Cisco Prime Security Manager

글로벌 인력 증가와 애플리케이션 및 장비의 확산으로 인해 네트워크의 복잡성이 증가하고 있습니다. 이에 따라 방화벽 관리자는 직원들이 언제나 어디에서나, 어떤 장비에서든지 액세스를 가능하게 하는 필수 생산성 기능과 비즈니스 보호에 필요한 보안의 완화 사이에서 선택을 해야 합니다. Cisco® ASA CX Context-Aware Security(컨텍스트 인식 보안)는 이러한 문제를 애플리케이션, 장비, 그리고 진화하는 글로벌 인력에 따라 액세스 제어를 활성화함으로써 해결합니다.

Cisco ASA CX는 종합 관리 솔루션인 Cisco PRSM(Prime™ Security Manager)을 통해 관리됩니다. CIsco PRSM은 네트워크에 전례없는 가시성을 제공하며, 세분화된 애플리케이션, 사용자, 그리고 장비 제어 제공와 함께 유연한 관리 아케텍쳐를 통해 보안 관리에 획기적인 발전을 주도한 솔루션입니다.

전례 없는 네트워크 가시성

Cisco Prime Security Manager는 보안 관리자에게 엔드 투 엔드 가시성을 제공하는 한편 상위 레벨 트래픽 패턴과 세분화된 로그 및 보안 장비들의 작동 상태와 성능 등의 정보를 제공합니다.

PRSM은 관리자가 네트워크 전체의 트래픽 흐름을 잘 파악할 수 있도록 트래픽 패턴 리포트를 제공합니다. 예를 들어, 그림 1은 상위 소스 리포트, 그림 2는 상위 대상 리포트입니다.

그림 1. 상위 소스 리포트

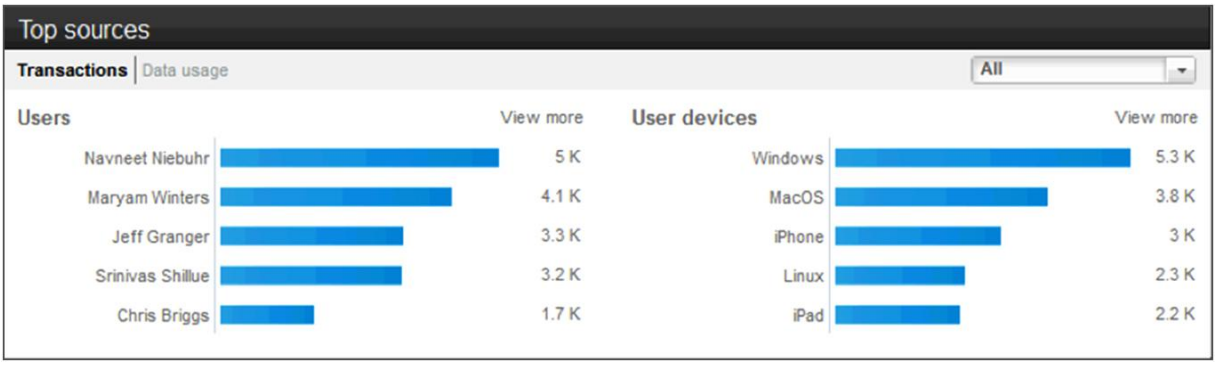
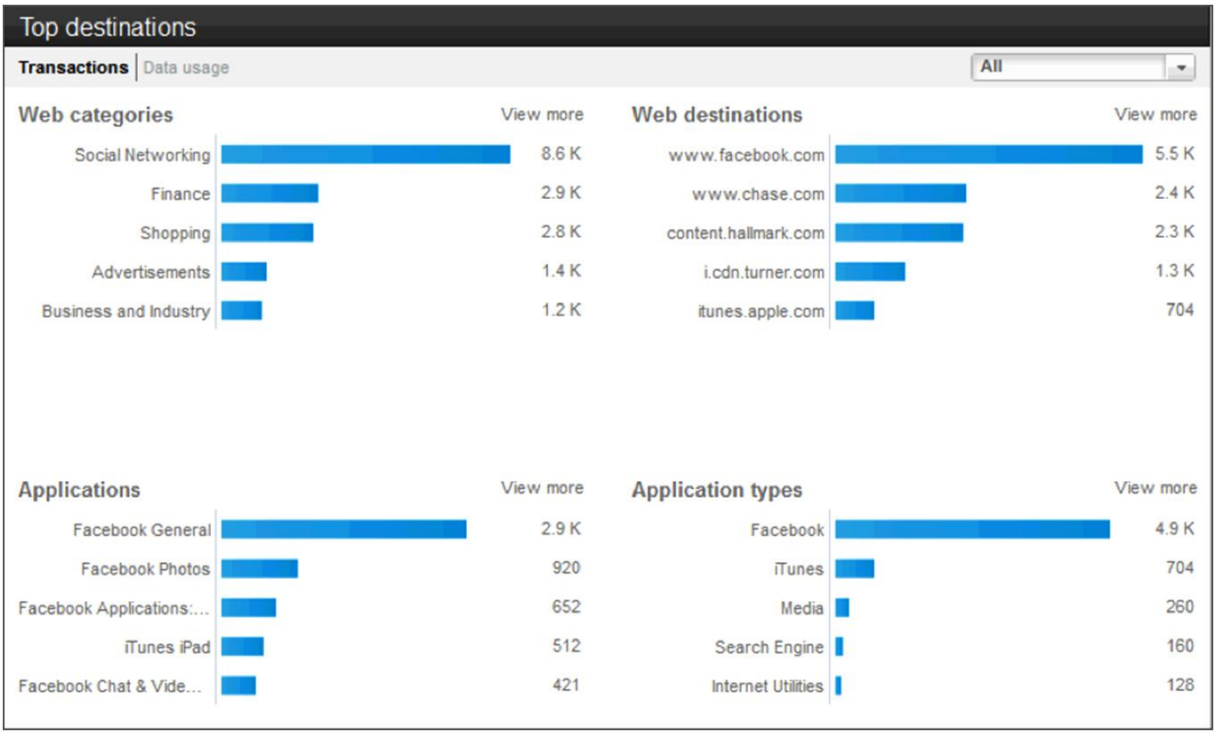


그림 2. 상위 대상 리포트



상위 레벨 리포트뿐만 아니라 Cisco Prime Security Manager는 사용자, 애플리케이션, 장비 및 기타 컨텍스트 요소에 대한 세부 정보 액세스를 관리자에게 제공합니다. 이에 관리자는 뛰어난 가시성과 제어 기능을 이용할 수 있습니다. 그림 3과 4가 그 예입니다. 표 1은 Cisco Prime Security Manager에서 제공하는 모든 리포트입니다.

그림 3. 네트워크 내의 Facebook 마이크로-애플리케이션 액세스 리포트

그림 4. 사용자별 Facebook 액세스

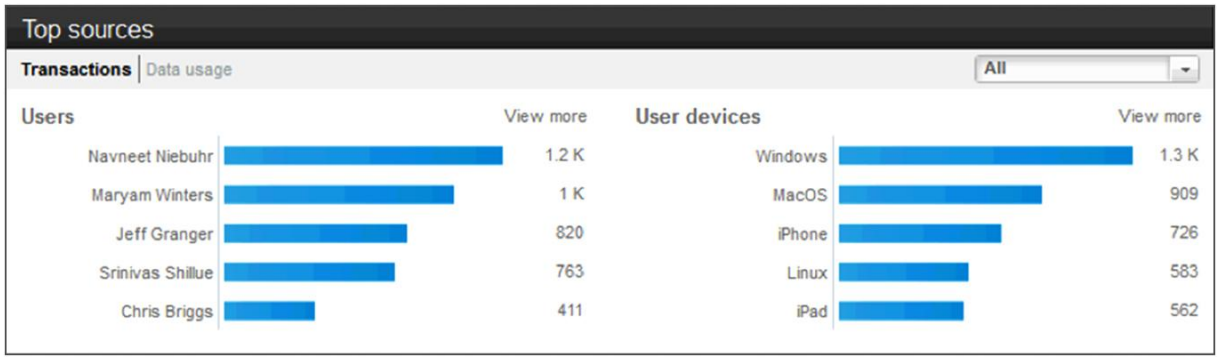


표 1. Cisco Prime Security Manager로 가능한 리포트

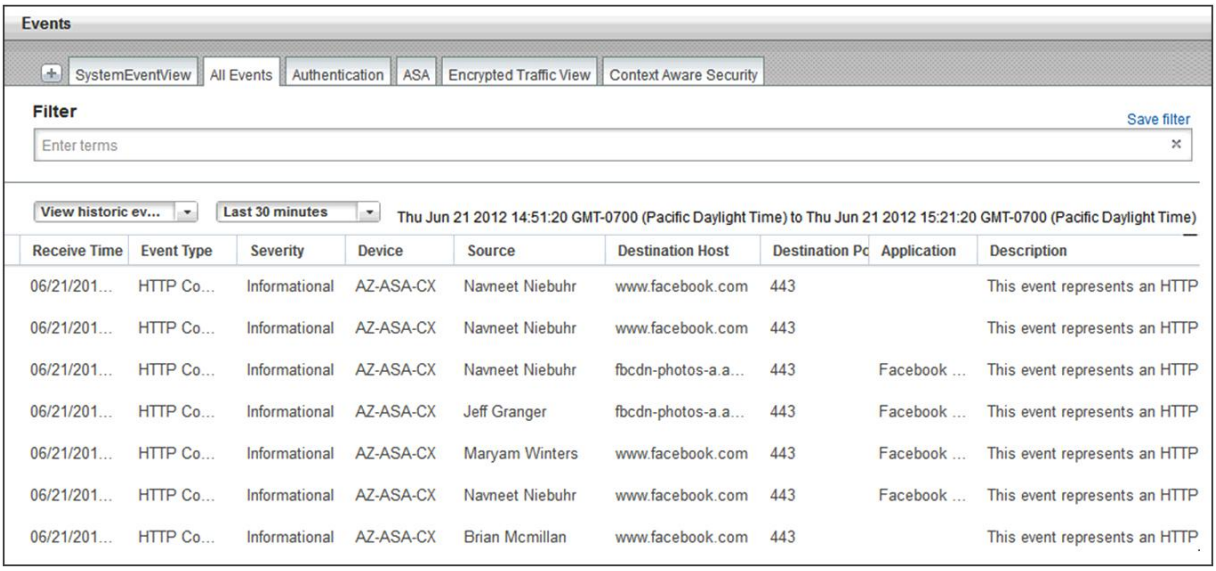
리포트 범주	설명	특정 리포트
트래픽 요약 리포트	네트워크 트래픽의 상위 레벨 요약 제공	• 트랜잭션별 트래픽 요약 - 허용 또는 거부된 트랜잭션에 대한 세부 정보 • 바이트별 트래픽 요약 - 수신 및 전송 데이터의 요약 제공 • 트랜잭션 및 바이트별, 웹 트래픽 대 비웹 트래픽 요약
애플리케이션 리포트	모니터링할 네트워크 애플리케이션 사용	• 트랜잭션별 상위 애플리케이션 • 차단된 트랜잭션별 상위 애플리케이션 • 자세한 애플리케이션 테이블
사용자 리포트	모니터링할 사용자 활동 활성	• 트랜잭션별 상위 사용자 • 차단된 트랜잭션별 상위 사용자 • 자세한 사용자 테이블
엔드포인트 리포트	네트워크에 액세스하는 엔드포인트 및 운영 체제에 대한 가시성 제공	• 트랜잭션별 상위 운영 체제 • 차단된 트랜잭션별 상위 운영 체제 • 자세한 운영 체제 테이블 • 위치 기반 트래픽 - 직접 연결된 장비에서 오는 트래픽 대 원격 액세스 메커니즘에서 오는 트래픽에 대한 세부 정보
URL 리포트	모니터링할 웹 활동 사용	• 트랜잭션별 상위 URL 범주 • 차단된 트랜잭션별 상위 URL 범주 • 자세한 URL 테이블
장비 리포트	네트워크 보안 장비의 사용 분석	• 트랜잭션별 상위 장비 - 가장 자주 사용되는 방화벽 표시 • 차단된 트랜잭션별 상위 장비 - 트래픽 대부분을 차단하는 방화벽 표시 • 상세한 장비 테이블 - 방화벽과 처리된 트랜잭션 및 총 처리량에 대한 자세한 목록

이벤트 분석 및 사전 모니터링

Top-N 리포트는 네트워크 전체의 트래픽 패턴에 대한 상위 레벨 정보를 제공하는 동안 Cisco Prime Security Manager는 특정 사용자, 애플리케이션, URL 및 장비에 대한 세부 정보 활성화를 통해 변칙적인 트래픽의 다음 레벨 분석에 필요한 정보를 제공합니다. 이를 통해 분석을 간소화 할 수 있습니다.

문제 해결 및 장기적인 보안 분석을 위한 로그 모니터링도 보안 관리자에게는 매우 중요합니다. Prime Security Manager는 심층 분석이 필요한 시나리오에서 관리자를 지원할 수 있도록, 리포팅 대시보드에서 원시 이벤트에 대한 직관적인 액세스를 제공합니다. 그림 5는 PRSM 이벤트 모니터를 나타냅니다. 실시간 및 기록 이벤트 분석을 지원하는 것은 물론 직관적인 필터링 기능을 보유하고 있습니다.

그림 5. Cisco Prime Security Manager 이벤트 모니터

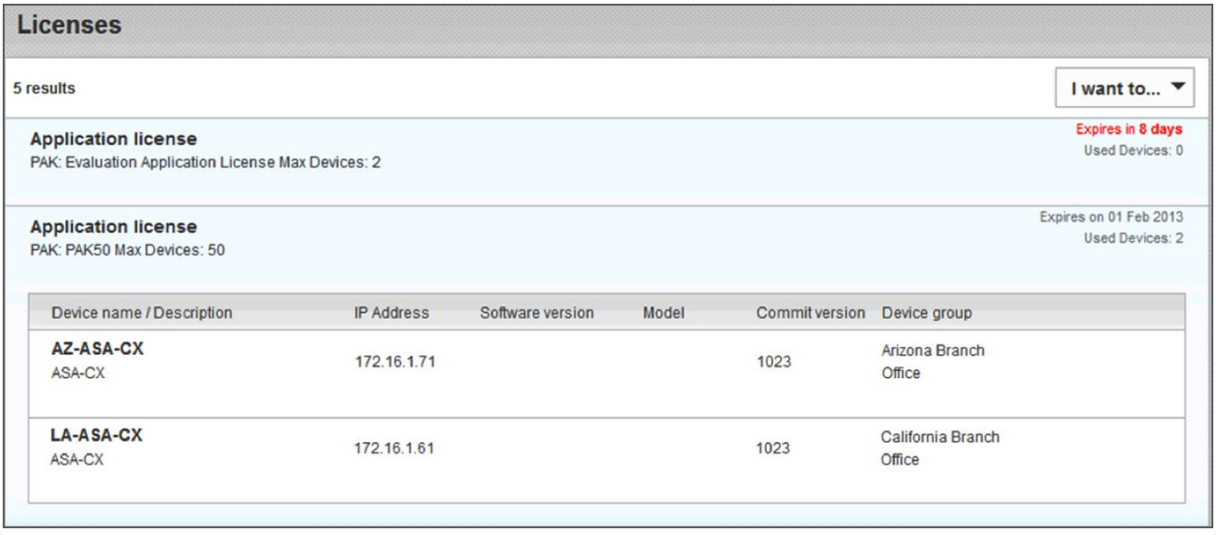


Cisco Prime Security Manager는 상태, 성능 및 라이센스 만료 정보의 제공을 통해 보안 팀은 운영에 악영향을 끼칠 수 있는 문제의 사전 관리가 가능합니다. 그림 6은 모든 네트워크 보안 장비의 일반적인 상태 정보를 나타냅니다.

그림 6. Prime Security Manager 작동 상태 모니터

마찬가지로 장비 목록 페이지는 보안 장비 및 서비스에 대한 라이센스 만료 정보를 제공합니다(그림 7 참조).

그림 7. Prime Security Manager 장비 목록 페이지



세분화된 애플리케이션, 사용자 및 장비 제어

Cisco Prime Security Manager는 애플리케이션, 마이크로-애플리케이션, 사용자, 장비 및 위치를 비롯한 풍부한 컨텍스트 요소 세트를 기반으로 정책을 작성하고 시행할 수 있습니다. 한 예로 전체 Facebook 애플리케이션을 허용 또는 거부하는 정책을 작성하기 보다는 비즈니스 용도로 사용되는 Facebook 내의 마이크로-애플리케이션은 활성화되도록 설정하고, Facebook 게임 등의 기타 비즈니스 외의 마이크로-애플리케이션은 비활성화 되도록 설정하는 것이 가능합니다. Embedded Application Browser 기능은 관리자에게 관심이 있는 애플리케이션 및 마이크로-애플리케이션 등의 신속한 검색을 제공합니다. 이를 통해 사용자 기반 액세스 기능을 활성화 설정할 수 있으며 개인 및 그룹 기반 액세스 정책을 애플리케이션 사용에 적용하여 제어할 수 있습니다. 이러한 프로세스는 직관적인 디렉토리 검색 기능을 통해 더욱 간소화됩니다.

그림 8은 소스, 대상, 서비스 등의 일반적인 액세스 정책 패러다임이 어떻게 사용자, 사용자 그룹, 웹 사이트와 웹 범주, 애플리케이션과 애플리케이션 범주, 장비 유형과 같은 컨텍스트 요소를 포함하여 확장되는지를 설명하고 있습니다. 또한 애플리케이션 또는 마이크로-애플리케이션 내의 동작 제어도 가능합니다. 예를 들면, 관리자는 Facebook 메세지 마이크로-애플리케이션에 대한 마케팅 및 영업 액세스는 허용하되 다운로드는 사용할 수 없도록 설정을 할 수 있습니다(그림 9 참조).

그림 8. 세분화된 컨텍스트 기반 액세스 제어

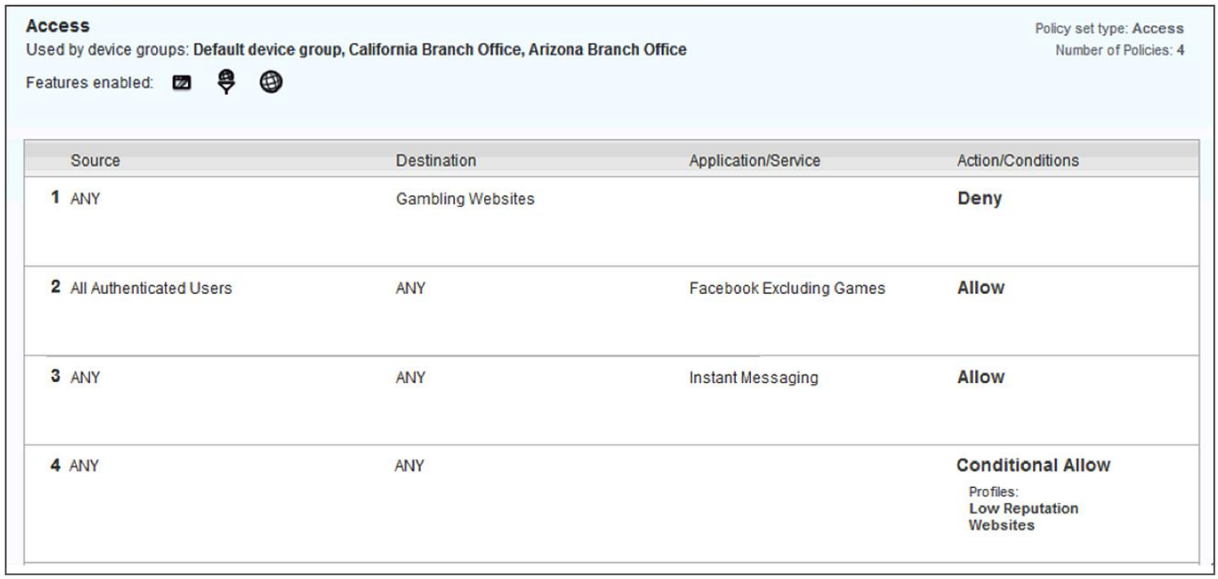
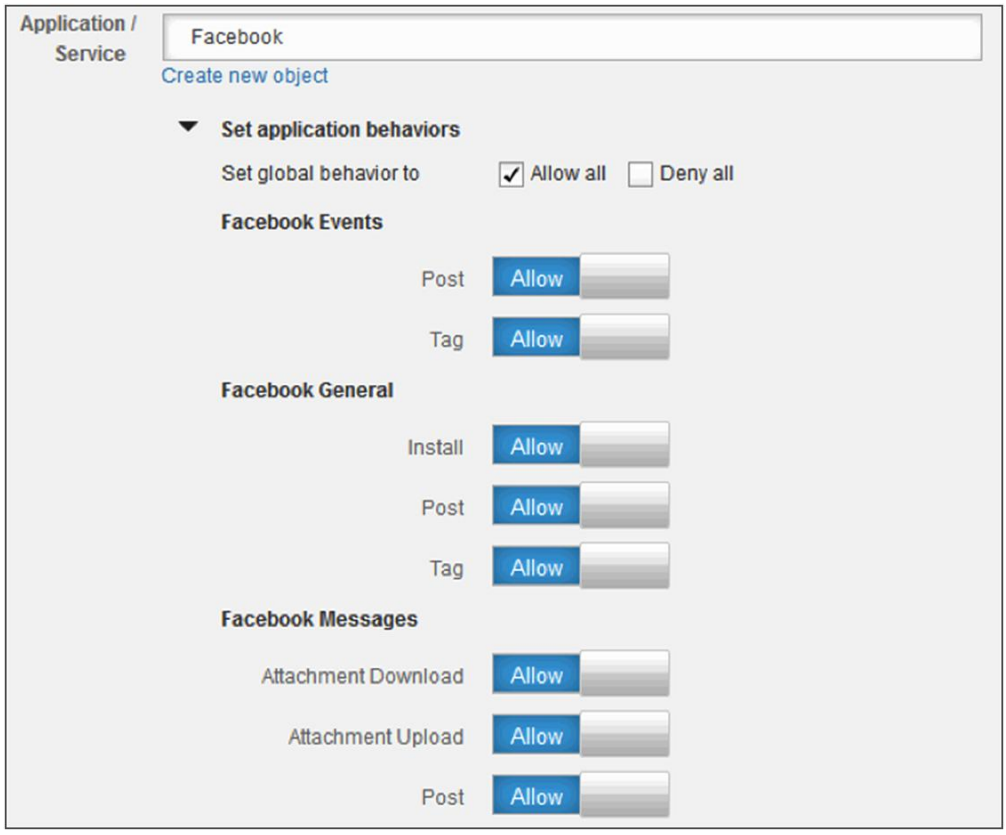


그림 9. 동작 기반 정책 제어



각 정책의 히트 수는 동적으로 제공되며, 각 정책의 실제 사용량이 명확하게 표에 표시됩니다. 여러 방화벽에서 정책을 공유할 수 있으므로, 관리자는 네트워크 인프라 전체에서 정책 일관성을 유지할 수 있습니다.

유연한 관리 아키텍처

직관적인 사용을 위해 새롭게 배포된 Cisco Prime Security Manager는 관리자에게 단일 장비 및 다중 장비 관리를 위한 일관된 관리 인터페이스를 제공합니다. 여러 장비를 관리할 경우 효율적인 중앙 집중식 제어를 위해 모든 액세스 요청이 기본 관리자로 옮겨지게 됩니다. 긴급 상황 발생 시 관리자는 단일 장비 관리를 위해 Cisco Prime Security Manager를 수동으로 재설정할 수 있습니다.

다양한 배포 요구에 맞게 Cisco Prime Security Manager를 물리적 어플라이언스 또는 VMWare ESXi 기반의 가상 어플라이언스로 사용하는 것이 가능합니다.

표 2는 Cisco Prime Security Manager의 기능 및 이점을 설명하고 있습니다.

표 2. Cisco Prime Security Manager의 기능 및 이점

기능	이점
세분화된 애플리케이션 제어	일반적으로 사용되는 1천개 이상의 애플리케이션과 7만5천개 이상되는 마이크로-애플리케이션은 물론 애플리케이션 동작(예: 파일 업로드를 통해 소셜 네트워킹 사이트에 발행)을 기반으로 액세스 정책을 개발 및 시행할 수 있습니다. 적은 정책으로 포트-홉핑 및 프로토콜-홉핑 애플리케이션도 효과적으로 차단할 수 있습니다.
사용자 ID	사용자 기반 및 역할 기반의 차별화된 액세스 제어를 위해 Active Directory 에이전트, LDAP(Lightweight Directory Access Protocol), Kerberos, NTLM(Windows NT LAN Manager) 등의 일반적인 ID 메커니즘을 지원합니다.

장비 유형 기반 시행	관리자가 네트워크에 액세스하려고 시도하는 장비 유형을 명확히 식별하고, 어떤 장비를 허용 또는 거부할지를 선택적으로 제어할 수 있습니다.
URL 필터링	인터넷 트래픽의 세분화된 제어를 지원하는 모든 기능을 갖춘 엔터프라이즈급 URL 필터링 솔루션을 포함합니다.
글로벌 인텔리전스	Cisco Security Intelligence Operations(SIO)를 통해, 글로벌 Cisco 보안 배포 장소에서 정기적으로 업데이트되는 위협 정보 피드를 사용해 제로 데이 악성코드를 차단하는 한편 애플리케이션에 대한 **안전한** 액세스를 제공합니다.
기존 네트워크 정의 사용	다른 SAS 보안 장비에서 기존 개체 정의를 불러와 새로운 정책 규칙을 만드는 데 사용하는 것이 가능합니다.
정책 규칙 공유	여러 방화벽에서 손쉽게 정책을 공유할 수 있습니다.
관리 RBAC(역할 기반 액세스 제어)	관리 애플리케이션에 대한 차별화된 역할 기반 액세스를 제공합니다. 예를 들면, 헬프데스크 사용자에게는 문제 해결을 위한 읽기 전용 액세스 권한을 제공하고 보안 관리자에게는 보안 정책을 관리할 수 있는 권한을 부여할 수 있습니다.

주문 정보

모든 Cisco ASA CX 컨텍스트 인식 보안 솔루션은 Cisco Prime Security Manager의 단일 장비 관리 버전과 함께 미리 탑재되어 제공됩니다. 여러 Cisco ASA CX 어플라이언스의 중앙 관리는 Cisco Prime Security Manager의 다중 장비 버전을 사용하여 구현할 수 있습니다. 이 버전은 물리적 어플라이언스 또는 VMWare ESXi 기반의 가상 어플라이언스로 사용할 수 있습니다. 두 경우 모두 라이센싱은 관리할 Cisco ASA CX 컨텍스트 인식 보안 어플라이언스의 수를 기반으로 합니다(표 3).

표 3. Cisco Prime Security Manager 라이센싱 정보

PID	설명	폼 팩터
PRSMv9-SW-5-K9	Prime Security Manager - 소프트웨어 - 5개 장비 관리	가상 어플라이언스
PRSMv9-SW-10-K9	Prime Security Manager - 소프트웨어 - 10개 장비 관리	가상 어플라이언스
PRSMv9-SW-25-K9	Prime Security Manager - 소프트웨어 - 25개 장비 관리	가상 어플라이언스
R-PRSMv9-SW-5-K9	Prime Security Manager - SW(eDelivery) - 5개 장비 관리자	가상 어플라이언스
R-PRSMv9-SW-10-K9	Prime Security Manager - SW(eDelivery) - 10개 장비 관리자	가상 어플라이언스
R-PRSMv9-SW-25-K9	Prime Security Manager - SW(eDelivery) - 25개 장비 관리자	가상 어플라이언스
PRSM-HW1-25-K9	Prime Security Manager - 소프트웨어 - 25개 장비 관리	물리적 어플라이언스

필요에 따라 기존 설치에 대한 추가 라이센스를 구매할 수 있으며, 가상 및 물리적 어플라이언스에 모두 적용할 수 있습니다(표 4).

표 4. Cisco Prime Security Manager용 추가 라이센스

PID	설명
PRSM-DEV-5=	PRSM - 라이센스 - 5개 추가 장비 관리
PRSM-DEV-10=	PRSM - 라이센스 - 10개 추가 장비 관리
L-PRSM-DEV-5=	PRSM - 라이센스 - 5개 추가 장비 관리
L-PRSM-DEV-10=	PRSM - 라이센스 - 10개 추가 장비 관리

제품 PID가 선택되었으면, 다음 단계는 Cisco Prime Security Manager용 지원 서비스를 알아보아야 합니다. Cisco Prime Security Manager의 가상 어플라이언스 버전은 SASU(Software Application Support plus Upgrades) 지원에 포함됩니다. 물리적 어플라이언스 버전은 Cisco SMARTnet®에 포함된다는 것을 참고해 주십시오. 제품 사용 및 업그레이드 환경의 간소화를 위해 제품을 구매하실 때 지원 서비스도 함께 구매하는 것이 좋습니다. 가장 적절한 서비스를 찾으려면 표 5를 참조하십시오.

표 5. Cisco Prime Security Manager용 서비스 라이센스

선택한 제품 PID		해당되는 지원 PID
PRSMv9-SW-5-K9	R-PRSMv9-SW-5-K9	CON-SAU-PRSM5
PRSMv9-SW-10-K9	R-PRSMv9-SW-10-K9	CON-SAU-PRSM10
PRSMv9-SW-25-K9	R-PRSMv9-SW-25-K9	CON-SAU-PRSM25
PRSM-DEV-5=	L-PRSM-DEV-5=	CON-SAU-PRSM5A
PRSM-DEV-10=	L-PRSM-DEV-10=	CON-SAU-PRSM10A
PRSM-DEV-25=	L-PRSM-DEV-25=	CON-SAU-PRSM25A

추가 정보

- Cisco ASA CX 컨텍스트 인식 보안: http://www.cisco.com/go/asacx
- Cisco Prime Security Manager: http://www.cisco.com/go/prsm
- Cisco ASA 5500 Series Adaptive Security Appliance: http://www.cisco.com/go/asa
- Cisco 보안 서비스: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

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.

인쇄지: 미국 C78-711823-00 07/12