

Cisco Adaptive Security Device Manager

Cisco Adaptive Security Device Manager 버전 5.2

데이터 시트

Cisco® Adaptive Security Device Manager(ASDM)는 사용하기 쉽고 직관적으로 설계된 웹 기반 관리 인터페이스를 통해 최고의 보안 관리와 모니터링 기능을 제공합니다. Cisco ASA 5500 시리즈 Adaptive Security Appliance(ASA) 및 Cisco PIX® Security Appliance 와 함께 번들로 제공되는 Cisco ASDM 은 지능형 마법사와 강력한 관리 툴, 그리고 업계 최고의 성능을 자랑하는 시스코 보안 어플라이언스 제품군의 고급 통합 보안 기능과 네트워킹 기능을 보완한 다양한 모니터링 서비스를 통해 보안 어플라이언스 배포를 가속화합니다. Cisco ASDM 은 안전한 웹 기반 설계를 통해 언제 어디서나 Cisco ASA 5500 시리즈 Adaptive Security Appliance(ASA)와 Cisco PIX Security Appliance 에 대한 액세스를 제공합니다.

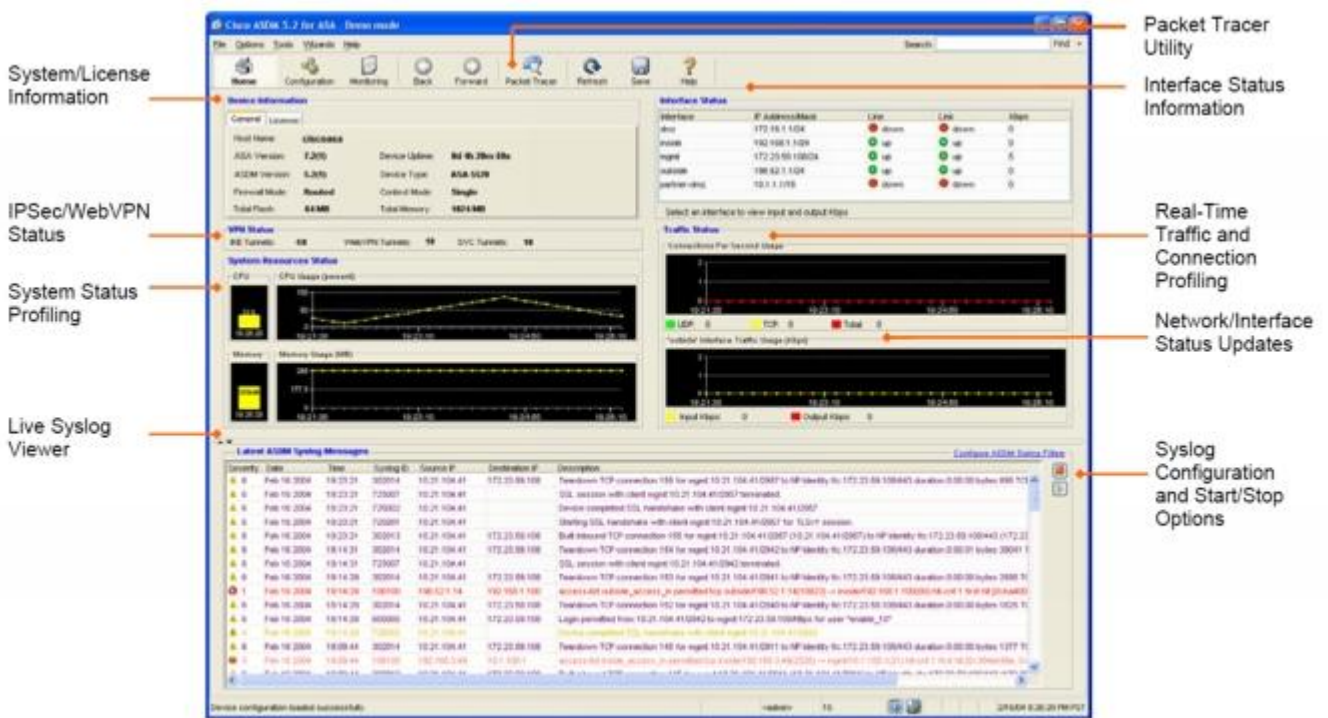
유연한 액세스 옵션을 제공하는 통합 관리 솔루션

Cisco Adaptive Security Device Manager(ASDM)는 네트워크에 연결된 Java 플러그인 사용이 가능한 컴퓨터의 웹 브라우저를 통해 바로 액세스할 수 있기 때문에 보안 관리자가 Cisco ASA 5500 시리즈 Adaptive Security Appliance나 Cisco PIX Security Appliance에 빠르고 안전하게 액세스할 수 있습니다. Cisco ASDM 은 관리자를 위한 고유한 옵션을 제공합니다. Microsoft Windows 기반 Luncher 애플리케이션을 보안 어플라이언스에서 관리 컴퓨터로 바로 다운로드할 수 있습니다. 이 Luncher 애플리케이션은 Cisco ASDM의 시작을 가속화하여 보안 어플라이언스 관리의 효율성을 높입니다. Cisco ASDM의 launcher 애플리케이션의 인스턴스를 개별적으로 실행함으로써 관리자는 단일 관리 워크스테이션의 편리함을 위해 여러 보안 어플라이언스에 연결될 수 있습니다. 소규모 비즈니스 환경에서 관리를 단순화해 줍니다.

중요한 실시간 상태 정보를 관리자에게 제공하는 대시보드

Cisco ASDM 버전 5.2는 전체 시스템 개요와 장치 상태에 관한 통계(그림 1)를 보여주는 동적 대시보드를 제공합니다. 대시보드는 구성할 시스코 보안 어플라이언스를 자동으로 감지하며, 소프트웨어 버전과 라이선스 정보 및 중요한 통계를 표시합니다. Cisco ASDM은 복잡한 네트워크 환경에서 관리자에게 실시간 상태 표시를 제공하고, 네트워크 주소, 포트 번호, 호스트 이름 등에 따라 syslog를 필터링하는 패턴 일치 및 심각도 기준 컬러링 기능을 통해 실시간 syslog 뷰어를 비롯한 분석 툴과 고급 모니터링 기능을 위한 시작 포인트를 제공합니다. 이번 5.2 버전에 포함된 구성 검색 엔진을 사용하면 관리자가 구성할 기능을 쉽게 찾을 수 있고, 검색 결과를 클릭하여 해당 위치로 바로 찾아갈 수 있습니다.

그림 1. Cisco ASDM 홈 페이지

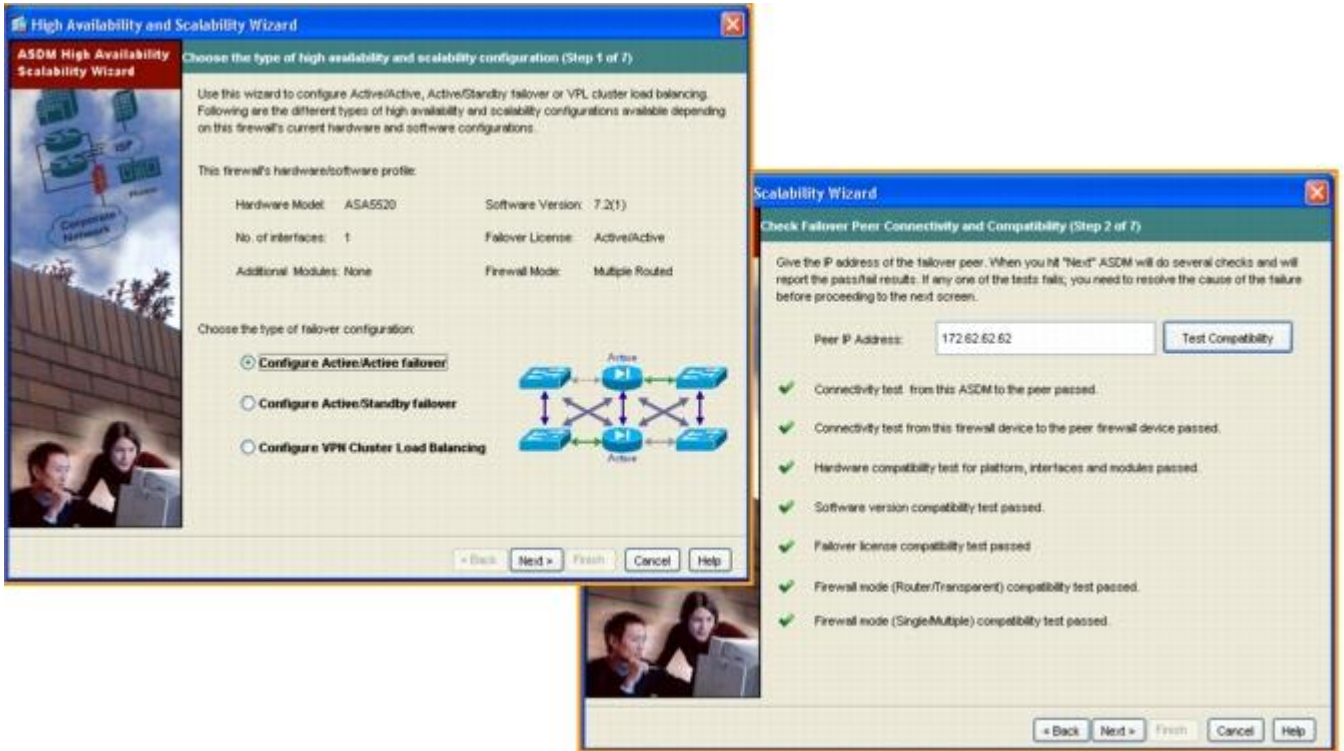


빠른 설치 마법사를 통한 보안 어플라이언스 배치 가속화

Cisco ASDM은 편리한 마법사를 통해 다양한 방화벽과 VPN 환경에서 Cisco ASA 및 Cisco PIX 보안 어플라이언스의 배치를 가속화합니다. 간단한 단계별 구성 패널을 제공하는 시작 마법사(Startup Wizard)를 통해 어플라이언스를 빠르게 설치 및 실행하고, 네트워크에서 안전한 트래픽 흐름이 가능하도록 강력한 구성 작업을 수행할 수 있습니다. 시작 마법사는 DHCP(Dynamic Host Control Protocol) 서버 설정, NAT(Network Address Translation) 및 관리 액세스, 그리고 어플라이언스 구성과 소프트웨어 이미지를 최신 상태로 유지하도록 해주는 혁신적인 보안 원격 관리 기능인 자동 업데이트(Auto Update)와 같은 선택적 기능들을 구성할 수 있도록 도와줍니다. VPN 마법사는 유사한 지능형 패널 세트를 통해 사용자가 사이트 간 VPN 터널을 빠르게 설치할 수 있도록 도와줍니다. VPN 터널은 보안 비즈니스 연결 또는 원격 액세스 VPN 터널을 확장하여 회사 리소스에 직원들이 안전하게 액세스할 수 있도록 합니다.

Cisco ASDM 버전 5.2에서는 High-Availability and Scalability Wizard(고가용성 및 확장성 마법사)를 새로 도입하여 장애복구 또는 VPN 클러스터링의 형태로 복원이 필요한 네트워크에 보안을 빠르게 배치할 수 있게 되었습니다. 이 새 마법사를 통해 사용자는 단일 관리 인터페이스를 사용하는 Active/Active 또는 Active/Standby 고가용성 모드에서 Cisco ASA 또는 Cisco PIX 보안 어플라이언스를 빠르게 설치할 수 있습니다. 직관적 인터페이스로 설계된 이러한 마법사를 사용하면 전체 배치 프로세스를 간소화할 수 있고, 연결 및 호환성에 대해 어플라이언스를 우선 점검한 다음에 각각의 장치에 필요한 매개변수를 설치하기 때문에 구성 오류를 없앨 수 있습니다. 그리고 Cisco ASA 어플라이언스의 VPN 클러스터링과 로드 밸런싱 기능을 지원합니다. 이러한 기능은 사용자가 VPN 사용자 용량을 안전하게 확장할 수 있도록 해줍니다. 기존 클러스터로 Cisco ASA 어플라이언스를 통합하거나, 아니면 새 클러스터로 초기화하는 작업을 단 몇 분 안에 완료할 수 있습니다. Cisco ASA 적응형 보안 어플라이언스 VPN 클러스터는 최대 10개 장치까지 지원할 수 있습니다. 그림 2는 Active/Active 고가용성을 구성 중인 High-Availability and Scalability Wizard(고가용성 및 확장성 마법사)를 보여줍니다.

그림 2. High-Availability and Scalability Wizard 의 Active/Active 구성

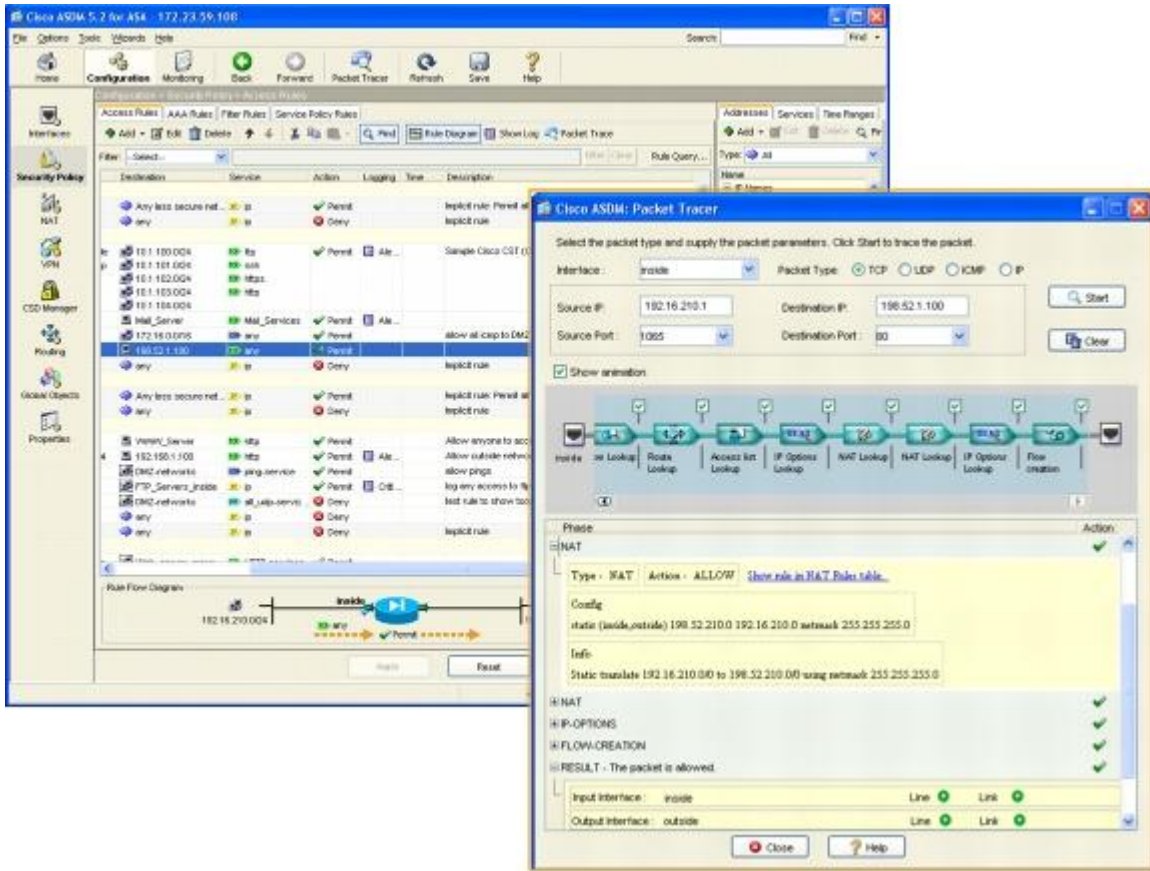


안전한 보안 정책 검사 및 시행을 위한 PACKET TRACER 유틸리티

오늘날과 같은 환경에서는 컨버지드 고급 보안 서비스를 지원할 수 있도록 제품이 개발되고 있으며, 업무 영역의 경계도 끊임없이 확대되고 있습니다. 또, 더 많은 사용자들이 연결되어 계속 사용자수가 증가되고 있습니다. 이러한 환경에 적응하기 위해 네트워크 보안 정책도 날로 복잡해지고 있습니다. 정책은 여러 네트워크 요소들을 고려해야 하며, 정책을 시행하고 변경사항을 관리하는 작업은 날마다 해야하는 힘든 작업입니다. 동시에 문제 해결 및 업데이트 모니터링은 전문적 기술과 지식을 요구합니다. 따라서 그 만큼 유지보수 비용이 높아지게 됩니다.

Cisco ASDM 버전 5.2는 현재 특허 출원 중인 혁신적인 기능의 Packet Tracer 유틸리티를 도입했습니다. 이 유틸리티는 복잡한 보안 정책, 수 많은 액세스 규칙, 여러 레이어 층의 보안 서비스 등을 포함한 보안 어플라이언스 배치에 관련된 문제점을 신속하게 해결해 줍니다. Packet Tracer 유틸리티는 움직이는 패킷 플로우 모델을 제공하기 때문에 보안 관리자가 특정 애플리케이션이나 프로토콜로 대상화할 수 있는 TCP/UDP/IP 플로우 시퀀스를 에뮬레이션할 수 있습니다. Packet Tracer를 시작하면 에뮬레이션된 패킷이 전체 장치 구성을 통해 가상으로 전달됩니다. Cisco ASDM은 구성된 매개변수를 통해 플로우를 진행하면서 각 트랜잭션 상태와, 패킷의 수명주기 단계에서 수행되는 동작을 시각적으로 보여줍니다. 각 단계의 시각적 표시는 관리자에게 부적합한 정책 정의를 알려줍니다. 이것은 오류가 난 네트워크 변환 정책이나 액세스 규칙, 검사 엔진 및 Cisco Security Service Module의 형식이 될 수 있습니다(그림 3). 관리자는 강조 표시된 오류 발생 정책을 클릭만 하면 됩니다. 해당 정책을 클릭하면 빠르게 문제를 해결할 수 있는 편집창이 열립니다. 패스쓰루 성공은 보안 정책이 정확하게 배포되어 정기적으로 실시간 트래픽을 처리할 수 있음을 나타냅니다.

그림 3. Cisco ASDM 버전 5.2 의 Packet Tracer 유틸리티

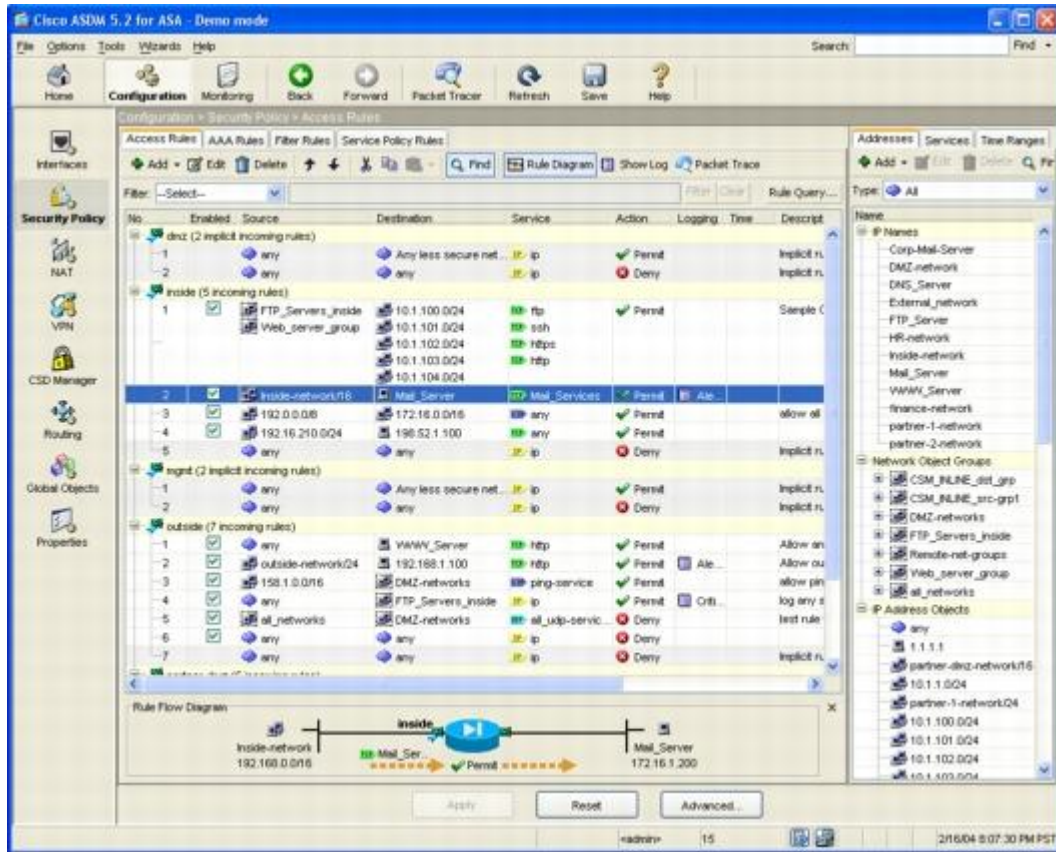


강력한 보안 정책 관리를 통한 운영비 절감

Cisco ASDM 버전 5.2는 보안 정책 정의와 지속적인 정책 관리를 단순화한 강력한 관리 서비스 기능을 제공합니다. 이러한 기능을 통해 보안 관리자는 재사용 가능한 네트워크 및 서비스 객체 그룹과 여러 보안 정책에서 참조할 수 있는 검사 정책 맵을 만들 수 있습니다. 5.2 버전에는 네트워크, 서비스, 프로토콜 및 ICMP(Internet Control Message Protocol) 유형의 객체 그룹을 지원하는 완벽한 관리 기능이 추가되었습니다. Cisco ASA Software Version 7.0 및 Cisco PIX Security Appliance Software Version 7.2에서 제공하는 강력한 액세스 제어 기능을 지원합니다. 예를 들어, 사용자/그룹/시간 기반의 액세스 목록과 인바운드/아웃바운드 액세스 목록과 같은 기능이 포함됩니다.

Cisco ASDM 버전 5.2는 완전히 새롭게 추가된 통합 정책 테이블 기능을 제공합니다. 이 테이블 기능을 통해 관리자는 애니메이션되는 단일 패널에서 전체 보안 정책을 편리하게 볼 수 있습니다. 목록에서 해당 정책을 클릭만 하면 관련된 매개변수를 편집할 수 있는 창이 뜹니다. 따라서 구성 변경과 업데이트 작업을 간단하게 수행할 수 있습니다. 사이드바에서 객체 그룹을 선택할 수 있는 아이콘을 눌러 모든 네트워크 및 서비스 객체 그룹을 즉시 편집할 수 있어서, 이러한 객체 그룹들이 실시간으로 빠르게 참조되고 수정될 수 있도록 합니다(그림 4) 이 외에도 Rule Query 옵션을 통해 다양한 네트워크 요소를 필터링하고, 보안 정책 모니터링 및 문제해결과 관련된 관심 객체 그룹도 빠르게 필터링할 수 있습니다.

그림 4. 통합 정책 규칙 테이블



비즈니스 차원의 보안 서비스 - 안전한 역할 기반 관리 액세스 시행

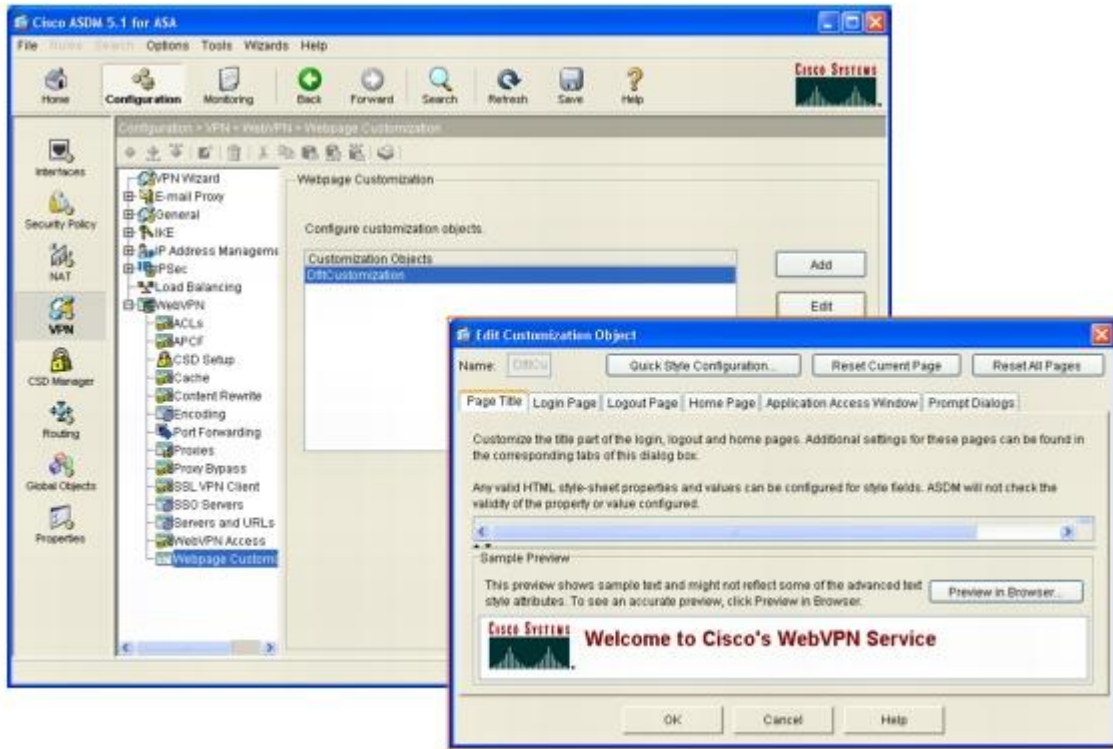
Cisco ASDM 버전 5.2는 장치에 대한 무단 관리 액세스를 방지하기 위해 다양한 보안 서비스를 통합했습니다. Cisco ASA 5500 시리즈 적응형 보안 어플라이언스 또는 Cisco PIX 보안 어플라이언스에서의 로컬 인증 데이터베이스, 또는 RADIUS/TACACS 서버 경유 방식을 포함하여 관리자를 인증하는 다양한 방법들을 지원합니다. Cisco ASDM(관리자의 컴퓨터에서 실행 중임)과 보안 어플라이언스 간의 모든 커뮤니케이션은 56비트 데이터 암호화 표준(DES) 또는 이보다 더 안전한 168비트 3중 DES 알고리즘을 사용한 SSL(Secure Sockets Layer)을 통해 암호화됩니다. Cisco ASDM 버전 5.2는 관리 액세스를 최대 16개 수준으로 사용자 정의할 수 있도록 지원함으로써 시스코 보안 어플라이언스를 관리하는 관리자와 작업 담당자에게 적절한 수준의 권한을 부여할 수 있습니다. 예를 들어, 구성에 대해 모니터링만 가능하게 또는 읽기만 가능하게 액세스를 제한할 수 있습니다.

VPN 관리를 통한 비즈니스 파트너 및 원격 사이트로 보안 연결 확장

Cisco ASDM 버전 5.2는 사이트 간 VPN 배치를 위해 회사에서 IKE(Internet Key Exchange)와 IPsec(IP Security) 정책을 설정하도록 지원해주는 편리한 프로비저닝을 위한 지능형 VPN 마법사를 비롯한 포괄적인 VPN 구성 기능을 제공합니다. 또한 Cisco ASDM은 VPN 클라이언트 보안 상태(security posture) 적용, 소프트웨어 자동 업데이트, VPN 클러스터링 등의 기능을 지원하는 Cisco Easy VPN 원격 액세스 VPN Concentrator 서비스를 위한 완벽한 관리를 제공합니다.

Cisco ASDM은 Cisco ASA 5500 시리즈에서 관리자가 인터넷 기반 웹 브라우저와 SSL 암호화를 통해 원격 액세스 접속을 활성화하고, 신속하게 프로비저닝을 할 수 있도록 지원하는 Cisco WebVPN의 풍부한 관리 기능(그림 5)이 통합되었습니다.

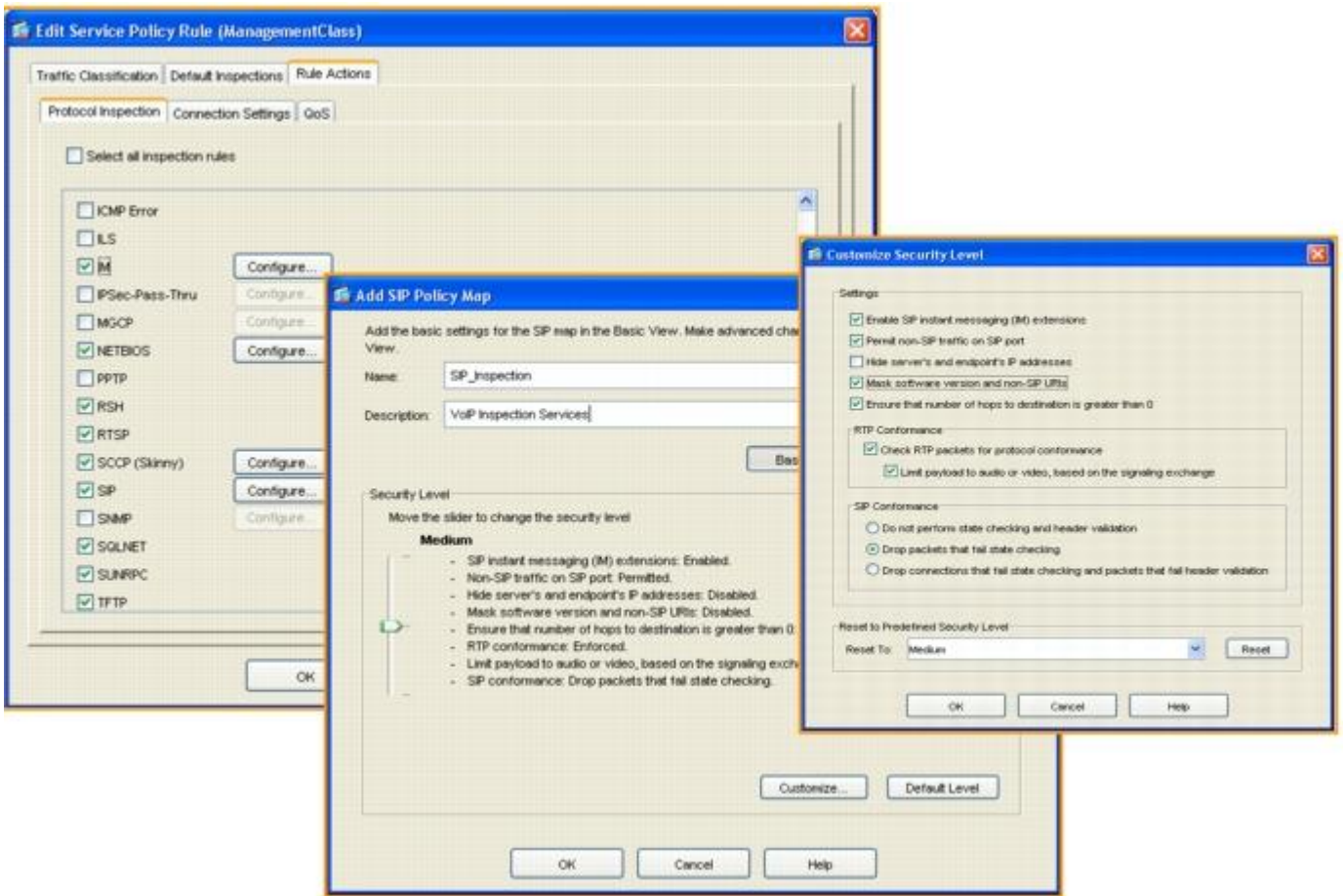
그림 5. WebVPN 구성



향상된 애플리케이션 검사를 보완한 포괄적인 관리 서비스

Cisco ASA Software Version 7.0 및 Cisco PIX Security Appliance Software Version 7.2는 HTTP, FTP, 인스턴트 메시징 프로토콜, SIP(Session Initiation Protocol), SCCP(Skinny Call Control Protocol), H.323, GTP(GPRS Tunneling Protocol), DNS, DCE-RPC & SunRPC(Microsoft and Sun Remote Procedure Call)와 같은 프로토콜에 대해 애플리케이션 검사 및 제어 서비스를 광범위하게 제공합니다. Cisco ASDM 버전 5.2는 사전 정의된 보안 프로파일(Low, Medium, High)을 통해 풍부한 애플리케이션 보안 서비스 배치를 가속화합니다. 그림 6은 SIP에 대해 설정된 Medium 보안 프로ファイルを 보여줍니다. 기본적인 애플리케이션 보안 배치의 경우 이와 같이 사전 정의된 프로 파일을 사용하여 보안 어플라이언스 간에 지원되는 애플리케이션과 프로토콜을 필요한 수준의 보안으로 빠르게 패스스루할 수 있습니다. 또한 사전 정의된 프로 파일을 사용자 정의하여, 트래픽 흐름을 보다 세부적으로 제어할 수 있도록 허용할 수도 있고, 보다 강력한 보호 프로 파일을 통해 강화된 애플리케이션을 제공할 수도 있습니다. 사용자는 새로운 애플리케이션 취약점과 공격으로부터 동적 위협 보호를 위해 본인만의 서명을 만들 수 있습니다. Cisco ASDM 버전 5.2에서는 사전 정의된 프로 파일과 사용자 정의 가능한 옵션을 결합하여 사용함으로써 업무용 애플리케이션과 중요한 리소스를 애플리케이션 오사용과 터널링 공격으로부터 보호하도록 Cisco ASA 및 Cisco PIX 보안 어플라이언스를 신속하게 배치할 수 있습니다.

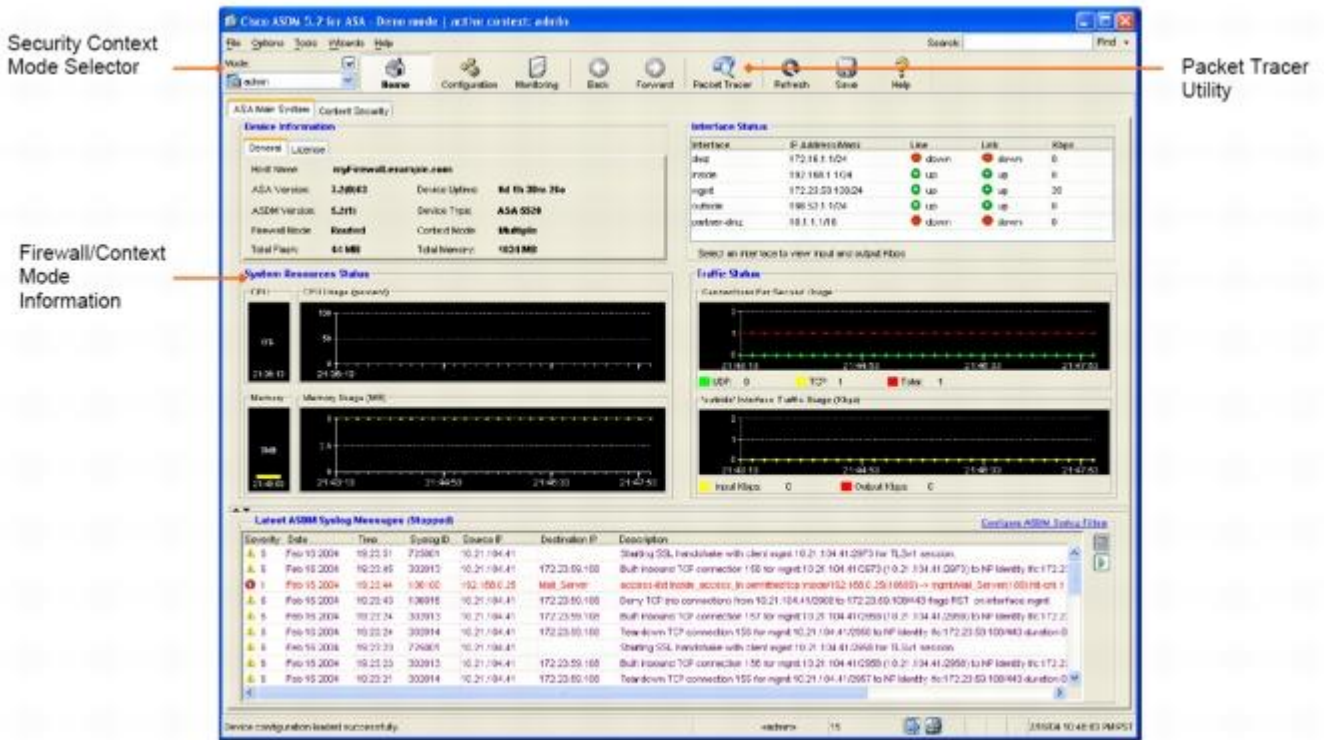
그림 6. SIP Inspection Services 의 고급 구성



인텔리전트한 사용자 인터페이스를 통해 복잡한 네트워크 환경의 통합 간소화

Cisco ASDM 버전 5.2는 Cisco ASA 5500 시리즈 및 Cisco PIX 보안 어플라이언스의 다양한 네트워크 통합 기능을 관리하기 위한 쉽고 편리한 액세스를 제공합니다. 가상화를 통해 동일한 보안 어플라이언스에 여러 개의 보안 컨텍스트를 생성할 수 있습니다. 이들 각각의 컨텍스트는 자체 보안 정책과 논리 인터페이스 및 관리 도메인 세트를 가지고 있습니다. Cisco ASDM은 인텔리전트한 가상화 관리 시스템을 통해 시스템 상의 모든 가상 방화벽과 기능을 전체적으로 볼 수 있도록 중앙의 시스템 관리자에게 무제한의 액세스를 제공합니다(그림 7). 개별 컨텍스트 사용자들은 동일한 관리 및 모니터링 기능뿐만 아니라, 동일한 Cisco ASDM 인터페이스를 경험할 수 있습니다. 그러나 구성과 기능에 대한 액세스는 중앙의 시스템 관리자가 지정한 대로, 컨텍스트 사용자로 할당 받은 경우에만 가능합니다. 개별 컨텍스트 사용자는 관리자가 만든 보안 정책에 따라 Cisco ASDM을 사용하는 가상 방화벽에 대한 구성을 사용자 정의할 수 있습니다.

그림 7. Security Context 의 시스템 관리자 뷰



Cisco ASDM 버전 5.2는 관리자에게 PIM(Protocol Independent Multicast), OSPF(Open Shortest Path First) 동적 라우팅, IEEE 802.1q 기반 VLAN 인터페이스 및 QoS(Quality of Service)와 같은 멀티캐스트 라우팅 프로토콜에 대한 완벽한 제어를 제공합니다. novice 사용자들을 위해 인텔리전트한 기본값과 상세한 온라인 도움말을 결합하여 이러한 네트워킹 서비스에 대한 구성을 단순화할 수 있습니다. 고급 사용자는 복잡한 라우팅 및 스위칭 환경으로 시스코 보안 어플라이언스를 통합하기 위해 기능의 깊이를 완벽하게 이용할 수는 없습니다.

적응형 보안 관리 인터페이스를 통한 통합 위험 관리 경험 강화

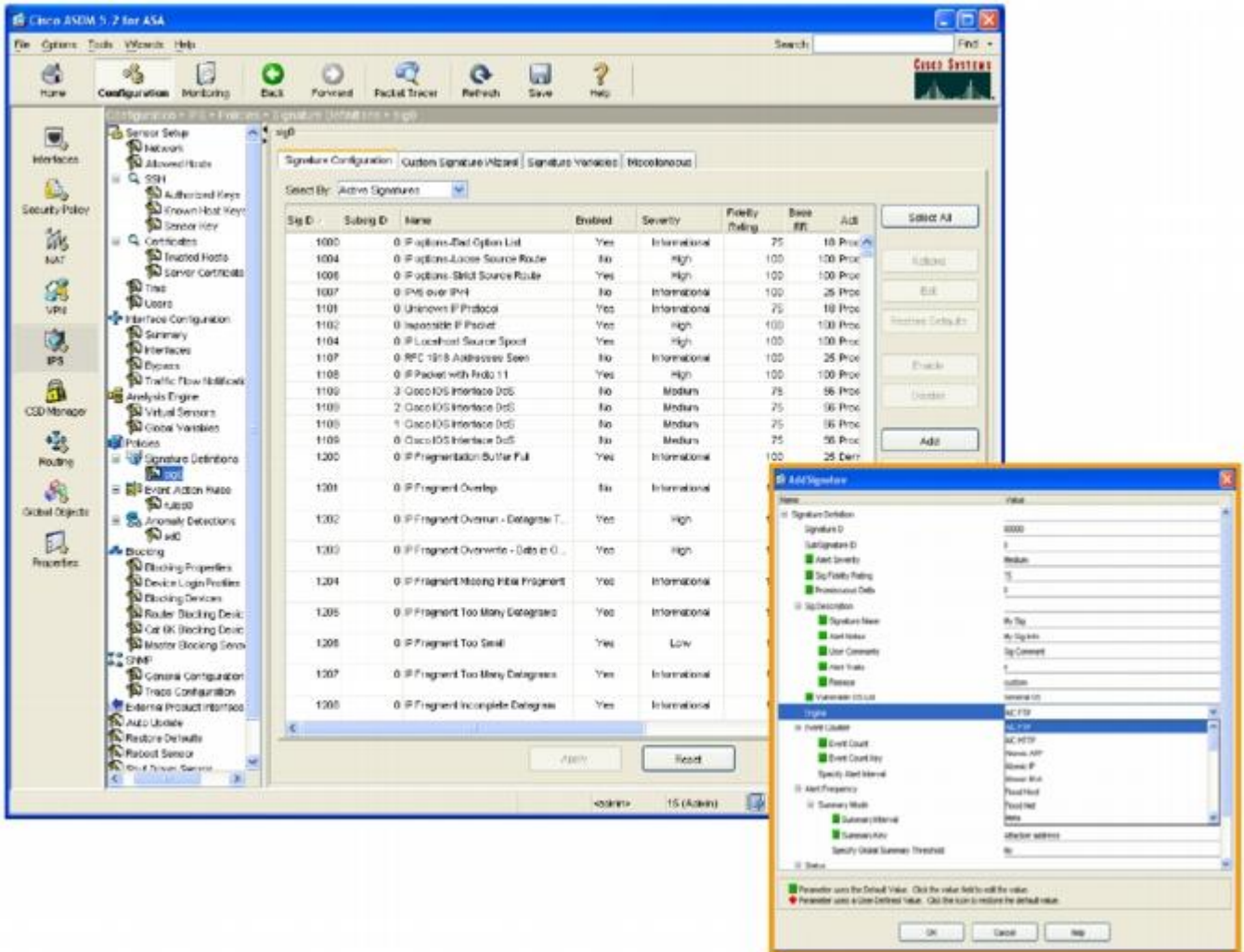
Cisco ASDM 5.2 버전은 Cisco ASA 5500 시리즈 및 Cisco PIX 보안 어플라이언스의 구성, 관리 및 모니터링을 위한 단일 솔루션을 제공합니다. Cisco ASA 5500 시리즈에서 제공되는 적응형 보안 서비스를 관리하는 비즈니스용 솔루션을 제공합니다.

인라인 침입 방지 서비스 관리 및 네트워크 기반 웹 방지

Cisco ASDM Version 5.2를 통해서 기업은 회사 네트워크 환경의 보안 수준을 높힐 수 있습니다. 반면 Cisco AIP-SSM(Advanced Inspection & Protection Security Services Module)을 통해 다양한 공격으로부터 보호 관리를 효율적으로 제공할 수 있어 운영비를 절감할 수 있습니다. 이러한 서비스는 침입, 네트워크 공격, DoS(denial of service) 공격 및 웜이나 애드웨어와 같은 악성 프로그램으로부터 보호를 제공합니다. Cisco ASDM을 통해 관리자는 Cisco Traffic Risk Rating 및 Cisco Meta Event Generator와 같은 고유한 보호 기술을 비롯하여 이러한 서비스를 신속하게 구성할 수 있습니다(그림 8). Cisco ASDM은 기업 고객에게 광범위한 공격으로부터 회사의 네트워크를 보호함으로써 합법적인 네트워크 트래픽이 누락되는 위

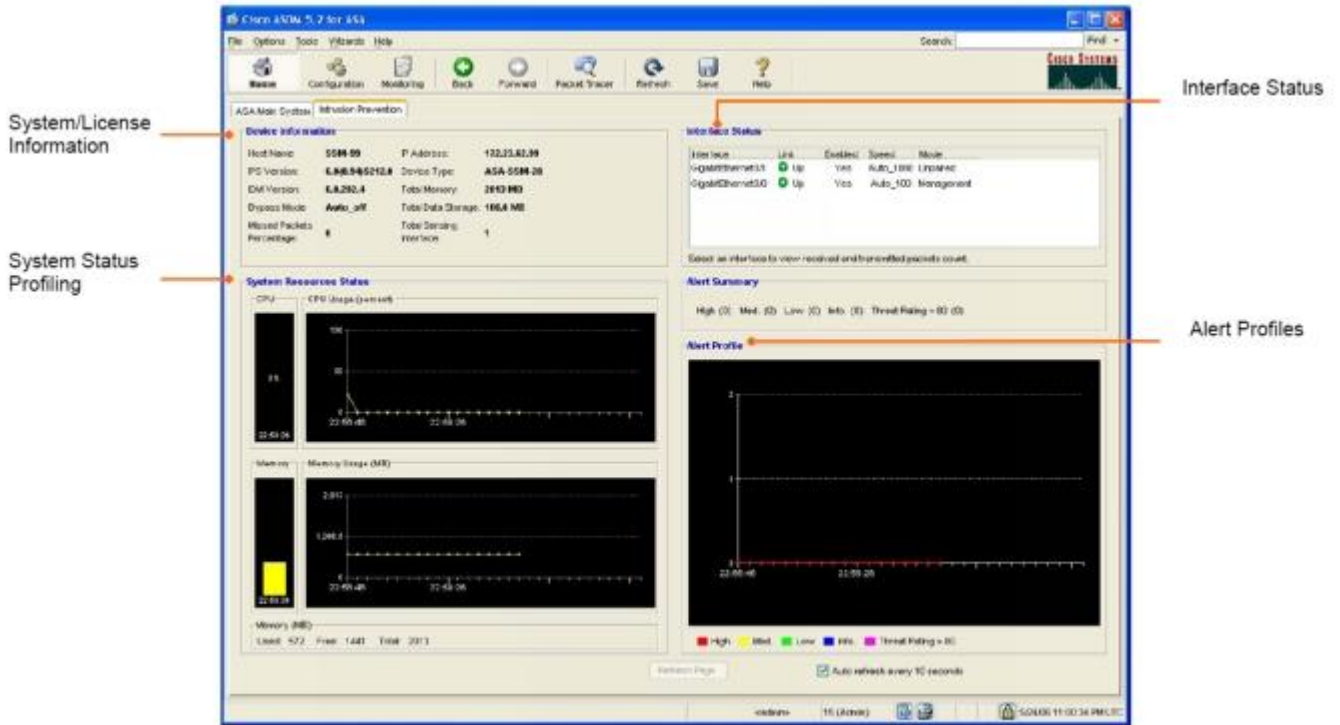
형을 제거할 수 있습니다.

Figure 8. Cisco AIP-SSM 의 이벤트 동작 구성



Cisco ASDM 버전 5.2는 실시간 모니터링 패널과 함께 AIP-SSM을 위한 새로운 침입 방지 홈페이지를 제공합니다. AIP-SSM이 설치되면 메인 ASDM 홈페이지가 자동으로 업데이트되어 새 Intrusion Prevention 패널에 표시됩니다(그림 9). 이 패널은 IPS 통계, 시스템 리소스, 위험 경고 등에 대한 지난 내역을 보여줍니다.

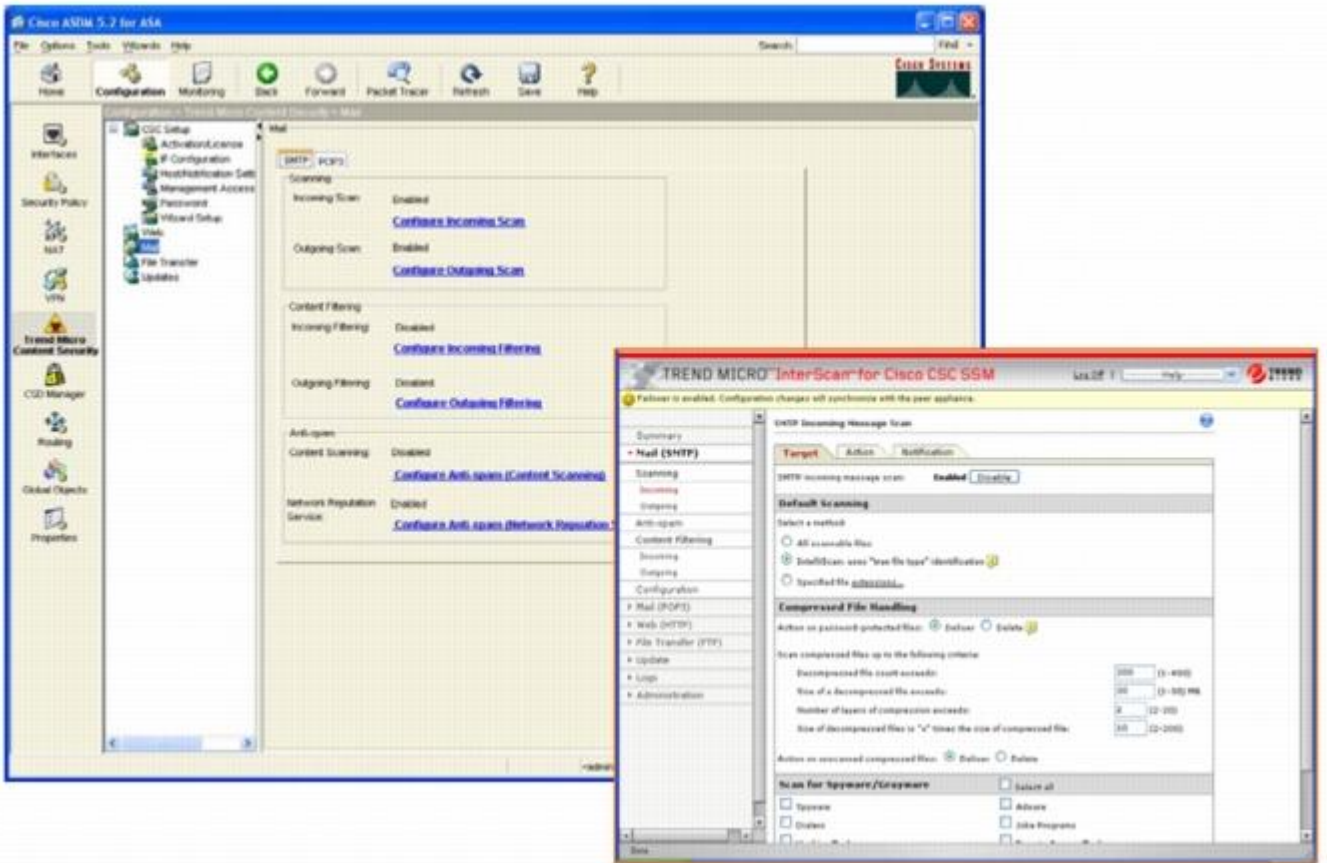
그림 9. Cisco ASDM 의 Intrusion Prevention 패널



컨텐츠 보안 및 안티바이러스 서비스 관리

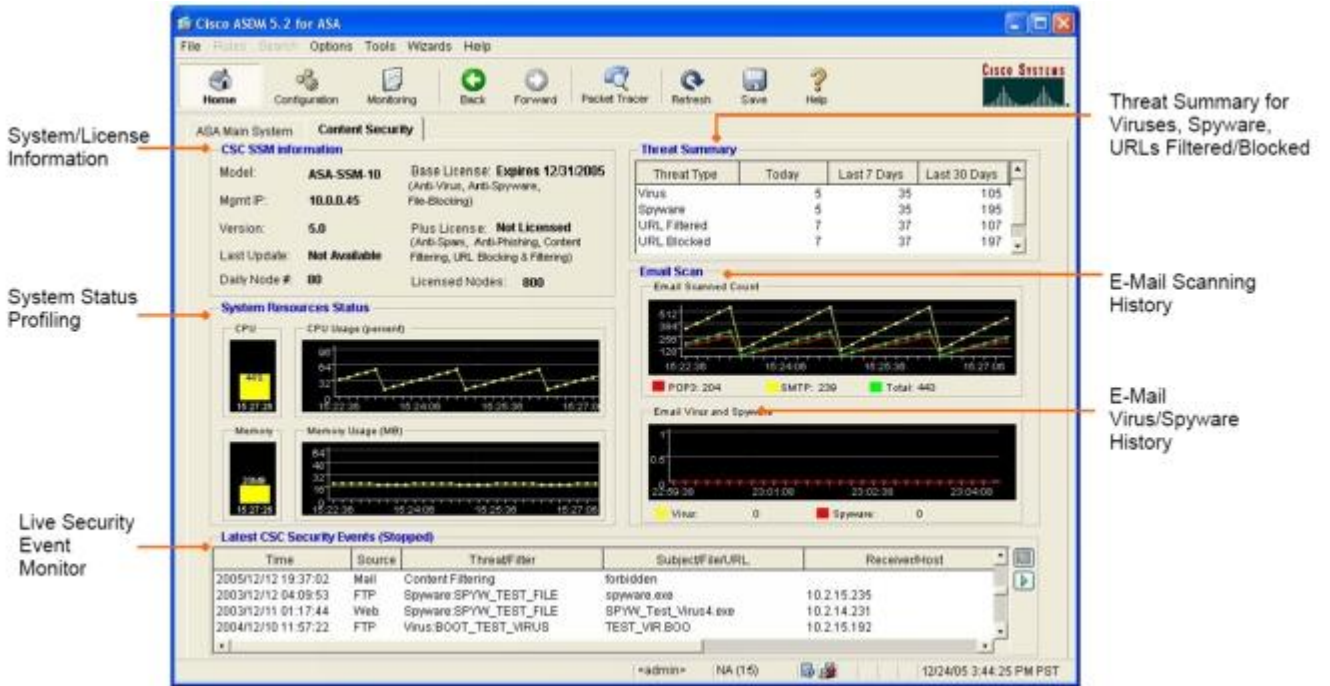
Cisco ASA 5500 Series Content Security 및 Control Security Services Module(CSC-SSM)은 단일 서비스 카드에서 고성능 안티바이러스 서비스를 제공합니다. Cisco CSC-SSM은 업계 최고의 기술로 인정받고 있고 수상 경력도 있는 Trend Micro의 컨텐츠 보안 관리를 위한 제품인 InterScan을 통합시켜 안티바이러스, 안티스팸, 안티피싱, URL 차단 및 필터링 서비스를 포함하여 인터넷 게이트웨이에 대한 포괄적인 보호와 제어를 제공합니다. CSC-SSM과 함께 Cisco ASDM 버전 5.2는 Cisco ASDM의 정교함에 Trend Micro의 HTML 기반 구성 패널의 단순함이 결합되어 업계 최고의 솔루션을 제공합니다(그림 10). 이를 통해 일관되게 정책을 시행할 수 있고, 통합 위협 관리 기능을 위한 전체 프로비저닝과 구성 및 모니터링 프로세스를 단순화합니다.

그림 10. Cisco CSC-SSM SMTP 수신 메일 검사 구성



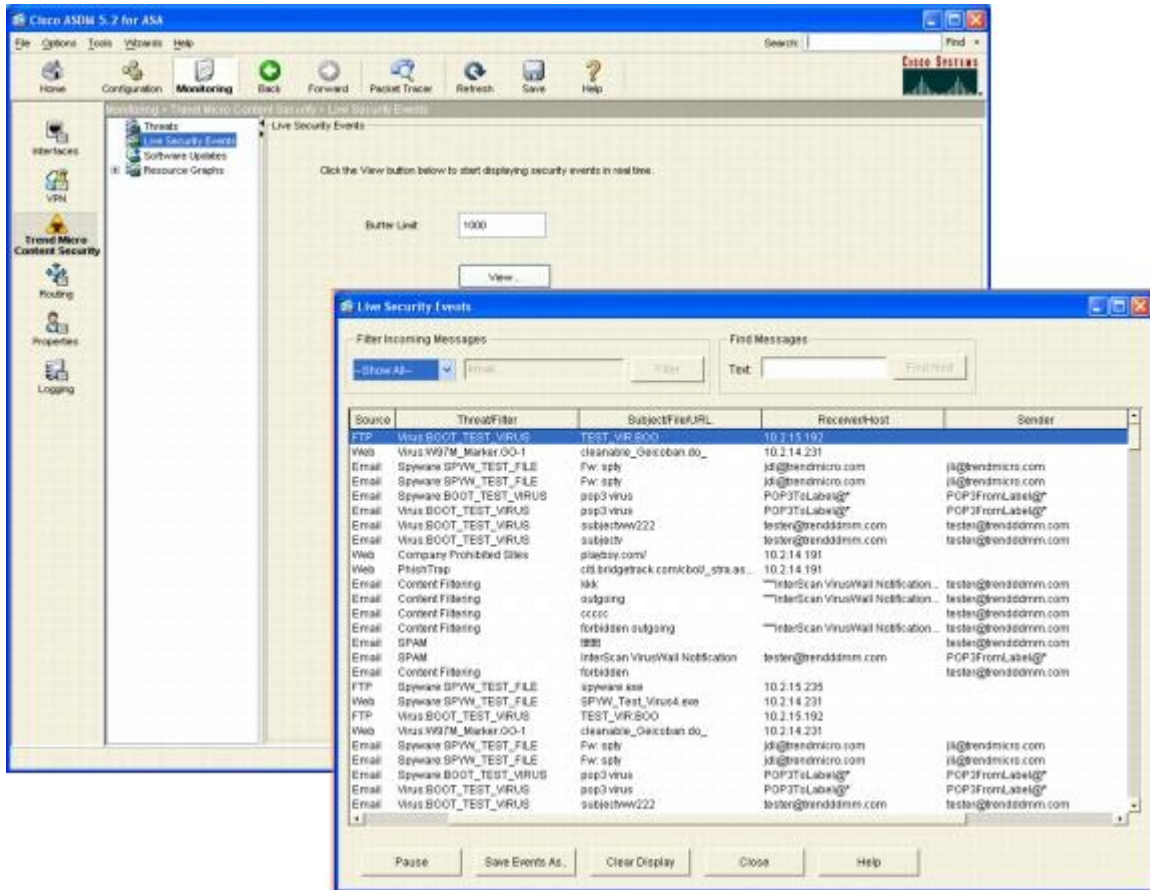
Cisco ASDM 버전 5.2는 새로운 CSC-SSM 홈페이지와 새로운 모니터링 패널을 통해 보다 개선된 모니터링 솔루션을 제공합니다. CSC-SSM이 설치되면 메인 ASDM 홈페이지가 자동으로 업데이트되어 새 CSC-SSM 패널에 표시됩니다(그림 11). 이 패널에는 최근 설치된 소프트웨어 및 서명 업데이트, 시스템 리소스 등과 같이 중요한 모듈 통계와 이메일 바이러스, 실시간 이벤트에 대한 이전 내역을 볼 수 있습니다.

그림 11. Cisco ASDM 버전 5.2의 CSC-SSM 홈페이지



Cisco ASDM 버전 5.2의 모니터링 섹션 내에 있는 다양한 분석 툴 세트는 위협, 소프트웨어 업데이트, 리소스 그래프 등에 대한 상세한 가시성을 제공합니다. Live Security Event Monitor(그림 12)는 새로운 문제 해결 및 모니터링 툴로서 스캔되었거나 차단된 전자메일 메시지, 차단된 바이러스/웜 방지 및 공격으로부터 검사되고 차단됩니다. 정규 표현식 구문 일치치를 통한 메시지 필터링 옵션을 관리자에게 제공합니다. 이러한 옵션을 통해 특정 공격 유형과 메시지에 포커스를 맞추고 상세하게 분석될 수 있습니다.

그림 12. Cisco CSC SSM 의 Monitoring 패널 및 Live Security Event 모니터링

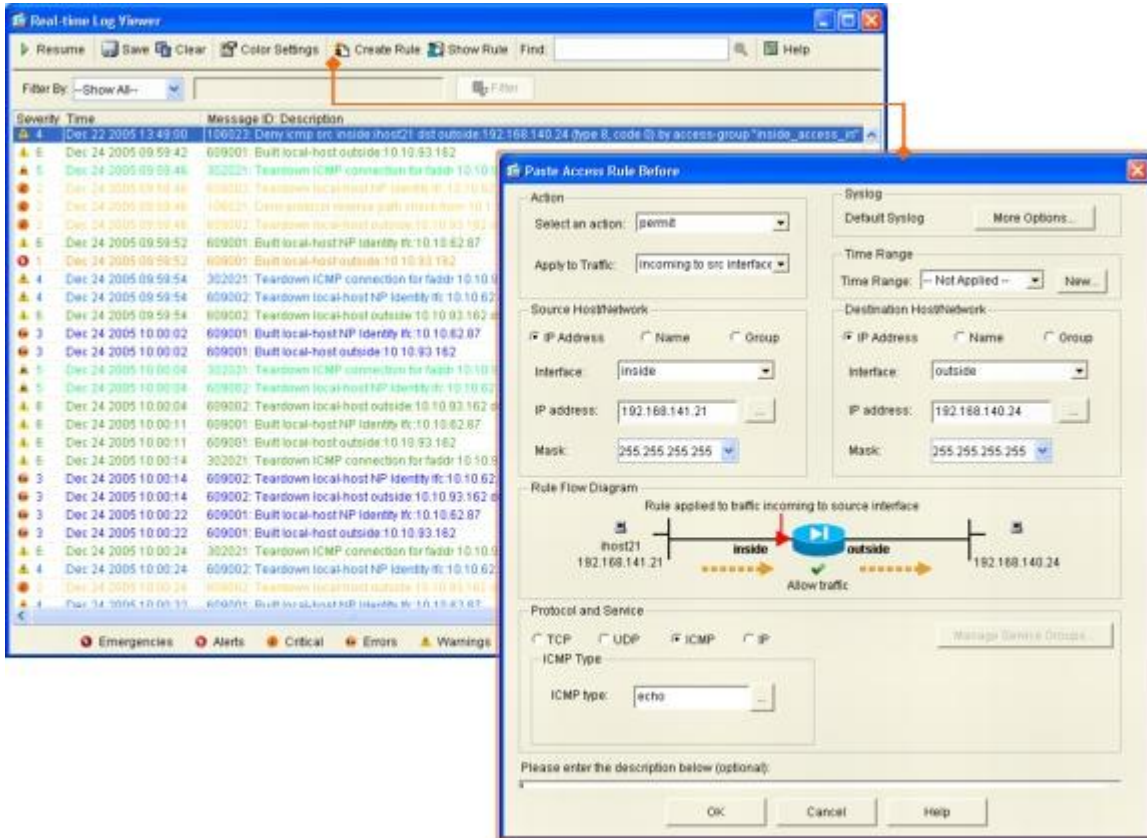


향상된 모니터링 및 보고 툴을 통해 중요한 BUSINESS-CRITICAL 분석 가능

Syslog to Access Rule Correlation

Cisco ASDM 버전 5.2는 매일 매일 이루어지는 보안 관리와 문제해결 활동을 대폭 강화한 Syslog to Access Rule Correlation 툴을 새로 도입했습니다. 이 동적 툴을 통해 보안 관리자는 대부분의 사용자 및 네트워크 연결 문제와 함께 일반적인 구성 문제를 빠르게 해결할 수 있습니다. 사용자는 Real-Time Syslog Viewer 패널에서 syslog 메시지를 선택할 수 있습니다. 패널 상단에 있는 "생성" 버튼을 클릭하면 특정 syslog에 대한 액세스 제어 옵션을 호출할 수 있습니다. 인텔리전트한 기본값을 사용하면 구성 프로세스를 단순화할 수 있습니다. 중요한 업무용 기능에 대한 운영 효율성과 응답 시간을 개선합니다. Syslog to Access Rule Correlation 툴은 사용자가 구성한 액세스 규칙에 의해 호출되는 syslog 메시지에 대한 직관적인 뷰를 제공합니다. 관리자는 엔터프라이즈 트래픽 패턴을 주로 관찰할 수 있고, 액세스 동작에 따른 리소스를 모니터링합니다. 그림 13은 사용자가 syslog 메시지를 선택하고 해당 플로우에 대한 정책을 정의하기 위해 Create 단추를 클릭하면 나타나는 Syslog to Access Rule Correlation입니다.

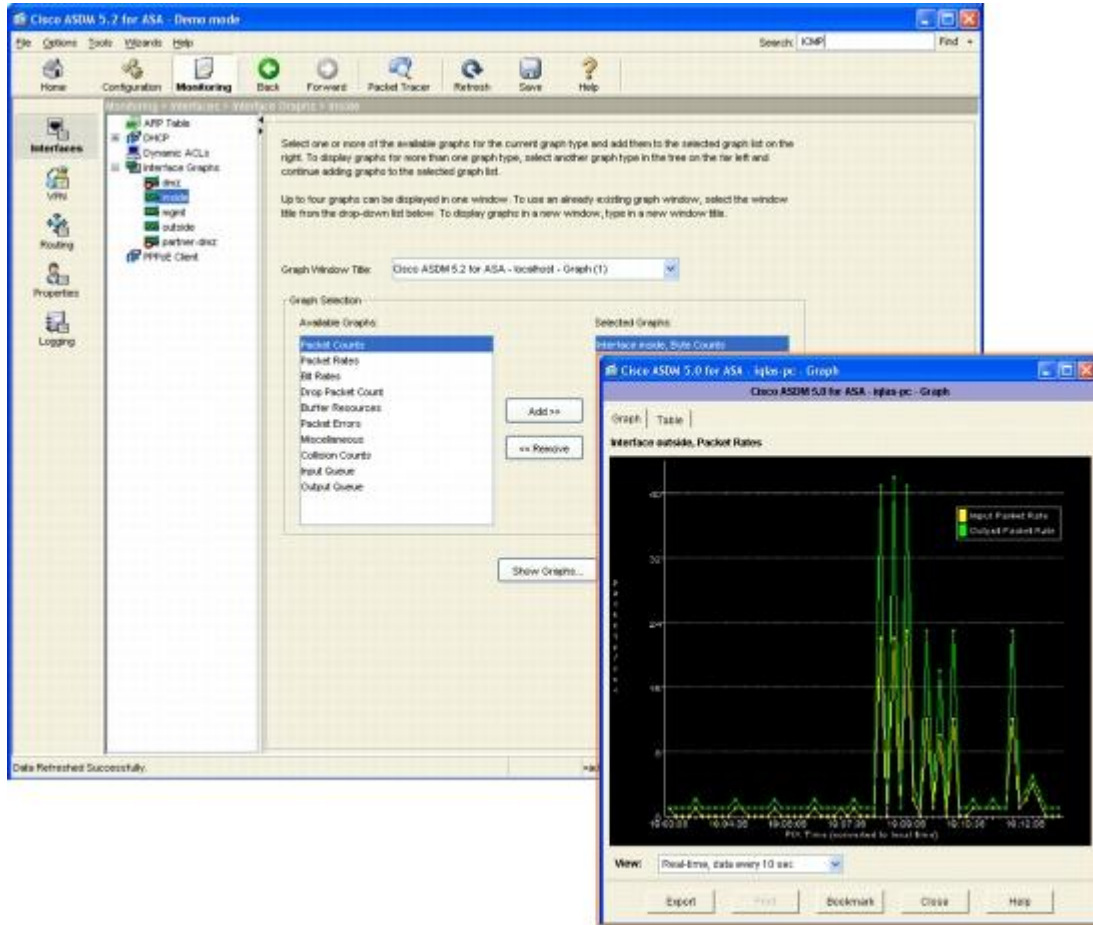
그림 13. Syslog to Access Rule Correlation 툴



모니터링 툴

Cisco ASDM 버전 5.2는 새로운 홈페이지에서 모니터링 기능을 한 눈에 볼 수 있는 기능뿐만 아니라 심도 있는 모니터링 및 보고 서비스를 제공합니다(그림 14). 다양한 분석 툴을 통해서 실시간 사용, 보안 이벤트 및 네트워크 활동을 보여주는 그래픽 요약 보고서를 만들 수 있습니다. 각 그래픽 보고서의 데이터는 사용자 정의 가능한 방식으로 표시할 수 있습니다. 예를 들어, 사용자가 10초의 스냅샷 또는 늘어난 시간 일정에 대한 분석 중 하나를 선택할 수 있습니다. 여러 그래프를 동시에 볼 수 있는 기능을 통해 사용자는 상세한 평가를 동시에 수행할 수 있습니다. 그래프는 편리하게 북마크되고, 나중에 액세스할 수 있도록 데이터를 내보낼 수 있습니다.

그림 14. Cisco ASDM 홈페이지의 Monitoring 화면



시스템 그래프(System graphs) - Cisco ASA 및 Cisco PIX 보안 어플라이언스에 대한 자세한 상태 정보를 제공합니다. 사용된 블록 수, 남은 블록 수, 현재 메모리 사용량, CPU 사용량 등에 대한 정보가 포함됩니다.

연결 그래프(Connection graphs) - 연결, 주소 변환, 인증, 권한 부여 및 계정(AAA) 트랜잭션, URL 필터링 요청 등의 데이터에 대한 초 단위 성능 모니터링과 실시간 세션을 추적합니다. 연결 그래프를 통해 네트워크 연결 및 활동에 대해 관리자에게 통보로 알려줍니다.

공격 보호 시스템 그래프(Attack protection system graphs) - 잠재적으로 해로운 활동을 보여주는 16개의 서로 다른 그래프를 제공합니다. 공격 서명(Attack signature) 정보는 IP, Internet Control Message Protocol, User Datagram Protocol(UDP), TCP 공격 및 Portmap 요청과 같은 활동을 표시합니다. 또한 자세한 공격자 목록과 이벤트 목록, 시스템 통계, Cisco AIP-SSM에 대한 진단을 제공합니다.

인터페이스 그래프(Interface graphs) - 보안 어플라이언스의 각 인터페이스에 대해 대역폭 사용을 실시간으로 모니터링한 정보를 제공합니다. 들어오고 나가는 커뮤니케이션에 대해 대역폭 사용이 표시됩니다. 사용자는 패킷 속도, 카운트 수, 오류 수, 비트 수, 바이트 수, 충돌 수 등을 볼 수 있습니다.

VPN 통계 및 연결 그래프(VPN statistics and connection graphs) - 터널 업타임 및 전송된 바이트/패킷, Cisco IPsec Flow Monitoring MIB에 대한 지원을 비롯한 터널당 자세한 통계를 제공하는 VPN 연결에 대한 완벽한 가시성을 제공합니다.

표 1은 Cisco ASDM 버전 5.2의 주요 기능과 이점을 나타냅니다.

표 1. Cisco ASDM 버전 5.2의 주요 기능과 이점 요약

제품 기능	이점
Cisco ASA Software Version 7.2 및 Cisco PIX Security Appliance Software Version 7.2 기능의 완벽한 지원	<ul style="list-style-type: none"> • Cisco ASA Software Version 7.2 및 Cisco PIX Security Appliance Software Version 7.2에 도입된 새로운 기능에 대한 다양한 구성 및 모니터링 지원을 제공합니다.
Packet Tracer 유틸리티(특히 출원 중)	<ul style="list-style-type: none"> • 실시간 트래픽 흐름이 전체 시스템 구성에 미치는 영향을 확인하는 문제 해결 프로세스를 가속화합니다. • 애니메이션되는 결과 스케치 - 각 정책을 엄격하게 테스트하고, exploration free 정책 조정에 대해 실패한 테스트를 교정하는 링크를 제공합니다.
모든 애플리케이션 검사 및 제어 기능에 대한 프로필 기반 관리	<ul style="list-style-type: none"> • 각 애플리케이션 검사 엔진에 사전 정의된 보안 프로필 (Low, Medium, High)을 사용하여 모든 보안 환경에서 배치를 신속하게 수행할 수 있습니다. • 보안 프로필에 대한 세분화된 사용자 정의를 통해 고급 애플리케이션의 요구를 충족할 수 있습니다. • 기존 보안 정책에 사용자 정의된 정규 표현식을 간단하게 통합할 수 있어 최신 애플리케이션 공격에 대한 위협에 신속하게 대응할 수 있습니다.
고가용성 및 확장성 마법사	<ul style="list-style-type: none"> • 편리한 단일 관리 연결을 통해 Active/Active 및 Active/Standby 고가용성 또는 VPN 클러스터링 및 로드 밸런싱 기능의 배치를 단순화합니다. • 포괄적인 연결 테스트와 오류 검사를 통해 정확하고 매끄러운 배포가 가능합니다.
통합 보안 정책 및 액세스 제어 테이블	<ul style="list-style-type: none"> • 모든 액세스 규칙, AAA 및 시스템 보안 정책에 대한 구체적인 정보를 제공함으로써 향상된 정책 구성과 관리 경험을 제공합니다. • 관리자가 네트워크 요소와 해당 정책을 빠르게 검색할 수 있도록 지원해주는 새로운 규칙 쿼리 옵션을 통해 문제를 신속하게 해결합니다. • 새로운 객체 그룹 선택기 패널을 통해 모든 네트워크 및 서비스 객체 그룹에 대한 편집을 신속하게 수행할 수 있습니다.
향상된 문제 해결 기능	<ul style="list-style-type: none"> • syslog 참조를 통합하여 보안 문제점을 신속하게 격리하고 해결하기 위해 각 메시지에 대한 간단한 설명과 권장 조치를 제공합니다. • 시간, 날짜, syslog ID 및 IP 주소에 기반한 사용자 정의 뷰에 대한 syslog 메시지의 구분 분석이 가능합니다. • 네트워크 연결 테스트 및 확인을 위한 Traceroute 지원

	<p>을 제공합니다.</p> <ul style="list-style-type: none"> • AAA, 로깅 필터, SSL VPN 클라이언트 등의 기능 구성 방법을 설명한 ASDM Assistance Guide를 제공합니다.
--	--

라이선스

Cisco ASDM 버전 5.2는 Cisco ASA Software Version 7.2 (1) 또는 Cisco PIX Security Appliance Software Version 7.2(1) 이상과 함께 제공됩니다.

따라서 Cisco ASDM에 대한 개별 라이선스는 필요 없으나, 호스트 Cisco ASA 5500 시리즈 Adaptive Security Appliance 또는 Cisco PIX Security Appliance에 사용되는 DES 또는 3DES 라이선스는 필요합니다. 현재 Cisco ASA 5500 시리즈 또는 Cisco PIX 보안 어플라이언스에서 암호화를 사용할 수 없는 사용자는 무료 DES/3DES 인증 키를 요청하시면 됩니다. 또는 온라인 포럼에서 무료로 현재 DES 라이선스를 3DES 라이선스로 업그레이드할 수 있습니다.

온라인 포럼: <http://www.cisco.com/go/license>

기술 사양

Cisco ASA 5500 시리즈의 시스템 요구사항

하드웨어

- 플랫폼: Cisco ASA 5505, 5510, 5520, 5540, 5550 ASA
- RAM: 256MB
- 플래시 메모리: 64MB

소프트웨어

- Cisco ASA 소프트웨어: 버전 7.2
- 암호화: DES 또는 3DES 사용

Cisco PIX Security Appliance 의 시스템 요구사항

하드웨어

- 플랫폼: Cisco PIX 515/515E, 525, 535 Security Appliances(Cisco PIX 501 및 506/506E 보안 어플라이언스는 지원되지 않음)
- RAM: 64MB

참고: 이 버전에서는 이전 소프트웨어 버전에서 요구되던 메모리 업그레이드 보다 더 많은 메모리가 Cisco PIX 515/515E Security Appliance 에 필요합니다.

- 플래시 메모리: 16MB

소프트웨어

- Cisco PIX Security Appliance Software Version 7.2
- 암호화: DES 또는 3DES 사용

사용자 시스템 요구사항

하드웨어

- 프로세서: Intel Pentium III 450MHz, Pentium 4 또는 동급 500MHz(권장)
- RAM: 256MB(최소)
- 표시 해상도: 1024 x 768 픽셀(최소)
- 표시 색상: 256(16 비트 하이컬러 권장)

소프트웨어

표 2는 Cisco ASDM 버전 5.2에서 지원되는 운영체제와 웹 브라우저를 나타냅니다.

표 2. 지원되는 운영체제 및 웹 브라우저

운영체제	웹 브라우저(JavaScript 사용 가능 및 Java 사용 가능)
<ul style="list-style-type: none"> • Windows 2000(서비스 팩 4 포함)(영어/일본어) • Windows XP(영어/일본어) 	<ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0(Java 플러그인 v1.4.2 또는 1.5.0) • Firefox 1.5(Java 플러그인 v1.4.2 또는 1.5.0) • Netscape Communicator 7.2(Java 플러그인 v1.4.2 또는 1.5.0)
<ul style="list-style-type: none"> • Sun Solaris 2.8 이상(CDE 실행) 	<ul style="list-style-type: none"> • Mozilla 1.7.3(Java 플러그인 v1.4.2 또는 1.5.0)
<ul style="list-style-type: none"> • Red Hat Linux 9.0(GNOME 또는 KDE 실행) • Red Hat Enterprise Linux WS Version 3 	<ul style="list-style-type: none"> • Firefox 1.5(Java 플러그인 v1.4.2 또는 1.5.0)

참고: Cisco ASDM 버전 5.2 는 Windows 95, Windows 98, Windows ME, Windows NT 또는 Sun Solaris OpenWindows 를 지원하지 않습니다.

네트워크 연결

연결 속도: 56Kbps(384Kbps 이상 권장)

서비스 및 지원

시스코는 고객의 성공을 촉진하는 다양한 서비스 프로그램을 제공합니다. 이러한 혁신적인 서비스 프로그램은 수준 높은 인력, 프로세스, 톨 및 파트너의 기술력이 어우러진 것으로서 그 결과는 높은 고객 만족도로 나타납니다. 시스코 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며, 새로운 애플리케이션에 대비해 네트워크 인텔리전스와 비즈니스 역량을 높일 수 있도록 도와줍니다. 시스코 서비스에 대한 자세한 내용은 [시스코 기술 지원 서비스](#) 또는 [시스코 어드밴스드 서비스](#)를 참조하십시오.

추가 정보

자세한 내용은 다음 연락처로 문의하십시오.

Cisco ASDM:

<http://www.cisco.com/go/asdm>

Cisco ASA 5500 시리즈 적응형 보안 어플라이언스:

<http://www.cisco.com/go/asa>

Cisco PIX® 보안 어플라이언스

<http://www.cisco.com/go/pix>

Cisco SAFE 청사진:

<http://www.cisco.com/go/safe>