를 완전히 비활성화하려면 Email Security Appliance 및 Security Management Appliance에서 모두 비활성화합니다.

Email Security Appliance에서만 외부 스팸 격리를 비활성화하면 외부 격리 또는 해당 메시지와 데이터가 삭제되지 않습니다.

스팸 격리 기능 문제 해결

- 허용 목록 및 차단 목록 문제 해결, 296 페이지
- 스팸 알림 문제 해결 , 305 페이지



9 장

중앙 정책, 바이러스, 보안 침해 격리

이 장에는 다음 섹션이 포함되어 있습니다.

중앙 집중식 격리 개요

Email Security Appliance에서 특정 필터, 정책 및 검색 작업으로 처리된 메시지는 추가 작업을 위한 임시 보관을 위해 격리로 이동될 수 있습니다. Cisco Content Security Management Appliance의 여러 Email Security Appliance로부터 격리를 중앙 집중화할 수 있습니다.

격리 중앙 집중화의 이점은 다음과 같습니다.

- 여러 Email Security Appliance에서 온 격리된 메시지를 한 장소에서 관리할 수 있습니다.
- 격리된 메시지는 DMZ 대신 방화벽 뒤에 저장되므로 보안 위험이 줄어듭니다.
- Security Management Appliance에서 표준 백업 기능의 일부로서 중앙 집중식 격리를 백업할 수 있습니다.

안티바이러스 검사, Outbreak Filter 및 Advanced Malware Protection (File Analysis)은 각각 단일 전용 격리를 가지고 있습니다. 메시지 필터링, 콘텐츠 필터링 및 데이터 유출 방지(Data Loss Prevention) 정책에서 포착된 메시지를 보관할 정책 격리를 만들 수 있습니다.

레거시 웹 인터페이스의 정책, 바이러스 및 보안 침해 격리 섹션은 새 웹 인터페이스에서 기타 격리라는 레이블로 지정됩니다. 자세한 내용은 격리의 메시지 보기 , 331 페이지을 참고하십시오.

격리에 대한 자세한 내용은 Email Security Appliance용 문서를 참조하십시오.

격리 유형

격리 유형	격리 이름	시스템에서 기본적으로 생성되는지 여부	설명	추가 정보
AMP(Advanced Malware Protection)	파일 분석	예	판정이 돌아올 때까지 파일 분석을 위해 전송된 메시지를 보관합니다.	• 정책, 바이러스 및 Outbreak 격리 관리 • 정책, 바이러스 또는 보안 침해 격리의 메시지 작업
바이러스	바이러스	예	안티바이러스 엔진의 결정에 따라, 악성코드를 전송할 가능성이 있는 메시지를 보관합니다.	
Outbreak	Outbreak	예	Outbreak Filter에서 잠재적으로 스팸 또는 악성코드로서 포착된 메시지를 보관합니다.	
정책	Policy	예	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업으로 포착된 메시지를 보관합니다. 기본 Policy(정책) 격리가 자동으로 생성됩니다.	
	분류되지 않음	예	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 지정된 격리가 삭제된 경우에만 메시지를 보관합니다. 이 격리를 다른 필터나 메시지 작업에 할당할 수 없습니다.	
	(자신이 만든 정책 격리)	아니오		

격리 유형	격리 이름	시스템에서 기본적으로 생성되는지 여부	설명	추가 정보
			메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 사용하기 위해 자신이 만든 Policy(정책) 격리.	
스팸	스팸	예	메시지 수신자 또는 관리자 검토를 위해 스팸이나 스팸으로 의심되는 메시지를 보관합니다. 스팸 격리는 정책, 바이러스 및 전파 확산 격리의 그룹에 포함되지 않으며 다른 모든 격리와 별도로 관리됩니다.	스팸 격리, 279 페이지

정책, 바이러스 및 **Outbreak** 격리 중앙 집중화

프로시저

	명령 또는 동작	목적
단계 **1**	Email Security Appliance가 DMZ에 있고 Security Management Appliance가 방화벽 뒤에 있는 경우 어플라이언스가 중앙 집중식 정책, 바이러스 및 보안 침해 격리 데이터를 교환할 수 있도록 방화벽에서 포트를 엽니다.	방화벽 정보, 563 페이지
단계 **2**	Security Management Appliance에서 기능을 활성화합니다.	Security Management Appliance에서 중앙 집중식 정책, 바이러스 및 Outbreak 격리 활성화 , 315 페이지
단계 **3**	Security Management Appliance에서 비 스팸 격리에 대한 디스크 공간을 할당합니다.	디스크 공간 관리 , 487 페이지
단계 **4**	(선택 사항)	• 정책, 바이러스, Outbreak 격리 구성 , 323 페이지

	명령 또는 동작	목적
	• Security Management Appliance에서 원하는 설정으로 중앙 집중식 정책 격리를 만듭니다. • 중앙 집중식 바이러스 및 전파 확산 격리에 대한 설정, 그리고 기본 정책 격리에 대한 설정을 구성합니다. 마이그레이션 전에 이러한 설정을 구성하는 경우 Email Security Appliance에서 기존 설정을 참조할 수 있습니다. 또한 맞춤형 마이그레이션을 구성하는 동안 필요한 격리를 만들 수 있습니다. 또는 자동 마이그레이션 중에 격리가 자동으로 생성됩니다. 마이그레이션 중에 생성된 모든 격리는 기본 설정을 갖습니다. 격리 이름이 동일하더라도, 로컬 격리는 중앙 집중식 격리에 유지되지 않습니다.	• 시스템 생성 격리의 설정 확인 , 323 페이지.
단계 **5**	Security Management Appliance에서 관리할 Email Security Appliance를 추가하거나, 이미 추가된 어플라이언스의 중앙 집중식 서비스에서 Policy, Virus and Outbreak Quarantines(정책, 바이러스 및 보안 침해 격리) 옵션을 선택합니다. • Email Security Appliance가 클러스터링된 경우, 클러스터의 Email Security Appliance에서 중앙 집중식 정책, 바이러스 및 보안 침해 격리를 활성화하기 전에 특정 레벨(머신, 그룹 또는 클러스터)에 속하는 모든 어플라이언스를 Security Management Appliance에 추가해야 합니다.	중앙 집중식 정책, 바이러스 및 Outbreak 격리 서비스를 관리되는 각 Email Security Appliance에 추가, 316 페이지
단계 **6**	변경 사항을 커밋합니다.	
단계 **7**	Security Management Appliance에서, Email Security Appliance에서 오는 기존 정책 격리의 마이그레이션을 구성합니다.	정책, 바이러스 및 Outbreak 격리의 마이그레이션 구성 , 317 페이지
단계 **8**	Email Security Appliance에서 중앙 집중식 정책, 바이러스 및 보안 침해 격리 기능을 활성화합니다. • 중요 정책, 바이러스 및 보안 침해 격리가 Email Security Appliance에 구성된 경우, 이 변경 사항을 커밋하자마자 격리 및 모든 메시지의 마이그레이션이 시작됩니다.	Email Security Appliance에 대한 문서의 "Cisco Content Security Management Appliance에서 서비스 중앙 집중화" 장에서 특히 다음 섹션을 참조하십시오. • "정책, 바이러스 및 Outbreak 격리의 마이그레이션 정보" • "정책, 바이러스 및 Outbreak 격리 중앙 집중화"
단계 **9**	추가 Email Security Appliance를 마이그레이션합니다.	

	명령 또는 동작	목적
	• 언제든 하나의 마이그레이션 프로세스만 진행할 수 있습니다. 이전 마이그레이션이 완료되기 전에 또 다른 Email Security Appliance에서 중앙 집중식 정책, 바이러스 및 보안 침해 격리를 활성화하지 마십시오.	
단계 **10**	중앙 집중식 격리 설정을 필요한 대로 수정합니다. • 마이그레이션 중에 생성된 격리는, 중앙 집중식 격리 이름과 로컬 격리 이름이 동일하더라도, 원래 로컬 격리의 설정이 아니라 기본 설정으로 생성됩니다.	정책, 바이러스, Outbreak 격리 구성 , 323 페이지
단계 **11**	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업을 중앙 집중식 격리의 이름으로 자동으로 업데이트할 수 없는 경우 Email Security Appliance에서 해당 구성을 수동으로 업데이트합니다. • 클러스터 구성에서 필터 및 메시지 작업은 필터 및 메시지 작업이 특정 레벨에서 정의된 경우에만 해당 레벨에서 자동으로 업데이트할 수 있습니다.	Email Security Appliance의 온라인 도움말 또는 사용 설명서에서 메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 대한 내용을 참조하십시오.
단계 **12**	(권장 사항) 원래 어플라이언스를 사용할 수 없는 경우 릴리스된 메시지를 처리할 Email Security Appliance를 지정합니다.	릴리스된 메시지를 처리할 대체 어플라이언스 지정, 319 페이지
단계 **13**	관리를 맞춤형 사용자 역할에 위임하는 경우 특정 방식으로 액세스를 구성해야 할 수 있습니다.	맞춤형 사용자 역할을 위해 중앙 집중식 격리 액세스 구성 , 320 페이지

Security Management Appliance에서 중앙 집중식 정책, 바이러스 및 Outbreak 격리 활성화

시작하기 전에

정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지의 표에서 이 절차 이전의 모든 단계를 완료합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 보안 침해 격리)**를 선택합니다.

단계 **3** **Enable(활성화)**을 클릭합니다.

단계 **4** Email Security Appliance와의 통신을 위한 인터페이스와 포트를 지정합니다.

- 변경해야 할 이유가 없는 한 기본 선택 사항을 수락합니다.
- Email Security Appliance가 Security Management Appliance와 동일한 네트워크에 있지 않은 경우 Management 인터페이스를 사용해야 합니다.
- 방화벽에서 열었던 것과 동일한 포트를 사용합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지의 표에서 다음 단계로 돌아갑니다.

중앙 집중식 정책, 바이러스 및 **Outbreak** 격리 서비스를 관리되는 각 **Email Security Appliance**에 추가

모든 Email Security Appliance에서 모든 격리의 통합 보기를 보려면, 격리를 중앙 집중화하기 전에 모든 Email Security Appliance를 추가하는 것을 고려해 보십시오.

시작하기 전에

정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지의 표에서 현 시점까지의 모든 절차를 완료해야 합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **3** 이 페이지의 목록에 Email Security Appliance를 이미 추가한 경우

a) Email Security Appliance의 이름을 클릭합니다.

b) **Policy, Virus, and Outbreak Quarantines(**정책, 바이러스 및 보안 침해 격리**)** 서비스를 선택합니다.

단계 **4** Email Security Appliance를 아직 추가하지 않은 경우

a) Add Email Appliance(이메일 어플라이언스 추가)를 클릭합니다.

b) Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 추가 중인 어플라이언스의 Management 인터페이스에 대한 IP 주소를 입력합니다.

참고 IP Address(IP 주소) 텍스트 필드에 DNS 이름을 입력하는 경우 **Submit(**제출**)**을 클릭하면 즉시 IP 주소로 해석됩니다.

c) Policy, Virus and Outbreak Quarantines(정책, 바이러스 및 Outbreak 격리) 서비스가 미리 선택되어 있습니다.

d) **Establish Connection(**연결 설정**)**을 클릭합니다.

e) 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다.

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

f) 페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** Centralized Policy, Virus, and Outbreak Quarantines(중앙 집중식 정책, 바이러스 및 보안 침해 격리)를 활성화할 각 Email Security Appliance에 대해 이 절차를 반복합니다.

예를 들어 클러스터에서 다른 어플라이언스를 추가합니다.

단계 **7** 변경 사항을 커밋합니다.

다음에 수행할 작업

정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지의 표에서 다음 단계로 돌아갑니다.

정책, 바이러스 및 **Outbreak** 격리의 마이그레이션 구성

시작하기 전에

- 다음의 표에서 현 시점까지의 모든 절차를 완료해야 합니다. 정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지
- 마이그레이션 프로세스에 대한 주의 사항과 정보는 Email Security Appliance의 설명서에서 "Cisco Content Security Management Appliance에서 서비스 중앙 집중화" 장의 "정책, 바이러스 및 보안 침해 격리 정보" 섹션을 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 보안 침해 격리**)**를 선택합니다.

단계 **3** **Launch Migration Wizard(**마이그레이션 마법사 구동**)**를 클릭합니다.

단계 **4** 마이그레이션 방법을 선택합니다.

해당되는 경우	선택	추가 정보
• 연결된 모든 Email Security Appliance에서 모든 기존 정책 격리를 마이그레이션하려는 경우 및 • 동일한 이름의 여러 정책 격리가 모든 Email Security Appliance에서 동일한 설정을 가지고 있는 경우 및 • 모든 Email Security Appliance에서 동일한 이름의 모든 정책 격리를 해당 이름의 중앙 집중식 단일 정책 격리로 병합하려는 경우	자동	Email Security Appliance에서 동일한 이름을 가진 격리의 설정과 상관없이 이 프로세스를 사용하여 만든 모든 중앙 집중식 격리는 자동으로 기본 설정으로 구성됩니다. 마이그레이션 후 그러한 설정을 업데이트해야 합니다.
• 동일한 이름의 여러 정책 격리가 서로 다른 Email Security Appliance에서 서로 다른 설정을 가지고 있으며 이러한 차별성을 유지하려는 경우 또는 • 일부 로컬 격리를 마이그레이션하고 다른 것은 모두 삭제하려는 경우 또는 • 로컬 격리를 다른 이름을 사용하여 중앙 집중식 격리로 마이그레이션하려는 경우 또는 • 서로 다른 이름의 로컬 격리를 중앙 집중식 단일 격리로 병합하려는 경우	맞춤형	마이그레이션 이전이 아니라 마이그레이션 중에 만드는 중앙 집중식 정책 격리는 새 격리에 대한 기본 설정으로 구성됩니다. 마이그레이션 후 그러한 설정을 업데이트해야 합니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** **Automatic(**자동**)**을 선택한 경우

마이그레이션할 정책 격리 및 이 페이지의 기타 정보가 예상과 일치하는지 확인합니다.

바이러스, Outbreak 및 파일 분석 격리도 마이그레이션됩니다.

단계 **7** **Custom(**사용자 지정**)**을 선택한 경우

- 모든 Email Security Appliance의 격리를 표시할지 하나만 표시할지를 선택하려면 **Show Quarantines from:(**다음의 격리 표시**:)** 목록에서 옵션을 선택합니다.

- 각 중앙 집중식 정책 격리로 이동할 로컬 정책 격리를 선택합니다.
- 필요에 따라 중앙 집중식 추가 정책 격리를 만듭니다. 여기에는 기본 설정이 사용됩니다.
- 격리 이름은 대/소문자를 구분합니다.
- 왼쪽 테이블에 남아 있는 격리는 마이그레이션되지 않으며, 마이그레이션이 완료될 때 Email Security Appliance에서 삭제됩니다.
- 오른쪽 테이블에서 격리를 선택하고 **Remove from Centralized Quarantine**(중앙 집중식 격리에서 제거)을 클릭하여 격리 매핑을 변경할 수 있습니다.

단계 **8** 필요에 따라 **Next**(다음)를 클릭합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지의 표에서 다음 단계로 돌아갑니다.

릴리스된 메시지를 처리할 대체 어플라이언스 지정

일반적으로 중앙 집중식 격리에서 메시지가 릴리스되면 Security Management Appliance에서는 이의 처리를 위해, 해당 메시지를 원래 중앙 집중식 격리로 전송한 Email Security Appliance로 반환합니다.

메시지가 시작된 Email Security Appliance를 사용할 수 없는 경우, 릴리스된 메시지를 다른 Email Security Appliance에서 처리 및 전달할 수 있습니다. 이 용도의 어플라이언스를 지정할 수 있습니다.

시작하기 전에

- 대체 어플라이언스가 릴리스된 메시지를 예상대로 처리 및 전달할 수 있는지 확인합니다. 예를 들어, 암호화 및 안티바이러스 재검사용 구성이 기본 어플라이언스의 동일한 구성과 일치해야 합니다.
- 대체 어플라이언스에서 중앙 집중식 정책, 바이러스 및 침투 격리 관련 내용을 충분히 구성해야 합니다. 해당 어플라이언스에 대한 정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지의 표에서 단계를 완료합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 집중식 서비스) > **Security Appliances**(보안 어플라이언스)를 선택합니다.

단계 **3** **Specify Alternate Release Appliance**(대체 릴리스 어플라이언스 지정) 버튼을 클릭합니다.

단계 **4** Email Security Appliance를 선택합니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

Email Security Appliance를 사용할 수 없을 때 메시지 릴리스 , 320 페이지

맞춤형 사용자 역할을 위해 중앙 집중식 격리 액세스 구성

맞춤형 사용자 역할의 관리자가 Email Security Appliance에서 메시지 및 콘텐츠 필터와 DLP 메시지 작업에 대해 중앙 집중식 정책 격리를 지정하도록 하려면 해당 사용자가 Security Management Appliance에서 관련 정책 격리에 액세스하도록 허용해야 합니다. 또한 Security Management Appliance에서 만든 맞춤형 사용자 역할 이름이 Email Security Appliance의 그것과 일치해야 합니다.

관련 주제

- 맞춤 이메일 사용자 역할 생성 , 407 페이지

중앙 집중식 정책, 바이러스 및 **Outbreak** 격리 비활성화

일반적으로 이러한 중앙 집중식 격리를 비활성화해야 하는 경우 Email Security Appliance에서 해야 합니다.

중앙 집중식 정책, 바이러스 및 보안 침해 격리 비활성화에 대한 자세한 내용, 그리고 그에 따른 영향력의 리스트는 Email Security Appliance에 대한 온라인 도움말이나 문서를 참조해 주십시오.

Email Security Appliance를 사용할 수 없을 때 메시지 릴리스

일반적으로 중앙 집중식 격리에서 메시지가 릴리스되면 Security Management Appliance에서는 이의 처리를 위해, 해당 메시지를 원래 중앙 집중식 격리로 전송한 Email Security Appliance로 반환합니다.

메시지가 시작된 Email Security Appliance를 사용할 수 없는 경우, 릴리스된 메시지를 다른 Email Security Appliance에서 처리 및 전달할 수 있습니다. 이 용도의 대체 릴리스 어플라이언스를 지정해야 합니다.

대체 어플라이언스를 사용할 수 없는 경우 다른 Email Security Appliance를 대체 릴리스 어플라이언스로서 지정할 수 있습니다. 그러면 해당 어플라이언스가 대기열의 메시지를 처리하고 전달합니다.

Email Security Appliance에 도달하려는 시도가 반복적으로 실패하면 경고문이 표시됩니다.

관련 주제

- 릴리스된 메시지를 처리할 대체 어플라이언스 지정, 319 페이지

정책, 바이러스 및 Outbreak 격리 관리

정책, 바이러스 및 Outbreak 격리를 위한 디스크 공간 할당

디스크 공간 할당에 대한 자세한 내용은 디스크 공간 관리 , 487 페이지를 참조하십시오.

여러 격리의 메시지는 단일 격리의 메시지와 동일한 디스크 공간을 사용합니다.

Outbreak Filter 및 Centralized Quarantines(중앙 집중식 격리)가 모두 활성화된 경우

- 보안 침해 규칙이 업데이트될 때마다 해당 메시지를 검사하기 위해, 로컬 정책, 바이러스 및 보안 침해 격리에 할당되었을 Email Security Appliance의 모든 디스크 공간이 보안 침해 격리에 메시지 복사본을 유지하는 데 대신 사용됩니다.
- 특정 관리되는 Email Security Appliance의 보안 침해 격리에 있는 메시지를 위한 Security Management Appliance의 디스크 공간은 해당 Email Security Appliance에 있는 격리된 메시지에 대해 사용 가능한 디스크 공간의 양에 의해 제한됩니다.
- 이 상황에 대한 자세한 내용은 다음을 참조해 주십시오. 격리에서 메시지의 보유 시간 , 321 페이지

관련 주제

- 격리 상태, 용량 및 활동 모니터링 , 326 페이지
- 격리 디스크 공간 사용량에 대한 알림 , 329 페이지
- 격리에서 메시지의 보유 시간 , 321 페이지

격리에서 메시지의 보유 시간

다음 상황에서는 메시지가 격리에서 자동으로 제거됩니다.

- 정상 만료 - 구성된 보유 시간이 격리에 있는 메시지에 대해 충족됩니다. 각 격리의 메시지에 대해 보유 시간을 지정합니다. 각 메시지에는 고유한 특정 만료 시간이 있으며, 이는 격리 리스트에 표시됩니다. 이 항목에 설명된 또 다른 상황이 발생하지 않는 한 메시지는 지정된 기간 동안 저장됩니다.

  참고 Outbreak Filter 격리에 있는 메시지의 정상 보유 시간은 전파 확산 격리가 아니라 각 메일 정책의 Outbreak Filter 섹션에서 구성합니다.

- 조기 만료 - 구성된 보유 시간에 도달하기 전에 격리에서 메시지에 적용됩니다. 다음과 같은 경우 발생할 수 있습니다.

  - 정책, 바이러스 및 Outbreak 격리를 위한 디스크 공간 할당 , 321 페이지에 정의된 대로 모든 격리에 대한 크기 제한에 도달합니다.

    크기 제한에 도달하면 격리와 상관없이 가장 오래된 메시지부터 처리되고, 모든 격리의 크기가 다시 크기 제한보다 작아질 때까지 각 메시지에 대해 기본 작업이 수행됩니다. FIFO(First In First Out) 정책이 적용됩니다. 여러 격리의 메시지는 최신 만료 시간을 기반으로 만료됩니다.

    (선택 사항) 디스크 공간 부족으로 인한 릴리스 또는 삭제가 면제되도록 개별 격리를 구성할 수 있습니다. 면제되도록 모든 격리를 구성한 상태에서 디스크 공간 용량에 도달하면 Security Management Appliance에 사용 가능한 공간이 마련될 때까지 메시지가 Email Security Appliance에 표시됩니다.

    Security Management Appliance는 메시지를 검사하지 않으므로, 메시지를 원래 처리한 Email Security Appliance에 중앙 집중식 보안 침해 격리의 각 메시지 복사본이 저장됩니다. 이렇게 하면 Email Security Appliance에서는 전파 확산 필터 규칙이 업데이트될 때마다 격리된 메시지를 다시 검사하여, 더 이상 위협이 아닌 것으로 간주되는 메시지를 릴리스하도록 Security Management Appliance에 알릴 수 있습니다. 전파 확산 격리의 두 복사본은 항상 동일한 메시지 집합을 보유해야 합니다. 따라서 드문 경우이긴 하지만 Email Security Appliance의 디스크 공간이 꽉 차면, 중앙 집중식 격리에 공간이 있더라도 두 어플라이언스에서 보안 침해 격리의 메시지 복사본이 조기에 만료됩니다.

    디스크 공간 주요 시점에 알림을 받게 됩니다. 격리 디스크 공간 사용량에 대한 알림 , 329 페이지를 참조하십시오.

- 메시지를 여전히 보유하고 있는 격리를 삭제합니다.

격리에서 메시지가 자동으로 제거되면 해당 메시지에 대한 기본 작업이 수행됩니다. 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 323 페이지를 참조하십시오.

참고 위 시나리오 외에도 검사 작업(신종 바이러스 필터(Outbreak Filter) 또는 파일 분석)의 결과에 따라 메시지가 격리에서 자동으로 제거될 수 있습니다.

보유 시간에 대한 시간 조정의 효과

- 일광 절약 시간 및 어플라이언스 표준 시간대 변경은 보유 기간에 영향을 미치지 않습니다.
- 격리의 보유 시간을 변경하면 새 메시지만 새 만료 시간의 적용을 받습니다.
- 시스템 시계가 변경되는 경우, 과거에 만료되었을 메시지는 가장 적절한 다음 시간에 만료됩니다.
- 만료가 진행 중인 메시지에는 시스템 시계 변경이 적용되지 않습니다.

자동으로 처리되는 격리 메시지에 대한 기본 작업

격리에서 메시지의 보유 시간 , 321 페이지에 설명된 상황이 발생하면 정책, 바이러스 또는 전파 확산 격리의 메시지에 대해 기본 작업이 수행됩니다.

두 가지 주요 기본 작업이 있습니다.

- 삭제 - 메시지가 삭제됩니다.
- 릴리스 - 전달을 위해 메시지가 릴리스됩니다.

릴리스되면 메시지에서 위협을 다시 검사할 수 있습니다. 자세한 내용은 격리된 메시지 재검사 정보 , 337 페이지를 참고해 주십시오.

또한 예상 보유 기간이 지나기 전에 릴리스된 메시지에 대해서는 X-Header 추가와 같은 별도의 작업이 수행될 수 있습니다. 자세한 내용은 정책, 바이러스, Outbreak 격리 구성 , 323 페이지를 참고해 주십시오.

중앙 집중식 격리에서 릴리스된 메시지는 처리를 위해 원래 Email Security Appliance로 반환됩니다.

시스템 생성 격리의 설정 확인

격리를 사용하기 전에 Unclassified(미분류) 격리를 포함한 기본 격리의 설정을 맞춤화하십시오.

관련 주제

- 정책, 바이러스, Outbreak 격리 구성 , 323 페이지

정책, 바이러스, Outbreak 격리 구성

시작하기 전에

- 기존 격리를 수정하는 경우 정책, 바이러스 및 Outbreak 격리 설정의 수정에 대한 정보 , 325 페이지 섹션을 참조해 주십시오.
- 보유 시간과 기본 작업을 포함하여 격리의 메시지가 자동으로 관리되는 방법을 이해합니다. 격리에서 메시지의 보유 시간 , 321 페이지 및 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 323 페이지 섹션을 참조해 주십시오.
- 각 격리에 액세스할 수 있도록 할 사용자를 결정하고, 그에 따라 사용자 및 맞춤형 사용자 역할을 만듭니다. 자세한 내용은 정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹 , 330 페이지 섹션을 참조해 주십시오.

단계 1 [새 웹 인터페이스에만 해당] **Quarantine(**격리**)** > **Other Quarantine(**기타 격리**)** > **View(**보기**)** > +를 선택합니다.

새 브라우저 창에 레거시 웹 인터페이스가 열리면 다시 로그인하여 정책, 바이러스 및 보안 침해 격리를 구성해야 합니다.

단계 2 **Email(**이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 신종 바이러스 격리**)**를 선택합니다.

단계 3 다음 중 하나를 수행합니다.

- **Add Policy Quarantine(**정책 격리 추가**)**을 클릭합니다.
- 수정할 격리를 클릭합니다.

단계 4 정보를 입력합니다.

다음에 유의해야 합니다.

- 파일 분석 격리의 보존 기간을 기본값인 1시간에서 변경하는 것은 권장되지 않습니다.
- 격리 디스크 공간이 꽉 차더라도 지정한 Retention Period(보유 기간)가 끝나기 전에 이 격리의 메시지가 처리되지 않도록 하려면 **Free up space by applying default action on messages upon space overflow(**공간 오버플로 시 메시지에 기본 작업을 적용하여 공간 비우기**)**의 선택을 취소합니다.

  이 옵션을 모든 격리에 대해 선택하지 마십시오. 시스템이 하나 이상의 격리에서 메시지를 삭제하여 공간을 마련할 수 있어야 합니다.
- 기본 작업으로 **Release(**릴리스**)**를 선택하는 경우 보유 기간이 지나기 전에 릴리스되는 메시지에 적용할 추가 작업을 지정할 수 있습니다.

옵션	정보
제목 수정	추가할 텍스트를 입력하고 이를 원래 메시지 제목의 앞에 추가할지 뒤에 추가할지를 지정합니다. 예를 들면 수신자에게 메시지에 부적절한 내용이 포함되어 있을 수 있다고 경고할 수 있습니다. 참고 제목에 비 ASCII 문자를 올바르게 표시하려면 RFC 2047에 따라 표현해야 합니다.
X-Header 추가	X-Header는 메시지에 대해 수행된 작업의 기록을 제공할 수 있습니다. 이는 예를 들어 특정 메시지가 전달된 이유에 대한 문의를 처리할 때 도움이 될 수 있습니다. 이름과 값을 입력합니다. 예: 이름 = Inappropriate-release-early Value = True
첨부 파일 제거	어태치된 파일 제거는 해당 파일에 있을 수 있는 바이러스로부터 보호합니다.

단계 **5** 격리에 액세스할 수 있는 사용자를 지정합니다.

사용자	정보
로컬 사용자	로컬 사용자 목록에는 격리에 액세스할 수 있는 역할의 사용자만 포함됩니다. 모든 관리자는 격리에 대한 완전한 액세스 권한을 가지고 있으므로 리스트에는 관리자 권한의 사용자가 제외됩니다.
외부에서 인증된 사용자	외부 인증을 구성한 상태여야 합니다.
맞춤형 사용자 역할	격리 액세스 권한이 있는 맞춤형 사용자 역할을 하나 이상 만든 경우에만 이 옵션이 표시됩니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

Message Filters(메시지 필터) 페이지, 161 페이지 및 Content Filters(콘텐츠 필터) 페이지, 162 페이지 참조

- Email Security Appliance에서 아직 격리를 마이그레이션하지 않은 경우

  마이그레이션 작업의 일부로서 이러한 격리를 메시지 및 콘텐츠 필터와 DLP 메시지 작업에 할당합니다.

- 중앙 집중식 격리로 이미 마이그레이션한 경우

  Email Security Appliance에 메시지 및 콘텐츠 필터, 그리고 메시지를 격리로 이동할 DLP 메시지 작업이 있는지 확인합니다. Email Security Appliance용 온라인 도움말 또는 사용 설명서를 참조하십시오.

정책, 바이러스 및 Outbreak 격리 설정의 수정에 대한 정보

참고

- 격리의 이름은 변경할 수 없습니다.
- 격리에서 메시지의 보유 시간 , 321 페이지도 참조해 주십시오.

격리 설정을 변경하려면 Appliance Configuarion(어플라이언스 구성) 페이지에서 Email(정책, 바이러스 및 보안 침해 격리 이메일) > Message Quarantine(메시지 격리) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 보안 침해 격리)를 선택하고 격리의 이름을 클릭합니다.

정책 격리를 할당할 필터 및 메시지 작업 결정

정책 격리와 관련된 메시지 필터, 콘텐츠 필터, DLP(Data Loss Prevention) 메시지 작업 및 DMARC 확인 프로필, 그리고 각각 구성된 Email Security Appliance를 볼 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Email**(정책, 바이러스 및 보안 침해 격리 이메일) > **Message Quarantine**(메시지 격리) > **Policy, Virus, and Outbreak Quarantines**(정책, 바이러스 및 보안 침해 격리)를 선택합니다.

단계 **3** 확인할 정책 격리의 이름을 클릭합니다.

단계 **4** 페이지 하단으로 스크롤하여 **Associated Message Filters/Content Filters/DLP Message Actions**(관련 메시지 필터/콘텐츠 필터/**DLP** 메시지 작업)를 봅니다.

정책 격리 삭제 정보

- 정책 격리를 삭제하기 전에 활성 필터 또는 메시지 작업과 연결되어 있는지 확인해 주십시오. 정책 격리를 할당할 필터 및 메시지 작업 결정 , 326 페이지를 참조하십시오.
- 필터 또는 메시지 작업에 할당되었더라도 정책 격리를 삭제할 수 있습니다.
- 디스크가 꽉 찼을 때 메시지를 삭제하지 않도록 하는 옵션을 선택했더라도, 비어 있지 않은 격리를 삭제하면 격리에 정의된 기본 작업이 모든 메시지에 적용됩니다. 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 323 페이지를 참조하십시오.
- 필터 또는 메시지 작업과 연결된 격리를 삭제한 이후에 해당 필터나 메시지 작업으로 격리된 메시지는 Unclassified(미분류) 격리로 전송됩니다. 격리를 삭제하기 전에 Unclassified(미분류) 격리의 기본 설정을 맞춤화해야 합니다.
- Unclassified(미분류) 격리는 삭제할 수 없습니다.

격리 상태, 용량 및 활동 모니터링

보려는 내용	수행해야 할 작업
모든 비 스팸 격리에 할당된 총 공간	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 집중식 서비스) > **Policy, Virus, and Outbreak Quarantines**(정책, 바이러스 및 보안 침해 격리) 를 선택하고 페이지의 첫 번째 섹션을 살펴봅니다. 할당을 변경하려면 디스크 공간 관리 , 487 페이지 섹션을 참조해 주십시오.

보려는 내용	수행해야 할 작업
모든 비 스팸 격리에 대해 현재 사용 가능한 공간	[새 웹 인터페이스에만 해당] **Quarantine(**격리**)** > **Other Quarantine(**기타 격리**)**을 선택합니다. 또는 **Email(**정책**,** 바이러스 및 보안 침해 격리 이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 보안 침해 격리**)**를 선택하고 테이블 바로 아래를 살펴봅니다. 정책, 바이러스 및 보안 침해 격리에 사용할 수 있는 공간이 Quarantines(격리) 섹션의 테이블 위에 표시됩니다.
현재 모든 격리에서 사용되고 있는 총 공간	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > System Status(**시스템 상태**)**를 선택합니다.
각 격리에 현재 사용된 공간	[새 웹 인터페이스에만 해당] **Quarantine(**격리**)** > **Other Quarantine(**기타 격리**)** > **View(**보기**)**를 선택합니다. 이 테이블에는 현재 각 격리에 사용된 공간이 표시됩니다. 또는 **Email(**정책**,** 바이러스 및 보안 침해 격리 이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 보안 침해 격리**)**를 선택하고, 격리 이름을 클릭하고, 격리 이름 바로 아래에 있는 테이블 행에서 이 정보를 살펴봅니다.
현재 모든 격리에 있는 총 메시지 수	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > System Status(**시스템 상태**)**를 선택합니다.

보려는 내용	수행해야 할 작업
현재 각 격리에 있는 메시지 수	[새 웹 인터페이스에만 해당] **Quarantine(**격리**)** > **Other Quarantine(**기타 격리**)** > **View(**보기**)**를 선택합니다. 테이블에 각 격리에 현재 사용할 수 있는 총 메시지 수가 표시됩니다. 또는 **Email(**정책**,** 바이러스 및 **Outbreak** 격리 이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 **Outbreak** 격리**)**를 선택하고 격리에 대한 테이블 행을 살펴봅니다.
모든 격리의 총 CPU 사용량	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > System Status(**시스템 상태**)**를 선택하고 System Information(시스템 정보) 섹션을 살펴봅니다.
마지막 메시지가 각 격리에 들어간 날짜와 시간(정책 격리 간 이동 제외)	[새 웹 인터페이스에만 해당] **Quarantine(**격리**)** > **Other Quarantine(**기타 격리**)** > **View(**보기**)**를 선택합니다. 테이블에 마지막 메시지를 격리한 날짜 및 시간이 표시됩니다. 또는 **Email(**정책**,** 바이러스 및 **Outbreak** 격리 이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 **Outbreak** 격리**)**를 선택하고 격리에 대한 테이블 행을 살펴봅니다.
정책 격리를 만든 날짜 정책 격리 만든 사람의 이름	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Email(**정책**,** 바이러스 및 보안 침해 격리 이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 보안 침해 격리**)**를 선택하고, 격리 이름을 클릭하고, 격리 이름 바로 아래에 있는 테이블 행에서 이 정보를 살펴봅니다. 시스템 생성 격리에 대해서는 만든 날짜와 만든 사람 이름을 사용할 수 없습니다.

보려는 내용	수행해야 할 작업
정책 격리와 연결된 필터 및 메시지 작업	정책 격리를 할당할 필터 및 메시지 작업 결정 , 326 페이지를 참조하십시오.

격리 디스크 공간 사용량에 대한 알림

정책, 바이러스, 보안 침해 격리의 총 크기가 용량의 75%, 85%, 95%에 도달하거나 이를 초과할 때마다 알림이 전송됩니다. 메시지가 격리에 놓일 때 확인이 수행됩니다. 예를 들어, 격리에 메시지를 추가하여 크기가 총 용량의 75%로 증가하거나 이를 초과하면 알림이 전송됩니다.

알림에 대한 자세한 내용은 경고 관리, 464 페이지 섹션을 참조하십시오.

정책 격리 및 로깅

AsyncOS는 격리된 모든 메시지를 개별적으로 로깅합니다.

Info: MID 482 quarantined to "Policy" (message filter:policy_violation)

메시지를 격리시킨 메시지 필터 및 Outbreak Filter 기능은 괄호로 표시됩니다. 메시지가 있는 각 격리에 대해 별도의 로그 항목이 생성됩니다.

AsyncOS는 또한 격리에서 제거된 메시지를 개별적으로 로깅합니다.

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

시스템은 모든 격리에서 제거되고 영구 삭제되거나 전달이 예약된 메시지를 개별적으로 로깅합니다. 예를 들면 다음과 같습니다.

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

메시지가 다시 주입되면 시스템은 새 MID(Message ID)로 새로운 Message 개체를 만듭니다. 이는 기존 로그 메시지를 사용하여 새 MID "byline"으로 로깅됩니다. 예를 들면 다음과 같습니다.

Info: MID 483 rewritten to 513 by Policy Quarantine

메시지 처리 작업을 다른 사용자들에게 분산

메시지 검토 및 처리 작업을 다른 관리 사용자들에게 분산할 수 있습니다. 예를 들면 다음과 같습니다.

- 인사 팀에서는 Policy Quarantine(정책 격리)을 검토 및 관리할 수 있습니다.
- 법무 팀에서는 Confidential Material Quarantine(기밀 자료 격리)을 관리할 수 있습니다.

격리에 대한 설정을 지정할 때 이러한 사용자에게 액세스 권한을 할당합니다. 사용자를 격리에 추가하려면 사용자가 존재해야 합니다.

각 사용자는 전체 또는 일부 격리에 액세스하거나 액세스하지 못할 수 있습니다. 격리를 볼 수 있는 권한이 없는 사용자는 GUI 또는 CLI의 격리 리스트 어디에서도 격리의 존재를 확인할 수 없습니다.

관련 주제

- 정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹 , 330 페이지
- 관리 작업 배포, 401 페이지

정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹

관리 사용자가 격리에 액세스하도록 허용하는 경우 이들이 수행할 수 있는 작업은 사용자 그룹에 따라 다릅니다.

- 관리자 또는 이메일 관리자 그룹의 사용자는 격리를 만들고 구성하고 삭제하고 중앙 집중화할 수 있으며 격리된 메시지를 관리할 수 있습니다.
- Operators, Guests, Read-Only Operators, Help Desk Users 그룹의 사용자와 격리 관리 권한이 있는 맞춤형 사용자 역할의 사용자는 격리에서 메시지를 검색하고 보고 처리할 수 있지만, 격리의 설정을 변경할 수 없고 격리를 만들거나 삭제하거나 중앙 집중화할 수도 없습니다. 이러한 사용자 중 누가 해당 격리에 액세스할 수 있는지를 각 격리에서 지정합니다.
- Technicians 그룹의 사용자는 격리에 액세스할 수 없습니다.

관련 기능(예: Message Tracking 및 Data Loss Prevention)에 대한 액세스 권한도 관리 사용자가 Quarantine(격리) 페이지에서 볼 수 있는 옵션과 정보에 영향을 미칩니다. 예를 들어 사용자가 Message Tracking(메시지 추적)에 액세스할 수 없으면 해당 사용자는 격리된 메시지에 대한 메시지 추적 정보를 볼 수 없습니다.

참고**:** Security Management Appliance에 구성된 맞춤형 사용자 역할의 사용자가 필터 및 DLP 메시지 작업에서 정책 격리를 지정하도록 하려면 맞춤형 사용자 역할을 위해 중앙 집중식 격리 액세스 구성 , 320 페이지 섹션을 참조하십시오.

최종 사용자는 정책, 바이러스 및 전파 확산 격리를 볼 수 없거나 이에 대한 액세스 권한이 없습니다.

정책, 바이러스 또는 보안 침해 격리의 메시지 작업

관련 주제

- 격리의 메시지 보기 , 331 페이지
- 정책, 바이러스 및 보안 침해 격리에서 메시지 검색 , 332 페이지
- 격리에 있는 메시지 수동 처리, 333 페이지
- 여러 격리에 있는 메시지 , 334 페이지
- 메시지 세부사항 및 메시지 내용 보기, 335 페이지
- 격리된 메시지 재검사 정보 , 337 페이지
- Outbreak 격리, 337 페이지

격리의 메시지 보기

변경 후	수행해야 할 작업
격리에 있는 모든 메시지 보기	[새 웹 인터페이스에만 해당] **Quarantine**(격리) > **Other Quarantine**(기타 격리) > **View**(보기)를 선택합니다. 또는 **Email**(정책, 바이러스 및 보안 침해 격리 이메일) > **Message Quarantine**(메시지 격리) > **Policy, Virus, and Outbreak Quarantines**(정책, 바이러스 및 보안 침해 격리)를 선택합니다. 관련 격리에 대한 행에서 테이블의 **Messages**(메시지) 열에 있는 파란색 번호를 클릭합니다.
Outbreak 격리에 있는 메시지 보기	[새 웹 인터페이스] **Quarantine**(격리) > **Other Quarantine**(기타 격리) > **View**(보기)를 선택합니다. 또는 **Email**(정책, 바이러스 및 보안 침해 격리 이메일) > **Message Quarantine**(메시지 격리) > **Policy, Virus, and Outbreak Quarantines**(정책, 바이러스 및 보안 침해 격리)를 선택합니다. 관련 격리에 대한 행에서 테이블의 **Messages**(메시지) 열에 있는 파란색 번호를 클릭합니다. [새 웹 인터페이스에만 해당] Manage by Rule Summary(규칙 요약에 의한 관리) 링크, 338 페이지 또는 규칙 요약 보기, 338 페이지의 내용을 참조하십시오.
격리에 있는 메시지의 리스트 탐색	Previous(이전), Next(다음), 페이지 번호 또는 이중 화살표 링크를 클릭합니다. 이중 화살표를 클릭하면 리스트의 첫 페이지(<<) 또는 마지막 페이지(>>)로 이동합니다. [새 웹 인터페이스에만 해당] 모든 새 메시지의 세부 정보를 표시하려면 테이블에서 아래로 스크롤하십시오.
격리에 있는 메시지의 리스트 정렬	머리글을 클릭합니다(여러 항목을 포함할 수 있는 열 또는 "In quarantines(기타 격리에)" 열 제외).
테이블 열 크기 조정	머리글 사이의 구분 기호를 드래그합니다.
테이블 열 맞춤화	 을 클릭하고 표시할 열을 선택한 다음 Close(닫기)를 클릭합니다.
메시지 격리를 일으킨 내용 보기	일치 콘텐츠 보기 , 336 페이지를 참조하십시오.

관련 주제

• 격리된 메시지 및 국제 문자 집합, 332 페이지

격리된 메시지 및 국제 문자 집합

제목에 국제 문자 집합(더블 바이트, 변수 길이, 비 ASCII 인코딩)의 문자가 포함된 메시지의 경우 Policy Quarantine(정책 격리) 페이지의 제목 줄은 디코딩된 형식의 비 ASCII 문자로 표시됩니다.

정책, 바이러스 및 보안 침해 격리에서 메시지 검색

참고
- 사용자는 액세스 권한이 있는 격리의 메시지만 찾고 볼 수 있습니다.
- 정책, 바이러스 및 Outbreak 격리에서 검색할 경우 스팸 격리의 메시지는 찾을 수 없습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 **Quarantine(**격리**)** > **Other Quarantine(**기타 격리**)** > **Search(**검색**)**를 클릭합니다.

단계 **2** [새 웹 인터페이스에만 해당] 해당 격리의 파란색 번호 링크를 클릭합니다.

팁 [새 웹 인터페이스에만 해당] 보안 침해 격리의 경우, 각 보안 침해 규칙에 의해 격리된 모든 메시지를 찾을 수도 있습니다. 보안 침해 격리에서 **Rule Summary(**규칙 요약**)** 탭을 클릭하고 관련 규칙을 클릭합니다.

단계 **3** **Email(**이메일**) > Message Quarantine(**메시지 격리**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 신종 바이러스 격리**)**를 선택합니다.

단계 **4** **Search Across Quarantines(**여러 격리에서 검색**)** 버튼을 클릭합니다.

팁 Outbreak 격리의 경우, 각 전파 확산 규칙에 의해 격리된 모든 메시지를 찾을 수도 있습니다. Outbreak(전파 확산) 테이블 행에서 **Manage by Rule Summary(**규칙 요약에 의한 관리**)** 링크를 클릭하고 관련 규칙을 클릭합니다.

단계 **5** (선택 사항) 기타 검색 기준을 입력합니다.

- Envelope Sender(봉투 발신자) 및 Envelope Recipient(봉투 수신자)의 경우: 아무 문자나 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
- 검색 결과에는 지정한 모든 기준과 일치하는 메시지만 포함됩니다. 예를 들어 Envelope Recipient(봉투 수신자) 및 Subject(제목)를 지정하면 Envelope Recipient(봉투 수신자) 및 Subject(제목)에 지정한 용어와 일치하는 메시지만 반환됩니다.

다음에 수행할 작업

격리 리스트를 사용하는 것과 동일한 방법으로 검색 결과를 사용할 수 있습니다. 자세한 내용은 격리에 있는 메시지 수동 처리, 333 페이지를 참고하십시오.

검색 기준 수정에 대한 자세한 내용은 검색 기준 수정, 333 페이지 항목을 참조하십시오.

검색 기준 수정

검색 기준을 맞춤형 시간 범위 또는 기타 격리로 수정할 수 있습니다.

검색 기준을 수정하려면 **Modify(수정)**를 클릭합니다.

격리에 있는 메시지 수동 처리

메시지를 수동으로 처리한다는 것은 Message Actions(메시지 작업) 페이지에서 메시지에 대한 Message Action(메시지 작업)을 수동으로 선택한다는 뜻입니다.

메시지에 대해 다음 작업을 수행할 수 있습니다.

- 삭제
- Release
- 격리에서 Delay Scheduled Exit(예약된 종료 지연)
- 지정한 이메일 주소로 메시지 복사본 전송
- 한 격리에서 다른 격리로 메시지 이동

일반적으로 다음을 수행할 때 표시되는 리스트의 메시지에 대해 작업을 수행할 수 있습니다. 그러나 모든 상황에서 모든 작업을 사용할 수 있는 것은 아닙니다.

- **Email(정책, 바이러스 및 보안 침해 격리 이메일) > Message Quarantine(메시지 격리) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 보안 침해 격리)** 페이지 또는 [새 웹 인터페이스에만 해당] **Quarantine(격리) > Other Quarantine(기타 격리) > View(보기)** 페이지의 격리 리스트에서 격리에 있는 메시지의 수를 클릭합니다.
- 격리 메시지의 확인란을 클릭하고 필요한 작업을 선택합니다.

다음과 같이 하여 한 번에 여러 메시지에서 이러한 작업을 수행할 수 있습니다.

- 메시지 리스트 상단에 있는 선택 리스트에서 옵션을 선택합니다.
- 페이지에 나열된 각 메시지 옆에 있는 확인란을 선택합니다.
- 메시지 리스트 상단에 있는 테이블 머리글의 확인란을 선택합니다. 이렇게 하면 화면에 보이는 모든 메시지에 작업이 적용됩니다. 다른 페이지의 메시지는 영향을 받지 않습니다.

전파 확산 격리에 있는 메시지에 대해 추가 옵션을 사용할 수 있습니다. *AsyncOS for Email Security Appliances*에 대한 온라인 도움말 또는 사용 설명서의 Outbreak Filters 장에서 Rule Summary(규칙 요약에 의한 관리) 보기에 대한 정보를 참조하십시오.

관련 주제

- 메시지의 복사본 전송, 334 페이지
- 정책 격리 간 메시지 이동 정보 , 334 페이지
- 여러 격리에 있는 메시지 , 334 페이지
- 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 323 페이지

메시지의 복사본 전송

Administrators 그룹에 속한 사용자만 메시지의 복사본을 전송할 수 있습니다.

메시지의 복사본을 전송하려면 Send Copy To:(복사본 전송 대상:) 필드에 이메일 주소를 입력하고 **Submit(**제출**)**을 클릭합니다. 메시지의 복사본을 전송할 경우 메시지에 대한 다른 작업이 수행되지는 않습니다.

정책 격리 간 메시지 이동 정보

단일 어플라이언스의 한 정책 격리에서 다른 정책 격리로 메시지를 수동으로 이동할 수 있습니다.

메시지를 다른 격리로 이동하는 경우

- 만료 시간이 변경되지 않습니다. 메시지에서 원래 격리의 보유 시간이 유지됩니다.
- 내용과 기타 관련 세부사항 불일치 등 메시지가 격리된 이유가 변경되지 않습니다.
- 한 메시지가 여러 격리에 있는 상태에서 이 메시지의 복사본이 이미 있는 대상으로 메시지를 이동하는 경우, 이동한 메시지 복사본의 만료 시간과 격리 이유가 원래 대상 격리에 있던 메시지 복사본의 내용을 덮어씁니다.

여러 격리에 있는 메시지

한 메시지가 하나 이상의 다른 격리에 있는 경우, 그러한 격리에 액세스 권한이 있는지와 상관없이 격리 메시지 리스트의 "In other quarantines(다른 격리에)" 열에 "Yes(예)"가 표시됩니다.

한 메시지가 여러 격리에 있는 경우

- 상주하는 모든 격리에서 릴리스되지 않는 한 전달되지 않습니다. 한 격리에서 메시지가 삭제되면 해당 메시지는 전달되지 않습니다.
- 상주하는 모든 격리에서 삭제 또는 릴리스되기 전에는 어떤 격리에서도 삭제되지 않습니다.

메시지를 릴리스하려는 사용자가 메시지가 상주하는 모든 격리에 액세스하지는 못할 수 있으므로 다음 규칙이 적용됩니다.

- 상주하는 모든 격리에서 릴리스되기 전에는 어떤 격리에서도 릴리스되지 않습니다.

- 한 격리에서 메시지가 Deleted(삭제됨)로 표시된 경우, 상주하는 다른 모든 격리에서 전달될 수 없습니다. (여전히 릴리스는 가능합니다.)

한 메시지가 여러 격리의 대기열에 있는 상태에서 사용자가 하나 이상의 다른 격리에 액세스할 수 없는 경우

- 사용자가 액세스할 수 있는 각 격리에 메시지가 있는지 여부에 대한 알림이 제공됩니다.
- GUI에는 사용자가 액세스할 수 있는 격리에서의 예약된 종료 시간만 표시됩니다. (어떤 메시지의 경우 각 격리에 대한 별도의 종료 시간이 있습니다.)
- 메시지가 있는 다른 격리의 이름은 사용자에게 표시되지 않습니다.
- 사용자는 자신이 액세스할 수 없는 격리로 메시지를 보낸 일치 콘텐츠를 볼 수 없습니다.
- 메시지의 릴리스는 사용자가 액세스할 수 있는 대기열에만 영향을 미칩니다.
- 사용자가 액세스할 수 없는 다른 격리의 대기열에도 메시지가 있는 경우, 나머지 격리에 대해 필요한 액세스 권한이 있는 사용자가 조치를 취할 때까지(또는 조기 만료나 정상 만료를 통해 "정상적으로" 릴리스될 때까지) 해당 메시지는 현재 상태 그대로 격리에 남아 있게 됩니다.

메시지 세부사항 및 메시지 내용 보기

메시지의 내용을 보고 Quarantined Message(격리된 메시지) 페이지에 액세스하려면 메시지의 제목 줄을 클릭합니다.

Quarantined Message(격리된 메시지) 페이지에는 Quarantine Details(격리 세부사항) 및 Message Details(메시지 세부사항)의 두 섹션이 있습니다.

Quarantined Message(격리된 메시지) 페이지에서 메시지를 읽거나, Message Action(메시지 작업)을 선택하거나, 메시지의 복사본을 전송하거나할 수 있습니다. Encrypt on Delivery(전달 시 암호화) 필터 작업에 따라 격리에서 릴리스될 때 메시지가 암호화될지 여부를 확인할 수도 있습니다.

Message Details(메시지 세부사항) 섹션에는 메시지 본문, 메시지 헤더 및 어태치 파일이 표시됩니다. 메시지 본문의 처음 100K만 표시됩니다. 메시지가 더 길면 처음 100K만 표시되고 그 뒤에 줄임표(...)가 나옵니다. 실제 메시지는 잘리지 않습니다. 단지 표시를 위한 것입니다. Message Details(메시지 세부사항) 하단의 Message Parts(메시지 부분) 섹션에서 [message body]를 클릭하여 메시지 본문을 다운로드할 수 있습니다. 어태치 파일의 이름을 클릭하여 메시지 어태치 파일을 다운로드할 수도 있습니다.

참고 Message Details(메시지 세부 정보) 페이지에서 첨부 파일은 최대 25MB까지 다운로드할 수 있습니다.

컴퓨터에 안티바이러스 소프트웨어를 설치한 상태에서 바이러스가 포함된 메시지를 보는 경우, 안티바이러스 소프트웨어에 바이러스 검색 알림이 표시될 수 있습니다. 이는 컴퓨터에 위협이 되지 않으며 안전하게 무시할 수 있습니다.

메시지에 대한 추가 세부사항을 보려면 **Message Tracking(**메시지 추적**)** 링크를 클릭합니다.

참고 특수 Outbreak 격리의 경우 추가 기능을 사용할 수 있습니다. Outbreak 격리, 337 페이지를 참조하십시오.

관련 주제

- 일치 콘텐츠 보기 , 336 페이지
- 어태치 파일 다운로드 , 337 페이지

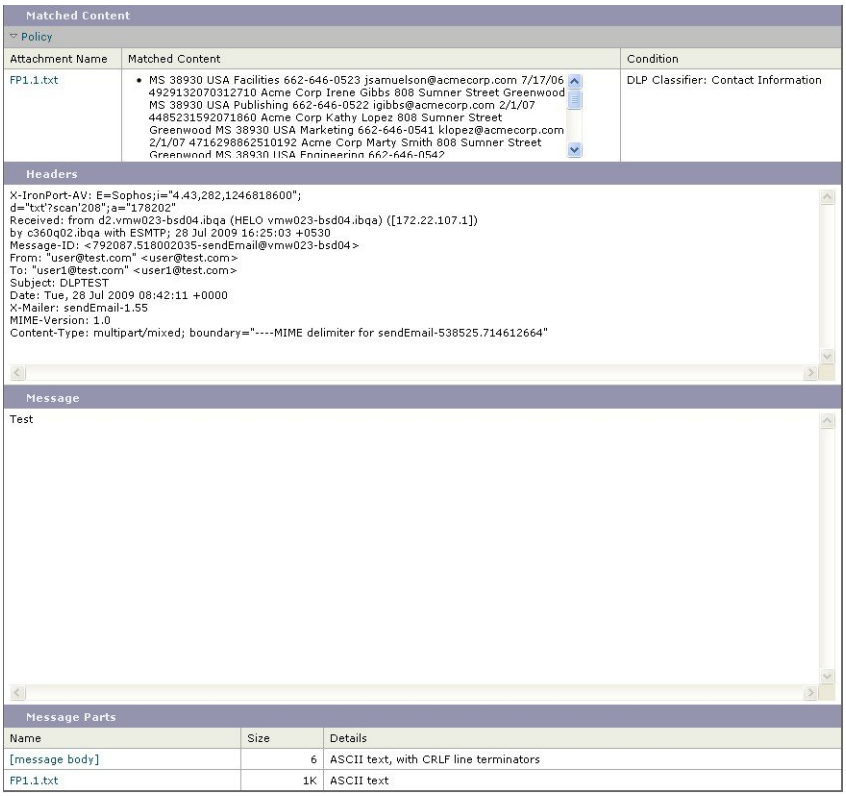
일치 콘텐츠 보기

Attachment Content(어태치 파일 내용) 조건, Message Body or Attachment(메시지 본문 또는 어태치 파일) 조건, Message Body(메시지 본문) 조건, Attachment Content(어태치 파일 내용) 조건을 구성할 때 격리된 메시지에서 일치 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 DLP 정책 위반 일치를 제외하고, 일치 콘텐츠가 노란색으로 강조 표시됩니다. 메시지의 일치 콘텐츠 또는 메시지 제목의 콘텐츠 필터 일치를 포함하려면 $MatchedContent 작업 변수를 사용할 수도 있습니다.

어태치 파일에 일치 콘텐츠가 포함되어 있으면 어태치 파일의 내용과 함께 DLP 정책 위반, 콘텐츠 필터 조건, 메시지 필터 조건, Image Analysis(이미지 분석) 판정 등의 격리된 이유가 표시됩니다.

메시지 또는 콘텐츠 필터 규칙을 트리거한 로컬 격리에 있는 메시지를 볼 때, 실제로 필터 작업을 트리거하지 않은 내용이 필터 작업을 트리거한 내용과 함께 GUI에 표시될 수 있습니다. GUI 표시는 콘텐츠 일치를 찾기 위한 지침으로 사용해야 하지만, 콘텐츠 일치의 정확한 리스트를 반영하는 것은 아닙니다. 이런 일이 발생하는 이유는 GUI가 필터에 사용되는 것보다 덜 엄격한 콘텐츠 일치 논리를 사용하기 때문입니다. 이 문제는 메시지 본문의 강조 표시 부분에만 적용됩니다. 메시지 각 부분의 일치하는 문자열을 관련 필터 규칙과 함께 나열하는 테이블이 정확합니다.

그림 ***5:*** 정책 격리에 표시되는 일치 콘텐츠



어태치 파일 다운로드

Message Parts(메시지 부분) 또는 Matched Content(일치 콘텐츠) 섹션에서 어태치 파일의 이름을 클릭하여 메시지 어태치 파일을 다운로드할 수 있습니다. AsyncOS는 알 수 없는 소스의 어태치 파일에 바이러스가 포함되어 있을 수 있다는 경고를 표시하고 계속 진행할지를 물어봅니다. 바이러스가 포함되어 있을 수 있는 어태치 파일을 다운로드할 경우 스스로 위험을 감수해야 합니다. Message Parts(메시지 부분) 섹션에서 [message body]를 클릭하여 메시지 본문을 다운로드할 수도 있습니다.

격리된 메시지 재검사 정보

격리된 모든 대기열에서 메시지가 릴리스되면, 메시지를 원래 격리한 메일 정책 및 어플라이언스에 대해 활성화된 기능에 따라 다음 재검사가 발생합니다.

- 정책 및 바이러스 격리에서 릴리스된 메시지는 안티바이러스, AMP(Advanced Malware Protection) 및 그레이메일 엔진을 통해 검사됩니다.
- Outbreak 격리에서 릴리스된 메시지는 안티스팸 및 안티바이러스 엔진에 의해 재검사됩니다.
- File Analysis(파일 분석) 격리에서 릴리스된 메시지에 대해서는 위협이 재검사됩니다.
- 어태치 파일이 있는 메시지는 Policy(정책), Virus(바이러스) 및 Outbreak 격리에서 릴리스될 때 파일 평판 서비스에 의해 재검사됩니다.

재검사 시, 현재의 판정이 이전 메시지 처리 시의 판정과 일치하면 메시지가 재격리되지 않습니다. 반대로, 판정이 다르면 메시지가 또 다른 격리로 전송될 수 있습니다.

이렇게 하는 이론적 근거는 메시지가 격리로 무제한 루프백되는 것을 방지하기 위함입니다. 예를 들어, 메시지가 암호화되어 Virus(바이러스) 격리로 전송된다고 가정해보겠습니다. 관리자가 메시지를 릴리스하면 안티바이러스 엔진에서는 여전히 이를 해독할 수 없습니다. 그러나 메시지를 재격리해서는 안 됩니다. 루프가 생성되어 메시지가 격리에서 영구적으로 릴리스되지 않을 것이기 때문입니다. 두 판정이 동일하면 시스템은 두 번째에 Virus(바이러스) 격리를 우회합니다.

Outbreak 격리

유효한 Outbreak Filter 기능 라이선스 키를 입력하면 Outbreak 격리가 표시됩니다. Outbreak Filter 기능은 설정된 임계값에 따라 Outbreak 격리로 메시지를 전송합니다. 자세한 내용은 Email Security Appliance용 온라인 도움말 또는 사용 설명서의 보안 침해 필터 장을 참조하십시오.

Outbreak 격리의 작동 방식은 다른 격리와 유사합니다. 메시지를 검색, 릴리스 또는 삭제할 수 있습니다.

보안 침해 격리에는 다음 보기가 있습니다.

보안 침해 격리에는 **Rule Summary(**규칙 요약**)** 보기, 메시지 세부 정보를 볼 때 **Send to Cisco(Cisco**로 전송**)** 기능, **Scheduled Exit(**예약된 종료**)** 시간별로 검색 결과의 메시지를 정렬하는 옵션 등 기타 격리에서 사용할 수 없는 몇 가지 추가 기능이 있습니다.

Outbreak Filter 기능에 대한 라이선스가 만료되면 Outbreak 격리에 메시지를 더 이상 추가할 수 없습니다. 현재 격리에 있는 메시지가 만료되어 Outbreak 격리가 비게 되면 GUI의 Quarantines(격리) 리스트에 더 이상 표시되지 않습니다.

관련 주제

- Outbreak 격리에 있는 메시지 재검사 , 338 페이지
- 규칙 요약 보기, 338 페이지
- Cisco Systems에 오탐 또는 의심스런 메시지 보고, 338 페이지

Outbreak 격리에 있는 메시지 재검사

격리된 메시지가 더 이상 위협이 아니라고 새로 게시된 규칙에서 결정하면 Outbreak 격리에 있는 메시지는 자동으로 릴리스됩니다.

어플라이언스에서 안티스팸과 안티바이러스가 활성화되어 있으면, 검사 엔진은 메시지에 적용된 메일 플로우 정책을 기반으로 Outbreak 격리에서 릴리스된 모든 메시지를 검사합니다.

규칙 요약 보기

Rule Summary(규칙 요약) 보기는 새 웹 인터페이스에서만 사용할 수 있습니다.

보안 침해 격리에서 규칙 ID로 그룹화된 보안 침해 격리의 내용 목록을 보려면 **Rule Summary(**규칙 요약**)** 탭을 클릭합니다.

메시지를 격리시킨 보안 침해 규칙을 기반으로 격리에 있는 모든 메시지에 대해 메시지 작업(릴리스 및 삭제)을 수행할 수 있습니다. 이것은 Outbreak 격리에서 상당수의 메시지를 삭제하기 위한 이상적인 방법입니다. 자세한 내용은 *AsyncOS for Email Security Appliances*에 대한 온라인 도움말 또는 사용 설명서의 "Outbreak Filters" 장에서 Outbreak Quarantine(보안 침해 격리) 및 Manage by Rule Summary(규칙 요약에 의한 관리) 보기 섹션을 참조하십시오.

Manage by Rule Summary(규칙 요약에 의한 관리) 링크

Manage by Rule Summary(규칙 요약에 의한 관리) 페이지를 보려면 격리 리스트에서 Outbreak 격리 옆에 있는 Manage by Rule Summary(규칙 요약에 의한 관리) 링크를 클릭합니다. 메시지를 격리시킨 전파 확산 규칙을 기반으로 격리에 있는 모든 메시지에 대해 메시지 작업(Release, Delete, Delay Exit)을 수행할 수 있습니다. 이것은 Outbreak 격리에서 상당수의 메시지를 삭제하기 위한 이상적인 방법입니다. 자세한 내용은 Email Security Appliance에 대한 온라인 도움말 또는 사용 설명서의 Outbreak Filter 장에서 Manage by Rule Summary(규칙 요약에 의한 관리) 보기에 관한 정보 를 참조하십시오.

Cisco Systems에 오탐 또는 의심스런 메시지 보고

Outbreak 격리의 메시지에 대한 메시지 세부사항을 볼 때 오탐 또는 의심스런 메시지를 보고하기 위해 Cisco에 메시지를 전송할 수 있습니다.

단계 **1** Outbreak 격리에 있는 메시지로 이동합니다.

단계 **2** 메시지의 확인란을 클릭하고 Send a Copy(사본 전송) 를 선택합니다.

단계 **3** 수신자 주소를 입력하고 Send(보내기)를 클릭합니다.

중앙 집중식 정책 격리 트러블슈팅

관리 사용자가 필터 및 **DLP** 메시지 작업에서 격리를 선택할 수 없음

문제

관리 사용자가 Email Security Appliance의 콘텐츠 및 메시지 필터 또는 DLP 작업에서 격리를 보거나 선택할 수 없습니다.

솔루션

맞춤형 사용자 역할을 위해 중앙 집중식 격리 액세스 구성 , 320 페이지를 참조하십시오.

중앙 집중식 **Outbreak** 격리에서 릴리스된 메시지가 재검사되지 않음

문제

Outbreak Quarantine(Outbreak 격리)에서 릴리스된 메시지는 전달 전에 재검사해야 합니다. 그러나 일부 오염된 메시지가 격리에서 전달되었습니다.

솔루션

이러한 문제는 다음에 설명된 상황에서 발생할 수 있습니다. 격리된 메시지 재검사 정보 , 337 페이지

10 장

Web Security Appliance 관리

이 장에는 다음 섹션이 포함되어 있습니다.

중앙 구성 관리 정보

중앙 집중식 구성 관리 기능을 사용하면 Cisco Content Security Management Appliance에서 최대 150개의 Web Security Appliance로 구성을 게시하여 다음을 수행할 수 있습니다.

- 각 Web Security Appliance에서가 아니라 Security Management Appliance에서 한 번만 설정을 구성 또는 업데이트함으로써 웹 보안 정책 관리를 간소화 및 가속화합니다.
- 분산된 네트워크에서 균일한 정책 시행을 보장합니다.

Web Security Appliance에 설정을 게시하기 위한 두 가지 방법이 있습니다.

- 구성 마스터 사용
- Web Security Appliance의 구성 파일 사용(고급 파일 게시 사용)

올바른 구성 게시 방법 결정

Security Management Appliance에서 구성을 게시하기 위한 두 가지 프로세스가 있으며, 각각은 다른 설정을 게시합니다. 일부 설정은 중앙에서 관리할 수 없습니다.

구성 항목	수행해야 할 작업
Web Security Appliance에서 Web Security Manager 메뉴 아래에 나타나는 기능(예: 정책 및 맞춤형 URL 범주). 예외: L4TM(L4 Traffic Monitor) 설정은 구성 마스터에 포함되지 않습니다. 지원되는 기능은 구성 마스터 버전에 따라 달라지며, 이는 AsyncOS for Web Security 버전에 대응합니다.	구성 마스터를 게시합니다. 구성 마스터에서 구성할 수 있는 기능 중 다수는 Web Security Appliance에 직접 구성이 있어야 작동합니다. 예를 들어 SOCKS 정책은 구성 마스터를 통해 구성할 수 있지만, 우선 Web Security Appliance에서 직접 SOCKS 프록시를 구성해야 합니다.
참고: Cisco ISE(Identity Services Engine)와의 통합은 각 Web Security Appliance에서 독립적으로 구성해야 합니다. Cisco Identity Services Engine 설정은 Cisco Content Security Management Appliance에서 게시할 수 없습니다.	고급 파일 게시를 사용합니다.
Federal Information Processing Standard를 위한 FIPS 모드, 네트워크/인터페이스 설정, DNS, WCCP(Web Cache Communication Protocol), 업스트림 프록시 그룹, 인증서, 프록시 모드, NTP와 같은 시간 설정, L4TM(L4 Traffic Monitor) 설정, 인증 리디렉션 호스트 이름.	관리되는 Web Security Appliance에서 직접 설정을 구성합니다. AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

중앙에서 WSA를 관리하기 위한 구성 마스터 설정

WSA - 초기 머신을 구성하려면 SSW 이후 구성 파일 또는 구성 마스터를 사용하기 전에 무엇을 구성해야 합니까? 구성 파일을 사용할 경우, IP 주소 문제가 발생하지는 않습니까? SMA에서 구성 파일을 게시할 경우 WSA에서 동일한 구성 파일을 여러 곳에 사용할 때와 달리 이러한 문제가 발생하지 않습니다.

어플라이언스	수행해야 할 작업	추가 정보
—	일반 구성 요구 사항 및 주의 사항을 점검합니다.	구성 마스터 사용에 대한 중요 참고 사항, 344 페이지를 참조하십시오.
—	각 Web Security Appliance에서 사용할 구성 마스터 버전을 확인합니다.	사용할 구성 마스터 버전 결정, 344 페이지를 참조하십시오.

어플라이언스	수행해야 할 작업	추가 정보
Web Security Appliance	Web Security Appliance의 구성 마스터에서 구성할 정책 및 기타 설정을 지원하는 데 필요한 기능을 모든 타겟 Web Security Appliance에서 활성화하고 구성합니다.	—
Web Security Appliance	(선택 사항) 모든 Web Security Appliance의 구성 모델로 사용할 수 있는 작동 중인 Web Security Appliance가 있는 경우, 해당 Web Security Appliance의 구성 파일을 사용하면 Security Management Appliance에서 구성 마스터의 구성 속도를 높일 수 있습니다.	Web Security Appliance에서 구성 파일을 다운로드하는 방법에 대한 지침은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 "어플라이언스 구성 저장 및 로드"를 참조하십시오.
Security Management Appliance	중앙 구성 관리를 활성화하고 구성합니다.	SMA에서 중앙 구성 관리 활성화, 344 페이지를 참조하십시오.
Security Management Appliance	구성 마스터를 초기화합니다.	구성 마스터 초기화 및 구성, 344 페이지를 참조하십시오.
Security Management Appliance	Web Security Appliance를 구성 마스터에 연결합니다.	Web Security Appliances와 구성 마스터 연결 정보, 345 페이지를 참조하십시오.
Security Management Appliance	구성 마스터에서 정책, 맞춤 URL 범주, 웹 프록시 바이패스 목록을 가져오거나 수동으로 구성합니다.	게시할 설정 구성 , 347 페이지을 참고하십시오.
Security Management Appliance	각 Web Security Appliance에서 활성화된 기능이 해당 어플라이언스에 할당된 구성 마스터에 대해 활성화된 기능과 일치해야 합니다.	일관성 있는 기능 활성화 보장 , 351 페이지를 참조하십시오.
Security Management Appliance	필요한 구성 마스터를 설정하고 알맞은 기능을 활성화했다면 Web Security Appliance에 구성을 게시합니다.	구성 마스터 게시 , 353 페이지를 참조하십시오.
Security Management Appliance	기존 구성 마스터 설정을 수정할 수 있는 만일의 URL 범주 설정 업데이트에 미리 대비합니다.	URL 범주 집합 업데이트 준비 및 관리 , 365 페이지

구성 마스터 사용에 대한 중요 참고 사항

참고 중앙에서 관리할 각 Web Security Appliance에서 동일한 이름의 영역에 대한 설정이 동일하지 않은 경우, Network(네트워크) > Authentication(인증)의 Realm Names(영역 이름)가 어플라이언스 전체에서 고유한지 확인합니다.

사용할 구성 마스터 버전 결정

서로 다른 기능을 지원하는 AsyncOS for Web Security의 서로 다른 버전을 실행하는 Web Security Appliance를 중앙에서 관리할 수 있도록, Security Management Appliance는 여러 구성 마스터를 제공합니다.

각 구성 마스터는 특정 버전의 AsyncOS for Web Security에 사용될 구성을 갖고 있습니다.

사용 중인 AsyncOS for Web Security 버전에 어떤 구성 마스터 버전을 사용할지 결정하려면 다음에서 호환성 매트릭스를 참조하십시오.http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

참고 호환성 매트릭스에 지정된 대로 구성 마스터 버전이 Web Security Appliance의 AsyncOS 버전과 일치해야 합니다. 더 새로운 Web Security Appliance에 더 이전의 구성 마스터 버전을 게시하는 경우, Web Security Appliance의 설정이 구성 마스터의 설정과 일치하지 않으면 게시가 실패할 수 있습니다. 이는 웹 어플라이언스 상태 세부사항 페이지에서 아무런 불일치가 없더라도 일어날 수 있습니다. 그러한 경우 각 어플라이언스의 구성을 직접 비교해야 합니다.

SMA에서 중앙 구성 관리 활성화

단계 **1** Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Web(**웹**) > Centralized Configuration Manager(**중앙 집중식 구성 관리자**)**를 선택합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

단계 **3** 시스템 설정 마법사를 실행한 후 처음 중앙 구성 관리를 활성화하는 경우 최종 사용자 라이센스 계약을 읽고 **Accept(**동의**)**를 클릭합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

구성 마스터 초기화 및 구성

• 구성 마스터 초기화 , 345 페이지
• WSA의 설정 가져오기 , 348 페이지

- 게시할 설정 구성 , 347 페이지

구성 마스터 초기화

참고: 구성 마스터를 초기화했다면 초기화 옵션은 사용할 수 없습니다. 그 대신 게시할 설정 구성 , 347 페이지에 설명된 방법 중 하나로 구성 마스터를 채웁니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Utilities(유틸리티) > Configuration Masters(구성 마스터)**를 선택합니다.

단계 **2** Options(옵션) 열에서 **Initialize(초기화)**를 클릭합니다.

단계 **3** Initialize Configuration Master(구성 마스터 초기화) 페이지에서

- 이전 릴리스의 구성 마스터가 이미 있고 새 구성 마스터에도 동일한 설정을 사용하거나 그 설정으로 시작하고 싶다면 **Copy Configuration Master(구성 마스터 복사)**를 선택합니다. 나중에 기존 구성 마스터의 설정을 가져올 수도 있습니다.
- 그렇지 않으면 **Use default settings(기본 설정 사용)**를 선택합니다.

단계 **4** **Initialize(초기화)**를 클릭합니다.

이제 구성 마스터를 사용할 수 있습니다.

단계 **5** 초기화할 구성 마스터 버전별로 반복합니다.

Web Security Appliances와 구성 마스터 연결 정보

구성 마스터와 웹 서비스 버전 간의 호환성에 대한 자세한 내용은 사용할 구성 마스터 버전 결정, 344 페이지를 참조하십시오.

구성 마스터에 어플라이언스를 추가하는 가장 간단한 방법은 상황에 따라 다릅니다.

상황	권장 절차
Web Security Appliance를 아직 Security Management Appliance에 추가하지 않은 경우	WSA 추가 및 구성 마스터 버전과 연결 , 345 페이지
Web Security Appliance를 이미 추가한 경우	구성 마스터 버전과 WSA 연결 , 346 페이지

WSA 추가 및 구성 마스터 버전과 연결

중앙에서 관리할 Web Security Appliance를 아직 추가하지 못한 경우 이 절차를 사용합니다.

시작하기 전에

아직 각 Web Security Appliance에 적합한 구성 마스터 버전을 선택하지 않았다면 지금 선택합니다. 사용할 구성 마스터 버전 결정, 344 페이지를 참조하십시오.

단계 **1** Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **2** Add Web Appliance(웹 어플라이언스 추가)를 클릭합니다.

단계 **3** Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 Web Security Appliance 관리 인터페이스의 IP 주소 또는 확인 가능 호스트 이름을 입력합니다.

참고 IP Address(IP 주소) 텍스트 필드에 DNS 이름을 입력하는 경우 **Submit(**제출**)**을 클릭하면 즉시 IP 주소로 해석됩니다.

단계 **4** 중앙 구성 관리자 서비스는 미리 선택되어 있습니다.

단계 **5** **Establish Connection(**연결 설정**)**을 클릭합니다.

단계 **6** 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다.

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

단계 **7** 페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.

단계 **8** 어플라이언스를 할당할 구성 마스터 버전을 선택합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

단계 **10** 중앙 구성 관리를 활성화하려는 각 WSA에서 이 절차를 반복합니다.

구성 마스터 버전과 **WSA** 연결

Security Management Appliance에 이미 Web Security Appliance를 추가한 경우 다음 절차를 사용하여 구성 마스터 버전에 Web Security Appliance를 신속하게 연결할 수 있습니다.

시작하기 전에

아직 각 Web Security Appliance에 적합한 구성 마스터 버전을 선택하지 않았다면 지금 선택합니다. 사용할 구성 마스터 버전 결정, 344 페이지를 참조하십시오.

단계 **1** Security Management Appliance에서 **Web(**웹**) > Utilities(**유틸리티**) > Configuration Masters(**구성 마스터**)**를 선택합니다.

참고 구성 마스터가 비활성으로 표시될 경우 Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시)를 클릭하고 **Edit Display Settings(**표시 설정 수정**)**를 클릭합니다. 해당 구성 마스터가 활성화할 수 있도록 확인란을 선택합니다. 자세한 내용은 게시할 기능 활성화 , 352 페이지을(를) 참고하십시오.

단계 **2** **Edit Appliance Assignment List(**어플라이언스 할당 목록 수정**)**를 클릭합니다.

단계 **3** 연결할 어플라이언스의 행에서 **Masters(**마스터**)** 열을 클릭하여 체크 표시를 입력합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

게시할 설정 구성

게시할 설정으로 구성 마스터를 설정합니다.

여러 방법으로 구성 마스터를 설정할 수 있습니다.

상황	수행해야 할 작업
이전 릴리스의 AsyncOS for Security Management에서 업그레이드하는 중 및 더 오래된 기존 구성 마스터를 새 버전에 복사하여 새 구성 마스터 버전을 초기화하지 않았습니다.	기존 버전을 가져옵니다. 기존 구성 마스터에서 가져오기 , 347 페이지를 참조하십시오.
Web Security Appliance를 이미 구성하고 그 동일한 구성을 여러 Web Security Appliance에 사용하려는 경우	그 Web Security Appliance에서 저장한 구성 파일을 구성 마스터로 가져옵니다. 중앙에서 WSA를 관리하기 위한 구성 마스터 설정 , 342 페이지를 검토하면서 이 구성 파일을 저장했을 것입니다. 가져오려면 WSA의 설정 가져오기 , 348 페이지를 참조하십시오.
가져온 설정을 수정해야 합니다.	구성 마스터에서 직접 웹 보안 기능 구성, 348 페이지를 참조하십시오.
아직 Web Security Appliance에서 정책 설정, URL 카테고리, 바이패스 설정을 구성하지 않은 경우	Web Security Appliance의 구성 마스터에서 직접 이 설정을 구성합니다. 구성 마스터에서 직접 웹 보안 기능 구성, 348 페이지를 참조하십시오.

기존 구성 마스터에서 가져오기

기존 구성 마스터를 새롭고 더 높은 버전의 구성 마스터로 업그레이드할 수 있습니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Utilities(유틸리티) > Configuration Masters(구성 마스터)**를 선택합니다.

단계 **2** Options(옵션) 열에서 **Import Configuration(구성 가져오기)**을 클릭합니다.

단계 **3** **Select Configuration Source(구성 소스 선택)**의 목록에서 구성 마스터를 선택합니다.

단계 **4** 이 구성에 기존 맞춤 사용자 역할을 포함할지 여부를 선택합니다.

단계 **5** **Import**(가져오기)를 클릭합니다.

다음에 수행할 작업

맞춤 웹 사용자 역할 정보 , 408 페이지

WSA의 설정 가져오기

Web Security Appliance 중 하나에서 기존에 사용하던 구성을 사용하려는 경우 Security Management Appliance에 구성 파일을 가져와 구성 마스터에서 정책 설정을 생성할 수 있습니다.

시작하기 전에

구성 파일과 구성 마스터 버전의 호환성을 확인합니다. 사용할 구성 마스터 버전 결정, 344 페이지를 참조하십시오.

주의 호환되는 웹 구성 파일을 원하는 만큼 자주 가져올 수 있습니다. 관리되는 Web Security Appliance에 구성을 이미 게시한 경우에도 마찬가지입니다. 구성 파일을 구성 마스터로 가져오면 선택한 구성 마스터와 연결된 설정을 완전히 덮어씁니다. 또한 Security Services Display(보안 서비스 표시) 페이지의 보안 서비스 설정은 가져온 구성과 일치하도록 설정됩니다.

참고 Security Management Appliance의 URL 카테고리 집합보다 이전 URL 카테고리 집합을 사용하는 구성 파일을 가져오려고 하면 로드에 실패합니다.

단계 **1** Web Security Appliance에서 구성 파일을 저장합니다.

단계 **2** Security Management Appliance에서 **Web**(웹) > **Utilities**(유틸리티) > **Configuration Masters**(구성 마스터)를 선택합니다.

단계 **3** Options(옵션) 열에서 **Import Configuration**(구성 가져오기)을 클릭합니다.

단계 **4** Select Configuration(구성 선택) 드롭다운 목록에서 **Web Configuration File**(웹 구성 파일)을 선택합니다.

단계 **5** New Master Defaults(새 마스터 기본값) 섹션에서 **Browse**(찾아보기)를 클릭하고 Web Security Appliance에서 유효한 구성 파일을 선택합니다.

단계 **6** **Import File**(파일 가져오기)를 클릭합니다.

단계 **7** **Import**(가져오기)를 클릭합니다.

구성 마스터에서 직접 웹 보안 기능 구성

버전에 따라 구성 마스터에서 다음 기능을 구성할 수 있습니다.

• ID/식별 프로필 • SaaS 정책 • 암호 해독 정책 • 라우팅 정책 • 액세스 정책 • 웹 트래픽 TAP 정책 참고 웹 트래픽 TAP 정책을 정의하려면 Web Security Appliance에서 웹 트래픽 TAP 기능을 활성화해야 합니다. • 전체 대역폭 제한	• Cisco 데이터 보안 • 아웃바운드 악성프로그램 검색 • 외부 데이터 손실 방지	• SOCKS 정책 • 맞춤형 URL 범주 • 정의된 시간 범위 및 할당량 • Bypass 설정 • L4 트래픽 모니터

구성 마스터에서 직접 각 기능의 설정을 구성하려면 **Web(웹) > Configuration Master(구성 마스터)** <*version*> **>** <*feature*>를 선택합니다.

구성 마스터에서 기능 구성 시 SMA만의 다른 점 , 349 페이지에서 설명한 몇 가지 항목을 제외하고, 구성 마스터에서 기능을 구성하기 위한 지침은 Web Security Appliance에서 동일한 기능을 구성하기 위한 지침과 동일합니다. 자세한 내용은 사용 중인 Web Security Appliance의 온라인 도움말 또는 구성 마스터 버전에 해당하는 AsyncOS 버전의 AsyncOS for Cisco Web Security Appliances User Guide를 참조하십시오. 필요한 경우 사용할 구성 마스터 버전 결정, 344 페이지 섹션을 참조하여 Web Security Appliance에 맞는 구성 마스터를 결정합니다.

모든 버전의 Web Security 사용자 가이드는 https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html에서 확인할 수 있습니다.

구성 마스터에서 기능 구성 시 SMA만의 다른 점

구성 마스터에서 기능을 구성할 때 Web Security Appliance에서 직접 구성하는 경우와 비교하면 다음과 같은 차이점이 있습니다.

표 *74:* 기능 구성*:* 구성 마스터와 *WSA*의 차이점

기능 또는 페이지	세부 사항
모든 기능, 특히 각 릴리스의 새로운 기능	구성 마스터에서 구성하는 각 기능은 Web Security Appliance의 Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시)에서 활성화해야 합니다. 자세한 내용은 일관성 있는 기능 활성화 보장 , 351 페이지을(를) 참고하십시오.
ID/식별 프로필	• 구성 마스터에서 ID/식별 프로필을 다루는 법 , 350 페이지를 참조하십시오. • 투명 사용자 식별을 지원하는 인증 영역을 가진 Web Security Appliance가 관리 어플라이언스로 추가된 경우 ID/식별 프로필 추가 또는 수정 시 **Identify Users Transparently(**투명하게 사용자 식별**)** 옵션이 제공됩니다.

기능 또는 페이지	세부 사항
Cisco ISE를 사용하여 사용자를 식별하는 정책	약 5분 간격으로 SGT(Secure Group Tag) 정보가 Web Security Appliance로부터 업데이트됩니다. 관리 어플라이언스는 ISE 서버와 직접 통신하지 않습니다. 온디맨드 방식으로 SGT 목록을 업데이트하려면 **Web(**웹**) > Utilities(**유틸리티**) > Web Appliance Status(**웹 어플라이언스 상태**)**를 선택하고 ISE 서버와 연결된 Web Security Appliance를 클릭한 다음 **Refresh Data(**데이터 새로고침**)**를 클릭합니다. 필요에 따라 다른 어플라이언스에서도 반복합니다. 일반적인 구축 시나리오는 회사에 모든 WSA가 연결할 ISE 서버(ISE의 전체 포인트)가 하나뿐인 경우입니다. 서로 다른 데이터가 있는 다중 ISE 서버는 지원되지 않습니다.
액세스 정책 > 그룹 수정	정책 구성원 정의 섹션에서 ID/식별 프로필 및 사용자 옵션을 구성할 때 외부 디렉터리 서버를 사용한다면 다음이 적용됩니다. 그룹 수정 페이지에서 그룹을 검색할 경우 일치하는 첫 500개 결과만 표시됩니다. 원하는 그룹이 없으면 "승인된 그룹" 목록에 추가할 수 있습니다. 디렉터리 검색 필드에 입력하고 **Add(**추가**)** 버튼을 클릭하면 됩니다.
액세스 정책 > 웹 평판 및 악성 코드 차단 설정	
SaaS 정책	투명한 사용자 식별을 지원하는 인증이 있는 Web Security Appliance가 관리되는 어플라이언스로 추가된 경우에만 인증 옵션 "Prompt SaaS users who have been discovered by transparent user identification(투명한 사용자 식별로 검색된 SaaS 사용자 프롬프트)"을 사용할 수 있습니다.

구성 마스터에서 ID/식별 프로필을 다루는 법

Security Management Appliance에서 ID/식별 프로필을 만들 때, 이를 특정 어플라이언스에만 적용할 수 있는 옵션이 있습니다. 예를 들어 Security Management Appliance를 구매하고 기존 Web Security Appliance 구성 및 각 Web Security Appliance에 대해 만든 정책을 유지하려는 경우, 시스템에 한 파일을 로드한 다음 다른 시스템의 정책을 직접 추가해야 합니다.

그 방법 중 하나는 어플라이언스별로 ID/식별 프로필 집합을 생성한 다음 이 ID/식별 프로필을 참조하는 정책을 마련하는 것입니다. Security Management Appliance에서 구성을 게시할 때 ID/식별 프로필 및 이를 참조하는 정책은 자동으로 제거되고 비활성화됩니다. 이 방법을 사용하면 아무것도 수동으로 구성할 필요 없습니다. 사실상 '어플라이언스별' ID/식별 프로필입니다.

이 방법의 유일한 난제는 사이트에 따라 다른 기본 정책 아니면 ID/식별 프로필이 있는 경우입니다. 예를 들어 어떤 사이트에서는 "인증 시 기본 허용", 다른 사이트에서는 "기본 거부"로 설정된 정책이 있습니다. 그러한 경우 기본 프로필 및 정책 바로 위에 어플라이언스별 ID/식별 프로필 및 정책을 생성하여 이른바 나만의 '기본' 정책을 생성해야 합니다.

일관성 있는 기능 활성화 보장

구성 마스터를 게시하기에 앞서 이 마스터가 게시될 것이고 그러면 기대했던 기능이 활성화되어 구성될 것임을 확인해야 합니다.

이렇게 하려면 다음을 모두 수행합니다.

- 활성화된 기능 비교 , 351 페이지
- 게시할 기능 활성화 , 352 페이지

참고 서로 다른 기능이 활성화된 여러 Web Security Appliance가 동일한 구성 마스터에 할당된 경우, 각 어플라이언스에 별도로 게시해야 하며 게시하기 전 다음 절차를 수행해야 합니다.

활성화된 기능 비교

각 Web Security Appliance에서 활성화된 기능이 해당 어플라이언스와 연결된 구성 마스터에 대해 활성화된 기능과 일치하는지 확인합니다.

참고 서로 다른 기능이 활성화된 여러 Web Appliance Service가 동일한 구성 마스터에 할당된 경우 각 어플라이언스에 따로 게시해야 하며 게시하기 전마다 이 점검을 수행해야 합니다.

단계 **1** Security Management Appliance에서 **Web(**웹**) > Utilities(**유틸리티**) > Web Appliance Status(**웹 어플라이언스 상태**)**를 선택합니다.

단계 **2** 구성 마스터를 게시할 Web Security Appliance의 이름을 클릭합니다.

단계 **3** **Security Services(**보안 서비스**)** 테이블로 스크롤합니다.

단계 **4** 모든 활성화된 기능에 대한 기능 키가 만료되지 않은 활성 상태임을 확인합니다.

단계 **5** **Services(**서비스**)** 열의 설정을 비교합니다.

Web Appliance Service(웹 어플라이언스 서비스**)** 열과 **Is Service Displayed on Management Appliance(**관리 어플라이언스에서 서비스 표시**)?** 열이 일치해야 합니다.

- 활성 = 예
- 비활성 및 구성되지 않음 = 아니요 또는 비활성
- N/A = 해당 없음 예를 들어 구성 마스터에서는 구성 불가한 옵션이지만 목록에 포함되어 기능 키 상태를 볼 수 있는 경우도 있습니다.

구성 불일치는 빨간색 텍스트로 표시됩니다.

다음에 수행할 작업

어떤 기능의 활성/비활성 설정이 일치하지 않을 경우 다음 중 하나를 수행합니다.

- 구성 마스터에 대한 설정을 변경합니다. 게시할 기능 활성화 , 352 페이지를 참조하십시오.
- WSA에서 기능을 활성화하거나 비활성화합니다. 일부 변경은 여러 기능에 영향을 미칠 수 있습니다. AsyncOS for Cisco Web Security Appliances 사용 설명서에서 관련 기능에 대한 정보를 참조하십시오.

게시할 기능 활성화

구성 마스터를 사용하여 설정을 게시하려는 기능을 활성화합니다.

시작하기 전에

어떤 기능을 활성화하고 비활성화할지 결정합니다. 활성화된 기능 비교 , 351 페이지를 참조하십시오.

단계 **1** Security Management Appliance에서 **Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시)**를 선택합니다.

단계 **2** **Edit Settings(설정 수정)**를 클릭합니다.

Edit Security Services Display(보안 서비스 표시 수정) 페이지에서는 각 구성 마스터에 나타난 기능을 나열합니다.

어떤 기능에 "N/A"라고 표시되면 해당 구성 마스터 버전에서는 사용할 수 없습니다.

참고 웹 프록시는 기능으로 나열되지 않습니다. Web Security Appliance의 관리 대상 정책 유형 중 하나라도 실행하려면 웹 프록시가 활성 상태여야 하기 때문입니다. 웹 프록시를 비활성화하면 Web Security Appliance에 게시된 정책이 모두 무시됩니다.

단계 **3** (선택 사항) 사용하지 않을 구성 마스터는 숨깁니다. 지침 및 주의 사항은 미사용 구성 마스터 비활성화 , 353 페이지의 내용을 참조하십시오.

단계 **4** 사용할 각 구성 마스터에 대해, 활성화할 각 기능의 Yes(예) 확인란을 선택하거나 선택 취소합니다.

특정 기능에 대한 특별한 참고 사항(사용 가능한 옵션은 구성 마스터 버전에 따라 다름):

- Transparent(투명) 모드. 전달 모드를 사용할 경우 프록시 바이패스 기능을 사용할 수 없습니다.
- HTTPS 프록시. HTTPS 프록시가 활성화되어야 해독 정책을 구성할 수 있습니다.
- 업스트림 프록시 그룹 라우팅 정책을 사용하려면 Web Security Appliance에서 업스트림 프록시 그룹이 사용 가능해야 합니다.

단계 **5** **Submit(제출)**을 클릭합니다. 보안 서비스 설정에 대해 변경한 내용이 Web Security Appliance에서 구성한 정책에 영향을 미치는 경우 GUI에 특정 경고 메시지가 표시됩니다. 변경 사항을 제출하려면 **Continue(계속)**를 클릭합니다.

단계 **6** **Security Services Display(보안 서비스 표시)** 페이지에서 선택한 각 옵션에 **Yes(예)**가 나타남을 확인합니다.

단계 **7** 변경 사항을 커밋합니다.

다음에 수행할 작업

- 모든 기능이 게시될 어플라이언스에 대해 올바르게 활성화 또는 비활성화되었음을 확인합니다. 활성화된 기능 비교 , 351 페이지를 참조하십시오.

- 게시할 각 Web Security Appliance에서, 구성 마스터에 대해 활성화한 기능과 일관되게 기능이 활성화되었는지 확인합니다.

미사용 구성 마스터 비활성화

미사용 구성 마스터는 표시하지 않게 할 수 있습니다.

그러나 하나 이상의 구성 마스터가 활성화되어야 합니다.

참고 구성 마스터가 비활성화된 경우, 해당 구성 마스터 탭을 비롯하여 이에 대한 모든 참조가 GUI에서 제거됩니다. 구성 마스터를 사용하는 보류 중인 게시 작업이 삭제되고, 숨겨진 구성 마스터에 할당된 모든 Web Security Appliance가 할당되지 않은 상태로 재분류됩니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시)**를 선택합니다.

단계 **2** **Edit Settings(설정 수정)**를 클릭합니다.

단계 **3** 미사용 구성 마스터의 확인란을 선택 취소합니다

단계 **4** 변경 사항을 제출 및 커밋합니다.

고급 파일 게시를 사용하기 위한 설정

구성 마스터를 사용하도록 시스템이 설정된 경우 이미 고급 파일 게시에 대해 설정된 상태입니다.

그렇지 않으면 다음 주제의 절차를 수행합니다. 이는 고급 파일 게시 및 구성 마스터 게시에도 적용됩니다.

- SMA에서 중앙 구성 관리 활성화, 344 페이지
- 구성 마스터 초기화 , 345 페이지
- Web Security Appliances와 구성 마스터 연결 정보, 345 페이지

WSA에 구성 게시

- 구성 마스터 게시 , 353 페이지
- 고급 파일 게시를 사용하여 구성 마스터 게시, 357 페이지

구성 마스터 게시

구성 마스터에서 설정을 수정하거나 가져온 후 구성 마스터와 연결된 Web Security Appliance에 게시할 수 있습니다.

구성 마스터를 게시하기 전에

구성 마스터를 게시하면 이와 연결된 Web Security Appliance에서 기존의 정책 정보를 덮어씁니다.

구성 마스터를 사용하여 구성할 수 있는 설정에 대한 자세한 내용은 올바른 구성 게시 방법 결정 , 342 페이지 섹션을 참조하십시오.

모든 게시 작업

- (처음에만) 중앙에서 WSA를 관리하기 위한 구성 마스터 설정 , 342 페이지의 절차를 수행해야 합니다.
- 구성 마스터의 게시를 보장하고 게시 후 원하는 기능 집합이 활성화되도록 하려면, 각 Web Security Appliance 및 연결된 구성 마스터의 기능 집합을 확인하고 필요한 대로 변경합니다. 활성화된 기능 비교 , 351 페이지 및 필요하다면 게시할 기능 활성화 , 352 페이지도 참조하십시오. 타겟 어플라이언스에서 활성화하지 않은 기능에 대해 구성을 게시할 경우 그 구성은 적용되지 않습니다.

동일한 구성 마스터에 할당된 서로 다른 Web Security Appliance에서 다양한 기능이 활성화된 경우 각 어플라이언스에 따로 게시해야 하며 게시하기 전마다 기능을 확인하고 활성화해야 합니다.

게시 중에 나타난 구성 불일치를 확인하려면 게시 기록 보기, 359 페이지를 참조하십시오.

- 게시된 구성에 문제가 있는 경우 기존 구성을 복원할 수 있도록 게시하기 전에 각 대상 Web Security Appliance에서 구성 파일을 저장합니다. 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.
- Web Security Appliance에서 커밋할 때 웹 프록시 재시작을 일으킬 수 있는 변경 사항은 Security Management Appliance에서 게시할 때에도 프록시 재시작을 일으키게 됩니다. 이 경우 경고가 표시됩니다.

웹 프록시가 재시작하면 일시적으로 웹 보안 서비스가 중단됩니다.

- ID/식별 프로필의 변경사항을 게시할 경우 모든 엔드유저가 재인증해야 합니다.

특수 상황

- 대상 Web Security Appliance에서 AsyncOS를 복귀할 경우 해당 어플라이언스에 다른 구성 마스터를 연결해야 할 수 있습니다.
- 활성화된 투명 사용자 식별로 구성된 영역이 없는 Web Security Appliance에 구성 마스터를 게시하지만 ID/식별 프로필 또는 SaaS 정책에서 투명 사용자 식별을 선택한 경우:
  - ID/식별 프로필의 경우 투명 사용자 식별이 비활성화되고 필수 인증 옵션이 대신 선택됩니다.
  - SaaS 정책에서는 투명 사용자 식별 옵션이 비활성화되고 기본 옵션(프록시 인증을 위해 항상 SaaS 사용자 프롬프트)이 대신 선택됩니다.

- 하나의 Security Management Appliance에서 RSA에 대해 구성되지 않은 여러 Web Security Appliance로 외부 DLP 정책을 게시할 경우, Security Management Appliance에서 다음 게시 상태 경고를 전송합니다.

"구성 마스터 <*version*>에 대해 구성된 보안 서비스 표시 설정이 현재 이 게시 요청과 연결된 웹 어플라이언스에 있는 보안 서비스 중 하나 이상의 상태를 반영하지 않습니다. 해당 어플라이언스는 "**<*WSA Appliance Names*>**"입니다. 이는 이 특정 구성 마스터에 대한 보안 서비스 표시 설정이 잘못 구성되었음을 나타낼 수 있습니다. 각 어플라이언스의 웹 어플라이언스 상태 페이지에서 세부사항을 확인하며 트러블슈팅할 수 있습니다. 구성 게시를 계속 진행하시겠습니까**?**"

게시를 계속 진행하기로 한 경우, RSA 서버에 대해 구성되지 않은 Web Security Appliance는 외부 DLP 정책을 수신하지만, 이러한 정책은 비활성화됩니다. 외부 DLP 서버가 구성되지 않은 경우 Web Security Appliance External DLP 페이지에는 게시된 정책이 표시되지 않습니다.

구성 마스터의 **ID/**식별 프로필에 있는 체계가 다음과 같은 경우	**WSA**의 **ID/**식별 프로필의 체계
Kerberos 사용	NTLMSSP 또는 기본 사용
Kerberos 또는 NTLMSSP 사용	NTLMSSP 사용
Kerberos, NTLMSSP 또는 기본 사용	NTLMSSP 또는 기본 사용

지금 구성 마스터 게시

시작하기 전에

구성 마스터를 게시하기 전에 , 354 페이지의 중요 요구 사항 및 정보를 참조하십시오.

단계 **1** Security Management Appliance에서 **Web(**웹**) > Utilities(**유틸리티**) > Publish to Web Appliances(**웹 어플라이언스에 게시**)**를 선택합니다.

단계 **2** **Publish Configuration Now(**지금 구성 게시**)**를 클릭합니다.

단계 **3** "시스템에서 생성한 작업 이름"이 기본적으로 선택되지만 80자 이하의 사용자 정의 작업 이름을 입력할 수 있습니다.

단계 **4** 게시할 구성 마스터를 선택합니다.

단계 **5** 구성 마스터를 게시할 Web Security Appliance를 선택합니다. 구성 마스터에 할당된 모든 어플라이언스에 구성을 게시하려면 "All assigned appliances(할당된 모든 어플라이언스)"를 선택합니다.

또는

"목록의 어플라이언스 선택"을 선택하여 구성 마스터에 지정된 어플라이언스의 목록을 표시합니다. 구성을 게시할 어플라이언스를 선택합니다.

단계 **6** **Publish(**게시**)**를 클릭합니다.

게시 진행 중 페이지의 빨간색 진행 표시줄 및 텍스트에서 게시 중에 오류가 발생했음을 알려줍니다. 다른 작업이 현재 게시 중일 경우 이전 작업이 완료되면 요청이 실행됩니다.

참고 진행 중 작업의 세부 사항이 **Web(웹) > Utilities(유틸리티) > Publish to Web Appliances(웹 어플라이언스에 게시)** 페이지에도 나타납니다. 진행 중 게시 페이지에 액세스하려면 **Check Progress(진행 상황 점검)**를 클릭합니다.

다음에 수행할 작업

게시가 성공적으로 완료되었음을 확인합니다. 게시 기록 보기, 359 페이지를 참조하십시오. 완전히 게시되지 않은 항목이 표시됩니다.

나중에 구성 마스터 게시

시작하기 전에

구성 마스터를 게시하기 전에 , 354 페이지의 중요 요구 사항 및 정보를 참조하십시오.

단계 **1** Security Management Appliance에서 **Web(웹) > Utilities(유틸리티) > Publish to Web Appliances(웹 어플라이언스에 게시)**를 선택합니다.

단계 **2** **Schedule a Job(작업 예약)**을 클릭합니다.

단계 **3** "시스템에서 생성한 작업 이름"이 기본적으로 선택되지만 80자 이하의 사용자 정의 작업 이름을 입력할 수 있습니다.

단계 **4** 구성 마스터를 게시할 날짜와 시간을 선택합니다.

단계 **5** 게시할 구성 마스터를 선택합니다.

단계 **6** 구성 마스터를 게시할 Web Security Appliance를 선택합니다. 구성 마스터에 할당된 모든 어플라이언스에 구성을 게시하려면 "All assigned appliances(할당된 모든 어플라이언스)"를 선택합니다.

또는

"목록의 어플라이언스 선택"을 선택하여 구성 마스터에 지정된 어플라이언스의 목록을 표시합니다. 구성을 게시할 어플라이언스를 선택합니다.

단계 **7** **Submit**을 클릭합니다.

단계 **8** **Web(웹) > Utilities(유틸리티) > Publish to Web Appliances(웹 어플라이언스에 게시)** 페이지에서 예약된 작업의 목록을 봅니다. 예약된 작업을 수정하려면 작업의 이름을 클릭합니다. 보류 중 작업을 취소하려면 해당 휴지통 아이콘을 클릭하고 작업을 삭제할 것임을 확인합니다.

단계 **9** 게시가 완전히 성공했는지 확인하기 위해 예약된 게시 시간 이후 직접 확인하기 위한(예: 자신의 달력에서) 미리 알림을 만들 수 있습니다.

참고 예약된 게시 작업이 발생하기 전에 어플라이언스를 재부팅 또는 업그레이드하려면 작업을 다시 예약해야 합니다.

다음에 수행할 작업

게시가 성공적으로 완료되었음을 확인합니다. 게시 기록 보기, 359 페이지를 참조하십시오. 완전히 게시되지 않은 항목이 표시됩니다.

명령행 인터페이스를 사용하여 구성 마스터 게시

참고 구성 마스터를 게시하기 전에 , 354 페이지의 중요 요구 사항 및 정보를 참조하십시오.

Security Management Appliance에서는 다음 CLI 명령을 사용하여 구성 마스터를 통해 변경사항을 게시할 수 있습니다.

publishconfig config_master [*--job_name*] [*--host_list* | *host_ip*]

여기서 **config_master**는 지원되는 구성 마스터 버전입니다. 이 키워드는 필수 항목입니다. *job_name* 옵션은 선택 사항이며, 지정하지 않으면 생성됩니다.

host_list 옵션은 Web Security Appliance가 게시될 호스트 이름 또는 IP 주소의 목록이며, 지정하지 않으면 구성 마스터에 지정된 모든 호스트에 게시됩니다. *host_ip* 옵션에서는 여러 호스트 IP 주소가 쉼표로 구분될 수도 있습니다.

publishconfig 명령의 성공을 확인하려면 **smad_logs** 파일을 점검합니다. Security Management Appliance GUI에서 **Web(웹) > Utilities(유틸리티) > Web Appliance Status(웹 어플라이언스 상태)**에서도 기록 게시가 성공했음을 확인할 수 있습니다. 이 페이지에서 기록 게시 세부사항을 표시할 웹 어플라이언스를 선택합니다. 또는 **Web(웹) > Utilities(유틸리티) > Publish(게시) > Publish History(기록 게시)**에서 기록 게시 페이지로 이동할 수 있습니다.

고급 파일 게시를 사용하여 구성 마스터 게시

로컬 파일 시스템에서 관리 대상 Web Security Appliance로 호환되는 XML 구성 파일을 푸시하려면 고급 파일 게시를 사용합니다.

고급 파일 게시를 사용하여 구성할 수 있는 설정에 대한 자세한 내용은 올바른 구성 게시 방법 결정 , 342 페이지를 참조하십시오.

고급 파일 게시를 수행하려면

- 고급 파일 게시: 지금 구성 게시, 357 페이지
- 고급 파일 게시: 나중에 게시, 358 페이지

고급 파일 게시: 지금 구성 게시

시작하기 전에

- 게시할 구성의 버전이 게시 대상 어플라이언스의 AsyncOS 버전과 호환되는지 확인합니다. http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html 에서 호환성 매트릭스를 참조하십시오.

- 각 대상 Web Security Appliance에서 Web Security Appliance의 기존 구성을 구성 파일로 백업합니다. 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

단계 **1** 소스 Web Security Appliance에서 구성 파일을 저장합니다.

Web Security Appliance에서 구성 파일을 저장하는 방법에 대한 지침은 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

단계 **2** Security Management Appliance 창에서 **Web(**웹**) > Utilities(**유틸리티**) > Publish to Web Appliances(**웹 어플라이언스에 게시**)**를 선택합니다.

단계 **3** **Publish Configuration Now(**지금 구성 게시**)**를 클릭합니다.

단계 **4** "시스템에서 생성한 작업 이름"이 기본적으로 선택되지만 80자 이하의 작업 이름을 입력할 수 있습니다.

단계 **5** **Configuration Master to Publish(**게시할 구성 마스터**)**에서 **Advanced file options(**고급 파일 옵션**)**를 선택합니다.

단계 **6** **Browse(**찾아보기**)**를 클릭하여 1단계에서 저장한 파일을 선택합니다.

단계 **7** 웹 어플라이언스 드롭다운 목록에서 **Select appliances in list(**목록의 어플라이언스 선택**)** 또는 **All assigned to Master(**마스터에 할당된 모두**)**를 선택하여 구성 파일을 게시할 어플라이언스를 선택합니다.

단계 **8** **Publish(**게시**)**를 클릭합니다.

고급 파일 게시: 나중에 게시

시작하기 전에

- 게시할 구성의 버전이 게시 대상 어플라이언스의 AsyncOS 버전과 호환되는지 확인합니다. http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html 에서 호환성 매트릭스를 참조하십시오.
- 각 대상 Web Security Appliance에서 Web Security Appliance의 기존 구성을 구성 파일로 백업합니다. 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

단계 **1** 소스 Web Security Appliance에서 구성 파일을 저장합니다.

Web Security Appliance에서 구성 파일을 저장하는 방법에 대한 지침은 AsyncOS for Cisco Web Security Appliances 사용 설명서를 참조하십시오.

단계 **2** Security Management Appliance에서 **Web(**웹**) > Utilities(**유틸리티**) > Publish to Web Appliances(**웹 어플라이언스에 게시**)**를 선택합니다.

단계 **3** **Schedule a Job(**작업 예약**)**을 클릭합니다.

단계 **4** 시스템에서 생성한 작업 이름이 기본적으로 선택되지만 80자 이하의 작업 이름을 입력할 수 있습니다.

단계 **5** 구성을 게시할 날짜와 시간을 선택합니다.

단계 **6** **Configuration Master to Publish(**게시할 구성 마스터**)**에서 **Advanced file options(**고급 파일 옵션**)**를 선택하고 **Browse(**찾아보기**)**를 클릭하여 1단계에서 저장한 구성 파일을 선택합니다.

단계 **7** 웹 어플라이언스 드롭다운 목록에서 **Select appliances in list(**목록의 어플라이언스 선택**)** 또는 **All assigned to Master(**마스터에 할당된 모두**)**를 선택하여 구성 파일을 게시할 어플라이언스를 선택합니다.

단계 **8** **Publish(**게시**)**를 클릭합니다.

게시 작업 상태 및 기록 보기

보려는 내용	수행해야 할 작업
예약되었지만 아직 실행되지 않은 게시 작업의 목록	**Web(**웹**) > Utilities(**유틸리티**) > Publish to Web Appliances(**웹 어플라이언스에 게시**)**를 선택하고 **Pending Jobs(**보류 중 작업**)** 섹션에서 찾아봅니다.
어플라이언스별로 마지막으로 게시한 구성의 목록	**Web(**웹**) > Utilities(**유틸리티**) > Web Appliance Status(**웹 어플라이언스 상태**)**를 선택하고 **Last Published Configuration(**마지막으로 게시된 구성**)** 정보를 확인합니다.
현재 진행 중인 게시 작업의 상태.	**Web(**웹**) > Utilities(**유틸리티**) > Publish to Web Appliances(**웹 어플라이언스에 게시**)**를 선택하고 **Publishing Progress(**게시 진행 상황**)** 섹션에서 찾아봅니다.
모든 또는 어떤 어플라이언스에 대한 모든 또는 어떤 게시 작업의 기록	게시 기록 보기를 참조하십시오.

게시 기록 보기

게시 기록 보기는 게시 중에 오류가 발생했는지 확인하거나 구성된 기능과 타겟 어플라이언스에서 활성화된 기능 간의 불일치를 찾아내는 데 유용합니다.

단계 **1** Security Management Appliance에서 **Web(**웹**) > Utilities(**유틸리티**) > Publish History(**기록 게시**)**를 선택합니다.

단계 **2** 특정 작업의 세부사항을 보려면 작업 이름 열에서 작업 이름을 클릭합니다.

단계 **3** 추가 정보를 확인합니다.

- 작업에서 특정 어플라이언스에 대한 상태 세부사항을 보려면 **Details(**세부사항**)** 링크를 클릭합니다.

웹 어플라이언스 게시 세부사항 페이지가 나타납니다.

- 작업에서 특정 어플라이언스에 대한 추가 세부사항을 보려면 어플라이언스 이름을 클릭합니다.

Web(웹**) > Utilities(**유틸리티**) > Web Appliance Status(**웹 어플라이언스 상태**)** 페이지가 나타납니다.

중앙 업그레이드 관리

단일 SMA(Security Management Appliance)를 사용하여 여러 WSA(Web Security Appliance)를 동시에 업그레이드할 수 있습니다. 또한 각 WSA에 서로 다른 소프트웨어 업그레이드를 적용할 수 있습니다.

Web Security Appliance에 대한 중앙 업그레이드 관리 설정

다음 단계에 따라 이 Security Management Appliance에서 중앙 집중식 업그레이드 서비스를 구성합니다.

중앙 업그레이드 관리자 활성화

시작하기 전에

- 중앙 집중식 업그레이드 관리를 활성화하려면 우선 모든 Web Security Appliance를 구성하고 예상대로 작동하는지 확인해야 합니다.
- 중앙 집중식 업그레이드를 수신할 각 관리되는 Web Security Appliance에서 개별적으로 중앙 집중식 업그레이드를 활성화해야 합니다.

참고 CLI에서 중앙 집중식 업그레이드를 활성화하려면 다음을 사용합니다.

```
applianceconfig > services > [...] > Enable Centralized Upgrade > Y
```

- Security Management Appliance에 적절한 기능 키가 설치되어 있어야 합니다.

단계 **1** Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**)** 페이지를 선택한 다음 **Centralized Services(**중앙 집중식 서비스**) > Centralized Upgrade Manager(**중앙 집중식 업그레이드 관리자**)**를 선택합니다.

단계 **2** **Edit Settings(**설정 편집**)**를 클릭합니다.

단계 **3** **Enable(**활성화**)** 체크 박스를 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

각 매니지드 **Web Security Appliance**에 중앙 집중식 업그레이드 서비스 추가

Manager Security Management Appliance에서 중앙 집중식 업그레이드 관리자를 활성화한 후 개별 매니지드 WSA에서 중앙 집중식 업그레이드를 활성화하여 Upgrade Manager 등록 명부에 원하는 Web Security Appliance를 추가해야 합니다.

단계 **1** Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**)** 페이지를 선택한 다음 **Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

단계 **2** Web Security Appliance를 아직 추가하지 않은 경우나 중앙 집중식 업그레이드 관리를 위한 추가 어플라이언스를 추가해야 할 경우 다음을 수행합니다.

a) **Add Web Appliance(**웹 어플라이언스 추가**)**를 클릭합니다.

b) Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 어플라이언스 이름과 Web Security Appliance의 Management 인터페이스에 대한 IP 주소를 입력합니다.

참고 DNS 이름은 IP Address(IP 주소) 텍스트 필드에 입력해야 합니다. 그러나 **Submit(**제출**)**을 클릭하면 IP 주소로 해석됩니다.

c) **Centralized Upgrades(**중앙 집중식 업그레이드**)**를 선택해야 합니다.

d) **Establish Connection(**연결 설정**)**을 클릭합니다.

e) 관리할 어플라이언스에서 관리자 계정의 사용자 이름과 암호를 입력하고 **Establish Connection(**연결 설정**)**을 클릭합니다.

참고 로그인 자격 증명을 입력하여 Security Management Appliance에서 원격 어플라이언스로의 파일 전송을 위한 공개 SSH 키를 전달합니다. 로그인 자격 증명은 Security Management Appliance에 저장되지 않습니다.

페이지의 테이블 위에 Success(성공) 메시지가 나타날 때까지 기다립니다.

f) Test Connection(테스트 연결)을 클릭합니다.

테이블 위의 테스트 결과를 읽습니다.

g) **Submit(**제출**)**을 클릭합니다.

Centralized Upgrades(중앙 집중식 업그레이드) 관리를 활성화하는 동시에 매니지드 Web Security Appliance 목록에 추가할 각 WSA에 대해 이 절차를 반복합니다.

단계 **3** 이 매니지드 어플라이언스 목록에 이미 있는 WSA에 대해 업그레이드 Centralized Upgrades(중앙 집중식 업그레이드) 관리를 활성화하려면 다음을 수행합니다.

a) Edit Web Security Appliance Settings(Web Security Appliance 편집 설정) 페이지를 열 Web Security Appliance의 이름을 클릭합니다.

b) WSA Centralized Services(WSA 중앙 집중식 서비스) 섹션에서 **Centralized Upgrades(**중앙 집중식 업그레이드**)**를 선택합니다.

c) **Submit(**제출**)**을 클릭합니다.

중앙 집중식 업그레이드 관리를 활성화하려는 각 WSA에 대해 이 절차를 반복합니다.

단계 **4** 변경 사항을 커밋합니다.

다음에 수행할 작업

매니지드 어플라이언스의 목록을 추가하고 편집하는 데 대한 자세한 내용은 관리 대상 어플라이언스 추가 정보, 29 페이지의 내용을 참조하십시오.

WSA 업그레이드 선택 및 다운로드

단계 **1** Security Management Appliance에서 **Web(웹)** 페이지를 선택한 다음 **Utilities(유틸리티) > Centralized Upgrade(중앙 집중식 업그레이드)**를 선택합니다.

가장 최근에 업그레이드하도록 선택한 모든 어플라이언스와, 업그레이드 상태가 나열됩니다.

단계 **2** Centralized Upgrade(중앙 집중식 업그레이드) 페이지에서 **Upgrade Appliances(어플라이언스 업그레이드)** 버튼을 클릭합니다.

업그레이드할 수 있는 모든 매니지드 WSA가 나열됩니다.

단계 **3** 목록에서 해당 이름 앞의 확인란을 선택하여 업그레이드할 각 Web Security Appliance를 선택합니다.

단계 **4** **Download Wizard(다운로드 마법사)** 또는 **Download and Install Wizard(다운로드 및 설치 마법사)**를 클릭합니다.

Download Wizard(다운로드 마법사)에서는 선택한 WSA에 다운로드할 업그레이드 패키지를 선택할 수 있습니다. 이 작업은 다운로드 전용입니다. 나중에 다운로드한 패키지를 설치하고 각 시스템을 다시 시작할 수 있습니다.

다운로드 및 설치 마법사에서는 선택한 WSA에 다운로드하여 즉시 설치할 업그레이드 패키지를 선택할 수 있습니다. 설치 후에는 각 시스템이 자동으로 다시 시작됩니다.

단계 **5** 시작된 마법사의 Fetch Upgrades(업그레이드 가져오기) 페이지가 나타납니다. 선택한 WSA에 대해 사용 가능한 모든 업그레이드를 가져온 경우(WSA 매트릭스의 **Status(상태)** 열에 'Completed Fetching Available Upgrades(사용 가능한 업그레이드 가져오기가 완료됨)'라고 표시됨) **Next(다음)**를 클릭하여 계속합니다.

단계 **6** Available Upgrades(사용 가능한 업그레이드) 페이지에 선택한 각 WSA에 대해 사용 가능한 모든 업그레이드 빌드가 나열됩니다. 비교를 위해 최대 5개까지 선택한 후 **Next(다음)**를 클릭합니다.

단계 **7** 마법사의 업그레이드 선택 페이지에 각 WSA에 대해 선택한 업그레이드의 호환성 매트릭스가 표시됩니다. 각 WSA에 대해 원하는 업그레이드 빌드를 선택하고 **Next(다음)**를 클릭합니다.

단계 **8** Summary(요약) 페이지에 선택한 각 WSA 및 업그레이드 빌드에 대한 요약 정보가 나열됩니다. **Next(다음)**를 클릭하여 마법사를 계속합니다.

단계 **9** WSA 연결 상태와 같은 일련의 다운로드 확인 후, Review(검토) 페이지에 각 WSA의 다운로드 상태 목록이 표시됩니다. **Begin Download(다운로드 시작)**을 클릭하여 선택한 각 WSA에 업그레이드 패키지를 다운로드합니다.

프로세스가 진행되는 동안 Centralized Upgrade(중앙 집중식 업그레이드) 페이지에 다운로드 상태 정보가 표시됩니다.

다음에 수행할 작업

- **Download Wizard(다운로드 마법사)** - 이 절차를 시작할 때 이 버튼을 클릭한 경우 다운로드가 완료되 면 **Web(웹) > Utilities(유틸리티) > Centralized Upgrade(중앙 집중식 업그레이드)**를 선택

하거나 브라우저 창에서 페이지 새로 고침 버튼을 클릭하여 Centralized Upgrade(중앙 집중식 업그레이드) 페이지를 새로 고칩니다.

업그레이드할 수 있는 모든 매니지드 WSA 목록 외에도 이제 업그레이드 패키지가 다운로드된 모든 WSA가 Centralized Upgrade(중앙 집중식 업그레이드) 페이지의 다른 섹션에 나열됩니다. 각 항목과 함께 표시되는 휴지통 버튼을 클릭하면 해당 WSA에서 다운로드된 업그레이드 패키지를 삭제할 수 있습니다.

언제든지 이 목록에서 하나 이상의 WSA를 선택한 다음 설치 마법사를 클릭하여 선택한 각 WSA에서 다운로드된 업그레이드 패키지의 설치를 시작할 수 있습니다. WSA에서 설치가 완료되면 다시 시작됩니다. 이 마법사를 사용하는 방법에 대한 자세한 내용은 설치 마법사 사용, 363 페이지의 내용을 참조하십시오.

- **Download and Install Wizard(**다운로드 및 설치 마법사**)** – 이 절차를 시작할 때 이 버튼을 클릭하면 다운로드가 완료된 경우에 업그레이드 설치가 자동으로 시작됩니다. 이 프로세스에 대한 자세한 내용은 2단계 첫 부분의 설치 마법사 사용, 363 페이지을 참조하십시오. 설치가 완료되면 WSA가 다시 시작됩니다.

설치 마법사 사용

설치 마법사가 시작되면, 다운로드 및 설치 프로세스의 일부로 자동으로, 또는 다운로드했지만 아직 설치하지 않은 업그레이드 패키지와 하나 이상의 WSA를 선택한 후 Centralized Upgrade(중앙 집중식 업그레이드) 페이지에서 Install Wizard(설치 마법사) 버튼을 클릭할 경우에 다음 단계에 따라 설치를 구성합니다.

단계 **1** 이전에 업그레이드 패키지를 다운로드한 경우

a) Centralized Upgrade(중앙 집중식 업그레이드) 페이지의 Downloaded AsyncOS Versions(다운로드된 AsyncOS 버전) 섹션(**Web(**웹**) > Utilities(**유틸리티**) > Centralized Upgrade(**중앙 집중식 업그레이드**)**)를 통해 Web Appliances(웹 어플라이언스)에서 원하는 WSA를 선택합니다.

b) **Install Wizard(**설치 마법사**)**를 클릭합니다.

단계 **2** 마법사의 Upgrade Preparation(업그레이드 준비) 페이지에서 선택한 각 WSA에 대해 다음을 수행합니다.

- 해당 시스템의 `configuration` 디렉터리에 저장된 WSA 현재 구성의 백업 사본을 만들려면 업그레이드하기 전에 **configuration** 디렉터리에 현재 구성 저장을 선택합니다.
- **Save current configuration(**현재 구성 저장**)** 옵션을 선택하면 구성 파일에서 암호 마스킹을 선택하여 백업 사본에서 현재 구성 암호를 모두 마스킹할 수 있습니다. **Load Configuration(**로드 구성**)** 명령은 마스킹된 암호로 백업 파일을 다시 로드하는 데 할 수 없습니다.
- **Save current configuration(**현재 구성 저장**)** 옵션을 선택하면 **Email file to(**이메일로 파일 전송**)** 필드에 하나 이상의 이메일 주소를 입력할 수 있습니다. 백업 구성 파일 사본이 각 주소에 메일로 전송됩니다. 주소가 여러 개인 경우 쉼표로 구분해 주십시오.

단계 **3** **Next(**다음**)**를 클릭합니다.

단계 **4** Upgrade Summary(업그레이드 요약) 페이지에 선택한 각 WSA에 대한 업그레이드 준비 정보가 나열됩니다. **Next(**다음**)**를 클릭하여 마법사를 계속합니다.

단계 **5** 연결 상태와 같은 일련의 디바이스 확인 후에, Review(검토) 페이지에 각 WSA의 설치 상태 목록이 표시됩니다. 오류를 나타내는 디바이스의 선택을 취소할 수 있습니다. **Begin Install(**설치 시작**)**을 클릭하여 선택한 각 WSA에 업그레이드 패키지를 설치하기 시작합니다.

설치 상태 정보가 표시되는 Centralized Upgrade(중앙 집중식 업그레이드) 페이지로 돌아갑니다.

참고 설치가 완료되면 각 WSA가 다시 시작됩니다.

다음에 수행할 작업

참고 또는 WSA 자체에서 이전에 다운로드된 패키지의 설치 프로그램을 실행할 수도 있습니다. 즉, 다운로드된 업그레이드 패키지가 WSA의 **System Administration(**시스템 관리**) > System Upgrade(**시스템 업그레이드**)** 페이지에 Install(설치) 버튼과 함께 나열됩니다. 자세한 내용은 Cisco Web Security Appliances 사용 설명서에서 "AsyncOS 및 보안 서비스 구성 요소 업그레이드 및 업데이트"를 참조하십시오.

Web Security Appliance 상태 보기

웹 어플라이언스 상태 요약 보기

Web(웹**) > Utilities(**유틸리티**) >** Web Appliance Status(웹 어플라이언스 상태) 페이지에서 Security Management Appliance에 연결된 Web Security Appliance를 요약하여 보여줍니다.

웹 어플라이언스 상태 페이지에서는 연결된 Web Security Appliance의 목록을 표시합니다. 여기에는 어플라이언스 이름, IP 주소, AsyncOS 버전, 마지막으로 게시된 구성 정보(사용자, 작업 이름, 구성 버전), 활성화되었거나 비활성화된 보안 서비스 수, 연결된 어플라이언스 총 개수(최대 150개)가 포함되어 있습니다. 경고 아이콘은 연결된 어플라이언스 중 하나에 주의가 필요할 때 나타납니다.

개별 Web Security Appliance 상태 보기

어플라이언스 상태 페이지에서는 연결된 각 어플라이언스의 상태를 자세히 보여줍니다.

웹 어플라이언스 상태 페이지에서 관리 대상 Web Security Appliance의 세부 정보를 보려면 어플라이언스 이름을 클릭합니다.

상태 정보에는 연결된 Web Security Appliance의 일반 정보, 게시된 구성, 게시 기록, 기능 키 상태 등이 포함되어 있습니다.

참고 중앙 집중식 관리가 지원되는 시스템만이 표시에 사용할 수 있는 데이터를 가질 수 있습니다.

참고 Web Security Appliance의 사용 정책 제어 엔진의 버전이 Security Management Appliance의 버전과 일치하지 않을 경우 경고 메시지가 나타납니다. Web Security Appliance에서 서비스가 비활성화되었거나 없다면 'N/A'가 표시됩니다.

웹 어플라이언스 상태 세부사항

이 페이지의 정보 대부분은 Web Security Appliance에서 가져온 것입니다.

- 시스템 상태 정보(가동 시간, 어플라이언스 모델 및 일련 번호, AsyncOS 버전, 빌드 날짜, AsyncOS 설치 날짜 및 시간, 호스트 이름)
- 구성 게시 기록(게시 날짜/시간, 작업 이름, 구성 버전, 게시 결과, 사용자)
- 중앙 보고 상태 - 마지막으로 시도한 데이터 전송 시간 포함
- Web Security Appliance의 기능 상태(각 기능이 활성화되었는지 여부, 기능 키 상태)
- 관리 대상 및 관리 어플라이언스의 사용 정책 제어 엔진 버전
- Web Security Appliance의 AnyConnect Secure Mobility 설정
- 이 Web Security Appliance가 연결된 Cisco ISE(Identity Services Engine) 서버
- 이 Web Security Appliance의 프록시 설정(업스트림 프록시 및 프록시에 대한 HTTP 포트)
- 인증 서비스 정보(서버, 체계, 영역, 시퀀스, 투명 사용자 식별 지원 여부, 인증 실패 시 트래픽 차단 또는 허용 여부)

팁 Web Security Appliance에서 발생한 최신 구성 변경 사항이 Web Appliance Status(웹 어플라이언스 상태) 페이지에 반영되기까지 몇 분 정도 걸릴 수 있습니다. 데이터를 즉시 새로 고치려면 **Refresh Data(**데이터 새로 고침**)** 링크를 클릭합니다. 페이지의 타임스탬프는 데이터를 마지막으로 새로고침한 때를 알려줍니다.

URL 범주 집합 업데이트 준비 및 관리

웹 사용 관리에 사용할 수 있는 사전 정의된 최신 URL 범주 집합을 시스템에서 사용할 수 있도록 WUC(Web Usage Controls)용 URL 범주 집합이 때때로 업데이트될 수 있습니다. 기본적으로 Web Security Appliance는 Cisco에서 URL 범주 집합 업데이트를 자동으로 다운로드하며, Security Management Appliance는 관리되는 Web Security Appliance로부터 이러한 업데이트를 몇 분 내에 자동으로 수신합니다.

이러한 업데이트는 기존의 구성 및 어플라이언스 동작에 영향을 미칠 수 있으므로, 업데이트에 미리 대비하고 업데이트 후 적절한 작업을 수행해야 합니다.

다음과 같은 작업을 수행할 수 있습니다.

- URL 범주 집합 업데이트의 영향 이해 , 366 페이지
- URL 범주 집합 업데이트에 대한 알림 수신 확인 , 366 페이지
- 신규 및 변경된 범주에 대한 기본 설정 지정 , 366 페이지
- URL 범주 집합이 업데이트될 때 정책 및 ID/식별 프로필 설정 확인 , 366 페이지

URL 범주 집합 업데이트의 영향 이해

URL 범주 집합 업데이트가 이루어지면 구성 마스터의 기존 정책의 동작이 바뀔 수 있습니다.

URL 카테고리 집합 업데이트 전후에 수행해야 할 작업에 대한 필수 정보는 설명서 , 571 페이지에서 제공되는 링크의 AsyncOS for Cisco Web Security Appliances 사용 설명서에서 "URL 필터" 장의 "URL 카테고리 집합에 대한 업데이트 관리" 섹션을 참조하십시오. 범주 설명은 동일한 장의 "URL 범주 설명"에 나와 있습니다.

URL 범주 집합 업데이트에 대한 알림 수신 확인

수신할 내용	수행해야 할 작업
URL 범주 집합 업데이트의 사전 알림	Cisco Content Security Appliance에 대한 알림(URL 범주 집합 업데이트에 대한 알림 포함)을 수신하려면 지금 신청하십시오. Cisco 알림 서비스 , 571 페이지를 참조하십시오.
URL 범주 집합 업데이트가 기존의 정책 설정에 영향을 미친 경우 알림	**Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Alerts**(알림)로 이동하여, System(시스템) 범주에서 Warning(경고) 레벨 알림을 수신하도록 구성했는지 확인합니다. 알림에 대한 자세한 내용은 경고 관리, 464 페이지 섹션을 참조하십시오.

신규 및 변경된 범주에 대한 기본 설정 지정

URL 카테고리 집합 업데이트가 발생하기 전에, URL 필터링을 제공하는 각 정책에서 새 카테고리 및 병합된 카테고리에 대한 기본 작업을 지정해야 합니다. 또는 이미 이러한 설정이 이미 구성된 Web Security Appliance에서 구성을 가져올 수도 있습니다.

자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서 또는 Web Security Appliance의 온라인 도움말에서 "URL 필터링" 장의 "신규 및 변경 카테고리에 대한 기본 설정 선택" 섹션을 참조하십시오.

URL 범주 집합이 업데이트될 때 정책 및 ID/식별 프로필 설정 확인

URL 범주 집합 업데이트는 2가지 유형의 알림을 실행합니다.

- 범주 변경에 대한 알림
- 범주 변경으로 인해 변경되었거나 비활성화된 정책에 대한 알림

URL 범주 집합 변경에 대한 알림을 수신할 때 기존 URL 범주 기반 정책 및 ID/식별 프로필이 여전히 정책 목표를 충족하는지 확인해야 합니다.

주의가 필요한 변경 유형에 대한 자세한 내용은 AsyncOS for Cisco Web Security Appliances 사용 설명서의 "URL 카테고리 집합 업데이트에 대한 알림에 대응" 섹션을 참조하십시오.

AVC(Application Visibility and Control) 업데이트

SMA는 관리하는 대부분의 Web Security Appliance에 존재하는 AVC 엔진의 버전을 자동으로 사용합니다.

구성 관리 문제 트러블슈팅

- 구성 마스터 ID/식별 프로필에서 사용 가능한 그룹이 없음 , 367 페이지
- Configuration Master(구성 마스터) > Access Policies(액세스 정책) > Web Reputation and Anti-Malware Settings(웹 평판 및 악성코드 차단 설정) 페이지의 설정이 예상과 다름, 368 페이지
- 구성 게시 문제 트러블슈팅 , 368 페이지

구성 마스터 ID/식별 프로필에서 사용 가능한 그룹이 없음

문제

Web(웹) > Configuration Master(구성 마스터) > Identities/Identification Profiles(ID/식별 프로필)에서 정책 멤버십 정의 페이지의 선택된 그룹 및 사용자 아래에 그룹 옵션이 표시되지 않습니다.

솔루션

여러 Web Security Appliance를 사용하는 경우: 각 WSA의 Network(네트워크) > Authentication(인증)에서, 동일한 이름의 영역에 대해 모든 설정이 동일하지 않다면 영역 이름이 전체 WSA에서 고유한지 확인합니다.

팁 각 WSA의 영역 이름을 보려면 **Web(웹) > Utilities(유틸리티) > Web Appliance Status(웹 어플라이언스 상태)**로 이동합니다. 각 어플라이언스 이름을 클릭하고 세부 정보 페이지의 맨 아래로 스크롤합니다.

Configuration Master(구성 마스터) > Access Policies(액세스 정책) > Web Reputation and Anti-Malware Settings(웹 평판 및 악성코드 차단 설정) 페이지의 설정이 예상과 다름

문제

구성 마스터의 **Access Policies(액세스 정책) > Web Reputation and Anti-Malware Settings(웹 평판 및 악성코드 차단 설정)** 페이지에서 Web Reputation Score(웹 평판 점수) 임계값 설정 및 악성코드 검사 엔진 선택 기능 등 있어야 하는 설정이 누락되었습니다. 또는 Web Security Appliance에서 Adaptive Security를 사용할 때 이러한 설정이 포함되었습니다.

솔루션

사용 가능한 옵션은 Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시) 설정에서 해당 구성 마스터에 대해 Adaptive Security를 선택했는지 여부에 따라 달라집니다.

구성 게시 문제 트러블슈팅

문제

구성 게시 실패.

솔루션

Web(웹) > Utilities(유틸리티) > Web Appliance Status(웹 어플라이언스 상태) 페이지를 확인합니다. 다음과 같은 경우 게시가 실패합니다.

- "웹 어플라이언스 서비스" 열의 상태와 "관리 어플라이언스에서 서비스 표시" 열의 상태가 일치하지 않습니다.
- 두 열에서, 기능이 활성화되었지만 해당 기능 키가 활성화되지 않았음을(예: 만료됨) 보여줍니다.
- 구성 마스터 버전은 Web Security Appliance의 AsyncOS 버전과 일치해야 합니다. 더 새로운 Web Security Appliance에 더 이전의 구성 마스터 버전을 게시하는 경우, Web Security Appliance의 설정이 구성 마스터의 설정과 일치하지 않으면 게시가 실패할 수 있습니다. Web Appliance Status(웹 어플라이언스 상태) 페이지에 차이점이 표시되지 않는 경우 이 문제가 발생할 수 있습니다.

다음 작업:

- 게시 기록 보기, 359 페이지
- 활성화된 기능 비교 , 351 페이지
- 게시할 기능 활성화 , 352 페이지

11 장

시스템 상태 모니터링

이 장에는 다음 섹션이 포함되어 있습니다.

Security Management Appliance 상태 소개

기본적으로 System Status(시스템 상태) 페이지는 브라우저에서 Cisco Content Security Management Appliance에 액세스할 때 처음 나타나는 페이지입니다. (랜딩 페이지를 변경하려면 기본 설정 , 500 페이지 섹션을 참조하십시오.)

그 밖의 경우에 System Status(시스템 상태) 페이지에 액세스하려면 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > System Status(**시스템 상태**)**를 선택합니다.

모니터링 서비스를 활성화하고 관리 대상 어플라이언스를 추가하기 전에는 시스템 정보 섹션에서 상태 정보만 제공합니다. 시스템 설정 마법사를 실행하고 중앙 서비스를 활성화하고 관리 대상 어플라이언스를 추가하면 Centralized Services(중앙 서비스) 섹션 및 Security Appliance Data Transfer Status(보안 어플라이언스 데이터 전송 상태) 섹션에 데이터가 채워집니다.

다음과 같은 상태 정보가 제공됩니다.

- 중앙 집중식 서비스**:** 처리 대기열 사용량 등 각 중앙 집중식 서비스의 상태
- 시스템 가동 시간**:** 어플라이언스가 실행된 기간
- **CPU** 사용량**:** 각 모니터링 서비스의 CPU 용량 사용률
- 시스템 버전 정보**:** 모델 번호, AsyncOS(운영 체제) 버전, 빌드 날짜, 설치 날짜, 일련 번호

관련 주제

- 처리 대기열 모니터링 , 370 페이지
- CPU 사용률 모니터링 , 371 페이지
- 관리 대상 어플라이언스로부터의 데이터 전송 상태 모니터링 , 371 페이지

Security Management Appliance 용량 모니터링

- 처리 대기열 모니터링 , 370 페이지
- CPU 사용률 모니터링 , 371 페이지

처리 대기열 모니터링

이메일/웹 보고 및 추적의 처리 대기열 사용률을 정기적으로 점검하여 어플라이언스가 최적의 용량으로 실행 중인지 확인할 수 있습니다.

처리 대기열은 중앙 집중식 보고 및 추적 파일이 Security Management Appliance에 의해 처리될 때까지 대기하는 동안 이를 저장합니다. 일반적으로 Security Management Appliance는 보고 및 추적 파일의 배치를 받아 처리합니다. 관리 대상 어플라이언스에서 파일을 받아 Security Management Appliance에서 처리하는 과정에 처리 대기열의 보고 또는 추적 파일 비율이 오르내립니다.

참고 처리 대기열 비율은 대기열에 있는 파일 수를 측정합니다. 파일 크기를 고려하지 않습니다. 이 비율은 Security Management Appliance 처리 로드에 대한 대략적인 추정치일 뿐입니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > System Status(**시스템 상태**)**를 선택합니다.

단계 **3** 페이지 상단에 있는 **Centralized Services(**중앙 집중식 서비스**)** 섹션에서 다음에 대한 Processing Queue(처리 대기열) 비율을 확인합니다.

a) Centralized Reporting(중앙 집중식 보고)(Email Security 하위 섹션)
b) 중앙 메시지 추적
c) 중앙 보고(웹 보안 하위 섹션)

단계 **4** 처리 대기열 사용률이 몇 시간째 또는 며칠째 높은 상태라면 시스템의 용량 한도에 도달했거나 초과한 것입니다.

이 경우 Security Management Appliance에서 관리 대상 어플라이언스 중 일부를 제거하거나 Security Management Appliance를 추가 설치하거나, 이 두 가지 모두를 수행해 봅니다.

CPU 사용률 모니터링

Security Management Appliance가 각 중앙 집중식 서비스에 사용하는 CPU 용량의 비율을 보려면 다음을 수행합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > System Status(**시스템 상태**)**를 선택합니다.

단계 **3** **System Information(**시스템 정보**)** 섹션으로 스크롤하여 **CPU Utilization(CPU** 사용률**)** 하위 섹션을 봅니다.

CPU 사용률은 기본 중앙 집중식 서비스 각각에 사용되고 있는 Security Management Appliance의 CPU 프로세싱을 나타냅니다. 일부 서비스의 사용률은 합산될 수 있습니다. 예를 들어 이메일 보고는 "보고 서비스"에 합산되고 스팸, 정책, 바이러스, 보안 침해 격리는 "격리 서비스"에 합산됩니다. Security Management Appliance의 다른 작업은 "Security Management Appliance" 일반 제목 아래 그룹화됩니다.

단계 **4** 브라우저 화면을 새로 고치면 최신 데이터가 표시됩니다.

CPU 사용률은 계속 바뀝니다.

관리 대상 어플라이언스로부터의 데이터 전송 상태 모니터링

Security Management Appliance에서 중앙 집중식 관리 기능을 수행하려면 매니지드 어플라이언스에서 Security Management Appliance로의 데이터 전송이 성공적으로 이루어져야 합니다. Security Appliance Data Transfer Status(보안 어플라이언스 데이터 전송 상태) 섹션에서는 Security Management Appliance에서 관리하는 각 어플라이언스의 상태 정보를 제공합니다.

기본적으로 Security Appliance Data Transfer Status(보안 어플라이언스 데이터 전송 상태) 섹션에서는 최대 10대의 어플라이언스를 표시합니다. Security Management Appliance에서 관리하는 어플라이언스가 10대를 초과할 경우 Items Displayed(표시 항목) 메뉴를 사용하여 표시할 어플라이언스 수를 선택할 수 있습니다.

참고 데이터 전송 상태에 대한 요약 정보가 System Status(시스템 상태) 페이지 맨 위의 Services(서비스) 섹션에 나타납니다. Security Appliance Data Transfer Status(보안 어플라이언스 데이터 전송 상태) 섹션에서는 어플라이언스별 데이터 전송 상태를 보여줍니다.

System Status(시스템 상태) 페이지의 Security Appliance Data Transfer Status(보안 어플라이언스 데이터 전송 상태) 섹션에서 특정 어플라이언스의 연결 상태 문제를 확인할 수 있습니다. 어플라이언스의 각 서비스에 대한 상태를 자세히 보려면 어플라이언스 이름을 클릭하여 그 데이터 전송 상태 페이지를 표시합니다.

Data Transfer Status(데이터 전송 상태): *Appliance_Name* 페이지에서는 각 모니터링 서비스에 대해 마지막으로 데이터 전송이 일어난 때를 표시합니다.

Email Security Appliance의 데이터 전송 상태는 다음 중 하나일 수 있습니다.

- **Not enabled(**활성화되지 않음**):** 모니터링 서비스가 Email Security Appliance에서 활성화되지 않았습니다.
- **Never connected(**연결되지 않음**):** Email Security Appliance에서 모니터링 서비스는 활성화되지만 Email Security Appliance와 Security Management Appliance 간에 연결이 설정되지 않았습니다.
- **Waiting for data(**데이터 대기 중**):** Email Security Appliance가 데이터 수신을 기다리고 있는 Security Management Appliance에 연결되었습니다.
- **Connected and transferred data(**연결되어 데이터 전송**):** Email Security Appliance와 Security Management Appliance 간의 연결이 설정되었고 데이터가 성공적으로 전송되었습니다.
- **File transfer failure(**파일 전송 실패**):** Email Security Appliance와 Security Management Appliance 간의 연결이 설정되었으나 데이터 전송에 실패했습니다.

Web Security Appliance의 데이터 전송 상태는 다음 중 하나일 수 있습니다.

- **Not enabled(**활성화되지 않음**):** Web Security Appliance에 대해 중앙 집중식 구성 관리자가 활성화되지 않았습니다.
- **Never connected(**연결되지 않음**):** Email Security Appliance에서 중앙 집중식 구성 관리자는 활성화되지만 Web Security Appliance와 Security Management Appliance 간에 연결이 설정되지 않았습니다.
- **Waiting for data(**데이터 대기 중**):** Web Security Appliance가 데이터 수신을 기다리고 있는 Security Management Appliance에 연결되었습니다.
- **Connected and transferred data(**연결되어 데이터 전송**):** Web Security Appliance와 Security Management Appliance 간의 연결이 설정되었고 데이터가 성공적으로 전송되었습니다.
- **Configuration push failure(**구성 푸시 실패**):** Security Management Appliance에서 Web Security Appliance에 구성 파일을 푸시하려 했으나 전송에 실패했습니다.
- Configuration push pending(구성 푸시 보류 중): Security Management Appliance에서 Web Security Appliance에 구성 파일을 푸시하는 중입니다.
- Configuration push success(구성 푸시 성공): Security Management Appliance에서 Web Security Appliance에 구성 파일을 성공적으로 푸시했습니다.

데이터 전송 문제는 일시적 네트워크 문제 또는 어플라이언스 구성 문제를 나타낼 수 있습니다. "Never connected(연결되지 않음)" 및 "Waiting for data(데이터 대기 중)"는 Security Management Appliance에 매니지드 어플라이언스를 처음 추가할 때 일시적으로 일어나는 정상적인 상태입니다. "Connected and transferred data(연결되어 데이터 전송)"으로 바뀌지 않는다면 구성 문제를 나타내는 것일 수도 있습니다.

어플라이언스에 대해 "File transfer failure(파일 전송 실패)" 상태가 나타날 경우 어플라이언스를 모니터링하여 네트워크 문제 또는 어플라이언스 구성 문제로 인한 것인지 확인합니다. 데이터 전송을 막

는 네트워크 문제가 없는데 상태가 “Connected and transferred data(연결되어 데이터 전송)”으로 바뀌지 않는다면 데이터 전송을 위해 어플라이언스 구성 변경이 필요할 수도 있습니다.

관리 대상 어플라이언스의 구성 상태 보기

Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.

Centralized Service Status(중앙 서비스 상태) 섹션은 어떤 서비스가 활성화되었는지 그리고 각 서비스에 대해 몇 개의 라이센스를 사용했는지 보여줍니다. Security Appliances(보안 어플라이언스) 섹션에서는 추가한 어플라이언스를 나열합니다. 체크 표시는 활성화된 서비스를 나타내며, Connection Established?(연결 설정?) 열은 파일 전송 액세스가 제대로 구성되었는지 여부를 보여줍니다.

관련 주제

- 릴리스된 메시지를 처리할 대체 어플라이언스 지정, 319 페이지
- 관리 대상 어플라이언스 추가 정보, 29 페이지

WSA 상태 추가 정보

Web Security Appliance에 대한 추가 상태 정보는 개별 Web Security Appliance 상태 보기, 364 페이지를 참조하십시오.

보고 데이터 가용성 상태 모니터링

Security Management Appliance에서는 지정된 시간에 대한 보고 데이터의 가용성을 모니터링할 수 있습니다. 어플라이언스에 대한 해당 섹션을 참조하십시오.

- 이메일 보안 보고 데이터 가용성 모니터링, 373 페이지

이메일 보안 보고 데이터 가용성 모니터링

Security Management Appliance에서 Email Security Appliance의 보고 데이터를 모니터링하려면 **Email(**이메일**) > Reporting(**보고**) > Reporting Data Availability(**보고 데이터 가용성**)** 페이지를 봅니다.

Reporting Data Availability(보고 데이터 가용성**)** 페이지에서는 Security Management Appliance가 지정된 기간에 Email Security Appliance로부터 수신한 보고 데이터의 비율을 확인할 수 있습니다. 시간 범위의 데이터 수신 완료율이 막대그래프로 표시됩니다.

전날, 전주, 전월, 전년의 보고 데이터 가용성을 모니터링할 수 있습니다. Security Management Appliance에서 Email Security Appliance의 보고 데이터 수신율이 100%에 미치지 못할 경우 데이터가 불완전할 수도 있습니다. 보고 데이터를 검증하고 시스템 문제를 트러블슈팅하는 데 데이터 가용성 정보를 활용합니다.

웹 보안 보고 데이터 가용성 모니터링

Security Management Appliance에서 Web Security Appliance의 보고 데이터를 모니터링하려면 **Web(웹) > Reporting(보고) > Data Availability(데이터 가용성)** 페이지를 봅니다.

데이터 가용성 페이지에서 데이터를 업데이트하고 정렬하면서 리소스 사용 및 웹 트래픽 문제 지점을 실시간으로 파악할 수 있습니다.

참고 Web Reporting Data Availability(웹 보고 데이터 가용성) 창에서는 웹 보고와 이메일 보고 둘 다 비활성화된 경우에만 웹 보고가 비활성으로 표시됩니다.

이 페이지에서는 모든 데이터 리소스 사용 및 웹 트래픽 문제 지점이 표시됩니다. 목록의 WSA 링크 중 하나를 클릭하면 그 어플라이언스의 보고 데이터 가용성을 볼 수 있습니다.

전날, 전주, 전월, 전년의 보고 데이터 가용성을 모니터링할 수 있습니다. Security Management Appliance에서 Web Security Appliance의 보고 데이터 수신율이 100%에 미치지 못할 경우 데이터가 불완전할 수도 있습니다. 보고 데이터를 검증하고 시스템 문제를 트러블슈팅하는 데 데이터 가용성 정보를 활용합니다.

데이터 가용성이 URL 범주에 대한 예약 보고서에 사용된 경우 어플라이언스 중 하나에서 데이터 공백이 있으면 페이지의 맨 아래에 "이 시간 범위의 일부 데이터를 사용할 수 없습니다"라는 메시지가 표시됩니다. 공백이 없으면 아무것도 표시되지 않습니다.

Web Security Appliance의 데이터 가용성 페이지에 대한 자세한 내용은 데이터 가용성 페이지, 211 페이지를 참조하십시오.

이메일 추적 데이터 상태 모니터링

이메일 추적 데이터의 상태를 모니터링하려면 **Email(이메일) > Message Tracking(메시지 추적) > Message Tracking Data Availability(메시지 추적 데이터 가용성)** 페이지를 봅니다.

관리 대상 어플라이언스의 용량 모니터링

Security Management Appliance에서 매니지드 어플라이언스의 용량을 모니터링할 수 있습니다. 모든 ESA 및 WSA의 종합 용량 및 개별 어플라이언스의 용량을 확인할 수 있습니다.

확인할 용량	참조:
매니지드 Web Security Appliance	System Capacity(시스템 용량) 페이지, 210 페이지
매니지드 Email Security appliances	System Capacity(시스템 용량) 페이지, 105 페이지

활성 **TCP/IP** 서비스 식별

Security Management Appliance에서 사용되는 활성 TCP/IP 서비스를 식별하려면 CLI에서 tcpservices 명령을 사용합니다.

하드웨어 고장 시 매니지드 어플라이언스 교체

하드웨어 문제 또는 기타 이유로 매니지드 어플라이언스를 교체했다면 교체된 어플라이언스의 데이터가 사라지지 않더라도 Security Management Appliance에서 제대로 표시되지 않습니다.

매니지드 어플라이언스를 교체할 때 SMA에서 호스트 목록에 새 어플라이언스를 추가하고 새로운 어플라이언스에 연결합니다. IP 주소가 동일하게 유지되는 경우 기존 호스트 항목의 IP를 기존에 없는 값으로 변경합니다.

12 장

LDAP와의 통합

이 장에는 다음 섹션이 포함되어 있습니다.

개요

기업 LDAP 디렉터리(예: Microsoft Active Directory, SunONE Directory Server, OpenLDAP 디렉터리)에서 엔드 유저 암호 및 이메일 별칭을 유지 관리할 경우 LDAP 디렉터리를 사용하여 다음 사용자를 인증할 수 있습니다.

- 스팸 격리에 액세스하는 엔드유저 및 관리자 사용자.

  사용자가 스팸 격리를 위해 웹 UI에 로그인할 경우 LDAP 서버가 로그인 이름 및 암호를 검증하고 AsyncOS에서 해당 이메일 별칭의 목록을 검색합니다. 사용자 이메일 별칭에 보내진 격리 메시지는 어플라이언스에서 재작성하지 않는 한 스팸 격리에 나타날 수 있습니다.

  스팸 격리를 사용하도록 LDAP 구성, 378 페이지를 참조하십시오.

- 외부 인증이 활성화 및 구성될 때 Cisco Content Security Management Appliance에 로그인하는 관리 사용자.

  LDAP를 사용하여 관리자 사용자의 외부 인증 구성 , 390 페이지를 참조하십시오.

스팸 격리를 사용하도록 LDAP 구성

LDAP 디렉터리와 작동하도록 Cisco Content Security Appliance를 구성할 때 수락, 라우팅, 별칭 사용 및 가장을 설정하려면 다음 단계를 완료해야 합니다.

단계 **1** **LDAP** 서버 프로필을 구성합니다.

서버 프로필에는 AsyncOS가 LDAP 서버와 연결하는 데 필요한 다음 정보가 포함됩니다.

- 서버 이름 및 포트
- 기본 DN
- 서버에 바인딩하기 위한 인증 요구 사항

서버 프로필 구성에 대한 자세한 내용은 LDAP 서버 프로필 생성, 378 페이지 섹션을 참조하십시오.

LDAP 서버 프로필 생성 시 하나 또는 여러 LDAP 서버에 연결하도록 AsyncOS를 구성할 수 있습니다. 자세한 내용은 여러 LDAP 서버를 사용하도록 AsyncOS 구성, 388 페이지을(를) 참고하십시오.

단계 **2** **LDAP** 쿼리를 구성합니다.

LDAP 서버 프로필에 대해 생성된 기본 스팸 격리 쿼리를 사용하거나 특정 LDAP 구현 및 스키마를 위한 맞춤 쿼리를 생성할 수 있습니다. 그런 다음 스팸 알림 및 엔드유저의 격리 액세스에 대한 활성 쿼리를 지정합니다.

쿼리에 대한 자세한 내용은 LDAP 쿼리 구성, 380 페이지를 참조하십시오.

단계 **3** 스팸 격리에 대한 **LDAP** 엔드유저 액세스 및 스팸 알림을 활성화합니다.

엔드유저가 격리 메시지를 보고 관리할 수 있도록 스팸 격리에 대한 LDAP 엔드유저 액세스를 활성화합니다. 사용자가 여러 알림을 받는 것을 방지하기 위해 스팸 알림에 대한 별칭 통합을 활성화할 수도 있습니다.

자세한 내용은 중앙 집중식 스팸 격리 설정 , 280 페이지를 참고하십시오.

LDAP 서버 프로필 생성

AsyncOS가 LDAP 디렉터리를 사용하도록 구성할 때 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필을 만들어야 합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > LDAP**를 선택합니다.

단계 **3** **Add LDAP Server Profile(LDAP** 서버 프로필 추가**)**을 클릭합니다.

단계 **4** **LDAP Server Profile Name(LDAP** 서버 프로필 이름**)** 텍스트 필드에 서버 프로필의 이름을 입력합니다.

단계 **5** **Host Name(s)**(호스트 이름) 텍스트 필드에 LDAP 서버의 호스트 이름을 입력합니다.

LDAP 서버에서 장애 조치 또는 부하분산을 구성하려면 여러 호스트 이름을 입력할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분하십시오. 자세한 내용은 여러 LDAP 서버를 사용하도록 AsyncOS 구성, 388 페이지를 참고하십시오.

단계 **6** 인증 방법을 선택합니다. 익명 인증을 사용하거나 사용자 이름과 암호를 지정할 수 있습니다.

참고 보고서에서 클라이언트 IP 주소 대신 클라이언트 사용자 ID를 표시하도록 LDAP 인증을 구성해야 합니다. LDAP 인증이 없으면 IP 주소로만 사용자를 참조할 수 있습니다. **Use Password**(암호 사용) 라디오 버튼을 선택하고 사용자 이름과 암호를 입력합니다. 이제 사용자 이름이 User Mail Summary(사용자 메일 요약) 페이지에 나타납니다.

단계 **7** LDAP 서버 유형(Active Directory, OpenLDAP, Unknown 또는 Other)을 선택합니다.

단계 **8** 포트 번호를 입력합니다.

기본 포트는 `3268`입니다. 이것은 다중 서버 환경에서 전역 카탈로그에 액세스하도록 하는 Active Directory용 기본 포트입니다.

단계 **9** LDAP 서버의 기본 DN(distinguishing name)을 입력합니다.

사용자 이름 및 암호로 인증하는 경우, 사용자 이름에는 암호를 포함하는 항목에 대한 전체 DN을 포함해야 합니다. 예를 들어 이메일 주소가 `joe@example.com`인 사용자는 마케팅 그룹의 사용자입니다. 이 사용자에 대한 항목은 다음과 같을 수 있습니다.

```
uid=joe, ou=marketing, dc=example dc=com
```

단계 **10** Advanced(고급)에서 LDAP 서버와의 통신에 SSL을 사용할지 여부를 선택합니다.

단계 **11** 캐시 TTL(time-to-live)을 입력합니다. 이 값은 캐시를 보유할 시간을 나타냅니다.

단계 **12** 보유되는 최대 캐시 항목 수를 입력합니다.

단계 **13** 최대 동시 연결 수를 입력합니다.

LDAP 서버 프로필에서 부하분산을 구성하는 경우 이러한 연결은 나열된 LDAP 서버 중에 분산됩니다. 예를 들어 10개의 동시 연결을 구성하며 3개 서버를 통해 연결의 부하를 분산하는 경우 AsyncOS는 각 서버에 대해 10개씩 총 30개의 연결을 만듭니다. 자세한 내용은 부하 균형, 389 페이지를 참고하십시오.

참고 최대 동시 연결 수에는 LDAP 쿼리에 사용되는 LDAP 연결이 포함됩니다. 그러나 스팸 격리에 대해 LDAP 인증을 활성화할 경우 어플라이언스에서는 엔드유저 격리를 위해 20개의 연결을 추가로 허용하여 총 30개의 연결이 가능해집니다.

단계 **14** Test Server(s)(서버 테스트) 버튼을 클릭하여 서버에 대한 연결을 테스트합니다. 여러 LDAP 서버를 지정한 경우 모든 서버가 테스트됩니다. 테스트 결과는 Connection Status(연결 상태) 필드에 나타납니다. 자세한 내용은 LDAP 서버 테스트, 380 페이지을 참고하십시오.

단계 **15** 확인란을 선택하고 필드를 완료하여 스팸 격리 쿼리를 만듭니다.

엔드유저 격리에 로그인할 때 사용자를 검증하도록 격리 엔드유저 인증 쿼리를 구성할 수 있습니다. 엔드유저가 각 이메일 별칭에 대한 격리 알림을 수신하지 않도록 별칭 통합 쿼리를 구성할 수 있습니다. 이 쿼리를 사용하려면 "Designate as the active query(활성 쿼리로 지정)" 확인란을 선택합니다. 자세한 내용은 LDAP 쿼리 구성, 380 페이지을(를) 참고하십시오.

단계 **16** Test Query(쿼리 테스트) 버튼을 클릭하여 스팸 격리 쿼리를 테스트합니다.

테스트 매개변수를 입력하고 Run Test(테스트 실행)를 클릭합니다. 테스트 결과는 Connection Status(연결 상태) 필드에 나타납니다. 쿼리 정의 또는 특성을 변경하려면 **Update(**업데이트**)**를 클릭합니다.

참고 비어 있는 암호와 바인딩하도록 LDAP 서버를 구성한 경우 쿼리는 비어 있는 암호 필드의 테스트를 통과할 수 있습니다.

단계 **17** 변경사항을 제출 및 커밋합니다.

Active Directory 서버 구성에서는 Windows 2000에서 TLS 인증을 허용하지 않습니다. 이는 Active Directory의 알려진 문제입니다. Active Directory와 Windows 2003의 TLS 인증은 정상적으로 작동합니다.

참고 서버 구성의 수는 무제한이지만 서버당 엔드유저 인증 쿼리 및 별칭 통합 쿼리는 하나씩만 구성할 수 있습니다.

LDAP 서버 테스트

LDAP 서버에 대한 연결을 테스트하려면 Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 Test Server(s)(서버 테스트) 버튼(또는 CLI에서 ldapconfig 명령의 test 하위 명령)을 사용합니다. AsyncOS는 서버 포트에 대한 연결의 성공 여부를 나타내는 메시지를 표시합니다. 여러 LDAP 서버를 구성한 경우 AsyncOS는 각 서버를 테스트하고 개별 결과를 표시합니다.

LDAP 쿼리 구성

다음 섹션에서는 각 스팸 격리 쿼리 유형에 대한 기본 쿼리 문자열 및 구성 세부사항을 제공합니다.

- 스팸 격리 최종 사용자 인증 쿼리**.** 자세한 내용은 스팸 격리 엔드유저 인증 쿼리, 381 페이지을 참조하십시오.
- 스팸 격리 별칭 통합 쿼리**.** 자세한 내용은 스팸 격리 별칭 통합 쿼리, 383 페이지을 참고하십시오.

격리에서 엔드유저 액세스 또는 스팸 알림에 LDAP 쿼리를 사용하게 하려면 “Designate as the active query(활성 쿼리로 지정)” 확인란을 선택합니다. 격리 액세스 제어를 위해 엔드유저 인증 쿼리를, 스팸 알림을 위해 별칭 통합 쿼리를 하나씩 지정할 수 있습니다. 기존 활성 쿼리는 모두 비활성화됩니다. Security Management Appliance에서 **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > LDAP** 페이지를 선택하면 활성 쿼리 옆에 별표(*)가 표시됩니다.

또한 도메인 기반 쿼리 또는 체인 쿼리를 활성 엔드유저 액세스 또는 스팸 알림 쿼리로 지정할 수도 있습니다. 자세한 내용은 도메인 기반 쿼리, 385 페이지 및 체인 쿼리, 386 페이지를 참조하십시오.

참고 쿼리가 예상 결과를 반환하는지 확인하려면 LDAP 페이지의 Test Query(쿼리 테스트) 버튼(또는 **ldaptest** 명령)을 사용합니다.

- LDAP 쿼리 구문, 381 페이지
- 토큰, 381 페이지

LDAP 쿼리 구문

LDAP 경로에는 공백을 사용할 수 있으며 따옴표는 필요하지 않습니다. CN 및 DC 구문은 대/소문자를 구분하지 않습니다.

Cn=First Last,oU=user,dc=domain,DC=COM

쿼리에 대해 입력하는 변수는 대/소문자를 구분하며, 제대로 작동하려면 LDAP 구현과 일치해야 합니다. 예를 들어 프롬프트에서 **mailLocalAddress**를 입력하면 **maillocaladdress**를 입력하는 경우와 다른 쿼리를 수행합니다.

토큰

LDAP 쿼리에 다음 토큰을 사용할 수 있습니다.

- {a} username@domainname
- {d} domain
- {dn} distinguished name
- {g} group name
- {u} user name
- {f} MAILFROM: address

참고 {f} 토큰은 수락 쿼리에서만 유효합니다.

예를 들면 Active Directory LDAP 서버에 대한 메일을 수락하기 위해 다음 쿼리를 사용할 수 있습니다.**(|(mail={a})(proxyAddresses=smtp:{a}))**

참고 Cisco에서는 작성하는 모든 쿼리를 테스트하는 데 LDAP 페이지의 Test(테스트) 기능(또는 **ldapconfig** 명령의 **test** 하위 명령)을 사용하고 리스너에서 LDAP 기능을 활성화하기 전에 예상 결과가 반환되는지 확인하는 것이 좋습니다. 자세한 내용은 LDAP 쿼리 테스트, 384 페이지를 참조하십시오.

스팸 격리 엔드유저 인증 쿼리

엔드유저 인증 쿼리는 사용자가 스팸 격리에 로그인할 때 사용자를 검증합니다. 토큰 {u}는 사용자를 지정합니다(사용자의 로그인 이름을 나타냄). 토큰 {a}는 사용자의 이메일 주소를 지정합니다. LDAP 쿼리는 이메일 주소에서 "SMTP:"를 제거하지 않습니다. AsyncOS가 주소에서 해당 부분을 제거합니다.

서버 유형을 기반으로 AsyncOS는 최종 사용자 인증 쿼리에 다음의 기본 쿼리 문자열 중 하나를 사용합니다.

- **Active Directory:** (sAMAccountName={u})
- OpenLDAP: (uid={u})

• 알 수 없음 또는 기타**:** [비어 있음]

기본적으로 기본 이메일 특성은 **mail**입니다. 고유한 쿼리 및 이메일 특성을 입력할 수 있습니다. CLI에서 쿼리를 만들려면 **ldapconfig** 명령의 isqauth 하위 명령을 사용합니다.

참고 사용자가 전체 이메일 주소로 로그인하도록 하려면 쿼리 문자열에 (mail=smtp:{a})를 사용합니다.

샘플 **Active Directory** 최종 사용자 인증 설정

이 섹션에서는 Active Directory 서버 및 최종 사용자 인증 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 Active Directory 서버에 대한 암호 인증, Active Directory 서버 엔드 유저 인증을 위한 기본 쿼리 문자열, mail 및 proxyAddresses 이메일 특성을 사용합니다.

표 ***75: LDAP*** 서버 및 스팸 격리 최종 사용자 인증 설정 예***: Active Directory***

인증 방법	암호 사용**(**검색을 위해 바인딩할 낮은 권한의 사용자를 만들거나 익명 검색을 구성해야 함**)**
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	[공백]
쿼리 문자열	(sAMAccountName={u})
이메일 특성	mail,proxyAddresses

샘플 **OpenLDAP** 엔드유저 인증 설정

이 섹션에서는 OpenLDAP 서버 및 최종 사용자 인증 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 OpenLDAP 서버에 대한 익명 인증, OpenLDAP 서버 엔드유저 인증을 위한 기본 쿼리 문자열, mail 및 mailLocalAddress 이메일 특성을 사용합니다.

표 ***76: LDAP*** 서버 및 스팸 격리 최종 사용자 인증 설정 예***: OpenLDAP***

인증 방법	**Anonymous**
서버 유형	OpenLDAP
포트	389
기본 DN	[비어 있음] (일부 오래된 스키마는 특정 기본 DN을 사용하고자 함.)
연결 프로토콜	[공백]

인증 방법	**Anonymous**
쿼리 문자열	(uid={u})
이메일 특성	mail,mailLocalAddress

스팸 격리 별칭 통합 쿼리

스팸 격리를 사용하는 경우 스팸 격리 별칭 통합 쿼리는 수신자가 각 별칭에 대해 격리 알림을 받지 않도록 이메일 별칭을 통합합니다. 예를 들어 john@example.com, jsmith@example.com 및 john.smith@example.com 이메일 주소에 대한 메일을 받는 수신자가 있다고 가정해보겠습니다. 별칭 통합을 사용하면 수신자는 모든 사용자 별칭으로 전송되는 메시지에 대해 선택된 기본 이메일 주소로 단일 스팸 알림을 수신합니다.

메시지를 기본 이메일 주소로 통합하려면 수신자의 대체 이메일 별칭을 검색할 쿼리를 만들고, Email Attribute(이메일 특성) 필드에 수신자의 기본 이메일 주소에 대한 특성을 입력합니다.

Active Directory 서버의 경우 기본 쿼리 문자열(실제 구축에서 다르거나 같을 수도 있음)은 (|(proxyAddresses={a})(proxyAddresses=smtp:{a}))이고 기본 이메일 특성은 mail입니다. OpenLDAP 서버의 경우 기본 쿼리 문자열은 (mail={a})이고 기본 이메일 특성은 mail입니다. 쉼표로 구분된 여러 특성을 포함하여, 고유한 쿼리 및 이메일 특성을 정의할 수 있습니다. 이메일 특성을 둘 이상 입력하는 경우 proxyAddresses와 같이 변경될 수 있는 여러 값을 가진 특성 대신 mail과 같은 단일 값을 사용하는 고유한 특성을 첫 번째 이메일 특성으로 입력하는 것이 좋습니다.

CLI에서 쿼리를 만들려면 ldapconfig 명령의 isqalias 하위 명령을 사용합니다.

- 샘플 Active Directory 별칭 통합 설정, 383 페이지
- 샘플 OpenLDAP 별칭 통합 설정, 384 페이지

샘플 **Active Directory** 별칭 통합 설정

이 섹션에서는 Active Directory 서버 및 별칭 통합 쿼리에 대한 샘플 설정을 보여줍니다. Active Directory 서버에 대한 익명 인증, Active Directory 서버에 대한 별칭 통합용 쿼리 문자열, 그리고 mail 이메일 특성이 다음 예에 사용됩니다.

표 ***77: LDAP*** 서버 및 스팸 격리 별칭 통합 설정 예***: Active Directory***

인증 방법	**Anonymous**
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	SSL 사용

인증 방법	**Anonymous**
쿼리 문자열	(|(mail={a})(mail=smtp:{a}))
이메일 특성	mail

샘플 OpenLDAP 별칭 통합 설정

이 섹션에서는 OpenLDAP 서버 및 별칭 통합 쿼리에 대한 샘플 설정을 보여줍니다. OpenLDAP 서버에 대한 익명 인증, OpenLDAP 서버에 대한 별칭 통합용 쿼리 문자열, 그리고 mail 이메일 특성이 다음 예에 사용됩니다.

표 ***78: LDAP*** 서버 및 스팸 격리 별칭 통합 설정 예***: OpenLDAP***

인증 방법	**Anonymous**
서버 유형	OpenLDAP
포트	389
기본 DN	[비어 있음] (일부 오래된 스키마는 특정 기본 DN을 사용하고자 함.)
연결 프로토콜	SSL 사용
쿼리 문자열	(mail={a}))
이메일 특성	mail

LDAP 쿼리 테스트

Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 Test Query(쿼리 테스트) 버튼(또는 CLI의 test 명령)을 사용합니다. AsyncOS는 쿼리 연결 테스트의 각 단계에 대한 세부사항을 표시합니다. 이를테면 첫 단계 SMTP 권한 부여의 성패와 상관없고 BIND 매칭이 참 또는 거짓 결과를 반환했는지 여부와 상관없습니다.

ldaptest 명령을 일괄 명령으로 사용할 수 있습니다. 예를 들면 다음과 같습니다.

ldaptest LDAP.isqalias foo@cisco.com

쿼리에 대해 입력하는 변수는 대/소문자를 구분하며, 제대로 작동하려면 LDAP 구현과 매칭해야 합니다. 예를 들어 이메일 특성으로 mailLocalAddress를 입력하면 maillocaladdress를 입력할 때와 다른 쿼리를 수행합니다.

쿼리를 테스트하려면 테스트 매개변수를 입력하고 Run Test(테스트 실행)를 클릭해야 합니다. Test Connection(연결 테스트) 필드에 결과가 나타납니다. 엔드유저 인증 쿼리가 성공할 경우 "Success: Action: match positive"가 표시됩니다. 별칭 통합 쿼리의 경우 "Success: Action: alias consolidation"이 표시되며 통합된 스팸 알림의 이메일 주소도 함께 나타납니다. 쿼리가 실패하면 일치하는 LDAP 레

코드가 없다거나 일치하는 레코드에 이메일 특성이 포함되어 있지 않다는 등의 실패 원인이 AsyncOS에 표시됩니다. 여러 LDAP 서버를 사용하는 경우 Cisco Content Security Appliance는 각 LDAP 서버에서 쿼리를 테스트합니다.

도메인 기반 쿼리

도메인 기반 쿼리는 유형별로 그룹화되고 도메인과 연결되는 LDAP 쿼리입니다. 서로 다른 LDAP 서버가 서로 다른 도메인과 연결되어 있지만 엔드유저 격리 액세스를 위해 모든 LDAP 서버에 대해 쿼리를 실행해야 하는 경우 도메인 기반 쿼리가 필요할 수 있습니다. 예를 들어 Bigfish라는 회사가 도메인 Bigfish.com, Redfish.com, Bluefish.com을 소유하는데 각 도메인과 연관된 직원을 위한 LDAP 서버를 따로 둡니다. Bigfish에서는 도메인 기반 쿼리를 사용하여 3개 도메인 모두의 LDAP 디렉터리에 대해 엔드유저를 인증할 수 있습니다.

스팸 격리에 대한 엔드유저 액세스 또는 알림을 제어하는 데 도메인 기반 쿼리를 사용하려면 다음 단계를 완료합니다.

단계 **1** 도메인 기반 쿼리에서 사용할 각 도메인에 대한 LDAP 서버 프로필을 만듭니다. 각 서버 프로필에서 도메인 기반 쿼리에서 사용할 쿼리를 구성합니다. 자세한 내용은 LDAP 서버 프로필 생성, 378 페이지을 참고하십시오.

단계 **2** 도메인 기반 쿼리를 만듭니다. 도메인 기반 쿼리를 만들 때에는 각 서버 프로필에서 쿼리를 선택하고, 스팸 격리에 대한 활성 쿼리로 도메인 기반 쿼리를 지정합니다. 쿼리 만들기에 대한 자세한 내용은 도메인 기반 쿼리 만들기, 385 페이지 섹션을 참조하십시오.

단계 **3** 스팸 격리에 대한 엔드유저 액세스 및 스팸 알림을 활성화합니다. 자세한 내용은 최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정 , 300 페이지를 참고하십시오.

도메인 기반 쿼리 만들기

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > LDAP**를 선택합니다.

단계 **3** LDAP 페이지에서 **Advanced(**고급**)**를 클릭합니다.

단계 **4** 도메인 기반 쿼리의 이름을 입력합니다.

단계 **5** 쿼리 유형을 선택합니다.

참고 도메인 기반 쿼리를 생성할 때 단일 쿼리 유형을 지정합니다. 쿼리 유형을 선택하면 쿼리 필드 드롭다운 목록은 LDAP 서버 프로필에 있던 적합한 쿼리로 이루어집니다.

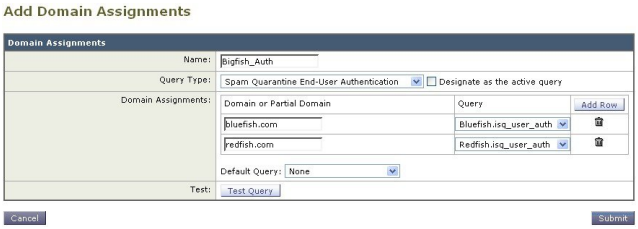
단계 **6** Domain Assignments(도메인 할당) 필드에 도메인을 입력합니다.

단계 **7** 도메인과 관련된 쿼리를 선택합니다.

단계 **8** 도메인 기반 쿼리에서 각 도메인에 대해 행을 추가하고 쿼리를 선택합니다.

단계 **9** 다른 모든 쿼리가 실패할 경우 실행할 기본 쿼리를 입력합니다. 기본 쿼리를 입력하지 않으려면 **None(없음)**을 선택합니다.

그림 ***6:*** 도메인 기반 쿼리의 예



단계 **10** Test Query(쿼리 테스트) 버튼을 클릭하고 Test Parameters(테스트 매개변수) 필드에 테스트할 사용자 로그인과 암호 또는 이메일 주소를 입력하여 쿼리를 테스트합니다. Connection Status(연결 상태) 필드에 결과가 나타납니다.

단계 **11** 스팸 격리에서 도메인 기반 쿼리를 사용하게 하려면 **Designate as the active query(활성 쿼리로 지정)** 확인란을 선택합니다.

참고 도메인 기반 쿼리는 지정된 쿼리 유형에 대한 활성 LDAP 쿼리가 됩니다. 예를 들어 도메인 기반 쿼리가 엔드유저 인증에 쓰일 경우 스팸 격리에 대한 활성 엔드유저 인증 쿼리가 됩니다.

단계 **12** **Submit(제출)**을 클릭하고 **Commit(커밋)**을 변경사항을 커밋합니다.

참고 명령행 인터페이스에서 동일한 구성을 수행하려면 명령행 프롬프트에서 `ldapconfig` 명령의 `advanced` 하위 명령을 입력합니다.

체인 쿼리

체인 쿼리는 AsyncOS에서 연속적으로 실행하는 일련의 LDAP 쿼리입니다. AsyncOS는 LDAP 서버가 긍정적인 응답을 반환할 때까지 또는 "체인"의 최종 쿼리가 부정적인 응답을 반환하거나 실패할 때까지 "체인"의 각 쿼리를 실행합니다. 체인 쿼리는 LDAP 디렉터리의 항목이 서로 다른 특성을 사용하여 유사한(또는 같은) 값을 저장하는 경우 유용할 수 있습니다. 예를 들어 기업의 여러 부서가 서로 다른 LDAP 디렉터리 유형을 사용합니다. IT 부서는 OpenLDAP를, 세일즈 부서는 Active Directory를 사용합니다. 두 LDAP 디렉터리 유형 모두에 대해 쿼리를 실행하기 위해 체인 쿼리를 사용할 수 있습니다.

스팸 격리에 대한 엔드유저 액세스 또는 알림을 제어하는 데 체인 쿼리를 사용하려면 다음 단계를 완료합니다.

단계 **1** 체인 쿼리에서 사용할 각 쿼리에 대한 LDAP 서버 프로필을 만듭니다. 각 서버 프로필에 대해 체인 쿼리에 사용할 쿼리를 구성합니다. 자세한 내용은 LDAP 서버 프로필 생성, 378 페이지을 참고하십시오.

단계 **2** 체인 쿼리를 생성하고 이를 스팸 격리를 위한 활성 쿼리로 지정합니다. 자세한 내용은 체인 쿼리 만들기, 387 페이지을(를) 참고하십시오.

단계 **3** 스팸 격리에 대한 LDAP 엔드유저 액세스 또는 스팸 알림을 활성화합니다. 스팸 격리에 대한 자세한 내용은 중앙 집중식 스팸 격리 설정 , 280 페이지를 참조하십시오.

체인 쿼리 만들기

팁 CLI에서 ldapconfig 명령의 advanced 하위 명령을 사용할 수도 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > LDAP > LDAP Server(LDAP** 서버**)**를 선택합니다.

단계 **3** LDAP Server Profiles(LDAP 서버 프로필) 페이지에서 **Advanced(**고급**)**를 클릭합니다.

단계 **4** **Add Chain Query(**체인 쿼리 추가**)**를 클릭합니다.

단계 **5** 체인 쿼리의 이름을 입력합니다.

단계 **6** 쿼리 유형을 선택합니다.

체인 쿼리를 생성할 때 그 구성 요소 쿼리 모두 동일한 쿼리 유형입니다. 쿼리 유형을 선택하면 쿼리 필드 드롭다운 목록은 LDAP 서버 프로필에 있던 적합한 쿼리를 표시합니다.

단계 **7** 체인의 첫 번째 쿼리를 선택합니다.

Cisco Content Security Appliance는 사용자가 구성한 순서대로 쿼리를 실행합니다. 체인 쿼리에 여러 쿼리를 추가하는 경우 구체적인 쿼리 다음에 일반적인 쿼리가 나오도록 쿼리 순서를 지정할 수 있습니다.

그림 ***7:*** 체인 쿼리의 예

단계 **8** Test Query(쿼리 테스트) 버튼을 클릭하고 Test Parameters(테스트 매개변수) 필드에 사용자 로그인과 암호 또는 이메일 주소를 입력하여 쿼리를 테스트합니다. Connection Status(연결 상태) 필드에 결과가 나타납니다.

단계 **9** 스팸 격리에서 도메인 쿼리를 사용하게 하려면 **Designate as the active query(**활성 쿼리로 지정**)** 확인란을 선택합니다.

참고 체인 쿼리는 지정된 쿼리 유형에 대한 활성 LDAP 쿼리가 됩니다. 예를 들어 체인 쿼리가 엔드유저 인증에 쓰일 경우 스팸 격리에 대한 활성 엔드유저 인증 쿼리가 됩니다.

단계 **10** 변경 사항을 제출 및 커밋합니다.

참고 명령행 인터페이스에서 동일한 구성을 수행하려면 명령행 프롬프트에서 `ldapconfig` 명령의 `advanced` 하위 명령을 입력합니다.

여러 LDAP 서버를 사용하도록 AsyncOS 구성

LDAP 서버 프로필을 구성할 때 여러 LDAP 서버 목록에 연결되도록 Cisco Content Security Appliance를 구성할 수 있습니다. 여러 LDAP 서버를 사용할 경우 이들은 동일한 정보를 포함하고 동일한 구조를 갖고 동일한 인증 정보를 사용해야 합니다. 기록을 통합할 수 있는 서드파티 제품이 있습니다.

다음 기능을 사용하려면 이중화 LDAP 서버에 연결하도록 Cisco Content Security Appliance를 구성합니다.

- 장애 조치. Cisco Content Security Appliance는 LDAP 서버에 연결할 수 없는 경우 목록의 다음 서버에 연결합니다.
- 부하분산. Cisco Content Security Appliance는 LDAP 쿼리를 수행할 때 LDAP 서버 목록 전체에 연결을 분산합니다.

Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > LDAP 페이지 또는 CLI ldapconfig 명령을 사용하여 이중화 LDAP 서버를 구성할 수 있습니다.

서버 및 쿼리 테스트

LDAP 서버에 대한 연결을 테스트하려면 Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 Test Server(s)(서버 테스트) 버튼(또는 CLI의 test 하위 명령)을 사용합니다. 여러 LDAP 서버를 사용하는 경우 AsyncOS는 각 서버를 테스트하고 각 서버에 대한 개별 결과를 표시합니다. AsyncOS는 또한 각 LDAP 서버에서 쿼리를 테스트하고 개별 결과를 표시합니다.

페일오버

쿼리 해결을 위한 LDAP 서버의 가용성을 보장하기 위해 페일오버에 대한 LDAP 프로필을 구성할 수 있습니다. LDAP 서버와의 연결이 실패할 경우 또는 쿼리에서 합당한 오류를 반환할 경우 어플라이언스는 목록에 지정된 다음 LDAP 서버에 대해 쿼리를 시도합니다.

Cisco Content Security Appliance는 지정된 기간에 LDAP 서버 목록에서 첫 번째 서버에 연결하려고 시도합니다. 어플라이언스가 목록에 있는 첫 번째 LDAP 서버에 연결하지 못할 경우 또는 쿼리에서 오류를 반환할 경우 목록에 있는 다음 LDAP 서버에 연결하려고 시도합니다. 기본적으로 어플라이언스는 항상 목록에 있는 첫 번째 서버에 연결하려고 시도하며, 나열된 순서대로 각각의 다음 서버에 연결하려고 시도합니다. Cisco Content Security Appliance가 기본적으로 주 LDAP 서버에 연결하도록 하려면 LDAP 서버 목록에 해당 서버를 첫 번째 서버로 입력합니다.

참고 지정된 LDAP 서버를 쿼리하는 시도만 페일오버합니다. 지정된 LDAP 서버와 연결된 리퍼럴 또는 연속 서버에 대한 쿼리 시도는 페일오버하지 않습니다.

Cisco Content Security Appliance는 두 번째 또는 그 이후의 LDAP 서버에 연결하는 경우 지정된 기간에 해당 서버에 연결된 상태를 유지합니다. 이 기간이 끝나면 어플라이언스는 목록에 있는 첫 번째 서버에 다시 연결하려고 시도합니다.

Cisco Content Security Appliance에서 LDAP 페일오버 구성

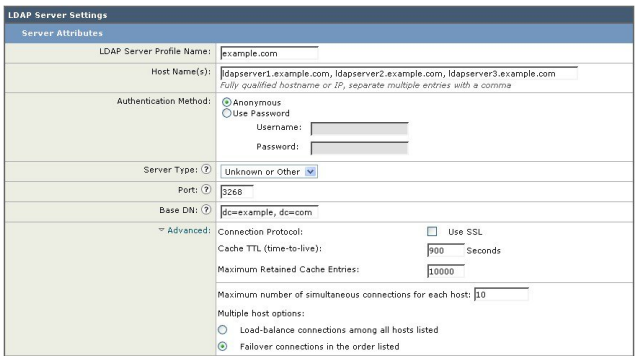
단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > LDAP**를 선택합니다.

단계 **3** 수정할 LDAP 서버 프로필을 선택합니다.

다음 예에서 LDAP 서버 이름은 example.com입니다.

그림 ***8: LDAP*** 페일오버 구성의 예



단계 **4** Hostname(호스트 이름) 텍스트 필드에 LDAP 서버를 입력합니다(예: **ldapserver.example.com**).

단계 **5** Maximum number of simultaneous connections for each host(호스트별 최대 동시 연결 수) 텍스트 필드에 최대 연결 수를 입력합니다.

이 예에서는 최대 연결 수가 **10**입니다.

단계 **6** **Failover connections in the order list(**순서 목록의 연결 페일오버**)** 옆의 라디오 버튼을 클릭합니다.

단계 **7** 필요하다면 다른 LDAP 옵션을 구성합니다.

단계 **8** 변경 사항을 제출하고 커밋합니다.

부하 균형

LDAP 연결을 LDAP 서버 그룹으로 분산하려면 LDAP 프로필에서 부하분산을 구성할 수 있습니다.

로드 밸런싱을 사용하는 경우 Cisco Content Security Appliance는 나열된 LDAP 서버로 연결을 분산합니다. 연결이 실패하거나 시간이 초과되면 어플라이언스는 어떤 LDAP 서버가 사용 가능한지 확인한 후 사용 가능한 서버에 다시 연결합니다. 어플라이언스는 사용자가 구성한 최대 연결 수를 기반으로 설정할 수 있는 동시 연결 수를 결정합니다.

나열된 LDAP 서버 중 하나가 응답하지 않으면 어플라이언스는 나머지 LDAP 서버로 연결을 분산합니다.

Cisco Content Security Appliance에서 부하분산 구성

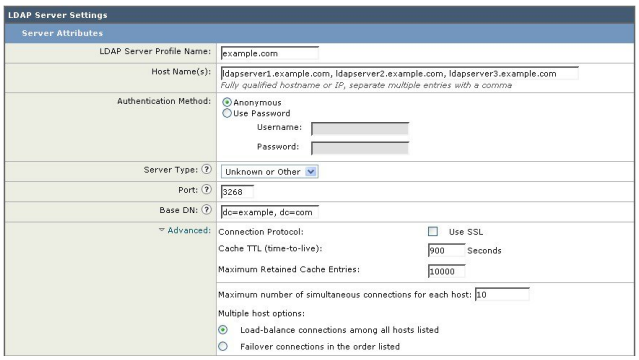
단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > LDAP**를 선택합니다.

단계 **3** 수정할 LDAP 서버 프로필을 선택합니다.

다음 예에서 LDAP 서버 이름은 example.com입니다.

그림 ***9: Loadbalancing*** 구성 예



단계 **4** Hostname(호스트 이름) 텍스트 필드에 LDAP 서버를 입력합니다(예: **ldapserver.example.com**).

단계 **5** Maximum number of simultaneous connections for each host(호스트별 최대 동시 연결 수) 텍스트 필드에 최대 연결 수를 입력합니다.

이 예에서는 최대 연결 수가 **10**입니다.

단계 **6** **Load balance connections among all hosts(**모든 호스트에서 연결 부하분산**)** 옆의 라디오 버튼을 클릭합니다.

단계 **7** 필요하다면 다른 LDAP 옵션을 구성합니다.

단계 **8** 변경 사항을 제출하고 커밋합니다.

LDAP를 사용하여 관리자 사용자의 외부 인증 구성

LDAP 사용자 이름 및 암호로 로그인하도록 허용함으로써 네트워크의 LDAP 디렉터리를 사용하여 관리 사용자를 인증하도록 Cisco Content Security Appliance를 구성할 수 있습니다.

단계 **1** **LDAP** 서버 프로필을 구성합니다**.** LDAP 서버 프로필 생성, 378 페이지를 참조하십시오.

단계 **2** 사용자 계정을 찾기 위한 쿼리를 만듭니다**.** LDAP 서버 프로필의 외부 인증 쿼리 섹션에서 LDAP 디렉터리의 사용자 계정을 검색하기 위한 쿼리를 만듭니다. 관리자 사용자 인증을 위한 사용자 계정 쿼리 , 391 페이지를 참조하십시오.

단계 **3** 그룹 멤버십 쿼리를 만듭니다**.** 사용자가 디렉터리 그룹의 구성원인지 확인하는 쿼리를 만들고 그룹의 모든 구성원을 찾는 쿼리를 따로 만듭니다. 자세한 내용은 관리자 사용자 인증을 위한 그룹 멤버십 쿼리 , 392 페이지및 Email Security Appliance에 대한 문서나 온라인 도움말을 참조하십시오.

참고 페이지의 외부 인증 쿼리 섹션에 있는 **Test Queries(**쿼리 테스트**)** 버튼(또는 ldaptest 명령)을 사용하여 쿼리가 예상한 결과를 반환함을 확인합니다. 관련 내용은 LDAP 쿼리 테스트, 384 페이지를 참조하십시오.

단계 **4** **LDAP** 서버를 사용하기 위한 외부 인증을 설정합니다**.** 사용자 인증에 LDAP 서버를 사용하고 사용자 역할을 LDAP 디렉터리의 그룹에 할당하도록 어플라이언스를 구성합니다. 자세한 내용은 관리자 사용자의 외부 인증 활성화 , 393 페이지및 Email Security Appliance에 대한 문서나 온라인 도움말의 "사용자 추가" 섹션을 참조하십시오.

관리자 사용자 인증을 위한 사용자 계정 쿼리

외부 사용자를 인증하기 위해 AsyncOS는 LDAP 디렉터리의 사용자 레코드 및 사용자 전체 이름이 포함된 특성을 검색하는 쿼리를 사용합니다. 선택하는 서버 유형에 따라 AsyncOS는 기본 쿼리 및 기본 특성을 입력합니다. RFC 2307, LDAP 사용자 레코드에 특성이 정의된 경우(**shadowLastChange**, **shadowMax** 및 **shadowExpire**) 어플라이언스에서 만료된 계정의 사용자를 거부하도록 할 수 있습니다. 사용자 레코드가 상주하는 도메인 레벨에 대해 기본 DN이 필요합니다.

다음 표에서는 AsyncOS가 Active Directory 서버에서 사용자 계정을 검색할 때 사용하는 기본 쿼리 문자열 및 전체 사용자 이름 특성을 보여줍니다.

표 ***79: Active Directory*** 서버를 위한 기본 쿼리 문자열

서버 유형	**Active Directory**
기본 DN	[비어 있음] (사용자 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
쿼리 문자열	(&(objectClass=user)(sAMAccountName={u}))
사용자의 전체 이름을 포함하는 특성	displayName

다음 표에서는 AsyncOS가 OpenLDAP 서버에서 사용자 계정을 검색할 때 사용하는 기본 쿼리 문자열 및 전체 사용자 이름 특성을 보여줍니다.

표 ***80: Open LDAP*** 서버를 위한 기본 쿼리 문자열

서버 유형	**OpenLDAP**
기본 DN	[비어 있음] (사용자 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
쿼리 문자열	(&(objectClass=posixAccount)(uid={u}))
사용자의 전체 이름을 포함하는 특성	gecos

관리자 사용자 인증을 위한 그룹 멤버십 쿼리

LDAP 그룹을 어플라이언스 액세스를 위한 사용자 역할과 연결할 수 있습니다.

AsyncOS는 사용자가 디렉터리 그룹의 구성원인지 확인하고 그룹의 모든 구성원을 찾는 데에도 각각 쿼리를 사용합니다. 디렉터리 그룹의 멤버십은 시스템 내 사용자의 권한을 결정합니다. GUI의 Management Appliance(관리 어플라이언스) >System Administration(시스템 관리) > Users(사용자) 페이지(또는 CLI의 userconfig)에서 외부 인증을 활성화할 때 LDAP 디렉터리의 그룹에 사용자 역할을 할당합니다. 사용자 역할은 사용자가 시스템에서 보유하는 권한을 결정하며, 외부에서 인증된 사용자의 경우 개별 사용자 대신 디렉터리 그룹에 역할이 할당됩니다. 예를 들면 IT 디렉터리 그룹의 사용자를 Administrator 사용자 역할에 할당하고 Support 디렉터리 그룹의 사용자를 Help Desk User 역할에 할당할 수 있습니다.

한 사용자가 서로 다른 사용자 역할의 여러 LDAP 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 가장 제한적인 역할에 대한 권한을 부여합니다. 예를 들어 한 사용자가 Operator 권한의 그룹과 Help Desk User 권한의 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 Help Desk User 역할에 대한 권한을 부여합니다.

그룹 멤버십을 쿼리하도록 LDAP 프로필을 구성할 때 그룹 레코드를 찾을 수 있는 디렉터리 레벨에 대한 기본 DN, 그룹 구성원의 사용자 이름을 가지고 있는 특성 및 그룹 이름을 가지고 있는 특성을 입력합니다. LDAP 서버 프로필에 대해 선택하는 서버 유형을 기반으로, AsyncOS는 사용자 이름 및 그룹 이름 특성에 대한 기본값과 기본 쿼리 문자열을 입력합니다.

참고 Active Directory 서버의 경우 사용자가 그룹의 구성원인지를 확인하는 기본 쿼리 문자열은 (&(objectClass=group)(member={u}))입니다. 그러나 LDAP 스키마가 "memberof" 목록에서 사용자 이름 대신 DN을 사용하는 경우 {u} 대신 {dn}을 사용할 수 있습니다.

다음 표에서는 AsyncOS가 Active Directory 서버에서 그룹 멤버십을 검색할 때 사용하는 기본 쿼리 문자열 및 특성을 보여줍니다.

표 ***81: Active Directory*** 서버를 위한 기본 쿼리 문자열 및 특성

Query String(쿼리 문자열**)**	**Active Directory**
기본 DN	[비어 있음] (그룹 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
사용자가 그룹 구성원인지 여부를 확인하는 쿼리 문자열	(&(objectClass=group)(member={u})) 참고 LDAP 스키마가 memberOf 목록에서 사용자 이름 대신 DN을 사용하는 경우 {u}를 {dn}으로 교체할 수 있습니다.
그룹의 전체 구성원을 결정하는 쿼리 문자열	(&(objectClass=group)(cn={g}))
각 구성원의 사용자 이름을 가지고 있는 특성(또는 사용자 레코드에 대한 DN)	member

Query String(쿼리 문자열)	Active Directory
그룹 이름을 포함하는 특성	cn

다음 표에서는 AsyncOS가 OpenLDAP 서버에서 그룹 멤버십을 검색할 때 사용하는 기본 쿼리 문자열 및 특성을 보여줍니다.

표 ***82: Open LDAP*** 서버를 위한 기본 쿼리 문자열 및 특성

Query String(쿼리 문자열)	OpenLDAP
기본 DN	[비어 있음] (그룹 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
사용자가 그룹 구성원인지 여부를 확인하는 쿼리 문자열	(&(objectClass=posixGroup)(memberUid={u}))
그룹의 전체 구성원을 결정하는 쿼리 문자열:	(&(objectClass=posixGroup)(cn={g}))
각 구성원의 사용자 이름을 가지고 있는 특성(또는 사용자 레코드에 대한 DN)	memberUid
그룹 이름을 포함하는 특성	cn

관리자 사용자의 외부 인증 활성화

LDAP 서버 프로필 및 쿼리를 구성한 다음 LDAP를 사용하여 외부 인증을 활성화할 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Users(**사용자**)** 페이지를 선택합니다.

단계 **3** **Enable(**활성화**)**을 클릭합니다.

단계 **4** **Enable External Authentication(**외부 인증 활성화**)** 확인란을 선택합니다.

단계 **5** 인증 유형으로 **LDAP**를 선택합니다.

단계 **6** 사용자를 인증하는 LDAP 외부 인증 쿼리를 선택합니다.

단계 **7** 어플라이언스가 시간 초과되기 전까지 서버의 응답을 기다리는 시간(초)을 입력합니다

단계 **8** 어플라이언스가 인증할 LDAP 디렉터리에서 그룹의 이름을 입력하고, 그룹의 사용자에 대한 역할을 선택합니다.

단계 **9** 선택적으로, **Add Row(**행 추가**)**를 클릭하여 또 다른 디렉터리 그룹을 추가합니다. 어플라이언스가 인증할 각 디렉터리 그룹에 대해 7~8단계를 반복합니다.

단계 **10** 변경 사항을 제출 및 커밋합니다.

13 장

SMTP 라우팅 구성

이 장에는 다음 섹션이 포함되어 있습니다.

SMTP 경로 개요

이 장에서는 Cisco Content Security Management Appliance를 거치는 이메일의 라우팅 및 전달에 대해 설명합니다. 또한 SMTP Routes(SMTP 경로) 페이지 및 **smtproutes** 명령의 사용에 대해서도 설명합니다.

SMTP 경로를 사용하면 특정 도메인에 대한 모든 이메일을 다른 MX(mail exchange) 호스트로 리디렉션할 수 있습니다. 예를 들면 example.com에서 groupware.example.com으로의 매핑을 만들 수 있습니다. 이렇게 매핑하면 봉투 수신자 주소의 @example.com 이메일이 groupware.example.com으로 대신 전달됩니다. 시스템은 groupware.example.com에서 "MX" 조회를 수행한 다음, 일반 메일 전달과 마찬가지로 호스트에서 "A" 조회를 수행합니다. 이 대체 MX 호스트는 DNS MX 레코드에 나열될 필요가 없으며, 이메일이 리디렉션되는 도메인의 구성원일 필요도 없습니다. 운영 체제에서는 Cisco Content Security Appliance에 대해 최대 10,000개의 SMTP 경로 매핑을 구성할 수 있습니다. (SMTP 경로 제한, 398 페이지 참조)

이 기능은 또한 호스트 "글로빙(globbing)"을 허용합니다. example.com과 같은 부분 도메인을 지정하면 example.com으로 끝나는 모든 도메인이 이 항목과 일치합니다. 예를 들어 fred@foo.example.com과 wilma@bar.example.com은 모두 매핑과 일치합니다.

SMTP 경로 테이블에서 호스트가 발견되지 않으면 DNS를 사용하여 MX 조회가 수행됩니다. 결과는 SMTP 경로 테이블에 대해 다시 확인되지 않습니다. foo.domain에 대한 DNS MX 항목이 bar.domain인 경우, foo.domain으로 전송된 이메일은 호스트 bar.domain으로 전달됩니다. 일부 다른 호스트에 대해 bar.domain의 매핑을 생성하는 경우 foo.domain으로 보낼 이메일에는 영향을 미치지 않습니다.

즉, 재귀 항목은 허용되지 않습니다. b.domain으로 리디렉션할 a.domain에 대한 항목이 있으며 b.domain에 대한 이메일을 a.domain으로 리디렉션하는 후속 항목이 있는 경우, 메일 루프가 생성되지 않습니다. 이 경우 a.domain으로 주소가 지정된 이메일은 b.domain에 의해 지정된 MX 호스트로 전달되지 않

으며, 반대로 b.domain으로 주소가 지정된 이메일은 a.domain에 의해 지정된 MX 호스트로 전달됩니다.

모든 이메일 전달 시 SMTP 경로 테이블을 위에서 아래로 읽습니다. 매핑과 일치하는 가장 구체적인 항목이 선정됩니다. SMTP 경로 테이블에 host1.example.com과 .example.com 모두에 대한 매핑이 있는 경우, 덜 구체적인 .example.com 항목 뒤에 나타나더라도 host1.example.com에 대한 항목이 좀 더 구체적이므로 이 항목이 사용됩니다. 그렇지 않으면 시스템은 봉투 수신자의 도메인에서 일반적인 MX 조회를 수행합니다.

SMTP 경로, 메일 전달 및 메시지 분리

수신: 한 메시지의 수신자가 10명이고 이들이 모두 동일한 Exchange 서버에 있는 경우, AsyncOS는 하나의 TCP 연결을 열고 메일 저장소에 10개의 개별 메시지가 아니라 정확히 하나의 메시지를 제시합니다.

발신: 유사하게 작동하지만, 한 메시지가 10개의 서로 다른 도메인에 있는 10명의 수신자에게 가는 경우 AsyncOS는 10개의 MTA에 대한 10개의 연결을 열고 각각에 하나의 이메일을 전달합니다.

분리: 수신 메시지 하나의 수신자가 10명이고 이들이 각각 별도의 수신 정책 그룹에 속한 경우(그룹 10개), 10명의 수신자가 모두 동일한 Exchange 서버에 있더라도 메시지가 분리됩니다. 따라서 단일 TCP 연결을 통해 10개의 개별 이메일이 전달됩니다.

SMTP 경로 및 아웃바운드 SMTP 인증

아웃바운드 SMTP 인증 프로필을 만든 경우 SMTP 경로에 적용할 수 있습니다. 이는 Cisco Content Security Appliance가 네트워크 에지에 있는 메일 릴레이 서버 뒤에 있는 경우 발신 메일에 대한 인증을 허용합니다.

로컬 도메인용 이메일 라우팅

Security Management Appliance는 다음 메일을 라우팅합니다.

- SMTP 라우팅을 무시하는 ISQ 릴리스 메시지
- Alerts(경고문)
- 메일을 통해 지정된 목적지로 보낼 수 있는 구성 파일
- 정의된 수신자에게도 보낼 수 있는 지원 요청 메시지

마지막 2가지 메시지 유형은 목적지에 도달하는 데 SMTP 경로를 사용합니다.

Email Security Appliance는 로컬 도메인에 대한 메일을 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > SMTP Routes(SMTP** 경로**)** 페이지(또는 **smtproutes** 명령)를 사용하여 지정한 호스트에 라우팅합니다. 이 기능은 sendmail **mailertable** 기능과 비슷합니다. SMTP Routes(SMTP 경로) 페이지 및 **smtproutes** 명령은 AsyncOS 2.0 도메인 리디렉션 기능의 확장입니다.

참고 GUI에서 시스템 설정 마법사를 완료하고 변경사항을 커밋한 경우 그 시점에 입력한 각 RAT 항목에 대한 첫 SMTP 경로 항목을 어플라이언스에서 정의한 것입니다.

기본 SMTP 경로

특수 키워드 ALL을 사용하여 기본 SMTP 경로를 정의할 수도 있습니다. 도메인이 SMTP 경로 목록에 있는 이전 매핑과 일치하지 않는 경우, 기본적으로 ALL 항목에 의해 지정된 MX 호스트로 리디렉션됩니다.

SMTP 경로 항목을 출력하면 기본 SMTP 경로가 ALL:로 나열됩니다. 기본 SMTP 경로는 삭제할 수 없습니다. 여기에 대해 입력한 값만 지울 수 있습니다.

Management Appliance(관리 어플라이언스**) > Network(**네트워크**) > SMTP Routes(SMTP** 경로**)** 페이지 또는 **smtproutes** 명령을 사용하여 기본 SMTP 경로를 구성합니다.

SMTP 경로 관리

SMTP 경로 정의

Email Security Appliance는 로컬 도메인에 대한 메일을 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > SMTP Routes(SMTP** 경로**)** 페이지(또는 **smtproutes** 명령)를 사용하여 지정한 호스트에 라우팅합니다. 이 기능은 sendmail mailer table 기능과 비슷합니다. SMTP Routes(SMTP 경로) 페이지 및 **smtproutes** 명령은 AsyncOS 2.0 도메인 리디렉션 기능의 확장입니다.

Management Appliance(관리 어플라이언스) > Network(네트워크) > SMTP Routes(SMTP 경로) 페이지(또는 **smtproutes** 명령)를 사용하여 경로를 작성합니다. 새 경로를 만들 경우, 먼저 영구 경로를 만들 도메인 또는 부분 도메인을 지정합니다. 그런 다음 대상 호스트를 지정합니다. 대상 호스트는 인증된 호스트 이름 또는 IP 주소로서 입력할 수 있습니다. 항목과 일치하는 메시지를 삭제하려면 /dev/null의 특수 대상 호스트를 지정할 수도 있습니다. (따라서 기본 경로에 대해 /dev/null을 지정하면 어플라이언스에 수신되는 메일이 전달되지 않습니다.)

여러 목적지 호스트 항목이 인증된 호스트 이름 및 IP 주소를 모두 포함할 수 있습니다. Separate multiple entries with commas.

하나 이상의 호스트가 응답하지 않는 경우 메시지는 도달 가능한 호스트 중 하나로 전달됩니다. 구성된 모든 호스트가 응답하지 않을 경우 해당 호스트에 대해 메일이 큐에 추가됩니다. MX 레코드를 사용하여 페일오버되지 않습니다.

SMTP 경로 제한

최대 10,000개의 경로를 정의할 수 있습니다. ALL의 최종 기본 경로는 이 제한에 대한 경로로 계산됩니다. 따라서 최대 9,999개의 사용자 지정 경로와 특수 키워드 ALL을 사용하는 하나의 경로를 정의할 수 있습니다.

SMTP 경로 추가

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > SMTP Routes(SMTP** 경로**)**를 선택합니다.

단계 **3** **Add Route(**경로 추가**)**를 클릭합니다.

단계 **4** 수신 도메인 및 목적지 호스트를 입력합니다. **Add Row(**행 추가**)**를 클릭하고 새 행에 다음 대상 호스트를 입력하여 여러 대상 호스트를 추가할 수 있습니다.

단계 **5** ":<*port number*>"를 목적지 호스트 example.com:25에 추가하여 포트 번호를 지정할 수 있습니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

SMTP 경로 내보내기

HAT(Host Access Table) 및 RAT(Recipient Access Table)와 마찬가지로 파일을 내보내고 가져와서 SMTP 경로 매핑을 수정할 수 있습니다.

단계 **1** SMTP Routes(SMTP 경로) 페이지에서 **Export SMTP Routes(SMTP** 경로 내보내기**)**를 클릭합니다.

단계 **2** 파일 이름을 입력하고 **Submit(**제출**)**을 클릭합니다.

SMTP 경로 가져오기

HAT(Host Access Table) 및 RAT(Recipient Access Table)와 마찬가지로 파일을 내보내고 가져와서 SMTP 경로 매핑을 수정할 수 있습니다.

단계 **1** SMTP Routes(SMTP 경로) 페이지에서 **Import SMTP Routes(SMTP** 경로 가져오기**)**를 클릭합니다.

단계 **2** 내보낸 SMTP 경로를 포함하는 파일을 선택합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 SMTP 경로가 교체된다는 경고가 표시됩니다. 텍스트 파일의 모든 SMTP 경로를 가져오게 됩니다.

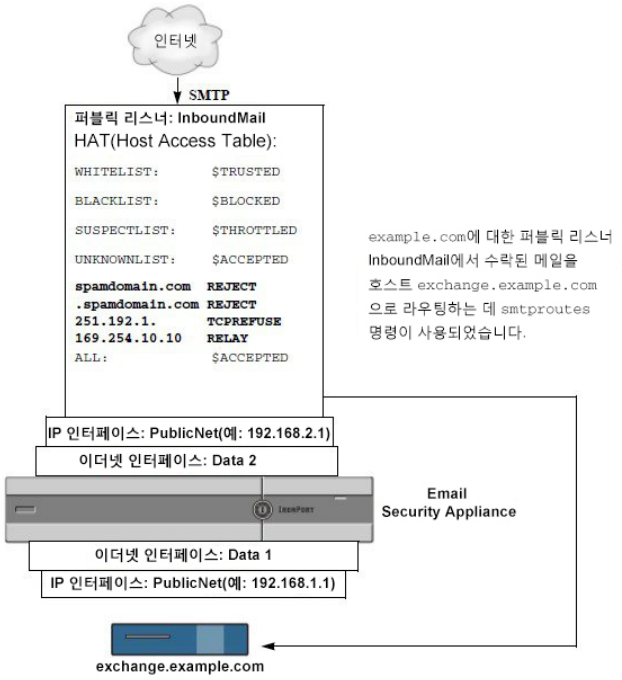
단계 **4** **Import(**가져오기**)**를 클릭합니다.

파일에 "코멘트"를 추가할 수 있습니다. '#' 문자로 시작되는 줄은 코멘트로 간주되어 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

```
# this is a comment, but the next line is not
ALL:
```

이 시점에서 이메일 게이트웨이(Email Gateway) 구성은 다음과 같습니다.

그림 ***10:*** 이메일 게이트웨이 구성



SMTP 경로 및 DNS

어플라이언스에서 MX 조회를 수행하여 특정 도메인에 대한 다음 홉(hop)을 확인하도록 하려면 특수 키워드 USEDNS를 사용합니다. 이는 하위 도메인에 대한 메일을 특정 호스트로 라우팅해야 할 경우 유용합니다. 예를 들어 example.com에 대한 메일을 회사의 Exchange 서버로 전송하려는 경우 다음 SMTP 경로와 유사한 것이 있을 것입니다.

```
example.com exchange.example.com
```

그러나 다양한 하위 도메인(foo.example.com)에 대한 메일에는 다음과 같은 SMTP 경로를 추가합니다.

```
.example.com USEDNS
```

14 장

관리 작업 배포

이 장에는 다음 섹션이 포함되어 있습니다.

관리 작업 배포 정보

사용자 계정에 지정하는 사용자 역할에 따라 다른 사람에게 Cisco Content Security Management Appliance의 관리 작업을 배포할 수 있습니다.

관리 작업 배포를 위해 설정하려면 사전 정의된 사용자 역할이 요구 사항에 부합하는지 확인하고 필요한 맞춤 사용자 역할이 있으면 생성하고 보안 어플라이언스 로컬에서 또는 자체 중앙 LDAP 또는 RADIUS 시스템을 사용하여 외부에서 관리자 사용자를 인증하도록 어플라이언스를 구성합니다.

또한 어플라이언스 및 어플라이언스의 특정 정보에 대한 액세스와 관련하여 추가 제어를 지정할 수 있습니다.

사용자 역할 할당

격리 액세스를 위한 추가 구성이 필요합니다. 격리 액세스 , 410 페이지를 참조하십시오.

사전 정의된 사용자 역할

명시된 경우를 제외하고, 다음 표에 설명한 권한의 사전 정의된 사용자 역할 또는 맞춤형 사용자 역할을 각 사용자에게 할당할 수 있습니다.

표 ***83:*** 사용자 역할의 설명

사용자 역할 이름	설명	웹 보고/예약된 보고서 기능
admin	**admin** 사용자는 시스템의 기본 사용자 계정으로 모든 관리 권한을 갖습니다. 관리 사용자 계정이 편의상 여기에 나열되어 있지만, 이 계정은 사용자 역할을 통해 할당할 수 없으며 수정하거나 삭제할 수도 없습니다. 단, 암호 변경은 가능합니다. 관리 사용자만 **resetconfig** 및 **revert** 명령을 실행할 수 있습니다.	예/예
Administrator(관리자)	관리자 역할의 사용자 계정은 시스템의 모든 구성 설정에 대한 모든 액세스 권한을 갖습니다.	예/예
Operator(운영자)	운영자 역할의 사용자 계정은 다음 작업에 제한이 있습니다. • 사용자 계정 만들기 또는 수정. • 어플라이언스 업그레이드. • `resetconfig` 명령 실행. • 시스템 설정 마법사 실행 • LDAP가 외부 인증에 대해 활성화된 경우 사용자 이름과 암호 외 LDAP 서버 프로필 설정 수정 • 격리 구성, 수정, 삭제 또는 중앙 집중화. 그 외에는 Administrator 역할과 동일한 권한을 보유합니다.	예/예
Technician(기술자)	이 역할의 사용자 계정은 업그레이드 및 재부팅과 같은 시스템 관리 활동을 시작하고 어플라이언스의 구성 파일을 저장하며 기능 키를 관리하는 등의 작업을 수행할 수 있습니다.	웹 및 이메일 탭에서 시스템 용량 보고서 액세스

사용자 역할 이름	설명	웹 보고/예약된 보고서 기능
Read-Only Operator(읽기 전용 운영자)	읽기 전용 작업자 역할의 사용자 계정은 구성 정보를 볼 수 있습니다. 이 역할의 사용자는 기능을 구성하는 방법을 알아보기 위해 변경을 수행하여 제출할 수 있지만 커밋할 수는 없으며 커밋이 필요하지 않은 변경도 수행할 수 없습니다. 이 역할의 사용자는 액세스가 활성화된 경우 격리의 메시지를 관리할 수 있습니다. 이 역할의 사용자는 다음 항목에 액세스할 수 없습니다. • 파일 시스템, FTP 또는 SCP. • 격리 만들기, 수정, 삭제 또는 중앙 집중화를 위한 설정.	예/아니요
Guest(게스트)	게스트 역할의 사용자 계정은 액세스가 활성화된 경우 보고서 및 웹 추적과 같은 상태 정보를 보고 격리의 메시지를 관리할 수 있습니다. 게스트 역할의 사용자는 메시지 추적 기능을 사용할 수 없습니다.	예/아니요
Web Administrator(웹 관리자)	이 역할의 사용자 계정은 **Web(웹)** 탭의 모든 구성 설정에 대한 모든 액세스 권한을 보유합니다.	예/예
Web Policy Administrator(웹 정책 관리자)	이 역할의 사용자 계정은 웹 어플라이언스 상태 페이지 및 구성 마스터의 모든 페이지에 액세스할 수 있습니다. 웹 정책 관리자는 ID, 액세스 정책, 해독 정책, 라우팅 정책, 프록시 바이패스, 맞춤 URL 범주, 시간 범위를 구성할 수 있습니다. 웹 정책 관리자는 구성을 게시할 수는 없습니다.	아니요/아니요
이메일 관리자	이 역할의 사용자 계정은 격리를 포함하여 이메일 메뉴에 한해 모든 구성 설정에 액세스할 수 있습니다.	아니요/아니요

사용자 역할 이름	설명	웹 보고/예약된 보고서 기능
Help Desk User	Help Desk 사용자 역할의 사용자 계정의 작업은 다음으로 제한됩니다. • Message Tracking(메시지 추적) • 격리의 메시지 관리 이 역할의 사용자는 CLI를 포함하여 시스템의 나머지에 액세스할 수 없습니다. 사용자에게 이 역할을 부여하면 이 사용자의 액세스를 허용하도록 격리를 구성해야 합니다.	아니요/아니요
사용자 지정 역할	맞춤 사용자 역할이 부여된 사용자 계정은 정책, 기능 또는 그 역할에 구체적으로 위임된 정책이나 기능의 인스턴스만 보고 구성할 수 있습니다. Add Local User(로컬 사용자 추가) 페이지에서 새 맞춤 이메일 사용자 역할 또는 새 맞춤 웹 사용자 역할을 생성할 수 있습니다. 그러나 이 맞춤 사용자 역할에 권한을 지정해야 역할 사용이 가능합니다. 권한을 지정하려면 **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > User Roles(사용자 역할)**에서 사용자 이름을 클릭합니다. 참고 맞춤 이메일 사용자 역할에 지정된 사용자는 CLI에 액세스할 수 없습니다. 자세한 내용은 맞춤형 사용자 역할 , 404 페이지를 참고하십시오.	아니요/아니요

맞춤형 사용자 역할

Security Management Appliance에서 Administration 권한의 사용자는 관리 기능을 맞춤형 역할에 위임할 수 있습니다. 맞춤형 역할은 사전 정의된 사용자 역할에 비해 사용자의 액세스를 좀 더 유연하게 제어할 수 있습니다.

맞춤 사용자 역할을 지정하는 사용자는 어플라이언스, 기능, 엔드유저 하위 집합에 대해 정책을 관리하거나 보고서에 액세스할 수 있습니다. 예를 들어 웹 서비스에 대해 위임받은 관리자가 본사와 다른 제한적 사용 정책을 갖는 다른 국가의 지사에 대한 정책을 관리하게 할 수 있습니다. 맞춤 사용자 역할을 생성하고 이 역할에 액세스 권한을 지정하는 방법으로 관리를 위임합니다. 위임받은 관리자가 어떤 정책, 기능, 보고서, 맞춤 URL 범주 등을 보고 수정할 수 있는지 결정해야 합니다.

자세한 내용은 다음 링크를 참조하십시오.

- 맞춤 이메일 사용자 역할 정보 , 405 페이지

• 맞춤 사용자 역할 삭제 , 410 페이지

맞춤 이메일 사용자 역할 정보

위임된 관리자가 Security Management Appliance에서 다음에 액세스하도록 맞춤형 역할을 할당할 수 있습니다.

- 모든 보고서(보고 그룹별로 제한 가능)
- 메일 정책 보고서(보고 그룹별로 제한 가능)
- DLP 보고서(보고 그룹별로 제한 가능)
- Message Tracking(메시지 추적)
- 쿼런틴

이 섹션에 이어 각 항목에 대해 자세히 설명합니다. 또한 이 권한 중 하나라도 부여받은 모든 사용자는 Management Appliance(관리 애플리케이션 탭 > Centralized Services(중앙 서비스) 메뉴에서 시스템 상태를 볼 수 있습니다. 맞춤형 이메일 사용자 역할이 할당된 사용자는 CLI에 액세스할 수 없습니다.

참고 Email Security Appliance의 맞춤형 사용자 역할은 Security Management Appliance의 사용자 역할에 비해 더 세부적인 액세스를 제공합니다. 예를 들어 메일과 DLP 정책 및 콘텐츠 필터에 대한 액세스를 위임할 수 있습니다. 자세한 내용은 Email Security Appliance에 대한 문서 또는 온라인 도움말의 "일반 관리" 장에서 "위임된 관리의 맞춤형 사용자 역할 관리" 섹션을 참조하십시오.

이메일 보고 액세스

다음 섹션에 설명한 것처럼, 맞춤형 사용자 역할에 Email(이메일) 보고서에 대한 액세스 권한을 부여할 수 있습니다.

Security Management Appliance의 Email Security Monitor(이메일 보안 모니터) 페이지에 대한 자세한 내용은 중앙 이메일 보안 보고 사용, 61 페이지의 해당 장을 참조하십시오.

모든 보고서

맞춤형 역할이 모든 보고서에 액세스하도록 허용하는 경우, 이 역할이 할당된 사용자는 모든 Email Security Appliance에 대해 또는 선택한 보고 그룹에 대해 다음 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.

- Mail Flow Summary(메일 플로우 요약)
- Mail FLow Details(메일 플로우 세부 정보)
- Outgoing Destinations(발신 대상)
- User Mail Summary
- DLP Incidents(DLP 인시던트)
- 콘텐츠 필터
- Virus Filtering(바이러스 필터링)

- TLS Encryption(TLS 암호화)
- 예약 보고서
- Archived Reports(보관된 보고서)

메일 정책 보고서

맞춤형 역할이 메일 정책 보고서에 액세스하도록 허용하는 경우, 이 역할이 할당된 사용자는 모든 Email Security Appliance에 대해 또는 선택한 보고 그룹에 대해 다음 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.

- Mail Flow Summary(메일 플로우 요약)
- Mail FLow Details(메일 플로우 세부 정보)
- Outgoing Destinations(발신 대상)
- User Mail Summary
- 콘텐츠 필터
- Virus Filtering(바이러스 필터링)
- Archived Reports(보관된 보고서)

DLP 보고서

DLP 역할이 모든 보고서에 액세스하도록 허용하는 경우, 이 역할이 할당된 사용자는 모든 Email Security Appliance에 대해 또는 선택한 보고 그룹에 대해 다음 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.

- DLP Incidents(DLP 인시던트)
- Archived Reports(보관된 보고서)

메시지 추적 데이터에 액세스

메시지 추적에 대한 맞춤형 역할 액세스 권한을 부여하는 경우 이 역할을 할당한 사용자는 Security Management Appliance에 의해 추적된 모든 메시지의 상태를 찾을 수 있습니다.

DLP 정책을 위반한 메시지의 민감 정보에 대한 액세스를 제어하려면 메시지 추적 시 중요 정보의 액세스 제어 , 426 페이지를 참조하십시오.

Security Management Appliance에서 메시지 추적에 액세스하도록 어플라이언스를 설정하는 방법에 대한 안내를 포함하여 메시지 추적에 대한 자세한 내용은 메시지 추적, 263 페이지을 참조하십시오.

맞춤 사용자 역할의 격리 액세스

격리에 대한 맞춤형 역할 액세스를 허용하는 경우 이 역할을 할당한 사용자는 Security Management Appliance의 모든 격리에서 메시지를 검색하고 보고 해제하거나 삭제할 수 있습니다.

사용자가 격리에 액세스하려면 먼저 해당 액세스를 활성화해야 합니다. 격리 액세스 , 410 페이지를 참조하십시오.

맞춤 이메일 사용자 역할 생성

이메일 보고, 메시지 추적, 격리에 액세스할 수 있는 맞춤 이메일 사용자 역할을 생성할 수 있습니다.

이러한 각 옵션이 허용하는 액세스에 대한 자세한 내용은 맞춤 이메일 사용자 역할 정보 , 405 페이지 및 해당 하위 섹션을 참조하십시오.

참고 좀 더 세부적인 액세스 또는 다른 기능, 보고서, 정책에 대한 액세스를 허용하려면 각 Email Security Appliance에서 직접 맞춤형 사용자 역할을 만들 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > User Roles(**사용자 역할**)**를 선택합니다.

단계 **3** **Add Email User Role(**이메일 사용자 역할 추가**)**을 클릭합니다.

팁 또는 기존 이메일 사용자 역할을 복제하여 새 역할을 생성할 수도 있습니다. 해당 테이블 행에서 복제 아이콘을 클릭하고 생성되는 복사본을 수정하면 됩니다.

단계 **4** 사용자 역할에 대한 고유한 이름(예: “dlp-auditor”) 및 설명을 입력합니다.

- 이메일 및 웹 맞춤형 사용자 역할 이름은 복제해서는 안 됩니다.
- 이름에는 소문자, 숫자 및 대시만 사용할 수 있습니다. 이름은 대시 또는 숫자로 시작할 수 없습니다.
- 이 역할의 사용자가 중앙 집중식 정책 격리에 액세스하도록 허용하며, Email Security Appliance의 메시지와 콘텐츠 필터 및 DLP 메시지 작업에서 중앙 집중식 격리를 지정할 수 있도록 하려면, 맞춤형 역할의 이름은 두 어플라이언스에서 동일해야 합니다.

단계 **5** 이 역할에 대해 활성화할 액세스 권한을 선택합니다.

단계 **6** **Submit(**제출**)**을 클릭하여 사용자 역할 페이지로 돌아가면 새 사용자 역할이 표시됩니다.

단계 **7** 보고 그룹별로 액세스를 제한할 경우 그 사용자 역할에 대해 이메일 보고 열에서 **no groups selected(**선택된 그룹 없음**)** 링크를 클릭하고 하나 이상의 보고 그룹을 선택합니다.

단계 **8** 변경 사항을 커밋합니다.

단계 **9** 이 역할에 격리에 대한 액세스 권한을 부여한 경우 이 역할을 위해 액세스를 활성화합니다.

참조:

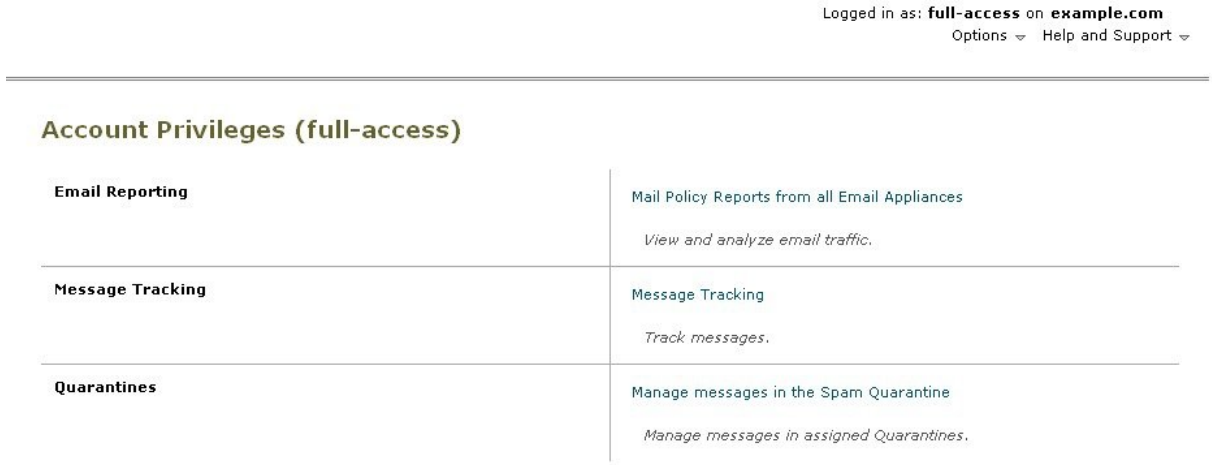
- 스팸 격리에 대한 관리 사용자 액세스 구성 , 285 페이지

• 정책, 바이러스, Outbreak 격리 구성 , 323 페이지

맞춤형 이메일 사용자 역할 사용

맞춤형 이메일 사용자 역할이 할당된 사용자가 어플라이언스에 로그인하면, 액세스 권한이 있는 보안 기능에 대한 링크만 표시됩니다. 사용자는 언제라도 Options(옵션) 메뉴에서 Account Privileges(계정 권한)를 선택하여 이 기본 페이지로 돌아올 수 있습니다. 이 사용자는 또한 웹 페이지 상단에 있는 메뉴를 사용하여 액세스 권한이 있는 기능에 액세스할 수 있습니다. 다음 예에서 사용자는 맞춤형 이메일 사용자 역할을 통해 Security Management Appliance에서 사용 가능한 모든 기능에 액세스할 수 있습니다.

그림 ***11:*** 맞춤형 이메일 사용자 역할이 할당된 위임 관리자의 ***Account Privileges(***계정 권한***)*** 페이지



맞춤 웹 사용자 역할 정보

맞춤형 웹 사용자 역할이 할당된 사용자는 정책을 여러 Web Security Appliance에 게시할 수 있으며, 맞춤형 구성을 수정하거나 여러 어플라이언스에 게시할 수 있습니다.

Security Management Appliance의 **Web(**웹**) > Configuration Master(**구성 마스터**) > Custom URL Categories(**맞춤형 **URL** 카테고리**)** 페이지에서 관리 및 게시가 허용된 URL 카테고리 및 정책을 볼 수 있습니다. 또한 **Web(**웹**) > Utilities(**유틸리티**) > Publish Configuration Now(**구성 지금 게시**)** 페이지에서도 가능한 구성을 볼 수 있습니다.

참고 게시 권한 기능을 가진 맞춤 역할을 생성할 경우 사용자가 로그인하면 사용 가능한 메뉴가 없습니다. 게시 메뉴가 없으며 수정 불가한 랜딩 화면이 표시됩니다. URL 및 정책 탭에 어떤 기능도 없기 때문입니다. 사실상 어떤 카테고리나 정책도 게시하거나 관리할 수 없는 사용자입니다. 사용자에게 게시 권한을 주되 어떤 카테고리 또는 정책도 관리할 수 없게 하려면 어떤 정책에서도 사용하지 않는 맞춤 카테고리를 생성하고 사용자가 게시 기능으로 그 맞춤 카테고리를 관리할 수 있게 하면 됩니다. 그러면 그 범주에서 URL을 추가하거나 삭제할 경우 어디에도 영향을 주지 않습니다.

맞춤 사용자 역할을 생성하고 수정하면서 웹 관리를 위임할 수 있습니다.

- 맞춤 웹 사용자 역할 생성, 409 페이지
- 맞춤 웹 사용자 역할 수정, 410 페이지
- 맞춤 사용자 역할 삭제 , 410 페이지

맞춤 웹 사용자 역할 생성

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > User Roles(**사용자 역할**)**를 선택합니다.

단계 **3** **Add Web User Role(**웹 사용자 역할 추가**)**을 클릭합니다.

팁 또는 기존 웹 사용자 역할을 복제하여 새 역할을 생성할 수도 있습니다. 해당 테이블 행에서 복제 아이콘을 클릭하고 생성되는 복사본을 수정하면 됩니다.

단계 **4** 사용자 역할에 대한 고유한 이름(예: “canadian-admins”) 및 설명을 입력합니다.

참고 이름은 소문자, 숫자, 대시만 포함할 수 있습니다. 대시로 시작할 수 없습니다.

단계 **5** 정책 또는 맞춤 URL 범주를 기본적으로 표시할지 아니면 숨길지 선택합니다.

단계 **6** 게시 권한을 활성화할지 아니면 비활성화할지 선택합니다.

사용자는 이 권한을 통해 액세스 정책이나 URL 범주의 수정이 가능한 구성 마스터를 게시할 수 있습니다.

단계 **7** 새 (빈) 설정을 시작할지 아니면 기존 고객 사용자 역할을 복사할지 선택합니다. 기존 사용자 역할을 복사하려는 경우 복사할 역할을 목록에서 사용합니다.

단계 **8** **Submit(**제출**)**을 클릭하여 사용자 역할 페이지로 돌아가면 새 사용자 역할이 표시됩니다.

참고 웹 보고에서 익명 기능을 활성화한 경우 웹 보고 액세스 권한을 갖는 모든 사용자 역할이 인터랙티브 보고서 페이지에서 인식 불가한 사용자 이름 및 역할을 갖게 됩니다. 중앙 웹 보고 및 추적 사용, 177 페이지장의 웹 보고서 예약 , 239 페이지 섹션을 참조하십시오. 예약 보고서에서 실제 사용자 이름을 볼 수 있는 관리자 역할은 예외입니다. 익명 기능이 활성화된 경우 운영자 및 웹 관리자가 생성하는 예약 보고서는 익명 처리됩니다.

Web(웹**) > Utilities(**유틸리티**) > Security Services Display(**보안 서비스 표시**) > Edit Security Services Display(**보안 서비스 표시 수정**)** 페이지를 사용하여 구성 마스터 중 하나를 숨길 경우 User Roles(사용자 역할) 페이지에서도 해당 구성 마스터 열이 숨겨집니다. 그러나 숨겨진 구성 마스터에 대한 권한 설정은 유지됩니다.

맞춤 웹 사용자 역할 수정

단계 **1** User Roles(사용자 역할) 페이지에서 Edit User Role(사용자 역할 수정) 페이지를 표시할 역할 이름을 클릭합니다.

단계 **2** 이름, 설명, 정책 표시 여부, 맞춤 URL 범주 등의 설정을 수정합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

맞춤 사용자 역할의 권한을 수정하려면

User Roles(사용자 역할) 페이지로 이동합니다.

- 액세스 정책 권한을 수정하려면 "Access policies(액세스 정책)"를 클릭하여 구성 마스터에 구성된 액세스 정책의 목록을 표시합니다. Include(포함) 열에서 이 사용자에게 수정 권한을 부여할 정책의 확인란을 선택합니다. **Submit(**제출**)**을 클릭하여 User Roles(사용자 역할) 페이지로 돌아갑니다.

-또는-

- 맞춤 URL 범주 권한을 수정하려면 Custom URL Categories(맞춤 URL 범주)를 클릭하여 구성 마스터에 정의된 맞춤 URL 범주의 목록을 표시합니다. Include(포함) 열에서 이 사용자에게 수정 권한을 부여할 맞춤 URL 범주의 확인란을 선택합니다. **Submit(**제출**)**을 클릭하여 User Roles(사용자 역할) 페이지로 돌아갑니다.

맞춤 사용자 역할 삭제

한 명 이상의 사용자에게 할당된 맞춤형 사용자 역할을 삭제하는 경우 오류가 표시되지 않습니다.

CLI 액세스 권한의 사용자 역할

일부 권한은 GUI 및 CLI 관리자, 운영자, 게스트, 기술자, 읽기 전용 운영자에 모두 액세스할 수 있습니다. GUI만 액세스 가능한 역할도 있습니다. 헬프데스크 사용자, 이메일 관리자, 웹 관리자, 웹 정책 관리자, URL 필터링 관리자(웹 보안), 맞춤 사용자입니다.

LDAP 사용

사용자 인증을 위해 LDAP 디렉터리를 사용하는 경우 개별 사용자 대신 사용자 역할에 디렉터리 그룹을 지정합니다. 디렉토리 그룹을 사용자 역할에 할당하는 경우 해당 그룹의 각 사용자는 해당 사용자 역할에 정의된 권한을 받습니다. 자세한 내용은 외부 사용자 인증 , 419 페이지를 참고하십시오.

격리 액세스

사용자가 격리에 액세스하려면 먼저 그 액세스 권한을 활성화해야 합니다. 다음 정보를 참조하십시오.

- 스팸 격리에 대한 관리 사용자 액세스 구성 , 285 페이지
- 메시지 처리 작업을 다른 사용자들에게 분산 , 329 페이지(정책 격리) 및 정책, 바이러스, Outbreak 격리 구성 , 323 페이지

- 맞춤형 사용자 역할을 위해 중앙 집중식 격리 액세스 구성 , 320 페이지.

Users(사용자) 페이지

이 섹션에 대한 정보	참조
사용자 Reset Passphrases(암호 재설정) 버튼	관리 작업 배포 정보 , 401 페이지 로컬 정의 관리자 사용자 관리 , 412 페이지 요구 시 사용자가 반드시 암호 변경하도록 설정 , 417 페이지
로컬 사용자 계정 및 암호 설정	암호 및 로그인 요구 사항 설정 , 414 페이지
외부 인증	외부 사용자 인증 , 419 페이지
DLP 추적 권한	메시지 추적 시 중요 정보의 액세스 제어 , 426 페이지

관리자 사용자 인증 정보

어플라이언스 로컬에서 권한 있는 사용자를 정의하는 방법 및/또는 외부 인증을 사용하여 어플라이언스에 대한 액세스를 제어할 수 있습니다.

- 관리 사용자의 암호 변경, 411 페이지
- 만료 후 사용자의 암호 변경, 412 페이지
- 로컬 정의 관리자 사용자 관리 , 412 페이지
- 외부 사용자 인증 , 419 페이지

관리 사용자의 암호 변경

관리자 레벨 사용자는 GUI 또는 CLI를 통해 "관리" 사용자의 암호를 변경할 수 있습니다.

GUI를 통해 암호를 변경하려면 다음을 수행합니다.

- [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.
- **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Users(사용자)** 페이지를 선택하고 관리 사용자를 선택합니다.

CLI에서 관리 사용자의 암호를 변경하려면 `passphrase` 명령을 사용합니다. `passphrase` 명령을 사용할 경우 보안을 위해 기존 암호를 입력해야 합니다.

"관리" 사용자 계정의 암호를 잊어버린 경우 고객 지원사에 문의하여 암호를 재설정합니다.

참고 암호 변경사항은 즉시 적용되며, 변경사항을 커밋할 필요는 없습니다.

만료 후 사용자의 암호 변경

계정이 만료되면 "Your passphrase expired. Please change your passphrase by clicking here.(비밀번호/암호가 만료되었습니다. 여기를 클릭하여 비밀번호/암호를 변경하십시오.)"라는 메시지가 표시됩니다.

링크를 클릭하고 로그인 세부 정보와 만료된 암호를 입력하여 Change Passphrase(암호 변경) 페이지로 이동합니다. 암호 설정에 대한 자세한 내용은 암호 및 로그인 요구 사항 설정 , 414 페이지을 참조하십시오.

참고 암호 변경사항은 즉시 적용되며, 변경사항을 커밋할 필요는 없습니다.

로컬 정의 관리자 사용자 관리

로컬 정의 사용자 추가

외부 인증을 사용하지 않는 경우 다음 절차를 수행하여 Security Management Appliance에 직접 사용자를 추가합니다. 또는 CLI에서 **userconfig** 명령을 사용합니다.

참고 외부 인증도 활성화된 경우 로컬 사용자 이름이 외부 인증 사용자 이름과 중복되어서는 안 됩니다.

어플라이언스에서 생성할 수 있는 사용자 계정 수에는 제한이 없습니다.

단계 **1** 맞춤 사용자 역할을 지정할 경우 이 역할을 먼저 정의하는 것이 좋습니다. 맞춤형 사용자 역할 , 404 페이지를 참조하십시오.

단계 **2** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **3** **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Users**(사용자)를 선택합니다.

단계 **4** **Add User**(사용자 추가)를 클릭합니다.

단계 **5** 사용자의 고유한 이름을 입력합니다. 시스템 예약어(예: "`operator`", "`root`")는 입력할 수 없습니다.

외부 인증도 사용할 경우 사용자 이름이 외부 인증 사용자 이름과 중복되어서는 안 됩니다.

단계 **6** 사용자의 전체 이름을 입력합니다.

단계 **7** 사전 정의 역할 또는 맞춤 역할을 선택합니다. 사용자 역할에 대한 자세한 내용은 사전 정의된 사용자 역할 , 402 페이지 섹션의 사용자 역할의 설명 표를 참조하십시오.

여기서 새 이메일 역할 또는 웹 역할을 추가할 경우 그 역할에 대한 이름을 입력합니다. 이름 지정 관련 제한은 맞춤 이메일 사용자 역할 생성 , 407 페이지 또는 맞춤 웹 사용자 역할 생성, 409 페이지를 참조하십시오.

단계 **8** 암호를 입력하고 재입력합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

단계 **10** 이 페이지에서 맞춤 사용자 역할을 추가한 경우 지금 그 역할에 권한을 지정합니다. 맞춤형 사용자 역할 , 404 페이지를 참조하십시오.

로컬 정의 사용자 수정

이 절차는 암호 등을 변경하는 데 사용합니다.

단계 **1** 사용자 목록에서 사용자 이름을 클릭합니다.

단계 **2** 사용자를 변경합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

로컬 정의 사용자 삭제

단계 **1** 사용자 목록의 사용자 이름에 해당하는 휴지통 아이콘을 클릭합니다.

단계 **2** 나타나는 경고 대화 상자에서 **Delete**(삭제)를 클릭하여 삭제를 확인합니다.

단계 **3** **Commit**(커밋)을 클릭하여 변경사항을 커밋합니다.

로컬 정의 사용자의 목록 보기

로컬 정의 사용자 목록을 보려면 다음을 수행합니다.

- [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

- **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Users**(사용자)를 선택합니다.

참고 별표는 위임 관리에 대한 맞춤 사용자 역할이 사용자에게 지정되었음을 나타냅니다. 사용자의 맞춤 역할이 삭제되면 "Unassigned(지정 없음)"가 빨간색으로 표시됩니다. 사용자 지정 사용자 역할에 대한 자세한 내용은 맞춤형 사용자 역할 , 404 페이지를 참조하십시오.

암호 설정 및 변경

- 사용자를 추가할 때 그 사용자의 최초 암호를 지정합니다.
- 시스템에 구성된 사용자의 암호를 변경하려면 GUI에서 Edit User(사용자 수정) 페이지를 사용합니다(자세한 내용은 로컬 정의 사용자 수정, 413 페이지 참조).
- 시스템 기본 관리 사용자 계정의 암호를 변경하려면 관리 사용자의 암호 변경, 411 페이지 섹션을 참조하십시오.
- 사용자가 반드시 암호를 변경하게 하려면 요구 시 사용자가 반드시 암호 변경하도록 설정 , 417 페이지 섹션을 참조하십시오.
- 사용자는 GUI 창 오른쪽 위의 Options(옵션) 메뉴를 클릭하고 Change Passphrase(암호 변경) 옵션을 선택하여 자신의 암호를 변경할 수 있습니다.

암호 및 로그인 요구 사항 설정

사용자 계정과 암호 제한을 정의하여 조직의 암호 정책을 적용할 수 있습니다. 사용자 계정과 암호 제한은 Security Management Appliance에 정의된 로컬 사용자에게 적용됩니다. 다음과 같은 설정을 구성할 수 있습니다.

- 사용자 계정 잠금. 사용자 계정이 잠기도록 로그인 실패 횟수를 정의할 수 있습니다
- 암호 수명 규칙. 사용자가 로그인한 후 암호를 변경해야 하기 전까지 암호를 유지할 수 있는 기간을 정의할 수 있습니다.
- 암호 규칙. 사용자가 선택할 수 있는 암호의 종류(예: 선택 문자 또는 필수 문자)를 정의할 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Users**(사용자)를 선택합니다.

단계 **3** 아래로 스크롤하여 로컬 사용자 계정 및 암호 설정 섹션으로 이동합니다.

단계 **4** **Edit Settings**(설정 수정)를 클릭합니다.

단계 **5** 설정을 구성합니다.

설정	설명
사용자 계정 잠금	사용자가 로그인에 실패한 후 사용자 계정을 잠글지 여부를 선택합니다. 사용자 계정을 잠그기 위한 로그인 실패 횟수를 지정합니다. 1~60의 숫자를 입력할 수 있습니다. 기본값은 5입니다. 계정 잠금을 구성할 때 로그인을 시도하는 사용자에게 표시할 메시지를 입력합니다. 7비트 ASCII 문자를 사용하여 텍스트를 입력합니다. 이 메시지는 잠긴 계정에 사용자가 올바른 암호를 입력할 때에만 표시됩니다. 사용자 계정이 잠긴 경우 관리자는 GUI의 Edit User(사용자 편집) 페이지 또는 `userconfig` CLI 명령을 사용하여 해당 계정을 잠금 해제할 수 있습니다. 로그인 실패는 사용자가 연결된 머신 또는 연결 유형(예: SSH 또는 HTTP)에 관계없이 사용자에 의해 추적됩니다. 사용자가 성공적으로 로그인하면 로그인 실패 횟수는 0으로 재설정됩니다. 최대 로그인 실패 횟수에 도달하여 사용자 계정이 잠긴 경우 관리자에게 경고를 보냅니다. 이 경고는 "Info" 심각도 수준으로 설정됩니다. 참고 개별 사용자 계정은 수동으로 잠글 수 있습니다. 사용자 계정 수동으로 잠금, 418 페이지를 참조하십시오.
암호 재설정	관리자가 암호를 변경한 후 사용자가 반드시 암호를 변경하게 할지 여부를 선택합니다. 암호 만료 후 사용자가 반드시 변경하게 할지 여부도 선택할 수 있습니다. 사용자가 비밀번호를 변경하기 전까지 암호가 유지되는 기간(일)을 입력합니다. 1~366의 숫자를 입력할 수 있습니다. 기본값은 90입니다. 사용자가 예약되지 않은 시간에 반드시 암호를 변경하게 하려면 요구 시 사용자가 반드시 암호 변경하도록 설정 , 417 페이지 섹션을 참조하십시오. 암호 만료 후 사용자가 반드시 암호를 변경하게 할 경우 비밀번호 만료 예정에 대한 알림을 표시할 수 있습니다. 비밀번호가 만료되기 며칠 전부터 사용자에게 알릴지 그 기간(일)을 선택합니다. 참고 사용자 계정이 암호 과제 대신 SSH 키를 사용하는 경우에도 Passphrase Reset(암호 재설정) 규칙이 적용됩니다. SSH 키의 사용자 계정이 만료될 때 계정과 연결된 키를 변경하려면 사용자는 이전 암호를 입력하거나 관리자에게 암호를 수동으로 변경해달라고 요청해야 합니다.
암호 규칙: 최소<number>자가 필요합니다.	암호에 포함해야 할 최소 문자 수를 입력합니다. 0 ~ 128의 수를 입력할 수 있습니다. 기본값은 8입니다. 암호의 문자 수는 여기에 지정한 것보다 클 수 있습니다.
암호 규칙: 적어도 하나의 숫자(0~9)가 필요합니다.	암호에 적어도 하나의 숫자가 포함되어야 하는지 여부를 선택합니다.

설정	설명
암호 규칙: 적어도 하나의 특수 문자가 필요합니다.	암호에 적어도 하나의 특수 문자가 포함되어야 하는지 여부를 선택합니다. 암호에는 다음과 같은 특수 문자가 포함될 수 있습니다. ~ ? ! @ # $ % ^ & * - _ + = \ | / [ ] ( ) < > { } ` ' " ; : , .
암호 규칙: 사용자 이름이나 사용자 이름을 변형한 암호를 사용할 수 없습니다.	연결된 사용자 이름 및 사용자 이름의 변형을 암호에 사용하도록 허용할지 여부를 선택합니다. 사용자 이름 변형이 금지된 경우 암호에 다음 규칙이 적용됩니다. • 대/소문자와 상관없이 암호는 사용자 이름과 동일해서는 안 됩니다. • 대/소문자와 상관없이 암호는 사용자 이름의 역순과 동일해서는 안 됩니다. • 암호는 다음의 대체 문자가 있는 사용자 이름 또는 사용자 이름의 역순과 동일할 수 없습니다. • "a": "@" 또는 "4" • "e": "3" • "i": "|", "!" 또는 "1" • "o": "0" • "s": "$" 또는 "5" • "t"" "+" 또는 "7"
암호 규칙: 지난 암호 <number>개를 재사용할 수 없도록 설정합니다.	사용자가 암호를 강제로 변경해야 하는 경우 최근에 사용한 암호를 사용하도록 허용할지 여부를 선택합니다. 최근 암호를 재사용하는 것을 허용하지 않을 경우 지난 암호 몇 개를 사용할 수 없는지 그 숫자를 입력합니다. 1~15의 숫자를 입력할 수 있습니다. 기본값은 3입니다.
암호 규칙: 암호에서 허용되지 않는 단어 목록	암호에서 허용되지 않는 단어 목록을 만들 수 있습니다. 금지 단어를 각각의 줄에 입력한 텍스트 파일을 만듭니다. 파일을 forbidden_passphrase_words.txt라는 이름으로 저장하고 SCP 또는 FTP를 사용하여 어플라이언스에 파일을 업로드합니다. 이 제한 사항을 선택된 상태에서 단어 목록을 업로드하지 않으면 제한 사항이 무시됩니다.

설정	설명
암호 강도	관리자나 사용자가 새 암호를 입력할 때 암호 강도 표시기를 표시할 수 있습니다. 이 설정은 강력한 암호를 생성하도록 강제하는 것은 아니며 단순히 입력한 암호를 얼마나 쉽게 추측할 수 있는가를 보여줍니다. 표시기를 표시할 역할을 선택합니다. 선택한 역할에 0보다 큰 숫자를 입력합니다. 숫자가 더 크면 등록되는 암호의 강도를 획득하기가 더 어렵다는 의미입니다. 이 설정에는 최대값이 없습니다. 예: • 30을 입력하면 하나 이상의 대문자, 소문자, 숫자 및 특수 문자를 포함하는 8자리 암호가 강력한 암호로 등록됩니다. • 18을 입력하면 모두 소문자이고 숫자 또는 특수 문자가 없는 8자리 암호가 강력한 비밀번호로 등록됩니다. 암호 강도는 로그 눈금 간격으로 측정됩니다. 평가는 NIST SP 800-63, 부록 A에 정의된 미국 NIST(National Institute of Standards and Technology) 엔트로피 규칙을 기반으로 합니다. 일반적으로 다음과 같은 암호가 더 강력합니다. • 긴 길이 • 대문자, 소문자, 숫자 및 특수 문자 포함 • 모든 언어의 사전에 있는 단어를 포함하지 않음 이러한 특성을 가지는 암호를 적용하려면 이 페이지의 다른 설정을 사용합니다.

단계 **6** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

사용자가 암호를 새로운 요구 사항에 부합하는 새 암호로 변경하게 합니다. 요구 시 사용자가 반드시 암호 변경하도록 설정 , 417 페이지를 참조하십시오.

요구 시 사용자가 반드시 암호 변경하도록 설정

모든 또는 선택된 사용자가 임의의 시점에 즉시 암호를 변경하게 하려면 다음 절차의 단계를 수행합니다. 이 작업은 한 번만 수행하면 됩니다.

정기적으로 암호를 변경해야 하는 요구 사항을 자동화하려면 암호 및 로그인 요구 사항 설정 , 414 페이지의 설명대로 Passphrase Reset(암호 재설정) 옵션을 사용합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Users(**사용자**)**를 선택합니다.

단계 **3** Users(사용자) 섹션에서 암호를 변경해야 하는 사용자 옆의 확인란을 선택합니다.

단계 **4** **Enforce Passphrase Changes(**암호 변경 지시**)**를 선택합니다.

단계 **5** 옵션을 선택합니다.

유예 기간의 전역 설정이 로컬 사용자 계정 및 암호 설정에서 구성됩니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

로컬 사용자 계정 잠금 및 잠금 해제

사용자 계정을 잠그면 로컬 사용자가 어플라이언스에 로그인할 수 없습니다. 다음 방법 중 하나로 사용자 계정을 잠글 수 있습니다.

- 구성된 시도 횟수 이후 사용자가 성공적으로 로그인하지 못할 경우 모든 로컬 사용자 계정이 잠기도록 구성할 수도 있습니다. 암호 및 로그인 요구 사항 설정 , 414 페이지를 참조하십시오.
- 관리자는 사용자 계정을 수동으로 잠글 수 있습니다. 사용자 계정 수동으로 잠금, 418 페이지를 참조하십시오.

Edit User(사용자 수정) 페이지에서 사용자 계정을 보면 사용자 계정이 잠긴 이유가 표시됩니다.

사용자 계정 수동으로 잠금

단계 **1** 처음에만, 사용자 계정 잠금을 활성화하도록 어플라이언스를 설정합니다.

단계 **2** a) [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

b) **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Users(**사용자**)**로 이동합니다.

c) 로컬 사용자 계정 및 암호 설정 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

d) **Display Locked Account Message if Administrator has manually locked a user account(**관리자가 수동으로 사용자 계정을 잠근 경우 잠긴 계정 메시지 표시**)** 확인란을 선택하고 메시지를 입력합니다.

e) 변경사항을 제출합니다.

단계 **3** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Users(**사용자**)**를 클릭하고 사용자 이름을 클릭합니다.

참고 Admin 계정을 잠그기 전에 잠금 해제가 가능함을 확인합니다. 사용자 계정 잠금 해제 , 419 페이지의 참고를 읽어보십시오.

단계 **4** **Lock Account(**계정 잠금**)**를 클릭합니다.

사용자가 어플라이언스에 로그인할 수 없음을 알리며 계속할 것인지 묻는 메시지가 표시됩니다.

사용자 계정 잠금 해제

사용자 계정 잠금을 해제하려면 Users(사용자) 목록에서 사용자 이름을 클릭하여 사용자 계정을 열고 Unlock Account(계정 잠금 해제)를 클릭합니다.

참고 admin 계정을 잠근 경우에는 직렬 통신으로 직렬 콘솔 포트에 연결하고 admin으로 로그인해야만 잠금을 해제할 수 있습니다. admin 사용자는 admin 계정이 잠긴 경우에도 항상 직렬 콘솔 포트를 사용하여 어플라이언스에 액세스할 수 있습니다. 직렬 콘솔 포트를 사용하여 어플라이언스에 액세스하는 방법에 대한 자세한 내용은 Email Security Appliance용 문서 또는 온라인 도움말의 "설정 및 설치" 장을 참조하십시오.

외부 사용자 인증

네트워크의 LDAP 또는 RADIUS 디렉터리에 사용자 정보를 저장하는 경우 어플라이언스에 로그인하는 사용자를 인증하는 데 외부 디렉터리를 사용하도록 Security Management Appliance를 구성할 수 있습니다.

참고 보기 맞춤화 , 499 페이지의 일부 기능은 외부 인증 사용자가 사용할 수 없습니다.

- 로컬 인증과 외부 인증을 모두 사용할 경우 로컬 사용자 이름이 외부 인증 사용자 이름과 중복되어서는 안 됩니다.
- 어플라이언스가 외부 디렉터리와 통신할 수 없는 경우, 외부 및 로컬 계정이 모두 있는 사용자는 어플라이언스의 로컬 사용자 계정으로 로그인할 수 있습니다.

참조:

- LDAP를 사용하여 관리자 사용자의 외부 인증 구성 , 390 페이지
- RADIUS 인증 활성화, 419 페이지

LDAP 인증 구성

LDAP 인증 구성 방법은 LDAP를 사용하여 관리자 사용자의 외부 인증 구성 , 390 페이지를 참조하십시오.

RADIUS 인증 활성화

RADIUS 디렉터리를 사용하여 사용자를 인증하고 사용자 그룹을 사용자 역할에 지정하여 어플라이언스를 관리할 수 있습니다. RADIUS 디렉터리의 사용자를 사용자 역할에 할당하기 위해 AsyncOS에서 사용하는 CLASS 특성을 RADIUS 서버에서 지원해야 합니다.

참고 외부 사용자가 RADIUS 그룹에 대한 사용자 역할을 변경하면 해당 사용자는 어플라이언스에서 로그아웃한 후 다시 로그인해야 합니다.

시작하기 전에

RADIUS 서버에 액세스하기 위한 Shared Secret(공유 암호) 키는 48자를 넘어서는 안 됩니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**)** > **System Administration(**시스템 관리**)** > **Users(**사용자**)** 페이지를 선택하고 **Enable(**활성화**)**을 클릭합니다.

단계 **3** **Enable External Authentication(**외부 인증 활성화**)** 확인란을 선택합니다.

단계 **4** 인증 유형으로 RADIUS를 선택합니다.

단계 **5** RADIUS 서버의 호스트 이름을 입력합니다.

단계 **6** RADIUS 서버의 포트 번호를 입력합니다. 기본 포트 번호는 `1812`입니다.

단계 **7** RADIUS 서버의 Shared Secret(공유 암호) 키를 입력합니다.

참고 Email Security Appliance의 클러스터에 대해 외부 인증을 활성화할 경우 클러스터의 모든 어플라이언스에서 동일한 Shared Secret(공유 암호) 키를 입력합니다.

단계 **8** 어플라이언스가 시간 초과 전까지 서버에서 응답을 기다리는 시간(초)을 입력합니다.

단계 **9** 인증 프로토콜에 PAP(Passphrase Authentication Protocol)를 사용할지, 아니면 CHAP(Challenge Handshake Authentication Protocol)을 사용할지를 선택합니다.

단계 **10** (선택 사항) 또 다른 RADIUS 서버를 추가하려면 **Add Row(**행 추가**)**를 클릭합니다. 어플라이언스에서 인증에 사용할 RADIUS 서버 각각에 대해 6~7단계를 반복합니다.

여러 외부 서버를 정의할 경우 어플라이언스는 어플라이언스에 정의된 순서대로 서버에 연결합니다. 한 서버가 일시적으로 사용 불가할 때 페일오버를 위해 여러 외부 서버를 정의하는 경우가 있습니다.

단계 **11** 웹 사용자 인터페이스에 외부 인증 자격 증명을 저장하기 위한 시간을 입력합니다.

참고 RADIUS 서버에서 일회용 암호(예: 토큰에서 생성된 암호)를 사용하는 경우 영(0)을 입력합니다. 값을 0으로 설정하면 AsyncOS는 현재 세션 중에는 인증을 위해 RADIUS 서버에 다시 연결하지 않습니다.

단계 **12** 그룹 매핑 구성:

설정	설명
Map externally authenticated users to multiple local roles (Recommended)(외부에서 인증된 사용자를 다중 로컬 역할에 매핑(권장))	AsyncOS는 RADIUS CLASS 특성에 따라 RADIUS 사용자를 어플라이언스 역할에 할당합니다. CLASS 특성 요구 사항: • 최소 3자 • 최대 253자 • 콜론, 쉼표 또는 줄 바꿈 문자 없음 • RADIUS 사용자마다 하나 이상의 매핑된 CLASS 특성이 있음(이 설정을 사용하는 경우 AsyncOS는 매핑된 CLASS 특성이 없는 RADIUS 사용자의 액세스를 거부합니다.) 여러 CLASS 특성이 있는 RADIUS 사용자의 경우 AsyncOS는 제한이 가장 많은 역할을 할당합니다. 예를 들어 RADIUS 사용자에게 운영자 및 읽기 전용 작업자 역할에 매핑되어 있는 CLASS 특성 2개가 있는 경우 AsyncOS는 운영자 역할보다 제한이 많은 읽기 전용 작업자 역할에 RADIUS 사용자를 할당합니다. 어플라이언스 역할은 가장 제한이 적은 역할에서 가장 제한이 많은 역할 순으로 정렬됩니다. • Administrator • 이메일 관리자 • 웹 관리자 • 웹 정책 관리자 • URL Filtering Administrator(Web Security용) • 맞춤형 사용자 역할(Email 또는 Web) 맞춤형 사용자 역할에 매핑된 여러 Class 특성을 한 사용자에게 할당한 경우, RADIUS 서버의 목록에 있는 마지막 Class 특성이 사용됩니다. • Technician • 운영자 • Read-Only Operator • Help Desk User • 게스트
Map all externally authenticated users to the Administrator role(외부에서 인증된 모든 사용자를 Administrator 역할에 매핑)	AsyncOS는 RADIUS 사용자를 Administrator 역할에 할당합니다.

단계 **13** (선택 사항) 다른 그룹을 추가하려면 **Add Row(**행 추가**)**를 클릭합니다. 어플라이언스에서 인증하는 사용자 그룹별로 11단계를 반복합니다.

단계 **14** 변경 사항을 제출 및 커밋합니다.

Security Management Appliance 액세스 추가 제어

IP 기반 네트워크 액세스 구성

어플라이언스에 직접 연결된 사용자 및 역방향 프록시를 통해 연결된 사용자(조직에서 원격 사용자에 대해 역방향 프록시를 사용하는 경우)에 대한 액세스 목록을 생성하여 사용자가 Security Management Appliance에 액세스하는 데 사용하는 IP 주소를 제어할 수 있습니다.

직접 연결

Security Management Appliance에 연결할 수 있는 시스템에 대한 IP 주소, 서브넷 또는 CIDR 주소를 지정할 수 있습니다. 사용자는 액세스 목록의 IP 주소를 사용하는 머신에서 어플라이언스에 액세스할 수 있습니다. 목록에 포함되어 있지 않은 주소에서 어플라이언스에 연결하려고 하는 사용자의 액세스는 거부됩니다.

프록시를 통한 연결

조직의 네트워크가 원격 사용자의 시스템과 Security Management Appliance 간에 역방향 프록시 서버를 사용하는 경우, AsyncOS에서 어플라이언스에 연결할 수 있는 프록시의 IP 주소를 포함하는 액세스 목록을 생성할 수 있습니다.

역 프록시를 사용하는 경우에도 AsyncOS는 사용자 연결이 허용된 IP 주소의 목록을 기준으로 원격 사용자 시스템의 IP 주소를 확인합니다. 원격 사용자의 IP 주소를 Email Security Appliance로 전송하려면, 프록시는 어플라이언스에 대한 연결 요청에 x-forwarded-for HTTP 헤더를 포함해야 합니다.

x-forwarded-for 헤더는 다음과 같은 형식의 비 RFC 표준 HTTP 헤더입니다.

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF .

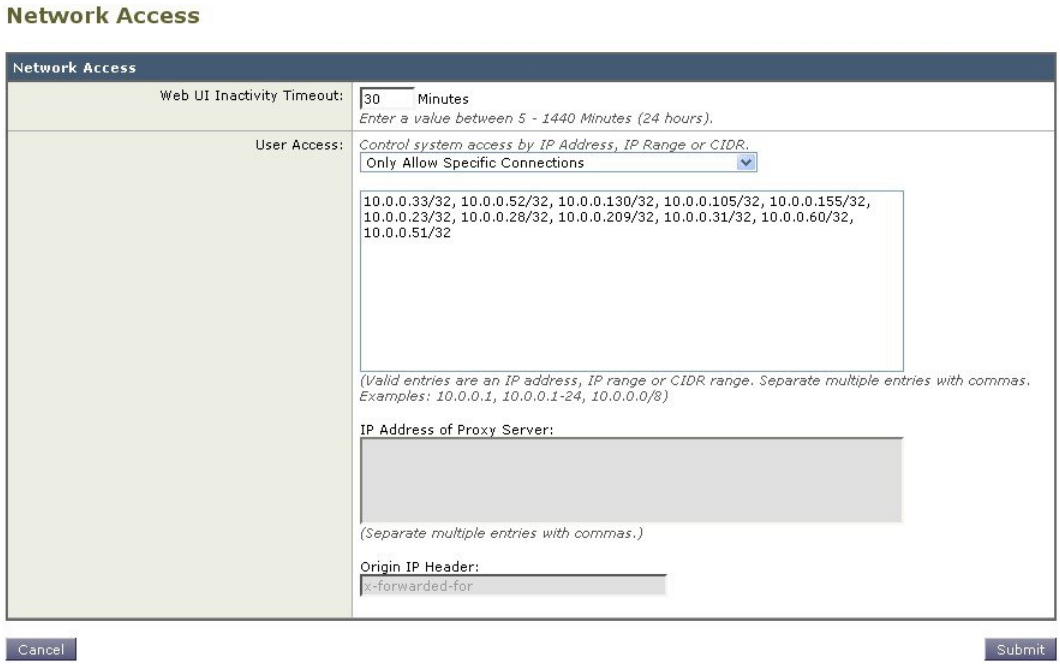
이 헤더의 값은 쉼표로 구분된 IP 주소 목록으로 맨 왼쪽의 주소는 원격 사용자 머신의 주소이며, 연결 요청을 전달한 일련의 프록시의 주소가 이어집니다. (헤더 이름은 구성할 수 있습니다.) Security Management Appliance는 헤더에 있는 원격 사용자의 IP 주소 및 연결하는 프록시의 IP 주소를 액세스 목록에 있는 허용되는 사용자 및 프록시 IP 주소와 비교합니다.

참고 AsyncOS는 x-forwarded-for 헤더에서 IPv4 주소만 지원합니다.

액세스 목록 만들기

GUI의 Network Access(네트워크 액세스) 페이지 또는 **adminaccessconfig > ipaccess** CLI 명령을 사용하여 네트워크 액세스 목록을 생성할 수 있습니다. 다음 그림에서는 Security Management Appliance에 직접 연결할 수 있는 사용자 IP 주소의 목록이 있는 Network Access(네트워크 액세스) 페이지를 보여줍니다.

그림 ***12:*** 네트워크 액세스 설정의 예



AsyncOS는 액세스 목록에 대해 다음 4가지 제어 모드를 제공합니다.

- 모두 허용. 이 모드에서는 어플라이언스에 대한 모든 연결을 허용합니다. 이는 초기 작동 모드입니다.
- 특정 연결만 허용. 이 모드에서는 사용자 IP 주소가 액세스 목록에 포함된 IP 주소, IP 범위 또는 CIDR 범위와 일치하는 경우 어플라이언스에 대한 사용자 연결을 허용합니다.
- 프록시를 통한 특정 연결만 허용. 이 모드에서는 다음 조건을 만족하는 경우 사용자는 역방향 프록시를 통해 어플라이언스에 연결할 수 있습니다.
  - 연결 프록시의 IP 주소가 액세스 목록의 IP Address of Proxy Server(프록시 서버의 IP 주소) 필드에 포함되어 있습니다.
  - 프록시의 연결 요청에 x-forwarded-header HTTP 헤더가 포함되어 있습니다.
  - x-forwarded-header의 값이 비어 있지 않습니다.

- 원격 사용자의 IP 주소가 x-forwarded-header에 포함되어 있고, 액세스 목록의 사용자에 대해 정의된 IP 주소, IP 범위 또는 CIDR 범위와 일치합니다.

- 직접 또는 프록시를 통한 특정 연결만 허용**.** 이 모드에서는 IP 주소가 액세스 목록에 포함된 IP 주소, IP 범위 또는 CIDR 범위와 일치하는 경우 사용자가 역방향 프록시를 통해 또는 직접 어플라이언스에 연결할 수 있습니다. 프록시를 통한 연결에 필요한 조건은 프록시를 통한 특정 연결만 허용 모드와 동일합니다.

다음 조건 중 하나가 참인 경우 변경사항을 제출하고 커밋한 후에는 어플라이언스에 대한 액세스를 잃게 됩니다.

- 특정 연결만 허용을 선택했지만 목록에 현재 머신의 IP 주소가 포함되어 있지 않음.
- **Only Allow Specific Connections Through Proxy(**프록시를 통한 특정 연결만 허용**)**를 선택한 상태에서, 어플라이언스에 현재 연결된 프록시의 IP 주소가 프록시 목록에 없고 Origin IP 헤더의 값이 허용되는 IP 주소의 목록에 없는 경우.
- **Only Allow Specific Connections Directly or Through Proxy(**직접 또는 프록시를 통한 특정 연결만 허용**)**를 선택한 상태에서
  - 원래 IP 헤더의 값이 허용되는 IP 주소 목록에 없음.

    또는

  - 원래 IP 헤더 값이 허용되는 IP 주소 목록에 없으며 어플라이언스에 연결된 프록시의 IP 주소가 허용되는 프록시 목록에 없음.

액세스 목록을 수정하지 않고 계속할 경우 AsyncOS는 변경사항이 커밋될 때 어플라이언스에서 해당 시스템 또는 프록시의 연결을 끊습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **System Administration(**시스템 관리**) > Network Access(**네트워크 액세스**)**를 선택합니다.

단계 **3** **Edit Settings(**설정 편집**)**를 클릭합니다.

단계 **4** 액세스 목록에 대한 제어 모드를 선택합니다.

단계 **5** 사용자가 어플라이언스에 연결하는 데 사용할 수 있는 IP 주소를 입력합니다.

IP 주소, IP 주소 범위 또는 CIDR 범위를 입력할 수 있습니다. 여러 항목을 구분하려면 쉼표를 사용합니다.

단계 **6** 프록시를 통한 연결이 허용되는 경우 다음 정보를 입력합니다.

- 어플라이언스에 연결할 수 있는 프록시의 IP 주소 여러 항목을 구분하려면 쉼표를 사용합니다.
- 프록시가 어플라이언스에 전송하는 원래 IP 헤더의 이름. 원격 사용자 머신 및 요청을 전달한 프록시 서버의 IP 주소를 포함합니다. 기본적으로 헤더의 이름은 x-forwarded-for입니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

웹 UI 세션 시간 초과 구성

비활성 때문에 AsyncOS에서 사용자를 로그아웃하기까지 Security Management Appliance의 웹 UI에서 사용자가 로그인을 유지할 수 있는 시간을 지정할 수 있습니다. 이 웹 UI 세션 시간 초과는 관리자를 비롯한 모든 사용자에게 적용되며, HTTP 및 HTTPS 세션에 모두 사용됩니다.

AsyncOS에서 사용자를 로그아웃하면 어플라이언스는 사용자의 웹 브라우저를 로그인 페이지로 리디렉션합니다.

참고 웹 UI 세션 시간 초과는 스팸 격리 세션에 적용되지 않습니다. 여기에는 30분의 시간 초과가 구성되어 있으며 변경 불가합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **System Administration(**시스템 관리**) > Network Access(**네트워크 액세스**)** 페이지를 사용합니다.

단계 **3** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **4** **Web UI Inactivity Timeout(**웹 **UI** 비활성 시간제한**)** 필드에 사용자가 로그아웃되기 전까지 비활성 상태를 유지할 수 있는 시간(분)을 입력합니다. 5~1440분의 시간제한 시간을 정의할 수 있습니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

CLI 세션 시간제한 구성

비활성 때문에 AsyncOS에서 사용자를 로그아웃하기까지 Security Management Appliance의 CLI에서 사용자가 로그인을 유지할 수 있는 시간을 지정할 수 있습니다. CLI 세션 시간제한이 적용되는 대상은 다음과 같습니다.

- 관리자를 포함한 모든 사용자
- SSH(Secure Shell), SCP 및 직접 직렬 연결을 사용한 연결만

참고 CLI 세션의 시간 초과 시점에 커밋되지 않은 구성 변경사항은 손실됩니다. 따라서 구성을 변경한 후 즉시 구성 변경사항을 커밋해야 합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **System Administration(**시스템 관리**) > Network Access(**네트워크 액세스**)** 페이지를 사용합니다.

단계 **3** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **4** **CLI Inactivity Timeout(**웹 **UI** 비활성 시간제한**)** 필드에 사용자가 로그아웃되기 전까지 비활성 상태를 유지할 수 있는 시간(분)을 입력합니다. 5~1440분의 시간제한 시간을 정의할 수 있습니다.

단계 **5** 변경사항을 제출하고 커밋합니다.

다음에 수행할 작업

CLI의 `adminaccessconfig` 명령을 사용하여 CLI 세션 시간 초과를 구성할 수도 있습니다. *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*를 참조하십시오.

메시지 추적 시 중요 정보의 액세스 제어

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Users(**사용자**)** 페이지로 이동합니다.

단계 **3** **Tracking Privileges(**추적 권한**)** 섹션에서 **Edit Settings(**설정 수정**)**을 클릭합니다.

단계 **4** 메시지 추적에서 중요 정보에 대한 액세스를 허용할 역할을 선택합니다.

메시지 추적 액세스 권한이 있는 맞춤 역할만 나열됩니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

이 설정이 적용되려면 Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) 아래에서 Centralized Email Message Tracking(중앙 집중식 이메일 메시지 추적) 기능이 활성화되어야 합니다.

관리자 사용자를 위한 메시지 표시

관리 사용자가 어플라이언스에 로그인할 때 보여줄 메시지를 표시할 수 있습니다.

메시지를 설정하거나 지우려면

단계 **1** 텍스트 파일을 가져올 경우 어플라이언스의 `/data/pub/configuration` 디렉터리에 저장합니다.

단계 **2** CLI(command-line interface)에 액세스합니다.

단계 **3** `adminaccessconfig > BANNER` 명령과 하위 명령을 사용합니다.

단계 **4** 변경사항을 커밋합니다.

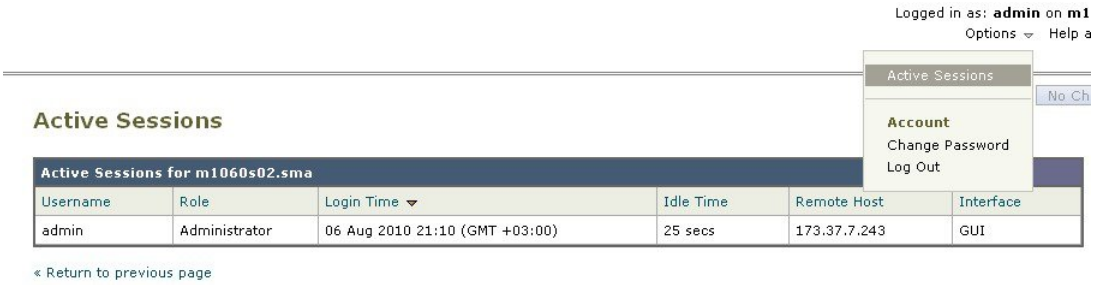
관리자 사용자 활동 보기

웹을 사용하여 활성 세션 보기

Security Management Appliance에서 모든 활성 세션 및 어플라이언스에 로그인한 사용자를 볼 수 있습니다.

창의 오른쪽 상단에서 **Options(옵션) > Active Sessions(활성 세션)**를 선택합니다.

그림 ***13: Active Sessions(활성 세션)*** 메뉴



Active Sessions(활성 세션) 페이지에서 사용자 이름, 사용자가 가지고 있는 역할, 사용자가 로그인한 시간, 유휴 시간, 사용자가 명령행에서 로그인했는지 GUI에서 로그인했는지 등을 볼 수 있습니다.

최근 로그인 시도 보기

웹 인터페이스, SSH 및/또는 FTP를 통해 최근 로그인 시도(실패 또는 성공)를 보려면

단계 **1** 로그인합니다.

단계 **2** 창 오른쪽 위에서 "Logged in as(로그인한 사용자)" 옆의 아이콘을 클릭합니다.

CLI를 통한 관리자 사용자 활동 보기

다음 명령은 어플라이언스에 대한 다중 사용자 액세스를 지원합니다.

- **who** 명령은 CLI 또는 웹 사용자 인터페이스를 통해 시스템에 로그인한 모든 사용자, 사용자의 역할, 로그인한 시간, 유휴 시간, 사용자가 로그인한 원격 호스트를 나열합니다.

- whoami 명령은 현재 로그인한 사용자의 사용자 이름 및 성명 그리고 사용자가 속한 그룹을 표시합니다.

```
mail3.example.com>
whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last 명령은 어플라이언스에 최근에 로그인한 사용자를 표시합니다. 원격 호스트의 IP 주소와 로그인, 로그아웃 및 총 시간도 표시됩니다.

```
mail3.example.com> last
Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

관리자 사용자 액세스 트러블슈팅

오류: 사용자에게 지정된 액세스 권한이 없음

문제

관리를 위임받은 사용자는 Security Management Appliance에 로그인할 수는 있으나 할당된 액세스 권한이 없다는 메시지를 보게 됩니다.

솔루션

이 사용자에게 할당한 맞춤형 사용자 역할에 권한을 할당했는지 확인합니다. Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Users(사용자)에서 지정된 사용자 역할을 확인하고 Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > User Roles(사용자 역할)로 이동하여 사용자 역할의 이름을 클릭하고 역할에 권한을 지정합니다.

보고 그룹에 따라 액세스 권한을 지정한 경우 Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > User Roles(사용자 역할) 페이지에서 이 사용자의 보고 그룹을 선택했어야 합니다. 그룹을 지정하려면 Delegated Administration(위임 관리) 테이블에서 해당 사용자 역할의 Email Reporting(이메일 보고) 열에 있는 **No groups selected**(선택된 그룹 없음) 링크를 클릭합니다.

사용자에게 활성 메뉴가 없음

문제

게시 권한을 부여받은 사용자가 로그인 시 활성 상태의 메뉴가 없습니다.

솔루션

하나 이상의 액세스 정책 또는 맞춤 URL 범주에 대한 액세스 권한을 부여했어야 합니다. 이 사용자 권한을 부여하여 어느 것도 수정하는 것을 원치 않는다면 Custom User Role(맞춤 사용자 역할) 페이지에서 어떤 정책에서도 사용되지 않는 맞춤 URL 범주를 생성하고 사용자에게 이 범주에 대한 권한을 부여합니다.

외부 인증 사용자에게 기본 설정 옵션 표시

문제

외부 인증 사용자에게 기본 설정 옵션이 나타납니다.

솔루션

Security Management Appliance에 직접 추가한 사용자가 외부 인증 데이터베이스에서 사용되지 않은 고유한 사용자 이름을 가지고 있는지 확인합니다.

15 장

일반 관리 작업

이 장에는 다음 섹션이 포함되어 있습니다.

관리 작업 수행

대부분의 시스템 관리 작업은 GUI(graphical user interface)의 System Administration(시스템 관리) 메뉴를 사용하여 수행할 수 있습니다. 그러나 일부 시스템 관리 기능은 CLI(command-line interface)에서만 사용 가능합니다.

또한 다음 장에 설명된 Monitor(모니터링) 메뉴에서 어플라이언스의 상태 모니터링 기능에 액세스합니다. 시스템 상태 모니터링, 369 페이지

참고 이 장에서 설명하는 몇 가지 기능 또는 명령은 라우팅 우선 순위에 영향을 미칠 수 있습니다. 자세한 내용은 IP 주소, 인터페이스 및 라우팅, 557 페이지를 참고하십시오.

Cisco Content Security Management Appliance 라이선싱

기능 키에 대한 작업

키는 어플라이언스의 일련 번호 및 활성화하는 기능과 관련 있습니다. 어떤 시스템의 키를 다른 시스템에 재사용할 수 없습니다.

이 섹션에서 설명하는 작업을 CLI에서 수행하려면 featurekey 명령을 사용합니다.

변경 후	수행해야 할 작업
• 어플라이언스의 모든 활성 기능 키 보기 • 활성화 보류 중인 기능 키 보기 • 발급된 새 키 검색 • 수동으로 기능 키 설치 • 기능 키 활성화	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Feature Keys(**기능 키**)**를 선택합니다. 새 기능 키를 수동으로 추가하려면 Feature Key(기능 키) 필드에 키를 붙여넣거나 입력하고 **Submit Key(**키 제출**)**를 클릭합니다. 키가 추가되지 않으면(예: 키가 정확하지 않음) 오류 메시지가 나타납니다. 그 밖의 경우에는 기능 키가 목록에 추가됩니다. 어플라이언스가 새 키가 발급되는 대로 자동으로 다운로드하고 설치하도록 구성된 경우 활성화 보류 중 목록은 항상 비어 있습니다.

변경 후	수행해야 할 작업
기능 키의 자동 다운로드 및 활성화를 활성화하거나 비활성화	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Feature Key Settings(**기능 키 설정**)**를 선택합니다. 기본적으로 어플라이언스는 정기적으로 새 키가 있는지 확인합니다.
만료된 기능 키 개신	Cisco 담당자에게 문의하십시오.

가상 어플라이언스 라이센싱 및 기능 키

라이선스 및 기능 키 만료 시 어플라이언스 동작에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html에 있는 *Cisco Content Security Virtual Appliance* 설치 설명서를 참조하십시오.

라이선스 정보를 보려면 CLI에서 show license 명령을 사용합니다.

CLI 명령으로 유지 보수 작업 수행

이 섹션에서 설명하는 작업 및 명령으로 Security Management Appliance에 대한 유지 보수 관련 작업을 수행할 수 있습니다. 여기서는 다음 작업 및 명령에 대해 설명합니다.

- shutdown
- reboot
- suspend
- suspendtransfers
- resume
- resumetransfers
- resetconfig
- version

Security Management Appliance 종료

Security Management Appliance를 종료하려면 다음 작업을 수행합니다.

- [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.
- **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Shutdown/Reboot(**종료/재부팅**)** 페이지로 이동합니다.

또는

- 명령행 프롬프트에서 `shutdown` 명령을 사용합니다.

어플라이언스를 종료하면 AsyncOS도 종료하며, 그러면 안전하게 어플라이언스의 전원을 끌 수 있습니다. 전달 대기열에 있는 메시지의 손실 없이 나중에 어플라이언스를 다시 시작할 수 있습니다. 어플라이언스 종료를 위한 지연 시간을 입력해야 합니다. 기본 지연은 30초입니다. AsyncOS에서는 이 지연 시간에 열려 있는 연결을 종료할 수 있게 합니다. 이 시간이 지나면 열려 있는 연결을 강제로 종료합니다.

Security Management Appliance 재부팅

Security Management Appliance를 재부팅하려면 GUI에서 System Administration(시스템 관리) 메뉴의 Shutdown/Reboot(종료/재부팅) 페이지를 사용하거나 CLI에서 reboot 명령을 사용합니다.

어플라이언스를 재부팅하면 AsyncOS도 재시작하며, 그러면 안전하게 어플라이언스의 전원을 껐다가 재부팅할 수 있습니다. 어플라이언스 종료를 위한 지연 시간을 입력해야 합니다. 기본 지연은 30초입니다. AsyncOS에서는 이 지연 시간에 열려 있는 연결을 종료할 수 있게 합니다. 이 시간이 지나면 열려 있는 연결을 강제로 종료합니다. 전달 대기열에 있는 메시지의 손실 없이 어플라이언스를 다시 시작할 수 있습니다.

Security Management Appliance 서비스 중단

시스템 유지 보수 등을 위해 어플라이언스를 오프라인 상태로 전환하려면 다음 명령 중 하나를 사용합니다.

Command(명령)	설명	지속성
`suspend`	• Email Security Appliance에서 Security Management Appliance로 보내는 격리된 메시지의 전송을 일시 중단합니다. • 격리 해제된 메시지의 전달을 일시 중단합니다. • 인바운드 이메일 연결이 허용되지 않습니다. • 아웃바운드 이메일 전송이 중단됩니다. • 로그 전송이 중단됩니다. • CLI에는 계속 액세스할 수 있음	재부팅 후 지속
`suspendtransfers`	관리 대상 ESA 및 WSA에서 CSMA에 보내는 보고 및 추적 데이터의 전송을 일시 중단합니다. 이 명령은 Email Security Appliance에서 보낸 격리된 메시지의 수신도 일시 중단합니다. 예비 어플라이언스를 기본 어플라이언스로 가동하기 위해 준비할 때 이 명령을 사용합니다.	재부팅 후 지속

이 명령을 사용할 경우 어플라이언스에 대한 지연 시간을 입력해야 합니다. 기본 지연은 30초입니다. AsyncOS에서는 이 지연 시간에 열려 있는 연결을 종료할 수 있게 합니다. 이 시간이 지나면 열려 있는 연결을 강제로 종료합니다. 열린 연결이 없을 경우 즉시 서비스가 중단됩니다.

suspend 또는 suspendtransfers 명령으로 일시 중단했던 서비스를 다시 활성화하려면 각각 resume 또는 resumetransfers 명령을 사용합니다.

관리 어플라이언스의 현재 온라인/일시 중단 상태를 확인하려면 웹 인터페이스에서 **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Shutdown/Reboot(**종료/재부팅**)**를 선택합니다.

다음 항목도 참고하십시오.

- Email Security Appliance용 문서 또는 온라인 도움말의 "이메일 전달 일시 중단", "이메일 전달 다시 시작", "수신 일시 중단", "수신 다시 시작"

CLI 예: suspend 및 suspendtransfers 명령

```
sma.example.com> suspend
Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
sma.example.com>
sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

일시 중단 상태에서 재개

resume 명령은 suspend 또는 suspenddel 명령으로 일시 중단되었던 어플라이언스를 정상 운영 상태로 되돌립니다.

resumetransfers 명령은 suspendtransfers 명령으로 일시 중단되었던 어플라이언스를 정상 운영 상태로 되돌립니다.

CLI 예: resume 및 resumetransfers 명령

```
sma.example.com> resume
Receiving resumed.
Mail delivery resumed.
sma.example.com>
sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.example.com>
```

공장 기본 구성으로 재설정

어플라이언스를 물리적으로 이전하거나 구성 문제 해결의 최후 수단 차원에서 공장 기본값으로 재설정하려는 경우가 있습니다.

⚠

주의 구성을 재설정하면 CLI 연결이 끊기고 어플라이언스 연결에 사용한 서비스(FTP, 텔넷, SSH, HTTP, HTTPS)가 비활성화되며 사용자 계정이 삭제됩니다.

변경 후	수행해야 할 작업
• 모든 구성을 공장 기본값으로 재설정 • 모든 보고 카운터 지우기 하지만 • 로그 파일 보존 • 격리된 메시지 보존	1. 재설정한 다음 기본 관리 사용자 계정 및 암호를 사용하여 어플라이언스와 연결 가능함을 확인합니다. 직렬 인터페이스를 사용하여 CLI에 또는 기본 설정을 사용하여 관리 포트에 연결합니다. 기본 설정의 어플라이언스 액세스에 대한 자세한 내용은 설정, 설치, 기본 구성, 17 페이지 장을 참조하십시오. 2. 어플라이언스에서 서비스를 일시 중단합니다. 3. **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Configuration File(구성 파일)**을 선택하고 **Reset(재설정)**을 클릭합니다. 참고 재설정하면 어플라이언스는 온라인 상태로 돌아갑니다. 재설정 전에 메일 전송이 일시 중단된 경우 재설정 후에 전달이 다시 시도됩니다.
• 모든 구성을 공장 기본값으로 재설정 • 모든 데이터 삭제	`diagnostic > reload` CLI 명령을 사용합니다. 주의 이 명령은 Cisco 라우터 또는 스위치에서 쓰이는 유사 명령과 같지 않습니다.

resetconfig 명령

```
mail3.example.com> suspend
Delay (seconds, minimum 30):
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com> resetconfig
Are you sure you want to reset all configuration values? [N]> Y
All settings have been restored to the factory default.
```

AsyncOS에 대한 버전 정보 표시

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > System Status(**시스템 상태**)**를 선택합니다.

단계 **3** 페이지 맨 아래로 스크롤하고 Version Information(버전 정보) 아래서 현재 설치된 AsyncOS의 버전을 확인합니다.

명령행 프롬프트에서 **version** 명령을 사용할 수도 있습니다.

원격 전원 제어 활성화

어플라이언스 섀시에 대한 전원을 원격으로 재설정하는 기능은 80- 및 90- 시리즈 하드웨어에서만 사용 가능합니다.

어플라이언스 전원을 원격으로 재설정하려면 이 섹션에 설명된 절차를 사용하여 미리 이 기능을 활성화 및 구성해야 합니다.

시작하기 전에

- RPC(전용 원격 전원 제어) 포트를 안전한 네트워크에 직접 연결합니다. 자세한 내용은 해당 모델의 하드웨어 설명서(설명서 , 571 페이지)를 참조하십시오.
- 어플라이언스에 원격에서 액세스 가능한지 확인합니다. 예를 들어 방화벽을 통해 필요한 포트를 엽니다.
- 이 기능을 사용하려면 전용 원격 전원 제어 인터페이스에 대한 고유한 IPv4 주소가 필요합니다. 이 인터페이스는 이 섹션에 설명된 절차를 통해서만 구성 가능하며, `ipconfig` 명령을 사용하여 구성할 수 없습니다.
- 어플라이언스 전원을 껐다가 켜려면 IPMI(Intelligent Platform Management Interface) 버전 2.0을 지원하는 디바이스를 관리할 수 있는 서드파티 툴이 필요합니다. 그러한 툴을 사용할 준비가 되었는지 확인합니다.
- CLI(Command Line Interface)에 액세스하는 방법에 대한 자세한 내용은 CLI 참조 가이드를 참조하십시오.

단계 **1** SSH, 텔넷 또는 직렬 콘솔 포트를 사용하여 명령줄 인터페이스에 액세스합니다.

단계 **2** 관리자 액세스 권한이 있는 계정을 사용하여 로그인합니다.

단계 **3** 다음과 같은 명령을 입력합니다.

```
remotepower

setup
```

단계 **4** 프롬프트를 따라 다음을 지정합니다.

- 이 기능의 전용 IP 주소와 넷마스크 및 게이트웨이.
- power-cycle 명령을 실행하는 데 필요한 사용자 이름과 암호.

이러한 자격 증명은 어플라이언스에 액세스하는 데 사용되는 다른 자격 증명과 다릅니다.

단계 **5** Commit을 입력하여 변경 사항을 저장합니다.

단계 **6** 구성을 테스트하여 어플라이언스 전원을 원격으로 관리할 수 있는지 확인합니다.

단계 **7** 입력한 자격 증명을 불확실한 미래에 사용할 수 있는지 확인합니다. 예를 들면 이 정보를 안전한 곳에 보관하고, 이 작업을 수행해야 하는 관리자가 필요한 자격 증명에 액세스할 수 있는지 확인합니다.

다음에 수행할 작업

어플라이언스 전원 원격 초기화 , 544 페이지

SNMP로 시스템 상태 모니터링

AsyncOS는 SNMP(Simple Network Management Protocol) v1, v2, v3을 통해 시스템 상태 모니터링을 지원합니다.

- SNMP를 활성화하고 구성하려면 CLI에서 `snmpconfig` 명령을 사용합니다.
- MIB는 http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html에서 사용할 수 있는 사용 가능한 최신 파일을 사용합니다.
- SNMPv3를 암호 인증 및 DES 암호화와 함께 사용해야 이 서비스를 활성화할 수 있습니다. SNMPv3에 대한 자세한 내용은 RFC 2571-2575를 참조하십시오. SNMP 시스템 상태 모니터링을 활성화하려면 8자 이상의 SNMPv3 패스프레이즈를 설정해야 합니다. SNMPv3 패스프레이즈를 처음 입력할 때는 확인을 위해 재입력해야 합니다. `snmpconfig` 명령은 다음에 이 명령을 실행할 때 이 패스프레이즈를 "기억"합니다.
- 연결 모니터링을 위해 SNMP를 설정할 경우

  connectivityFailure SNMP 트랩을 구성하면서 url-attribute를 입력할 경우 URL이 디렉터리 아니면 파일을 가리키는지 확인합니다.

  - 디렉터리라면 끝에 슬래시(/)를 추가합니다.
  - 파일이라면 끝에 슬래시(/)를 추가하지 않습니다.

- SNMP와 AsyncOS를 함께 사용하는 것에 대한 자세한 내용은 WSA 또는 ESA의 온라인 도움말을 참조하십시오.

예: snmpconfig 명령

```
sma.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP
Do you want to enable SNMP?
[Y]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: sma.example.com)
[1]>
Which port shall the SNMP daemon listen on interface "Management"?
[161]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2
Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests?
[N]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
```

```
[N]> Y
Do you want to disable any of these traps?
[Y]> n
Do you want to enable any of these traps?
[Y]> y
Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> SMA.Administrator@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: SMA.Administrator@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
sma.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
sma.example.com>
```

Security Management Appliance 데이터 백업

백업할 데이터

모든 데이터 또는 다음 데이터의 조합을 백업하도록 선택할 수 있습니다.

- 스팸 격리 - 메시지 및 메타데이터 포함
- 중앙 정책, 바이러스, 바이러스 격리 - 메시지 및 메타데이터 포함
- 이메일 추적(메시지 추적) - 메시지 및 메타데이터 포함
- 웹 추적
- 보고(이메일 및 웹)
- 허용 목록/차단 목록

데이터 전송이 끝나면 두 어플라이언스의 데이터가 똑같아집니다.

구성 및 로그는 이 프로세스에서 백업되지 않습니다. 이 항목을 백업하려면 기타 중요 백업 작업 , 446 페이지를 참조하십시오.

최초 백업 복사 이후의 각 백업에서는 지난 백업 이후에 생성된 정보만 복사합니다.

백업 제한 및 요구 사항

백업을 예약하기 전에 다음 제한 및 요구 사항을 해결해야 합니다.

제한 사항	요건
AsyncOS 버전	소스 및 타겟 Security Management Appliance의 AsyncOS 버전은 동일해야 합니다. 버전이 호환되지 않을 경우 백업을 예약하기 전에 동일한 릴리스로 어플라이언스를 업그레이드합니다.
네트워크의 타겟 어플라이언스	타겟 어플라이언스가 네트워크에 설정되어 있어야 합니다. 타겟 어플라이언스가 새 시스템일 경우 시스템 설정 마법사를 실행하여 필요한 정보를 입력합니다. 자세한 내용은 설정, 설치, 기본 구성, 17 페이지을 참조하십시오.
소스 어플라이언스와 타겟 어플라이언스의 통신	소스 및 타겟 Security Management Appliance는 SSH를 사용하여 통신할 수 있어야 합니다. 따라서 • 두 어플라이언스 모두 포트 22가 열려 있어야 합니다. 기본적으로 이 포트는 시스템 설정 마법사를 실행할 때 열립니다. • DNS(Domain Name Server)에서 A 레코드 및 PTR 레코드를 모두 사용하여 두 어플라이언스의 호스트 이름을 확인할 수 있어야 합니다.

제한 사항	요건
타겟 어플라이언스는 서비스 상태가 아니어야 합니다.	기본 어플라이언스에서만 관리 대상 ESA 및 WSA로부터 데이터를 가져와야 합니다. 이를 확인하려면 타겟 어플라이언스에서 관리 대상 어플라이언스의 데이터를 직접 가져올 수 없도록 설정 , 443 페이지를 참조하십시오. 또한 백업 어플라이언스에 예약된 구성 게시 작업이 있으면 모두 취소합니다.
어플라이언스 용량	타겟 어플라이언스의 디스크 공간 용량이 소스 어플라이언스의 용량과 같거나 더 커야 합니다. 타겟 어플라이언스의 각 데이터 유형(보고, 추적, 격리 등)에 할당된 디스크 공간이 소스 어플라이언스의 해당 할당량보다 적어서는 안 됩니다. 타겟 어플라이언스에 각 데이터 유형에 대해 백업되는 모든 데이터를 수용할 충분한 공간이 있을 경우 더 큰 소스에서 더 작은 타겟 Security Management Appliance로 백업하도록 예약할 수 있습니다. 소스 어플라이언스가 타겟 어플라이언스보다 클 경우 소스 어플라이언스에 할당된 공간을 줄여 더 작은 타겟 어플라이언스의 가용 공간에 맞춰야 합니다. 디스크 공간 할당 및 용량을 보고 관리하려면 디스크 공간 관리 , 487 페이지를 참조하십시오. 가상 어플라이언스의 디스크 용량에 대해서는 *Cisco Content Security Virtual Appliance* 설치 설명서를 참조하십시오.
다중, 동시 및 체인 백업	한 번에 하나의 백업 프로세스만 실행할 수 있습니다. 이전 백업이 완료되기 전에 실행하도록 예약된 백업이 있으면 이를 건너뛰며 경고를 보냅니다. Security Management Appliance의 데이터를 단일 Security Management Appliance에 백업할 수 있습니다. (한 백업에서 또 다른 백업으로의) 연쇄 백업은 지원되지 않습니다.

백업 소요 시간

전체 최초 백업의 경우 800GB 백업에 최대 10시간이 걸릴 수 있습니다. 매일 백업은 각각 최대 3시간이 걸릴 수 있습니다. 주간 및 월간 백업은 더 오래 걸릴 수 있습니다. 이 수치는 달라질 수 있습니다.

최초 백업 이후의 백업 프로세스에서는 지난 백업 이후에 변경된 파일만 전송합니다. 따라서 후속 백업의 소요 시간이 최초 백업보다 짧아야 합니다. 후속 백업에 필요한 시간은 축적된 데이터의 양, 변경된 파일 수, 지난 백업 이후 파일이 변경된 정도에 따라 달라집니다.

백업 중 서비스 가용성

Security Management Appliance를 백업하면 '소스' Security Management Appliance의 활성 데이터 세트를 '타겟' Security Management Appliance에 복사하되 원래 소스 어플라이언스에 줄 지장을 최소화합니다.

백업 프로세스의 단계 및 서비스 가용성에 미칠 영향은 다음과 같습니다.

- 1단계 - 소스 어플라이언스와 타겟 어플라이언스 간의 데이터 전송으로 시작합니다. 데이터 전송 과정에서 소스 어플라이언스의 서비스는 계속 실행되므로 데이터 수집도 계속될 수 있습니다. 그러나 타겟 어플라이언스에서는 서비스가 종료됩니다. 소스 어플라이언스에서 타겟 어플라이언스로의 데이터 전송이 완료되면 2단계가 시작합니다.
- 2단계 - 2단계가 시작하면 소스 어플라이언스의 서비스가 종료됩니다. 최초 종료 이후에 소스 어플라이언스와 타겟 어플라이언스 간의 데이터 전송 과정에서 수집된 다른 점이 타겟 어플라이언스에 복사되고 양쪽 어플라이언스의 서비스가 백업 시작 시점의 상태로 돌아갑니다. 그러면 소스 어플라이언스에서 최대 가동 시간이 유지되고 양쪽 모두 데이터 손실이 없습니다.

백업 중에 데이터 가용성 보고서가 작동하지 않을 수 있으며, 메시지 추적 결과를 볼 때 각 메시지에 대한 호스트 이름에 'unresolved' 레이블이 붙을 수 있습니다.

보고서를 예약하려 하는데 백업이 진행 중임을 잊은 경우 **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**)**를 선택하여 시스템 상태를 확인할 수 있습니다. 이 창에서는 시스템 백업이 진행 중임을 알리는 경고를 페이지 맨 위에서 볼 수 있습니다.

백업 프로세스 중단

참고 백업을 수행하는 동안 예기치 않게 소스 어플라이언스가 재부팅될 경우 타겟 어플라이언스는 이를 알지 못합니다. 타겟 어플라이언스에서 백업을 취소해야 합니다.

완료되지 않은 백업 프로세스가 중단된 경우 다음에 백업을 시도할 때 Security Management Appliance에서 중단된 지점부터 백업 프로세스를 시작할 수 있습니다.

진행 중인 백업을 취소하는 것은 권장되지 않습니다. 기존 데이터가 불완전해지며, 후속 백업이 완료될 때까지 특히 오류 메시지가 나타난 경우라면 사용할 수 없기 때문입니다. 진행 중인 백업을 취소해야 하는 경우 가급적 빨리 전체 백업을 실행함으로써 사용 가능한 최신 백업을 상시 확보해야 합니다.

타겟 어플라이언스에서 관리 대상 어플라이언스의 데이터를 직접 가져올 수 없도록 설정

단계 **1** 타겟 어플라이언스의 명령행 인터페이스에 액세스합니다. 자세한 내용은 CLI(Command Line Interface) 액세스, 24 페이지 섹션을 참조해 주십시오.

단계 **2** `suspendtransfers` 명령을 실행합니다.

단계 **3** 프롬프트가 다시 나타날 때까지 기다립니다.

단계 **4** `suspend` 명령을 실행합니다.

단계 **5** 프롬프트가 다시 나타날 때까지 기다립니다.

단계 **6** 타겟 어플라이언스의 명령행 인터페이스를 종료합니다.

백업 상태 알림 수신

백업이 완료될 때 그리고 문제가 생겼을 때 알림을 수신하려면 어플라이언스에서 System(시스템) 유형, Info(정보) 심각도의 알림을 보내도록 구성합니다. 경고 관리, 464 페이지를 참조하십시오.

단발 백업 또는 반복 백업 예약

미리 지정된 시간에 단발 백업 또는 반복 백업이 수행되도록 예약할 수 있습니다.

참고 원격 시스템에서 진행 중인 백업이 있을 경우 백업 프로세스가 시작하지 않습니다.

시작하기 전에

- 백업 제한 및 요구 사항 , 441 페이지의 항목을 처리합니다.

단계 **1** 관리자로 소스 어플라이언스의 CLI에 로그인합니다.

단계 **2** 명령 프롬프트에 **backupconfig**를 입력하고 **Enter**를 누릅니다.

단계 **3** 소스 어플라이언스와 타겟 어플라이언스 간의 연결 속도가 느리면 데이터 압축을 활성화합니다.

setup을 입력하고 **Y**를 입력합니다.

단계 **4** **Schedule**을 입력하고 **Enter**를 누릅니다.

단계 **5** Security Management Appliance의 IP 주소를 입력합니다.

단계 **6** 타겟 어플라이언스를 식별할 유의미한 이름(최대 20자)을 입력합니다.

단계 **7** 타겟 어플라이언스의 관리자 이름 및 암호를 입력합니다.

단계 **8** 어떤 데이터를 백업할지 묻는 프롬프트에 응답합니다.

단계 **9** 단발 백업을 예약하려면 **2**(Schedule a single backup)를 입력하고 **Enter**를 누릅니다.

단계 **10** 반복 백업을 예약하려면

a) 반복 백업 예약을 설정하기 위해 **1**을 입력하고 **Enter**를 누릅니다.

b) 정기 백업의 빈도를 선택하고 **Enter**를 누릅니다.

단계 **11** 백업을 시작할 날짜, 요일, 시간을 입력하고 **Enter**를 누릅니다.

단계 **12** 백업 프로세스의 이름을 입력합니다.

단계 **13** 백업이 성공적으로 예약되었음을 확인합니다. 명령 프롬프트에 **View**를 입력하고 **Enter**를 누릅니다.

단계 **14** 기타 중요 백업 작업 , 446 페이지도 참고하십시오.

즉시백업 시작

참고 타겟 시스템에서 진행 중인 백업이 있을 경우 백업 프로세스가 시작하지 않습니다.

시작하기 전에

백업 제한 및 요구 사항 , 441 페이지의 모든 요구 사항을 충족합니다.

단계 **1** 관리자로 소스 어플라이언스의 CLI에 로그인합니다.

단계 **2** 명령 프롬프트에 `backupconfig`를 입력하고 **Enter**를 누릅니다.

단계 **3** 소스 어플라이언스와 타겟 어플라이언스 간의 연결 속도가 느리면 데이터 압축을 활성화합니다.

setup을 입력하고 **Y**를 입력합니다.

단계 **4** **Schedule**을 입력하고 **Enter**를 누릅니다.

단계 **5** Security Management Appliance의 IP 주소를 입력합니다.

단계 **6** 타겟 어플라이언스를 식별할 유의미한 이름(최대 20자)을 입력합니다.

단계 **7** 타겟 어플라이언스의 관리자 이름 및 암호를 입력합니다.

단계 **8** 어떤 데이터를 백업할지 묻는 프롬프트에 응답합니다.

단계 **9** 지금 단발 백업을 시작하기 위해 **3**을 입력하고 **Enter**를 누릅니다.

단계 **10** 백업 작업을 위한 유의미한 이름을 입력합니다.

백업 프로세스가 몇 분 후 시작합니다.

단계 **11** (선택 사항) 백업 진행 상황을 보려면 명령행 프롬프트에서 **Status**를 입력합니다.

단계 **12** 기타 중요 백업 작업 , 446 페이지도 참고하십시오.

백업 상태 확인

단계 **1** 관리자로 기본 어플라이언스의 CLI에 로그인합니다.

단계 **2** 명령 프롬프트에 **backupconfig**를 입력하고 **Enter**를 누릅니다.

확인할 상태	수행해야 할 작업
예약된 백업	View 작업을 선택합니다.

확인할 상태	수행해야 할 작업
진행 중인 백업	Status 작업을 선택합니다. 알림을 구성한 경우 이메일을 확인하거나 최근 알림 보기 , 466 페이지 섹션을 참조하십시오.

다음에 수행할 작업

관련 주제

로그 파일의 백업 정보 , 446 페이지

로그 파일의 백업 정보

백업 로그는 백업 프로세스를 처음부터 끝까지 기록합니다.

백업 예약에 대한 정보는 SMA 로그에 있습니다.

관련 주제

- 백업 상태 확인 , 445 페이지

기타 중요 백업 작업

여기서 설명한 백업 프로세스에서 백업하지 않는 항목이 사라지는 것을 방지하고 어플라이언스 오류에 대비하여 대체 Security Management Appliance를 신속하게 설정하기 위해 다음 작업을 수행할 수 있습니다.

- 기본 Security Management Appliance에서 설정을 저장하려면 구성 설정 저장 및 가져오기 , 479 페이지 섹션을 참조하십시오. 기본 Security Management Appliance가 아닌 안전한 곳에 구성 파일을 저장합니다.
- 구성 마스터를 채우는 데 사용한 Web Security Appliance 구성 파일이 있으면 저장합니다.
- Security Management Appliance의 로그 파일을 대체 위치에 저장하려면 로그 서브스크립션, 527 페이지 섹션을 참조하십시오.

또한 백업 로그에 대한 로그 서브스크립션을 설정할 수 있습니다. GUI에서 로그 서브스크립션 만들기, 529 페이지를 참조하십시오.

백업 어플라이언스를 기본 어플라이언스로 지정

어플라이언스 하드웨어를 업그레이드하는 경우 또는 다른 이유로 어플라이언스를 바꿔야 하는 경우 다음 절차를 사용합니다.

시작하기 전에

Security Management Appliance 데이터 백업 , 440 페이지의 정보를 검토합니다.

단계 **1** 기존/기본/소스 어플라이언스에 있는 구성 파일의 복사본을 새 어플라이언스에서 접근 가능한 위치에 저장합니다. 구성 설정 저장 및 가져오기 , 479 페이지를 참조하십시오.

단계 **2** 신규/백업/타겟 어플라이언스에서 시스템 설정 마법사를 실행합니다.

단계 **3** 백업 제한 및 요구 사항 , 441 페이지의 요구 사항을 충족합니다.

단계 **4** 기존/기본/소스 어플라이언스에서 백업을 실행합니다. 즉시백업 시작, 445 페이지의 지침을 참조하십시오.

단계 **5** 백업이 완료될 때까지 기다립니다.

단계 **6** 기존/기본/소스 어플라이언스에서 suspendtransfers 및 suspend 명령을 실행합니다.

단계 **7** 2번째 백업을 실행하여 기존/기본/소스의 최신 데이터를 신규/백업/타겟 어플라이언스에 전송합니다.

단계 **8** 신규/백업/타겟 어플라이언스에 구성 파일을 가져옵니다.

단계 **9** 신규/백업/타겟 어플라이언스에서 resumetransfers 및 resume 명령을 실행합니다.

기존/원본 기본/소스 어플라이언스에서 이 명령을 실행해서는 안 됩니다.

단계 **10** 신규/백업/타겟 어플라이언스와 관리 대상 ESA 및 WSA 간의 연결을 설정합니다.

단계 **11**
a) [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.
b) **Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)**를 선택합니다.
c) 어플라이언스 이름을 클릭합니다.
d) **Establish Connection(**연결 설정**)** 버튼을 클릭합니다.
e) **Test Connection(**테스트 연결**)**을 클릭합니다.
f) 어플라이언스 목록으로 돌아갑니다.
g) 관리 대상 어플라이언스마다 반복합니다.

단계 **12** 이제 신규/타겟 어플라이언스가 기본 어플라이언스로 작동하고 있음을 확인합니다.

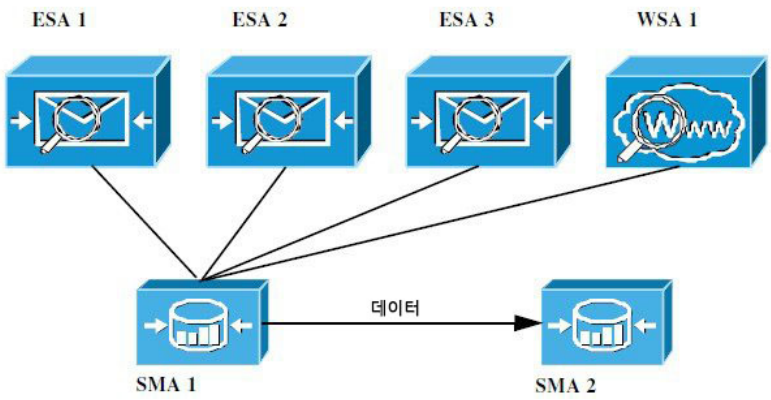
Management Appliance(관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > System Status(**시스템 상태**)**를 선택하고 데이터 전송 상태를 확인합니다.

Security Management Appliance의 재해 복구

Security Management Appliance에서 예기치 않게 오류가 발생할 경우 다음 절차에 따라 보안 관리 서비스를 복원하고 에 따라 정기적으로 저장하는 백업 데이터도 복원합니다Security Management Appliance 데이터 백업 , 440 페이지.

일반 어플라이언스 구성은 다음 그림에 표시된 것처럼 보일 수 있습니다.

그림 *14:* 재해 복구*:* 일반 환경



이 환경에서 SMA 1이 ESA 1-3 및 WSA 1로부터 데이터를 수신하는 기본 Security Management Appliance입니다. SMA 2는 SMA 1로부터 백업 데이터를 수신하는 백업 Security Management Appliance입니다.

오류가 발생하면 SMA 2를 기본 Security Management Appliance로 구성해야 합니다.

SMA 2를 새로운 기본 Security Management Appliance로 구성하고 서비스를 복원하려면 다음과 같은 작업을 수행해야 합니다.

프로시저

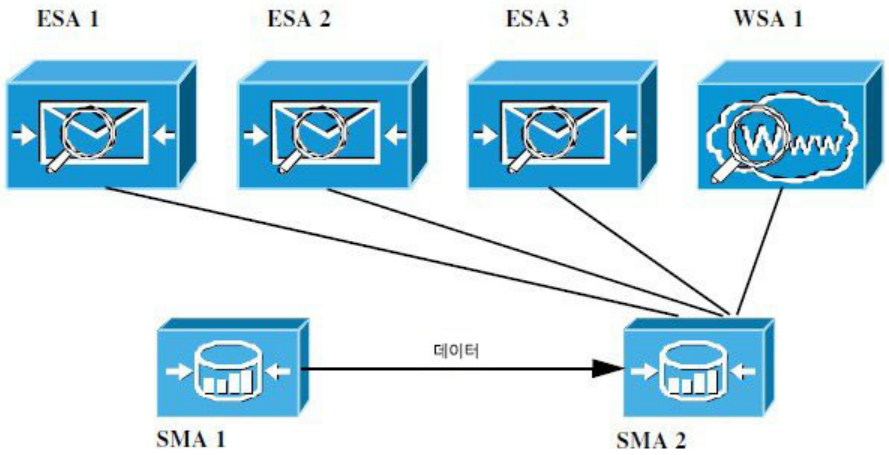
	명령 또는 동작	목적
단계 **1**	중앙 집중식 정책, 바이러스 및 보안 침해 격리를 사용 중인 경우 • 각 Email Security Appliance에서 중앙 집중식 격리를 비활성화합니다.	Email Security Appliance 설명서에서 중앙 집중식 정책, 바이러스, 보안 침해 격리를 비활성화하는 방법에 대한 지침을 참조하십시오. 그러면 나중에 새 Security Management Appliance를 마이그레이션할 각 Email Security Appliance에서 로컬 격리가 생성됩니다.
단계 **2**	기본 Security Management Appliance(SMA1)에서 저장한 구성 파일을 백업 Security Management Appliance(SMA2)에 로드합니다.	구성 파일 로드, 481 페이지를 참조하십시오.
단계 **3**	오류가 발생한 SMA 1의 IP 주소를 재생성하여 SMA 2의 IP 주소가 되게 합니다.	1. SMA 2에서 **Network(**네트워크**) > IP Interfaces(IP** 인터페이스**) > Add IP Interfaces(IP** 인터페이스 추가**)**를 선택합니다. 2. **Add IP Interfaces(IP** 인터페이스 추가**)** 페이지에서 오류가 발생한 SMA 1의 모든 관련 IP 인터페이스 정보를 텍스트 필드에 입력하여 SMA 2에서 인터페이스를 생성합니다. IP 인터페이스 추가에 대한 자세한 내용은 IP 인터페이스 구성, 548 페이지를 참조하십시오.

	명령 또는 동작	목적
단계 **4**	변경사항을 제출 및 커밋합니다.	
단계 **5**	새 Security Management Appliance(SMA 2)에서 해당되는 모든 중앙 집중식 서비스를 활성화합니다.	Security Management Appliance의 서비스 구성, 30 페이지를 참조하십시오.
단계 **6**	새 Security Management Appliance(SMA 2)에 모든 어플라이언스를 추가합니다. • 어플라이언스와 연결을 설정하고 연결을 테스트하는 방법으로 각 어플라이언스가 활성화되었고 제대로 작동하고 있는지 확인합니다.	관리 대상 어플라이언스 추가 정보, 29 페이지를 참조하십시오.
단계 **7**	중앙 집중식 정책, 바이러스, 보안 침해 격리를 사용하는 경우 새 Security Management Appliance에서 격리 마이그레이션을 구성하고 각 Email Security Appliance에서 마이그레이션을 활성화 및 구성합니다.	정책, 바이러스 및 Outbreak 격리 중앙 집중화 , 313 페이지를 참조하십시오.
단계 **8**	필요하다면 추가 데이터를 복원합니다.	기타 중요 백업 작업 , 446 페이지를 참조하십시오.

다음에 수행할 작업

이 프로세스가 끝나면 SMA 2는 기본 Security Management Appliance가 됩니다. 다음 그림에서 보듯이 ESA 1-3 및 WSA 1의 모든 데이터가 이제 SMA 2에 전송됩니다.

그림 ***15:*** 재해 복구*:* 최종 결과



어플라이언스 하드웨어 업그레이드

백업 어플라이언스를 기본 어플라이언스로 지정 , 446 페이지를 참조하십시오.

AsyncOS 업그레이드

업그레이드를 위한 배치 명령

업그레이드 절차의 배치 명령은 다음 위치의 AsyncOS for Email용 CLI 참조 설명서에 설명되어 있습니다. http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

업그레이드 및 업데이트를 위한 네트워크 요구 사항 확인

Cisco CSA(Content Security Appliance)의 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 AsyncOS 업그레이드를 위한 고정 위치를 구성해야 할 수 있습니다. 방화벽 설정상 업그레이드를 위한 고정 IP가 필요할 경우 Cisco 고객 지원에 문의하여 필요한 URL 주소를 얻으십시오.

참고 포트 22, 25, 80, 4766 등을 통해 upgrades.cisco.com에서 레거시 업그레이드를 다운로드하도록 허용하는 기존 방화벽 규칙이 있는 경우 이러한 규칙을 제거하고 수정된 방화벽 규칙으로 교체해야 합니다.

업그레이드 방법 선택: 원격과 스트리밍

Cisco는 어플라이언스의 AsyncOS를 업그레이드하도록 2가지 방법(또는 '소스')을 제공합니다.

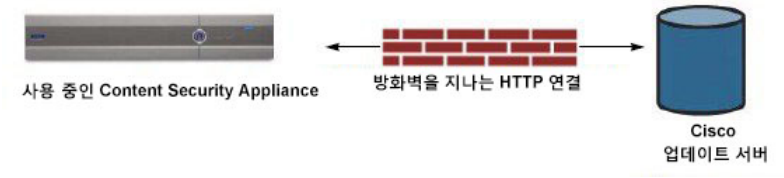
- 스트리밍 업그레이드 - 각 어플라이언스는 HTTP를 통해 Cisco 콘텐츠 보안 업데이트 서버로부터 직접 AsyncOS 업그레이드를 다운로드합니다.
- 원격 업그레이드 - Cisco에서 업그레이드 이미지를 한 번만 다운로드한 다음 어플라이언스에 제공합니다. 그러면 어플라이언스는 네트워크 내의 서버로부터 AsyncOS 업그레이드를 다운로드하는 것입니다.

업그레이드 및 서비스 업데이트 설정 구성, 453 페이지에서 업그레이드 방법을 구성합니다. CLI에서 **updateconfig** 명령을 사용할 수도 있습니다.

스트리밍 업그레이드 개요

스트리밍 업그레이드에서는 각 Cisco Content Security Appliance가 Cisco 콘텐츠 보안 업데이트 서버에 직접 연결하여 업그레이드를 검색하고 다운로드합니다.

그림 ***16:*** 스트리밍 업데이트 방법

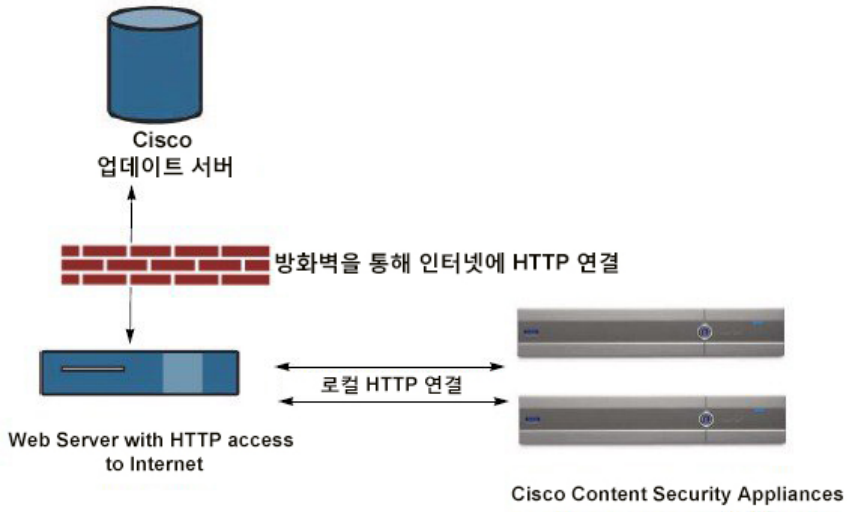


이 방법에서는 어플라이언스에서 직접 네트워크를 통해 Cisco 콘텐츠 보안 업데이트 서버에 연결합니다.

원격 업그레이드 개요

Cisco 콘텐츠 업데이트 서버에서 직접 업데이트를 얻는 방법(스트리밍 업그레이드) 대신 AsyncOS 업데이트를 자체 네트워크 로컬에 다운로드하고 호스팅할 수도 있습니다(로컬 업그레이드). 이 기능을 사용하면 암호화된 업데이트 이미지가 HTTP를 통해 네트워크의 인터넷 액세스 가능한 서버로 다운로드됩니다. 업데이트 이미지를 다운로드하려는 경우 AsyncOS 이미지를 Security Management Appliance에 호스팅하도록 내부 HTTP 서버("업데이트 관리자")를 구성할 수 있습니다.

그림 ***17:*** 원격 업데이트 방법



기본 프로세스는 다음과 같습니다.

단계 **1** 원격 업그레이드를 위한 하드웨어 및 소프트웨어 요구 사항, 452 페이지 및 원격 업그레이드 이미지 호스팅, 452 페이지를 참조하십시오.

단계 **2** 업그레이드 파일을 검색하여 제공하도록 로컬 서버를 구성합니다.

단계 **3** 업그레이드 파일을 다운로드합니다.

단계 **4** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **5** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Update Settings(**업데이트 설정**)**를 선택합니다.

이 페이지에서 어플라이언스가 로컬 서버를 사용하도록 구성합니다.

단계 **6** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > System Upgrade(**시스템 업그레이드**)**를 선택합니다.

단계 **7** **Available Upgrades(**사용 가능한 업그레이드**)**를 클릭합니다.

참고 명령줄 프롬프트에서 **updateconfig** 명령을 실행한 다음 **upgrade** 명령도 실행할 수 있습니다.

자세한 내용은 AsyncOS 업그레이드, 450 페이지를 참조하십시오.

원격 업그레이드를 위한 하드웨어 및 소프트웨어 요구 사항

AsyncOS 업그레이드 파일을 다운로드하려면 다음 항목이 지원되는 내부 네트워크의 시스템이 필요합니다.

- Cisco CSA 업데이트 서버에 대한 인터넷 액세스
- 웹 브라우저.

참고 이 릴리스에서 이 주소에 대한 HTTP 액세스를 허용하도록 방화벽 설정을 구성해야 하는 경우, 특정 IP 주소가 아니라 DNS 이름을 사용하여 구성해야 합니다.

AsyncOS 업데이트 파일을 호스팅하려면 다음이 지원되는 내부 네트워크의 서버가 필요합니다.

- 다음과 같은 웹 서버(예: Microsoft IIS(Internet Information Services) 또는 Apache 오픈 소스 서버):
  - 24자가 넘는 디렉터리 또는 파일 이름의 표시 지원
  - 디렉터리 찾아보기 가능
  - 익명(인증 없음) 또는 기본("단순") 인증을 위해 구성됨
  - 각 AsyncOS 업데이트 이미지용 최소 350MB 빈 디스크 공간 포함

원격 업그레이드 이미지 호스팅

로컬 서버를 설정한 후 **http://updates.ironport.com/fetch_manifest.html**로 이동하여 업그레이드 이미지의 ZIP 파일을 다운로드합니다. 이미지를 다운로드하려면 Cisco Content Security Appliance 일련 번호 및 버전 번호를 입력합니다. 그러면 사용 가능한 업그레이드 목록이 표시됩니다. 업그레이드 이미지의 ZIp 파일을 다운로드하기 위해 업그레이드 버전을 클릭합니다. AsyncOS 업그레이드를 위한 업그레이드 이미지를 사용하려면 Edit Update Settings(업데이트 설정 수정) 페이지에 로컬 서버의 기본 URL을 입력합니다. 또는 CLI에서 updateconfig를 사용합니다.

네트워크에서 Cisco Content Security Appliance에 대해 사용 가능한 업그레이드를 http://updates.ironport.com/fetch_manifest.html에서 선택한 버전으로 제한하는 로컬 서버 XML 파일도 호스팅할 수 있습니다. Cisco Content Security Appliance는 여전히 Cisco 서버에서 업그레이드를 다운로드합니다. 로컬 서버에서 업그레이드 목록을 호스팅하려는 경우 ZIP 파일을 다운로드하고 asyncos/phoebe-my-upgrade.xml 파일을 로컬 서버의 루트 디렉터리에 풉니다. AsyncOS 업그레이드를 위한 업그레이드 목록을 사용하려면 Edit Update Settings(업데이트 설정 수정) 페이지에 XML 파일의 전체 URL을 입력합니다. 또는 CLI에서 updateconfig를 사용합니다.

원격 업그레이드에 대한 자세한 내용은 기술 자료(기술 자료(TechNotes) , 573 페이지)를 참조하거나 지원 업체에 문의하십시오.

원격 업그레이드 방법의 중요한 차이점

로컬 서버에서 AsyncOS를 업그레이드할 경우 스트리밍 업그레이드 방법과의 차이점을 확인합니다.

- 다운로드가 진행되는 동안 즉시 업그레이드가 설치됩니다.
- 업그레이드 프로시스 시작 시 10초 동안 배너가 표시됩니다. 이 배너가 표시되어 있을 때 Ctrl-C를 입력하면 다운로드가 시작되기 전 업그레이드 프로세스를 종료할 수 있습니다.

업그레이드 및 서비스 업데이트 설정 구성

Cisco Content Security Appliance에서 보안 서비스 업데이트(예: 표준 시간대 규칙) 및 AsyncOS 업그레이드를 다운로드하는 방법을 구성할 수 있습니다. 예를 들어 Cisco 서버 아니면 이미지를 확보한 로컬 서버로부터 동적으로 업그레이드 및 업데이트를 다운로드할지 선택하거나 업데이트 간격을 구성하거나 자동 업데이트를 비활성화할 수 있습니다.

AsyncOS는 정기적으로 업데이트 서버를 쿼리하여 신규 AsyncOS 업그레이드를 제외하고 모든 보안 서비스 구성 요소에 대한 새로운 업데이트가 있는지 확인합니다. AsyncOS를 업그레이드하려면 수동으로 AsyncOS에서 사용 가능 업그레이드를 쿼리해야 합니다.

GUI에서 업그레이드 및 업데이트 설정을 구성하거나(다음 두 섹션 참조) CLI에서 updateconfig 명령을 사용할 수 있습니다.

업그레이드 알림 설정도 구성할 수 있습니다.

업그레이드 및 업데이트 설정

다음 표에서는 구성 가능한 업데이트 및 업그레이드 설정에 대해 설명합니다.

표 **84:** 보안 서비스 설정 업데이트

설정	설명
Update Servers(업데이트 서버)(이미지)	AsyncOS 업그레이드 및 서비스 업데이트 소프트웨어 이미지(표준 시간대 규칙, 기능 키 업데이트 등)를 Cisco 서버에서 아니면 로컬 웹 서버에서 다운로드할지 선택합니다. 기본 설정은 업그레이드 및 업데이트 모두 Cisco 서버입니다. 다음과 같은 경우에 로컬 웹 서버를 사용할 수 있습니다. • 고정 주소로부터 어플라이언스에 이미지를 다운로드해야 합니다. 엄격한 방화벽 정책이 있는 환경을 위한 고정 업그레이드 및 업데이트 서버 설정 , 455 페이지를 참조하십시오. • 사용자의 편의에 따라 어플라이언스에 AsyncOS 업그레이드 이미지를 다운로드하려 합니다. 여전히 Cisco 업데이트 서버에서 동적으로 서비스 업데이트 이미지를 다운로드할 수도 있습니다. 로컬 업데이트 서버를 선택하는 경우 업그레이드와 업데이트를 다운로드하는 데 사용되는 서버에 대한 기본 URL 및 포트 번호를 입력합니다. 서버에 인증이 필요한 경우 유효한 사용자 이름과 암호를 입력할 수도 있습니다. 자세한 내용은 업그레이드 방법 선택: 원격과 스트리밍 , 450 페이지 및 원격 업그레이드 개요, 451 페이지를 참조하십시오.
업데이트 서버(목록)	사용 가능한 업그레이드 및 서비스 업데이트 목록을 Cisco 서버에서 다운로드할지 아니면 로컬 웹 서버에서 다운로드할지 선택합니다. 업그레이드 및 업데이트에 대한 기본값은 Cisco 서버입니다. 업그레이드 및 업데이트에 대해 서로 다른 설정을 선택할 수도 있습니다. 해당되는 경우 엄격한 방화벽 정책이 있는 환경을 위한 고정 업그레이드 및 업데이트 서버 설정 , 455 페이지를 참조하십시오. 로컬 업데이트 서버를 선택하는 경우, 파일 이름과 서버의 포트 번호를 포함하여 각 목록에 대한 매니페스트 XML 파일의 전체 경로를 입력합니다. 포트 필드를 비워두면 AsyncOS에서는 포트 80을 사용합니다. 서버에 인증이 필요한 경우 유효한 사용자 이름과 암호를 입력할 수도 있습니다. 자세한 내용은 업그레이드 방법 선택: 원격과 스트리밍 , 450 페이지 및 원격 업그레이드 개요, 451 페이지를 참조하십시오.
Automatic Updates(자동 업데이트)	표준 시간대 규칙에 대한 자동 업데이트를 활성화할지 여부를 선택합니다. 활성화한 경우 업데이트 확인 사이의 대기하는 시간을 입력합니다. 분에는 **m**, 시간에는 **h**, 일에는 **d**를 끝에 추가합니다.
인터페이스	표준 시간대 규칙 및 AsyncOS 업그레이드를 위해 업데이트 서버에 연결할 때 사용할 네트워크 인터페이스를 선택합니다. 사용 가능한 프록시 데이터 인터페이스가 표시됩니다. 기본적으로 어플라이언스는 사용할 인터페이스를 선택합니다.

설정	설명
HTTP 프록시 서버**:**	업스트림 HTTP 프록시 서버가 있고 인증을 요구하는 경우 여기에 서버 정보와 사용자 이름 및 암호를 입력합니다. 프록시 서버를 지정할 경우 GUI에 나열된 서비스 액세스 및 업데이트에 사용됩니다. 이 프록시 서버는 클라우드에서 파일 분석 보고서 세부사항을 얻는 데에도 사용됩니다. 파일 분석 보고서 요구 사항 정보 , 94 페이지(웹 보고서) 또는 파일 분석 보고서 요구 사항 정보 , 199 페이지(이메일 보고서)도 참조하십시오.
HTTPS Proxy Server((HTTPS 프록시 서버**)**	업스트림 HTTPS 프록시 서버가 있고 인증을 요구하는 경우 여기에 서버 정보와 사용자 이름 및 암호를 입력합니다. 프록시 서버를 지정할 경우 GUI에 나열된 서비스 액세스 및 업데이트에 사용됩니다. 이 프록시 서버는 클라우드에서 파일 분석 보고서 세부 정보를 얻는 데에도 사용됩니다. 파일 분석 보고서 요구 사항 정보 , 94 페이지(웹 보고서) 또는 파일 분석 보고서 요구 사항 정보 , 199 페이지(이메일 보고서)도 참조하십시오.

엄격한 방화벽 정책이 있는 환경을 위한 고정 업그레이드 및 업데이트 서버 설정

AsyncOS 업데이트 서버는 동적 IP 주소를 사용합니다. 환경에 엄격한 방화벽 정책이 있어 고정 IP 주소가 필요할 경우 업데이트 설정 페이지에서 다음 설정을 사용합니다.

그림 ***18:*** 업데이트 서버***(***이미지***)*** 설정을 위한 고정 ***URL***

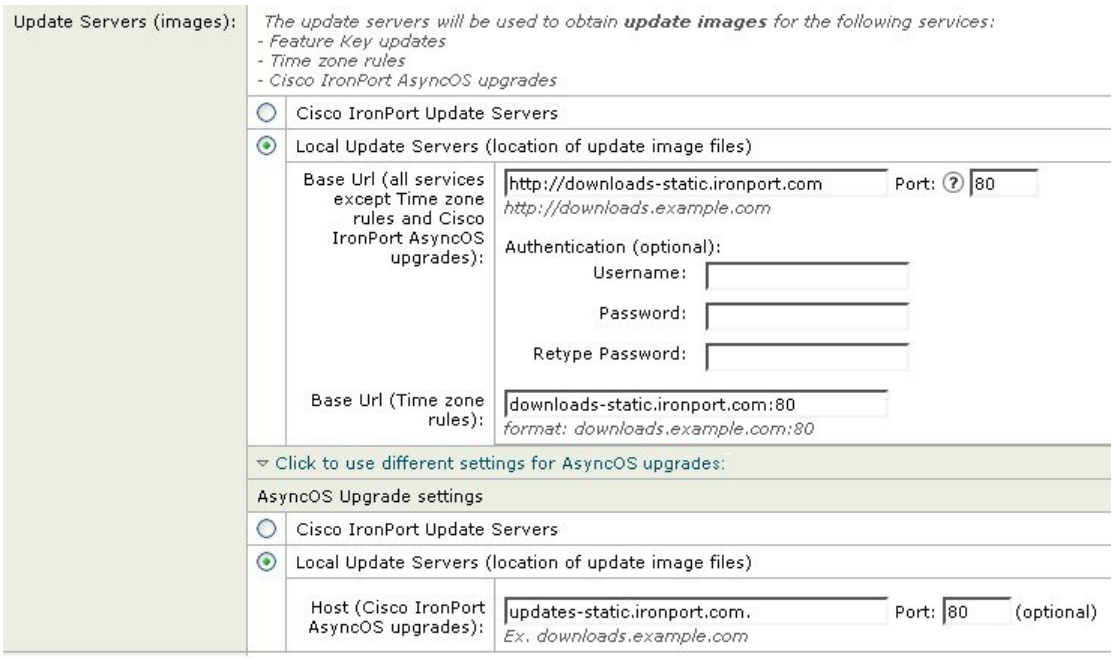


그림 ***19:*** 업데이트 서버*(*목록*)* 설정을 위한 고정 ***URL***

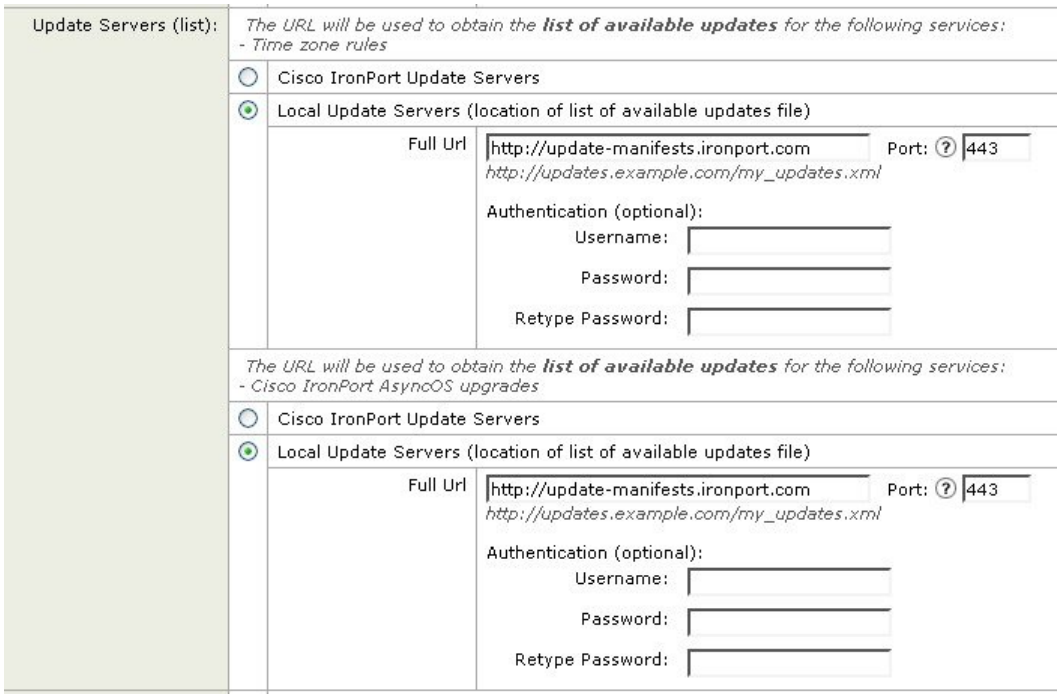


표 ***85:*** 엄격한 방화벽 정책이 있는 환경을 위한 고정 주소

섹션	설정	고정 **URL/IP** 주소 및 포트
업데이트 서버(이미지):	기본 URL(표준 시간대 규칙 및 AsyncOS 업그레이드를 제외한 모든 서비스)	http://downloads-static.ironport.com 204.15.82.8 포트 80
	기본 URL(표준 시간대 규칙)	downloads-static.ironport.com 204.15.82.8 포트 80
	호스트(AsyncOS 업그레이드)	updates-static.ironport.com 208.90.58.25 포트 80

섹션	설정	고정 URL/IP 주소 및 포트
업데이트 서버(목록):	물리적 하드웨어 어플라이언스의 업데이트: 전체 URL	update-manifests.ironport.com 208.90.58.5 포트 443
	가상 어플라이언스의 업데이트의 경우: Full URL(전체 URL)	update-manifests.sco.cisco.com 포트 443
	업그레이드의 경우: Full URL(전체 URL)	update-manifests.ironport.com 208.90.58.5 포트 443

중요 CLI에서 `updateconfig` 명령의 `dynamichost` 하위 명령을 사용하여 `update-manifests` URL 및 포트 번호를 구성해야 합니다. 이렇게 하면 서비스 업데이트가 검증됩니다.

GUI에서 업데이트 및 업그레이드 설정 구성

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Update Settings(**업데이트 설정**)**를 선택합니다.

단계 **3** **Edit Update Settings(**업데이트 설정 수정**)**를 클릭합니다.

업그레이드 및 업데이트 설정, 453 페이지의 설명에 따라 이 절차의 설정을 구성합니다.

단계 **4** **Update Servers (images)(**업데이트 서버 **-** 이미지**)** 섹션에서 어떤 서버로부터 업데이트용 이미지를 다운로드할지 지정합니다.

단계 **5** 어떤 서버로부터 AsyncOS 업그레이드용 이미지를 다운로드할지 지정합니다.

a) 동일한 섹션의 맨 아래서 **Click to use different settings for AsyncOS upgrades(AsyncOS** 업그레이드에 다른 설정을 사용하려면 클릭**)** 링크를 클릭합니다.

b) AsyncOS 업그레이드용 이미지를 다운로드하기 위한 서버 설정을 지정합니다.

단계 **6** **Update Servers (list)(**업데이트 서버 **-** 목록**)** 섹션에서 사용 가능 업데이트 및 AsyncOS 업그레이드의 목록을 얻기 위한 서버를 지정합니다.

맨 위의 하위 섹션이 업데이트에 적용됩니다. 맨 아래의 하위 섹션은 업그레이드에 적용됩니다.

단계 **7** 표준 시간대 규칙 및 인터페이스에 대한 설정을 지정합니다.

단계 **8** (선택 사항) 프록시 서버에 대한 설정을 지정합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

단계 **10** 기대한 결과임을 확인합니다.

아직 업데이트 설정 페이지가 나타나지 않을 경우 **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Update Settings(**업데이트 설정**)**를 선택합니다.

일부 URL은 서버 URL에 "asyncos" 디렉터리가 붙을 수 있습니다. 이 차이는 무시해도 됩니다.

업그레이드 알림

기본적으로 관리자 및 기술자 권한이 있는 사용자는 어플라이언스에서 AsyncOS 업그레이드를 사용할 수 있을 때 웹 인터페이스 상단에 표시되는 알림을 볼 수 있습니다.

변경 후	수행해야 할 작업
최신 업그레이드에 대한 자세한 정보 보기	업그레이드 알림 위에 마우스를 올려놓습니다.
사용 가능한 업그레이드 목록 보기	알림에서 아래쪽 화살표를 클릭합니다.
현재 알림 해제. 새 업그레이드를 사용할 수 있을 때까지 어플라이언스에 또 다른 알림이 표시되지 않습니다.	아래쪽 화살표를 클릭하고 **Clear the notification(**알림 지우기**)**을 선택한 다음 **Close(**닫기**)**를 클릭합니다.
앞으로의 알림 방지(사용자 및 관리자 권한만 가능)	**Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > System Upgrade(**시스템 업그레이드**)**로 이동합니다.

업그레이드를 시작하기 전에: 중요 단계

시작하기 전에

업그레이드 및 업데이트를 위한 네트워크 요구 사항 확인 , 450 페이지의 네트워크 요구 사항을 참조하십시오.

단계 **1** 데이터 손실을 방지하거나 최소화하는 조치를 취합니다.

- 새 어플라이언스는 충분한 디스크 용량을 갖추고 전송될 각 데이터 유형에 대해 동일하거나 더 큰 크기가 할당되어야 합니다. 디스크 공간 최대값 및 할당량 정보, 489 페이지를 참조하십시오.
- 디스크 공간 경고가 표시될 경우 업그레이드하기 전에 디스크 공간 문제를 해결합니다.

단계 **2** XML 구성 파일을 어플라이언스 외부에 저장합니다. 현재 구성 파일 저장 및 내보내기, 480 페이지의 주의사항을 참조하십시오.

어떤 이유로든 이전 업그레이드 릴리스로 돌아가야 할 경우 이 파일이 필요합니다.

단계 **3** 허용 목록/차단 목록 기능을 사용 중인 경우 목록을 어플라이언스 외부로 내보냅니다.

Management Appliance(관리 어플라이언스) > **System Administration**(시스템 관리) > **Configuration File**(구성 파일)을 클릭하고 아래로 스크롤합니다.

단계 **4** CLI에서 업그레이드를 실행할 경우 **suspendlistener** 명령을 사용하여 리스너를 일시 중단합니다. GUI에서 업그레이드를 수행하는 경우 리스너가 자동으로 일시 중단됩니다.

단계 **5** 메일 대기열 및 전달 대기열을 비웁니다.

단계 **6** 업그레이드 설정이 올바르게 구성되었음을 확인합니다. 업그레이드 및 서비스 업데이트 설정 구성, 453 페이지를 참조하십시오.

AsyncOS 업그레이드

다운로드와 설치를 동시에 수행할 수도 있고, 백그라운드에서 다운로드한 후 나중에 설치할 수도 있습니다.

참고 Cisco 서버가 아니라 로컬 서버에서 AsyncOS의 다운로드와 업그레이드를 동시에 수행하는 경우, 다운로드 중에 업그레이드가 즉시 설치됩니다. 업그레이드 프로시스 시작 시 10초 동안 배너가 표시됩니다. 이 배너가 표시되어 있을 때, Ctrl-C를 입력하면 다운로드가 시작되기 전 업그레이드 프로세스를 종료할 수 있습니다.

시작하기 전에

- Cisco에서 업그레이드를 직접 다운로드할지, 아니면 네트워크의 서버에서 업그레이드 이미지를 호스트할지를 선택합니다. 그런 다음 선택한 방법을 지원하도록 네트워크를 설정합니다. 그런 다음 선택한 소스에서 업그레이드를 가져오도록 어플라이언스를 구성합니다. 업그레이드 방법 선택: 원격과 스트리밍 , 450 페이지 및 업그레이드 및 서비스 업데이트 설정 구성, 453 페이지를 참조하십시오.
- 업그레이드를 설치하기 전에 업그레이드를 시작하기 전에: 중요 단계 , 458 페이지의 지침을 수행합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **System Upgrade**(시스템 업그레이드)를 선택합니다.

단계 **3** **Upgrade Options**(업그레이드 옵션)를 클릭합니다.

단계 **4** 옵션을 선택합니다.

변경 후	수행해야 할 작업
업그레이드의 다운로드 및 설치를 한 번에 진행	**Download and Install(**다운로드 및 설치**)**을 클릭합니다. 이미 설치 프로그램을 다운로드한 경우 기존 다운로드를 덮어쓴다는 메시지가 표시됩니다.
업그레이드 설치 프로그램 다운로드	**Download only(**다운로드만**)**를 클릭합니다. 이미 설치 프로그램을 다운로드한 경우 기존 다운로드를 덮어쓴다는 메시지가 표시됩니다. 서비스 중단 없이 설치 프로그램이 백그라운드에서 다운로드됩니다.
다운로드한 업그레이드 설치 프로그램 설치	**Install(**설치**)**을 클릭합니다. 설치 프로그램이 다운로드된 경우에만 이 옵션이 나타납니다. 설치될 AsyncOS 버전이 Install(설치) 옵션 아래에 표시됩니다.

단계 **5** 전에 다운로드한 설치 프로그램을 설치하지 않은 경우 사용 가능한 업그레이드 목록에서 AsyncOS 버전을 선택합니다.

단계 **6** 설치 중인 경우

a) 현재 구성을 어플라이언스의 configuration 디렉터리에 저장할지 여부를 선택합니다.

b) 구성 파일에서 암호를 마스크 처리할지 여부를 선택합니다.

참고 마스킹된 암호의 구성 파일은 GUI의 Configuration File(구성 파일) 페이지 또는 CLI의 `loadconfig` 명령으로 로드할 수 없습니다.

c) 구성 파일의 복사본을 이메일로 전송하려면 해당 이메일 주소를 입력합니다. 여러 이메일 주소를 입력하는 경우 쉼표를 사용하여 구분합니다.

단계 **7** **Proceed(**진행**)**를 클릭합니다.

단계 **8** 설치 중인 경우

a) 프로세스 중에 프롬프트에 응답할 준비를 합니다.

응답할 때까지 프로세스가 일시 중지됩니다.

페이지 상단 근처에 진행률 표시줄이 나타납니다.

b) 프롬프트에서 **Reboot Now(**지금 재부팅**)**를 클릭합니다.

참고 재부팅 후 20분 이상이 경과할 때까지 (업그레이드 문제의 트러블슈팅을 포함하여) 어떤 이유로든 어플라이언스의 전원을 끄지 마십시오.

c) 약 10분 후에 어플라이언스에 다시 액세스하여 로그인합니다.

다음에 수행할 작업

- 프로세스가 중단된 경우 프로세스를 다시 시작해야 합니다.

- 업그레이드를 다운로드했지만 설치하지 않은 경우:

  업그레이드를 설치할 준비가 되면 '시작하기 전에' 섹션의 전제 조건을 포함하여 처음부터 이러한 지침을 수행하되, Install(설치) 옵션을 선택합니다.

- 업그레이드를 설치한 경우 업그레이드 후 , 461 페이지를 참조하십시오.

백그라운드 다운로드 상태 보기, 취소 또는 삭제

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > System Upgrade(**시스템 업그레이드**)**를 선택합니다.

단계 **3** **Upgrade Options(**업그레이드 옵션**)**를 클릭합니다.

단계 **4** 옵션을 선택합니다.

변경 후	수행해야 할 작업
다운로드 상태 보기	페이지 중간 부분을 살펴봅니다. 진행 중인 다운로드가 없으며 설치를 기다리는 완료된 다운로드가 없으면 다운로드 상태 정보가 표시되지 않습니다. 업그레이드 상태는 업그레이드 로그에도 나타납니다.
다운로드 취소	페이지 중간에 있는 **Cancel Download(**다운로드 취소**)** 버튼을 클릭합니다. 이 옵션은 다운로드가 진행 중인 경우에만 나타납니다.
다운로드된 설치 프로그램 삭제	페이지 중간의 **Delete File(**파일 삭제**)** 버튼을 클릭합니다. 설치 프로그램이 다운로드된 경우에만 이 옵션이 나타납니다.

업그레이드 후

업그레이드가 완료되면 다음을 수행합니다.

- (Email Security Appliance가 연결된 구축의 경우) 리스너를 다시 활성화합니다.
- (Web Security Appliance가 연결된 구축의 경우) 시스템에서 최신 구성 마스터를 지원하도록 구성합니다. 중앙에서 WSA를 관리하기 위한 구성 마스터 설정 , 342 페이지를 참조하십시오.
- 구성을 저장해두는 것도 좋습니다. 자세한 내용은 구성 설정 저장 및 가져오기 , 479 페이지를 참고하십시오.

- 업그레이드 후 온라인 도움말을 보기 전에 브라우저 캐시를 비우고 브라우저를 종료한 다음 다시 엽니다. 그러면 브라우저 캐시에서 오래된 콘텐츠가 지워집니다.

AsyncOS 이전 버전으로 복귀

비상 시 이전의 검증된 AsyncOS 버전으로 돌아갈 수 있습니다.

어플라이언스의 모든 데이터를 지우고 새로운 깨끗한 구성으로 시작하려는 경우에도 현재 실행 중인 빌드로 복귀할 수 있습니다.

관련 주제

- 복귀의 영향에 대한 중요 참고 사항, 462 페이지
- AsyncOS 복귀 , 462 페이지

복귀의 영향에 대한 중요 참고 사항

Cisco Content Security Appliance에서 revert 명령을 사용하는 것은 매우 위험합니다. 이 명령은 모든 기존 구성 및 데이터를 영구적으로 삭제합니다. 또한 어플라이언스를 다시 구성할 때까지 메일 처리가 중단됩니다.

복귀는 기능 키 또는 가상 어플라이언스 라이센스 만료일에 영향을 주지 않습니다.

AsyncOS 복귀

시작하기 전에

- 보존해야 할 데이터는 어플라이언스 외부에 백업하거나 저장합니다.
- 복귀할 버전의 구성 파일이 있어야 합니다. 구성 파일은 이전 버전과 호환되지 않습니다.
- 이 명령은 모든 구성을 삭제하므로 복귀할 때 어플라이언스에 대한 물리적 로컬 액세스를 확보하는 것이 좋습니다.
- Email Security Appliance에서 격리가 활성화된 경우 중앙 집중화를 비활성화하여 메시지가 해당 어플라이언스의 로컬에서 격리되게 합니다.

단계 **1** 복귀할 버전의 구성 파일이 있는지 확인합니다. 구성 파일은 이전 버전과 호환되지 않습니다.

단계 **2** 어플라이언스의 현재 구성의 백업 복사본을 다른 시스템에 저장합니다(암호 마스킹 없이). 이렇게 하려면 이메일을 통해 파일을 자신에게 전송하거나 FTP를 통해 파일을 올릴 수 있습니다. 이를 위한 간단한 방법은 `mailconfig` CLI 명령을 실행하는 것입니다. 그러면 현재 어플라이언스의 구성 파일을 지정된 이메일 주소에 보냅니다.

참고 이것은 복귀 후 로드할 구성 파일이 아닙니다.

단계 **3** 허용 목록/차단 목록 기능을 사용하는 경우 허용 목록/차단 목록 데이터베이스를 다른 시스템에 저장합니다.

단계 **4** ESA의 리스너를 일시 중단합니다.

단계 **5** 메일 대기열이 비워질 때까지 기다립니다.

단계 **6** 복귀할 어플라이언스의 CLI에 로그인합니다.

`revert` 명령을 실행하면 몇 가지 경고 프롬프트가 표시됩니다. 이러한 경고 프롬프트에 동의하면 즉시 복귀 작업이 수행됩니다. 따라서 복귀 전 단계를 완료하기 전에는 복귀 프로세스를 시작하지 마십시오.

단계 **7** 명령줄 프롬프트에서 **revert** 명령을 입력하고 프롬프트에 응답합니다.

다음 예제는 **revert** 명령을 보여줍니다.

예제:

```
m650p03.prep> revert
This command will revert the appliance to a previous version of AsyncOS.
WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco Spam Quarantine message and end-user safelist/blocklist data
Only the network settings will be preseved.
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passphrases
unmasked)
- exported the Cisco Spam Quarantine safelist/blocklist database
   to another machine (if applicable)
- waited for the mail queue to empty
Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired version.
Do you want to continue? yes
Are you sure you want to continue? yes
Available versions
=================
 1. 7.2.0-390
 2. 6.7.6-020
Please select an AsyncOS version: 1
You have selected "7.2.0-390".
Reverting to "testing" preconfigure install mode.
The system will now reboot to perform the revert operation.
```

단계 **8** 어플라이언스가 두 번 재부팅될 때까지 기다립니다.

단계 **9** CLI를 사용하여 어플라이언스에 로그인합니다.

단계 **10** 하나 이상의 Web Security Appliance를 추가하고 몇 분간 기다려 이 어플라이언스에서 URL 카테고리 업데이트를 다운로드할 수 있게 합니다.

단계 **11** URL 범주 업데이트가 완료되면 복귀하려는 버전의 XML 구성 파일을 로드합니다.

단계 **12** 허용 목록/차단 목록 기능을 사용하는 경우 허용 목록/차단 목록 데이터베이스를 가져오고 복원합니다.

단계 **13** ESA의 리스너를 다시 활성화합니다.

단계 **14** 변경 사항을 커밋합니다.

복귀된 Cisco Content Security Appliance가 이제 선택한 AsyncOS 버전을 사용하여 실행됩니다.

참고 복귀가 완료될 때까지 15분에서 20분 정도 소요될 수 있으며, Cisco Content Security Appliance에 대한 콘솔 액세스가 다시 사용 가능해집니다.

업데이트 정보

서비스 업데이트는 정기적으로 다운로드 가능하게 제공됩니다. 이러한 다운로드의 설정을 지정하려면 다음 섹션을 참조하십시오. 업그레이드 및 서비스 업데이트 설정 구성, 453 페이지

관련 주제

- 업그레이드 및 서비스 업데이트 설정 구성, 453 페이지

웹 사용 제어를 위한 URL 범주 집합 업데이트

- URL 범주 집합 업데이트 준비 및 관리 , 365 페이지
- URL 카테고리 집합 업데이트 및 보고 , 193 페이지

생성된 메시지에 대한 반환 주소 구성

다음과 같은 상황을 위해 AsyncOS에 의해 생성된 메일의 봉투 발신자를 구성할 수 있습니다.

- 바운스 메시지
- 보고서

반환 주소의 표시, 사용자 및 도메인 이름을 지정할 수 있습니다. 도메인 이름에 가상 게이트웨이 도메인을 사용하도록 선택할 수도 있습니다.

GUI의 System Administration(시스템 관리) 메뉴에 있는 반환 주소 페이지를 사용하거나 CLI에서 **addressconfig** 명령을 사용합니다.

GUI에서 시스템 생성 이메일 메시지의 반환 주소를 수정하려면 반환 주소 페이지에서 **Edit Settings(**설정 수정**)**를 클릭합니다. 수정할 주소를 변경하고 **Submit(**제출**)**을 클릭한 다음 변경사항을 커밋합니다.

경고 관리

어플라이언스에서 일어나는 이벤트에 대한 이메일 알림을 보냅니다.

변경 후	수행해야 할 작업
여러 관리자 사용자에게 다양한 유형의 알림 전송	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Alerts(알림)**를 선택합니다. 시스템 설정 중에 AutoSupport를 활성화한 경우, 기본적으로 모든 심각도 및 클래스에 대한 알림이 지정된 이메일 주소로 전송됩니다. 언제든 이 구성을 변경할 수 있습니다. 주소가 여러 개인 경우 쉼표로 구분해 주십시오.
알림에 대한 전역 설정 구성: • 알림 발신자(FROM:) 주소 • 중복 알림 제어 • AutoSupport 설정	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Alerts(알림)**를 선택합니다. 중복 알림 정보 , 466 페이지를 참고하십시오. Cisco AutoSupport, 467 페이지를 참고하십시오.
최근 알림 목록 보기 이 목록에 대한 설정 관리	최근 알림 보기 , 466 페이지를 참고하십시오.
알림 및 그 설명에 대한 목록 보기	참조: 하드웨어 알림 설명 , 467 페이지. 시스템 알림 설명 , 468 페이지
알림 전달 메커니즘 이해	알림 전달, 466 페이지를 참조하십시오.

알림 유형 및 심각도

알림 유형:

- 하드웨어 알림. 하드웨어 알림 설명 , 467 페이지를 참조하십시오.
- 시스템 알림. 시스템 알림 설명 , 468 페이지를 참조하십시오.
- 업데이터 알림.

알림은 다음과 같은 심각도를 가질 수 있습니다.

- Critical(중대): 즉각적인 조치 필요.
- Warning(경고): 추가 모니터링 및 잠재적으로 즉각적인 조치가 필요한 문제 또는 오류.
- Info(정보): 이 디바이스의 일반적인 작동 중에 생성되는 정보.

알림 전달

알림 메시지는 Cisco Content Security Appliance 내 문제를 알려주기 위해 사용될 수 있으므로 AsyncOS의 일반 메일 전달 시스템을 사용하여 전송되지 않습니다. 대신 알림 메시지는 AsyncOS에서 중요한 시스템 실패가 발생할 경우 작동하도록 설계된 별도의 평행 이메일 시스템을 통해 전달됩니다.

알림 메일 시스템은 AsyncOS와 동일한 구성을 공유하지 않습니다. 즉, 알림 메시지는 다른 메일 전달과 약간 다르게 작동할 수 있습니다.

- 알림 메시지는 표준 DNS MX 및 A 레코드 조회를 사용하여 전달됩니다.
  - 알림 메시지는 DNS 항목을 30분 동안 캐시하며 캐시는 30분마다 새로 고쳐지므로, DNS 실패가 발생해도 알림은 전송됩니다.
- 구축에 Email Security Appliance를 포함하는 경우
  - 알림 메시지는 작업 대기열을 거치지 않으므로 바이러스나 스팸 검사가 수행되지 않습니다. 메시지 필터 또는 콘텐츠 필터도 거치지 않습니다.
  - 알림 메시지는 전달 대기열을 거치지 않으므로 반송 프로필 또는 대상 제어 제한의 영향을 받지 않습니다.

최근 알림 보기

변경 후	수행해야 할 작업
최근 알림 목록 보기	관리자 및 운영자 액세스 권한이 있는 사용자는 **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Alerts(**알림**)**를 선택하고 **View Top Alerts(**상위 알림 보기**)** 버튼을 클릭할 수 있습니다. 이메일 전송에 문제가 있더라도 알림은 표시됩니다.
목록 정렬	열 제목을 클릭합니다.
이 목록에 저장할 수 있는 최대 알림 수 지정	CLI에서 alertconfig 명령을 사용합니다.
이 기능 비활성화	CLI에서 alertconfig 명령을 사용하여 최대 알림 수를 0으로 설정합니다.

중복 알림 정보

AsyncOS가 중복 알림을 전송하기 전 기다릴 초기 시간(초)을 지정할 수 있습니다. 중복 알림 요약이 전송되지 않고 대신 모든 중복 알림이 지연 없이 전송됩니다(이 경우 짧은 시간 동안 대량의 이메일이 전송될 수 있음). 중복 알림 전송 사이에 기다릴 시간(초)(알림 간격)은 각 알림이 전송된 후 늘어납

니다. 대기 시간(초)에 마지막 간격의 두 배를 더한 값이 늘어납니다. 따라서 5초 대기의 경우 5초, 15초, 35초, 75초, 155초, 315초 등에 알림이 전송됩니다.

결국 간격이 상당히 커질 수 있습니다. 중복 알림을 전송하기 전 기다릴 최대 시간(초) 필드를 통해 간격 사이에 기다릴 시간(초)의 최대값을 설정할 수 있습니다. 예를 들어 초기값을 5초로 설정하고 최대값을 60초로 설정하면 5초, 15초, 35초, 60초, 120초 등에 알림이 전송됩니다.

Cisco AutoSupport

Cisco에서 더 나은 지원을 제공하고 향후 시스템 변경을 더 잘 설계하도록 돕기 위해 시스템에 의해 생성되는 모든 알림 메시지의 복사본을 Cisco에 전송하도록 Cisco Content Security Appliance를 구성할 수 있습니다. 'AutoSupport'라고 하는 이 기능은 Cisco 지원 팀이 사용자의 요구를 사전 대처식으로 지원하도록 도와주는 유용한 방법입니다. AutoSupport는 또한 시스템의 가동 시간, **status** 명령의 출력 및 사용된 AsyncOS 버전을 알려주는 주간 보고서를 전송합니다.

기본적으로 시스템 알림 유형에 대해 정보 심각도 레벨 알림을 수신하도록 설정된 알림 수신자는 Cisco로 전송되는 모든 메시지의 복사본을 수신합니다. 주간 알림 메시지를 내부적으로 전송하지 않으려는 경우 이 기능을 비활성화할 수 있습니다. 이 기능을 활성화하거나 비활성화하려면 **Management Appliance(**관리 어플라이언스**) > System Administration Alerts(**시스템 관리 알림**)**를 선택하고 Edit Settings(설정 수정)를 클릭합니다.

기본적으로 AutoSupport를 활성화하면, Information(정보) 레벨에서 System(시스템) 알림을 수신하도록 설정된 알림 수신자에게 주간 AutoSupport 보고서가 전송됩니다.

하드웨어 알림 설명

표 ***86:*** 하드웨어 알림 설명

알림 이름	설명	심각도
INTERFACE.ERRORS	인터페이스 오류가 탐지될 때 전송됨.	경고
MAIL.MEASUREMENTS_FILESYSTEM	디스크 파티션이 용량에 근접할 때(75%) 전송됨.	경고
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	디스크 파티션이 용량의 90%(95%, 96%, 97% 등)에 도달할 때 전송됨.	중대
SYSTEM.RAID_EVENT_ALERT	중대한 RAID 이벤트가 발생할 경우 전송됨.	경고
SYSTEM.RAID_EVENT_ALERT_INFO	RAID 이벤트가 발생할 경우 전송됨.	정보

시스템 알림 설명

표 ***87:*** 시스템 알림 설명

알림 이름	설명	심각도
COMMON.APP_FAILURE	알 수 없는 애플리케이션 실패가 발생할 경우 전송됨.	중대
COMMON.KEY_EXPIRED_ALERT	기능 키가 만료된 경우 전송됨.	경고
COMMON.KEY_EXPIRING_ALERT	기능 키가 곧 만료되는 경우 전송됨.	경고
COMMON.KEY_FINAL_EXPIRING_ALERT	기능 키가 곧 만료된다는 최종 알림으로 전송됨.	경고
DNS.BOOTSTRAP_FAILED	어플라이언스가 루트 DNS 서버에 연결할 수 없을 경우 전송됨.	경고
COMMON.INVALID_FILTER	잘못된 필터가 발견될 경우 전송됨.	경고

알림 이름	설명	심각도
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	알림 메시지: • The host at <IP address> has been added to the blacklist because of an SSH DOS attack. • The host at <IP address> has been permanently added to the ssh whitelist. • The host at <IP address> has been removed from the blacklist SSH를 통해 어플라이언스에 연결하려고 시도하지만 유효한 자격 증명을 제공하지 않는 IP 주소는 10분 내에 실패한 시도 수가 10을 넘으면 SSH 블랙리스트에 추가됩니다. 사용자가 동일한 IP 주소에서 성공적으로 로그인하면 해당 IP 주소는 화이트리스트에 추가됩니다. 화이트리스트의 주소는 블랙리스트에서도 발견되더라도 액세스가 허용됩니다.	경고
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP 그룹 쿼리가 실패할 경우 전송됨.	중대
LDAP.HARD_ERROR	LDAP 쿼리가 완전히 실패할 경우 전송됨(모든 서버 시도 후).	중대
LOG.ERROR.*	각종 로깅 오류.	중대
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	수신자별 검사 중에 LDAP 그룹 쿼리가 실패할 경우 전송됨.	중대
MAIL.QUEUE.ERROR.*	각종 메일 대기열 하드 오류.	중대
MAIL.RES_CON_START_ALERT.MEMORY	RAM 사용률이 시스템 리소스 절약 임계값을 초과할 경우 전송됨.	중대

알림 이름	설명	심각도
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	메일 대기열이 과부화되어 시스템 리소스 보존이 활성화될 경우 전송됨.	중대
MAIL.RES_CON_START_ALERT.QUEUE	대기열 사용률이 시스템 리소스 절약 임계값을 초과할 경우 전송됨.	중대
MAIL.RES_CON_START_ALERT.WORKQ	작업 대기열 크기가 너무 커서 리스너가 일시 중단되는 경우 전송됨.	중대
MAIL.RES_CON_START_ALERT	어플라이언스가"리소스 절약" 모드로 들어갈 경우 전송됨.	중대
MAIL.RES_CON_STOP_ALERT	어플라이언스가"리소스 절약" 모드에서 나올 경우 전송됨.	중대
MAIL.WORK_QUEUE_PAUSED_NATURAL	작업 대기열이 일시 중지될 경우 전송됨.	중대
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	작업 대기열이 다시 시작될 경우 전송됨.	중대
NTP.NOT_ROOT	NTP가 루트로 실행되고 있지 않아서 어플라이언스가 시간을 조정할 수 없을 경우 전송됨.	경고
PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS	도메인 지정 파일에 오류가 있을 경우 전송됨.	중대
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY	도메인 지정 파일이 비어 있을 때 전송됨	중대
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING	도메인 지정 파일이 없을 때 전송됨	중대
REPORTD.DATABASE_OPEN_FAILED_ALERT	보고 엔진이 데이터베이스를 열 수 없을 경우 전송됨.	중대
REPORTD.AGGREGATION_DISABLED_ALERT	시스템에 디스크 공간이 부족할 경우 전송됨. 로그 항목에 대한 디스크 사용량이 로그 사용량 임계값을 초과하면 보고용 집계가 비활성화되고 알림이 전송됩니다.	경고

알림 이름	설명	심각도
REPORTING.CLIENT.UPDATE_FAILED_ALERT	보고 엔진이 보고 데이터를 저장할 수 없을 경우 전송됨.	경고
REPORTING.CLIENT.JOURNAL.FULL	보고 엔진이 새 데이터를 저장할 수 없을 경우 전송됨.	중대
REPORTING.CLIENT.JOURNAL.FREE	보고 엔진이 새 데이터를 다시 저장할 수 있게 될 경우 전송됨.	정보
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE_ALERT	보고 엔진이 보고서를 작성할 수 없을 경우 전송됨.	중대
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE_ALERT	보고서를 이메일로 보낼 수 없을 경우 전송됨.	중대
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE_ALERT	보고서를 보관할 수 없을 경우 전송됨.	중대
SENDERBASE.ERROR	SenderBase로부터의 응답을 처리하는 동안 오류가 발생할 경우 전송됨.	정보
SMAD.ICCM.ALERT_PUSH_FAILED	하나 이상의 호스트에 대해 구성 푸시가 실패할 경우 전송됨.	경고
SMAD.TRANSFER.TRANSFERS_STALLED	SMA 로그에서 2시간 동안 추적 데이터를 또는 6시간 동안 보고 데이터를 가져올 수 없을 때 전송됨.	경고
SMTPAUTH.FWD_SERVER_FAILED_ALERT	SMTP 인증 전달 서버에 도달할 수 없을 경우 전송됨.	경고
SMTPAUTH.LDAP_QUERY_FAILED	LDAP 쿼리에 실패할 경우 전송됨.	경고
SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT	재부팅 시 시스템 종료에 문제가 있을 경우 전송됨.	경고
SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN	시스템 종료에 문제가 있을 경우 전송됨.	경고
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	수신자 검증 업데이트가 실패할 경우 전송됨.	중대

알림 이름	설명	심각도
SYSTEM.SERVICE_TUNNEL.DISABLED	Cisco 지원 서비스용으로 생성된 터널이 비활성화될 경우 전송됨.	정보
SYSTEM.SERVICE_TUNNEL.ENABLED	Cisco 지원 서비스용으로 생성된 터널이 활성화될 경우 전송됨.	정보

네트워크 설정 변경

이 섹션에서는 어플라이언스의 네트워크 작업을 구성하는 데 사용되는 기능에 대해 설명합니다. 이러한 기능을 사용하면 시스템 설정 마법사 실행, 25 페이지의 시스템 설정 마법사를 통해 구성한 호스트 이름, DNS 및 라우팅 설정에 직접 액세스할 수 있습니다.

다음과 같은 기능에 대해 설명합니다.

- `sethostname`
- DNS 구성(GUI 및 CLI의 `dnsconfig` 명령)
- 라우팅 구성(GUI 및 CLI의 `routeconfig`, `setgateway` 명령)
- `dnsflush`
- 암호

시스템 호스트 이름 변경

호스트 이름은 CLI 프롬프트에서 시스템을 식별하는 데 사용됩니다. 정규 호스트 이름을 입력해야 합니다. sethostname 명령은 CSA의 이름을 설정합니다. 새 호스트 이름은 commit 명령을 실행할 때까지 적용되지 않습니다.

sethostname 명령

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

호스트 이름 변경을 적용하려면 commit 명령을 입력해야 합니다. 호스트 이름 변경을 성공적으로 커밋하면 새 이름이 CLI 프롬프트에 나타납니다.

```
oldname.example.com> commit
Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

새 호스트 이름이 다음과 같이 프롬프트에 나타납니다. mail3.example.com>

DNS(Domain Name System) 설정 구성

GUI에서 Management Appliance(관리 어플라이언스) > Network(네트워크) > DNS 페이지를 통해 또는 dnsconfig 명령을 사용하여 CSA의 DNS 설정을 구성할 수 있습니다.

다음 설정을 구성할 수 있습니다.

- 인터넷의 DNS 서버를 사용할지 아니면 자신의 서버를 사용할지 여부, 그리고 사용할 서버
- DNS 트래픽에 사용할 인터페이스
- 역방향 DNS 조회가 시간 초과될 때까지 기다릴 시간(초)
- DNS 캐시 지우기

DNS 서버 지정

AsyncOS에서는 인터넷 루트 DNS 서버, 조직의 자체 DNS 서버 또는 사용자가 지정한 공인 DNS 서버를 사용할 수 있습니다. 인터넷 루트 서버를 사용할 때 특정 도메인에 대해 사용할 대체 서버를 지정할 수 있습니다. 대체 DNS 서버는 단일 도메인에 적용되므로, 해당 도메인에 대해 신뢰할 수 있는 서버여야 합니다(확정된 DNS 레코드 제공).

인터넷의 DNS 서버를 사용하지 않을 경우 AsyncOS는 DNS 서버의 "분리"를 지원합니다. 자체 내부 서버를 사용 중인 경우 예외 도메인 및 관련된 DNS 서버를 지정할 수 있습니다.

"분리 DNS"를 설정할 때 in-addr.arpa(PTR) 항목도 설정해야 합니다. 예를 들어 ".eng" 쿼리를 네임서버 1.2.3.4로 리디렉션하고자 하며 현재 .eng 항목이 172.16 네트워크에 있는 경우, 분리 DNS 구성에서 도메인으로 "eng,16.172.in-addr.arpa"를 지정해야 합니다.

여러 항목 및 우선 순위

입력하는 각 DNS 서버에 대해 숫자 우선 순위를 지정할 수 있습니다. AsyncOS는 0과 가장 가까운 우선 순위의 DNS 서버를 사용하려고 시도합니다. 해당 DNS 서버가 응답하지 않으면 AsyncOS는 다음 우선 순위의 서버를 사용하려고 시도합니다. 동일한 우선 순위의 DNS 서버에 대해 여러 항목을 지정하는 경우 시스템은 쿼리를 수행할 때마다 해당 우선 순위의 DNS 서버 목록을 임의로 지정합니다. 시스템은 첫 번째 쿼리가 만료 또는 "시간 초과"될 때까지 잠깐 기다리고, 두 번째 쿼리에 대해서는 조금 더 기다리는 식으로 진행합니다. 대기 시간은 DNS 서버 수 및 구성된 우선 순위에 따라 달라집니다. 대기 시간 길이는 특정 우선 순위의 모든 IP 주소에 대해 동일합니다. 첫 번째 우선 순위의 시간 초과가 가장 짧고, 이후의 우선 순위는 시간 초과가 조금씩 길어집니다. 시간 초과 기간은 약 60초입니다. 우선 순위가 하나 있는 경우 해당 우선 순위에서 각 서버에 대한 시간 초과는 60초입니다. 우선 순위가 2개 있는 경우 첫 번째 우선 순위에서 각 서버의 시간 초과는 15초이고, 두 번째 우선 순위에서 각 서버의 시간 초과는 45초입니다. 우선 순위가 3개 있는 경우 시간 초과는 각각 5, 10, 45입니다.

예를 들어 4개의 DNS 서버를 구성하고 있으며 그중 2개의 우선 순위는 0, 하나는 1, 하나는 2라고 가정해보겠습니다.

표 ***88: DNS*** 서버, 우선 순위 및 시간 초과 간격의 예

Priority(우선순위)	서버	시간초과(초)
0	1.2.3.4, 1.2.3.5	5, 5

Priority(우선순위)	서버	시간 초과(초)
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS는 우선 순위 0인 두 서버 가운데에서 임의로 하나를 선택합니다. 우선 순위 0 서버 중 하나가 다운되면 나머지가 사용됩니다. 우선 순위 0 서버가 둘 다 다운되면 우선 순위 1 서버(1.2.3.6)가 사용되고, 그런 다음 최종적으로 우선 순위 2(1.2.3.7) 서버가 사용됩니다.

시간 초과 기간은 우선 순위 0 서버 둘에 대해 동일하며, 우선 순위 1 서버에 대해서는 좀 더 길고, 우선 순위 2 서버에 대해 더 깁니다.

인터넷 루트 서버 사용

AsyncOS DNS 확인자는 고성능 이메일 전달을 위해 필요한 대량의 동시 DNS 연결을 수용하도록 설계되었습니다.

참고 기본 DNS 서버를 인터넷 루트 서버가 아닌 다른 서버로 설정하기로 선택하는 경우, 해당 서버는 자신이 인증된 서버로 있지 않은 도메인에 대한 쿼리를 재귀적으로 확인할 수 있어야 합니다.

역방향 **DNS** 조회 시간 초과

Cisco Content Security Appliance는 이메일을 전송 또는 수신하기 위해 리스너에 연결된 모든 원격 호스트에서 "이중 DNS 조회"를 수행하려고 시도합니다. 즉 시스템은 이중 DNS 조회를 수행하여 원격 호스트 IP 주소의 유효성을 획득하고 확인합니다. 이는 연결하는 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회 및 그 뒤에 오는 PTR 조회의 결과에 대한 정방향 DNS(A) 조회로 구성됩니다. 그런 다음 시스템은 A 조회의 결과가 PTR 조회의 결과와 일치하는지를 확인합니다. 결과가 일치하지 않거나 A 레코드가 존재하지 않으면 시스템은 IP 주소만 사용하여 HAT(Host Access Table)의 항목 일치를 확인합니다. 이 특별한 시간 초과 기간은 이 조회에만 적용되며 여러 항목 및 우선 순위, 473 페이지에서 설명한 일반 DNS 시간 초과와는 관련이 없습니다.

기본값은 20초입니다. 시간(초)으로 '0'을 입력하여 모든 리스너에서 전역적으로 역방향 DNS 조회 시간 초과를 비활성화할 수 있습니다. 값을 0초로 설정하면, 역방향 DNS 조회가 시도되지 않으며 대신 표준 시간 초과 응답이 즉시 반환됩니다.

DNS 알림

때때로 어플라이언스가 재부팅될 때 "Failed to bootstrap the DNS cache(DNS 캐시 부트스트랩 실패)"라는 메시지와 함께 알림이 생성될 수 있습니다. 이러한 메시지는 시스템이 기본 DNS 서버에 연결할 수 없음을 나타냅니다. 이는 네트워크 연결이 설정되기 전 DNS 하위 시스템이 온라인 상태가 되는 경우 부팅 시 발생할 수 있습니다. 이 메시지가 다른 때에 나타나면 네트워크 문제를 나타내거나 DNS 구성이 유효한 서버를 가리키고 있지 않음을 나타낼 수 있습니다.

DNS 캐시 지우기

GUI의 **Clear Cache**(캐시 지우기) 버튼 또는 dnsflush 명령(dnsflush 명령에 대한 자세한 내용은 설명서, 571 페이지에 명시된 위치에서 IronPort AsyncOS CLI 참조 설명서 참조)은 DNS 캐시의 모든 정보를 지웁니다. 로컬 DNS 시스템이 변경되었을 때 이 기능을 사용하도록 선택할 수 있습니다. 이 명령은 즉시 수행되며, 캐시가 다시 채워지는 동안 일시적으로 성능 저하가 발생할 수 있습니다.

그래픽 사용자 인터페이스를 통해 DNS 설정 구성

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **Network**(네트워크) > **DNS** 페이지에서 **Edit Settings**(설정 수정) 버튼을 클릭합니다.

단계 **3** 인터넷 루트 DNS 서버를 사용할지 아니면 자체 내부 DNS 서버를 사용할지를 선택한 다음 정식 DNS 서버를 지정합니다.

단계 **4** 자체 DNS 서버를 사용하거나 정식 DNS 서버를 지정하려면 서버 ID를 입력하고 **Add Row**(행 추가)를 클릭합니다. 각 서버에 대해 이를 반복합니다. 자체 DNS 서버를 입력할 때 우선 순위도 지정합니다. 자세한 내용은 DNS 서버 지정, 473 페이지을 참고하십시오.

단계 **5** DNS 트래픽에 대한 인터페이스를 선택합니다.

단계 **6** 역방향 DNS 조회를 취소하기 전에 기다릴 시간(초)을 입력합니다.

단계 **7** **Clear Cache**(캐시 지우기)를 클릭하여 DNS 캐시를 지울 수도 있습니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

TCP/IP 트래픽 경로 구성

일부 네트워크 환경에서는 표준 기본 게이트웨이 이외의 트래픽 경로를 사용해야 합니다. GUI에서 **Management Appliance**(관리 어플라이언스) > **Network**(네트워크) > **Routing**(라우팅) 페이지를 사용하거나 CLI에서 **`routeconfig`** 명령을 사용하여 고정 경로를 관리할 수 있습니다.

- GUI에서 고정 경로 관리, 475 페이지
- 기본 게이트웨이 수정(GUI), 476 페이지

GUI에서 고정 경로 관리

Management Appliance(관리 어플라이언스) > Network(네트워크) > Routing(라우팅) 페이지에서 고정 경로를 생성, 수정, 삭제할 수 있습니다. 이 페이지에서 기본 게이트웨이를 수정할 수도 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **Network**(네트워크) > **Routing**(라우팅) 페이지의 경로 목록에서 **Add Route**(경로 추가)를 클릭합니다. 경로의 이름을 입력합니다.

단계 **3** 대상 IP 주소를 입력합니다.
단계 **4** 게이트웨이 IP 주소를 입력합니다.
단계 **5** 변경 사항을 제출 및 커밋합니다.

기본 게이트웨이 수정(GUI)

단계 **1** Routing(라우팅) 페이지의 경로 목록에서 Default Route(기본 경로)를 클릭합니다.
단계 **2** 게이트웨이 IP 주소를 변경합니다.
단계 **3** 변경 사항을 제출 및 커밋합니다.

기본 게이트웨이 구성

GUI에서 Management Appliance(관리 어플라이언스) > Network(네트워크) > Routing(라우팅) 페이지를 사용하거나(기본 게이트웨이 수정(GUI), 476 페이지 참조) CLI에서 setgateway 명령을 사용하여 기본 게이트웨이를 구성할 수 있습니다.

보안 통신 프로토콜 지정

- SSL v3는 안전하지 않으므로 사용하지 말아야 합니다.
- 다음 각 항목에 사용할 통신 프로토콜을 선택할 수 있습니다.
  - 업데이터 서버
  - 스팸 격리에 대한 엔드 유저 액세스
  - 어플라이언스에 대한 웹 기반 관리 인터페이스
  - LDAPS
- 현재 선택된 프로토콜 및 사용 가능한 옵션을 보거나 프로토콜을 변경하려면 명령줄 인터페이스에서 sslconfig 명령을 사용합니다.
- Cisco 업데이트 서버는 SSL v3를 지원하지 않습니다.
- 로컬 (원격) 업데이트 서버를 사용하는 경우 사용 중인 서버와 도구 다른 모든 서비스 및 웹 브라우저에 대해 선택한 프로토콜을 지원하고 활성화해야 합니다.
- 사용하는 각 서비스에 대해 사용 가능한 옵션 중 하나를 활성화해야 합니다.
- sslconfig 명령을 사용하여 변경한 사항은 커밋이 필요합니다.
- sslconfig 명령을 사용하여 변경한 사항을 커밋한 후 영향을 받는 서비스는 잠시 중단됩니다.

시스템 시간 구성

참고 Security Management Appliance는 보고서용 데이터를 수집할 때, Security Management Appliance에서 시간 설정을 구성할 때 지정된 정보에서 타임스탬프를 가져와 적용합니다. 자세한 내용은 Security Management Appliance에서 보고서를 위한 데이터를 수집하는 방법, 34 페이지를 참조하십시오.

CLI에서 시간 관련 설정을 하려면 ntpconfig, settime, settz 명령을 사용합니다.

변경 후	수행해야 할 작업
시스템 시간 설정	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Time Settings(**시간 설정**)**를 선택합니다**.** NTP(Network Time Protocol) 서버 사용, 477 페이지 섹션도 참조해 주십시오.
표준 시간대 설정	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Time Zone(**표준 시간대**)**을 선택합니다. 다음 항목도 참고하십시오. • GMT 차감 시간 선택, 478 페이지 • 표준 시간대 파일 업데이트, 478 페이지

NTP(Network Time Protocol) 서버 사용

NTP 서버를 사용하여 Security Management Appliance 시스템 시계를 네트워크의 다른 컴퓨터 또는 인터넷과 동기화할 수 있습니다.

기본 NTP 서버는 time.sco.cisco.com입니다.

기본 NTP 서버를 포함하여 외부 NTP 서버를 사용할 경우 방화벽을 통해 필수 포트를 엽니다. 방화벽 정보, 563 페이지를 참고하십시오.

관련 주제

- 시스템 시간 구성, 477 페이지
- 표준 시간대 파일 수동 업데이트 , 478 페이지

GMT 차감 시간 선택

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Time Zone(**표준 시간대**)**을 선택합니다.

단계 **3** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **4** 지역 목록에서 GMT Offset(GMT 차감 시간)을 선택합니다. Time Zone Setting(표준 시간대 설정) 페이지가 Time Zone(표준 시간대) 필드에 GMT 차감 시간을 포함하도록 업데이트됩니다.

단계 **5** Time Zone(표준 시간대) 필드에서 차감 시간을 선택합니다. 차감 시간이란 GMT(Greenwich Mean Time) 본초자오선에 도달하기 위해 추가하거나 빼야 할 시간을 가리킵니다. 앞에 빼기 기호("-")가 오는 시간은 본초자오선의 서쪽입니다. 더하기 기호("+")는 본초자오선의 동쪽을 가리킵니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

표준 시간대 파일 업데이트

어떤 국가에서든 표준 시간대 규칙의 변동이 있을 때마다 어플라이언스의 표준 시간대 파일을 업데이트해야 합니다.

- 표준 시간대 파일 자동 업데이트 , 478 페이지
- 표준 시간대 파일 수동 업데이트 , 478 페이지

표준 시간대 파일 자동 업데이트

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Update Settings(**업데이트 설정**)**를 선택합니다.

단계 **3** **Enable automatic updates for Time zone rules(**표준 시간대 규칙 자동 업데이트 활성화**)** 확인란을 선택합니다.

단계 **4** 간격을 입력합니다. 페이지에서 **?** 도움말을 클릭하면 중요한 정보가 표시됩니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

표준 시간대 파일 수동 업데이트

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Time Settings(**시간 설정**)**를 선택합니다.

단계 **3** **Time Zone File Updates(**표준 시간대 파일 업데이트**)** 섹션을 살펴봅니다.

단계 **4** 사용 가능한 표준 시간대 파일 업데이트가 있으면 **Update Now(**지금 업데이트**)**를 클릭합니다.

Configuration File(구성 파일) 페이지

이 섹션에 대한 정보	참조
현재 구성 저장	구성 설정 저장 및 가져오기 , 479 페이지
저장된 구성 로드	구성 설정 저장 및 가져오기 , 479 페이지
최종 사용자 허용 목록/차단 목록 데이터베이스(스팸 쿼런틴)	허용 목록/차단 목록 백업 및 복원 , 296 페이지
구성 재설정	공장 기본 구성으로 재설정, 436 페이지

구성 설정 저장 및 가져오기

참고 이 섹션에 설명된 구성 파일은 Security Management Appliance를 구성하는 데 사용됩니다.

Security Management Appliance의 구성 설정 대부분은 단일 구성 파일을 통해 관리할 수 있습니다. 파일은 XML(Extensible Markup Language) 형식으로 유지됩니다.

몇 가지 방법으로 이 파일을 사용할 수 있습니다.

- 기본 Security Management Appliance에서 예기치 않은 장애가 발생할 경우 신속하게 두 번째 Security Management Appliance에서 서비스를 복원하도록 구성할 수 있습니다.
- 중요 구성 데이터를 백업 및 보존하려면 구성 파일을 다른 시스템에 저장할 수 있습니다. 어플라이언스를 구성하는 동안 실수한 경우 최근에 저장된 구성 파일로 "롤백"할 수 있습니다.
- 어플라이언스의 전체 구성을 빠르게 검토하려면 기존 구성 파일을 다운로드할 수 있습니다. (다수의 최신 브라우저에서는 XML 파일을 직접 렌더링할 수 있습니다.) 이는 현재 구성에 존재할 수 있는 작은 오류(예: 오타)를 해결하는 데 도움이 될 수 있습니다.
- 기존 구성 파일을 다운로드하고 내용을 변경하고 동일한 어플라이언스에 업로드할 수 있습니다. 이 기능은 구성을 변경할 수 있도록 사실상 CLI와 GUI를 모두 "우회"합니다.
- FTP 액세스를 통해 전체 구성 파일을 업로드하거나 구성 파일의 일부를 CLI에 직접 붙여넣을 수 있습니다.
- 파일이 XML 형식이므로 구성 파일의 모든 XML 엔티티를 설명하는 관련 DTD(document type definition)도 함께 제공됩니다. 업로드 전 XML 구성 파일을 검증하려면 DTD를 다운로드할 수 있습니다. 인터넷에서 XML 검증 툴을 쉽게 이용할 수 있습니다.

- 구성 파일을 사용하여 다른 어플라이언스, 이를테면 복제된 가상 어플라이언스의 구성을 신속하게 수행할 수 있습니다.

구성 파일 관리

- 허용 목록/차단 목록 백업 및 복원 , 296 페이지
- 공장 기본 구성으로 재설정, 436 페이지
- 이전에 커밋한 구성으로 롤백 , 483 페이지

현재 구성 파일 저장 및 내보내기

Management Appliance(관리 어플라이언스**) > System Administration(**시스템 관리**) > Configuration File(**구성 파일**)** 페이지의 Current Configuration(현재 구성)을 사용하여 현재 구성 파일을 로컬 시스템에 저장하거나, 어플라이언스에 저장하거나(FTP/SCP 루트의 configuration 디렉터리), 이메일을 통해 지정된 주소로 전송할 수 있습니다.

암호 마스킹

확인란을 선택하여 사용자의 암호를 마스킹할 수 있습니다. 암호를 마스크 처리하면 내보내거나 저장한 파일에서 원래의 암호화된 암호가 "*****"로 교체됩니다.

참고 마스킹된 암호가 있는 구성 파일은 다시 AsyncOS에 로드할 수 없습니다.

암호 암호화

Encrypt passwords in the Configuration Files(구성 파일에서 비밀번호 암호화) 확인란을 클릭하여 사용자의 암호를 암호화할 수 있습니다. 다음은 암호화될 컨피그레이션 파일의 주요 보안 매개변수입니다.

- 인증서 개인 키
- RADIUS 비밀번호
- LDAP 바인드 비밀번호
- 로컬 사용자의 비밀번호 해시
- SNMP 비밀번호
- 발신 SMTP 인증 비밀번호
- PostX 암호화 키
- PostX 암호화 프록시 비밀번호
- FTP 푸시 로그 서브스크립션 비밀번호
- IPMI LAN 비밀번호

- 업데이터 서버 URL

CLI에서 `saveconfig` 명령을 사용하여 이를 구성할 수도 있습니다.

구성 파일 로드

구성을 로드할 어플라이언스와 동일한 AsyncOS 버전을 실행하는 어플라이언스로부터 구성 파일을 저장한 상태여야 합니다.

마스킹된 암호가 있는 구성 파일은 로드할 수 없습니다.

방법과 상관없이 구성 상단에 다음 태그를 포함해야 합니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
 ... your configuration information in valid XML
</config>
```

구성 정보 뒤에 닫는 </config> 태그를 사용해야 합니다. Cisco Content Security Appliance의 구성 디렉터리에 있는 DTD(document type definition)를 기준으로 XML 구문의 값이 구문 분석 및 검증됩니다. DTD 파일의 이름은 config.dtd입니다. loadconfig 명령을 사용할 때 명령줄에서 검증 오류가 보고되면 변경 사항이 로드되지 않습니다. 업로드 전 어플라이언스 외부에서 구성 파일을 검증하려면 DTD를 다운로드할 수 있습니다.

어떤 가져오기 방법을 사용하든 선언 태그(위)를 포함하며 <config></config> 태그 내에 포함되어 있는 한, 전체 구성 파일(최고 레벨 태그인 <config></config> 사이에 정의된 정보) 또는 구성 파일의 *complete* 및 *unique* 하위 섹션을 가져올 수 있습니다.

"Complete"란 DTD에 정의된 대로 지정된 하위 섹션에 대한 전체 시작 및 종료 태그가 포함되어 있음을 의미합니다. 예를 들어 다음 코드를 업로드하거나 붙여넣으면 검증 오류가 발생합니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

그러나 다음 코드를 업로드하거나 붙여넣으면 검증 오류가 발생하지 않습니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

"Unique"란 업로드하거나 붙여넣는 구성 파일의 하위 집합이 구성에 대해 모호하지 않다는 의미입니다. 예를 들어 시스템은 호스트 이름을 하나만 가질 수 있으므로 다음 코드(선언 및 <config></config> 태그 포함)를 업로드하는 것이 허용됩니다.

```
<hostname>mail4.example.com</hostname>
```

그러나 한 시스템에 대해 여러 리스너가 정의될 수 있으며 각각에 대해 서로 다른 Recipient Access Table이 정의되므로 다음 코드를 업로드하면 모호해집니다.

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

태그는 "complete" 구문이라도 모호하므로 허용되지 않습니다.

⚠

주의 구성 파일 또는 구성 파일의 하위 섹션을 업로드하거나 구문 분석할 때 커밋되지 않은(대기 중일 수 있는) 변경 사항을 지울 가능성이 있습니다.

빈 태그와 생략된 태그

구성 파일의 섹션을 업로드하거나 구분 분석할 때는 주의해야 합니다. 태그를 포함하지 않으면 구성 파일을 로드할 때 구성의 해당 값이 수정되지 않습니다. 그러나 빈 태그를 포함하면 해당 구성 설정이 지워집니다.

예를 들어 다음 코드를 업로드하면 시스템에서 모든 리스너가 삭제됩니다.

```
<listeners></listeners>
```

⚠

주의 구성 파일의 하위 섹션을 업로드하거나 구문 분석할 때, GUI나 CLI에서 연결이 끊어지고 대량의 구성 데이터가 손실될 가능성이 있습니다. 또 다른 프로토콜, Serial 인터페이스 또는 Management 포트의 기본 설정을 사용하여 어플라이언스에 다시 연결할 수 있는 경우가 아니면 이 명령으로 서비스를 비활성화하지 마십시오. 또한 DTD에 의해 정의된 정확한 구성 구문을 확실히 알고 있지 않다면 이 명령을 사용하지 마십시오. 새 구성 파일을 로드하기 전에 항상 구성 데이터를 백업하십시오.

로그 서브스크립션용 암호 로드에 대한 참고 사항

암호(예: FTP 푸시를 사용할 비밀번호)가 필요한 로그 서브스크립션이 포함된 구성 파일을 로드하려고 하는 경우 `loadconfig` 명령은 암호 누락에 대해 경고하지 않습니다. `logconfig` 명령을 사용하여 올바른 암호를 구성할 때까지 FTP 푸시가 실패하고 알림이 생성됩니다.

문자 집합 인코딩에 대한 참고 사항

오프라인으로 파일을 조작하기 위해 사용하는 문자 집합과 상관없이, XML 구성 파일의 "encoding" 특성은 "ISO-8859-1"이어야 합니다. showconfig, saveconfig 또는 mailconfig 명령을 실행할 때마다 파일에 인코딩 특성이 지정됩니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

현재 구성 재설정

현재 구성을 재설정하면 Cisco Content Security Appliance가 원래 공장 기본값으로 되돌아갑니다. 재설정하기 전에 구성을 저장합니다.

공장 기본 구성으로 재설정, 436 페이지를 참조하십시오.

이전에 커밋한 구성으로 롤백

언제든 이전에 커밋한 구성으로 롤백할 수 있습니다.

CLI에서 rollbackconfig 명령을 사용하여 최근 10건의 커밋 중 하나를 선택합니다.

롤백 커밋 프롬프트에서 No를 입력하면 다음에 변경사항을 커밋할 때 롤백이 커밋됩니다.

관리자 액세스 권한이 있는 사용자만 rollbackconfig 명령을 사용할 수 있습니다.

참고 이전 구성 복원 시 로그 메시지 또는 알림이 생성되지 않습니다.

참고 기존 데이터를 유지할 수 없는 크기에 디스크 공간을 재할당하는 등의 특정 커밋을 수행하면 데이터가 손실될 수 있습니다.

구성 파일에 대한 CLI 명령

다음 명령을 사용하여 구성 파일을 다룰 수 있습니다.

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `rollbackconfig`
- `resetconfig`(공장 기본 구성으로 재설정, 436 페이지 참조)
- `publishconfig`
- `backupconfig`(Security Management Appliance 데이터 백업 , 440 페이지 참조)
- `trailblazerconfig`

showconfig, mailconfig 및 saveconfig 명령

구성 파일 명령 `showconfig`, `mailconfig` 및 `saveconfig`의 경우 메일로 보내거나 표시할 파일에 암호를 포함할지 선택하라는 메시지가 표시됩니다. 암호를 포함하지 않기로 선택할 경우 암호 필드를 비워 둡니다. 보안 위협이 염려된다면 암호를 포함하지 않기로 선택할 수 있습니다. 그러나 암호가 없는 구성 파일은 `loadconfig` 명령을 사용하여 로드할 때 실패하게 됩니다. 로그 서브스크립션용 암호 로드에 대한 참고 사항, 482 페이지를 참조하십시오.

참고 암호를 포함하기로 선택할 경우("Do you want to include passphrases?"에 예라고 답함) 구성 파일을 저장하거나 표시하거나 메일로 보낼 때 암호가 암호화됩니다. 그러나 개인 키와 인증서는 암호화되지 않은 PEM 형식으로 포함됩니다.

showconfig 명령은 현재 구성을 화면에 출력합니다.

```
mail3.example.com> showconfig
Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: model number
Messaging Gateway Appliance(tm)
  Model Number: model number
  Version: version of AsyncOS installed
  Serial Number: serial number
  Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

사용자에게 현재 구성을 이메일로 보내려면 mailconfig 명령을 사용합니다. XML 형식의 구성 파일(이름 config.xml)이 메시지에 첨부됩니다.

```
mail3.example.com> mailconfig
Please enter the email address to which you want to send
the configuration file.
[]> administrator@example.com
Do you want to include passphrases? Please be aware that a configuration
without passphrases will fail when reloaded with loadconfig.  [N]> y
The configuration file has been sent to administrator@example.com.
```

Security Management Appliance의 saveconfig 명령은 모든 구성 마스터 파일(ESA)을 고유한 파일 이름과 함께 configuration 디렉터리에 저장합니다.

```
mail3.example.com> saveconfig
Do you want to include passphrases? Please be aware that a configuration without passphrases

will fail when reloaded with loadconfig.  [N]> y
The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
 directory.
mail3.example.com>
```

loadconfig 명령

어플라이언스에 새 구성 정보를 로드하려면 loadconfig 명령을 사용합니다. 2가지 방법 중 하나로 정보를 로드할 수 있습니다.

- configuration 디렉터리에 정보를 배치하고 업로드
- CLI에 직접 구성 정보 붙여넣기

자세한 내용은 구성 파일 로드, 481 페이지를 참조하십시오.

rollbackconfig 명령

이전에 커밋한 구성으로 롤백 , 483 페이지를 참조하십시오.

publishconfig 명령

구성 마스터 변경사항을 게시하려면 publishconfig 명령을 사용합니다. 구문은 다음과 같습니다.

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

여기서 *config_master*는 지원되는 구성 마스터이며 http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html에서 해당 릴리스의 릴리즈 노트에 있는 호환성 매트릭스에 나열되어 있습니다. 이 키워드는 필수 항목입니다. *job_name* 키워드는 선택 사항이며, 지정되지 않으면 생성됩니다.

키워드 *host_list*는 게시할 WSA의 호스트 이름 또는 IP 주소 목록이며, 지정되지 않으면 구성 마스터에 지정된 모든 호스트에 게시됩니다. 선택 사항인 *host_ip*에서는 여러 호스트 IP 주소가 쉼표로 구분될 수도 있습니다.

publishconfig명령의 성공을 확인하려면 smad_logs 파일을 점검합니다. Security Management Appliance GUI에서 **Web(웹) > Utilities(유틸리티) > Web Appliance Status(웹 어플라이언스 상태)**에서도 기록 게시가 성공했음을 확인할 수 있습니다. 이 페이지에서 기록 게시 세부사항을 표시할 웹 어플라이언스를 선택합니다. 또는 **Web(웹) > Utilities(유틸리티) > Publish(게시) > Publish History(기록 게시)**에서 기록 게시 페이지로 이동할 수 있습니다.

trailblazerconfig 명령

trailblazerconfig 명령을 사용하여 새로운 웹 인터페이스의 HTTP 및 HTTPS 포트를 통해 수신 및 발신 연결을 라우팅할 수 있습니다.

참고 새로운 웹 인터페이스에서만 CLI를 사용하여 trailblazerconfig 명령을 활성화할 수 있습니다. 레거시 웹 인터페이스 또는 엔드 유저 스팸 격리 포털은 영향을 받지 않습니다.

다음 단계 중 하나를 수행하여 브라우저에서 탐색을 원활하게 수행할 수 있습니다.

- 웹 인터페이스에서 사용되는 인증서를 수락하고 새 브라우저 창에서 URL 구문 https://hostname:<https_api_port>(예: https://some.example.com:6443)를 사용하여 인증서를 수락합니다. 여기서 <https_api_port>는 **Network(네트워크) > IP Interfaces(IP 인터페이스)**에 구성된 AsyncOS API HTTPS 포트입니다. 또한 API 포트(HTTP/HTTPS)가 방화벽에서 열려 있는지 확인합니다.
- 기본적으로 trailblazerconfig CLI 명령은 어플라이언스에서 활성화됩니다. HTTP/HTTPS 포트가 방화벽에서 열려 있는지 확인합니다. 또한 어플라이언스에 액세스하기 위해 지정한 호스트 이름을 DNS 서버에서 확인할 수 있는지 확인합니다.

  trailblazerconfig CLI 명령이 비활성화된 경우 다음 문제를 방지하기 위해 CLI를 사용하여 trailblazerconfig > enable 명령을 실행할 수 있습니다.

  - 특정 브라우저에서 API 포트에 대해 여러 인증서를 추가해야 합니다.

- 스팸 격리, 허용 목록 또는 차단 목록 페이지를 새로 고칠 때 레거시 웹 인터페이스로 리디렉션됩니다.
- Advanced Malware Protection 보고서 페이지의 메트릭 표시줄에 데이터가 포함되어 있지 않습니다.

구문은 다음과 같습니다.

```
trailblazerconfig enable <https_port> <http_port>
trailblazerconfig disable
trailblazerconfig status
```

여기서 각 항목은 다음을 나타냅니다.

'enable'은 기본 포트(HTTPS: 4431 또는 HTTP: 801)에서 trailblazer를 실행합니다.

'disable'은 trailblazer를 종료합니다.

'status'는 trailblazer의 상태를 확인합니다.

참고 어플라이언스에서 `trailblazerconfig` 명령을 활성화한 경우 요청 URL에는 호스트 이름에 추가된 HTTP/HTTPS 포트 번호가 포함됩니다.

CLI를 사용하여 구성 변경 사항 업로드

단계 **1** CLI 외부에서 어플라이언스의 configuration 디렉토리에 액세스할 수 있는지 확인합니다. 자세한 내용은 IP 인터페이스 및 어플라이언스 액세스, 547 페이지를 참조하십시오.

단계 **2** 어플라이언스의 configuration 디렉터리에 전체 구성 파일 또는 구성 파일의 하위 섹션을 배치하거나 `saveconfig` 명령을 사용하여 생성한 기존 구성을 편집합니다.

단계 **3** CLI 내에서 `loadconfig` 명령을 사용하여 2단계에서 디렉토리에 배치한 구성 파일을 로드하거나 텍스트(XML 구문)를 CLI에 직접 붙여 넣습니다.

이 예제에서는 이름이 changed.config.xml인 파일을 업로드하고 변경 사항을 커밋합니다.

예제:

```
mail3.example.com>
1
oadconfig
1. Paste via CLI
2. Load from file
[1]> 2
Enter the name of the file to import:
[]> changed.config.xml
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

이 예제에서는 새 구성 파일을 명령줄에 직접 붙여 넣습니다. 붙여넣기 명령을 종료하려면 빈 행에서 Ctrl-D를 눌러야 합니다. 그런 다음 시스템 설정 마법사를 사용하여 기본 호스트 이름, IP 주소, 기본 게이트웨이 정보를 변경합니다. (자세한 내용은 시스템 설정 마법사 실행, 25 페이지를 참조하십시오.) 마지막으로 변경 사항을 커밋합니다.

예제:

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 1
Paste the configuration file now. Press CTRL-D on a blank line when done.
[The configuration file is pasted until the end tag
</config>
. Control-D is entered on a separate line.]
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings
```

디스크 공간 관리

조직에서 사용하는 기능에 가용 디스크 공간을 최대 한도 내에서 할당할 수 있습니다.

(가상 어플라이언스 전용) 사용 가능한 디스크 공간 늘리기

ESXi 5.5 및 VMFS 5를 실행하는 가상 어플라이언스의 경우 2TB가 넘는 디스크 공간을 할당할 수 있습니다. ESXi 5.1을 실행하는 어플라이언스의 경우 제한은 2TB입니다.

참고 ESXi의 디스크 공간 감소는 지원되지 않습니다. 자세한 내용은 VMware 문서를 참조하십시오.

가상 어플라이언스 인스턴스에 디스크 공간을 추가하려면

시작하기 전에

필요한 디스크 공간 증가를 신중하게 결정합니다.

단계 **1** Cisco Content Security Management Appliance 인스턴스를 줄입니다.

단계 **2** VMware에서 제공하는 유틸리티 또는 관리 도구를 사용하여 디스크 공간을 늘립니다.

VMware 문서에서 가상 디스크 구성 변경에 대한 정보를 참조하십시오.

ESXi 5.5에 대한 정보는 다음 위치에서 사용할 수 있습니다. http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html

단계 **3** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **4** **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Disk Management**(디스크 관리)로 이동하여 변경사항이 적용되었음을 확인합니다.

디스크 공간, 할당량 및 사용률 보기

변경 후	수행해야 할 작업
어플라이언스에서 사용 가능한 총 디스크 공간 보기	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Disk Management**(디스크 관리)를 선택합니다. "Total Space Allocated"의 값(예:184G/204G)을 확인합니다.
Security Management Appliance의 모니터링 서비스 각각에 할당되고 현재 사용 중인 디스크 공간의 양 보기	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Disk Management**(디스크 관리)를 선택합니다.
현재 사용 중인 격리에 대한 할당량의 비율 표시	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 서비스) > **System Status**(시스템 상태)를 선택하고 Centralized Services(중앙 서비스) 섹션을 살펴봅니다.

디스크 공간 최대값 및 할당량 정보

참고 Security Management Appliance의 중앙 집중식 보고 디스크 공간은 이메일 및 웹 데이터 모두에 사용됩니다. 중앙 이메일 보고 또는 중앙 웹 보고 중 하나를 활성화할 경우 이 공간 모두 활성화된 기능의 전용이 됩니다. 둘 다 활성화할 경우 이메일 및 웹 보고 데이터가 공간을 공유하며 선착순으로 할당받습니다.

- 중앙 웹 보고를 활성화했지만 보고에 할당된 디스크 공간이 없을 경우 중앙 웹 보고는 디스크 공간이 할당될 때까지 작동하지 않습니다.
- 기타 할당량을 현재 사용량보다 낮은 수준으로 줄이기에 앞서 불필요한 데이터를 삭제해야 합니다. 기타 할당량에 대한 디스크 공간 관리 , 489 페이지를 참조하십시오.
- 정책, 바이러스, 바이러스 격리를 위해 디스크 공간을 관리하는 방법에 대한 자세한 내용은 정책, 바이러스 및 Outbreak 격리를 위한 디스크 공간 할당 , 321 페이지 및 격리에서 메시지의 보유 시간 , 321 페이지를 참조하십시오.
- 기타 데이터 유형은 기존 할당량을 현재 사용량보다 낮출 경우 모든 데이터가 새 할당량에 수용될 때까지 가장 오래된 데이터부터 삭제됩니다.
- 새 할당량이 현재 사용된 디스크 공간보다 클 경우 데이터가 사라지지 않습니다.
- 할당량을 0으로 설정하면 어떤 데이터도 보존하지 않습니다.

디스크 공간에 대한 알림을 수신하는지 확인

Miscellaneous(기타) 디스크 사용량이 할당량의 75%에 도달하면 경고 레벨에서 시스템 알림을 수신하기 시작합니다. 이러한 알림을 받으면 조치를 취해야 합니다.

이러한 알림을 받도록 하려면 경고 관리, 464 페이지 섹션을 참조하십시오.

기타 할당량에 대한 디스크 공간 관리

기타 할당량은 시스템 데이터 및 사용자 데이터를 포함합니다. 시스템 데이터는 삭제할 수 없습니다. 관리할 수 있는 사용자 데이터에는 다음과 같은 파일 유형이 포함됩니다.

관리할 내용	수행해야 할 작업
로그 파일	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**로 이동하고 • Size(크기) 열 제목을 클릭하여 어떤 로그에서 가장 많은 디스크 공간을 사용하는지 확인합니다. • 생성되고 있는 모든 로그 서브스크립션이 필요한지 확인합니다. • 로그 레벨이 필요 이상으로 자세하지 않은지 확인합니다. • 가능한 경우 롤오버 파일 크기를 줄입니다.
패킷 캡처	**Help and Support(도움말 및 지원)**(화면의 오른쪽 상단 근처) > **Packet Capture(패킷 캡처)**로 이동합니다. 불필요한 캡처를 삭제합니다.
구성 파일 (이러한 파일은 디스크 공간 사용량이 많지 않을 수 있습니다.)	FTP를 통해 어플라이언스의 /data/pub 디렉터리로 이동합니다. 어플라이언스에 대한 FTP 액세스 구성 방법은 다음을 참조하십시오. FTP를 통한 어플라이언스 액세스, 549 페이지
할당량 크기	[새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다. **System Administration(시스템 관리) > Disk Management(디스크 관리)**로 이동합니다.

디스크 공간 할당량 재할당

사용하지 않는 기능에 디스크 공간이 할당된 경우 또는 특정 기능에서는 자주 디스크 공간이 부족해지는데 다른 기능은 여유 공간이 있을 경우 디스크 공간을 재할당할 수 있습니다.

모든 기능에 대해 추가 공간이 필요할 경우 하드웨어를 업그레이드하거나 가상 어플라이언스에 추가 디스크 공간을 할당하는 것이 좋습니다. (가상 어플라이언스 전용) 사용 가능한 디스크 공간 늘리기 , 487 페이지를 참조하십시오.

시작하기 전에

- 디스크 할당량을 변경하면 기존 데이터 및 기능의 가용성에 영향을 미칠 수 있습니다. 디스크 공간 최대값 및 할당량 정보, 489 페이지의 정보를 참조하십시오.
- 격리된 메시지를 수동으로 해제하거나 삭제하는 방법으로 임시로 공간을 생성할 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 2 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Disk Management**(디스크 관리)를 선택합니다.

단계 3 **Edit Disk Quotas**(디스크 할당량 수정)를 클릭합니다.

단계 4 **Edit Disk Quotas**(디스크 할당량 수정) 페이지에서 각 서비스에 할당된 디스크 공간의 양(기가바이트)을 입력합니다.

단계 5 **Submit**을 클릭합니다.

단계 6 확인 대화 상자에서 **Set New Quotas**(새 할당량 설정)를 클릭합니다.

단계 7 **Commit**(커밋)을 클릭하여 변경사항을 커밋합니다.

ESA 시스템 상태 그래프의 참조 임계값 조정

참고 이 임계값과 관련된 알림을 수신하려면 각 매니지드 Email Security Appliance에서 임계값을 구성합니다. 자세한 내용은 Email Security Appliance 릴리스의 사용 설명서 또는 온라인 도움말에서 시스템 상태 임계값 구성에 대한 내용을 참조하십시오. 개별 어플라이언스에서 온디맨드 시스템 상태 점검도 실행할 수 있습니다. 어플라이언스 상태 점검에 대한 자세한 내용은 Email Security Appliance 릴리스의 사용 설명서 또는 온라인 도움말을 참조하십시오.

단계 1 [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 2 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **System Health**(시스템 상태)를 클릭합니다.

단계 3 **Edit Settings**(설정 수정)를 클릭합니다.

단계 4 옵션을 구성합니다.

옵션	설명
전체 CPU 사용	기본값: 85%
메시지 페이지 스와핑	기본값: 5000페이지
작업 대기열의 최대 메시지	기본값: 500개 메시지

단계 5 변경 사항을 제출 및 커밋합니다.

SAML 2.0을 사용하는 SSO

• SSO 및 SAML 2.0 정보, 492 페이지

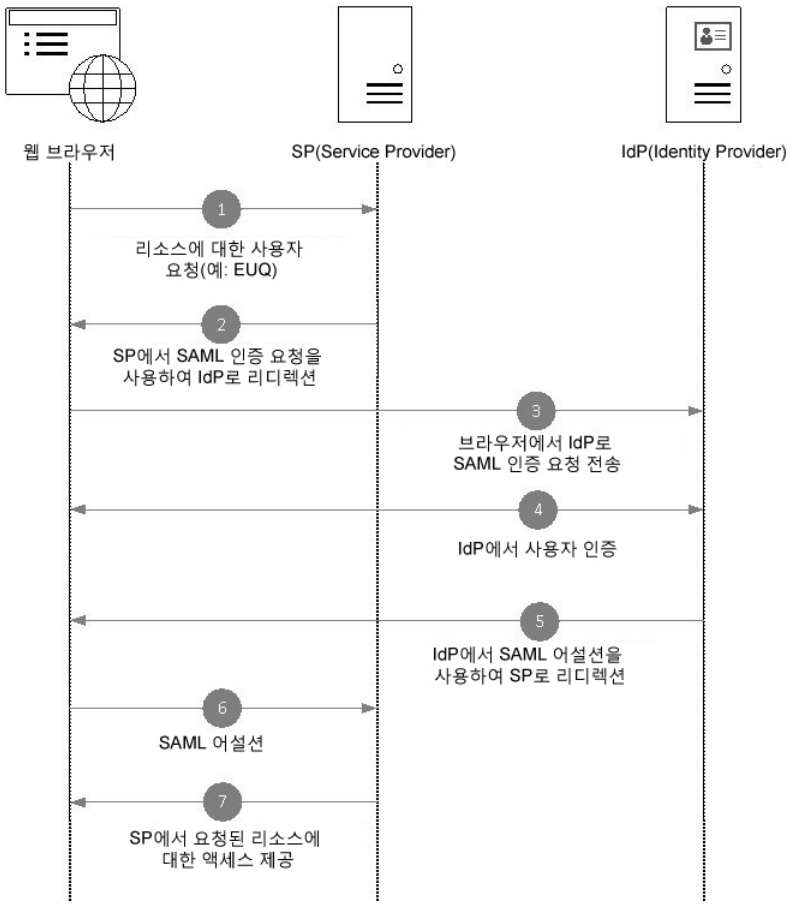
SSO 및 SAML 2.0 정보

Cisco Content Security Management Appliance는 이제 SAML 2.0 SSO를 지원하므로 엔드 유저가 조직 내에서 다른 SAML 2.0 SSO가 활성화된 서비스에 액세스하는 데 사용되는 크리덴셜과 같은 크리덴셜을 사용하여 스팸 격리에 액세스할 수 있습니다. 예를 들어, Ping Identity를 SAML IdP(Identity Provider)로 활성화하고 SAML 2.0 SSO가 활성화된 Rally, Salesforce, Dropbox에 계정이 있는 경우, Cisco Content Security Management Appliance에서 SAML 2.0 SSO를 SP(서비스 제공자)로 지원하도록 구성하면 엔드 유저가 한 번만 로그인하여 스팸 격리를 포함한 이 모든 서비스에 액세스할 수 있습니다.

SAML 2.0 SSO 워크플로

SAML 2.0 SSO 워크플로가 다음 그림에 표시되어 있습니다.

그림 ***20: SAML 2.0 SSO*** 워크플로



워크플로

1. 엔드 유저는 웹 브라우저를 사용하여 서비스 제공자(어플라이언스)에게 리소스를 요청합니다. 예를 들어, 엔드 유저는 스팸 알림에서 스팸 격리 링크를 클릭합니다.
2. 서비스 제공자는 SAML 인증 요청을 통해 웹 브라우저에 요청을 리디렉션합니다.
3. 웹 브라우저는 SAML 인증 요청을 IdP(Identity Provider)에 릴레이합니다.
4. IdP(Identity Provider)는 엔드 유저를 인증합니다. IdP(Identity Provider)가 엔드 유저에 로그인 페이지를 표시하고 엔드 유저가 로그인합니다.
5. IdP(Identity Provider)가 SAML 어설션을 생성하고 이를 다시 웹 브라우저에 전송합니다.
6. 웹 브라우저는 SAML 어설션을 서비스 제공자에게 릴레이합니다.
7. 서비스 제공자가 요청된 리소스에 대한 액세스를 부여합니다.

SAML 2.0에 대한 지침 및 제한 사항

Logout

엔드 유저가 스팸 격리에서 로그아웃할 경우 다른 SAML 2.0 SSO가 활성화된 애플리케이션에서는 로그아웃되지 않습니다.

일반

Cisco Content Security Management Appliance에서는 서비스 제공자 및 IdP(Identity Provider) 인스턴스를 하나만 구성할 수 있습니다.

관리자의 스팸 격리 액세스

스팸 격리에 대해 SSO를 활성화한 경우 항상 염두에 관리자가 더 이상 스팸 격리 URL(http://<appliance_hostname>:<port>)을 사용하여 스팸 격리에 액세스할 수 없으므로 주의하십시오. 관리자는 웹 인터페이스(**Email**(이메일) > **Message Quarantine**(메시지 격리) > **Spam Quarantine**(스팸 격리))를 사용하여 스팸 격리에 액세스할 수 있습니다.

스팸 격리에 대해 SSO를 구성하는 방법

	수행해야 할 작업	추가 정보
1단계	사전 요구 사항을 검토합니다.	사전 요구 사항, 494 페이지
2단계	어플라이언스를 서비스 제공자로 구성합니다.	Cisco Content Security Management Appliance 서비스 제공자로 구성, 494 페이지

	수행해야 할 작업	추가 정보
3단계	[IDP에서] 어플라이언스와 함께 사용할 IdP(Identity Provider)를 구성합니다.	IdP(Identity Provider)를 Cisco Content Security Management Appliance와 통신하도록 구성, 496 페이지
4단계	어플라이언스에서 IdP(Identity Provider) 설정을 구성합니다.	Cisco Content Security Management Appliance에서 서비스 제공자 설정 구성, 498 페이지
5단계	어플라이언스에서 스팸 격리에 대해 SSO 활성화	스팸 격리에 대해 SSO 활성화, 499 페이지
6단계	새 인증 메커니즘에 대해 엔드 유저에게 알립니다.	

사전 요구 사항

- 조직에서 사용하는 IdP(Identity Provider)를 Cisco Content Security Management Appliance에서 지원하는지 여부를 확인합니다. 지원되는 IdP(Identity Provider)는 다음과 같습니다.
  - Microsoft AD FS(Active Directory 통합 서비스) 2.0
  - Ping Identity PingFederate 7.2
  - Cisco Web Security Appliance 9.1
- 어플라이언스와 IdP(Identity Provider) 간의 통신을 보호하는 데 필요한 다음 인증서를 가져옵니다.
  - 어플라이언스에서 SAML 인증 요청에 서명하도록 하려는 경우 또는 IdP(Identity Provider)가 SAML 어설션을 암호화하도록 하려는 경우 셀프 서명 인증서 또는 신뢰할 수 있는 CA 및 연결된 개인 키의 인증서를 가져와야 합니다.
  - IdP(Identity Provider)가 SAML 어설션에 서명하도록 하려면 IdP(Identity Provider)의 인증서를 가져옵니다. 어플라이언스는 이 인증서를 사용하여 서명된 SAML 어설션을 확인합니다.

Cisco Content Security Management Appliance 서비스 제공자로 구성

시작하기 전에

사전 요구 사항, 494 페이지을/를 검토합니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **SAML**을 선택합니다.

단계 **3** Service Provider(서비스 제공자) 섹션에서 **Add Service Provider**(서비스 제공자 추가)클릭합니다.

단계 **4** 다음 세부사항을 입력합니다.

필드	설명
Profile Name(프로필 이름)	서비스 제공자 프로필의 이름을 입력합니다.
구성 설정	
엔터티 ID	서비스 제공자의 전역 고유 이름을 입력합니다(이 경우 어플라이언스). 서비스 제공자 엔터티 ID 형식은 일반적으로 URI입니다.
이름 ID 형식	IdP(Identity Provider)가 SAML 어설션에서 사용자를 지정하는 데 사용해야 할 형식입니다. 이 필드는 구성할 수 없습니다. IdP(Identity Provider)를 구성하는 동안 이 값이 필요합니다.
어설션 소비자 URL	인증이 완료된 후 IdP(Identity Provider)가 SAML 어설션을 보내는 URL입니다. 이 경우, 이것은 스팸 격리의 URL입니다. 이 필드는 구성할 수 없습니다. IdP(Identity Provider)를 구성하는 동안 이 값이 필요합니다.
SP 인증서	참고 개인 키 파일은 .pem 형식이어야 합니다. 인증 요청 서명 어플라이언스가 SAML 인증 요청에 서명하도록 하려면 다음 작업을 수행합니다. **1.** 인증서 및 연결된 개인 키를 업로드합니다. **2.** 개인 키 대한 암호를 입력합니다. **3.** **Sign Request(**서명 요청**)**를 선택합니다. 암호화된 어설션 암호 해독 IdP(Identity Provider)에서 SAML 어설션을 암호화하도록 구성하려면 다음 작업을 수행합니다. **1.** 인증서 및 연결된 개인 키를 업로드합니다. **2.** 개인 키 대한 암호를 입력합니다.
서명 어설션	IdP(Identity Provider)에서 SAML 어설션에 서명하도록 하려면 **Sign Assertions(**서명 어설션**)**를 선택합니다. 이 옵션을 선택하는 경우 어플라이언스에 IdP(Identity Provider)의 인증서를 추가해야 합니다. Cisco Content Security Management Appliance에서 서비스 제공자 설정 구성, 498 페이지를 참조하십시오.
조직 세부 정보	조직 세부 정보를 입력합니다. IdP(Identity Provider)에서 오류 로그에서 이 정보를 사용합니다.

필드	설명
기술 문의	기술 문의처의 이메일 주소를 입력하십시오. IdP(Identity Provider)에서 오류 로그에서 이 정보를 사용합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** SSO Settings(SSO 설정) 페이지에 표시되는 서비스 제공자 메타데이터(엔티티 ID 및 어설션 고객 URL)와 Service Provider Settings(서비스 제공자 설정) 페이지에 표시되는 Name ID Format(이름 ID 형식)을 기록합니다. IdP(Identity Provider)에서 서비스 제공자 설정을 구성하는 동안 다음 세부 정보가 필요합니다.

선택적으로 메타데이터를 파일로 내보낼 수 있습니다. **Export Metadata(**메타데이터 내보내기**)**를 클릭하고 메타데이터 파일을 저장합니다. 일부 IdP(Identity Provider)를 통해 메타데이터 파일에서 서비스 제공자 세부 정보를 로드할 수 있습니다.

다음에 수행할 작업

IdP(Identity Provider)를 어플라이언스와 통신하도록 구성합니다. IdP(Identity Provider)를 Cisco Content Security Management Appliance와 통신하도록 구성, 496 페이지를 참조하십시오.

IdP(Identity Provider)를 Cisco Content Security Management Appliance와 통신하도록 구성

시작하기 전에

다음을 확인하십시오.

- 어플라이언스를 서비스 제공자로 구성합니다. Cisco Content Security Management Appliance 서비스 제공자로 구성, 494 페이지를 참조하십시오.
- 서비스 제공자 메타데이터 정보를 복사했거나 메타데이터 파일을 내보냈습니다. Cisco Content Security Management Appliance 서비스 제공자로 구성, 494 페이지를 참조하십시오.

단계 **1** IdP(Identity Provider)에서 다음 중 하나를 수행합니다.

- 서비스 제공자(어플라이언스)의 세부 정보를 수동으로 구성합니다.
- 일부 IdP(Identity Provider)를 통해 메타데이터 파일에서 서비스 제공자 세부 정보를 로드할 수 있으면 메타데이터 파일을 가져옵니다.

어플라이언스에서 SAML 인증 요청에 서명하도록 구성했거나 SAML 어설션을 암호화하려는 경우 IdP(Identity Provider)에 관련 인증서를 추가해야 합니다.

IdP(Identity Provider)별 지침을 참조하십시오.

- AD FS 2.0을 Cisco Content Security Management Appliance와 통신하도록 구성, 497 페이지
- PingFederate 7.2를 Cisco Content Security Management Appliance와 통신하도록 구성, 497 페이지

- **AsyncOS for Cisco Web Security Appliances** 사용 설명서 의 어플라이언스를 *IdP(Identity Provider)*로 구성 섹션 http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

단계 **2** IdP(Identity Provider) 메타데이터를 기록하거나 메타데이터를 파일로 내보냅니다.

다음에 수행할 작업

어플라이언스에서 IdP(Identity Provider) 설정을 구성합니다. Cisco Content Security Management Appliance에서 서비스 제공자 설정 구성, 498 페이지를 참조하십시오.

AD FS 2.0을 Cisco Content Security Management Appliance와 통신하도록 구성

AD FS 2.0을 어플라이언스와 통신하도록 구성하려면 다음과 같은 높은 수준의 작업을 수행해야 합니다. 자세한 전체 지침은 Microsoft 문서를 참조하십시오.

- 서비스 제공자(어플라이언스)의 어설션 소비자 URL을 신뢰 당사자로 추가합니다.
- Relaying Party Trusts(신뢰 당사자 트러스트) > Properties(속성) > Identifiers(ID) > Relaying Party Identifier(신뢰 당사자 ID) 아래에서 서비스 제공자(어플라이언스)의 엔터티 ID를 입력합니다. 이 값은 어플라이언스의 Service Provider(서비스 제공자) 설정에 지정된 엔터티 ID 값과 동일해야 합니다.
- 서비스 제공자(어플라이언스)에서 서명된 SAML 인증 요청을 전송하도록 구성한 경우, Relaying Party Trusts(신뢰 당사자 트러스트) > Properties(속성) > Signature(서명) 아래에서 서비스 제공자의 인증서(인증 요청에 서명하는 데 사용)를 .cer 형식으로 업로드합니다.
- AD FS에서 암호화된 SAML 어설션을 전송하도록 구성하려면 Relaying Party Trusts(신뢰 당사자 트러스트) > Properties(속성) > Encryption(암호화) 아래에서 서비스 제공자(어플라이언스)의 인증서를 .cer 형식으로 업로드합니다.
- Relaying Party Trusts(신뢰 당사자 트러스트) > Properties(속성) > Advanced(고급) 아래에서 보안 해시 알고리즘을 SHA-1로 설정합니다.
- 이메일 주소의 LDAP 특성을 발신 클레임 유형(이메일 주소)으로 전송하도록 클레임 규칙을 편집하고 발급 변환 규칙을 추가합니다.
- 응답에 SPNameQualifier를 포함하도록 맞춤형 규칙을 추가합니다. 다음은 샘플 맞춤형 규칙입니다.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
 =
 c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<appliance-hostname>:83");
```

PingFederate 7.2를 Cisco Content Security Management Appliance와 통신하도록 구성

PingFederate 7.2를 어플라이언스와 통신하도록 구성하려면 다음과 같은 높은 수준의 작업을 수행해야 합니다. 자세한 전체 지침은 Ping Identity 설명서를 참조하십시오.

- 프로토콜 설정 아래에서 서비스 제공자(어플라이언스)의 어설션 소비자 URL을 엔드포인트로 추가합니다.
- SP Connection(SP 연결) > General Info(일반 정보) > Partner's Entity ID(Connection ID)(파트너의 엔터티 ID(연결 ID)) 아래에서 서비스 제공자(어플라이언스)의 엔터티 ID를 입력합니다. 이 값은 어플라이언스의 Service Provider(서비스 제공자) 설정에 지정된 엔터티 ID 값과 동일해야 합니다.
- 서명된 SAML 인증 요청을 전송하도록 서비스 제공 자가 (어플라이언스)를 구성한 경우 서명 확인 섹션 아래에서 서비스 제공자의 인증서를 업로드 (SP 연결 > 크리덴셜 > 서명 확인 > 서명 확인 인증서)입니다.
- PingFederate에서 암호화된 SAML 어설션을 전송하도록 구성하려면 Signature Verification(서명 확인) 섹션(SP Connection(SP 연결) > Credentials(크리덴셜) > Signature Verification(서명 확인) > Select XML Encryption Certificate(XML 암호화 인증서 선택)) 아래에서 서비스 제공자(어플라이언스)의 인증서를 업로드합니다.
- LDAP 특성 - 이메일 주소를 전송하도록 특성 계약을 편집합니다(Attribute Sources & User Lookup(특성 소스 및 사용자 조회) > Attribute Contract Fulfillment(특성 계약 실행)).

Cisco Content Security Management Appliance에서 서비스 제공자 설정 구성

시작하기 전에

다음을 확인하십시오.

- IdP(Identity Provider)를 어플라이언스와 통신하도록 구성합니다. IdP(Identity Provider)를 Cisco Content Security Management Appliance와 통신하도록 구성, 496 페이지를 참조하십시오.
- IdP(Identity Provider) 메타데이터 정보를 복사했거나 메타데이터 파일을 내보냈습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**)** > **System Administration(**시스템 관리**)** > **SAML**을 선택합니다.

단계 **3** IdP(Identity Provider) 섹션에서 **Add Identity Provider(IdP(Identity Provider)** 추가**)**를 클릭합니다.

단계 **4** 다음 세부사항을 입력합니다.

필드	설명
Profile Name(프로필 이름)	IdP(Identity Provider) 프로필의 이름을 입력합니다.
구성 설정(IdP(Identity Provider) 설정을 수동으로 구성)	
엔터티 ID	IdP(Identity Provider)의 전역 고유 이름을 입력합니다. IdP(Identity Provider) 엔터티 ID 형식은 일반적으로 URI입니다.
SSO URL	서비스 제공자가 SAML 인증 요청을 전송해야 할 URL을 지정합니다.
인증서	IdP(Identity Provider)가 SAML 어설션에 서명하는 경우, IdP(Identity Provider)의 서명 인증서를 업로드해야 합니다.

필드	설명
구성 설정(IdP(Identity Provider) 메타데이터 가져오기)	
IDP 메타데이터 가져오기	**Import Metadata**(메타데이터 가져오기)를 클릭하고 메타데이터 파일을 선택합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

스팸 격리에 대해 SSO 활성화, 499 페이지

스팸 격리에 대해 **SSO** 활성화

시작하기 전에

다음을 확인하십시오.

- **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **SAML** 페이지에서 모든 설정을 구성했는지 확인합니다.
- 스팸 격리를 활성화했는지 확인합니다. 스팸 격리, 279 페이지를 참조하십시오.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance**(관리 어플라이언스) > **Centralized Services**(중앙 집중식 서비스) > **Spam Quarantine**(스팸 격리)을 선택합니다.

단계 **3** **Edit Settings**(설정 수정)를 클릭하고 End-User Quarantine Access(엔드 유저 격리 액세스) 섹션으로 스크롤합니다.

단계 **4** 엔드 유저 격리 액세스를 활성화해야 합니다.

단계 **5** 엔드 유저 인증 방법을 **SAML2.0**로 설정합니다.

단계 **6** (선택 사항) 메시지가 릴리스되기 전에 메시지 본문을 표시할지 여부를 지정합니다.

단계 **7** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

새 인증 메커니즘에 대해 엔드 유저에게 알립니다.

보기 맞춤화

- 즐겨찾기 페이지 사용 , 500 페이지

• 기본 설정 , 500 페이지
• 웹 인터페이스 렌더링 향상 , 501 페이지

즐겨찾기 페이지 사용

(로컬 인증 관리자 사용자만) 가장 많이 사용하는 페이지의 빠른 액세스 목록을 만들 수 있습니다.

변경 후	수행해야 할 작업
즐겨찾기 목록에 페이지 추가	추가할 페이지로 이동하고, 창의 상단 오른쪽에 있는 My Favorites(내 즐겨찾기) 메뉴에서 **Add This Page To My Favorites(**이 페이지를 내 즐겨찾기에 추가**)**를 선택합니다. My Favorites(내 즐겨찾기)를 변경하는 경우에는 커밋이 필요하지 않습니다.
즐겨찾기 순서 바꾸기	**My Favorites(**내 즐겨찾기**) > View All My Favorites(**내 즐겨찾기 모두 보기**)**를 선택하고 즐겨찾기를 원하는 순서로 끌어옵니다.
즐겨찾기 페이지, 이름, 설명 수정	**My Favorites(**내 즐겨찾기**) > View All My Favorites(**내 즐겨찾기 모두 보기**)**를 선택하고 수정할 즐겨찾기의 이름을 클릭합니다.
즐겨찾기 삭제	**My Favorites(**내 즐겨찾기**) > View All My Favorites(**내 즐겨찾기 모두 보기**)**를 선택하고 즐겨찾기를 삭제합니다.
즐겨찾기 페이지로 이동	창의 오른쪽 상단 근처에 있는 **My Favorites(**내 즐겨찾기**)** 메뉴에서 페이지를 선택합니다.
기본 인터페이스로 돌아가기	즐겨찾기를 선택하거나 페이지 맨 아래의 **Return to previous page(**이전 페이지로 돌아가기**)**를 클릭합니다.

기본 설정

Security Management Appliance에서 구성된 관리 사용자

로컬 인증 사용자는 사용자가 Security Management Appliance에 로그인할 때마다 적용되는 다음 기본 설정을 선택할 수 있습니다.

- 언어(GUI에 적용)
- 랜딩 페이지(로그인하면 표시되는 페이지)
- 보고서 페이지의 기본 시간 범위(사용 가능한 옵션은 이메일 및 웹 보고 페이지에서 제공되는 시간 범위의 하위 집합임)
- 보고서 페이지의 테이블에 표시되는 행의 수

각 옵션은 사용자 역할에 따라 달라집니다.

이 기본 설정을 하려면 **Options(**옵션**) > Preferences(**기본 설정**)**를 선택합니다. 옵션 메뉴는 GUI 창의 오른쪽 위에 있습니다. 완료하면 변경사항을 제출합니다. 커밋이 필요하지 않습니다.

팁 기본 설정 페이지에 액세스하기 전에 보고 있던 페이지로 돌아가려면 페이지 맨 아래의 **Return to previous page(**이전 페이지로 돌아가기**)** 링크를 클릭합니다.

외부에서 인증된 사용자

외부에서 인증된 사용자는 Options(옵션) 메뉴에서 직접 표시 언어를 선택할 수 있습니다.

웹 인터페이스 렌더링 향상

웹 인터페이스 렌더링을 개선하려면 Internet Explorer 호환성 모드 재정의를 활성화하는 것이 좋습니다.

참고 이 기능 활성화가 조직의 정책과 맞지 않으면 이 기능을 비활성화할 수 있습니다.

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**)** > **System Administration(**시스템 관리**)** > **General Settings(**일반 설정**)**를 선택합니다.

단계 **3** **Override IE Compatibility Mode(IE** 호환성 모드 재정의**)** 확인란을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

어플라이언스에 활성화된 서비스의 상태 다시 시작 및 보기

CLI에서 `diagnostic > services` sub 명령을 사용하여 다음 작업을 수행할 수 있습니다.

- 어플라이언스를 재부팅하지 않고도 어플라이언스에 활성화된 서비스를 다시 시작합니다.
- 어플라이언스에 활성화된 서비스의 상태를 봅니다.

예**:** 보고 서비스의 상태 보기

다음 예에서는 어플라이언스에 활성화된 보고 서비스의 상태를 보기 위해 `services` 명령이 사용됩니다.

```
mail.example.com> diagnostic
```

```
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> reporting

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

Reporting has been up for 28d 20h 45m 35s.
```

예: 메시지 추적 서비스 다시 시작

다음 예에서는 어플라이언스에 활성화된 메시지 추적 서비스의 상태를 보기 위해 `services` 명령이 사용됩니다.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> tracking

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart
```

16 장

로깅

이 장에는 다음 섹션이 포함되어 있습니다.

로깅 개요

로그 파일은 시스템 활동에 대한 일반 작업은 물론 예외도 기록합니다. 로그 파일을 사용하여 Cisco Content Security Appliance를 모니터링하고 문제를 해결하고 시스템 성능을 평가할 수 있습니다.

대부분의 로그는 일반 텍스트(ASCII) 형식으로 기록되지만 추적 로그는 리소스 효율성을 위해 이진 형식으로 기록됩니다. ASCII 텍스트 정보는 텍스트 편집기에서 읽을 수 있습니다.

로깅 대 보고

로깅 데이터를 사용하면 메시지 플로우를 디버그하고, FTP 연결 세부사항, HTTP 로그 파일, 규정 준수 아카이빙 같은 기본적인 일상 운영 정보를 확인할 수 있습니다.

Email Security Appliance에서 직접 로깅 데이터에 액세스할 수도 있고, 보관하거나 읽기 위해 외부 FTP 서버로 전송할 수도 있습니다. 로그에 액세스하기 위해 어플라이언스에 FTP로 연결하거나 백업을 위해 외부 서버에 일반 텍스트 로그를 푸시할 수 있습니다.

로그 데이터를 보려면 어플라이언스 GUI에서 보고서 페이지를 사용합니다. 어떤 방법으로도 기반 데이터에는 액세스할 수 없으며, 이 데이터는 Cisco Content Security Management Appliance 이외의 다른 곳으로 전송할 수 없습니다.

참고 Security Management Appliance는 스팸 격리 데이터를 제외하고 모든 보고 및 추적에 대한 정보를 가져옵니다. 이 데이터는 ESA에서 푸시됩니다.

로그 검색

로그 파일은 다음 표의 설명대로 파일 전송 프로토콜을 사용하여 검색할 수 있습니다. GUI에서 로그 서브스크립션을 생성하거나 수정할 때 또는 CLI에서 `logconfig` 명령을 사용하여 프로토콜을 설정합니다.

FTP Poll	이 파일 전송 유형에서는 원격 FTP 클라이언트가 로그 파일 검색을 위해 관리자 레벨 또는 운영자 레벨 사용자 이름 및 암호를 사용하여 어플라이언스에 액세스합니다. FTP Poll 방법을 사용하도록 로그 서브스크립션을 구성할 경우 보존할 최대 로그 파일 수를 제시해야 합니다. 최대 한도에 도달하면 시스템에서 가장 오래된 것부터 삭제합니다.
FTP Push	이 파일 전송 유형에서는, Cisco Content Security Appliance가 주기적으로 로그 파일을 원격 컴퓨터의 FTP 서버에 푸시합니다. 서브스크립션에는 사용자 이름, 암호, 원격 컴퓨터의 목적지 디렉터리가 필요합니다. 구성된 롤오버 일정에 따라 로그 파일이 전송됩니다.
SCP Push	이 파일 전송 유형에서는, Cisco Content Security Appliance가 주기적으로 로그 파일을 원격 컴퓨터의 SCP 서버에 푸시합니다. 이 방법을 사용하려면 SSH2 프로토콜을 사용하는 원격 컴퓨터에 SSH SCP 서버가 필요합니다. 서브스크립션에는 원격 컴퓨터의 사용자 이름, SSH 키 및 대상 디렉토리가 필요합니다. 구성된 롤오버 일정에 따라 로그 파일이 전송됩니다.
Syslog Push	이 파일 전송 유형에서는, Cisco Content Security Appliance가 원격 syslog 서버로 로그 메시지를 전송합니다. 이 방법은 RFC 3164를 준수합니다. Syslog 서버에 대한 호스트 이름을 제출하고 UDP 또는 TCP를 로그 전송에 사용해야 합니다. 사용되는 포트는 514입니다. 로그를 위한 기능(facility)을 선택해야 합니다. 그러나 로그 유형의 기본값이 드롭다운 메뉴에 미리 선택되어 있습니다. 텍스트 기반 로그만 syslog push를 사용하여 전송할 수 있습니다.

파일 이름 및 디렉터리 구조

AsyncOS는 로그 서브스크립션에 지정된 로그 이름을 기반으로 각 로그 서브스크립션에 대한 디렉터리를 만듭니다. 디렉터리에 있는 로그의 파일 이름은 로그 서브스크립션에 지정된 파일 이름, 로그

파일이 시작된 시점의 타임스탬프 및 단일 문자 상태 코드로 구성됩니다. 다음 예는 디렉터리 및 파일 이름의 표기 규칙을 보여줍니다.

/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>

상태 코드는 .c("current") 또는 .s("saved")일 수 있습니다. 저장된 상태의 로그 파일만 전송할 수 있습니다.

로그 롤오버 및 전송 예약

로그 서브스크립션을 만들 때 로그가 롤오버되고, 오래된 파일이 전송되고, 새 로그 파일이 생성되는 트리거를 지정할 수 있습니다.

다음 트리거 중에서 선택합니다.

- 파일 크기
- 시간
  - 초, 분, 시간, 일 단위의 지정된 간격.

    값을 입력할 때 화면의 예를 따릅니다.

    복합 간격을 입력하려면(예: 2.5시간) 2h30m의 예를 따릅니다.

    또는
  - 매일, 사용자 지정 시간에

    또는
  - 사용자가 선택한 요일, 사용자가 지정한 시간에

시간을 지정할 경우 24시간 형식을 사용합니다(예: 오후 11시는 23:00).

하루에 여러 롤오버 시간을 예약하려면 쉼표로 구분합니다. 예를 들어 자정과 정오에 로그를 롤오버하려면 00:00, 12:00을 입력합니다.

와일드카드 문자로 별표(*)를 입력합니다. 예를 들어 1시간 30분마다 정확히 로그를 롤오버하려면 *:00, *:30을 입력합니다.

지정된 한도에 도달하거나 또는 크기 및 시간 한도를 모두 구성한 경우 가장 먼저 오는 한도에 도달하면 로그 파일이 롤오버됩니다. FTP poll 전송 방식의 로그 서브스크립션은 파일을 생성하고 어플라이언스의 FTP 디렉터리에 저장합니다. 파일이 검색되거나 시스템에서 로그 파일을 위한 더 많은 공간이 필요할 때까지 이 상태로 유지됩니다.

참고 다음 한도에 도달했을 때 롤오버가 진행 중이라면 새 롤오버는 건너뜁니다. 오류가 로깅되고 알림이 전송됩니다.

로그 파일의 타임스탬프

다음 로그 파일에는 로그 자체의 시작 날짜와 종료 날짜, AsyncOS의 버전 및 GMT 오프셋(로그의 시작 부분에 초 단위로 제공)이 포함됩니다.

- 메일 로그
- 허용 목록/차단 목록 로그
- 시스템 로그

기본적으로 활성화된 로그

Security Management Appliance는 다음 로그 서브스크립션이 활성화된 상태로 사전에 구성됩니다.

표 ***89:*** 사전 구성된 로그 서브스크립션

로그 이름	로그 유형	검색 방법
cli_logs	CLI 감사 로그	FTP Poll
euq_logs	스팸 격리 로그	FTP Poll
euqgui_logs	스팸 격리 GUI 로그	FTP Poll
gui_logs	HTTP 로그	FTP Poll
mail_logs	텍스트 메일 로그	FTP Poll
reportd_logs	보고 로그	FTP Poll
reportqueryd_logs	보고 쿼리 로그	FTP Poll
slbld_logs	허용 목록/차단 목록 로그	FTP Poll
smad_logs	SMA 로그	FTP Poll
system_logs	시스템 로그	FTP Poll
trackerd_logs	추적 로그	FTP Poll

모든 사전 구성된 로그 서브스크립션은 로깅 레벨이 Information(정보)으로 설정되어 있습니다. 로그 레벨에 대한 자세한 내용은 로그 레벨 설정, 528 페이지를 참조하십시오.

적용한 라이센스 키에 따라 추가 로그 서브스크립션을 구성할 수 있습니다. 로그 서브스크립션 생성 및 수정에 대한 자세한 내용은 로그 서브스크립션, 527 페이지를 참조하십시오.

로그 유형

- 로그 유형의 요약, 507 페이지

로그 유형의 요약

로그 서브스크립션은 로그 유형을 이름, 로깅 레벨 및 기타 특성(예: 크기 및 대상 정보)과 연결합니다. 모든 로그 유형에 여러 서브스크립션이 허용됩니다(구성 기록 로그 제외). 로그 유형은 로그에 기록되는 데이터를 결정합니다. 로그 서브스크립션을 만들 때 로그 유형을 선택합니다. 자세한 내용은 로그 서브스크립션, 527 페이지를 참조하십시오.

AsyncOS는 다음 로그 유형을 생성합니다.

표 ***90:*** 로그 유형

로그 유형	설명
인증 로그	인증 로그는 GUI 및 CLI로 Security Management Appliance에 로그인하는 로컬 및 외부 인증 사용자에 대해 성공한 로그인과 실패한 로그인 시도를 기록합니다. 디버그 모드 및 좀 더 자세한 모드에서는 외부 인증이 켜져 있는 경우 모든 LDAP 쿼리가 이 로그에 나타납니다.
백업 로그	백업 로그는 백업 프로세스를 처음부터 끝까지 기록합니다. 백업 예약에 대한 정보는 SMA 로그에 있습니다.
CLI Audit Logs	CLI 감사 로그는 시스템의 모든 CLI 활동을 기록합니다.
구성 기록 로그	구성 기록 로그는 Security Management Appliance에서 무엇이 언제 변경되었는지에 대한 정보를 기록합니다. 사용자가 변경 사항을 커밋할 때마다 새 구성 기록 로그가 생성됩니다.

로그 유형	설명
FTP 서버 로그	FTP 로그는 인터페이스에서 활성화된 FTP 서비스에 대한 정보를 기록합니다. 연결 세부사항 및 사용자 활동이 기록됩니다.
GUI 로그	GUI 로그에는 웹 인터페이스, 세션 데이터, 사용자가 액세스하는 페이지에서 수행된 페이지 새로 고침의 기록이 포함됩니다. gui_log를 사용하면 사용자 활동을 추적하고 GUI에서 사용자에게 표시되는 오류를 조사할 수 있습니다. 오류 추적은 대개 이 로그에 포함됩니다. GUI 로그에는 SMTP 트랜잭션에 대한 정보도 포함됩니다(예: 어플라이언스에서 이메일로 보내는 예약된 보고서에 대한 정보).
HTTP 로그	HTTP 로그는 인터페이스에서 활성화된 HTTP 및 보안 HTTP 서비스에 대한 정보를 기록합니다. GUI는 HTTP를 통해 액세스하므로 GUI의 HTTP 로그는 사실상 CLI 감사 로그와 같습니다. 세션 데이터(예: 새 세션 및 만료된 세션)가 기록되고 GUI에서 액세스한 페이지도 기록됩니다.
Haystack 로그	Haystack 로그는 웹 트랜잭션 추적 데이터 프로세싱을 기록합니다.
텍스트 메일 로그	텍스트 메일 로그는 이메일 시스템의 운영에 대한 정보(예: 메시지 수신, 메시지 전달 시도, 연결 열기 및 닫기, 메시지 반송 등)를 기록합니다. 메일 로그에 첨부 파일 이름이 포함되는 시점에 대한 자세한 내용은 추적 서비스 개요, 263 페이지를 참조하십시오.
LDAP 디버그 로그	System Administration(시스템 관리) > LDAP에서 LDAP를 구성할 때 이 로그를 사용하여 디버깅합니다. 예를 들어 이 로그는 Test Server(서버 테스트) 및 Test Queries(쿼리 테스트) 버튼을 클릭한 결과를 기록합니다. 실패한 LDAP 인증에 대한 자세한 내용은 인증 로그를 참조하십시오.
NTP 로그	NTP 로그는 어플라이언스와 구성된 NTP(Network Time Protocol) 서버 간의 대화를 기록합니다. NTP 서버 구성에 대한 자세한 내용은 시스템 시간 구성, 477 페이지를 참조하십시오.
보고 로그	보고 로그는 중앙 집중식 보고 서비스의 프로세스와 관련된 작업을 기록합니다.
쿼리 보고 로그	보고 쿼리 로그는 어플라이언스에서 실행되는 보고 쿼리와 관련된 작업을 기록합니다.
SMA 로그	SMA 로그는 일반적인 Security Management Appliance 프로세스와 연결된 작업을 기록하며 중앙 집중식 보고, 중앙 집중식 추적 및 스팸 격리 서비스의 프로세스는 포함하지 않습니다. 이 로그는 백업 예약에 대한 정보를 포함합니다.

로그 유형	설명
SNMP 로그	SNMP 로그는 SNMP 네트워크 관리 엔진과 관련된 디버그 메시지를 기록합니다. 추적 또는 디버그 모드에서는 Security Management Appliance에 대한 SNMP 요청이 포함됩니다.
허용 목록/차단 목록 로그	허용 목록/차단 목록 로그는 허용 목록/차단 목록 설정 및 데이터베이스에 대한 데이터를 기록합니다.
스팸 격리 GUI 로그	스팸 격리 GUI 로그는 GUI를 통한 격리 구성, 엔드유저 인증, 엔드유저 작업(이메일 릴리스 등)을 포함하여 스팸 격리 GUI와 관련된 작업을 기록합니다.
스팸 격리 로그	스팸 격리 로그는 스팸 격리 프로세스와 관련된 작업을 기록합니다.
Status Logs	상태 로그는 CLI 상태 명령(status detail, dnsstatus 등)에서 발견되는 시스템 통계를 기록합니다. 기록 기간은 logconfig의 setup 하위 명령을 사용하여 설정합니다. 상태 로그에 보고되는 각 카운터 또는 점수는 카운터가 마지막으로 재설정된 이후의 값입니다.
시스템 로그	시스템 로그는 부팅 정보, DNS 상태 정보, 사용자가 commit 명령으로 입력한 코멘트 등을 기록합니다. 시스템 로그는 어플라이언스의 상태 문제를 해결하는 데 유용합니다.
Tracking Logs	추적 로그는 추적 서비스의 프로세스와 관련된 작업을 기록합니다. 추적 로그는 메일 로그의 하위 집합입니다.
업데이터 로그	표준 시간대 업데이트와 같은 서비스 업데이트에 대한 정보입니다.
업그레이드 로그	업그레이드 다운로드 및 설치에 대한 상태 정보.

로그 유형 비교

다음 표에는 각 로그 유형의 특성이 요약되어 있습니다.

표 ***91:*** 로그 유형 비교

						Contains(포함)					
	트랜잭션	상태 비저장	텍스트로 기록됨	이진으로 기록됨	헤더 로깅	주기적 상태 정보	메시지 수신 정보	제공 정보	개별 하드 반송	개별 소프트 반송	구성 정보
인증 로그	•		•								
백업 로그	•		•								

						Contains(포함)					
CLI 감사 로그	•		•			•					
구성 기록 로그	•		•								•
FTP 서버 로그	•		•			•					
HTTP 로그	•		•			•					
헤이스택(Haystack) 로그	•		•								
텍스트 메일 로그	•		•		•	•	•	•	•	•	
LDAP 디버그 로그	•		•								
NTP 로그	•		•			•					
보고 로그	•		•			•					
쿼리 보고 로그	•		•			•					
SMA 로그	•		•			•					
SNMP 로그	•		•								
허용 목록/차단 목록 로그	•		•			•					
스팸 격리 GUI	•		•			•					

						Contains(포함)					
스팸 격리	•		•			•					
상태 로그		•	•			•					
시스템 로그	•		•			•					
Tracking Logs	•			•	•		•	•	•	•	
Updater Logs	•		•								

구성 기록 로그 사용

구성 기록 로그는 사용자 이름이 나열된 추가 섹션이 있는 구성 파일, 구성에서 사용자가 어디를 변경했는가에 대한 설명, 사용자가 변경을 커밋할 때 입력한 코멘트로 구성됩니다. 사용자가 변경을 커밋할 때마다 변경 후 구성 파일을 포함하는 새 로그가 생성됩니다.

예

이 예에서 구성 기록 로그는 사용자(admin)가 시스템에 로그인이 허용된 로컬 사용자를 정의하는 테이블에 게스트 사용자를 추가한 것을 보여줍니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  XML generated by configuration change.
  Change comment: added guest user
  User: admin
  Configuration are described as:
    This table defines which local users are allowed to log into the system.
  Product: M160 Messaging Gateway(tm) Appliance
  Model Number: M160
  Version: 6.7.0-231
  Serial Number: 000000000ABC-D000000
  Number of CPUs: 1
  Memory (GB): 4
  Current Time: Thu Mar 26 05:34:36 2009
  Feature "Centralized Configuration Manager": Quantity = 10, Time Remaining = "25 days"
  Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"
  Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"
  Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
  Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"
-->
<config>
```

CLI 감사 로그 사용

다음 표에서는 CLI 감사 로그에 기록된 통계에 대해 설명합니다.

표 ***92: CLI*** 감사 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
PID	명령어가 입력된 특정한 CLI 세션의 프로세스 ID
Message	메시지는 입력한 CLI 명령, CLI 출력(메뉴, 목록 등 포함) 및 표시된 프롬프트로 구성됩니다.

예

이 예에서 CLI 감사 로그는 PID 16434에 대해 who, textconfig CLI 명령이 입력되었음을 보여줍니다.

```
Thu Sep  9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '
Thu Sep  9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername  Login Time  Idle Time  Remote Host  What\n
========  ==========  ==========  ============  ====\n
admin     Wed 11AM    3m 45s     10.1.3.14    tail\nadmin     02:32PM     0s        10.1.3.14
    cli\nmail3.example.com> '
Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n- NEW
 - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

FTP 서버 로그 사용

다음 표에서는 FTP 서버 로그에 기록된 통계에 대해 설명합니다.

표 ***93: FTP*** 서버 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
ID	Connection ID. 각 FTP 연결에 대한 별도의 ID
Message	로그 항목의 메시지 섹션에는 로그 파일 상태 정보 또는 FTP 연결 정보(로그인, 업로드, 다운로드, 로그아웃 등)가 올 수 있습니다.

예

이 예에서 FTP 서버 로그는 연결(ID:1)을 기록합니다. 수신 연결의 IP 주소, 활동(파일 업로드 및 다운로드) 및 로그아웃이 표시됩니다.

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile
Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21
```

```
Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:03:06 2004 Info: System is coming up
Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds
Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86
Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes
Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

HTTP 로그 사용

다음 표에서는 HTTP 로그에 기록된 통계에 대해 설명합니다.

표 ***94: HTTP*** 로그에 기록된 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
ID	세션 ID
req	연결하는 시스템의 IP 주소
user	연결하는 사용자의 사용자 이름
메시지	수행된 작업에 대한 정보. GET 또는 POST 명령, 시스템 상태 등이 포함될 수 있습니다.

예

이 예에서 HTTP 로그는 admin 사용자의 GUI와의 상호 작용을 보여줍니다. (시스템 설치 마법사 실행 등)

```
Wed Sep  8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443
Wed Sep  8 18:17:23 2004 Info: http service listening on 192.168.0.1:80
Wed Sep  8 18:17:23 2004 Info: https service listening on 192.168.0.1:443
Wed Sep  8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds
Wed Sep  8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303
Wed Sep  8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200
Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200
Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190 HTTP/1.1
 200
Wed Sep  8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep  8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

스팸 격리 로그 사용

다음 표에서는 스팸 격리 로그에 기록된 통계에 대해 설명합니다.

표 95: 스팸 격리 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 수행한 작업(격리된 메시지 또는 격리에서 릴리스된 메시지 등)으로 구성됩니다.

예

이 예에서 로그는 격리에서 admin@example.com으로 릴리스되고 있는 메시지(MID 8298624, MID 8298625)를 보여줍니다.

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

스팸 격리 GUI 로그 사용

다음 표에서는 스팸 격리 GUI 로그에 기록된 통계에 대해 설명합니다.

표 96: 스팸 격리 GUI 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

예

이 예에서 로그는 성공적인 인증, 로그인 및 로그아웃을 보여줍니다.

표 97: 스팸 격리 GUI 로그 예

`Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82`
`Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83`
`Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin`
`Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228`
`Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO session:10.251.23.228`

```
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

텍스트 메일 로그 사용

이메일 수신, 이메일 전송 및 반송에 대한 세부 정보를 포함합니다. 이러한 로그는 특정 메시지의 전달을 이해하고 시스템 성능을 분석하는 데 유용한 정보 소스입니다.

여기에는 특별한 구성이 필요하지 않습니다. 그러나 첨부 파일 이름을 보려면 시스템을 적절히 구성해야 합니다. 첨부 파일 이름은 항상 기록되지는 않을 수 있습니다. 자세한 내용은 추적 서비스 개요, 263 페이지를 참조하십시오.

다음 표 에서는 텍스트 메일 로그에 표시되는 정보를 보여줍니다.

표 ***98:*** 텍스트 메일 로그 상태

통계	설명
ICID	Injection Connection ID. 시스템에 대한 개별 SMTP 연결의 숫자 식별자입니다. 시스템에 대한 단일 SMTP 연결을 통해 단일 메시지 또는 수천 개의 개별 메시지를 보낼 수 있습니다.
DCID	Delivery Connection ID. 1~1000개 메시지 전달을 위한 개별 SMTP의 또 다른 서버 연결에 대한 숫자 식별자입니다. 각각의 경우 단일 메시지 전송에서 RID의 일부 또는 전체가 전달됩니다.
RCID	RPC Connection ID. 개별 RPC의 스팸 격리 연결에 대한 숫자 식별자입니다. 스팸 격리를 드나드는 메시지 추적에 사용됩니다.
MID	메시지 ID 로그를 통해 흐르는 메시지 추적에 사용됩니다.
RID	수신자 ID. 각 메시지 수신자에게 ID가 지정됩니다.
New	새 연결이 시작되었습니다.
Start	새 메시지가 시작되었습니다.

샘플 텍스트 메일 로그

다음 샘플을 로그 파일 해석을 위한 가이드로 사용하십시오.

참고 로그 파일의 각 줄에 번호가 매겨지지는 않습니다. 샘플의 편의상 여기에서만 번호를 매긴 것입니다.

표 ***99:*** 텍스트 메일 로그 세부사항

1	`Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes`
2	`Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`
7	`Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25`
8	`Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]`
9	`Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]`
10	`Mon Mar 31 20:11:03 2003 Info: DCID 8 close`

다음 표 위 로그 파일을 읽기 위한 가이드로 사용할 수 있습니다.

표 ***100:*** 텍스트 메일 로그 세부사항 예

라인 번호	설명
1	시스템에 대한 새 연결이 시작되고 ICID(Injection ID) "5"가 할당됩니다. 연결이 Management IP 인터페이스에서 수신되었고 10.1.1.209의 원격 호스트에서 시작되었습니다.
2	클라이언트에서 MAIL FROM 명령이 실행된 후 메시지에 MID(Message ID) "6"이 지정되었습니다.
3	발신자 주소가 식별 및 수락됩니다.
4	수신자가 식별되고 RID(Recipient ID) "0"이 할당됩니다.
5	MID 5가 수락되고 디스크에 기록되고 인식됩니다.

라인 번호	설명
6	수신에 성공하고 수신 연결이 종료됩니다.
7	메시지 전달 프로세스가 시작됩니다. 192.168.42.42에서 10.5.3.25로 DCID(Delivery Connection ID) "8"이 할당됩니다.
8	RID "0"으로 메시지 전달이 시작됩니다.
9	MID 6의 RID "0"에 대한 전달이 성공합니다.
10	전달 연결이 종료됩니다.

텍스트 메일 로그 항목의 예

다음 예에서는 다양한 상황에 따른 로그 항목을 보여줍니다.

메시지 수신

단일 수신자에 대한 메시지가 어플라이언스에 주입됩니다. 메시지가 성공적으로 전달됩니다.

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com (1.2.3.4)
 address 2.3.4.5 reverse dns host unknown verified no
Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970
Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>
Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID '<37gva9$5uvbhe@mail.example.com>'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative
Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery
Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4
Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]
Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close
Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0] [('X-SBRS',
 'None')]
Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery
Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

성공적인 메시지 전달의 예

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]
Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]
Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

메시지 전달 실패(하드 반송)

수신자가 2명인 메시지가 어플라이언스에 주입됩니다. 전달 시 대상 호스트가 둘 중 한 수신자에게 메시지를 전달할 수 없음을 나타내는 5XX 오류를 반환합니다. 어플라이언스는 발신자에게 알리고 대기열에서 수신자를 제거합니다.

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address 64.81.204.225
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

최종적으로 전달 성공한 소프트 반송의 예

메시지가 어플라이언스에 주입됩니다. 첫 번째 전달 시도에서 메시지가 소프트 반송되고 향후 전달을 위해 대기열에 추가됩니다. 두 번째 시도에서 메시지가 성공적으로 전달됩니다.

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23 2003
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

메시지 검사 결과**(scanconfig)**

이 프롬프트와 같이 메시지를 구성 요소 부분으로 분해할 수 없을 때(첨부 파일 제거 시) 시스템 동작을 결정하는 데 scanconfig 명령을 사용할 경우:

```
If a message could not be deconstructed into its component parts in order to remove specified
 attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>
```

다음은 메일 로그에 나타난 것입니다.

메시지를 분해할 수 없을 경우 전달하도록 *scanconfig*가 설정되었습니다.

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line seen
 before first header
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

메시지를 분해할 수 없을 경우 삭제하도록 *scanconfig*가 설정되었습니다.

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
```

```
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line seen
 before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

첨부 파일이 있는 메시지

이 예에서는 첨부 파일 이름 식별을 활성화하기 위해 "Message Body Contains" 조건의 콘텐츠 필터가 구성되었습니다.

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

세 첨부 파일 중 두 번째는 유니코드입니다. 유니코드를 표시할 수 없는 터미널에서는 이러한 첨부 파일이 QP(quoted-printable) 형식으로 표시됩니다.

생성된 또는 재작성된 메시지

재작성/리디렉션 작업과 같은 일부 기능(alt-rcpt-to 필터, 안티 스팸 rcpt 재작성, bcc() 작업, 안티바이러스 리디렉션 등)은 새 메시지를 생성합니다. 로그를 살펴보면서 결과를 확인하여 MID를 더 추가해야 할 수 있습니다(DCID도 필요할 수 있음). 항목은 다음과 같을 수 있습니다.

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

또는

```
Tue Jan  6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter 'testfilt'
```

참고 'rewritten' 항목은 로그에서 새 MID 사용을 나타내는 줄 뒤에 나타날 수 있습니다.

스팸 격리에 메시지 전송

메시지를 격리로 전송하면 메일 로그는 RPC 연결을 식별하기 위해 RCID(RPC connection ID)를 사용하여 격리로 드나드는 이동을 추적합니다. 다음 메일 로그에서 메시지는 스팸으로 태그가 지정되어 스팸 격리로 전송됩니다.

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To: <stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
 a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
 DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local Spam
Quarantine
Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

NTP 로그 사용

다음 표에서는 NTP 로그에 기록된 통계를 보여줍니다.

표 ***101: NTP*** 로그에 기록된 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 서버에 대한 SNTP(Simple Network Time Protocol) 쿼리 또는 adjust: 메시지로 구성됩니다.

예

이 예에서 NTP 로그는 어플라이언스가 NTP 호스트를 두 번 폴링하는 것을 보여줍니다.

```
Thu Sep  9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep  9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep  9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep  9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

보고 로그 사용

다음 표은 보고 로그에 기록된 통계를 보여줍니다.

표 ***102:*** 보고 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

예

이 예에서 보고 로그는 어플라이언스가 정보 로그 레벨에서 설정된 것을 보여줍니다.

```
Wed Oct  3 13:39:53 2007 Info: Period minute using 0 (KB)
Wed Oct  3 13:39:53 2007 Info: Period month using 1328 (KB)
Wed Oct  3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
Wed Oct  3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692
Wed Oct  3 13:40:53 2007 Info: Period hour using 36800 (KB)
Wed Oct  3 13:40:53 2007 Info: Period day using 2768 (KB)
Wed Oct  3 13:40:53 2007 Info: Period minute using 0 (KB)
Wed Oct  3 13:40:53 2007 Info: Period month using 1328 (KB)
Wed Oct  3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds
Wed Oct  3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41
Wed Oct  3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692
Wed Oct  3 13:41:53 2007 Info: Period hour using 36800 (KB)
Wed Oct  3 13:41:53 2007 Info: Period day using 2768 (KB)
Wed Oct  3 13:41:53 2007 Info: Period minute using 0 (KB)
Wed Oct  3 13:41:53 2007 Info: Period month using 1328 (KB)
Wed Oct  3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

보고 쿼리 로그 사용

다음 표는 보고 쿼리 로그에 기록된 통계를 보여줍니다.

표 ***103:*** 보고 쿼리 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

예

이 예에서 보고 쿼리 로그는 어플라이언스가 2007년 8월 29일에서 10월 10일까지 매일 발신 이메일 트래픽 쿼리를 실행한 것을 보여줍니다.

```
Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804479.
Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610228.
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
```

```
PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from 0
to 2 sort_ascendin
g=False.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
 with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning results
 from 0 to 2 sort
_ascending=False.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

허용 목록/차단 목록 로그 사용

다음 표은 허용 목록/차단 목록 로그에 기록된 통계를 보여줍니다.

표 ***104:*** 허용 목록/차단 목록 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

예

이 예에서 허용 목록/차단 목록 로그는 어플라이언스가 두 시간마다 데이터베이스 스냅샷을 만드는 것을 보여줍니다. 또한 발신자가 데이터베이스에 추가된 시간을 보여줍니다.

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version: 6.0.0-425
 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC: 10800 seconds
Fri Sep 28 14:22:33 2007 Info: System is coming up.
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
.........................
Mon Oct  1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
Mon Oct  1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
Mon Oct  1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct  1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct  1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

SMA 로그 사용

다음 표에서는 SMA 로그에 기록된 통계를 보여줍니다.

표 ***105: SMA*** 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

예

이 예의 SMA 로그는 ESA로부터 추적 파일을 다운로드하는 중앙 추적 서비스 및 ESA로부터 보고 파일을 다운로드하는 중앙 보고 서비스를 보여줍니다.

```
Wed Oct  3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
 - /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct  3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
 - /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct  3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
 - /export/tracki
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct  3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
 - /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
Wed Oct  3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from 172.29.0.15
 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct  3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
 - /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct  3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from 172.29.0.17
 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct  3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
 - /export/tracki
ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

상태 로그 사용

상태 로그는 CLI status 명령(status, status detail, dnsstatus 포함)에서 발견되는 시스템 통계를 기록합니다. 기록 기간은 logconfig의 setup 하위 명령을 사용하여 설정합니다. 상태 로그에 보고되는 각 카운터 또는 점수는 카운터가 마지막으로 재설정된 이후의 값입니다.

표 ***106:*** 상태 로그 통계

통계	설명
CPULd	CPU 사용률.
DskIO	디스크 I/O 사용률.
RAMUtil	RAM 사용률.
QKUsd	사용된 큐(킬로바이트).

통계	설명
QKFre	사용 가능한 큐(킬로바이트).
CrtMID	MID(Message ID).
CrtICID	ICID(Injection Connection ID).
CRTDCID	DCID(Delivery Connection ID).
InjMsg	주입된 메시지.
InjRcp	주입된 수신자.
GenBncRcp	생성된 반송 수신자.
RejRcp	거부된 수신자.
DrpMsg	삭제(drop)된 메시지.
SftBncEvnt	소프트 반송 이벤트.
CmpRcp	완료된 수신자.
HrdBncRcp	하드 반송 수신자.
DnsHrdBnc	DNS 하드 반송.
5XXHrdBnc	5XX 하드 반송.
FltrHrdBnc	필터 하드 반송.
ExpHrdBnc	만료된 하드 반송.
OtrHrdBnc	기타 하드 반송.
DlvRcp	전달된 수신자.
DelRcp	삭제된 수신자.
GlbUnsbHt	전역 수신 거부 횟수.
ActvRcp	활성 수신자.
UnatmptRcp	전달을 시도하지 않은 수신자.
AtmptRcp	전달을 시도한 수신자.
CrtCncIn	현재 인바운드 연결.
CrtCncOut	현재 아웃바운드 연결.
DnsReq	DNS 요청.

통계	설명
NetReq	네트워크 요청.
CchHit	캐시 성공률.
CchMis	캐시 실패율.
CchEct	캐시 예외 사항.
CchExp	캐시 만료.
CPUTTm	애플리케이션에서 사용한 총 CPU 시간.
CPUETm	애플리케이션 시작 이후 경과 시간.
MaxIO	메일 프로세스에 대한 초당 최대 디스크 I/O 작업.
RamUsd	할당된 메모리(바이트).
SwIn	메모리 스왑 인
SwOut	메모리 스왑 아웃
SwPgIn	메모리 페이지 인
SwPgOut	메모리 페이지 아웃
MMLen	시스템에 있는 총 메시지 수.
DstInMem	메모리에 있는 목적지 개체의 수.
ResCon	리소스 보존 타핏(tarpit) 값. 과중한 시스템 로드 때문에 수신 메일의 수락이 지정된 시간(초)만큼 지연됩니다.
WorkQ	현재 작업 대기열에 있는 메시지의 수.
QuarMsgs	시스템 격리에 있는 개별 메시지의 수(여러 격리에 있는 메시지는 한 번만 계산됨).
QuarQKUsd	시스템 격리 메시지에서 사용하는 킬로바이트.
LogUsd	사용된 로그 파티션의 비율.
CASELd	CASE 검사에 사용된 CPU 비율.
TotalLd	총 CPU 사용량.
LogAvail	로그 파일에 사용 가능한 디스크 공간의 양.
EuQ	스팸 격리에 있는 메시지 수.
EuqRls	스팸 격리 릴리스 대기열에 있는 메시지 수.

예

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
 DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc
0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp
 0 CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
 17G EuQ 0 EuqRls 0
```

시스템 로그 사용

다음 표에서는 시스템 로그에 기록된 통계를 보여줍니다.

표 ***107:*** 시스템 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	로깅된 이벤트.

예

이 예에서 시스템 로그는 커밋을 실행한 사용자의 이름 및 입력된 코멘트를 비롯한 몇몇 커밋 항목을 보여줍니다.

```
Wed Sep  8 18:02:45 2004 Info: Version: 6.0.0-206 SN: XXXXXXXXXXXX-XXX
Wed Sep  8 18:02:45 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:02:45 2004 Info: System is coming up
Wed Sep  8 18:02:49 2004 Info: bootstrapping DNS cache
Wed Sep  8 18:02:49 2004 Info: DNS cache bootstrapped
Wed Sep  8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Passphrase
Wed Sep  8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW
Thu Sep  9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds
Thu Sep  9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI log
 for examples
Thu Sep  9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

추적 로그 이해

추적 로그는 AsyncOS의 이메일 작업에 대한 정보를 기록합니다. 로그 메시지는 메일 로그에 기록된 메시지의 하위 집합입니다.

추적 로그는 메시지 추적 구성 요소가 메시지 추적 데이터베이스를 구축하는 데 사용됩니다. 로그 파일은 데이터베이스 구축 과정에서 소모되므로 추적 로그는 일시적입니다. 추적 로그의 정보는 사람이 보거나 분석하도록 설계되지 않습니다.

추적 로그는 리소스 효율성을 위해 이진 형식으로 기록 및 전송됩니다. 정보는 논리적인 방식으로 배치되며 Cisco에서 제공하는 유틸리티를 사용하여 변환한 후에 사용자가 읽을 수 있습니다. 변환 툴은 다음 URL에서 이용할 수 있습니다. http://tinyurl.com/3c5l8r

로그 서브스크립션

로그 서브스크립션 구성

로그 서브스크립션은 Cisco Content Security Appliance에 저장되거나 원격으로 저장되는 개별 로그 파일을 만듭니다. 로그 서브스크립션은 푸시(다른 컴퓨터로 전달)되거나 폴링(어플라이언스에서 검색)됩니다. 일반적으로 로그 서브스크립션은 다음과 같은 특성을 가지고 있습니다.

표 ***108:*** 로그 파일 특성

속성	설명
로그 유형	기록할 정보 유형 및 로그 서브스크립션의 형식을 정의합니다. 자세한 내용은 로그 유형의 요약, 507 페이지을(를) 참고하십시오.
이름	나중에 참조하기 위해 로그 서브스크립션에 부여하는 설명적 이름.
로그 파일 이름	디스크에 기록되는 파일의 실제 이름. 시스템이 여러 CSA를 포함하는 경우 로그 파일을 생성한 어플라이언스를 식별하도록 고유한 로그 파일 이름을 사용합니다.
Rollover by File Size(파일 크기별 롤오버)	롤오버 전에 파일이 도달할 수 있는 최대 크기.
Rollover by Time(시간별 롤오버)	시간을 기준으로 로그 파일을 롤오버할 시점. 로그 롤오버 및 전송 예약, 505 페이지에서 여러 옵션을 참조하십시오.
로그 레벨	각 로그 서브스크립션에 대한 상세 수준.
검색 방법	어플라이언스로부터 로그 파일을 전송하는 방법.

Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지(또는 CLI의 `logconfig` 명령)을 사용하여 로그 서브스크립션을 구성합니다. 로그 유형의 요약, 507 페이지에서 보여주는 것처럼 로그 유형을 묻는 프롬프트가 표시됩니다. 대부분의 로그 유형에서는 로그 서브스크립션에 대한 로그 레벨도 선택해야 합니다.

참고 구성 기록 로그만: 구성 기록 로그로부터 구성을 로드하려는 경우 마스크 처리된 암호를 포함하는 구성은 로드할 수 없습니다. **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Log Subscriptions(**로그 서브스크립션**)** 페이지에서 로그에 암호를 포함할지 물으면 `Yes(예)`를 선택합니다. CLI에서 `logconfig` 명령을 사용하는 경우 프롬프트에서 `y`를 입력합니다.

로그 레벨 설정

로그 레벨은 로그에서 전달하는 정보의 양을 결정합니다. 로그는 다섯 가지 세부사항 레벨 중 하나일 수 있습니다. 로그 레벨 설정이 세부적일수록 로그 파일 크기가 더 커지고 시스템 성능에 더 큰 영향을 미칩니다. 로그 레벨 설정이 세부적이면 축약 로그 레벨 설정의 모든 메시지와 함께 다른 메시지도 포함합니다. 세부사항 레벨이 높아질수록 시스템 성능이 저하됩니다.

참고 각 로그 유형에 대해 서로 다른 로깅 레벨을 지정할 수 있습니다.

표 ***109:*** 로그 레벨

로그 레벨	설명
Critical(중대)	오류만 기록됩니다. 가장 축약된 로그 레벨 설정입니다. 이 로그 레벨에서는 성능 및 중요 어플라이언스 활동을 모니터링할 수 없습니다. 그러나 로그 파일이 세부적인 로깅 레벨만큼 빠르게 최대 크기에 도달하지 않습니다. 이 로그 레벨은 syslog 레벨 Alert(알림)와 같습니다.
경고	모든 시스템 오류 및 경고가 로깅됩니다. 이 로그 레벨에서는 성능 및 중요 어플라이언스 활동을 모니터링할 수 없습니다. 로그 파일은 중대 로그 레벨보다 빠른 속도로 최대 크기에 도달합니다. 이 로그 레벨은 syslog 레벨 Warning(경고)과 같습니다.
정보	시스템의 초 단위 작업을 로깅합니다. 예를 들어 연결이 열리거나 전달이 시도되는 것을 기록합니다. Information(정보) 레벨은 로그에 대한 권장 설정입니다. 이 로그 레벨은 syslog 레벨 Info(정보)와 같습니다.
디버그	정보 로그 레벨보다 자세한 정보가 로깅됩니다. 오류를 트러블슈팅할 때는 디버그 로그 레벨을 사용합니다. 이 설정은 임시로 사용한 다음 기본 레벨로 돌려놓으십시오. 이 로그 레벨은 syslog 레벨 Debug(디버그)와 같습니다.
Trace	제공되는 모든 정보가 로깅됩니다. 추적 로그 레벨은 개발자들에게만 권장됩니다. 이 레벨을 사용하면 시스템 성능이 심각하게 저하되므로 사용하지 않는 것이 좋습니다. 이 로그 레벨은 syslog 레벨 Debug(디버그)와 같습니다.

GUI에서 로그 서브스크립션 만들기

단계 **1** [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 **2** **Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > Log Subscriptions(**로그 서브스크립션**)** 페이지에서 **Add Log Subscription(**로그 서브스크립션 추가**)**을 클릭합니다.

단계 **3** 로그 유형을 선택하고 로그 이름(로그 디렉터리의) 및 로그 파일 자체의 이름을 선택합니다.

단계 **4** 가능하다면 최대 파일 크기를 지정합니다.

단계 **5** 가능하다면 로그 롤오버 일수, 시간대 또는 간격을 지정합니다. 자세한 내용은 로그 롤오버 및 전송 예약, 505 페이지을(를) 참고하십시오.

단계 **6** 가능하다면 로그 레벨을 지정합니다.

단계 **7** (구성 기록 로그만) 로그에 암호를 포함할지 여부를 선택합니다.

참고 마스크 처리된 암호를가 있는 구성은 로드할 수 없습니다. 구성 기록 로그로부터 구성을 로드하려는 경우 로그에 암호를 포함할지 물으면 Yes(예)를 선택합니다.

단계 **8** 로그 검색 방법을 구성합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

로그 서브스크립션 수정

단계 **1** Log Subscriptions(로그 서브스크립션) 페이지 Log Name(로그 이름) 열에서 로그의 이름을 클릭합니다.

단계 **2** 로그 서브스크립션을 업데이트합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

전역 로깅 설정 구성

시스템은 주기적으로 텍스트 메일 로그 및 상태 로그 내에 시스템 메트릭을 기록합니다. Log Subscriptions(로그 서브스크립션) 페이지의 Global Settings(전역 설정) 섹션에 있는 **Edit Settings(**설정 수정**)** 버튼(또는 CLI의 logconfig -> setup 명령)을 사용하여 다음을 구성할 수 있습니다.

- 시스템이 메트릭 기록 간에 대기하는 시간(초)입니다.
- 메시지 ID 헤더의 기록 여부.
- 원격 응답 상태 코드의 기록 여부.
- 원본 메시지 제목 헤더의 기록 여부.
- 각 메시지에 대해 기록해야 할 헤더

모든 Cisco Content Security Appliance 로그에는 다음 세 가지 항목이 선택적으로 포함됩니다.

- Message-ID: 이 옵션이 구성되면 모든 메시지의 메시지 ID 헤더(사용 가능한 경우)가 기록됩니다. 이 메시지 ID는 수신된 메시지에서 올 수도 있고 AsyncOS 자체에서 생성될 수도 있습니다. 예를 들면 다음과 같습니다.

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

- Remote Response: 이 옵션이 구성되면 모든 메시지의 원격 응답 상태 코드(사용 가능한 경우)가 기록됩니다. 예를 들면 다음과 같습니다.

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

원격 응답 문자열은 사람이 읽을 수 있는 텍스트로, 전달 SMTP 대화 중에 DATA 명령에 대한 응답 후 수신됩니다. 이 예에서 연결 호스트가 데이터 명령을 실행한 후 원격 응답은 "queued as 9C8B425DA7"입니다.

```
[...]
250 ok hostname
250 Ok: queued as 9C8B425DA7
```

문자열의 시작에서 공백, 구두점 및 OK 문자(250 응답의 경우)가 제거됩니다. 문자열의 끝에서는 공백만 제거됩니다. 예를 들어 Cisco Content Security Appliance는 기본적으로 250 Ok: Message MID accepted 문자열로 DATA 명령에 응답합니다. 따라서 원격 호스트가 또 다른 Cisco Content Security Appliance인 경우 "Message MID accepted" 항목이 기록됩니다.

- Original Subject Header: 이 옵션이 활성화되면 각 메시지의 원래 제목 헤더가 로그에 포함됩니다.

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

메시지 헤더 로깅

경우에 따라 메시지가 시스템을 통과할 때 메시지 헤더의 존재와 내용을 기록해야 합니다. Log Subscriptions Global Settings(로그 서브스크립션 전역 설정) 페이지에서(또는 CLI의 logconfig -> logheaders 하위 명령을 통해) 기록할 헤더를 지정합니다. 어플라이언스는 텍스트 메일 로그 및 추적 로그에 지정된 메시지 헤더를 기록합니다. 헤더가 있으면 시스템은 헤더의 이름과 값을 기록합니다. 헤더가 없으면 로그에 아무것도 기록되지 않습니다.

참고 시스템은 헤더에 대해 로깅이 지정되었는지와 상관없이 메시지 기록을 처리하는 동안 언제든지 메시지에 있는 모든 헤더를 평가합니다.

참고 SMTP 프로토콜에 대한 RFC는 http://www.faqs.org/rfcs/rfc2821.html에 있으며 사용자 정의 헤더를 정의합니다.

참고 logheaders 명령을 통해 기록할 헤더를 구성한 경우 전달 정보 후 헤더 정보가 나타납니다.

표 ***110:*** 헤더 로그

헤더 이름	헤더의 이름
값	로깅된 헤더의 내용

예를 들어, 로깅할 헤더로 "date, x-subject"를 지정하면 메일 로그에 다음 줄이 나타납니다.

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0] [('date', 'Tue, 31 May
 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

GUI를 사용하여 전역 로깅 설정 구성

단계 **1** Log Subscriptions(로그 서브스크립션) 페이지의 Global Settings(전역 설정) 섹션에 있는 **Edit Settings(**설정 수정**)** 버튼을 클릭합니다.

단계 **2** 시스템 측정 빈도, 메일 로그에 메시지 ID 헤더를 포함할지 여부, 원격 응답을 포함할지 여부, 각 메시지의 원래 제목 헤더를 포함할지 여부 등의 정보를 지정합니다.

이 설정에 대한 자세한 내용은 전역 로깅 설정 구성, 529 페이지를 참조하십시오.

단계 **3** 로그에 포함할 다른 헤더를 입력합니다. 각 항목을 쉼표로 구분하십시오.

단계 **4** 변경 사항을 제출 및 커밋합니다.

로그 서브스크립션 롤오버

AsyncOS에서 로그 파일을 롤오버할 때

- 롤오버의 타임스탬프로 새 로그 파일을 만들고 "**c**" 확장자로 파일을 현재로 지정합니다.
- 'saved'를 의미하는 "**s**" 확장자로 현재 로그 파일 이름을 변경합니다.
- 새로 저장된 로그 파일을 원격 호스트로 전송합니다(푸시 기반일 경우).
- 동일한 서브스크립션에서 전에 실패한 로그 파일을 전송합니다(푸시 기반일 경우).
- 보관할 수 있는 총 파일 수가 초과된 경우 로그 서브스크립션에서 가장 오래된 파일을 삭제합니다(폴링 기반일 경우).

향후 작업

로그 서브스크립션의 로그 롤오버

로그 롤오버 및 전송 예약, 505 페이지를 참조하십시오.

GUI를 사용하여 로그를 즉시 롤오버

단계 **1** Log Subscriptions(로그 서브스크립션) 페이지에서 롤오버할 로그 오른쪽에 있는 확인란을 선택합니다.
단계 **2** 모든 로그를 롤오버하려면 **All(**모두**)** 확인란을 선택할 수 있습니다.
단계 **3** **Rollover Now(**지금 롤오버**)** 버튼을 클릭합니다.

다음에 수행할 작업

- 로그 서브스크립션의 로그 롤오버 , 531 페이지
- CLI를 통해 로그를 즉시 롤오버, 532 페이지

CLI를 통해 로그를 즉시 롤오버

모든 로그 파일을 즉시 롤오버하려면 rollovernow 명령을 사용하거나, 목록에서 특정 로그 파일을 선택합니다.

GUI에서 최근 로그 항목 보기

GUI에서 Log Subscriptions(로그 서브스크립션) 페이지 Log File(로그 파일) 열에서 로그 서브스크립션을 클릭하여 로그 파일을 볼 수 있습니다. 로그 서브스크립션에 대한 링크를 클릭하면 암호를 입력하라는 프롬프트가 표시됩니다. 그러면 해당 서브스크립션에 대한 로그 파일 목록이 나타납니다. 브라우저에서 보거나 디스크에 저장할 로그 파일 하나를 클릭할 수 있습니다. GUI를 통해 로그를 보려면 관리 인터페이스에서 FTP 서비스를 활성화해야 합니다.

로그의 최신 항목 보기(tail 명령)

AsyncOS는 어플라이언스에 있는 구성된 로그의 최신 항목을 보여주는 tail 명령을 지원합니다. tail 명령을 실행하고 최근에 구성한 로그를 선택하여 확인합니다. tail 명령을 종료하려면 Ctrl-C를 누릅니다.

참고 tail 명령을 사용하면 구성 기록 로그는 볼 수 없습니다. FTP 또는 SCP를 사용해야 합니다.

예

다음 예에서 tail 명령은 시스템 로그를 보는 데 사용됩니다. tail 명령은 매개변수로 표시되는 로그 이름(예: tail system_logs)도 받습니다

```
Welcome to the M600 Messaging Gateway(tm) Appliance
example.srv> tail
Currently configured logs:
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: " Spam Quarantine Logs" Retrieval: FTP Poll
```

```
3. "euqgui_logs" Type: "Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10
Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>

.
```

호스트 키 구성

Cisco Content Security Appliance에서 다른 서버로 로그를 푸시할 때 SSH와 함께 사용할 호스트 키를 관리하려면 logconfig -> hostkeyconfig 하위 명령을 사용합니다. SSH 서버에는 호스트 키 쌍(개인 키 및 공개 키)이 있어야 합니다. 개인 호스트 키는 SSH 서버에 있으며 원격 시스템에서 읽을 수 없습니다. 공개 호스트 키는 SSH 서버와 상호 작용해야 할 클라이언트 시스템에 배포됩니다.

참고 사용자 키 관리에 대한 자세한 내용은 Email Security Appliance용 사용 설명서 또는 온라인 도움말에서 "SSH(Secure Shell) 키 관리"를 참조하십시오.

hostkeyconfig 하위 명령은 다음 기능을 수행합니다.

표 ***111:*** 호스트 키 관리 **-** 하위 명령 목록

Command(명령**)**	설명
New	새 키를 추가합니다.
Edit	기존 키를 수정합니다.
Delete	기존 키를 삭제합니다.
Scan	호스트 키를 자동으로 다운로드합니다.
Print	키를 표시합니다.
Host	시스템 호스트 키를 표시합니다. 이 값은 원격 시스템의 "known_hosts" 파일에 저장됩니다.

Command(명령)	설명
Fingerprint	시스템 호스트 키 지문을 표시합니다.
User	로그를 원격 시스템으로 푸시하는 시스템 계정의 공개 키를 표시합니다. 이것은 SCP 푸시 서브스크립션을 설정할 때 표시되는 것과 동일한 키입니다. 이 값은 원격 시스템의 "authorized_keys" 파일에 저장됩니다.

예

다음 예의 명령은 호스트 키를 검사하고 호스트에 대해 추가합니다.

```
mail3.example.com> logconfig
Currently configured logs:
[ list of logs
 ]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan
Please enter the host or IP address to lookup.
[]> mail3.example.com
Choose the ssh protocol type:
1. SSH2:rsa
2. SSH2:dsa
3. All
[3]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed
 ]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed
 ]
Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed
 ]
2. mail3.example.com ssh-rsa [ key displayed
 ]
3. mail3.example.com 1024 35 [ key displayed
```

```
 ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
Currently configured logs:
[ list of configured logs
 ]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
mail3.example.com> commit
```

17 장

문제 해결

이 장에는 다음 섹션이 포함되어 있습니다.

시스템 정보 수집

일련 번호를 포함하여 어플라이언스 및 그 상태에 대한 정보를 얻을 수 있습니다. 참조 시스템 상태 모니터링, 369 페이지

하드웨어 문제 트러블슈팅

하드웨어 어플라이언스의 전면 및/또는 후면 패널에 있는 표시등은 어플라이언스의 상태를 나타냅니다. 이러한 지표의 설명은 에 지정된 위치에서 사용 가능한 하드웨어 설명서(예: *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*)를 참조하십시오.

어플라이언스 사양(예: 온도 범위)도 이러한 문서에서 확인할 수 있습니다.

참고 x80 또는 x90 어플라이언스를 껐다 켜야 하는 경우 어플라이언스가 켜질 때까지 20분 이상 기다린 다음(모든 LED가 녹색) 전원 버튼을 누릅니다.

기능 설정 관련 문제 해결

기능을 성공적으로 구성하는 데 어려움이 있는 경우 각 기능에 대해 완료해야 할 작업의 요약을 참조하십시오. 여기에는 각각에 대한 구체적인 정보의 링크도 포함되어 있습니다.

- 중앙 웹 보고 및 추적 설정 , 179 페이지
- 중앙 이메일 보고 설정, 62 페이지
- 중앙 집중식 메시지 추적 설정 , 264 페이지
- 중앙 집중식 스팸 격리 설정 , 280 페이지
- 중앙 정책, 바이러스, 보안 침해 격리, 311 페이지
- 중앙에서 WSA를 관리하기 위한 구성 마스터 설정 , 342 페이지

일반 트러블슈팅 리소스

일반 트러블슈팅 리소스에는 다음 항목이 포함됩니다.

- 최신 알림. 최근 알림 보기 , 466 페이지를 참조하십시오.
- 로그 파일. 로깅, 503 페이지을 참고하십시오.
- 릴리즈 노트. 문서 업데이트 섹션 포함 설명서 , 571 페이지를 참조하십시오.
- Cisco Bug Search 툴(액세스 방법은 릴리즈 노트 참조)
- 기술 자료(TechNotes) , 573 페이지
- Cisco Support Community, 573 페이지

특정 기능 관련 문제 트러블슈팅

기능 설정 관련 문제 해결 , 538 페이지도 참조하십시오.

웹 보안 관련 기능

- 모든 보고서 트러블슈팅 , 45 페이지
- 웹 보고 및 추적 트러블슈팅 , 258 페이지
- 구성 관리 문제 트러블슈팅 , 367 페이지
- 기능 관련 문제는 웹 보안 어플라이언스의 설정 때문에 발생할 수 있습니다. 설명서 , 571 페이지에 지정된 위치에서 사용 중인 릴리스에 대한 릴리스 정보, 온라인 도움말 또는 사용 설명서를 참조하십시오.

이메일 보안 관련 문제

- 모든 보고서 트러블슈팅 , 45 페이지
- 메시지 추적 트러블슈팅, 277 페이지
- 스팸 격리 기능 문제 해결 , 309 페이지
- 중앙 집중식 정책 격리 트러블슈팅 , 339 페이지
- 기능 관련 문제는 Email Security Appliance의 설정 때문에 발생할 수 있습니다. 설명서 , 571 페이지에 지정된 위치에서 사용 중인 릴리스에 대한 릴리스 정보, 온라인 도움말 또는 사용 설명서를 참조하십시오.

일반 문제

- 구성 파일을 로드할 수 없을 경우 디스크 공간 할당량이 **Management Appliance**(관리 어플라이언스) > **System Administration**(시스템 관리) > **Disk Management**(디스크 관리) 페이지의 테이블에 나타난 기능별 현재 크기보다 큰지 확인합니다.
- 최근에 업그레이드했는데 온라인 도움말이 오래된 듯하거나 새 기능에 대한 정보를 찾을 수 없으면 브라우저 캐시를 지우고 브라우저 창을 다시 엽니다.
- 여러 브라우저 창 또는 탭을 동시에 사용하면서 웹 인터페이스에서 설정을 구성할 경우 예기치 않은 동작이 발생할 수 있습니다.
- 경고문에 응답 , 539 페이지를 참조하십시오.
- 관리자 사용자 액세스 트러블슈팅 , 428 페이지를 참조하십시오.

경고문에 응답

- 경고: 380 또는 680 하드웨어의 배터리 재인식 시간 초과(RAID 이벤트), 539 페이지
- 추가 알림 설명 , 539 페이지

경고: 380 또는 680 하드웨어의 배터리 재인식 시간 초과(RAID 이벤트)

문제: 380 또는 680 하드웨어에서 “Battery Relearn Timed Out” 알림을 수신합니다.

솔루션: 이 경고문은 문제를 나타낼 수도 있고 그렇지 않을 수도 있습니다. 배터리 재인식 시간 초과 자체가 RAID 컨트롤러에 문제가 있음을 의미하지는 않습니다. 후속 재인식에서 컨트롤러가 복구될 수 있습니다. 이것이 다른 문제의 부작용이 아닌지 확인하려면 앞으로 48시간 동안 다른 RAID 경고문이 이메일로 전달되는지 모니터링하십시오. 시스템에서 다른 RAID 관련 경고문이 없으면 이 경고문을 무시할 수 있습니다.

추가 알림 설명

다른 알림에 대해서는 다음을 참조하십시오.

- 하드웨어 알림 설명 , 467 페이지

- 시스템 알림 설명 , 468 페이지

향후 작업

- 경고 관리, 464 페이지

기술 지원 이용

어플라이언스에서 지원 사례 열기 또는 업데이트

이 방법으로 Cisco TAC 또는 자체 지원 서비스에 문의할 수 있습니다.

시작하기 전에

Cisco TAC에 문의하려는 경우

- 긴급한 문제인 경우 이 방법을 사용하지 마십시오. 대신 고객 지원 , 573 페이지에 나열된 다른 방법 중 하나를 사용하여 고객 지원에 문의하십시오.
- 도움을 받을 수 있는 다른 옵션을 고려합니다.
- 이 절차를 사용하여 지원 사례를 열면 어플라이언스 구성 파일이 Cisco 고객 지원으로 전송됩니다. 어플라이언스 구성을 전송하지 않으려면 다른 방법을 사용하여 고객 지원에 연락할 수 있습니다.
- 어플라이언스가 인터넷에 연결되어 있고 이메일을 전송할 수 있어야 합니다.
- 기존 사례에 대한 정보를 전송하는 경우 사례 번호가 있어야 합니다.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** **Help and Support**(도움말 및 지원) > **Contact Technical Support**(기술 지원에 문의)를 선택합니다.

단계 **3** 지원 요청의 수신자를 확인합니다.

Cisco TAC에 요청을 보내려면	**Cisco** 기술 지원 확인란을 선택합니다.
내부 지원 팀에게만 요청을 보내려면	• **Cisco Technical Support(Cisco** 기술 지원**)** 확인란을 선택하지 않습니다. • 지원 데스크의 이메일 주소를 입력합니다.
(선택 사항) 다른 수신자를 포함하려면	이메일 주소를 입력합니다.

단계 **4** 양식을 작성합니다.

단계 **5** **Send**(보내기)를 클릭합니다.

가상 어플라이언스에 대한 지원 받기

Cisco 콘텐츠 보안 가상 어플라이언스에 대한 지원 사례를 보관하려면 VLN(Virtual License Number), 계약 번호 및 PID(Product Identifier) 코드를 제공해야 합니다.

구매 주문을 참조하거나 다음 표를 통해 가상 어플라이언스에서 실행되는 소프트웨어 라이센스를 기반으로 PID를 식별할 수 있습니다.

기능	**PID**	설명
모든 중앙 웹 보안 기능	SMA-WMGT-LIC=	—
모든 중앙 이메일 보안 기능	SMA-EMGT-LIC=	

Cisco 고객 지원 담당자를 위한 원격 액세스 활성화

Cisco 고객 지원에서만 이러한 방법을 사용하여 사용자 어플라이언스에 액세스할 수 있습니다.

- Cisco 고객 지원 담당자를 위한 원격 액세스 활성화 , 541 페이지
- 직접 인터넷에 연결되지 않은 어플라이언스에 대한 원격 액세스 활성화 , 542 페이지
- 기술 지원 터널 비활성화 , 542 페이지
- 원격 액세스 비활성화 , 542 페이지
- 지원 연결의 상태 확인 , 543 페이지

인터넷이 연결되는 어플라이언스에 대한 원격 액세스 활성화

기술 지원에서는 이 절차에서 어플라이언스와 upgrades.ironport.com 서버 간에 생성하는 SSH 터널을 통해 어플라이언스에 액세스합니다.

시작하기 전에

인터넷에서 도달할 수 있는 포트를 식별합니다. 기본값은 포트 25입니다. 시스템에서도 이메일 메시지를 전송하기 위해 해당 포트를 통한 일반 액세스가 필요하므로. 대부분의 방화벽 구성에서 이 포트를 통한 연결이 허용됩니다.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** GUI 창의 오른쪽에서 **Help and Support(**도움말 및 지원**) > Remote Access(**원격 액세스**)**를 선택합니다.

단계 **3** **Enable(**활성화**)**을 클릭합니다.

단계 **4** 정보를 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

지원 담당자의 원격 액세스가 더 이상 필요하지 않은 경우 기술 지원 터널 비활성화 , 542 페이지 섹션을 참조해 주십시오.

직접 인터넷에 연결되지 않은 어플라이언스에 대한 원격 액세스 활성화

직접 인터넷에 연결되지 않은 어플라이언스의 경우 인터넷에 연결된 두 번째 어플라이언스를 통해 액세스할 수 있습니다.

시작하기 전에

- 문제의 어플라이언스는 포트 22에서 인터넷에 연결된 두 번째 어플라이언스에 연결할 수 있어야 합니다.
- 인터넷이 연결되는 어플라이언스에서 인터넷이 연결되는 어플라이언스에 대한 원격 액세스 활성화 , 541 페이지의 절차에 따라 문제의 어플라이언스에 대한 지원 터널을 생성합니다.

단계 **1** 지원이 필요한 어플라이언스의 CLI에서 `techsupport` 명령을 입력합니다.

단계 **2** `sshaccess`를 입력합니다.

단계 **3** 프롬프트에 따라 수행합니다.

다음에 수행할 작업

지원 담당자의 원격 액세스가 더 이상 필요하지 않은 경우 다음을 참조하십시오.

- 원격 액세스 비활성화 , 542 페이지
- 기술 지원 터널 비활성화 , 542 페이지

기술 지원 터널 비활성화

활성화된 techsupport 터널은 7일 동안 upgrades.ironport.com에 연결되어 있습니다. 그 이후에는 설정된 연결이 끊어지는 것이 아니라, 끊어진 터널에 다시 연결할 수 없게 됩니다.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** GUI 창의 오른쪽에서 **Help and Support**(도움말 및 지원) > **Remote Access**(원격 액세스)를 선택합니다.

단계 **3** **Disable**(비활성화)을 클릭합니다.

원격 액세스 비활성화

techsupport 명령을 사용하여 만든 원격 액세스 계정은 비활성화할 때까지 활성 상태가 유지됩니다.

단계 **1** CLI에서 `techsupport` 명령을 입력합니다.

단계 **2** `sshaccess`를 입력합니다.
단계 **3** `disable`을 입력합니다.

지원 연결의 상태 확인

단계 **1** CLI에서 `techsupport` 명령을 입력합니다.
단계 **2** status를 입력합니다.

패킷 캡처 실행

패킷 캡처를 사용하면 지원 담당자가 어플라이언스에서 들어가고 나오는 TCP/IP 데이터 및 기타 패킷을 볼 수 있습니다. 이를 통해 고객 지원에서는 네트워크 설정을 디버그하고 어떤 네트워크 트래픽이 어플라이언스에 도달하는지 또는 어플라이언스를 떠나는지를 확인할 수 있습니다.

단계 **1** **Help and Support(**도움말 및 지원**) > Packet Capture(**패킷 캡처**)**를 선택합니다.
단계 **2** 패킷 캡처 설정을 지정합니다.

a) **Packet Capture Settings(**패킷 캡처 설정**)** 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.
b) (선택 사항) 패킷 캡처의 기간, 제한 사항 및 필터를 입력합니다.

지원 담당자가 이러한 설정을 안내해줄 수 있습니다.

시간 단위를 지정하지 않고 캡처 기간을 입력하면 기본적으로 초 단위가 사용됩니다.

Filters(필터) 섹션에서

- 맞춤 필터는 UNIX `tcpdump` 명령에서 지원하는 구문(예: host 10.10.10.10 && port 80)을 사용할 수 있습니다.
- 클라이언트 IP는 어플라이언스에 연결하는 머신(예: Email Security Appliance를 통해 메시지를 전송하는 메일 클라이언트)의 IP 주소입니다.
- 서버 IP는 어플라이언스가 연결하는 머신(예: 어플라이언스가 메시지를 전달하는 Exchange Server)의 IP 주소입니다.

Email Security Appliance를 중간에 둔 특정 클라이언트와 특정 서버 간 트래픽을 추적하려면 클라이언트 및 서버 IP 주소를 사용할 수 있습니다.

c) **Submit(**제출**)**을 클릭합니다.

단계 **3** **Start Capture(**캡처 시작**)**를 클릭합니다.

- 한 번에 캡처를 하나만 실행할 수 있습니다.
- 패킷 캡처가 실행 중이면 현재 통계(예: 파일 크기 및 경과 시간)와 함께 Packet Capture(패킷 캡처) 페이지에 진행 중인 캡처의 상태가 표시됩니다.
- GUI에는 CLI가 아니라 GUI에서 시작된 패킷 캡처만 표시됩니다. 마찬가지로 CLI에는 CLI에서 시작된 현재 패킷 캡처의 상태만 표시됩니다.

- 패킷 캡처 파일은 10개 부분으로 나누어집니다. 패킷 캡처가 끝나기 전에 파일이 최대 크기 제한에 도달하면 파일의 가장 오래된 부분이 삭제되고(데이터가 삭제됨) 현재 패킷 캡처 데이터로 새 부분이 시작됩니다. 한 번에 패킷 캡처 파일의 1/10만 삭제됩니다.
- GUI에서 시작되어 실행 중인 캡처는 세션 간에 유지됩니다. (CLI에서 시작되어 실행 중인 캡처는 세션이 끝나면 중단됩니다.)

단계 **4** 지정된 기간에 캡처가 실행되도록 합니다. 또는 캡처가 무한정 실행되도록 한 경우 **Stop Capture(**캡처 중단**)**를 클릭하여 캡처를 수동으로 중단합니다.

단계 **5** 패킷 캡처 파일에 액세스합니다.

- **Manage Packet Capture Files(**패킷 캡처 파일 관리**)** 리스트에서 파일을 클릭하고 **Download File(**파일 다운로드**)**을 클릭합니다.
- 어플라이언스의 captures 하위 디렉터리에 있는 파일에 액세스하려면 FTP 또는 SCP를 사용합니다.

다음에 수행할 작업

고객 지원에서 파일을 사용할 수 있도록 합니다.

- 어플라이언스에 대한 원격 액세스를 허용하면 기술 지원 담당자가 FTP 또는 SCP를 사용하여 패킷 캡처 파일에 액세스할 수 있습니다. Cisco 고객 지원 담당자를 위한 원격 액세스 활성화 , 541 페이지를 참조하십시오.
- 이메일로 파일을 고객 지원에 전송합니다.

어플라이언스 전원 원격 초기화

어플라이언스를 하드 초기화해야 하는 경우 서드파티 IPMI(Intelligent Platform Management Interface) 툴을 사용하여 어플라이언스 섀시를 원격으로 재부팅할 수 있습니다.

제한 사항

- 원격 전원 제어는 특정 하드웨어에서만 이용할 수 있습니다.

  자세한 내용은 원격 전원 제어 활성화 , 437 페이지 섹션을 참조하십시오.

- 이 기능을 사용하려면 먼저 활성화해야 합니다.

  자세한 내용은 원격 전원 제어 활성화 , 437 페이지 섹션을 참조하십시오.

- 다음 IPMI 명령만 지원됩니다.

  ```
  status, on, off, cycle, reset, diag, soft
  ```

  지원되지 않는 명령을 실행하면 "insufficient privileges(권한 부족)" 오류가 표시됩니다.

시작하기 전에

- IPMI 버전 2.0을 사용하여 장비를 관리할 수 있는 유틸리티를 구해 설치합니다.
- 지원되는 IPMI 명령 사용 방법을 이해합니다. IPMI 툴에 대한 문서를 참조해 주십시오.

단계 **1** IPMI를 사용하여 필요한 크리덴셜과 함께 초기에 구성된 원격 전력 제어 포트에 할당된 IP 주소에 대해 지원되는 power-cycling 명령을 실행합니다.

예를 들어 IPMI가 지원되는 UNIX 유형의 머신에서는 다음 명령을 실행할 수 있습니다.

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

여기서 `192.0.2.1`은 원격 전원 제어 포트에 할당된 IP 주소이고 remoteresetuser 및 passphrase는 이 기능을 사용하도록 설정하는 동안 입력한 크리덴셜입니다.

단계 **2** 어플라이언스가 재부팅될 때까지 11분 이상 기다립니다.

A 부록

IP 인터페이스 및 어플라이언스 액세스

이 장에는 다음 섹션이 포함되어 있습니다.

IP 인터페이스 및 어플라이언스 액세스

어플라이언스에서 만든 IP 인터페이스에 다양한 Cisco Content Security Appliance 서비스를 통해 액세스할 수 있습니다.

기본적으로 다음 서비스는 각 인터페이스에서 활성화되었거나 비활성화되어 있습니다.

표 ***112: IP*** 인터페이스에서 기본적으로 활성화되는 서비스

		기본적으로 활성화되는지 여부	
서비스	기본 포트	관리 인터페이스	새로 만드는 **IP** 인터페이스
FTP	21	아니요	아니요
Telnet	23	예	아니요
SSH	22	예	아니요
HTTP	80	예	아니요
HTTPS	443	예	아니요

IP 인터페이스

IP 인터페이스에는 네트워크에 개별적으로 연결하는 데 필요한 네트워크 구성 데이터가 포함되어 있습니다. 하나의 물리적 이더넷 인터페이스에 대해 여러 IP 인터페이스를 구성할 수 있습니다. IP 인터페이스를 통해 스팸 격리에 대한 액세스도 구성할 수 있습니다. 이메일 전달 및 Virtual Gateway의 경우 각 IP 인터페이스는 특정 IP 주소 및 호스트 이름과 함께 하나의 Virtual Gateway 주소로 작동합니

다. 또한 여러 인터페이스를 별개의 그룹으로 "결합"할 수 있으며(CLI를 통해), 이 경우 시스템은 이메일 전달 시 이러한 그룹을 순환합니다. Virtual Gateway의 결합 또는 그룹화는 여러 인터페이스에 걸친 대규모 이메일 캠페인의 부하 균형에 유용합니다. 또한 VLAN을 만들고 다른 인터페이스처럼 구성할 수 있습니다(CLI를 통해). 자세한 내용은 Email Security Appliance 사용 설명서 또는 온라인 도움말의 "고급 네트워킹" 장을 참조하십시오.

IP 인터페이스 구성

Management Appliance(관리 어플라이언스) > Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지(및 interface config 명령)으로 IP 인터페이스를 추가, 수정, 삭제할 수 있습니다.

참고 Security Management Appliance의 관리 인터페이스와 관련된 이름 또는 이더넷 포트를 변경할 수 없습니다. 또한 Security Management Appliance에서는 아래에 설명된 모든 기능을 지원하지는 않습니다(예: 가상 게이트웨이).

다음 정보는 IP 인터페이스를 구성할 때 필요합니다.

표 ***113: IP*** 인터페이스 구성 요소

이름	인터페이스의 별칭.
IP 주소	동일한 서브넷 내의 IP 주소는 별도의 물리적 이더넷 인터페이스에서 구성할 수 없습니다.
넷마스크(또는서브넷마스크)	점으로 구분된 옥텟의 표준 형식(예: 255.255.255.0) 또는 16진수 형식(예: 0xffffff00)으로 넷마스크를 입력할 수 있습니다. 기본 넷마스크는 255.255.255.0, 일반 클래스 C 값입니다.
브로드캐스트 주소	AsyncOS는 IP 주소 및 넷마스크로부터 기본 브로드캐스트 주소를 자동으로 계산합니다.
호스트 이름	인터페이스와 관련된 호스트 이름. SMTP 대화 중에 서버를 식별하는 데 사용합니다. 사용자는 각 IP 주소와 연결된 유효한 호스트 이름을 입력해야 합니다. DNS가 호스트 이름을 매칭하는 IP 주소로 올바르게 확인하는지 아니면 역방향 DNS에서 지정된 호스트 이름이 나오는지 소프트웨어에서 확인하지 않습니다.
허용된 서비스	FTP, SSH, 텔넷, 스팸 격리, HTTP, HTTPS는 인터페이스에서 활성화 또는 비활성화될 수 있습니다. 각 서비스에 대해 포트를 구성할 수 있습니다. 스팸 격리에 대해 HTTP/HTTPS, 포트, URL을 지정할 수도 있습니다.

참고 설정, 설치, 기본 구성, 17 페이지의 설명대로 시스템 설정 마법사를 완료하고 변경사항을 커밋한 경우 관리 인터페이스가 어플라이언스에 이미 구성되어 있어야 합니다.

GUI를 사용하여 IP 인터페이스 생성

단계 1 [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 2 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)**를 선택합니다.

단계 3 **Add IP Interface(IP** 인터페이스 추가**)**를 클릭합니다.

단계 4 인터페이스의 이름을 입력합니다.

단계 5 이더넷 포트를 선택하고 IP 주소를 입력합니다.

단계 6 IP 주소에 대한 넷마스크를 입력합니다.

단계 7 인터페이스의 호스트 이름을 입력합니다.

단계 8 이 IP 인터페이스에서 활성화할 각 서비스의 옆에 있는 확인란을 선택합니다. 필요하다면 해당 포트를 변경합니다.

단계 9 인터페이스에서 어플라이언스 관리를 위해 HTTP에서 HTTPS로의 리디렉션을 활성화할지 여부를 선택합니다.

단계 10 스팸 격리를 사용하는 경우 HTTP 및/또는 HTTPS를 선택하고 각각에 대해 포트 번호를 지정할 수 있습니다. 또한 HTTP 요청을 HTTPS에 리디렉션할지 여부를 선택할 수 있습니다. 마지막으로 IP 인터페이스가 스팸 격리에 대한 기본 인터페이스인지 여부 및 호스트 이름을 URL로 사용할지 아니면 맞춤 URL을 제공할지 여부를 지정할 수 있습니다.

단계 11 변경 사항을 제출 및 커밋합니다.

FTP를 통한 어플라이언스 액세스

⚠

주의 Management Appliance(관리 어플라이언스) > Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지에서 또는 interfaceconfig 명령으로 서비스를 비활성화함으로써 어플라이언스와의 연결 상태에 따라 GUI 또는 CLI와의 연결을 끊을 수 있습니다. 또 다른 프로토콜, Serial 인터페이스 또는 Management 포트의 기본 설정을 사용하여 어플라이언스에 다시 연결할 수 있는 경우가 아니면 이 명령으로 서비스를 비활성화하지 마십시오.

단계 1 [새 웹 인터페이스에만 해당] Cloud Email Security Management Console에서 기어 ⚙ 아이콘을 클릭하여 레거시 웹 인터페이스를 클릭합니다.

단계 2 **Management Appliance(**관리 어플라이언스**) > Network(**네트워크**) > IP Interfaces(IP** 인터페이스**)** 페이지(또는 `interfaceconfig` 명령)를 사용하여 인터페이스에 대한 FTP 액세스를 활성화합니다.

참고 다음 단계로 진행하려면 먼저 변경사항을 커밋해야 합니다.

단계 3 FTP를 통해 인터페이스에 액세스합니다. 인터페이스에 대한 IP 주소가 올바른지 확인하십시오.

예: `ftp 192.168.42.42`

IP 인터페이스 및 어플라이언스 액세스

또한 많은 브라우저에서도 FTP를 통한 인터페이스 액세스를 허용합니다.

예: `ftp://192.10.10.10`

단계 **4** 수행하려는 특정 작업에 대한 디렉터리로 이동합니다. FTP를 통해 인터페이스에 액세스한 경우 다음 디렉터리로 이동하여 파일을 복사 및 추가("GET" 및 "PUT")할 수 있습니다. 다음 표를 참조하십시오.

표 ***114:*** 액세스 가능한 디렉터리

디렉터리 이름	설명
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지 또는 logconfig 및 rollovernow 명령을 통해 로깅을 위해 자동으로 생성되었습니다. 각 로그에 대한 자세한 내용은 Email Security Appliance 사용 설명서 또는 온라인 도움말의 "로깅" 장을 참조하십시오. 각 로그 파일 형식 간 차이점은 "로깅" 장의 "로그 파일 유형 비교"를 참조하십시오.
/configuration	다음 페이지 및 명령을 통해 (저장된) 데이터를 내보내거나 가져올 수 있는 디렉터리: • 가상 게이트웨이 매핑(altsrchost) • XML 형식의 구성 데이터(Saveconfig, loadconfig) • HAT(Host Access Table) 페이지(hostaccess) • RAT(Recipient Access Table) 페이지(rcptaccess) • SMTP 경로 페이지(smtproutes) • 별칭 테이블(aliasconfig) • 가장 테이블(masquerade) • 메시지 필터(filters) • 전역 수신 거부 데이터(unsubscribe) • trace 명령에 대한 테스트 메시지
/MFM	Mail Flow Monitoring 데이터베이스 디렉터리는 GUI에서 사용 가능한 Mail Flow Monitor 기능을 위한 데이터를 포함하고 있습니다. 각 하위 디렉터리에 README 파일이 있어 각 파일의 기록 형식을 문서화합니다. 기록 보관용으로 파일을 여러 시스템에 복사하거나 데이터베이스에 파일을 로드하고 직접 분석 애플리케이션을 개발할 수도 있습니다. 기록 형식은 모든 디렉터리, 모든 파일에서 동일합니다. 향후 릴리스에서는 이 형식이 바뀔 수 있습니다.

디렉터리 이름	설명
/periodic_reports	시스템에 구성된 모든 아카이브 보고서가 저장되는 디렉터리.

단계 **5** 해당 디렉터리에서 파일을 업로드 및 다운로드하려면 FTP 프로그램을 사용해 주십시오.

scp(Secure Copy 액세스

클라이언트 운영 체제에서 secure copy(scp) 명령을 지원할 경우 액세스 가능한 디렉터리 테이블에 나열된 디렉터리에 파일을 복사하거나 복사해올 수 있습니다. 예를 들면 다음 예에서 /tmp/test.txt파일은 클라이언트 시스템에서 호스트 이름이 mail3.example.com인 어플라이언스의 구성 디렉터리로 복사됩니다.

참고 사용자의 암호(admin)를 입력하라는 메시지가 표시됩니다. 다음 예는 참조용입니다. scp(secure copy) 구현은 운영 체제에 따라 다를 수 있습니다.

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's passphrase: (type the passphrase)
test.txt              100% |****************************|  1007       00:00
%
```

다음 예에서는 동일한 파일이 어플라이언스에서 클라이언트 시스템으로 복사됩니다.

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's passphrase: (type the passphrase)
test.txt              100% |****************************|  1007       00:00
```

Content Security Appliance와 파일을 주고받기 위해 FTP 대신 secure copy(scp)를 사용할 수 있습니다.

참고 Operators 및 Administrators 그룹의 사용자만이 secure copy(scp)를 사용하여 어플라이언스에 액세스할 수 있습니다. 자세한 내용은 AsyncOS 이전 버전으로 복귀, 462 페이지를 참고하십시오.

시리얼 연결을 통해 액세스

시리얼 연결을 통해 어플라이언스에 연결하는 경우 콘솔 포트에 대해 다음 정보를 사용하십시오.

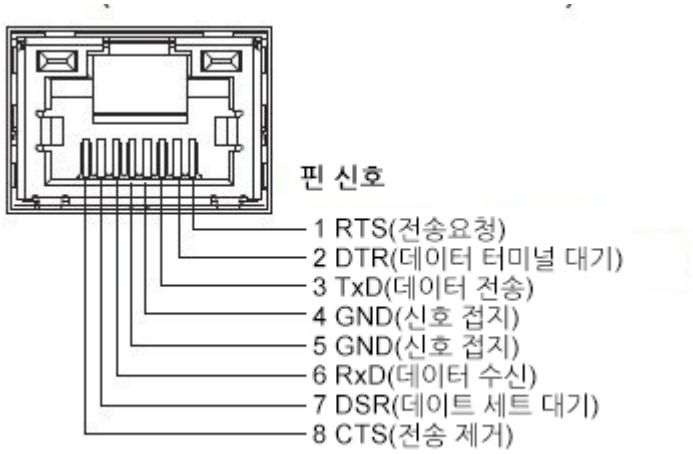
이 포트에 대한 자세한 정보는 사용 중인 어플라이언스의 하드웨어 설치 가이드에 나와 있습니다.

관련 주제

- 설명서 , 571 페이지

80-Series 및 90-Series 하드웨어에서 시리얼 포트에 대한 핀아웃 세부사항

그림 *21: 80-Series* 및 *90-Series* 하드웨어에서 시리얼 포트에 대한 핀아웃 세부사항



70-Series 하드웨어에서 시리얼 포트에 대한 핀아웃 세부사항

다음 표에서는 시리얼 포트 커넥터에 대한 핀 번호를 보여주고, *Serial Port Pin Assignments(*시리얼 포트 핀 할당*)* 테이블에서는 시리얼 포트 커넥터에 대한 핀 할당 및 인터페이스 신호를 정의합니다.

그림 *22:* 시리얼 포트에 대한 핀아웃 번호

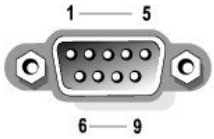


표 *115:* 시리얼 포트 핀 할당

PIN	신호	I/O	정의
1	DCD		Data carrier detect
2	SIN		Serial input
3	SOUT		Serial output
4	DTR		데이터 터미널 대기
5	GND	해당 없음	Signal ground

IP 인터페이스 및 어플라이언스 액세스

PIN	신호	I/O	정의
6	DSR		데이터 세트 대기
7	RTS		전송 요청
8	CTS		전송 제거
9	RI		Ring indicator
Shell	해당 없음	해당 없음	섀시 접지

IP 인터페이스 및 어플라이언스 액세스

B 부록

네트워크 및 IP 주소 할당

이 부록에는 다음 섹션이 포함되어 있습니다.

이더넷 인터페이스

Cisco CSA(Content Security Appliance)는 구성(선택 사항인 광 네트워크 인터페이스 유무)에 따라 시스템의 후면 패널에 최대 4개의 이더넷 인터페이스가 장착되어 있습니다. 다음과 같은 레이블이 지정됩니다.

- Management
- Data1
- Data2
- Data3
- Data4

IP 주소 및 넷마스크 선택

네트워크를 구성할 때 CSA는 발신 패킷을 전송할 고유 인터페이스를 선택할 수 있어야 합니다. 이 요구 사항에 따라 이더넷 인터페이스의 IP 주소 및 넷마스크 선택에서 몇 가지가 결정됩니다. 하나의 네트워크(인터페이스의 IP 주소에 넷마스크를 적용하여 결정됨)에는 하나의 인터페이스만 있다는 것이 규칙입니다.

IP 주소는 지정된 네트워크에서 물리적 인터페이스를 식별합니다. 물리적 이더넷 인터페이스는 패킷을 수신하는 IP 주소를 여러 개 가질 수 있습니다. IP 주소가 여러 개 있는 이더넷 인터페이스는 패킷의 소스 주소와 같은 IP 주소를 사용하는 인터페이스를 통해 패킷을 전송할 수 있습니다. 이러한 특성은 가상 게이트웨이 기술을 구현하는 데 사용됩니다.

넷마스크의 목적은 IP 주소를 네트워크 주소와 호스트 주소로 구분하는 것입니다. 네트워크 주소는 IP 주소의 네트워크 파트(넷마스크와 일치하는 비트)로 간주될 수 있습니다. 호스트 주소는 IP 주소의 나머지 비트입니다. 중요한 네 개 옥텟 주소의 비트 수는 때때로 CIDR(Classless Inter-Domain Routing) 스타일로 표현됩니다. 이는 비트 수(1-32) 뒤의 슬래시입니다.

이러한 수를 이진으로 계산하여 넷마스크를 표현할 수 있습니다. 따라서 255.255.255.0은 "/24"가 되고 255.255.240.0은 "/20"이 됩니다. ”

인터페이스 구성 샘플

이 섹션에서는 일부 일반 네트워크를 기반으로 한 샘플 인터페이스 구성을 보여줍니다. 다음 예에는 Int1 및 Int2라는 두 인터페이스가 사용됩니다. CSA의 경우 이 인터페이스 이름은 3개의 인터페이스(Management, Data1, Data2) 중 2개를 나타낼 수 있습니다.

Network 1:

각 인터페이스는 별도의 네트워크에 있는 것으로 표시되어야 합니다.

인터페이스	IP 주소	Netmask	네트워크주소
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

주소가 192.168.1.X(여기서 X는 1-255의 숫자, 자체 주소 제외, 이 경우 10)로 지정된 데이터는 Int1을 이용합니다. 주소가 192.168.0.X로 지정된 데이터는 Int2를 이용합니다. 이러한 형식이 아닌 다른 주소로 지정된 패킷(대부분 WAN이나 인터넷)은 이러한 네트워크 중 하나에 있는 기본 게이트웨이로 전송됩니다. 그러면 기본 게이트웨이는 해당 패킷을 전달합니다.

Network 2:

다른 두 인터페이스의 네트워크 주소(IP 주소의 네트워크 부분)는 동일할 수 없습니다.

이더넷인터페이스	IP 주소	Netmask	네트워크주소
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

이 상황은 두 가지 다른 이더넷 인터페이스의 네트워크 주소가 동일하여 충돌이 발생한 경우입니다. CSA의 패킷이 192.168.1.11로 전송되면 패킷을 전달하기 위해 어떤 이더넷 인터페이스를 사용해야 할지를 결정할 방법이 없습니다. 두 이더넷 인터페이스가 서로 다른 두 물리적 네트워크에 연결되어 있는 경우 해당 패킷은 잘못된 네트워크로 전달되어 목적지를 찾지 못할 수 있습니다. CSA에서는 충돌이 발생하도록 네트워크를 구성할 수 없습니다.

두 이더넷 인터페이스를 동일한 물리적 네트워크에 연결할 수 있지만, CSA가 고유한 전달 인터페이스를 선택할 수 있도록 IP 주소와 넷마스크를 구성해야 합니다.

IP 주소, 인터페이스 및 라우팅

GUI 또는 CLI에서 인터페이스를 선택하도록 허용하는 명령이나 기능(예: AsyncOS 업그레이드 또는 DNS 구성 등)을 수행하기 위해 인터페이스를 선택할 때 선택에 앞서 라우팅(기본 게이트웨이)이 발생합니다.

예를 들어 각각 서로 다른 네트워크 세그먼트에 3개의 네트워크 인터페이스가 구성된 CSA가 있다고 가정해보겠습니다(모두 /24로 가정).

이더넷	IP
Management	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

기본 게이트웨이는 192.19.0.1입니다.

이제 AsyncOS 업그레이드(또는 인터페이스 선택을 허용하는 다른 명령이나 기능)를 수행하면서 Data1(192.19.1.100)에 있는 IP를 선택하면, 모든 TCP 트래픽이 Data1 이더넷 인터페이스에서 발생할 것이라고 예상할 수 있습니다. 그러나 트래픽은 기본 게이트웨이로 설정된 인터페이스(이 경우 Management)에서 나가지만, Data1에서 IP의 소스 주소로 스탬프 처리됩니다.

요약

CSA는 패킷이 전달되는 고유한 인터페이스를 항상 식별할 수 있어야 합니다. 이 결정을 내리기 위해 CSA는 패킷의 목적지 IP 주소, 이더넷 인터페이스의 네트워크와 IP 주소 설정을 함께 사용합니다. 다음 표에는 위의 예가 요약되어 있습니다.

	동일한 네트워크	다른 네트워크
동일한 물리적 인터페이스	허용됨	허용됨
다른 물리적 인터페이스	허용되지 않음	허용됨

어플라이언스와 Cisco Threat Response 포털 통합

Cisco Threat Response 포털에 어플라이언스를 통합하고 Cisco Threat Response 포털에서 다음 작업을 수행할 수 있습니다.

- 조직의 여러 어플라이언스에서 이메일 보고, 메시지 추적, 그리고 웹 추적 데이터를 봅니다.
- 이메일 보고서, 메시지 추적 및 웹 추적에서 관찰된 위협을 식별하고 조사하고 치료합니다.
- 식별된 위협을 신속하게 해결하고 식별된 위협에 대해 수행할 권장 조치를 제공합니다.

네트워크 및 IP 주소 할당

- 포털에서 위협에 대해 문서화하여 조사를 저장하고, 포털의 다른 디바이스 간에 정보 협업을 활성화합니다.

참고 Cisco Threat Response 포털에서 Content Security Management Appliance의 통합을 지원하는 경우에만 위의 작업을 수행할 수 있습니다. Cisco Threat Response 포털에서 AsyncOS 12.0 for Cisco Content Security Management Appliance - Limited Deployment Release를 지원하지 않습니다.

Cisco Threat Response 포털에 어플라이언스를 통합하려면 Cisco Threat Response 포털에 어플라이언스를 등록해야 합니다.

시작하기 전에

- Cisco Threat Response 포털에서 관리자 액세스 권한이 있는 사용자 계정을 생성해야 합니다. Cisco Threat Response 포털 사용자 계정을 생성하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.
- Cisco Threat Response 포털에 어플라이언스를 등록하려면 다음 FQDN에 대해 HTTPS(In 및 Out) 443 포트를 열어야 합니다.
  - api-sse.cisco.com
  - est.sco.cisco.com

자세한 내용은 방화벽 정보, 563 페이지의 내용을 참고하십시오.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** **Networks**(네트워크) **> Cloud Service Settings**(**Cloud** 서비스 설정)를 선택합니다.

단계 **3** **Edit Settings**(설정 편집)를 클릭합니다.

단계 **4** **Enable**(활성화) 체크 박스를 선택합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

단계 **6** 몇 분 후 다시 Cloud Service Settings(클라우드 서비스 설정) 페이지로 이동하여 Cisco Threat Response 포털에 어플라이언스를 등록합니다.

단계 **7** Cisco Threat Response 포털에서 등록 토큰을 가져와 Cisco Threat Response 포털에 어플라이언스를 등록합니다. 자세한 내용은 Cisco Threat Grid 설명서(https://visibility.amp.cisco.com/#/help/module-sma)를 참고하십시오.

단계 **8** Cisco Threat Response 포털에서 가져온 등록 토큰을 입력하고 **Register**(등록)를 클릭합니다.

단계 **9** 9. Cisco Threat Response 포털에 통합 모듈로 어플라이언스를 추가합니다. 자세한 내용은 Cisco Threat Grid 설명서(https://visibility.amp.cisco.com/#/help/module-sma)를 참고하십시오.

다음에 수행할 작업

Cisco Threat Response 포털에 통합 모듈로 어플라이언스를 추가한 후에는 Cisco Threat Response 포털의 어플라이언스에서 이메일 보고, 메시지 추적, 그리고 웹 추적 정보를 볼 수 있습니다. 자세한 내용은 Cisco Threat Grid 설명서(https://visibility.amp.cisco.com/#/help/module-sma)를 참고하십시오.

참고 Cisco Threat Response 포털에서 어플라이언스 연결의 등록을 취소하려면 어플라이언스의 Cloud Services Settings(클라우드 서비스 설정) 페이지에서 **Deregister(등록 취소)**를 클릭합니다.

CLI를 사용하여 Cisco Threat Response 포털에 어플라이언스 통합

이 섹션은 다음 CLI 명령으로 구성됩니다.

- threatresponseconfig, 559 페이지
- cloudserviceconfig, 560 페이지

threatresponseconfig

설명

`threatresponseconfig` 명령은 다음 작업에 사용됩니다.

- 어플라이언스에서 Cisco Threat Response 기능을 활성화합니다.
- 어플라이언스에서 Cisco Threat Response 기능을 비활성화합니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

예

다음 예에서는 `threatresponseconfig` 명령을 사용하여 어플라이언스에서 Cisco Threat Response 기능을 활성화할 수 있습니다.

```
mail1.example.com> threatresponseconfig

Choose the operation you want to perform:
- ENABLE - To enable the Cisco Threat Response feature on your appliance.
[]> enable
```

```
The Cisco Threat Response feature is currently enabled on your appliance. Use the
cloudserviceconfig command to register your appliance with the Cisco Threat
Response portal.

mail1.example.com> commit

Please enter some comments describing your changes:
[]>

Changes committed: Mon Nov 19 10:04:35 2018 GMT
```

다음 예에서는 `threatresponseconfig` 명령을 사용하여 어플라이언스에서 Cisco Threat Response 기능을 비활성화할 수 있습니다.

```
mail1.example.com> threatresponseconfig

Choose the operation you want to perform:
- DISABLE - To disable the Cisco Threat Response feature on your appliance.
[]> disable

The Cisco Threat Response feature is currently disabled on your appliance.

mail1.example.com> commit

Please enter some comments describing your changes:
[]>

Changes committed: Mon Nov 19 10:04:35 2018 GMT
```

cloudserviceconfig

설명

`cloudserviceconfig` 명령은 다음 작업에 사용됩니다.

- Cisco Threat Response 포털에 어플라이언스를 등록합니다.
- Cisco Threat Response 포털에서 어플라이언스를 등록 취소합니다.

Usage(사용**)**

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령**:** 이 명령은 배치 형식을 지원합니다.

예

다음 예에서는 `cloudserviceconfig` 명령을 사용하여 Cisco Threat Response 포털에 어플라이언스를 등록할 수 있습니다.

```
mail1.example.com> cloudserviceconfig

Choose the operation you want to perform:

- REGISTER - To register the appliance with the Cisco Threat Response portal.
[]> register
```

```
Enter a registration token key to register your appliance with the Cisco Threat
Response portal.
[]> de7c55f3ff0absdfsf4a25aae94dfb064642

The appliance registration is in progress.
```

다음 예에서는 `threatresponseconfig` 명령을 사용하여 Cisco Threat Response 포털에서 어플라이언스 등록을 취소할 수 있습니다.

```
mail1.example.com> cloudserviceconfig

The Content Security Management appliance is successfully registered with the
Cisco Threat Response portal.

Choose the operation you want to perform:
- DEREGISTER - To deregister the appliance from the Cisco Threat Response
portal.
[]> deregister

Do you want to deregister your appliance from the Cisco Threat Response portal.

If you deregister, you will not be able to access the Cloud Service features. [N]> yes

The Content Security Management appliance deregistration is in progress.
```

CSA 연결을 위한 전략

어플라이언스를 연결할 때 다음 사항을 염두에 두어야 합니다.

- 관리 트래픽(CLI, 웹 인터페이스, 로그 전달)은 이메일 트래픽에 비해 일반적으로 규모가 작습니다.
- 이더넷 인터페이스가 동일한 네트워크 스위치에 연결되어 있지만 또 다른 호스트 다운스트림의 단일 인터페이스로 끝나는 경우 또는 모든 데이터가 모든 포트로 에코되는 네트워크 허브에 연결된 경우 두 인터페이스 사용에 따른 이점이 없습니다.
- 1000Base-T에서 작동하는 인터페이스를 통한 SMTP 대화는 100Base-T에서 작동하는 동일한 인터페이스를 통한 대화보다 약간 빠르지만, 이상적인 조건에서 그렇습니다.
- 전달 네트워크의 다른 부분에 병목이 있으면 네트워크에 대한 연결 최적화가 도움이 되지 않습니다. 병목은 인터넷 연결에서, 더 나아가 연결 공급업체에서 가장 자주 발생합니다.

연결하기 위해 선택하는 인터페이스의 수 및 이를 확인하는 방법은 기반 네트워크의 복잡성에 의해 결정됩니다. 네트워크 토폴로지 또는 데이터 볼륨에서 요구하지 않는 경우 여러 인터페이스에 연결할 필요가 없습니다. 게이트웨이에 친숙해질 때까지 우선 연결을 간단하게 유지한 다음, 볼륨 및 네트워크 토폴로지에서 요구할 때 연결을 확장할 수도 있습니다.

C 부록

방화벽 정보

이 장에는 다음 섹션이 포함되어 있습니다.

방화벽 정보

다음 표에는 Cisco Content Security Appliance의 적절한 작동을 위해 열어야 할 수 있는 가능한 포트가 기본값으로 나열되어 있습니다.

표 ***116:*** 방화벽 포트

기본 포트	**Protocol(**프로토콜**)**	**In/Out**	**Hostname**	목적
20/21	TCP	In/Out	AsyncOS IP, FTP 서버	로그 파일의 어그리게이션을 위한 FTP. 데이터 포트 TCP 1024 이상은 모두 열려 있어야 합니다. 자세한 내용은 기술 자료의 FTP 포트 정보를 검색하십시오. 기술 자료(TechNotes) , 573 페이지 를 참조하십시오.
22	SSH	Out	AsyncOS IP	중앙 구성 관리자 구성 푸시. 백업에도 사용.
22	TCP	In	AsyncOS IP	CLI에 대한 SSH 액세스, 로그 파일의 어그리게이션.
22	TCP	Out	SCP 서버	로그 서버에 SCP 푸시.
23	텔넷	In	AsyncOS IP	CLI에 텔넷 액세스.

방화벽 정보

23	텔넷	아웃	텔넷 서버	텔넷 업그레이드
25	TCP	Out	모두	이메일을 전송하기 위한SMTP입니다.
25	TCP	In	AsyncOS IP	반송된 메일 또는 방화벽 외부에서 주입되는 메일을 수신하기 위한 SMTP.
53	UDP/TCP	Out	DNS 서버	인터넷 루트 서버 또는 방화벽 외부의 다른 DNS 서버를 사용하도록 구성된 경우 DNS. SenderBase 쿼리에도 해당.
80	HTTP	In	AsyncOS IP	시스템 모니터링용 GUI에 대한 HTTP 액세스.
80	HTTP	Out	downloads.ironport.com	AsyncOS 업그레이드
80	HTTP	Out	upgrades.ironport.com	AsyncOS 업그레이드.
801	HTTP	In 및 Out	AsyncOS IP	`trailblazerconfig` CLI 명령을 사용하여 GUI에 대한 HTTP 액세스.
82	HTTP	In	AsyncOS IP	스팸 격리를 보는 데 사용.
83	HTTPS	In	AsyncOS IP	스팸 격리를 보는 데 사용.
110	TCP	Out	POP 서버	스팸 격리를 위한 엔드유저 POP 인증.
123	UDP	In 및 Out	NTP 서버	시간 서버가 방화벽 외부에 있는 경우 NTP.
143	TCP	Out	IMAP 서버	스팸 격리를 위한 엔드유저 IMAP 인증.
161	UDP	In	AsyncOS IP	SNMP 쿼리.
162	UDP	Out	관리 스테이션	SNMP 트랩.
389 또는 3268	LDAP	Out	LDAP 서버	LDAP 디렉터리 서버가 방화벽 외부에 있는 경우 LDAP. Cisco Spam Quarantine을 위한 LDAP 인증.
636 또는 3269	LDAPS	Out	LDAPS	LDAPS - ActiveDirectory의 Global Catalog Server(SSL 사용).

443	TCP	In	AsyncOS IP	시스템 모니터링용 GUI에 대한 보안 HTTP(https) 액세스.
443	TCP	Out	update-static.ironport.com	업데이트 서버에 대한 최신 파일을 확인합니다.
443	TCP	Out	update-manifests.ironport.com	업데이트 서버에서 최신 파일 목록을 가져옵니다(물리적 하드웨어 어플라이언스용).
443	TCP	Out	update-manifests.sco.cisco.com	업데이트 서버에서 최신 파일 목록을 가져옵니다(가상 어플라이언스용).
443	TCP	Out	phonehome.senderbase.org	Outbreak Filter 수신/전송.
443	TCP	Out	Security Services(보안 서비스) > Anti-Malware and Reputation(악성코드 차단 및 평판) 페이지, Advanced(고급) 섹션 > Advanced Settings for File Analysis(파일 분석 고급 설정)에서 WSA에 대해 구성된 파일 분석 서버 URL. Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석) 페이지, Advanced Settings for File Analysis(파일 분석 고급 설정) 섹션에서 ESA에 대해 구성된 파일 분석 서버 URL.	파일 분석 서버에 파일 분석 세부 결과 표시. • 웹 보안 보고: (클라우드 파일 분석) 관리 어플라이언스에서 파일 분석 서버와 연결할 수 있음을 확인, 199 페이지
443	HTTPS	In 및 Out	api-sse.cisco.com	Cisco Threat Response 포털에 어플라이언스를 등록하는 데 사용됩니다.
443	HTTPS	In 및 Out	est.sco.cisco.com	인증서를 다운로드하여 어플라이언스가 Cisco Threat Response 포털에 등록할 때 확인된 사이트에 액세스하고 있는지 확인하는 데 사용됩니다.
4431	HTTPS	In 및 Out	AsyncOS IP	`trailblazerconfig` CLI 명령을 사용하여 GUI에 대한 HTTPS 액세스.
514	UDP/TCP	Out	Syslog 서버	Syslog 로깅.

방화벽 정보

1024 이상	—	—	—	포트 21(FTP)은 위 정보를 참조하십시오.
7025	TCP	In/Out	AsyncOS IP	이 기능이 중앙에서 관리되는 경우 Email Security Appliance와 Security Management Appliance 간 통과 정책, 바이러스 및 보안 침해 격리 데이터.
32137	TCP			
6080	HTTP	In or Out		HTTP 서버용 API 포트 액세스
6443	HTTPS	In or Out		HTTPS 서버용 API 포트 액세스

부록 D

웹 보안 관리의 예

이 장에는 다음 섹션이 포함되어 있습니다.

웹 보안 관리의 예

이 부록에서는 Cisco Content Security Management Appliance의 기능을 구현하는 여러 일반적인 방법을 설명하며 다음과 같이 구성되었습니다.

Web Security Appliance의 예

이 섹션에서는 Security Management Appliance 및 Web Security Appliance를 사용하는 예를 설명합니다.

참고 이 모든 시나리오는 Security Management Appliance 및 Web Security Appliance에서 웹 보고 및 웹 추적을 활성화했다고 가정합니다. 웹 추적 및 웹 보고를 활성화하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오. 중앙 웹 보고 및 추적 사용, 177 페이지

예 1: 사용자 조사

이 예에서는 시스템 관리자가 회사의 특정 사용자를 조사하는 방법을 보여줍니다.

이 시나리오에서 관리자가 어떤 직원이 업무 중에 부적절한 웹 사이트를 방문한다는 불만 신고를 접수했습니다. 시스템 관리자가 이를 조사하려면 웹 활동의 세부 사항을 추적해야 합니다.

웹 활동을 추적한 다음 해당 직원의 탐색 기록에 대한 정보와 함께 웹 보고서가 생성됩니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > Users(사용자)**를 선택합니다.

단계 **2** **Users(사용자)** 테이블에서 조사할 사용자 **ID** 또는 클라이언트 **IP** 주소를 클릭합니다.

사용자 ID 또는 클라이언트 IP 주소를 모를 경우 텍스트 필드에 그 사용자 ID 또는 클라이언트 IP 주소에 대해 기억나는 것을 입력하고 **Find User ID or Client IP address(사용자 ID 또는 클라이언트 주소 찾기)**를 클릭합니다. IP 주소가 정확하게 일치하지 않아도 결과를 얻을 수 있습니다. 지정한 사용자 ID 및 클라이언트 IP 주소로 사용자 테이블이 채워집니다. 여기서는 클라이언트 IP 주소 `10.251.60.24`에 대한 정보를 찾고 있습니다.

단계 **3** IP 주소 **`10.251.60.24`**를 클릭합니다.

`10.251.60.24`에 대한 사용자 세부 정보 페이지가 나타납니다.

사용자 세부사항 페이지에서 총 트랜잭션의 URL 범주, 총 트랜잭션의 추이, 매칭된 URL 범주, 매칭된 도메인, 매칭된 애플리케이션, 탐지된 악성코드 위협, 매칭된 정책을 확인할 수 있습니다.

이 카테고리를 통해 이를테면 사용자 `10.251.60.24`가 차단된 URL을 액세스하려 했음을 알 수 있습니다. 이 URL은 페이지의 도메인 섹션 아래 차단된 트랜잭션 열에 있습니다.

단계 **4** 매칭된 도메인 테이블 아래의 **Export(내보내기)**를 클릭하여 사용자가 액세스하려 한 도메인 및 URL의 전체 목록을 표시합니다.

여기서 웹 추적 기능을 사용하여 이 사용자의 웹 사용을 추적하고 볼 수 있습니다.

참고 웹 보고에서는 사용자가 이동한 모든 도메인 정보를 검색할 수 있습니다. 즉 액세스한 특정 URL이 아닐 수도 있습니다. 사용자가 액세스하고 있는 특정 URL, 그 URL로 이동한 시간, URL 허용 여부 등을 알아보려면 웹 추적 페이지의 프록시 서비스 탭을 사용합니다.

단계 **5** **Web(웹) > Reporting(보고) > Web Tracking(웹 추적)**을 선택합니다.

단계 **6** **Proxy Services(프록시 서비스)** 탭을 클릭합니다.

단계 **7** User/Client IP Address(사용자/클라이언트 IP 주소) 텍스트 필드에 사용자 이름 또는 IP 주소를 입력합니다.

여기서는 사용자 `10.251.60.24`의 웹 추적 정보를 검색하고 있습니다.

검색 결과가 나타납니다.

이 페이지에서 IP 주소가 `10.251.60.24`인 컴퓨터의 사용자가 방문한 URL 및 트랜잭션의 전체 목록을 볼 수 있습니다.

관련 주제

다음 표에는 이 예에서 다룬 주제가 각각 나열됩니다. 링크를 클릭하면 각 항목에 대한 세부사항이 표시됩니다.

표 ***117:*** 사용자 조사 관련 주제

기능 이름	기능 정보
사용자 페이지	사용자 보고서(웹) , 187 페이지

기능 이름	기능 정보
사용자 세부사항 페이지	사용자 세부사항(웹 보고) , 189 페이지
보고서 데이터 내보내기	보고/추적 데이터 인쇄 및 내보내기 , 41 페이지
웹 추적 페이지의 프록시 서비스 탭	웹 프록시 서비스에서 처리한 트랜잭션 검색 , 245 페이지

예 2: URL 추적

이 시나리오에서는 세일즈 관리자가 지난주 최다 방문 회사 웹 사이트 5개를 찾으려 합니다. 또한 어떤 사용자가 이 웹 사이트를 찾는지 알고 싶습니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > Web Sites(웹 사이트)**을 선택합니다.

단계 **2** Time Range(시간 범위) 드롭다운 목록에서 **Week(주)**를 선택합니다.

단계 **3** 아래로 스크롤하여 도메인 섹션에서 방문한 도메인 또는 웹 사이트를 확인합니다.

상위 25개 웹 사이트가 매칭된 도메인 테이블에 표시됩니다. 같은 테이블에서 도메인 또는 IP 열의 링크를 클릭하면 해당 주소 또는 사용자의 실제 웹 사이트가 표시됩니다.

관련 주제

다음 표에는 이 예에서 다룬 주제가 각각 나열됩니다. 링크를 클릭하면 각 항목에 대한 세부사항이 표시됩니다.

표 ***118: URL*** 추적 관련 주제

기능 이름	기능 정보
웹 사이트 페이지	웹 사이트 보고서 , 190 페이지

예 3: 최다 방문 URL 범주 조사

이 시나리오에서는 인사팀 관리자가 직원들이 30일간 가장 많이 방문한 URL 범주 3개를 알아내려 합니다. 또한 네트워크 관리자는 이 정보를 활용하여 대역폭 사용 현황을 모니터링함으로써 네트워크에서 대역폭 사용량이 가장 많은 URL을 확인하고 싶습니다.

아래의 예에서는 여러 사람의 여러 관심사에 대한 데이터를 수집하되 단일 보고서로 통합하는 방법을 보여줍니다.

단계 **1** Security Management Appliance에서 **Web(웹) > Reporting(보고) > URL Categories(URL 카테고리)**를 선택합니다.

이 예의 URL 범주 페이지를 보면 총 트랜잭션 기준 상위 10개 URL 범주 그래프가 나타납니다. 282,000개의 미분류 URL에 액세스했고 인스턴트 메시징, 혐오 발언, 타투 사이트 등도 있었습니다.

이제 **Export(**내보내기**)** 링크를 클릭하여 이 원시 데이터를 Excel 스프레드시트로 내보내고 인사팀 관리자에게 파일을 보낼 수 있습니다. 하지만 네트워크 관리자도 각 URL의 대역폭 사용량을 알아야 합니다.

단계 **2** NEEDS NEW ILLO - 아래로 스크롤하여 **URL Categories Matched(**일치하는 **URL** 카테고리**)** 테이블에서 Bandwidth Used(대역폭 사용) 열을 확인합니다.

URL Categories Matched(매칭한 **URL** 범주**)** 테이블에서는 모든 URL 범주의 대역폭 사용량을 확인할 수 있습니다. 여기서도 **Export(**내보내기**)** 링크를 클릭하여 네트워크 관리자에게 이 파일을 보낼 수 있습니다. 하지만 더 세부적인 분석을 위해 인스턴트 메시징 링크를 클릭하여 어떤 사용자가 대역폭을 사용하고 있는지 확인합니다. 다음 페이지가 나타납니다.

네트워크 관리자는 이 페이지에서 인스턴트 메시징 사이트의 최다 이용자 10명을 확인할 수 있습니다.

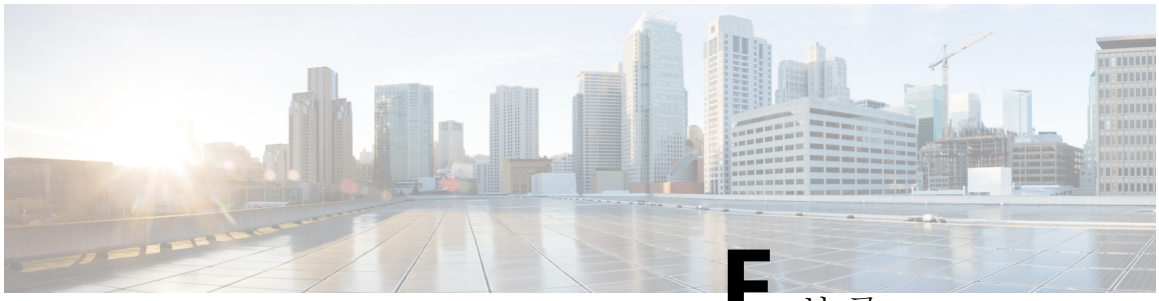
또한 지난 30일간 사용자 10.128.4.64가 인스턴트 메시징 사이트에서 19시간 57분을 보냈으며 이 시간의 대역폭 사용량은 10.1MB였음을 이 페이지에서 알 수 있습니다.

관련 주제

다음 표에는 이 예에서 다룬 주제가 각각 나열됩니다. 링크를 클릭하면 각 항목에 대한 세부사항이 표시됩니다.

표 ***119:*** 상위 ***URL*** 범주 조사 관련 주제

기능 이름	기능 정보
URL 범주 페이지	URL 범주 보고서 , 191 페이지
보고서 데이터 내보내기	보고/추적 데이터 인쇄 및 내보내기 , 41 페이지



E 부록

추가 리소스

이 장에는 다음 섹션이 포함되어 있습니다.

Cisco 알림 서비스

보안 자문, 현장 통지, 판매 중단 및 지원 종료 안내문, 소프트웨어 업데이트 및 알려진 문제에 대한 정보 등 Cisco Content Security Appliance와 관련된 알림을 수신하려면 신청하십시오.

알림 빈도, 수신할 정보 유형 등의 옵션을 지정할 수 있습니다. 사용하는 각 제품에 대한 알림을 받으려면 개별적으로 신청해야 합니다.

등록하려면 다음 위치를 방문하십시오. http://www.cisco.com/cisco/support/notifications.html

Cisco.com 계정이 필요합니다. 계정이 없으면 Cisco 계정 등록 , 573 페이지 섹션을 참조해 주십시오.

설명서

이 제품 및 관련 제품에 대한 문서는 다음 위치에서 구할 수 있습니다.

Cisco Content Security 제품용 설명서:	위치:
Security Management Appliance	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html 하드웨어 및 가상 어플라이언스 정보: http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html MIB: SNMP로 시스템 상태 모니터링 , 438 페이지를 참조하십시오.
Web Security Appliance	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Email Security Appliance	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
콘텐츠 보안 제품 명령행 참조 설명서	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

어플라이언스 GUI의 오른쪽 상단에 있는 **Help and Support**(도움말 및 지원)를 클릭하여 사용 설명서의 HTML 온라인 도움말 버전에 직접 액세스할 수 있습니다.

서드파티 지원업체

AsyncOS에 포함된 일부 소프트웨어는 FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc. 및 기타 서드파티 기여자의 소프트웨어 라이센스 계약의 약관과 통지에 따라 배포되며, 모든 해당 약관은 Cisco 라이센스 계약에 통합되어 있습니다.

타사 라이선스에 대한 정보는 http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html 및 https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html의 라이선싱 문서에서 확인할 수 있습니다.

AsyncOS에 포함된 소프트웨어의 일부는 Tobi Oetiker가 명시적으로 서면 동의한 RRDtool을 기반으로 합니다.

이 문서의 일부는 Dell Computer Corporation의 허가로 다시 작성되었습니다. 이 문서의 일부는 McAfee, Inc.의 허가로 다시 작성되었습니다. 이 문서의 일부는 Sophos Plc.의 허가로 다시 작성되었습니다.

교육

교육 옵션은 다음을 참조하십시오.

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

기술 자료(TechNotes)

프로시저

	명령 또는 동작	목적
단계 1	기본 제품 페이지 (http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html)로 이동합니다.	
단계 2	**TechNotes**라는 이름의 링크를 찾습니다.	

Cisco Support Community

Cisco 지원 커뮤니티는 Cisco 고객, 파트너, 직원을 위한 온라인 포럼입니다. 여기서 일반적인 콘텐츠 보안 문제에 대해 논의하고 특정 Cisco 제품에 대한 기술 정보를 얻을 수 있습니다. 포럼에 주제를 게시하여 궁금한 점을 질문하고 다른 사용자와 정보를 공유할 수 있습니다.

다음 URL에서 Cisco 지원 커뮤니티에 액세스하십시오.

- 이메일 보안 및 관련 관리:

  https://supportforums.cisco.com/community/5756/email-security

- 웹 보안 및 관련 관리:

  https://supportforums.cisco.com/community/5786/web-security

고객 지원

다음 방법을 사용하여 지원을 받을 수 있습니다.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

레거시 IronPort에 대한 지원 사이트:http://www.cisco.com/web/services/acquisitions/ironport.html

리셀러 또는 다른 공급자를 통해 지원을 구매한 경우 제품 지원 문제는 해당 공급자에게 직접 문의해 주십시오.

어플라이언스에서 지원 사례 열기 또는 업데이트 , 540 페이지도 참조하십시오.

가상 어플라이언스에 대해서는 *Cisco Content Security Virtual Appliance* 설치 설명서를 참조하십시오.

Cisco 계정 등록

Cisco.com의 많은 리소스에 액세스하려면 Cisco 계정이 필요합니다.

Cisco.com 사용자 ID가 없는 경우 다음에서 등록할 수 있습니다. https://tools.cisco.com/RPF/register/register.do

관련 주제

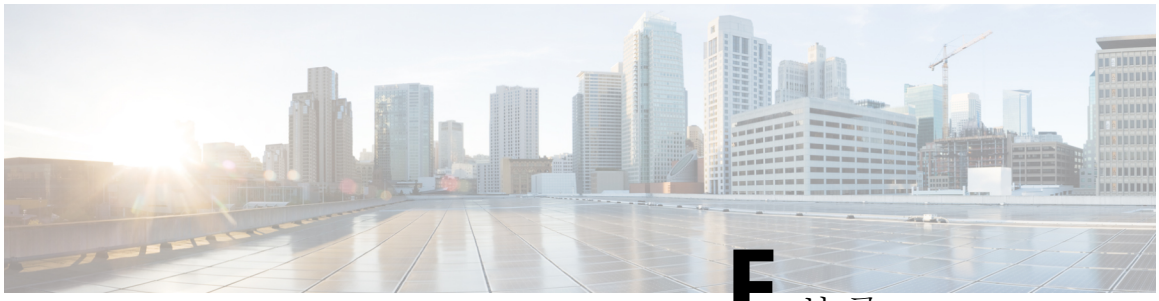
- Cisco 알림 서비스 , 571 페이지
- 기술 자료(TechNotes) , 573 페이지

Cisco에 의견 보내기

기술 출판 팀은 더 우수한 제품 설명서를 제공하기 위해 최선을 다하고 있습니다. 소중한 의견과 제안을 언제라도 보내주십시오. 다음 이메일 주소로 의견을 보내실 수 있습니다.

contentsecuritydocs@cisco.com

메시지의 제목에 이 책의 제목 및 제목 페이지에 표시된 발행일을 기재해주십시오.



F 부 록

최종 사용자 라이센스 계약

이 장에는 다음 섹션이 포함되어 있습니다.

Cisco Systems 최종 사용자 라이센스 계약

중요: 본 최종 사용자 라이센스 계약을 주의 깊게 읽으십시오. 귀하가 **CISCO** 소프트웨어 또는 장비를 승인된 소스로부터 구매하고 있는지, 그리고 귀하 또는 귀하가 대표하는 실체("고객"으로 통칭)가 본 **CISCO** 최종 사용자 라이센스 계약의 목적에 맞게 최종 사용자로 등록되었는지를 확인하는 것이 매우 중요합니다. 귀하는 최종 사용자로 등록되어 있지 않은 경우 소프트웨어를 사용할 라이센스가 없으며 본 최종 사용자 라이센스 계약의 제한된 보증이 적용되지 않습니다. **CISCO** 또는 **CISCO** 제공 소프트웨어를 승인된 소스로부터 구매하고 다운로드, 설치 또는 사용하는 경우 귀하는 본 계약에 동의하는 것입니다.

Cisco Systems, Inc. 또는 CISCO SYSTEMS, INC. 대신 소프트웨어를 라이센싱하는 자회사("CISCO")는 귀하가 소프트웨어를 승인된 소스로부터 구매한 경우 그리고 본 최종 사용자 라이센스 계약에 포함된 모든 약관 및 제품에 수반되거나 주문 시 사용 가능한 보충 라이센스 계약("계약"으로 통칭)에 명시된 모든 추가 제한 사항에 동의하는 경우에만 본 소프트웨어의 라이센스를 부여합니다. 본 최종 사용자 라이센스 계약 및 보충 라이센스 계약의 조건이 상충하는 경우 보충 라이센스 계약이 적용됩니다. 소프트웨어를 다운로드, 설치 또는 사용함으로써 귀하는 소프트웨어를 승인된 소스로부터 구매하였으며 계약을 준수할 것임을 나타내는 것입니다. 귀하가 계약의 모든 조건에 동의하지 않는 경우 CISCO는 귀하에게 소프트웨어에 대한 라이센스를 부여하지 않으며, (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고 (B) 귀하는 전액 환불을 위해 소프트웨어를 반환(개봉하지 않은 CD 패키지 및 서면 자료 포함)할 수 있으며, 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 귀하는 전액 환불을 위해 전체 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권리는 승인된 소스로부터 구매한 지 30일 후에 만료되며, 귀하가 등록되어 있는 원래 최종 사용자 구매자인 경우에만 적용됩니다. 본 최종 사용자 라이센스 계약에서 "승인된 소스"란 (A) CISCO 또는 (B) 해당 지역 내에서 최종 사용자에게 CISCO 장비, 소프트웨어 및 서비스를 배포하도록 CISCO에서 승인한 총판사 또는 시스템 통합업체 또는 (C) 그러한 총판사 또는 시스템 통합업체에서 CISCO와 총판사의 계약 조건에 따라 해당 지역 내에서 최종 사용자에게 CISCO 장비, 소프트웨어 및 서비스를 배포/판매하도록 승인한 리셀러를 의미합니다.

최종 사용자 라이센스 계약

다음의 계약 조건은 고객의 소프트웨어 사용*(*아래에 정의*)*을 제어하되, *(A)* 고객과 고객의 소프트웨어 사용을 제어하는 *CISCO* 간에 별도의 서명된 계약이 있는 경우 또는 *(B)* 고객의 소프트웨어 사용을 제어하는 설치 또는 다운로드 프로세스의 일부로서 소프트웨어에 별도의 *"*클릭-동의*"* 라이센스 계약 또는 서드파티 라이센스 계약이 포함된 경우는 예외입니다. 앞서 언급한 문서의 조항이 상충하는 경우 우선순위는 *(1)* 서명된 계약, *(2)* 클릭-동의 계약 또는 서드파티 라이센스 계약, *(3)* 본 계약입니다. 본 계약에서 *"*소프트웨어*"*란 컴퓨터 프로그램*(*승인된 소스에서 고객에게 제공된 *CISCO* 장비에 내장된 펌웨어 및 컴퓨터 프로그램 포함*)*, 업그레이드, 업데이트, 버그 픽스 또는 이에 따른 수정 버전*(*"업그레이드"로 통칭*)*, *CISCO* 소프트웨어 양도 및 재라이센싱 정책*(CISCO*에서 수시로 수정 가능*)*에 따라 재라이센스된 것 또는 그러한 것의 백업 사본을 의미합니다.

라이센스. 본 계약의 약관을 준수하는 범위에서 Cisco는 고객이 승인된 소스에 필요한 라이센스 요금을 지불한 소프트웨어 및 문서를 고객의 내부 비즈니스 목적으로 사용할 비독점적이고 양도 불가능한 라이센스를 부여합니다. "문서"란 소프트웨어에 관해 작성되어 승인된 소스에서 어떤 방식으로든 (CD-ROM 또는 온라인) 소프트웨어와 함께 사용하도록 제공하는 정보(사용자 또는 기술 매뉴얼, 교육 자료, 사양 등)를 의미합니다. 소프트웨어를 사용하려면 고객은 등록 번호나 제품 인증 키를 입력하고 Cisco 웹사이트에서 소프트웨어의 고객 사본을 온라인으로 등록하여 필요한 라이센스 키 또는 라이센스 파일을 얻어야 할 수 있습니다.

고객의 소프트웨어 사용 라이센스 및 소프트웨어 사용 범위는 단일 하드웨어 섀시나 카드로 제한되거나, 해당 보충 라이센스 계약에 명시되거나 승인된 소스가 동의했고 고객이 승인된 소스에 필요한 라이센스 요금을 지불한 해당 구매 발주서("구매 발주서")에 명시된 기타 제한 사항으로 제한됩니다.

문서 또는 해당되는 보충 라이센스 계약에 달리 명시하지 않는 한 고객은 소프트웨어를 내장된 대로 실행에 사용하거나, (해당 문서에서 비 Cisco 장비에 설치를 허용한 경우) 고객이 소유하거나 임대한 Cisco 장비와의 통신 및 고객의 내부 비즈니스 용도로 사용할 수 있습니다. 암시, 금반언 등에 의해 다른 어떤 라이센스도 부여되지 않습니다.

Cisco에서 라이센스 요금을 부과하지 않는 평가판 또는 베타 사본의 경우 위의 라이센스 요금 지불 요건이 적용되지 않습니다.

일반 제한 사항. 타이틀의 양도가 아니라 소프트웨어 및 문서에 대한 라이센스이므로 Cisco는 소프트웨어 및 문서의 모든 사본에 대한 소유권을 보유합니다. 소프트웨어 및 문서에는 개별 프로그램의 특정 내부 설계와 구조 및 관련 인터페이스 정보를 포함하여(이에 제한되지 않음) Cisco 또는 공급업체나 라이센스 허가업체의 영업 비밀이 포함되어 있음을 고객은 인지합니다. 계약에 달리 명시하지 않는 한 고객은 승인된 소스로부터 구매한 Cisco 장비의 사용과 연결해서만 소프트웨어를 사용하며, 고객은 다음에 대해 권리가 없고 다음을 수행하지 않을 것에 특별히 동의합니다.

(i) 타인 또는 다른 실체에 라이센스 권리를 양도하거나 하위 라이센스를 부여하거나(Cisco 재라이센싱/양도 정책 적용의 준수 외), 고객이 승인된 소스로부터 구매하지 않은 Cisco 장비 또는 중고 Cisco 장비에서 소프트웨어를 사용하는 행위. 고객은 양도, 하위 라이센스 부여 또는 사용을 시도하는 행위가 무효임을 인지합니다.

(ii) 오류를 고치거나 소프트웨어를 달리 수정 또는 각색하거나 소프트웨어를 기반으로 파생물을 만들거나 서드파티에 동일한 일을 하도록 허용하는 행위.

(iii) 소프트웨어를 리버스 엔지니어링 또는 디컴파일, 해독, 디스어셈블하거나 인간이 읽을 수 있는 형식으로 축소하는 행위. 단, 이러한 제한에도 불구하고 적용법에 따라 명시적으로 허가되거나 적용되는 오픈 소스 라이센스에 따라 Cisco가 특정 활동을 허가해야 하는 경우는 예외입니다.

(iv) 소프트웨어에서 실행되는 벤치마크 테스트의 결과를 게시하는 행위.

(v) Cisco의 명시적인 서면 인증 없이 서비스 사무소에서 또는 시간 공유 기반으로 서드파티의 서비스를 수행하는 데 소프트웨어를 사용하거나 사용하도록 허가하는 행위.

(vi) Cisco의 사전 서면 승인 없이 소프트웨어 및 문서 내에 포함된 영업 비밀을 서드파티에서 사용할 수 있도록 공개, 제공 또는 달리 조작하는 행위. 고객은 그러한 영업 비밀을 보호하기 위해 합당한 보안 조치를 취해야 합니다.

적용법의 요구에 따라 그리고 고객의 서면 요청에 따라 Cisco는 해당 요금을 Cisco에 지불하는 경우 소프트웨어와 다른 독립적으로 생성된 프로그램 간 상호 운용성을 위해 필요한 인터페이스 정보를 고객에게 제공합니다. 고객은 그러한 정보와 관련된 기밀 유지의 책임을 엄격히 준수해야 하며, Cisco에서 그러한 정보를 사용 가능하게 하는 해당 약관에 따라 그러한 정보를 사용해야 합니다.

소프트웨어, 업그레이드 및 추가 사본. 계약의 다른 조항에도 불구하고 (1) 사본이나 업그레이드를 만들거나 얻은 시점에 고객이 이미 원본 소프트웨어에 대한 유효한 라이선스를 보유하고 있으며 업그레이드 또는 추가 사본에 대해 승인된 소스에 해당 요금을 이미 지불한 경우가 아닌 한, 고객은 추가 사본 또는 업그레이드를 만들거나 사용할 라이선스 또는 권리가 없습니다. (2) 업그레이드 사용은 고객이 원래 엔드 유저 구매자 또는 임차인이거나 업그레이드할 소프트웨어 사용에 대한 유효한 라이선스를 보유하고 있는, 승인된 소스가 제공한 CISCO 장비로 제한됩니다. (3) 추가 사본을 만들고 사용하는 것은 필요한 백업용으로만 제한됩니다.

소유 자산 통지. 고객은 어떤 형식이든 모든 저작권, 소유 자산 및 기타 통지를, 그러한 저작권 및 기타 소유 자산 통지가 소프트웨어에 포함되어 있는 것과 동일한 형식과 방법으로, 소프트웨어의 모든 사본에서 유지 및 재현할 것에 동의합니다. 계약에 명시적으로 승인된 경우를 제외하고, 고객은 Cisco의 사전 서면 승인 없이 소프트웨어의 사본이나 복제본을 만들지 않습니다.

기간 및 종료. 계약 및 여기에 부여된 라이센스는 종료될 때까지 유효합니다. 고객은 소프트웨어와 문서의 모든 사본을 폐기함으로써 언제든지 계약과 라이센스를 종료할 수 있습니다. 고객이 계약의 조항을 준수하지 않으면 계약에 따른 고객의 권리는 Cisco에서의 통보 없이 즉시 종료됩니다. 종료 시 고객은 소유 또는 제어하는 모든 소프트웨어 및 문서의 사본을 폐기해야 합니다. 고객의 모든 기밀 유지 책임, "일반 제한 사항" 섹션에서 고객에게 부여된 모든 제약 조건과 제한 사항 그리고 모든 책임과 면책조항과 보증의 제한과 제약은 계약의 종료 이후에도 유지됩니다. 또한 "미국 정부 최종 사용자 구매자" 및 "제한된 보증 안내문 및 최종 사용자 라이센스 계약에 적용되는 일반 약관" 섹션의 조항은 계약 종료 이후에도 유지됩니다.

고객 레코드. 고객은 본 계약의 준수 여부를 확인하기 위해 정상 영업시간에 고객의 장부, 레코드 및 회계를 검토할 권리를 Cisco 및 해당 독립 회계업체에 부여합니다. 그러한 감사에서 본 계약의 위반이 발견되면 고객은 적절한 라이센스 요금 및 감사에 따른 합당한 비용을 즉시 Cisco에 지불해야 합니다.

수출, 재수출, 양도 및 규제 사용. 계약에 따라 Cisco에서 제공하는 소프트웨어, 문서와 기술 또는 그에 따른 직접 제품(이후 "소프트웨어 및 기술")은 미국의 법률과 규정 및 기타 해당 국가의 법률과 규정에 따라 수출 규제의 대상이 됩니다. 고객은 Cisco 소프트웨어 및 기술의 수출, 재수출, 양도, 사용을 관장하는 관련 법률과 규정을 준수해야 하며 미국 및 현지의 모든 필요한 승인, 허가 또는 라이센스를 얻어야 합니다. Cisco와 고객은 권한 또는 라이센스의 보호와 관련하여 상대방에 합리적으로 요구할 수 있는 기타 정보, 지원 문서 및 지원을 제공할 것에 각각 동의합니다. 수출, 재수출, 양도 및 사용의 규정준수와 관련된 정보는 다음 URL에서 찾을 수 있습니다.

http://www.cisco.com/c/en/us/about/legal/global-export-trade/general-export/contract-compliance.html.

최종 사용자 라이센스 계약

미국 정부 최종 사용자 구매자. 소프트웨어 및 문서는 Federal Acquisition Regulation("FAR")(48 C.F.R.) 2.101에 정의된 대로 "상용 품목"이며, FAR 12.212에 사용된 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서" 같은 용어로 구성되어 있습니다. FAR 12.212 및 DoD FAR Supp. 227.7202-1~227.7202-4와 일치하고 계약에 통합되어 있을 수 있는 다른 계약에 반하는 FAR 또는 기타 계약 조항이 있더라도, 고객은 정부 최종 사용자에게 소프트웨어 및 문서를 제공할 수 있으며, 계약이 직접적인 경우 정부 최종 사용자는 계약에 명시된 권리만으로 소프트웨어 및 문서를 취득하게 됩니다. 소프트웨어나 문서 또는 둘을 모두 사용하는 경우 소프트웨어 및 문서는 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서"라는 정부와의 계약이 성립되고, 여기에 명시된 권리와 제약 조건을 따르는 것으로 간주됩니다.

식별된 구성 요소*:* 추가 용어. 소프트웨어는 하나 이상의 구성 요소를 포함하거나 그러한 구성 요소와 함께 제공될 수 있으며, 그러한 구성 요소에는 Cisco가 문서, readme.txt 파일, 서드파티 클릭-동의 또는 다른 곳(예: http://www.cisco.com/)에서 식별한 서드파티 구성 요소("식별된 구성 요소")가 포함될 수 있고, 여기에 명시된 것과 다른 라이선스 계약 조건, 보증의 면책조항, 제한된 보증 또는 기타 약관("추가 조건"으로 통칭)이 적용될 수 있습니다. 귀하는 그러한 식별된 구성 요소에 적용되는 추가 조건에 동의합니다.

제한된 보증

여기에 명시된 제한 사항과 조건에 따라 Cisco는 (a) 소프트웨어를 담아 제공하는 미디어는 정상적으로 사용할 경우 재질 및 제조상 결함이 없으며, (b) 소프트웨어는 실제로 문서와 일치한다는 점을, 고객에게 배송된 날짜부터 시작(Cisco 이외의 승인된 소스에 의해 재판매되는 경우 Cisco의 원래 배송일 이후 90일 기간에 시작)하여 (a) 90일 동안 또는 (b) 소프트웨어가 포함된 제품("제품")에 동봉된 보증 카드에 소프트웨어에 대해 특별히 명시된 보증 기간(있는 경우) 동안 보증합니다. Cisco 제품 배송 날짜는 제품이 배송되는 포장 재료에 명시됩니다. 상기 내용을 제외하고 소프트웨어는 "있는 그대로" 제공됩니다. 본 제한된 보증은 처음 등록된 최종 사용자인 고객이 승인된 소스로부터 구매한 소프트웨어에만 적용됩니다. 본 제한된 보증에 따라 고객의 유일한 보상 및 Cisco와 공급업체의 전체 책임은 (i) 결함 있는 미디어의 교체 및/또는 (ii) Cisco의 선택에 따른 수리, 교체 또는 소프트웨어 구매 가격의 환불이며, 두 경우 모두 본 제한된 보증의 위반을 구성하는 오류나 결함은 보증된 기간 내에 고객에게 소프트웨어를 제공한 승인된 소스로 보고된 것이어야 합니다. Cisco 또는 고객에게 소프트웨어를 제공하는 승인된 소스는 보상의 조건으로서 선택적으로 소프트웨어 및/또는 문서의 반환을 요구할 수 있습니다. 어떤 경우에도 Cisco는 소프트웨어에 오류가 없음과 고객이 문제 또는 중단 없이 소프트웨어를 작동할 수 있을 것임을 보증합니다. 또한 네트워크 침입과 공격을 위한 지속적인 신기술 개발 때문에 Cisco는 소프트웨어 또는 소프트웨어가 사용되는 장비, 시스템 또는 네트워크가 침입이나 공격에 취약하지 않을 것이라고 보증하지 않습니다.

제약 조건. 소프트웨어, 제품 또는 소프트웨어 사용이 인증된 기타 장비가 (a) 변경된 경우(Cisco 또는 공인 대리점에서 변경한 경우 제외), (b) Cisco에서 제공한 지침에 따라 설치, 작동, 수리 또는 유지 관리된 경우, (c) 비정상적인 물리적 또는 전기적 스트레스, 비정상적인 환경 조건, 오용, 부주의, 사고를 겪은 경우 또는 (d) 베타, 평가, 테스트 또는 데모 목적으로 라이센스가 부여된 경우에는 본 보증이 적용되지 않습니다. 또한 (e) 임시 소프트웨어 모듈, (f) Cisco 소프트웨어 센터에 게시되지 않은 소프트웨어, (g) Cisco가 Cisco 소프트웨어 센터에 "있는 그대로" 기반으로 명시적으로 제공하는 소프트웨어, (h) 승인된 소스에서 라이센스 요금을 받지 않는 소프트웨어, (i) 승인된 소스가 아닌 서드파티에서 제공하는 소프트웨어에도 소프트웨어 보증이 적용되지 않습니다.

최종 사용자 라이센스 계약

보증의 면책조항

본 보증 섹션에 지정된 내용을 제외하고, 상업성, 특정 목적에의 적합성, 비위반, 만족스런 품질, 비간섭, 정보 내용의 정확성을 포함하여(이에 제한되지 않음) 또는 거래, 법률, 사용 또는 무역 관행에서 발생하는 모든 명시적 또는 암시적 조건, 표현 및 보증은 적용법에서 허용하는 한도까지 제외되며 **CISCO,** 공급업체 또는 라이선스 허가업체에 의해 명시적으로 부인됩니다**.** 동일한 것 중 어떤 것도 제외할 수 없는 경우, 그러한 암시적 조건, 표현 및/또는 워런티는 위의 "제한적 워런티" 섹션에 나와 있는 명시적 워런티 기간까지로 제한됩니다**.** 일부 국가나 관할 지역에서는 암시적 보증의 지속 기간에 대한 제한을 허용하지 않으므로 위의 제한 사항이 적용되지 않을 수 있습니다**.** 본 보증은 고객에게 특별한 법적 권리를 제공하며**,** 고객은 관할 지역에 따라 다른 권리를 보유할 수 있습니다**.** 위에 기술한 명시적 보증이 본질적 목적에 맞지 않는 경우에도 본 면책조항 및 예외는 적용됩니다.

책임의 면책조항 - 책임의 제한 사항. 미국, 라틴아메리카, 캐나다, 일본 또는 카리브해에서 소프트웨어를 구매한 경우 계약에 반대되는 내용이 있더라도, Cisco, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 모든 책임은 계약, 불법 행위(태만 포함), 워런티 위반 등 무엇이든 고객이 클레임의 원인이 된 소프트웨어에 대해 승인된 소스에 지불한 가격을 넘지 않으며, 소프트웨어가 또 다른 제품의 일부인 경우 해당 제품에 대해 지불한 가격을 넘지 않습니다. 소프트웨어에 대한 이 책임의 제한은 누적되며 사건당 적용되지 않습니다(즉, 클레임이 둘 이상 있는 경우에도 이 제한이 확대되지 않습니다).

유럽, 중동, 아프리카, 아시아 및 오세아니아에서 소프트웨어를 구매한 경우 계약에 반대되는 내용이 있더라도, CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 모든 책임은 계약, 불법 행위(태만 포함), 보증 위반 등 무엇이든 고객이 클레임의 원인이 된 소프트웨어에 대해 CISCO에 지불한 가격을 넘지 않으며, 소프트웨어가 또 다른 제품의 일부인 경우 해당 제품에 대해 지불한 가격을 넘지 않습니다. 소프트웨어에 대한 이 책임의 제한은 누적되며 사건당 적용되지 않습니다(즉, 클레임이 둘 이상 있는 경우에도 이 제한이 확대되지 않습니다). 계약의 어떤 내용도 (I) 과실로 인한 개인 상해 또는 사망에 대해 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 책임을 제한하지 않고, (II) CISCO의 기만적 허위진술에 대한 책임을 제한하지 않으며, 또는 (III) 적용법에 따라 제외할 수 없는 CISCO의 책임을 제한하지 않습니다.

책임의 면책조항 - 결과적 손해 및 기타 손실의 면제. 미국, 라틴아메리카, 카리브해 또는 캐나다에서 소프트웨어를 구매한 경우 여기에 명시된 보상이 본질적 목적 또는 다른 것과 맞는지 여부와 상관없이 어떤 경우에도, CISCO 및 공급업체는 책임 이론과 상관없이 또는 소프트웨어의 사용 또는 사용 불가로 인해 발생하는지 여부와 상관없이 그리고 CISCO와 공급업체 또는 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다. 일부 국가나 관할 지역에서는 결과적 또는 우연적 손해의 제한 또는 예외를 허용하지 않으므로 위의 제한 사항이 귀하에게 적용되지 않을 수 있습니다.

일본에서 소프트웨어를 구매한 경우 사망이나 개인 상해, 기만적 허위진술로 인해 발생하거나 이와 관련된 책임을 제외하고, 여기에 명시된 보상이 본질적 목적 또는 다른 것과 맞는지 여부와 상관없이 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체는 책임 이론과 상관없이 또는 소프트웨어의 사용 또는 사용 불가로 인해 발생하는지 여부와 상관없이 그리고 CISCO, 승인된 소스, 해당 공급업체 또는 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다.

유럽, 중동, 아프리카, 아시아 또는 오세아니아에서 소프트웨어를 구매한 경우 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체는 계약, 불법 행위(태만 포함)로 인해 발생하든

최종 사용자 라이센스 계약

소프트웨어의 사용 또는 사용 불가로 인해 발생하든 상관없이 그리고 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다. 일부 국가나 관할 지역에서는 결과적 또는 우연적 손해의 제한 또는 예외를 허용하지 않으므로 위의 제한 사항이 귀하에게 충분히 적용되지 않을 수 있습니다. 위의 예외는 다음과 관련하여 발생하는 책임에는 적용되지 않습니다. (I) 사망 또는 개인 상해, (II) 기만적 허위진술, 또는 (III) 적용법에서 제외할 수 없는 조건과 관련된 CISCO의 책임.

고객은 Cisco가 여기에 명시된 보증의 면책조항 및 책임의 제한 사항에 의존하여 가격을 책정하고 계약을 체결했으며, 동일한 내용이 양방 간 위험의 할당을 반영하며(계약 보상이 본질적 목적에 맞지 않고 결과적 손해를 초래할 위험 포함), 동일한 내용이 쌍방 간 거래의 필수적인 기초를 형성함을 인지하고 이에 동의합니다.

규제 법률, 관할지. 승인된 소스에서 수락한 구매 발주서의 주소를 참조하여 미국, 라틴아메리카 또는 카리브해에서 소프트웨어를 취득한 경우 계약 및 보증("보증")은, 법 조항에 충돌이 있더라도, 미국 캘리포니아 주의 법에 따라 제어되고 해석됩니다. 캘리포니아 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 캐나다에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은 법 조항에 충돌이 있더라도, 캐나다 온타리오 주의 법에 따라 제어되고 해석됩니다. 온타리오 주 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 유럽, 중동, 아프리카, 아시아 또는 오세아니아(오스트레일리아 제외)에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 영국의 법에 따라 제어되고 해석됩니다. 영국 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 또한 계약이 영국 법에 의해 제어되는 경우 계약 당사자가 아닌 사람은 Contracts(Rights of Third Parties) Act 1999 조건의 적용 또는 혜택을 받을 수 없습니다. 소프트웨어를 일본에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 일본 법에 따라 제어되고 해석됩니다. 일본 도쿄 지방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 오스트레일리아에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 오스트레일리아 뉴 사우스 웨일스 주의 법에 따라 제어되고 해석됩니다. 뉴 사우스 웨일스 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 기타 국가에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 미국 캘리포니아 주의 법에 따라 제어되고 해석됩니다. 캘리포니아 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다.

위에서 언급한 모든 국가에서 당사자들은 국제물품매매계약에 관한 국제연합협약(UN Convention on Contracts for the International Sale of Goods)을 부인합니다. 위의 내용에도 불구하고, 당사자는 자신의 지적 재산권 또는 소유권의 위반 혐의와 관련하여 해당 관할 지역의 법원에 임시 금지 명령 구제를 요청할 수 있습니다. 계약 및 보증의 일부가 무효이거나 집행 불가능한 것으로 판명되는 경우 나머지 조항은 완전한 효력을 유지합니다. 명시적으로 기술된 경우를 제외하고, 본 계약은 소프트웨어 및 문서의 라이센스에 대한 양방 간 완전한 합의를 구성하며, 구매 발주서 등에 포함된 충돌하는 조건 또는 추가 조건에 우선하며, 그러한 모든 조건은 제외됩니다. 본 계약은 영어로 작성되었으며, 양방은 영어 버전이 적용됨에 동의합니다.

Cisco 제품에 적용되는 제품 보증 조항 및 기타 정보는 다음 URL에서 확인할 수 있습니다.

http://www.cisco.com/c/en/us/products/warranty-listing.html

Cisco Systems Content Security 소프트웨어에 대한 보충 최종 사용자 라이센스 계약

중요: 신중하게 읽어보십시오.

본 보충 최종 사용자 라이센스 계약("SEULA")에는 귀하(여기에서 "귀하"란 귀하 및 귀하가 대표하는 기업체 또는 "회사"를 의미함)와 Cisco 간 최종 사용자 라이센스 계약("EULA")("계약"으로 통칭)에 따라 라이센스가 부여된 소프트웨어에 대한 추가 약관이 포함되어 있습니다. 본 SEULA에 사용되었지만 정의되지 않은 대문자로 표시된 용어는 EULA에서 정의된 의미로 사용됩니다. EULA와 본 SEULA의 약관 사이에 충돌이 있는 경우 본 SEULA의 약관이 우선 적용됩니다.

소프트웨어의 액세스 및 사용에 대해 EULA에 명시된 제한 사항 외에도 귀하는 언제나 본 SEULA에 제공된 약관을 준수할 것에 동의합니다.

소프트웨어를 다운로드, 설치 또는 사용하는 것은 계약에 대한 동의를 의미하며, 귀하 및 귀하가 대표하는 사업체는 계약을 준수해야 합니다. 귀하가 계약의 모든 조건에 동의하지 않는 경우 CISCO는 귀하에게 소프트웨어에 대한 라이센스를 부여하지 않으며, (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고 (B) 귀하는 전액 환불을 위해 소프트웨어를 반환(개봉하지 않은 CD 패키지 및 서면 자료 포함)할 수 있으며, 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 귀하는 전액 환불을 위해 전체 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권리는 CISCO 또는 승인된 CISCO 리셀러로부터 구매한 지 30일 후에 만료되며, 귀하가 원래 최종 사용자 구매자인 경우에만 적용됩니다.

본 SEULA에서, 귀하가 주문한 제품 이름 및 제품 설명은 Cisco Systems Email Security Appliance("ESA"), Cisco Systems Web Security Appliance("WSA") 및 Cisco Systems Security Management Application("SMA")("Content Security"로 통칭) 및 가상 어플라이언스 해당 제품("소프트웨어") 중 하나입니다.

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

최종 사용자 라이센스 계약

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

정의

본 SEULA에서는 다음과 같은 의미로 용어가 사용되었습니다.

"회사 서비스"란 회사의 내부 비즈니스 수행을 위해 최종 사용자에게 제공되는 회사의 이메일, 인터넷, 보안 관리 서비스를 의미합니다.

"최종 사용자"란 (1) WSA와 SMA의 경우, 회사에서 회사 서비스를 통해 인터넷 및 SMA에 액세스하도록 승인한 직원, 계약직원 및 기타 에이전트를 의미하고, (2) ESA의 경우, 회사에서 회사 서비스를 통해 이메일 서비스에 액세스하고 사용하도록 승인한 직원, 계약직원 또는 기타 에이전트의 이메일 편지함을 의미합니다.

주문 문서란 회사와 Cisco 또는 회사와 Cisco 리셀러 간 구매 계약, 평가 계약, 베타, 사전 릴리스 계약 또는 유사한 계약, 또는 본 계약에서 허용한 소프트웨어 라이센스에 대한 구매 조건을 포함하여 이와 따라 Cisco에서 수락하는 모든 구매 발주서의 유효한 조건을 의미합니다.

"개인 식별 가능 정보"란 개인의 이름, 사용자 이름, 이메일 주소 및 기타 개인 식별이 가능한 정보를 포함하여(이에 제한되지 않음) 개인을 식별하는 데 사용할 수 있는 정보를 의미합니다.

"서버"란 여러 사용자를 위한 네트워크 리소스를 관리 또는 제공하는 네트워크상의 단일 물리적 컴퓨터 또는 디바이스를 의미합니다.

"서비스"란 Cisco 소프트웨어 구독 서비스를 의미합니다.

"서비스 설명"은 http://www.cisco.com/c/en/us/about/legal/service-descriptions.html의 소프트웨어 서브스크립션 지원 서비스에 대한 설명을 의미합니다.

"텔레메트리 데이터"란 회사 이메일 및 웹 트래픽의 샘플을 의미합니다. 여기에는 이메일 메시지 및 웹 요청 특성에 대한 데이터, 그리고 회사의 Cisco 하드웨어 제품에서 서로 다른 유형의 이메일 메시지 및 웹 요청이 처리된 방식에 대한 정보가 포함됩니다. 텔레메트리 데이터에 포함된 이메일 메시지

메타데이터 및 웹 요청은 개인 식별 가능 정보를 제거하기 위해 알아볼 수 없도록 익명으로 처리됩니다.

"기간"이란 주문 문서에 표시된 대로 귀하가 주문한 소프트웨어 구독의 기간을 의미합니다.

"가상 어플라이언스"란 Cisco Email Security Appliance, Web Security Appliance 및 Security Management Appliance의 가상 버전을 의미합니다.

"가상 머신"이란 자체 운영 체제를 실행할 수 있고 서버처럼 애플리케이션을 실행할 수 있는 소프트웨어 컨테이너를 의미합니다.

추가 라이센스 약관

데이터 수집 조건에 대한 라이센스 허가 및 승낙

소프트웨어 라이센스

소프트웨어 및 문서를 사용함으로써 회사는 본 계약의 조건을 준수할 것에 동의하며, 회사가 본 계약을 준수하는 한 Cisco는 Cisco 하드웨어 제품에서만, 또는 가상 어플라이언스의 경우 최종 사용자에 대한 회사 서비스의 조항과 관련하여 가상 머신에서만 지정된 기간 동안 소프트웨어를 사용하도록, 하위 라이센스 부여나 양도가 불가능한 비배타적이며 세계적인 라이센스를 회사에 부여합니다. 소프트웨어를 사용할 수 있는 라이센스가 부여되는 최종 사용자의 수는 주문 문서에 지정된 최종 사용자의 수로 제한됩니다. 회사 서비스 조항과 관련된 최종 사용자의 수가 주문 문서에 지정된 최종 사용자의 수를 초과하면 회사는 승인된 소스에 연락하여 소프트웨어의 추가 라이센스를 구매해야 합니다. 본 라이센스의 기간과 범위는 주문 문서에 자세히 정의되어 있습니다. 주문 문서는 소프트웨어 라이센스의 조건과 관련하여 EULA에 우선합니다. 여기에서 부여된 라이센스 권리 외에 Cisco, Cisco의 리셀러 또는 개별 라이센스 허가업체는 회사에 어떤 권리, 타이틀 또는 이권도 부여하지 않습니다. 귀하의 소프트웨어 업그레이드 자격은 서비스 설명의 적용을 받습니다. 본 계약과 서비스는 동시에 종료됩니다.

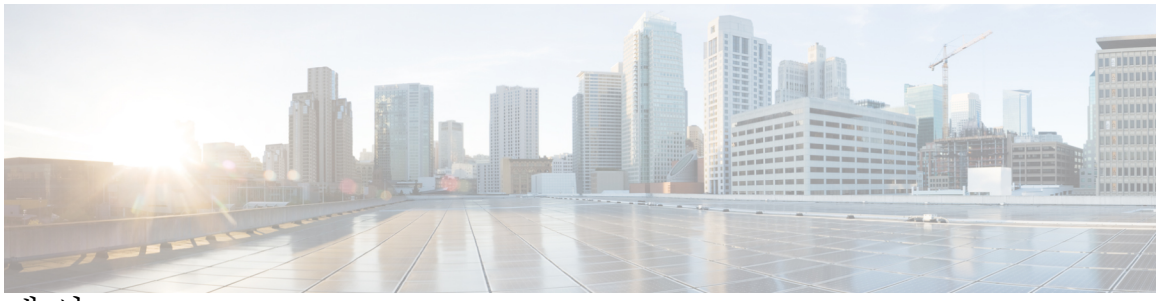
데이터 사용에 대한 동의 및 라이센스

Cisco 개인정보 보호정책(http://www.cisco.com/web/siteassets/legal/privacy.html)에 따라 회사는 Cisco가 회사에서 텔레메트리 데이터를 수집하고 사용하도록 허락하며 해당 권한을 부여합니다. Cisco는 텔레메트리 데이터에서 개인 식별 가능 정보를 수집하거나 사용하지 않습니다. 사용자 환경과 소프트웨어, 그리고 기타 Cisco 보안 제품 및 서비스의 개선을 위해 Cisco는 집계된 익명의 텔레메트리 데이터를 서드파티와 공유할 수 있습니다. 회사는 소프트웨어에서 SenderBase 네트워크 참여를 비활성화하여 언제든지 Cisco의 텔레메트리 데이터 수집 권리를 종료할 수 있습니다. SenderBase 네트워크 참여의 활성화 또는 비활성화에 대한 지침은 소프트웨어 구성 가이드에서 찾아볼 수 있습니다.

기타 권리 및 의무에 대한 설명

Cisco Systems, Inc. 최종 사용자 라이센스 계약, 개인정보 취급방침 및 소프트웨어 구독 지원 서비스의 서비스 설명을 참조하십시오.

최종 사용자 라이센스 계약



색 인

H

I

J

K

M

N

P

R

S

T