Cisco Security Manager

기업은 보안 운영과 관련된 새로운 과제에 직면해 있습니다. 나날이 증가하는 보안 기술과 복잡성과 비교 동시에 보안 관리 담당 IT 직원의 감소 및 재배치로 인해 작업자 오류의 가능성이 크게 높아졌으며, 이는 곧 보안 노출 및 사고로 이어질 수 있습니다. 이러한 과제에 대응하려면 지속적인 정책 시행을 강화하고, 보안 이벤트의 문제를 신속하게 해결할 수 있도록 지원하며, 구축된 보안 솔루션 전반에 대한 내용을 요약된 보고서로 제공할 수 있는 통합된 엔드 투 엔드 관리 솔루션이 보안 운영 팀에 반드시 필요합니다.

Cisco® Security Manager는 이러한 모든 기능과 그 이상을 수행하는 포괄적인 관리 솔루션입니다. 이 솔루션의 확장 가능한 중앙 집중식 관리 기능을 통해 관리자는 광범위한 Cisco 보안 장치를 효율적으로 관리하고, 네트워크 구축 전반에 대한 가시성을 확보하고, 높은 수준의 보안을 유지하면서 다른 중요한 네트워크 서비스(예: 규정 준수 시스템 및 고급 보안 분석 시스템)와 정보를 공유할 수 있습니다. 또한 운영 효율성을 목표로 설계된 Cisco Security Manager에는 상태 및 성능 모니터링 기능, 소프트웨어 이미지 관리 기능, 자동 충돌 감지 기능, 장애 처리 시스템과의 통합 등 강력한 자동화 기능도 다수 포함되어 있습니다.

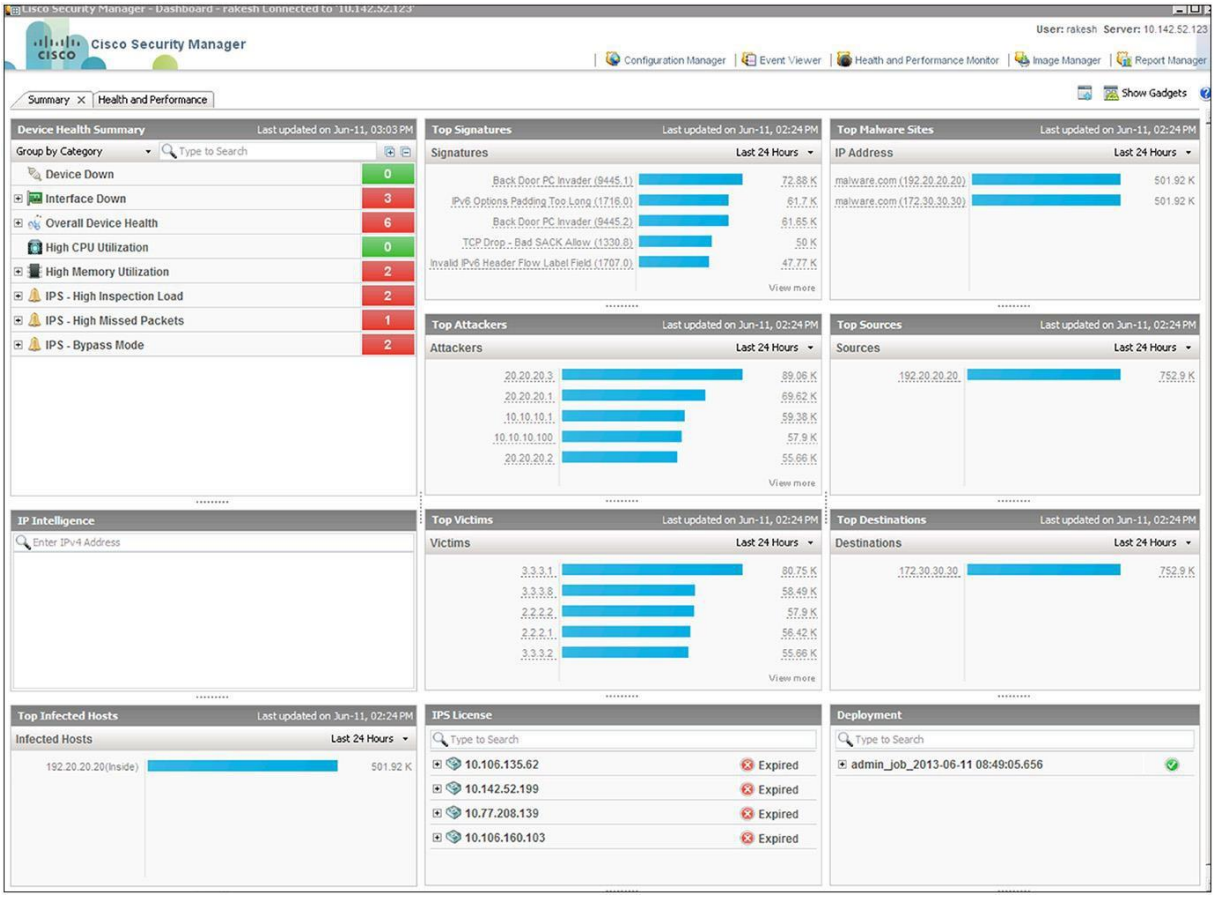
Cisco Security Manager는 광범위한 Cisco 보안 장치를 지원하며 여기에는 Cisco ASA 5500 Series 및 ASA 5500-X Series Adaptive Security Appliances, Cisco IPS 4200, 4300, 4500 Series Sensor, Cisco SR 500 Series Secure Router, Cisco AnyConnect® Secure Mobility Client가 포함됩니다.

Cisco Security Manager에는 효율적이고 능률화된 보안 관리를 실현하기 위한 몇 가지 중요한 기능이 있습니다. 다음 섹션에서는 이러한 기능에 대해 설명합니다.

대시보드

Cisco Security Manager 대시보드(그림 1)는 네트워크 보안 설정의 상태, 작동 및 기타 중요한 성능 지표를 한눈에 볼 수 있도록 지원하는 위젯 기반의 홈 화면입니다. Device Health Summary(장치 상태 요약), Top Attackers(상위 공격자), Top Victims(상위 표적), Top Signatures(상위 서명)를 비롯한 여러 위젯에서는 관리자가 알고 있어야 하는 우선적인 보안 문제를 알아보기 쉬운 요약 형태로 제공합니다. 이러한 위젯은 보안 준비 상태 분석을 위한 시작점 역할을 합니다. 예를 들어, 사용자가 Signatures(서명) 위젯에서 특정 서명이 제출된 횟수를 클릭하면 해당 서명에 대한 이벤트를 분석할 수 있는 Event Viewer(이벤트 뷰어)로 연결됩니다. 마찬가지로, 관리자는 Top Attackers(상위 공격자) 위젯에서 IP 주소를 클릭하여 해당 IP 주소와 관련된 중요한 정보를 살펴볼 수 있습니다. 즉, 대시보드 화면은 Cisco Security Manager에서 보안 관리자의 업무 시작 지점입니다. 각 관리자의 요구 사항에 맞게 대시보드를 맞춤화할 수도 있습니다.

그림 1. Cisco Security Manager 대시보드

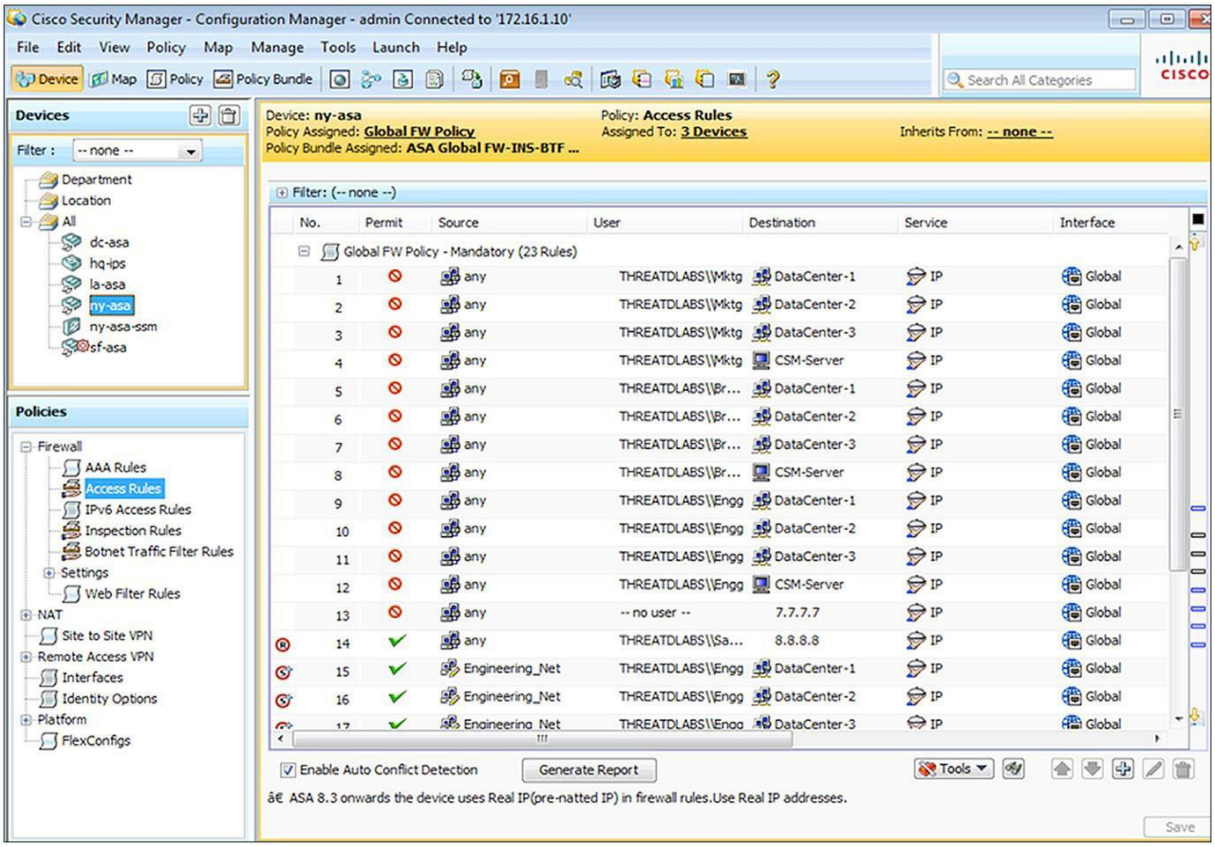


통합 정책 및 객체 관리

Cisco Security Manager는 보안 규칙 및 객체의 재사용을 지원하며, 구축 과정 전체에서 보안 위협을 모니터링하는 기능을 향상하여 오류 발생 가능성을 최소화하고 효율성을 극대화합니다.

관리자는 온디맨드 또는 예약 방식으로 보안 구축을 구현할 수 있으며, 필요한 경우 이전 구성으로 롤백할 수 있습니다. 역할 기반 액세스 제어 및 구축 워크플로에서는 규정 준수 프로세스를 수행하도록 보장합니다(그림 2 참조).

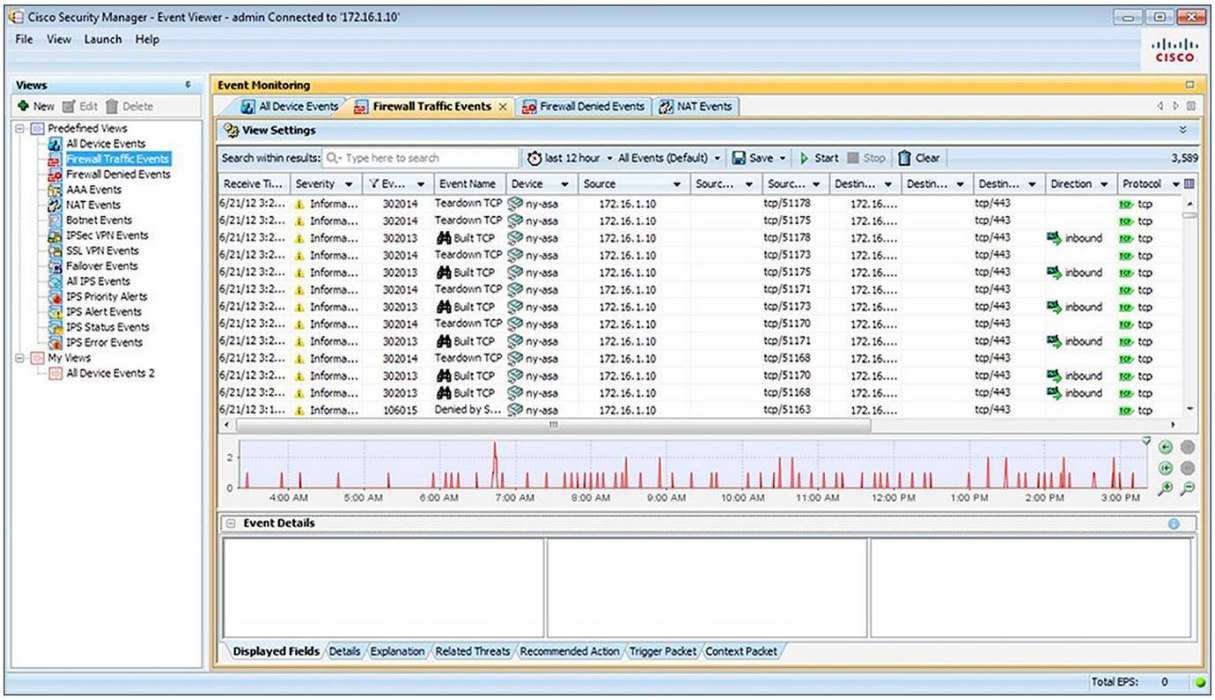
그림 2. Cisco Security Manager를 사용한 보안 정책 관리



이벤트 관리 및 문제 해결

통합 이벤트 관리에서는 신속한 인시던트 분석 및 문제 해결을 위해 실시간으로 내역 이벤트를 볼 수 있으며, 이벤트에서 소스 정책으로 빠르게 이동할 수 있습니다. 또한 관리자는 고급 필터링 및 검색 기능을 사용하여 관심 있는 이벤트를 빠르게 식별하고 격리할 수 있습니다. Event Manager와 Configuration Manager를 연결하여 방화벽 규칙 및 IPS(침입 방지 시스템) 서명의 문제 해결 시간을 단축합니다.

그림 3. Cisco Security Manager를 통한 이벤트 관리 및 문제 해결



Cisco Security Manager의 Event Manager는 다음 기능들을 제공합니다.

- Cisco ASA 어플라이언스, Cisco FWSM(Firewall Services Module) 및 Cisco Catalyst® 6500 Series ASA Services Module에서 생성된 syslog 메시지는 물론 Cisco IPS 센서의 SDEE(Security Device Event Exchange) 메시지도 지원
- 실시간 및 기록 이벤트 보기
- 소스 정책으로의 신속한 이동을 위한 방화벽 액세스 규칙 및 IPS 서명 교차 연결
- 미리 번들화된 방화벽, IPS 및 VPN 보기
- 특정 장치 또는 시간 범위를 모니터링을 위한 사용자 지정 보기
- 이벤트의 검색, 분류 및 필터링을 위한 직관적인 GUI 제어
- 특정 보안 장치에 대한 이벤트 수집 설정 또는 해제할 수 있는 관리 옵션
- 추가적인 문제 해결을 위한 ping, traceroute 및 패킷 추적기 등의 툴

멀티 벤더 환경을 위한 이벤트 관리, 이벤트 상관관계 및 내역 이벤트 분석에 대한 자세한 내용은 http://www.cisco.com/go/securitypartners를 참조하십시오.

보고

Cisco Security Manager는 보안 구축 전반에서 수집된 이벤트 및 기타 필수 정보를 기반으로 자세한 시스템 리포트를 생성합니다(그림 4). 표 1에는 사용 가능한 시스템 리포트가 나열되어 있습니다. 또한 관리자는 특정 리포팅 요구의 충족을 위해 미리 정의된 리포트를 정의 및 저장할 수 있습니다. 시스템에서 생성되었든 사전 정의되었든 모든 리포트를 내보낼 수 있으며, PDF 또는 CSV 파일로 내보내고 이메일을 통해 전송하도록 예약할 수 있습니다. 사용자는 특정 차트에서 자세한 정보를 찾아 상세 분석을 위한 추가 정보를 확인할 수 있습니다.

그림 4. Cisco Security Manager의 Report Manager

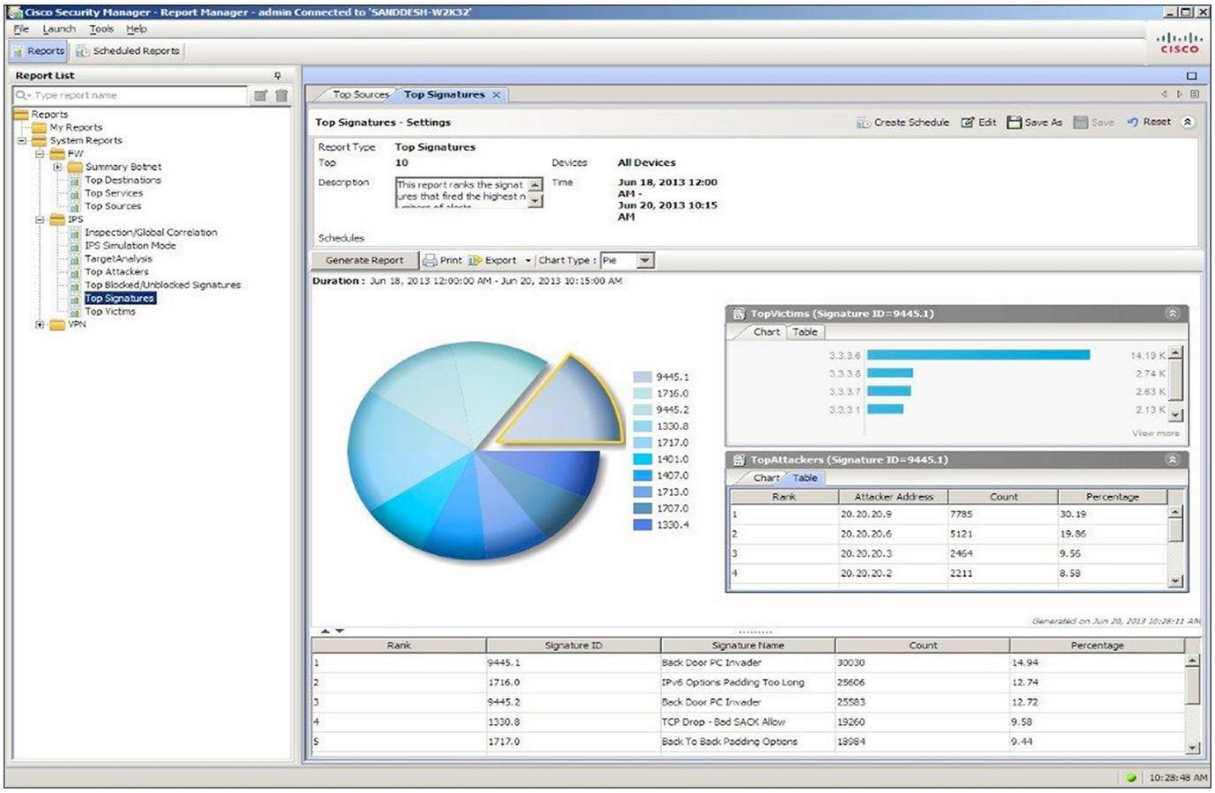


표 1. Cisco Security Manager 시스템 보고서

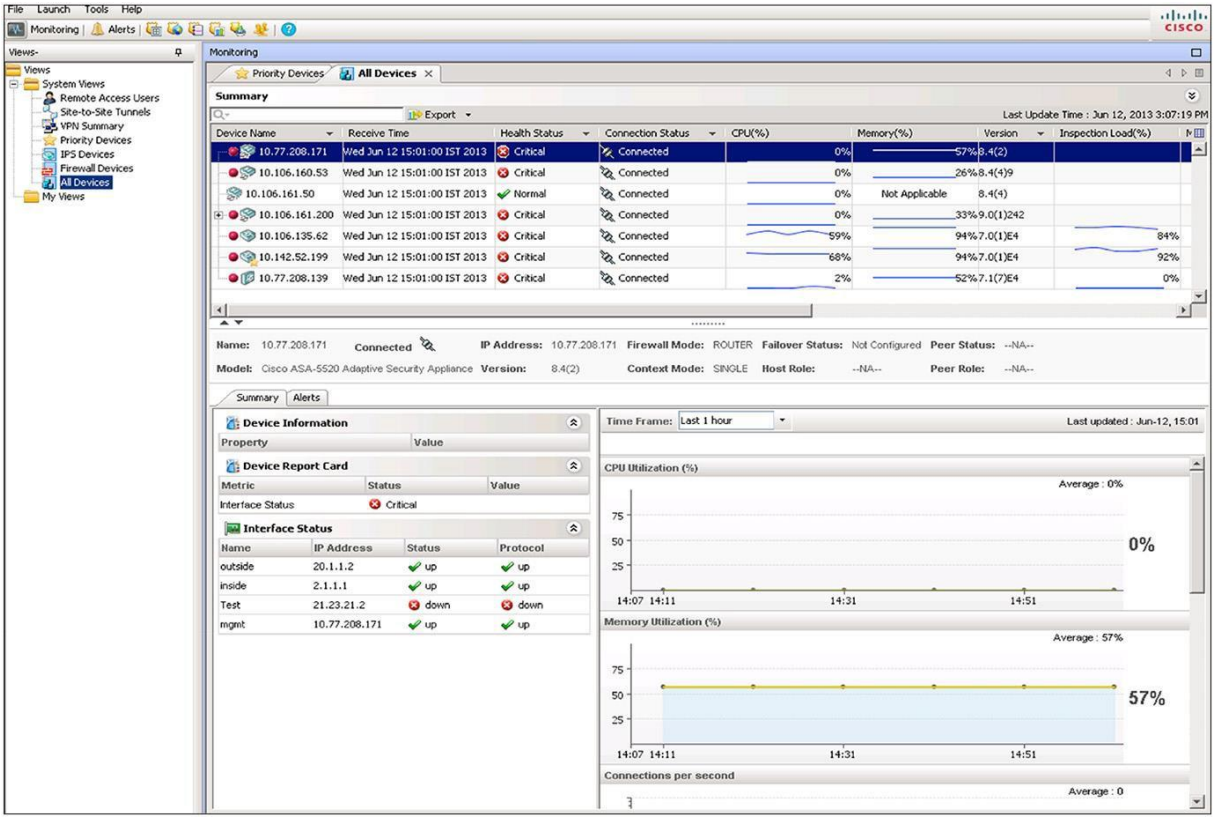
방화벽	IPS	VPN
• 상위 감염 호스트 • 상위 악성코드 포트 • 상위 악성코드 사이트 • 상위 대상 • 상위 서비스 • 상위 소스	• 검사/Global Correlation • IPS 시뮬레이션 모드 • 대상 분석 • 상위 공격자 • 상위 차단된/차단되지 않은 서명 • 상위 서명 • 상위 희생자	• 상위 대역폭 사용자(SSL/IPsec) • 상위 지속 시간 사용자(SSL/IPsec) • 상위 처리량 사용자(SSL/IPsec) • 사용자 보고서 • VPN 장치 사용 보고서

상태 및 성능 모니터링

관리자는 보안 환경을 지속적으로 분석하고 미리 설정된 임계값 도달 시 경고를 알리는 통합 Health and Performance Monitor를 통해 생산성을 높일 수 있습니다. 중요 방화벽 장애 조치, IPS 센서 애플리케이션 오류 또는 과도한 CPU/메모리 사용률과 같은 이벤트에 대해 사용자 지정 가능한 경고 알림을 설정할 수 있습니다.

관리자는 간단한 색상 코드 인터페이스를 사용하여 심각한 상태에 있는 장치를 즉시 식별하고 자주 모니터링되는 특성(예: CPU 또는 메모리 사용률)을 관찰함으로써 구축된 보안 전반에 걸쳐 모든 장치의 일반적인 상태와 성능을 신속하게 확인할 수 있습니다. 원하는 경우 세부적인 차트를 사용하여 각 장치의 상태, 트래픽 및 성능 메트릭을 심층적으로 파악할 수 있습니다. 그림 5는 기본 모니터링 인터페이스입니다.

그림 5. Cisco Security Manager의 Health and Performance Monitor

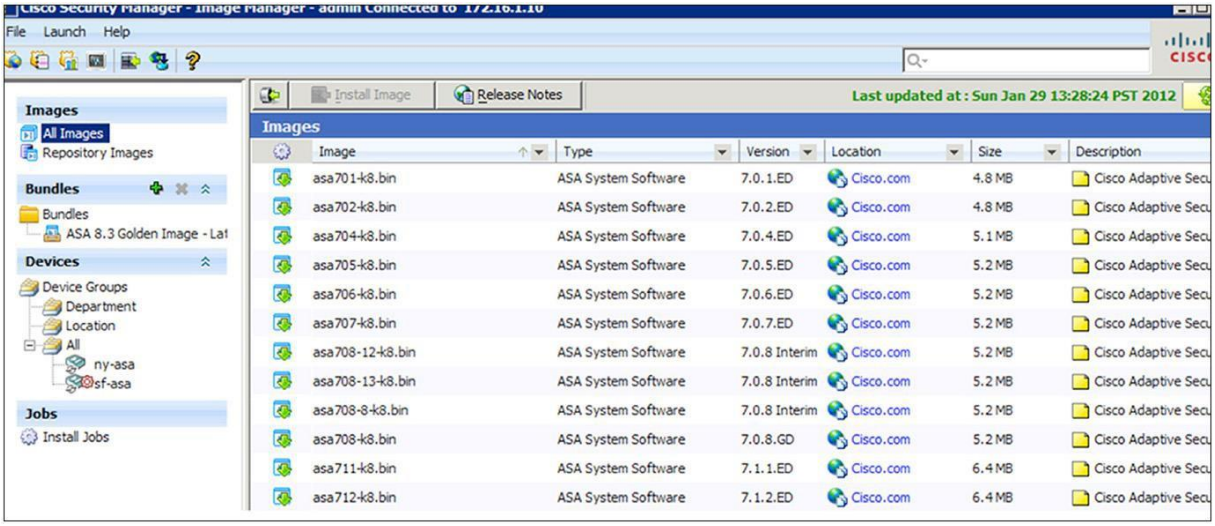


이러한 상태 및 모니터링 기능은 새로운 Cisco ASA 클러스터링 기능에서도 사용할 수 있습니다.

소프트웨어 이미지 업그레이드

직관적인 마법사를 사용해 방화벽 소프트웨어 이미지를 업그레이드할 수 있습니다. 마법사는 이미지를 다운로드하고, 이미지 번들을 생성하고, 해당 이미지가 각 장치에 적합한지 확인하는 데 필요한 단계로 관리자를 안내합니다. 그런 다음 백업을 수행하고 장치를 중단한 다음 업데이트를 수행합니다. 각 방화벽에 개별적으로 업데이트를 적용하거나 그룹으로 업데이트를 실행하여 속도와 효율성을 극대화할 수 있습니다. 이 프로세스는 자동화되어 있으므로 야간 또는 사용량이 적은 시간대에 실행하여 운영 환경에 미치는 영향을 줄일 수 있습니다. 그림 6에는 Cisco Security Manager의 기본 이미지 관리 인터페이스가 나와 있습니다.

그림 6. Cisco Security Manager의 소프트웨어 이미지 업그레이드 마법사



Cisco Security Manager에 대한 API 기반 액세스

Cisco Security Manager에서는 매우 안전한 API 기반 액세스를 통해 다른 중요한 네트워크 서비스(예: 규정 준수 및 고급 보안 분석 시스템)와 정보를 공유하여 보안 운영 및 규정준수를 간소화할 수 있습니다. REST(Representational State Transfer) 사용을 통해 외부 방화벽 규정 준수 시스템에서 Cisco Security Manager로 관리되는 모든 보안 장치의 데이터에 대한 액세스를 바로 요청할 수 있습니다. 이러한 타사 클라이언트 프로그램 역시 API를 통해 CSM에서 방화벽 액세스 정책 및 정책 객체를 추가, 삭제 또는 수정할 수 있습니다. 이러한 API는 CSM의 워크플로 기능과 원활하게 통합되므로, CSM API를 통해 정책 구성이 자동화되면 관리자는 엄격한 제어를 적용할 수 있습니다.

추가 기능 및 혜택

표 2에는 Cisco Security Manager의 추가 기능 및 혜택이 요약되어 있습니다.

표 2. Cisco Security Manager: 추가 기능 및 혜택

기능	혜택
방화벽 구성	
Cisco 보안 구축 관리	다음과 같은 Cisco 보안 환경을 간편하게 중앙에서 관리합니다. • Cisco ASA 5500 Series 및 5500-X Series Adaptive Security Appliances • Cisco IPS 4200, 4300, 4500 Series Sensor • Cisco AnyConnect Secure Mobility Client • Cisco SR 500 Series Secure Router • Cisco Catalyst 6500 Series Firewall Services Module 및 ASA Services Module • Cisco IOS® 소프트웨어 보안 이미지를 실행하는 Cisco ISR(Integrated Services Router) 플랫폼

기능	혜택
영역 기반 정책	원하는 경우 지원되는 장치 플랫폼에 영역 기반 방화벽 정책을 설정합니다.
봇네트(botnet) 트래픽 필터	애플리케이션 레이어를 검사하고 봇네트의 "phone-home" 활동을 차단할 수 있도록 Cisco ASA 플랫폼에서 Cisco 봇네트(botnet) 트래픽 필터를 지원합니다.
Cisco TrustSec® 보안 그룹 태그와 통합	Cisco TrustSec 보안 그룹 태그와의 통합을 제공하므로 Cisco Security Manager 사용자는 구축 전반에 걸쳐 상세하고 의미 있는 정책을 구성할 수 있습니다.
Cisco ASA 클러스터링	고급 장애 조치 기능을 제공하여 다양한 Cisco ASA 어플라이언스를 지원하며, 부하 공유 메커니즘을 통해 다운타임을 줄이고 가용성을 향상합니다.
콘텐츠 필터링	심층적인 콘텐츠 검사를 기반으로 트래픽을 필터링할 수 있도록 Cisco IOS 소프트웨어 기반 장치 플랫폼에 대한 콘텐츠 필터링을 지원합니다. 한 가지 규칙 테이블을 사용하여 다양한 장치 플랫폼을 관리할 수 있습니다.
효율적인 정책 정의	와일드카드를 비롯하여 어떤 규칙이 특정 소스, 대상 및 서비스 흐름과 일치하는지를 명확히 표시함으로써 관리자가 정책을 정의할 수 있는 효율성을 높입니다.
Syslog 포워딩	Cisco Security Manager는 ASA 방화벽에서 생성된 로그를 Cisco Security Manager에 내장된 Event Viewer(이벤트 뷰어) 외에도 원격 컬렉터 2개에 전달하도록 지원합니다.
설정 간소화	소프트웨어에 추가되었거나 장치 자체에서 검색된 장치 관련 정보를 장치 저장소 또는 구성 파일로 가져오도록 지원하여 구성을 능률화하고 초기 보안 관리 설정을 간소화합니다.
운영 능률화	다음을 통해 수동 작업을 크게 감소화 시키는 한편 오류의 감소 및 보안 환경을 최적화합니다. • 규칙 충돌 감지, 히트 수 분석, 규칙 결합 및 규칙 집합을 분석하고 최적화하는 기타 강력한 툴 • 오류 없는 구축 및 프로세스 규정준수 보장을 지원하는 역할 기반 액세스 제어 및 워크플로
인터페이스 역할	인터페이스 그룹에 규칙 정책을 적용하고 이를 중앙 집중식으로 관리하여 유연성과 확장성을 극대화할 수 있습니다.
IPS 구성	
구성 및 업데이트 정책	다음에 대한 IPS 기반 구성 및 업데이트 정책을 효율적으로 쉽게 관리합니다. • Cisco IPS 4200 및 4300 Series Sensor • Cisco ASA AIP-SSM(Advanced Inspection and Prevention Security Services Module) • Cisco ASA AIP-SSC(Advanced Inspection and Prevention Security Services Module) • Cisco Catalyst 6500 Series IDSM-2(Intrusion Detection 시스템 서비스 모듈 2) • Cisco IDS Network Module • Cisco IPS AIM(Advanced Integration Module) • Cisco IOS IPS
서명 업데이트	엔터프라이즈에 배포하기 전에 새로운 서명과 업데이트된 서명을 점진적으로 프로비저닝할 수 있습니다.
위협 조사	디지털 서명 업데이트를 배포하기 전에 관리자가 SIO(Security Intelligence Operations), Cisco IntelliShield® Alert Manager Service 및 Cisco IPS Security Research Team에서 수집한 심층적인 정보를 기반으로 환경을 구성할 수 있습니다.
업데이트 마법사	상태 및 세부 정보 알림과 함께 효율적인 자동 IPS 업데이트, 예약 및 정책 배포를 지원합니다.
재사용 가능한 정책	IP 서명 정책과 이벤트 작업 필터가 모든 장치에 상속되고 할당되도록 설정합니다. 모든 IPS 정책을 다른 IPS 장치에 할당하고 공유할 수 있습니다.
정책 롤백	IPS 정책 롤백, 구성 아카이브, 서명의 복제 또는 생성이 포함됩니다.
간편한 운영	서명 및 이러한 서명에 대해 생성된 이벤트를 손쉽게 탐색할 수 있는 도구를 제공하며, 직관적인 사용자 인터페이스에서는 서명을 조정하고 관리할 수 있는 간단한 메커니즘을 제공합니다.
위험 등급 범주	위험 등급 값을 동적으로 계산하여 이를 위험 범위로 그룹화하고 범주로 정의할 수 있습니다. 서명에는 위험 등급 범주가 할당될 수 있으며, 서명이 제출된 경우 취해야 하는 조치는 해당 범주에 따라 할당됩니다.
전역 이벤트 작업	위험 등급 범주에 여러 이벤트 작업을 추가할 수 있으며, 이러한 작업은 해당 위험 등급 범위에 속하는 모든 서명에 전체적으로 적용됩니다. 또한, 필요한 경우 특정 작업을 이벤트에 대한 서명에서 필터링할 수 있습니다.
서명 주석	여러 사용자가 서명에 메모를 추가할 수 있으며, 이러한 메모는 나중에 해당 서명에 대한 통합된 방식으로 볼 수 있습니다.
CSV 내보내기	서명, 이벤트 작업 필터, 서명 델타 설정 같은 특정 IPS 기능을 CSV(쉼표로 구분된 값)로 내보냄으로써 Cisco Security Manager 서버 인스턴스 간에 이러한 데이터를 편리하게 저장하고 교환할 수 있습니다.
VPN 구성	
VPN 마법사	Site-to-Site, 허브 앤 스포크(hub and spoke), 풀 메시, 엑스트라넷 VPN을 손쉽게 구성할 수 있습니다.

기능	혜택
일반적인 VPN 구축 시나리오 지원	동적 IP 인증서 및 계층적 인증서 모두를 대상으로 GET VPN(그룹 암호화 전송 VPN), DMVPN(Dynamic Multipoint VPN), GRE(Generic Routing Encapsulation) IPsec(IP Security)을 지원하는 일반적인 VPN 배포 시나리오를 지원합니다.
다중 컨텍스트 구성	정책을 세분화하고 여러 위치에 분산된 서로 다른 지사 간에 유연하게 보안을 구성하도록 지원합니다.
원격 구성	VPN을 중앙 집중식으로 관리합니다.
효율성 및 사용 용이성 기능	
티켓팅 통합	여러 장애 처리 시스템에서 변경한 내용을 단일 티켓 식별자로 태그 처리하여, 감사 시 손쉽게 쿼리할 수 있습니다.
전체 검색	구성 데이터베이스에서 특정 IP 주소 또는 서비스를 사용하는 모든 장치, 정책 및 정책 객체를 찾을 수 있습니다.
사용량 찾기	특정 정책 객체를 사용하는 정확한 규칙을 가리키고 객체를 사용하는 모든 정책에 대한 세부 정보를 제공하므로, 관리자는 객체에 대한 사용량 정보를 신속하게 검색할 수 있습니다.
자동 충돌 감지	규칙 최적화 및 문제 해결을 간소화할 수 있도록 규칙 충돌에 대한 명확한 가시성을 제공합니다.
IPv4와 IPv6 간 호환성	통합된 IPv4 및 IPv6 정책 및 규칙 구성을 지원하여 두 정책 구성 간의 구축 속도를 높이고 호환성을 향상합니다.
통합 이벤트 관리	다음을 제공하여 관리자가 보안 정보의 상태를 확인하고 문제를 해결할 수 있도록 지원합니다. • Cisco ASA 어플라이언스에서 syslog 메시지 수신 및 Cisco IPS 센서에서 SDEE(Security Device Event Exchange) 메시지 수신 • 실시간 및 내역 이벤트 보기 • 소스 정책으로의 신속한 이동을 위한 방화벽 액세스 규칙 및 IPS 서명 교차 연결 • 방화벽, IPS, VPN 모니터링용 보기 집합을 미리 번들화 • 특정 장치 또는 시간 범위를 모니터링을 위한 사용자 지정 보기 • 이벤트의 검색, 분류 및 필터링을 위한 직관적인 GUI 제어 • 특정 보안 장치에 대한 이벤트 수집 설정 또는 해제할 수 있는 관리 옵션 • 환경에서 ASA CX 구축이 감지될 경우 Cisco Prime™ Security Manager를 시작하며, 이는 Cisco Security Manager를 통해 CX를 관리할 수 있는 방법으로 제공됨
리포트 관리자	시스템 리포트 및 미리 정의된 리포트 생성 지원 및 이 모두에 대해 다음을 수행할 수 있습니다. • 차트 및 그리드로 보기 • PDF 또는 Excel 파일로 내보내기 • 이메일을 통한 배달 예약 • 자세한 내용 스캔
대량 운영	장치 수가 많은 네트워크의 관리 부담이 줄어듭니다. 기능에는 다음이 포함됩니다. • 정책 객체의 대량 가져오기 및 내보내기 • 오프라인 장치의 대량 추가 • 장치 수준 재지정의 대량 가져오기 • 네트워크 전체에 구축된 모든 Cisco ASA 어플라이언스에 대한 소프트웨어 이미지 대량 자동 업데이트(규모에 적합한 유연하고 일관된 빠른 구축 업데이트 방법 제공)
장치 그룹화	관리자가 비즈니스 기능 또는 위치를 기반으로 장치 그룹을 생성하고 정의한 후, 그룹의 모든 장치를 단일 장치로 관리할 수 있도록 지원
정책 객체 관리자	네트워크 주소, 서비스, 장치 설정, 시간 범위 또는 VPN 매개 변수 같은 객체를 한 번만 정의하여 이후에는 값을 직접 입력할 필요 없이 몇 번이든 사용할 수 있도록 지원
기타 기능	
타사 장치 지원	"관리되지 않는" 엔드포인트 및 타사 장치 지원
보안 서비스 관리	VPN용 QoS(Quality of Service), 라우팅, Cisco NAC(Network Admission Control)를 비롯한 통합 보안 서비스 관리
다중 애플리케이션 보기	서로 다른 사용 사례 및 환경 수준을 지원할 수 있도록 애플리케이션에 대한 여러 보기 제공
유연한 설치 옵션	온디맨드 또는 예약 방식으로 보안 구축 구현 가능
롤백	필요한 경우 구축을 이전 구성으로 롤백 가능
역할 기반 액세스 제어	관리자 역할을 최대 5개까지 정의하여 적용할 수 있으며, 옵션으로 제공되는 Cisco ACS(Secure Access Control Server)를 사용할 경우 추가 역할 사용 가능
워크플로	공식적인 변경 제어 및 추적을 통해 정책을 구축하는 동안 각 관리자에게 특정 작업 할당 가능

기능	혜택
분산 구축	동적 주소 또는 NAT 주소가 사용될 수 있는 많은 수의 원격 방화벽에 대한 업데이트를 간소화하도록 Auto Update Server 및 Cisco Network Services Configuration Engine 포함
Cisco Cloud Web Security와 통합	사용자가 Cisco Security Manager를 통해 방화벽에 규칙을 정의할 수 있도록 지원하고 Cisco Cloud Web Security에 웹 트래픽을 전달할 수 있는 옵션 제공
운영 관리	소프트웨어 배포 또는 장치 재고 리포팅 등의 운영 기능을 지원할 수 있도록 CiscoWorks RWAN(Resource Manager Essentials)를 포함
상태 및 성능 모니터링	정상적인 클러스터 보안 환경을 지속적으로 분석하고 사전 설정된 임계값에 도달할 경우 알림 전송
IP 인텔리전스	여러 기능에 IP 인텔리전스가 포함되어 있어서, 사용자는 홈 화면의 Top Attackers(상위 공격자), Top Victims(상위 표적) 같은 여러 위젯, Report Manager의 특정 차트 분석 기능, Health and Performance Monitor를 통해 IP 주소에 대한 중요한 정보(예: FQDN)와 위치 정보를 살펴볼 수 있습니다. IP 인텔리전스는 대시보드에 추가할 수 있는 개별 위젯으로도 존재합니다.

기술 사양

Cisco Security Manager의 자세한 하드웨어 사양 및 규모 조정 지침은 http://www.cisco.com/go/csmanager 페이지를 참조하십시오.

장치 지원

표 3에는 Cisco Security Manager에서 지원하는 장치 제품군이 요약되어 있습니다. 지원되는 장치 소프트웨어 버전을 비롯한 자세한 목록은 http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html 의 "Supported Devices and OS Versions for Cisco Security Manager"(Cisco Security Manager의 지원되는 장치 및 OS 버전)를 참조하십시오.

표 3. Cisco Security Manager에서 지원되는 Cisco 장치의 개요

지원되는 장치
Cisco PIX Security Appliance
Cisco ASA 5500 Series 및 ASA 5500-X Series Adaptive Security Appliances
Cisco Integrated Services Router(800, 1800, 2800 및 3800 Series 포함)
Cisco Integrated Services Router G2(1900, 2900 및 3900 Series 포함)
Cisco ASR 1000 Series Aggregation Service Router
Cisco 7600 시리즈 라우터
Cisco 7500 시리즈 라우터
Cisco 7300 시리즈 라우터
Cisco 7200 시리즈 라우터
Cisco 7100 Series Routers
Cisco 3200 Series Routers
Cisco 2600 시리즈 라우터
Cisco Catalyst 6500 Series FWSM(Firewall Services Module)
Cisco Catalyst 6500 Series VPNSM(VPN Services Modules)
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN SPA(VPN Shared Port Adapter)
Cisco Catalyst 6500 Series IDSM-2(Intrusion Detection 시스템 서비스 모듈 2)
Cisco IPS 4200 Series Sensor
Cisco ASA 5500 Series용 Cisco AIP-SSM
Cisco ASA 5500 Series용 Cisco AIP-SSC
Integrated Services Router용 Cisco IPS AIM
Access Router NM-CIDS(Network Module - Cisco Intrusion Detection System)용 Cisco IPS Module
Cisco Catalyst 3550, 3560, 3560E, 3750, 3750 Metro 및 4500 Series 스위치, Cisco Catalyst 4948 및 4948 10기가비트 이더넷 스위치

주문 정보

Cisco Security Manager 제품 게시판에서 라이센싱 옵션 및 주문 세부 정보를 제공합니다. 게시판 주소는 http://www.cisco.com/go/csmanager입니다.

주문 가능한 Cisco Security Manager의 최신 버전은 4.7 버전입니다.

시스코 서비스

Cisco는 라이프사이클 방식을 사용해 서비스에 접근합니다. 기업이 공격 및 중단에 대해 중요한 비즈니스 프로세스를 보호하며 개인정보를 보호하고 정책과 규정 준수 제어를 지원하는 네트워크 플랫폼을 설계, 구현, 운영하며, 최적화할 수 있도록 파트너와 함께 폭넓은 보안 서비스 포트폴리오를 제공합니다.

Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하고, 새로운 애플리케이션에 맞게 네트워크를 준비하여 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. 시스코 서비스에 대해 자세히 알아보려면 http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html을 방문하십시오.

- **Cisco Security Intelligence Operations(SIO)**는 위협과 취약성 인텔리전스 및 분석, Cisco IPS 서명, 완화 기법에 대한 조기 경고를 위한 중앙 위치를 제공합니다. http://www.cisco.com/security를 방문하여 Cisco SIO를 즐겨찾기에 추가하십시오.
- **Cisco Security IntelliShield Alert Manager Service**는 조직이 환경에 있는 잠재적 취약성에 대해 정확하고 믿을 수 있는 정보를 적시에 쉽게 액세스할 수 있도록 해주는 사용자 지정 가능한 웹 기반의 위협 및 취약성 경고 서비스를 제공합니다.
- **Cisco SAS(Software Application Support) Service**는 Cisco Security Manager가 지속적으로 가동 및 운영되면서 기술 지원 및 소프트웨어 업데이트에 연중무휴 액세스하도록 지원합니다.
- **Cisco Security Optimization Service**는 조직이 최고 사용 네트워크 상태를 유지하도록 지원합니다. 네트워크 인프라는 민첩하고 적응력 뛰어난 비즈니스의 기반입니다. Cisco Security Optimization Service는 계획과 평가의 조합, 설계, 성능, 조정, 시스템 변경에 대한 지속적인 지원을 결합하여, 끊임없이 변화하는 보안 위협에 대처하기 위해 계속해서 확장되는 보안 시스템을 지원합니다.

Cisco Security Manager 소프트웨어는 다음과 같은 특징이 있는 Cisco SAS(Software Application Support) 서비스 계약에 따라 기술 지원 서비스를 받을 수 있습니다.

- Cisco Technical Assistance Center(TAC) 무제한 액세스를 통해 수준 높은 지원을 받을 수 있습니다. Cisco 보안 소프트웨어 애플리케이션에 대해 교육을 받은 Cisco 소프트웨어 애플리케이션 전문가가 기술 지원을 제공합니다. 지원은 전 세계적으로 연중무휴 제공됩니다.
- 등록을 통해 네트워크 보안 문제의 진단과 새로운 기술의 이해 및 혁신적인 소프트웨어의 최신 개선 사항을 유지하는 데 도움이 되는 애플리케이션 툴과 기술 문서가 풍부하게 저장되어 있는 Cisco.com에 액세스합니다. 유틸리티, 백서, 애플리케이션 설계 데이터 시트, 구성 문서 및 사례 관리 툴은 내부 기술 역량을 확장하는 데 도움이 됩니다.
- 애플리케이션 소프트웨어 버그 픽스 및 유지 관리와 간단한 소프트웨어 릴리스에 액세스합니다.

추가 정보

Cisco Security Manager에 대한 자세한 내용은 http://www.cisco.com/en/US/products/ps6498/index.html을 참조하거나, 어카운트 매니저 또는 Cisco Authorized Technology Provider에게 문의하십시오. 다음 주소로 이메일을 보낼 수도 있습니다. ask-csmanager@cisco.com.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-730892-01 08/14