데이터 시트

CISCO 1800, 2800 및 3800 Integrated Services Routers의 보안 기능

이 데이터 시트에서는 Cisco® 1800, 2800 및 3800 Integrated Services Routers의 보안 기능에 대해 설명합니다.

제품 개요

시스코 시스템즈®는 새로운 계열의 Integrated Services Routers를 통해 최고 수준의 라우팅을 재정의하고 있습니다. 이러한 Integrated Services Routers는 동시에 발생하는 데이터, 음성 및 비디오 서비스를 안전하게 전달하도록 최적화되어 있습니다. 20년 간의 주도권과 혁신을 바탕으로 개발된 모듈형 Cisco® 1800, 2800 및 3800 Integrated Services Routers는 중요한 비즈니스 애플리케이션을 빠르고 정확하게 제공하기 위해 업계에서 가장 다양한 종류의 보안 서비스를 제공함으로써 복원성이 뛰어난 단일 시스템에 데이터와 보안을 인텔리전트하게 포함시킵니다. Cisco 1800, 2800 및 3800 Integrated Services Routers는 소규모 비즈니스와 엔터프라이즈 지사에 가장 적합하며 원격 오피스, 모바일 사용자 및 파트너 엑스트라넷이나 서비스 제공업체에서 관리하는 CPE(Customer Premises Equipment)를 연결할 수 있는 다양한 기능의 통합 솔루션을 제공합니다.

Cisco Self-Defending Network의 핵심 구성 요소인 시스코 Integrated Services Routers를 통해 고객이 라우팅 및 보안 정책을 동기화하고 운영 비용을 절감하는 동시에 네트워크 전체 보안 수준을 향상시킬 수 있습니다. 시스코는 Cisco IOS® 소프트웨어 기반 VPN, 방화벽 및 IPS와 함께 고급 VPN 가속, 침입 감지 시스템(IDS) 및 컨텐트 엔진 네트워크 모듈(Cisco 2800 및 3800 Series)을 통해 업계에서 가장 강력하고 적응성이 뛰어난 보안 솔루션을 지사 라우터에 제공합니다.

통합 보안 솔루션은 세계적 수준의 보안 기능과 입증된 Cisco IOS 기능 및 업계 최고의 LAN/WAN 연결을 결합함으로써 고객에게 다음과 같은 혜택을 제공합니다.

- "기존의 인프라 활용"-기존의 네트워크 인프라를 활용함으로써 추가적인 하드웨어를 배치하지 않고도 Cisco IOS를 통해 라우터 상에 새로운 보안 기능을 구현할 수 있습니다.
- "가장 필요한 곳에 보안 구축"-보안의 이점을 극대화하기 위해 네트워크의 어느 위치에든 방화벽, IPS 및 VPN과 같은 보안 기능을 유연하게 적용할 수 있습니다.
- "게이트웨이 보호"-네트워크의 모든 엔트리 포인트에 최고 수준의 보안 기능을 배치할 수 있습니다.
- "시간과 비용 절감"-장치 수를 줄임으로써 교육 및 관리 비용을 절감합니다.
- "인프라 보호"-DDoS 공격과 같이 네트워크 인프라를 직접 대상으로 하는 공격을 차단함으로써 라우터를 보호합니다.

Cisco Self-Defending Network (자가 방어 네트워크)

Cisco 1800, 2800 및 3800 라우터는 Cisco Self-Defending Network의 한 부분으로써 광범위한 종류의 보안 기능을 지원하며,보안의 위협을 식별 및 차단하고 이 위협에 적응할 수 있도록 도와주는 전략입니다. Cisco Self-Defending Network에는 라우터에 적용되는 다음과 같은 네 종류의 보안 범주가 있습니다.

- 보안 연결-확장이 가능한 안전한 네트워크 연결을 제공함으로써 여러 종류의 트래픽을 통합합니다. 예로는 VPN, DMVPN(Dynamic Multipoint VPN), Multi-VRF/MPLS Secure Contexts, V3PN(Voice and Video Enabled VPN) 및 보안 음성이 있습니다.
- 위협 차단-네트워크 서비스를 사용하여 네트워크 공격 및 위협을 차단하고 이에 대응합니다. 예로는 시스코 침입 차단 시스템(IPS) 및 Cisco IOS Firewall이 있습니다.
- 신뢰성 및 신원 확인-NAC(Network Admission Control), 신원 확인(Identity) 서비스 및 AAA 서비스와 같은 기술을 네트워크에 사용하여 엔드포인트를 인텔리전트하게 보호하도록 합니다.
- 네트워크 인프라 보호-공격과 취약성으로부터 네트워크 인프라를 보호합니다(특히 네트워크 수준에서 보호). 예로는 CPP(Control-Plane Policing), NBAR(Network-Based Application Recognition) 및 AutoSecure가 있습니다.

Integrated Services Routers의 기능

Cisco 1800, 2800 및 3800 Series에서 보안 기능을 사용하기 위해 다음과 같은 Cisco IOS Software 기능 세트를 사용할 수 있습니다.

- 고급 엔터프라이즈 서비스
- 고급 IP 서비스
- 고급 보안

적절한 기능 세트를 선택하는 방법에 대한 자세한 내용은
http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletin09186a00801af451.html을 방문하십시오.

보안 연결: VPN 터널링/암호화, DMVPN, EASY VPN, V3PN 및 Multi-VRF Secure Contexts

VPN 터널링 및 암호화

VPN은 가장 빠르게 성장하고 있는 네트워크 연결의 한 종류입니다. 시스코는 VPN 하드웨어를 Integrated Services Routers에 포함시킴으로써 VPN을 새로운 표준으로 만들고 있습니다. Cisco 1800, 2800 및 3800 라우터에는 기본 제공되는 하드웨어 기반의 암호화 가속이 포함되어 있으며 이를 통해 IPSec(AES, 3DES 및 DES) 암호화 및 VPN 프로세스의 부하를 분산시킴으로써 라우터 CPU에 최소한의 영향을 미치면서 VPN 전송량을 늘릴 수 있습니다. VPN 전송량이나 확장성이 추가로 필요한 경우 VPN 암호화 AIM(Advanced Integration Modules)을 옵션으로 사용할 수 있습니다. 그 결과 전반적인 라우터 CPU의 사용량은 줄어들면서 VPN 성능은 이전의 모델보다 최고 4배나 더 빨라집니다. 옵션인 AIM은 이전의 모델보다 최고 10배나 빠른 터널 확장성이나 암호화 성능을 제공합니다. 기본 제공되는 암호화 가속과 AIM 기반 VPN 가속의 핵심 기능은 다음과 같습니다.

- 여러 개의 전이중 T3/E3에 적합한 속도로 IPSec를 가속화합니다.
- 모든 모듈(기본 제공 및 AIM)에 대해 하드웨어 DES, 3DES 및 AES(128, 192 및 256) 암호화 알고리즘을 가속화합니다.
- 인증을 위해 RSA(Rivest, Shamir, Aldeman) 알고리즘 서명과 Diffie-Hellman을 지원합니다.
- 데이터의 무결성을 위해 SHA-1(Secure Hash Algorithm 1) 또는 MD5(Message Digest Algorithm 5) 해싱 알고리즘을 사용합니다.
- VPN 암호화 모듈을 추가할 때 하드웨어에서 레이어 3(IPPCP) 압축을 지원합니다.

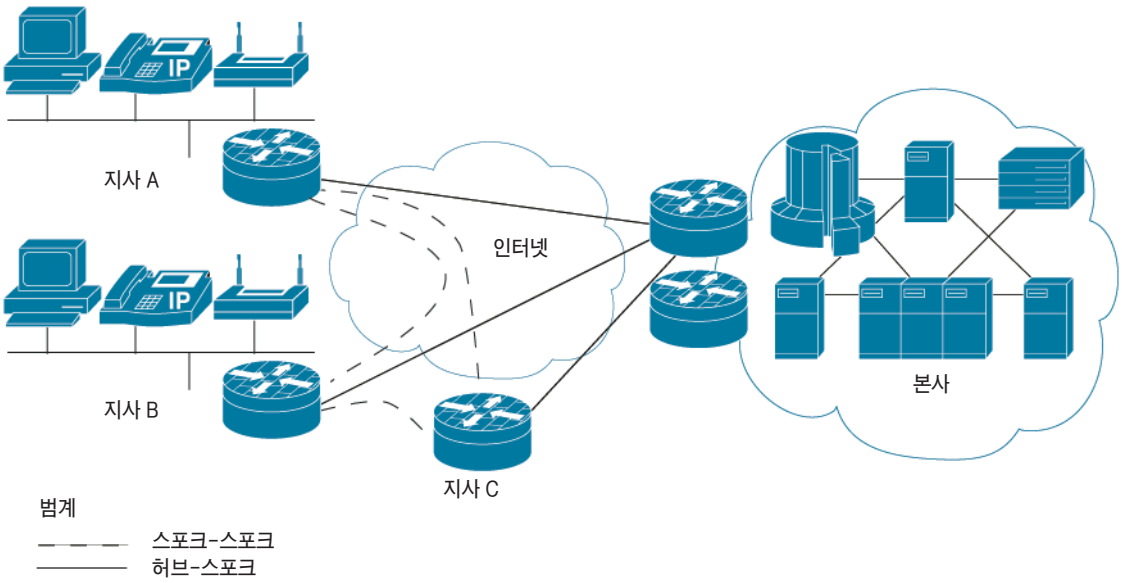
Integrated Services Routers에서는 또한 일반적인 IPSec 이외에도 IPSec 및 GRE(Generic Routing Encapsulation) 프로토콜을 결합한 대체 터널링 기술을 사용할 수도 있습니다. GRE 터널링 기술을 사용하는 IPSec는 시스코 고유의 솔루션이며 이 솔루션을 사용하여 VPN을 통해 동적 라우팅 프로토콜을 전송할 수 있으므로 IPSec 전용 솔루션에 비해 네트워크의 유연성이 더 향상됩니다.

GRE 터널은 결함에 견딜 수 있는 장애 복구 메커니즘을 제공할 뿐만 아니라 멀티캐스트 및 브로드캐스트 패킷과 비 IP 프로토콜을 암호화하는 기능도 제공합니다. 시스코 Integrated Services Routers는 IPSec와 함께 GRE를 사용함으로써 AppleTalk 및 Novell IPX(Internetwork Packet Exchange)와 같은 프로토콜뿐만 아니라, 비디오와 같은 멀티캐스트 및 브로드캐스트 애플리케이션을 지원할 수 있습니다.

DMVPN(Dynamic Multipoint VPN)

시스코는 DMVPN 기능을 제공하는 라우터를 최초로 제공함으로써 업계를 선도하고 있습니다. Cisco DMVPN은 필요 시에 확장이 가능한 풀 메시 VPN을 가능케 함으로써 지연 시간을 줄이고 대역폭을 보존하며 VPN 배치를 단순화할 수 있습니다(그림 1 참조). DMVPN 기능은 GRE 터널, IPSec 암호화, NHRP(Next Hop Resolution Protocol), OSPF 및 EIGRP를 동적으로 구성할 수 있도록 해주는 Cisco IPSec 및 라우팅 전문 기술에 바탕을 두고 있습니다. 이와 같이 QoS 및 멀티캐스트와 같은 기술을 VPN 터널과 결합하여 동적으로 구성함으로써 음성 및 비디오와 같은 시간 지연에 민감한 애플리케이션을 최적화할 수 있습니다. 또한, DMVPN을 사용하면 새로운 스포크를 추가하거나 스포크-스포크 연결을 구성할 때 허브에서 구성이 필요 없으므로 관리상의 부담이 줄어듭니다.

그림 1
DMVPN의 예



Easy VPN

Easy VPN은 최소한의 노력과 뛰어난 확장성으로 허브-스포크 VPN 토폴로지를 지원하도록 설계된 IPSec 솔루션입니다. Easy VPN은 PIX 방화벽 및 VPN 3000과 모든 규모의 라우터 사이에서 VPN 솔루션의 준비와 관리를 단순화해 줍니다. 수많은 고객 설치를 통해 입증된 Easy VPN은 "정책 푸시(policy-push)" 기술을 사용하여 구성을 단순화함과 동시에 기능의 다양성을 유지하고 정책을 제어합니다.

Easy VPN은 다음과 같은 혜택을 제공합니다.

- Easy VPN은 동일한 중앙 사이트 라우터를 사용하여 하드웨어 액세스 라우터 CPE와 소프트웨어 원격 액세스 클라이언트를 모두 지원합니다. 추가 비용 없이 라우터 기반의 VPN에 원격 액세스 연결을 추가하기 위해 Cisco VPN 소프트웨어 클라이언트를 PC, Mac 및 UNIX 시스템에 추가할 수 있습니다. 하드웨어 CPE와 소프트웨어 클라이언트에 하나의 단일 기술(Easy VPN)을 사용하여 준비 및 모니터링 작업과 AAA 서비스를 단순화하고 통합함으로써 총소유 비용을 절감합니다.
- Easy VPN은 라우터 기반의 로컬 RADIUS와 중앙 방식의 RADIUS 그리고 CPE 라우터와 개별 사용자에 대한 AAA 인증 옵션을 제공합니다. 또한 802.1x 인증을 사용하여 각 CPE 위치에서 호스트를 인증할 수 있습니다.
- Easy VPN은 디지털 인증서를 제공하므로 공유 키 인증을 통해 보안이 향상됩니다.

- 여러 개의 중앙 사이트 Easy VPN 집중 장치에 대해 부하 균형 조정을 사용함으로써 부하를 여러 Easy VPN 서버에 자동으로 분산시킵니다. 정책 푸시 기술을 사용하여 백업 집중 장치 정보를 CPE에 푸시(push)함으로써 CPE를 재구성하지 않고도 솔루션을 확장할 수 있습니다.
- 가상화된 Easy VPN 서버를 통해 서비스 제공업체가 여러 고객용 VPN 서비스를 단일 플랫폼으로 제공할 수 있습니다.
- Easy VPN은 성능 모니터링을 위해 동적 QoS 정책 할당, 방화벽, IPS, 분할 터널링, SAA(Service Assurance Agent) 및 NetFlow를 비롯한 완벽한 기능의 통합을 제공합니다.
- Cisco SDM(Security Device Manager)을 사용하여 마법사를 통해 신속하게 Easy VPN을 배치할 수 있습니다. 이 배치에는 AAA와 방화벽이 통합되며 원격 Easy VPN 클라이언트를 실시간 그래픽으로 모니터링합니다. Easy VPN 서버 관리자는 원격 클라이언트를 로그오프시키는 권한이 있습니다.
- Easy VPN은 Cisco IOS Software, Cisco PIX® 방화벽 및 Cisco VPN 3000 Series 집중 장치와 같은 모든 Cisco VPN 서비스 제품군에서 지원됩니다.

V3PN(Voice and Video Enabled VPN)

Cisco 1800, 2800 및 3800에서는 V3PN을 지원합니다. V3PN은 QoS 기반의 안전한 IPSec 네트워크 상에서 데이터, 음성 및 비디오를 통합할 수 있는 VPN 인프라를 제공합니다. 또한, V3PN을 통해 고객은 대체 WAN 연결의 경우와 동일한 음성 및 비디오 애플리케이션 성능을 IP 전송의 경우에도 안전하게 효과적으로 얻을 수 있습니다. 시장에 출시되어 있는 여러 VPN 장치와 달리 시스코 Integrated Services Routers는 멀티서비스 IPSec VPN을 가능케 하는 다양한 종류의 네트워크 토폴로지 및 트래픽 요구사항을 충족시킵니다. V3PN의 완벽한 네트워크 아키텍처는 시스코 보안을 지원하는 라우터와 Cisco IOS Software를 함께 사용하여 음성 트래픽을 보호합니다.

IPSec VPN을 통해 높은 품질의 음성 및 비디오를 전송하기 위해서는 단순히 트래픽을 암호화할 뿐만 아니라, 여러 종류의 고급 멀티서비스 및 IPSec VPN 기술이 필요합니다. Cisco V3PN을 가능케 하는 기본적인 Cisco IOS Software 기술로는 멀티서비스 중심의 QoS, 다양한 종류의 트래픽 지원, 멀티서비스 네트워크 토폴로지 지원 및 고급 네트워크 장애 복구 기능이 있습니다.

서비스 제공업체를 위한 Multi-VRF 및 MPLS Secure Contexts

VRF-Lite라고도 불리는 Multi-VRF는 동일한 물리적 라우터에 있는 라우팅 및 전송 테이블에서 둘 이상의 인스턴스를 구성하고 관리할 수 있는 기능을 제공합니다. 이더넷 VLAN 기술 및 WAN VPN 기술(예: 프레임 릴레이)과 함께 Multi-VRF를 사용하면 하나의 물리적 네트워크를 사용하는 여러 대의 논리 서버의 프로비저닝이 가능하기 때문에 프라이버시와 보안을 지사 LAN으로 확장할 수 있습니다.

Multi-VRF를 사용하는 한 대의 시스코 라우터를 통해 중복 IP 주소를 가지는 여러 조직을 지원할 수 있으며 데이터 구분, 라우팅 및 물리적 인터페이스를 관리할 수 있습니다. Multi-VRF에 대한 자세한 정보는 Product Bulletin을 방문하십시오.

위협 차단: Cisco IOS Firewall, 투명한 방화벽, 침입 차단, URL 필터링 및 컨텐트 보안

Cisco IOS Firewall

Cisco IOS Firewall은 시스코 라우터에 사용할 수 있는 상태보존형 검사 방화벽 옵션입니다. Cisco IOS Firewall은 시장을 선도하는 PIX 방화벽 기술을 사용합니다. Cisco IOS Firewall은 Cisco IOS Software 고급 보안 이상의 기능 세트가 있는 모든 Integrated Services Routers에서 지원됩니다. Cisco IOS Firewall은 네트워크에 연결되는 WAN 엔트리 포인트를 보호하는 데 가장 적합한 단일 보안 및 라우팅 솔루션입니다. 허브는 공격에 사용되는 트래픽을 차단하고 검사하는 일반적인 위치이지만, 이 위치에만 보안을 배치하도록 고려해서는 안됩니다. 지사도 또한 공격에 사용되는 트래픽을 차단하고 검사해야 하는 중요한 네트워크 위치입니다.

Cisco IOS Firewall의 핵심 기능은 다음과 같습니다.

- 서비스 거부(Denial of Service) 공격 차단을 비롯한 상태보존형 방화벽
- 애플리케이션을 식별, 검사 및 제어하기 위한 향상된 애플리케이션, 트래픽 및 사용자 식별
- 음성, 비디오 및 기타 애플리케이션을 위한 고급 프로토콜 검사
- 사용자, 인터페이스 또는 하위 인터페이스 별 보안 정책

- 사용자 별 인증 및 권한 부여를 제공하기 위해 긴밀하게 통합된 신원 확인(Identity) 서비스
- 역할 기반 액세스/CLI 뷰와 같은 기능을 통해 관리 용이(Cisco SDM에서 NetOps, SecOps, 최종 사용자 및 방화벽 정책 뷰 사이에 라우터의 안전하고 논리적인 구분이 가능하도록 허용)

Cisco IOS Firewall을 통해 단일 위치에서 네트워크를 보호할 수 있을 뿐만 아니라, 네트워크에서 보안 정책을 시행할 수 있습니다. 통합된 전용 보안 정책을 유연한 방식과 저렴한 비용으로 시행함으로써 지사나 원격 사무소의 엑스트라넷 및 인트라넷과 인터넷 연결에 맞는 보안 솔루션을 신속하게 구현할 수 있습니다. Cisco IOS Software를 통해 네트워크에 통합된 Cisco IOS Firewall을 통해 고객은 또한 동일한 라우터에 있는 고급 서비스 품질(QoS) 기능을 사용할 수 있습니다.

Cisco IOS는 IPv4 및 IPv6 혼합 환경에서의 배치를 가능케 하는 IPv6 방화벽을 지원합니다. Cisco IOS Firewall IPv6는 IPv6 패킷에 대한 상태 프로토콜 검사 기능과 IPv6 서비스 거부 공격(DoS) 완화 기능을 제공합니다.

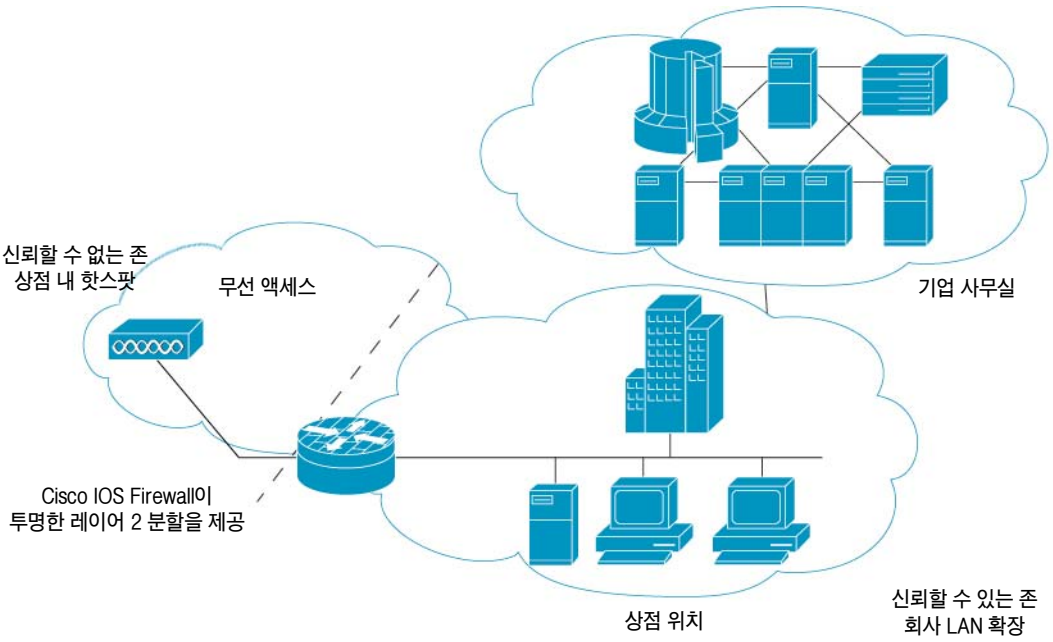
투명한 방화벽

Cisco 1800, 2800 및 3800은 레이어 3 상태 방화벽뿐만 아니라 투명한(transparent) 방화벽도 지원할 수 있습니다. 투명한 방화벽이란 레이어 2 연결을 위해 레이어 3 방화벽을 제공하는 것을 말합니다. 투명한 방화벽의 이점은 다음과 같습니다.

- 기존의 네트워크에 방화벽을 쉽게 추가할 수 있으며 IP 서브넷 번호 변경이 필요 없음
- 하위 인터페이스와 VLAN 트렁크를 지원
- 확장 트리 프로토콜 지원–802.1d 별로 BPDU(Bridge Protocol Data Unit) 패킷을 올바르게 처리하며 단순히 "통과 또는 폐기"로 처리하는 것이 아님
- 동일한 라우터에서 레이어 2 및 레이어 3 방화벽을 혼합할 수 있도록 지원
- 인터페이스의 IP 주소가 필요 없음
- 모든 표준 관리 툴을 지원
- 반대쪽 인터페이스에 DHCP(Dynamic Host Configuration Protocol) 주소를 할당할 수 있도록 DHCP 패스쓰루를 지원(양방향 지원)

그림 2는 투명한 방화벽의 애플리케이션을 나타냅니다.

그림 2
주소를 변경하지 않고도 기존의 네트워크 배치를 보안 신뢰 존으로 분할



침입 차단 시스템(IPS)

시스코는 IPS 기능을 제공하는 라우터를 최초로 제공함으로써 업계를 선도하고 있습니다. Cisco IOS IPS는 Cisco IOS Software를 통해 네트워크 공격을 완화할 수 있도록 도와주는 검사 기반의 직렬식 솔루션입니다. 침입 차단 및 이벤트 알림에 사용되는 Cisco IOS IPS는 Cisco IDS 4200 Series Appliances, Catalyst 6500 IDS 서비스 모듈 및 네트워크 모듈 하드웨어 IDS 장비를 비롯한 Cisco IDS Sensor 제품군의 기술을 활용합니다. Cisco IOS Software IPS는 직렬식이기 때문에 트래픽을 폐기하거나 경보를 보내거나 연결을 재설정할 수 있으며, 이를 통해 보안의 위협에 신속하게 대처하여 네트워크를 보호할 수 있습니다.

허브는 공격에 사용되는 트래픽을 차단하고 검사하는 일반적인 위치이지만, 이 위치에만 보안을 배치하도록 고려해서는 안됩니다. 공격은 지사에서도 발생할 수 있습니다. IPSec VPN, GRE 및 Cisco IOS Firewall과 함께 Cisco IOS IPS를 사용하여 첫 번째 네트워크 엔트리 포인트(지사 또는 허브)에서 암호 해독, 터널 종료, 방화벽 및 트래픽 검사를 수행할 수 있으며 이는 업계 최초입니다. Cisco IOS IPS는 공격에 사용되는 트래픽을 최대한 신속하게 차단해 줍니다.

Cisco 1800, 2800 및 3800 라우터의 릴리스에는 다음과 같은 새로운 기능이 제공됩니다.

- Cisco IDS Sensor Appliances와 동일한 방식으로 해당 IDS 서명을 가져와서 사용하는 기능
- Cisco IDS Sensor 플랫폼에서 지원하는 700개 이상의 서명에 더하여 서명을 추가로 지원
- 사용자가 기존의 서명을 수정하거나 새 서명을 만들어 새로 발견된 위협을 해결하는 기능(경보를 보내거나 패킷을 폐기하거나 연결을 재설정하도록 각 서명을 설정할 수 있음)

최대한의 침입 차단을 원하는 사용자는 추가 기능을 통해 사용이 쉬운 서명 파일을 선택할 수 있습니다. 이 서명 파일에는 "가장 가능성이 높은" 웜 및 공격의 서명이 포함되어 있습니다. 이러한 가능성이 높은 웜 및 공격의 서명과 일치하는 트래픽은 폐기되도록 구성됩니다. Cisco SDM에서는 이러한 서명을 쉽게 제공할 수 있는 직관적인 사용자 인터페이스를 공급하며 이러한 서명에 맞게 라우터를 적절히 구성합니다. 여기에는 소프트웨어 이미지를 변경하지 않고도 Cisco.com에서 새 서명을 업로드하는 기능도 포함됩니다.

URL 필터링(Off-box/On-box 옵션)

시스코에는 Cisco IOS Firewall을 지원하는 URL 필터링이 있으며, 이를 통해 고객이 시스코 보안 라우터와 함께 Websense 또는 N2H2 URL 필터링 제품을 사용할 수 있습니다. Websense URL 필터링 기능은 Cisco IOS Firewall이 Websense 또는 N2H2 URL 필터링 소프트웨어와 상호 작용하도록 도와주며 보안 정책에 따라 사용자가 특정 웹 사이트에 액세스하는 것을 차단할 수 있습니다. Cisco IOS Firewall은 Websense 및 N2H2 서버와 함께 사용되어 특정 URL의 허용 또는 거부(차단) 여부를 알아냅니다. 완벽한 On-box URL 필터링 및 컨텐트 보안에 대해서는 Cisco 2800의 URL 필터링용 컨텐트 엔진 네트워크 모듈 기능을 참조하십시오.

고급 보안 네트워크 모듈(Cisco 2800 및 3800 옵션)

IDS 및 컨텐트 보안을 위한 하드웨어 기반의 전용 솔루션을 찾고 있는 고객은 Cisco 2800 및 3800 라우터 용으로 2개의 보안 네트워크 모듈을 사용할 수 있습니다.

침입 감지 네트워크 모듈

Cisco 2800 또는 3800 라우터에 추가된 Cisco IDS 네트워크 모듈(부품 번호 NM-CIDS)은 Cisco IDS Sensor 제품군의 일부분으로 완벽한 IDS 시스템이 되도록 지원합니다. 이와 같은 IDS Sensor 제품은 Cisco IDS 관리 콘솔, CiscoWorks VPN/보안 관리 솔루션(VMS) 및 Cisco IDS 장치 관리자를 비롯한 다른 IDS 구성 요소와 함께 동작하여 데이터 및 정보 인프라를 효율적으로 보호해 줍니다. Cisco IDS 네트워크 모듈에는 IDS 전용 CPU와 지원되는 1000개 이상의 IPS 서명을 기록할 수 있는 20-GB의 하드 드라이브가 있습니다. IPSec VPN 및 GRE 트래픽과 함께 이 모듈을 사용하여 첫 번째 네트워크 엔트리 포인트(지사 또는 허브)에서 암호 해독, 터널 종료 및 트래픽 검사를 수행할 수 있으며 이는 업계 최초입니다. 이렇게 하면 시스템을 지원하는 데 일반적으로 필요한 추가 장치를 사용하지 않아도 되므로 보안은 향상되고 운영 및 자본 지출 비용은 줄어듭니다.

컨텐트 보안 네트워크 모듈

Cisco 2800 또는 3800 라우터와 함께 Cisco Content Engine Network Module(부품 번호 NM-CE)을 사용하여 라우터 통합 컨텐트 제공 시스템에 컨텐트 보안 기능을 제공합니다. Cisco Content Engine Network Module은 인텔리전트 캐싱 및 컨텐트 라우팅 이외에도 URL 필터링을 제공합니다. 각 컨텐트 엔진 네트워크 모듈에는 SecureComputing URL 필터링 소프트웨어가 함께 제공됩니다.

엔드포인트 보호 및 제어: NAC(Network Admission Control), AAA(Authentication, Authorization, Accounting), 802.1X 및 이동 가능한 자격 증명서

NAC(Network Admission Control)

NAC는 바이러스와 웜으로 인한 손실을 줄이기 위해 시스코 시스템즈에서 주도하고 있는 산업 전반의 협력 과정이며, 모든 엔드포인트가 액세스 권한을 부여 받기 위해서는 네트워크 보안 정책을 준수해야 합니다. NAC는 네트워크에 연결된 장치가 네트워크 보안 정책을 준수하는지 확인함으로써 네트워크 액세스를 제어합니다.

NAC는 회사의 최신 바이러스 예방 및 운영 체제 패치 정책에 상응하는 신뢰할 수 있는 엔드포인트 장치만이 네트워크에 액세스하도록 허용함으로써 네트워크에서 취약한 시스템을 식별하고 네트워크 권한 허가를 효과적으로 제어합니다. 정책을 준수하지 않는 취약한 호스트는 패치가 적용되어 안전해질 때까지 격리되며 제한된 네트워크 액세스가 지정되므로, 이러한 호스트가 웜 및 바이러스 감염의 소스나 대상이 되는 것을 막아줍니다.

NAC는 Cisco IOS Software 고급 보안, 고급 IP 서비스 또는 고급 엔터프라이즈 서비스 기능 세트와 함께 Cisco 1800, 2800 및 3800에서 사용될 수 있습니다.

NAC는 다음과 같은 이점을 제공합니다.

- 광범위한 제어 범위-호스트가 네트워크에 연결하는 데는 일반적으로 라우터 WAN 연결, IPSec 원격 액세스 및 전화 접속 연결과 같은 방법이 사용됩니다.
- 멀티 공급업체 솔루션-시스코에서 주도하는 NAC는 Network Associates, Symantec, Trend Micro 등과 같은 여러 선두 바이러스 백신 공급업체의 협력의 결과입니다.
- 기존 기술과 표준을 확대-NAC는 EAP(Extensible Authentication Protocol), 802.1x 및 RADIUS 서비스와 같은 기존 통신 프로토콜 및 보안 기술의 사용을 확대합니다.
- 기존의 네트워크와 바이러스 예방에 투자 확대-NAC는 기존의 네트워크 인프라 투자와 바이러스 예방 기술을 결합하여 권한 허가 제어 시설을 제공합니다.

AAA(Authentication, Authorization, Accounting)

Cisco IOS Software AAA 네트워크 보안 서비스는 라우터나 액세스 서버에 액세스 제어를 구현하기 위한 기본적인 토대를 제공합니다. AAA를 통해 관리자가 회선 별(사용자 별) 또는 서비스 별(IP, IPX 또는 VPDN)로 인증 및 권한 부여 형식을 동적으로 구성할 수 있으며 이를 위해 특정 서비스나 인터페이스에 적용되는 절차 목록을 사용합니다.

802.1x

802.1x 애플리케이션은 보호되는 정보 리소스에 불법으로 액세스하는 것을 막기 위해 유효한 액세스 자격 증명서를 요청합니다. 또한 802.1x 애플리케이션을 배치함으로써 네트워크 관리자는 사용자가 안전하지 않은 무선 액세스 포인트를 배치하지 못하도록 효과적으로 차단할 수 있습니다. 이를 통해 배치가 쉬운 WLAN 장비의 가장 큰 문제점 중 하나를 해결할 수 있습니다.

USB 포트/이동 가능한 자격 증명서

온보드 USB 1.1 포트는 모든 Cisco 1800, 2800 및 3800 라우터에 통합됩니다. 이 포트는 VPN 자격 증명서의 안전한 구성 배포와 플랫폼 외부 저장을 위해 옵션 USB 토큰과 함께 사용할 수 있도록 나중에 구성할 수 있습니다. 네트워크 관리자가 보안 자격 증명에 USB 토큰을 사용하여 라우터와 토큰을 별도로 보냄으로써 안전한 관리를 보장할 수 있습니다.

네트워크 장치 보호(Cisco IOS Software, IP BASE 이상에 포함): CPP(Control-Plane Policing), AutoSecure, NBAR, CPU/메모리 한도 제한, SSHV2, SNMP 및 역할 기반 CLI

CPP(Control Plane Policing)

가장 강력한 소프트웨어 구현과 하드웨어 아키텍처조차도 서비스 거부(DoS) 공격에 취약할 수 있습니다. DoS 공격은 제어 프로세서로 향하는 특정 형식의 제어 패킷으로 위장된 쓸모 없는 트래픽을 네트워크 인프라에 보냄으로써 인프라를 마비시키는 악의적 행위입니다. 네트워크의 중심부로 향하는 이와 유사한 위협을 차단하기 위해 Cisco IOS Software에는 프로그래밍이 가능한 차단 기능이 포함되어 있습니다. 이 차단 기능은 제어 프로세서로 향하는 트래픽의 속도를 제한하거나 "단속"할 수 있습니다. CPP(Control Plane Policing)라고 불리는 이 기능을 사용하여 특정 형식의 트래픽을 식별하여 완전하게 제한하거나 지정된 한도 수준 이상일 때 트래픽을 제한할 수 있습니다.

AutoSecure

Cisco IOS Software의 한 기능인 AutoSecure는 라우터의 보안 구성을 단순화해주고 구성 오류의 위험을 줄여줍니다. 숙련된 사용자에게 적합한 양방향(interactive) 모드에서는 사용자가 보안 설정과 라우터 서비스를 사용자 정의할 수 있으므로 라우터의 보안 기능을 더 정확하게 제어할 수 있습니다. 숙련되지 않은 사용자가 별다른 간섭 없이 신속하게 라우터의 보안을 구성하려면 AutoSecure의 단방향 모드를 사용할 수 있습니다. 이 모드에서는 시스코 시스템즈에서 설정한 기본값에 따라 라우터 보안 기능이 자동으로 설정됩니다. 단일 명령으로 라우터의 보안 상태를 신속하게 구성하고 불필요한 시스템 프로세스와 서비스를 해제함으로써 네트워크의 잠재적인 보안 위협을 줄입니다.

NBAR

Cisco IOS Software에 있는 NBAR은 웹 기반 프로토콜과 기타 분류가 어려운 프로토콜(동적 TCP/UDP 포트 할당을 사용)을 비롯한 다양한 종류의 애플리케이션을 식별하기 위해 상태 패킷 검사를 사용하는 분류(classification) 엔진입니다. 보안 환경에서 NBAR을 사용하여 페이로드 서명에 따라 웜을 찾아낼 수 있습니다. NBAR에서 애플리케이션을 식별하고 분류하면 네트워크에서 이 애플리케이션에 해당하는 서비스를 호출할 수 있습니다. 또한, NBAR은 QoS 기능을 사용하여 네트워크 대역폭이 효율적으로 사용되는지 확인함으로써 보장된 대역폭, 대역폭 한도, 트래픽 구성 및 패킷 분류 기능을 제공합니다. SDM 2.0(아래의 Security Device Manager 참조)에는 NBAR을 손쉽게 설정할 수 있는 마법사가 있으며 또한 애플리케이션 트래픽을 그래픽 뷰로 제공합니다.

CPU/메모리 한도 제한

Cisco IOS Software의 기능을 통해 라우터의 메모리 사용량에 대해 전역 메모리 한도를 설정할 수 있으며 한도에 도달할 경우 알림 기능을 통해 알려줍니다. 이 기능을 통해 CPU와 메모리를 남겨두게 되면 공격으로 인해 높은 부하가 발생하더라도 계속해서 라우터가 동작할 수 있습니다.

Secure Shell 버전 2

Secure Shell 버전 2(SSHv2)는 강력하고 새로운 인증 및 암호화 기능을 제공합니다. 이제 암호화된 연결을 통해 더 많은 종류의 트래픽을 전달하기 위해 더 많은 옵션을 사용할 수 있습니다(예: 파일 복사 및 전자 메일 프로토콜). 디지털 인증서와 더 많은 인증 옵션을 비롯하여 보다 다양해진 인증 기능을 통해 네트워크 보안이 향상됩니다.

SNMPv3(Simple Network Management Protocol Version 3)

SNMPv3는 네트워크 관리에 사용되는 표준 기반 프로토콜이며 상호 운영이 가능합니다. SNMPv3는 네트워크에서 패킷을 인증하고 암호화함으로써 장치에 안전한 액세스를 제공합니다. SNMPv3에서 제공하는 보안 기능은 다음과 같습니다.

- 메시지 무결성–패킷이 전송 중에 변경되지 않았는지 확인합니다.
- 인증–메시지가 올바른 소스에서 도달했는지 확인합니다.
- 암호화–패킷의 내용을 암호화하면 승인되지 않은 소스에서 패킷 내용을 볼 수 없습니다.

SNMPv3는 보안 모델과 보안 수준을 둘 다 고려합니다. 보안 모델은 사용자와 이 사용자가 위치하는 그룹에 대해 수립된 인증 전략입니다. 보안 수준은 보안 모델 내에서 허용된 보안 수준입니다. 보안 모델과 보안 수준은 SNMP 패킷을 처리할 때 사용할 보안 메커니즘을 결정합니다. SNMPv1, SNMPv2c 및 SNMPv3의 세 가지 보안 모델을 사용할 수 있습니다.

역할 기반 CLI 액세스

역할 기반 CLI 액세스 기능을 통해 네트워크 관리자가 "뷰"를 정의할 수 있습니다. 뷰는 Cisco IOS Software에 선택적 또는 부분적 액세스를 제공하는 일련의 연산 명령 및 구성 기능입니다. 뷰는 Cisco IOS CLI(command-line interface)와 구성 정보에 대한 사용자 액세스를 제한하며 어떤 명령이 허용되고 어떤 구성 정보가 표시되는지를 정의할 수 있습니다. 역할 기반 CLI 액세스의 애플리케이션으로는 네트워크 관리자가 특정 기능에 대한 액세스를 보안 직원에게 제공하는 것이 있습니다. 또한 서비스 제공업체가 이 기능을 사용하여 최종 고객에게 제한적인 액세스를 부여함으로써 네트워크의 문제 해결을 지원할 수 있습니다. Cisco SDM에는 관리자, 읽기 전용(최종 사용자용), 방화벽 정책(Firewall Policy) 및 EzVPN 원격을 위한 공장 기본값 뷰가 제공됩니다. 역할 기반의 특정 액세스 권한을 가진 사용자가 Cisco SDM에 로그인하여 자신의 역할에 해당하는 GUI 화면만을 볼 수 있습니다.

포함된 서비스 관리: 시스코 라우터 및 SDM (Security Device Manager)

시스코 라우터 및 SDM(Security Device Manager)

모든 Cisco 1800, 2800 및 3800 시리즈에는 Cisco Router and Security Device Manager (SDM) 가 함께 제공됩니다. Cisco SDM은 시스코 라우터를 배치하고 관리하기 위한 웹 기반 장치 관리자(GUI)입니다. 그림 1을 참조하십시오. Cisco SDM을 통해 시작 마법사를 사용하여 라우터를 쉽게 구성하고 모니터링할 수 있으며 스마트 마법사를 사용하여 보안 및 라우팅 기능, Cisco TAC(Technical Assistance Center) 승인 라우터 구성 그리고 주제에 관련된 교육용 컨텐트를 사용할 수 있습니다.

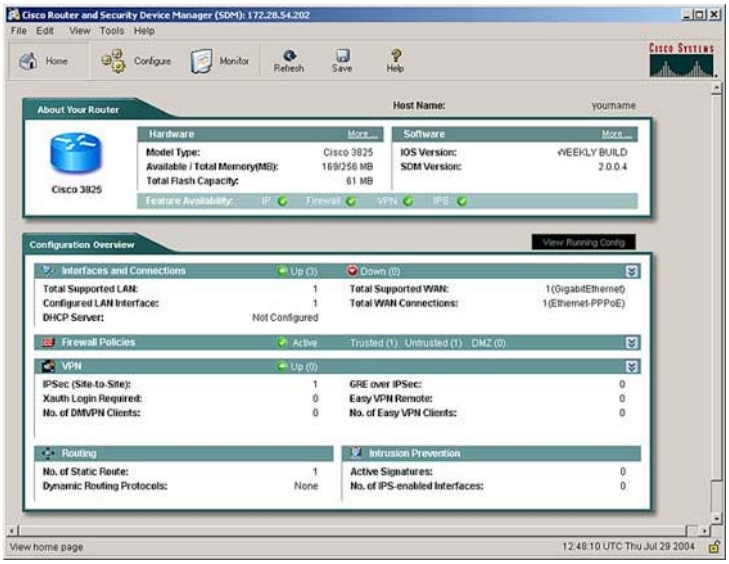
Cisco SDM 2.0에서는 사용이 쉬운 스마트 마법사와 완벽한 문제 해결 기능을 라우팅 및 보안 서비스 관리 기능에 결합함으로써 라우터에 서비스를 통합할 때의 이점을 지원하는 툴을 제공합니다. 이제 고객은 네트워크 전체에서 라우팅 및 보안 정책을 동기화할 수 있으며 라우터 서비스 상태를 광범위하게 볼 수 있고 운영 비용을 절감할 수 있습니다.

Cisco SDM 2.0의 새로운 핵심 기능은 다음과 같습니다.

- 직렬식 IPS – 업데이트가 가능한 서명, 사용자 정의 동적 서명 업데이트 및 서명 사용자 정의(IPS 참조)
- 역할 기반 라우터 액세스
- Easy VPN 서버 및 AAA
- IPSec VPN용 디지털 인증서
- VPN 및 WAN 연결 문제 해결
- QoS 정책 구성 및 NBAR 기반 애플리케이션 트래픽 모니터링

Cisco SDM에 대한 자세한 내용은 http://www.cisco.com/go/sdm을 방문하십시오.

그림 3
시스코 Security Device Manager(SDM)



방화벽 및 VPN 기능을 관리하기 위해 CiscoWorks VPN/보안 관리 솔루션(VMS) 관리 번들을 사용할 수 있습니다. CiscoWorks VMS에 대한 자세한 내용은 http://www.cisco.com/go/vms를 방문하십시오.

표 1은 Cisco 1800, 2800 및 3800의 주요 기능을 나타냅니다.

표 1. Cisco 1800, 2800 및 3800의 하드웨어 기능

기능	Cisco 3800	Cisco 2800	Cisco 1800
기본 제공 VPN 암호화 가속 (IPSec DES, 3DES 및 AES 128, 192 및 256)	모든 모델에 기본으로 제공됩니다. 또한 Cisco IOS Software 고급 보안 이상의 기능 세트를 사용해야 합니다.	모든 모델에 기본으로 제공됩니다. 또한 Cisco IOS Software 고급 보안 이상의 기능 세트를 사용해야 합니다.	모든 모델에 기본으로 제공됩니다. 또한 Cisco IOS Software 고급 보안 이상의 기능 세트를 사용해야 합니다.
고급 VPN 암호화 가속 IPPCP를 사용하는 하드웨어 지원 압축	추가적인 성능 및 터널 확장성을 위한 옵션 성능 향상 부품 번호 Cisco 3825: AIM-VPN/EPII-PLUS Cisco 3845: AIM-VPN/HPII-PLUS	추가적인 성능 및 터널 확장성을 위한 옵션 성능 향상 (부품 번호 AIM-VPN/EPII-PLUS)	추가적인 성능 및 터널 확장성을 위한 옵션 성능 향상 (부품 번호 AIM-VPN/BPII-PLUS)
IDS 네트워크 모듈*	옵션 성능 향상 (부품 번호 NM-CIDS)	옵션 성능 향상 (부품 번호 NM-CIDS*)	없음
컨텐트 보안을 위한 컨텐트 엔진 네트워크 모듈*	Cisco Content Engine Network Module을 통한 옵션 성능 향상 (부품 번호 CE-NM)	Cisco Content Engine Network Module을 통한 옵션 성능 향상 (부품 번호 CE-NM*)	없음

* Cisco 2801에서는 지원되지 않습니다.

표 2는 Cisco 1800, 2800 및 3800의 기능과 혜택을 나타냅니다.

표 2. Cisco 1800, 2800 및 3800의 주요 기능 및 혜택

기능	혜택
보안 연결	
모든 Integrated Services Routers 상에서 기본 제공 VPN 암호화 가속	• 이 기능은 AIM 슬롯을 사용하지 않고도 IPSec DES, 3DES 및 AES 128, 192 및 256 암호화를 지원합니다.
AIM 기반 보안 가속	• 옵션 전용 보안 AIM이 레이어 3 IPPCP 압축과 함께 추가적인 성능과 확장성을 제공할 수 있도록 지원합니다.
MPLS(Multiprotocol Label Switching) VPN 지원	• 지사에 맞게 최적화된 CE(Customer Edge) 기능과 Multi-VRF 식별 방화벽 및 IPSec를 통해 고객 MPLS-VPN 네트워크를 CE로 확장하는 메커니즘
Multi-VRF 및 MPLS Secure Contexts	• 부서, 자회사 또는 고객을 구분하기 위해 지사 위치에서 여러 개의 독립 컨텍스트(주소, 라우팅 및 인터페이스)를 지원합니다. 모든 컨텍스트는 코어에 연결되는 단일 업링크 연결(IPSec VPN 또는 프레임 릴레이/ATM)을 공유할 수 있으며 이들 간에 안전한 구분을 유지할 수 있습니다.
Cisco Easy VPN 원격 및 서버 지원	• 이 기능을 통해 새로운 보안 정책을 단일 헤드 엔드에서 원격 사이트에 적용함으로써 일-대-일 VPN을 쉽게 관리하고 운영할 수 있습니다.
V3PN	• VPN을 통해 효율적인 비용으로 통합 음성, 비디오 및 데이터를 모든 위치에 제공합니다.
DMVPN	• 지점 간에 가상 풀 메시 IPSec 터널을 구성할 수 있는 유연한 방법을 제공합니다. 새로운 스포크를 추가할 때 허브에서 구성이 필요 없습니다.
위협 차단	
Cisco IOS Firewall	• 네트워크에 연결되는 WAN 엔트리 포인트를 보호하는 데 가장 적합한 보안 및 라우팅 솔루션입니다. 이제 IPv6 지원이 함께 제공됩니다.
투명한 방화벽	• 주소를 변경하지 않고도 기존의 네트워크 배치를 보안 신뢰 존으로 분할합니다. 하위 인터페이스 및 VLAN 트렁크를 지원합니다. 투명한 방화벽과 레이어 3 방화벽을 동시에 지원합니다.
침입 차단	• Cisco IOS Software를 통해 네트워크 공격을 완화할 수 있도록 도와주는 검사 기반의 직렬식 솔루션입니다. IPS는 직렬식이기 때문에 트래픽을 폐기하거나 경보를 보내거나 연결을 재설정할 수 있으며 이를 통해 보안의 위협에 신속하게 대처하여 네트워크를 보호할 수 있습니다.
URL 필터링(Off-box)	• Cisco IOS Firewall이 Websense 또는 N2H2 URL 필터링 소프트웨어와 상호 작용하도록 도와주며 보안 정책에 따라 사용자가 특정 웹 사이트에 액세스하는 것을 차단할 수 있습니다.
엔드포인트 보호 및 제어	
NAC(Network Admission Control)	• 설정된 액세스 및 보안 정책과 일치하는 신뢰할 수 있는 장치에만 액세스를 허용함으로써 네트워크에서 바이러스와 웜의 확산을 차단합니다.
AAA	• AAA를 통해 관리자가 회선 별(사용자 별) 또는 서비스 별(IP, IPX 또는 VPDN)로 인증 및 권한 부여 형식을 동적으로 구성할 수 있습니다.
통합 스위치 상에서 표준 802.1x 지원	• 표준 802.1x 애플리케이션은 보호되는 정보 리소스에 불법으로 액세스하는 것을 막고 안전하지 않은 무선 액세스 포인트를 쉽게 배치하지 못하도록 유효한 액세스를 요청합니다.
이동 가능한 자격 증명서	• 이동이 가능한 VPN 자격 증명서(VPN 키)를 사용하여 VPN 인증서와 라우터 구성을 미리 준비할 수 있습니다.
온보드 USB 1.1 포트	• 이 포트는 VPN 자격 증명서의 안전한 구성 배포와 플랫폼 외부 저장을 위해 옵션 USB 토큰과 함께 사용할 수 있도록 나중에 구성할 수 있습니다.

표 2. Cisco 1800, 2800 및 3800의 주요 기능 및 혜택(계속)

기능	혜택
네트워크 장치 보호	
CPP(Control Plane Policing)	• 제어 프로세서로 들어오는 트래픽의 속도를 제한함으로써 DoS 공격의 성공 가능성을 줄이고, 이를 통해 공격 중에도 네트워크를 사용할 수 있도록 합니다.
AutoSecure	• 라우터의 보안 구성을 단순화해 주고 구성 오류의 위험을 줄여줍니다.
NBAR	• Cisco IOS Software의 이 분류 엔진은 다양한 종류의 애플리케이션을 식별할 수 있습니다. 애플리케이션이 식별되면 네트워크에서 이 애플리케이션에 해당하는 특정 서비스를 호출할 수 있으므로 적절한 수준의 제어를 제공할 수 있습니다.
CPU/메모리 한도 제한	• 이 기능을 통해 CPU와 메모리를 남겨두게 되면 공격으로 인해 높은 부하가 발생하더라도 계속해서 라우터가 동작할 수 있습니다.
역할 기반 CLI 액세스	• CLI 명령에 뷰 기반의 액세스를 제공하므로 NetOps, SecOps 및 최종 사용자 사이에 라우터의 안전하고 논리적인 구분이 가능합니다.
관리	
시스코 라우터 및 SDM (Security Device Manager)를 통한 보안 관리	• Cisco IOS Software 액세스 라우터 내에 포함된 사용이 쉽고 직관적인 웹 기반 장치 관리 툴에 HTTPS 및 SSH(Secure Shell) 프로토콜을 사용하여 원격으로 액세스할 수 있습니다.
엔터프라이즈 보안 관리	• 엔터프라이즈 보안 배치를 위해 다음과 같은 두 가지 툴을 사용할 수 있습니다. – CiscoWorks VMS는 중간 규모 및 대규모 VPN 배치에 사용되는 광범위한 관리 툴이며 IPSec 터널과 방화벽 규칙을 구성할 수 있습니다. – Cisco ISC(IP Solution Center) 3.0은 서비스 제공업체 MPLS IPSec 관리 툴입니다.

인증

시스코는 전세계 고객에게 적극적인 제품 인증 및 평가 프로그램을 제공하기 위해 노력하고 있습니다. Cisco IOS VPN은 FIPS 140-2, ICSA 및 Common Criteria EAL4+ 인증을 달성했으며 Cisco IOS Firewall 인증은 거의 완료 단계에 있습니다. 시스코는 이와 같은 인증이 통합 보안 전략의 중요한 요소라는 것을 인식하고 FIPS, ICSA 및 Common Criteria 인증을 지속적으로 추구하기 위해 노력하고 있습니다.

FIPS

Cisco 1800, 2800 및 3800은 FIPS 140-1 Level 2 보안을 충족시키도록 설계되었습니다. NIST는 FIPS 140-1을 FIPS 140-2로 업그레이드했습니다. 이제 시스코는 수많은 자체 라우터를 FIPS 140-2, Level 2에 맞출 예정입니다.

ICSA

ICSA는 다양한 종류의 보안 제품에 대해 ICSA IPSec 및 ICSA 방화벽 인증을 제공하는 보안 인증 영리 기관입니다. 시스코는 ICSA의 IPSec 프로그램과 방화벽 프로그램에 참여하고 있습니다.

Common Criteria

Common Criteria는 IT 보안을 평가하기 위한 국제적인 표준입니다. 이 표준은 국가별로 존재하는 기존의 수많은 보안 평가 프로세스를 국제적인 단일 표준으로 대체하기 위해 여러 국가에 의해 컨소시엄의 형태로 개발되었습니다. 현재 14개국에서 Common Criteria를 공식적으로 인정하고 있습니다. 현재 여러 버전의 Cisco IOS Software IPSec 및 시스코 라우터가 AISEP(Australasian Information Security Evaluation Program) 하에서 ITSEC 또는 Common Criteria 표준에 대해 평가되고 있습니다.

주문 정보

주문을 하려면 시스코 주문(Cisco Ordering) 홈 페이지를 방문하십시오. 표 3에서는 Cisco 1800, Cisco 2800 및 Cisco 3800의 주문 정보를 제공합니다.

표 3. Cisco 1800, Cisco 2800 및 Cisco 3800의 주문 정보

제품 이름	부품 번호
Cisco 1841 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO1841-SEC/K9
Cisco 2801 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO2801-SEC/K9
Cisco 2811 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO2811-SEC/K9
Cisco 2821 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO2821-SEC/K9
Cisco 2851 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO2851-SEC/K9
Cisco 3825 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO3825-SEC/K9
Cisco 3845 보안 번들(고급 보안 Cisco IOS Software 포함)	CISCO3845-SEC/K9
Cisco 1841 고급 보안 번들(AIM-VPN BPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO1841-HSEC/K9
Cisco 2801 고급 보안 번들(AIM-VPN BPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO2801-HSEC/K9
Cisco 2811 고급 보안 번들(AIM-VPN BPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO2811-HSEC/K9
Cisco 2821 고급 보안 번들(AIM-VPN EPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO2821-HSEC/K9
Cisco 2851 고급 보안 번들(AIM-VPN EPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO2851-HSEC/K9
Cisco 3825 고급 보안 번들(AIM-VPN EPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO3825-HSEC/K9
Cisco 3845 고급 보안 번들(AIM-VPN HPII-PLUS, 고급 IP Cisco IOS Software 포함)	CISCO3845-HSEC/K9
Cisco 2801 V3PN 번들(AIM-VPN EPII-PLUS, PVDM2-8, 고급 IP Cisco IOS Software, 64M 플래시, 256DRAM 포함)	CISCO2801-V3PN/K9
Cisco 2811 V3PN 번들(AIM-VPN EPII-PLUS, PVDM2-16, 고급 IP Cisco IOS Software, FL-SRST-36, 64M 플래시, 256DRAM 포함)	CISCO2811-V3PN/K9
Cisco 2821 V3PN 번들(AIM-VPN EPII-PLUS, PVDM2-32, 고급 IP Cisco IOS Software, FL-SRST-48, 64M 플래시, 256DRAM 포함)	CISCO2821-V3PN/K9
Cisco 2851 V3PN 번들(AIM-VPN EPII-PLUS, PVDM2-48, 고급 IP Cisco IOS Software, FL-SRST-72, 64M 플래시, 256DRAM 포함)	CISCO2851-V3PN/K9
Cisco 3825 V3PN 번들(AIM-VPN HPII-PLUS, PVDM2-64, FL-SRST-168, 고급 IP Cisco IOS Software, 64M 플래시, 256DRAM 포함)	CISCO3825-V3PN/K9
Cisco 3845 V3PN 번들(AIM-VPN HPII-PLUS, PVDM2-64, FL-SRST-240, 고급 IP Cisco IOS Software, 64M 플래시, 256DRAM 포함)	CISCO3845-V3PN/K9

표 3. Cisco 1800, Cisco 2800 및 Cisco 3800의 주문 정보(계속)

제품 이름	부품 번호
고급 성능 DES, 3DES 및 AES VPN 암호화 및 압축(Cisco 1800용)	AIM-VPN/BPII-PLUS
고급 성능 DES, 3DES 및 AES VPN 암호화 및 압축(Cisco 2800용)	AIM-VPN/EPII-PLUS
고급 성능 DES, 3DES 및 AES VPN 암호화 및 압축(Cisco 3800용)	AIM-VPN/HPII-PLUS
Cisco 1841 고급 보안(Cisco IOS Software)	c184x-advsecurityk9
Cisco 2801 고급 보안(Cisco IOS Software)	S28NASK9
Cisco 2800 고급 보안(Cisco IOS Software)	S28NASK9
Cisco 3825 고급 보안(Cisco IOS Software)	S382ASK9
Cisco 3845 고급 보안(Cisco IOS Software)	S384ASK9
Cisco 1841 고급 IP 서비스(Cisco IOS Software)	c184x-advipservicesk9-mz
Cisco 2801 고급 IP 서비스(Cisco IOS Software)	S28AISK9
Cisco 2800 고급 IP 서비스(Cisco IOS Software)	S28AISK9
Cisco 3825 고급 IP 서비스(Cisco IOS Software)	S382AISK9
Cisco 3845 고급 IP 서비스(Cisco IOS Software)	S384AISK9
Cisco 1841 고급 엔터프라이즈 서비스(Cisco IOS Software)	c184x-adventerprisek9-mz
Cisco 2801 고급 엔터프라이즈 서비스(Cisco IOS Software)	S28AESK9
Cisco 2800 고급 엔터프라이즈 서비스(Cisco IOS Software)	S28NAESK9
Cisco 3825 고급 엔터프라이즈 서비스(Cisco IOS Software)	S382AESK9
Cisco 3845 고급 IP 서비스(Cisco IOS Software)	S384AESK9
침입 감지 시스템(IDS) 네트워크 모듈	NM-CIDS-K9
컨텐트 엔진 NM-기본 성능-20GB	NM-CE-BP-20G-K9
컨텐트 엔진 NM-기본 성능-40GB	NM-CE-BP-40G-K9
컨텐트 엔진 NM-기본 성능-80GB	NM-CE-BP-80G-K9

서비스 및 지원

시스코는 고객의 성공을 촉진시켜 주는 수많은 종류의 서비스 프로그램을 제공합니다. 이러한 혁신적인 서비스 프로그램을 제공하기 위해 사람, 프로세스, 툴, 파트너가 서로 협력하므로 높은 수준의 고객 만족도를 실현할 수 있습니다. 시스코 서비스는 귀하가 네트워크 투자를 보호하고, 네트워크 운영을 최적화하며, 새로운 애플리케이션에 대비하여 네트워크를 준비함으로써 인텔리전트 네트워크와 비즈니스의 역량을 확장하도록 도와줍니다. 시스코 서비스에 대한 자세한 내용은 시스코 기술 지원 서비스(Cisco Technical Support Services) 또는 시스코 고급 서비스(Cisco Advanced Services)를 참조하십시오.

추가 정보

Cisco 1800, 2800 및 3800에 대한 자세한 내용은 http://www.cisco.com/go/routing을 방문하거나 지역 시스코 고객 담당자에게 문의하십시오.

www.cisco.com/kr

2004-10-04

■ Gold 파트너	• (주)데이타크레프트코리아	02-6256-7000	• (주)인네트	02-3451-5300	• (주)인성정보	02-3400-7000
	• 한국아이비엠(주)	02-3781-7800	• (주)콤텍시스템	02-3289-0114	• 쌍용정보통신(주)	02-2262-8114
	• 에스넷시스템(주)	02-3469-2400	• (주)링네트	02-6675-1216	• 한국후지쯔(주)	02-3787-6000
	• 한국휴렛팩커드(주)	02-2199-0114	• (주)LG씨엔에스	02-6363-5000		
■ Silver 파트너	• (주)시스폴	02-6009-6009	• 포스데이타주식회사	031-779-2114	• SK씨앤씨(주)	02-2196-7114/8114
■ Local 디스트리뷰터	• (주)소프트뱅크커머스코리아	02-2187-0176	• (주)아이넷뱅크	02-3400-7486	• SK 네트웍스	02-3788-3673
■ IPT 전문파트너	• 에스넷시스템(주)	02-3469-2900	• (주)인성정보	02-3400-7000	• 크리스넷	1566-3827
	• LG기공	02-2630-5280	• (주)컴웨어	02-2631-4300		
■ IP/VC(Video Conferencing)	• (주)텔레트론	031-340-7102	• (주)컴웨어	02-2631-4300		
■ IPCC전문파트너	• 한국IBM	02-3781-7114	• 한국HP	02-2199-4272	• LG기공	02-2630-5280
	• (주)인성정보	02-3400-7000	• 삼성네트웍스주식회사	02-3415-6754		
■ WLAN 전문 파트너	• (주)에어키	02-584-3717	• (주)텔레트론	02-6245-7600		
■ Security 전문 파트너	• 코코넛	02-6007-0133	• (주)토탈인터넷시큐리티시스템	051-743-5940	• 이노비스	02-6288-1500
	• UNNET Systems	02-565-7034				
■ Optical 전문 파트너	• (주)LG씨엔에스	02-6363-5000	• 에스넷시스템(주)	02-3469-2900	• 미리넷주식회사	02-2142-2800
■ CN 전문 파트너	• 메버릭시스템	02-6283-7425				
■ Storage 전문 파트너	• (주)패킷시스템즈코리아	02-558-7170	• 메크로임팩트	02-3446-3508		