Cisco Traffic Anomaly Detector Module 데이터시트

데이터 시트

Cisco Traffic Anomaly Detector Module

Cisco® Catalyst® 6500/Cisco 7600 Router Traffic Anomaly Detector Module 은 Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터를 위한 통합 서비스 모듈입니다. 이 모듈은 대규모 조직이 분산 서비스 거부(DDoS) 공격이나 기타 네트워크 공격을 차단하도록 도와주며 사용자가 신속하게 공격 차단 서비스를 시작하여 공격이 비즈니스에 악영향을 미치기 전에 차단할 수 있습니다.

특허를 획득한 고유의 MVP(MultiVerification Process) 아키텍처를 기반으로 하는 Cisco Traffic Anomaly Detector Module 은 최신 기술인 행위 분석 및 공격 탐지 기술을 사용하여 모든 종류의 온라인 공격을 능동적으로 감지하고 식별합니다. Cisco Traffic Anomaly Detector Module 은 개별 장치가"정상"작동 조건에서 어떻게 동작하는지를 나타내는 상세 프로필을 만들기 위해 웹 서버 또는 전자 상거래 애플리케이션 서버와 같은 보호된 장치로 향하는 트래픽을 지속적으로 모니터링합니다. 이 프로필에서 플로우 별 이상을 감지한 Cisco Traffic Anomaly Detector Module 은 이 이상 동작을 잠재적인 공격으로 간주하고 다음과 같은 사용자 기본 설정에 따라 대응합니다. 즉, 수동 대응을 시작하라는 경보를 운영자에게 보내거나 기존 관리 시스템을 트리거하거나 Cisco Anomaly Guard Module 을 실행하여 즉시 차단 서비스를 시작합니다.

Cisco Anomaly Guard Module 과 함께 Cisco Traffic Anomaly Detector Module 을 사용하면 업계에서 가장 광범위한 DDoS 차단 시스템이 됩니다. MVP 아키텍처를 통해 Cisco Traffic Anomaly Detector Module 과 Cisco Anomaly Guard Module 이 합법적인 트랜잭션에는 영향을 미치지 않고 악성 공격 흐름을 감지, 우회, 격리 및 제거할 수 있으므로, 네트워크와 비즈니스에 필수적인 트래픽을 확실하게 보호할 수 있습니다.

작동 방식

DDoS 공격은 오늘날 온라인 비즈니스에서 가장 급속도로 전파하는 온라인 위협 형태입니다. 이 공격은 단순히 유명세를 얻으려는 파괴 행위로부터 시작하여 희생 대상 비즈니스의 운영을 파괴하려는 고도로 집중된 이벤트로 발전해왔습니다. 이 공격은 갈수록 무자비하고 악성화되어 많은 비즈니스에 상당한 피해를 주고 있습니다.

또한, 공격 기술도 더욱 정교해지고 있습니다. 공격자가 인터넷 데이터 센터와 기존 방어 체계를 무너뜨리기 위해 올바른 요청을 가장하고 발신자 신원을 위장하고 일련의 감염된"좀비"호스트를 사용하기 때문에, 신원을 확인하고 악성 트래픽 흐름을 차단하는 것은 거의 불가능합니다.

Cisco Traffic Anomaly Detector Module 과 Cisco Anomaly Guard Module 을 함께 사용하면 DDoS 공격으로부터 엔터프라이즈, 호스팅 센터, 정부 기관 및 서비스 제공업체 환경을 보호하는 완벽한 감지 및 방지 솔루션을 제공할 수 있습니다. Traffic Anomaly Detector Module 은 알려진"정상"동작에서 이상 동작을 감지하여 잠재적인 공격을 식별한 후 Anomaly Guard Module 에게 우회를 시작하라고 통보합니다. 이 우회 기능은 대상 장치로 향하는 트래픽을

검사하기 위해 트래픽의 방향을 우회시킵니다. 다른 모든 트래픽은 계속해서 그대로 전달되므로 단일 Anomaly Guard Module 이 보호할 수 있는 장치나 구역의 수가 증가합니다.

우회된 트래픽은 Cisco Anomaly Guard Module 을 통해 재라우팅되며"악성"트래픽과 합법적인 트랜잭션을 식별하고 구분합니다. 공격 패킷이 식별되어 제거되고 합법적인 트래픽은 원래의 목적지로 전달됩니다. 이렇게 하면 올바른 사용자와 트랜잭션이 항상 전달되고 가용성이 극대화됩니다.

구성 및 배치 옵션

Cisco Traffic Anomaly Detector Guard Module 에서는 통합 모드와 전용 모드의 두 가지 별도 배치 옵션을 제공합니다.

통합 모드에서는 데이터 센터에 배치되거나 정상적인 레이어 3 데이터 경로에 위치하는 기존의 Cisco Catalyst 6500 Series 또는 Cisco 7600 Series 섀시에 하나 이상의 Traffic Anomaly Detector Module 이 설치됩니다. 리소스를 보호하기 위해 모니터링 중인 경우 이 리소스로 향하는 트래픽의 복제 본이 SPAN(Switched Port Analyzer) 세션이나 실제 포트/VLAN 또는 VLAN 액세스 제어 목록(VACL) 캡처에 의해 Traffic Anomaly Detector Module 로 보내져야 합니다.

전용 모드에서는 전용 Cisco Catalyst 6500 Series 스위치 또는 7600 Series 라우터(다운스트림 스위치에 인접한 라우터 또는 보호 중인 장치나 구역 부근의 라우터)에 Traffic Anomaly Detector Module 이 설치되므로, 성장하는 대규모 환경에 확장성이 뛰어난 솔루션을 제공합니다. 이구성에서는 트래픽의 복제 본이 원격 SPAN 또는 분광기를 통해 전용 스위치나 라우터로 보내져야 합니다.

통합 또는 전용 모드에서 Cisco Traffic Anomaly Detector Module 을 설치하면 1 단계 또는 2 단계 패킷 캡처 프로세스를 사용하여 모니터링용으로 트래픽의 복제 본을 받아볼 수 있습니다. 통합 모드나 전용 모드에서 공격이 감지되면 다음의 세 방식 중 하나로 Traffic Anomaly Detector Module 이 대응합니다. 즉, 수동 대응을 시작하라는 경보를 보내거나 기존 관리 시스템이 조치를 취하도록 트리거하거나 Cisco Anomaly Guard Module 또는 Cisco Guard XT 장치를 자동으로 실행하여 즉시 차단 서비스를 시작합니다.

애플리케이션

Cisco DDoS 이상 감지 및 방지 솔루션은 엔터프라이즈 및 서비스 제공업체 환경에 서비스를 제공하는 다양한 토폴로지에 배치될 수 있습니다(그림 1-3).

그림 1. 엔터프라이즈 또는 호스팅 데이터 센터에서 Cisco DDoS 이상 감지 및 차단

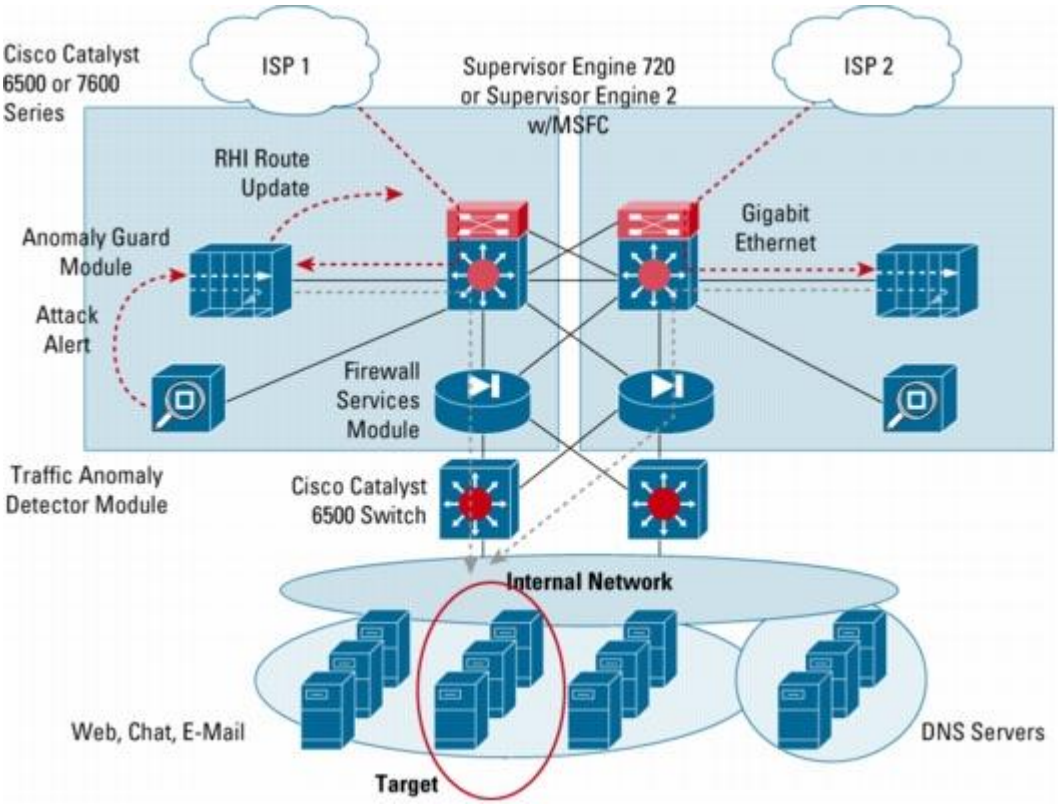


그림 2. 서비스 제공업체 환경에서 Cisco DDoS 분배/에지 보호

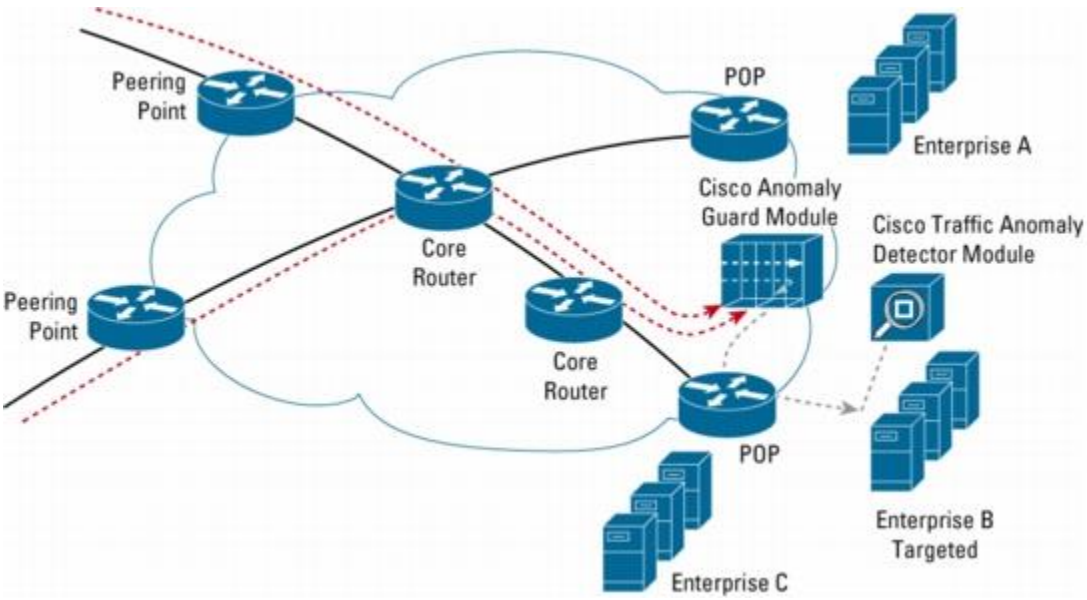
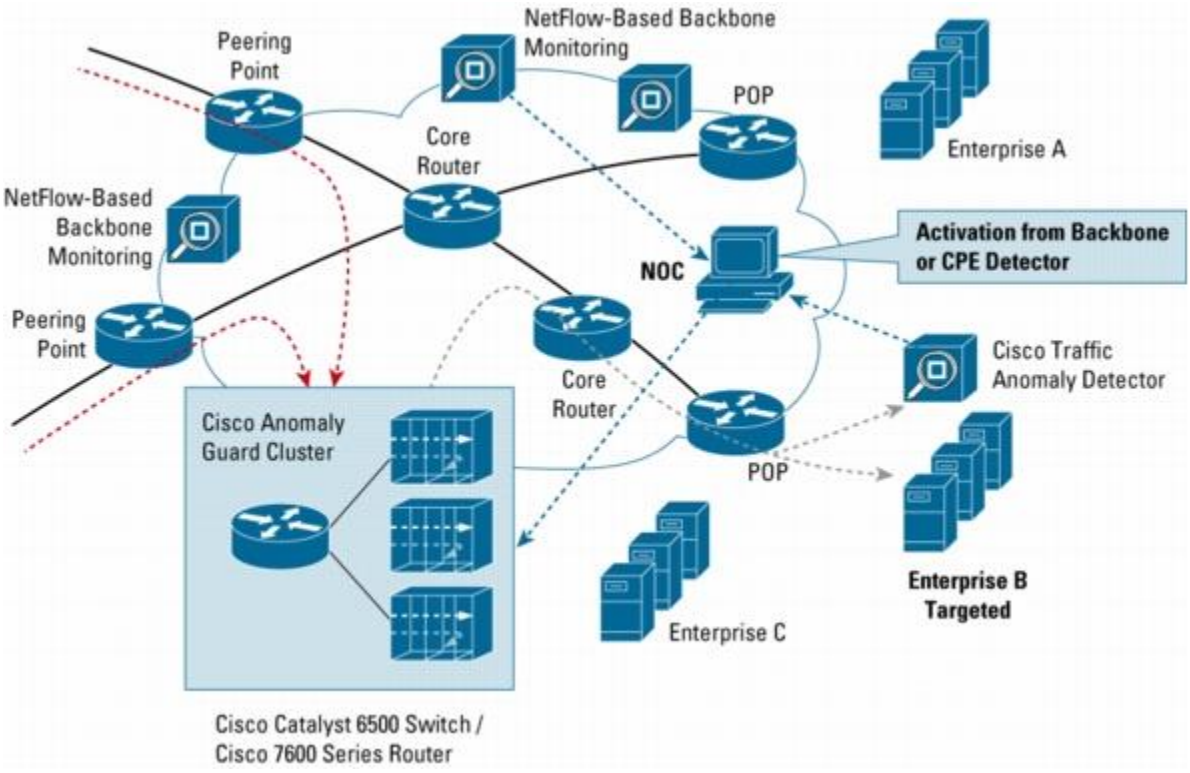


그림 3. 서비스 제공업체의 중앙 Scrubbing Center 에서 Cisco DDoS 이상 감지 및 차단



기능 및 이점

감지 및 학습

Cisco Traffic Anomaly Detector Module 은 Cisco Catalyst 6500 Series 또는 Cisco 7600 Series 섀시를 통해 전달되는 인바운드 트래픽의 미러링된 복사본을 모니터링하며, 귀중한 스위치 또는 라우터 자산을 소모하지 않고도 보호된 각 장치의"정상"동작 상세 프로필을 만들 수 있습니다.

Cisco Traffic Anomaly Detector Module 은 정교한 동작 기반 이상 감지 기술을 사용하여 이 프로필에서 벗어나는 모든 행위를 전역 세션 수준과 미세 세션 수준에서 감지합니다. 이를 통해 알려진 모든 유형의 공격과 Day Zero 공격을 매우 정확하게 식별할 수 있습니다. 모든 패킷에 대해 커넥션 별 상태 분석을 수행함으로써 정교하고 예측할 수 없는 대부분의 공격을 신속하고 완벽하게 감지하고 식별할 수 있습니다. 이러한 공격에는 서서히 느린 속도로 서버 자원을 소모하는 공격과 수십만 개의 분산된 좀비에 의해 개시되는 대규모 공격이 있습니다.

Traffic Anomaly Detector Module 의 행위 감지 방식을 사용하면 문자열 서명을 계속해서 업데이트할 필요가 없으며 정적 서명 기반 방식에서흔히 나타나는 엄청난 수의 경보와 확실하지 않은 정보를 줄일 수 있습니다. 뿐만 아니라, 즉시 작동이 가능하도록 기본 프로필로 미리 구성된 Cisco Traffic Anomaly Detector Module 이 제공되므로, 자동화된 학습을 통해 사용자가 구체적인 조정 권장 사항을 만들 수 있으며 운영자가이 권장사항을 확인할 수 있습니다.

멀티기가비트 성능

고성능 Cisco Traffic Anomaly Detector Module 은 단일 공격에서 모듈 당 100,000 개 이상의 발신자를 식별할 수 있는 완전 기가비트 이더넷 회선 속도로 공격 흐름을 모니터링합니다. 이를 통해 분산 공격으로부터 고용량 대규모의 환경을 확실하게 보호합니다.

또한, 완벽하게 미러링된 트래픽을 다단계로 분석함으로써 느린 속도의 가장 은밀한 공격까지도 신속하게 식별할 수 있습니다. 최상의 보호를 제공하기 위해 Cisco Traffic Anomaly Detector Module 을 다운스트림 Cisco Catalyst 섀시(데이터 센터의 보호되는 리소스 인근)에 배치하거나 업스트림 섀시에 배치하여 보다 광범위한 커버리지를 제공할 수 있습니다.

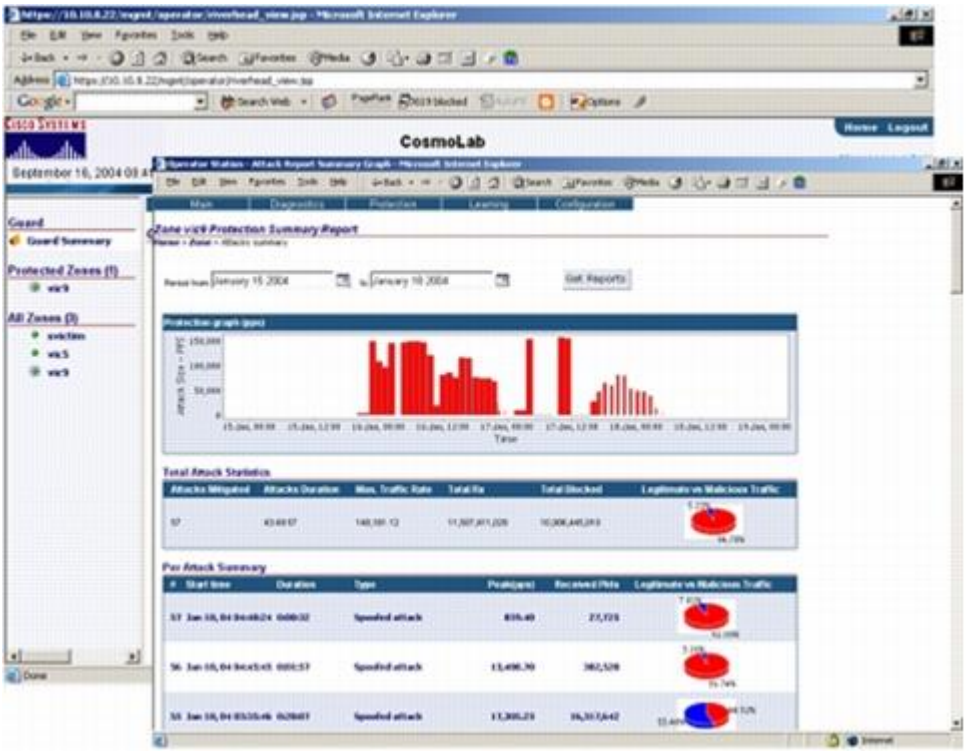
보고 및 관리

Cisco Traffic Anomaly Detector Module 에서는 웹 기반 GUI 를 사용합니다. 이 인터페이스는 간단하고 직관적인 방식으로 정보를 표시하므로 구성, 운영, 공격 식별 및 분석이 상당히 단순화됩니다.
여러 수준의 실시간 기록 및 보고 기능은 상세한 정보를 네트워크 운영자, 보안 관리자 및 고객에게 제공하여 공격 감지, 정책 설정 및 차단을 지원합니다.

(그림 4). 백엔드 커스터마이즈나 추후 검토를 위해 보고서 통계를 텍스트 및 XML(Extensible Markup Language) 스키마 형식의 파일로 내보낼 수 있습니다.

뿐만 아니라, 공격 상황에 신속하게 대응하기 위해 네트워크 운영자와 Cisco Anomaly Guard Module 에게 경보를 보내도록 Cisco Traffic Anomaly Detector Module 을 구성할 수 있습니다. 여기에는 신속하게 공격을 막아주는 자동화된 완화 서비스가 포함됩니다. SNMP(Simple Network Management Protocol) MIB 를 통해 장치 수준별, 보호된 구역 수준별 및 공격 수준별 통계를 표준 기반 관리 시스템에서 모두 사용할 수도 있습니다.

그림 4. 여러 수준의 모니터링 및 보고를 통해 상세한 실시간 성능 정보 제공



통합의 이점

배치의 유연성

Cisco Catalyst 6500 Series 스위치나 Cisco 7600 Series 라우터 내에 설치되는 Cisco Traffic Anomaly Detector Module 은 완벽한 DDoS 감지 기능을 네트워크 인프라에 통합합니다. 기존의 스위치나 라우터에 모듈을 쉽게 설치할 수 있으므로, 인터페이스 포트를 사용하지 않고도 때와 장소에 상관없이 강력한 DDoS 보호 서비스를 배치할 수 있습니다. 또한, 모든 범위의 섀시 크기와 고가용성, DC 전원 및 NEBS(Network Equipment Building Standards) 옵션을 사용하여 고밀도의 전용 장치나 멀티서비스 보안 스위치를 배치할 수 있습니다. 호환되는 라인 카드는 미디어의 유연성을 보장해줍니다. 패킷 캡처는 완전히 섀시 내에서만 일어나거나, 또는 원격 SPAN 또는 광섬유 연결 분할기를 사용하는 여러 장치상에서 일어날 수 있습니다.

확장성

고용량의 보호가 필요한 경우, 최대 4 개의 모듈을 단일 스위치에 설치하여 급속하게 확장되는 대규모 환경을 지원할 수 있습니다. 또한, Traffic Anomaly Detector Module 의 멀티프로세서 아키텍처와 여러 개의 기가비트 백플레인 인터페이스가 향후에 라이센스 소프트웨어 업그레이드를 지원하므로 모듈 당 수 기가비트의 성능이 가능합니다.

안정성 및 고가용성

Cisco Traffic Anomaly Detector Module 은 독립형 Traffic Anomaly Detector XT 장치의 성능, 안정성 및 강력한 아키텍처를 그대로 유지합니다. Cisco Catalyst 6500 Series 스위치나 Cisco 7600 Series 라우터에 배치된 Traffic Anomaly Detector Module 은 중복 수퍼바이저 엔진, 백플레인, 전원 공급 장치 및 팬을 비롯하여 안정성이 높은 중복

구성을 지원합니다. 또한, Cisco Catalyst 6500 Series 스위치와 Cisco 7600 Series 라우터가 DDoS 차단 및 고가용성 옵션을 위해 CPP(Control Plane Policing)를 제공합니다.

소유 비용 절감

Cisco Anomaly Guard Module 이 다른 서비스 모듈과 함께 Cisco Catalyst 6500 Series 스위치나 Cisco 7600 Series 라우터에 통합되므로 관리할 장치가 줄어서 운영 비용이 절감됩니다. 뿐만 아니라, 애플리케이션 소프트웨어가 장치 애플리케이션 소프트웨어와 유사하므로 교육 비용이 최소화됩니다.

요약

Cisco Anomaly Guard Module 과 함께 사용되는 Cisco Traffic Anomaly Detector Module 은 가장 심각한 DDoS 공격에서도 비즈니스 운영이 중단되는 것을 막아주는 완벽한 보안 솔루션입니다. 이러한 중요한 경쟁 우위를 통해 소중한 비즈니스 자산의 가용성을 완벽하게 보장하고 보호할 수 있습니다.

시스템 요구 사항

• Cisco Traffic Anomaly Detector Module MVP-OS Software Release 4.0 이상.

• MSFC2(Multilayer Switch Feature Card 2)가 있는 Cisco Catalyst 6500 Series Supervisor Engine 2 또는 Cisco Catalyst 6500 Series
Supervisor Engine 720(Cisco Catalyst 6500 Series Supervisor Engine 1 은 지원되지 않음).

• 1 Gbps 이상의 트래픽을 처리하기 위해 Supervisor Engine 2 에 필요한 SFM(Switch Fabric Module).

• 기본 Cisco IOS®Software Release 12.2(18)SXD3 이상. Cisco 7600 Series 라우터를 사용하는 경우, 공식적인 지원은 Cisco IOS Software Release 12.2(18)SXE 에서만 제공됩니다.

• Cisco Catalyst 6500 Series 스위치 또는 Cisco 7600 Series 라우터에서 슬롯 1 개 점유.

• 최대 4 개의 Cisco Traffic Anomaly Detector Module 을 단일 섀시에 배치하여 로드 공유 모드에서 동일한 목적지나 다른 목적지를 보호할 수
있습니다. Cisco Anomaly Guard Module 과 Traffic Anomaly Detector Module 을 동일한 섀시에 배치하는 경우 총 8 개의 모듈을 조합하여 설치할 수 있습니다. 비표준 설치에 대해서는 릴리스 노트를 참조하거나 시스코 기술 지원 대리점에 문의하십시오.

• 리던던시형 수퍼바이저 엔진은 NSF(Nonstop Forwarding)의 SSO(Stateful Switchover) 모드에서 사용되어야 합니다(RPR[Route Processor Redundancy] 또는 RPR+가 아님).

호환성

최초 고객 배송(FCS) 시에 동일한 스위치나 라우터에서 Cisco Traffic Anomaly Detector Module 이 다음과 같은 장치와 호환되도록 인증됩니
다.

• Cisco IOS Firewall

• Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터용 Cisco FWSM(Firewall Services Module)

• Cisco Catalyst 6500 Series 스위치용 Cisco IDSM-2(Intrusion Detection System Services Module)

• Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터용 Cisco CSM(Content Switching Module)

최근의 호환성 인증 상태에 대해서는 시스코 기술 지원 서비스에 문의하십시오.

기능

표 1 은 Cisco Traffic Anomaly Detector Module 의 기능을 나타냅니다.

표 1. Traffic Anomaly Detector Module 기능

기능	설명
용량	• 1Gbps 인터페이스 1 개 • 150 만개의 동시 연결
다중 보안 컨텍스트	• 다른 정책과 기준을 동시에 모니터링할 수 있는 90 개의 구역
관리	• 커맨드 라인 인터페이스(CLI)에 대한 콘솔 • CLI 에 대한 SSH(Secure Shell Protocol) • Cisco Guard Device Manager 에 대한 SSL(Secure Sockets Layer) • SNMP MIB, MIBII 및 트랩
인증, 권한 부여 및 계정 관리(AAA) 지원	• TACACS+를 통해 AAA 와 통합 • 권한 수준 및 명령 수준의 권한 부여 및 계정 관리
보안	• 관리 인터페이스상에서 IP 테이블 및 자가-DDoS 보호
로깅	• 광범위한 시스로그 로깅 및 이벤트
공격 차단	• 스푸핑 공격 및 스푸핑 이외의 공격 • TCP 공격(syns, syn-acks, acks, fins, fragments) • UDP(User Datagram Protocol) 공격(random port floods, fragments) • ICMP(Internet Control Message Protocol) 공격(unreachable, echo, fragments) • DNS(Domain Name System) 공격 • 클라이언트 공격 • 비활성 및 전체 연결 공격 • HTTP Get Flood 공격 • BGP(Border Gateway Protocol) 공격

제품 사양

표 2 는 Cisco Traffic Anomaly Detector Module 의 제품 사양을 나타냅니다.

표 2. 제품 사양

기능	설명

메모리	• 7 GB DDRAM, 1 GB 컴팩트 플래시
무게	• 다른 정책과 기준을 동시에 모니터링할 수 있는 90 개의 구역 • 최소: 3 파운드(1.36 kg) • 최대: 5 파운드(2.27 kg)
높이	1.18 인치(30 mm)
가로	15.51 인치(394 cm)
세로	16.34 인치(415 cm)
동작온도	32 ~ 104°F (0 ~ 40°C)
비동작 온도	-40 ~ 167°F (-40 ~ 75°C)
습도	10 - 90%, 비응축
관리	• 안전한 웹 기반 GUI • CLI: 콘솔, 텔넷, SSH • Cisco(Riverhead) SNMP MIB 및 MIB II • TACACS+ • Syslog
인증	• UL 승인 • CE • FCC Rules Part 15 호환

주문 정보

표 3 은 Cisco Traffic Anomaly Detector Module 의 주문 정보를 나타냅니다.

표 3. 주문 정보

제품명	부품번호	SMARTnet 번호
Cisco Catalyst 6500/Cisco 7600 Router Traffic Anomaly Detector Module	WS-SVC-ADM-K9-1	CON-SNT-WSADMK9
Cisco Catalyst 6500/Cisco 7600 Router Traffic Anomaly Detector Module MVP-OS R4.0 소프트웨어	SC-ADM-4.0-K9	

주문을 하려면 시스코 주문 홈 페이지를 방문하십시오.

기술 지원 서비스

대규모 조직이든 무역 회사이든 서비스 공급자이든 상관없이 시스코 시스템즈는 귀사의 네트워크 투자를 극대화하기 위해 노력하고 있습니다. 시스코는 시스코 제품이 효율적으로 동작하고, 높은 가용성을 유지하며, 최신 시스템 소프트웨어를 사용할 수 있도록 다양한 기술 지원 서비스를제공합니다.
시스코 기술 지원 서비스(Cisco Technical Support Services) 조직에서는 다음과 같은 특징을 제공합니다. 이러한 특징을 통해 업무에 필수적인 애플리케이션이 실행 중인 시스템의 네트워크 투자를 보호하고 가동 중단 시간을 최소화할 수 있습니다.

• 온라인과 전화를 통해 시스코 네트워킹 전문 지식을 제공합니다.
• 소프트웨어 업데이트와 업그레이드를 통해 능동적인 지원 환경을 구축합니다. 이 지원 환경은 고장이나 문제가 발생했을 때 단순히 이러한 고장이나 문제를 해결하는 역할뿐만 아니라 네트워크의 지속적인 운영에 있어 핵심적인 역할을 수행합니다.
• 귀하가 원할 때에 시스코 기술 정보와 리소스를 사용할 수 있습니다.
• 기술 직원의 리소스를 늘려서 생산성을 향상시킵니다.
• 현장 하드웨어 교체를 통해 원격 기술 지원을 보완합니다.

<업데이트: 2005 년 6 월 16 일>