데이터 시트

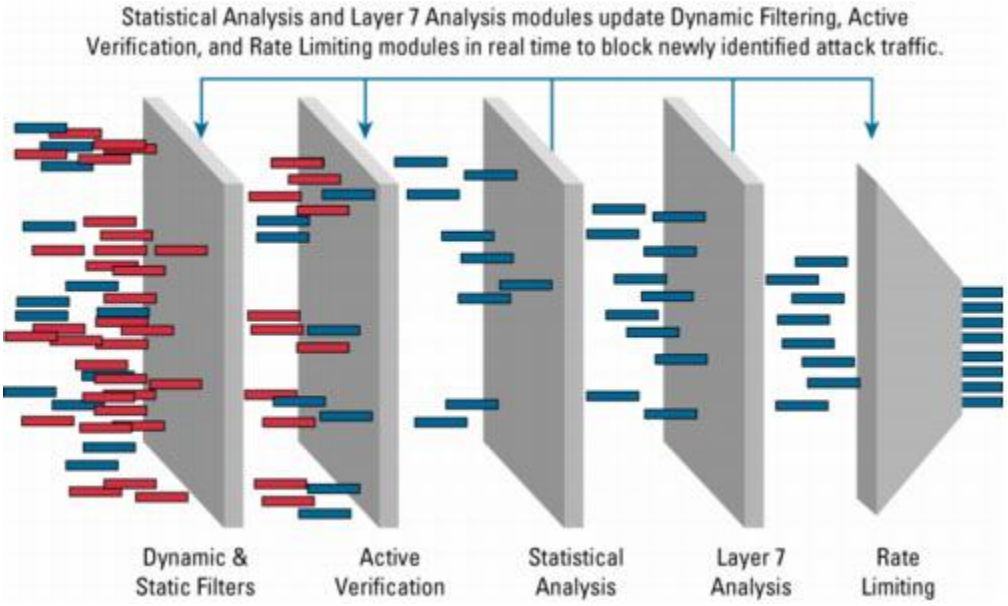
Cisco Anomaly Guard Module

Cisco® Catalyst® 6500/Cisco 7600 Router Anomaly Guard Module 은 Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터용 통합 서비스 모듈이며, 대규모의 분산 서비스 거부(DDoS) 공격으로부터 온라인 리소스를 보호하기 위한 강력하고 광범위한 솔루션을 제공합니다. Cisco Anomaly Guard Module 은 가장 엄격한 성능이 필요한 대기업 및 서비스 제공업체 환경의 성능 및 확장성 요구사항을 충족시키도록 설계되었으며, 점점 더 복잡해지고 예측할 수 없는 공격을 차단하기 위한 최상의 보호 성능을 제공합니다.

단일 Cisco Anomaly Guard Module 은 Gbps 회선 속도로 공격 트래픽을 처리할 수 있는 플랫폼을 제공합니다. Anomaly Guard Module 에서는 고유의"주문형"배치 모델을 사용하므로, 다른 트래픽에는 영향을 미치지 않고 대상 장치나 구역으로 향하는 트래픽만을 우회시켜서 정화할 수 있습니다. 해당 모듈 내에 통합된 여러 방어 레이어를 사용하여 Anomaly Guard Module 이 악성 공격 트래픽을 식별하고 차단할 수 있으며, 합법적인 트랜잭션은 본래 목적지로 계속해서 보낼 수 있습니다. 따라서 심각한 공격에서도 비즈니스를 계속 운영할 수 있습니다.
단일 모듈 속도의 몇 배에 달하는 속도를 지원하기 위해 단일 섀시에 여러 개의 Cisco Anomaly Guard Module 을 사용하여 점차적으로 확장할 수 있으므로 대기업, 성장 중인 기업, 서비스 제공업체 환경에 쉽게 적응이 가능한 확장형 솔루션을 제공할 수 있습니다. Anomaly Guard Module 의 마이크로프로세서 아키텍처에서는 향후에 라이센스 소프트웨어 업그레이드를 지원하여 대규모 공격의 방어 성능을 강화 및 향상시킬 수 있습니다.

진화하는 DDoS 공격
오늘날의 DDoS 공격은 갈수록 더 악의적이고 파괴적이며 집중적입니다. 이러한 공격은 특정 사이트나 경쟁업체를 대상으로 불만이 있는 사용자, 비양심적 기업, 부당 취득자로 인해 시작되며 대부분의 일반적인 방어 수단을 쉽게 무용지물로 만들 수 있습니다. DDoS 공격은 합법을 가장한 요청, 엄청난 수의 좀비 소스 및 ID Spoofing 등으로 구성되기 때문에 악의적 플로우의 식별과 차단이 거의 불가능합니다. 이 공격은 피해 시스템을 마비시키고 정상적인 비즈니스 수행을 방해하여, 트랜잭션과 고객 손실에서 명성 하락과 법적 책임에 이르기까지 연간 수십 억 달러의 손실을 유발합니다.
Cisco Anomaly Guard Module 은 모든 유형의 DDoS 공격을 차단하므로, 기업에서는 업무상 필수적인 기능과 수익 관련 기능을 저하시키지 않고도 악성 트래픽을 식별하고 차단할 수 있습니다. 특허를 받은 MVP(MultiVerification Process) 아키텍처 기반인 Cisco Anomaly Guard Module 에서는 우수한 비정상 감지 기능을 사용하여 통합 소스 검사와 고성능 필터링 기능이 있는 위장 방지 기술을 동적으로 적용함으로써 개별 공격을 식별하고 차단하는 동시에 합법적인 트랜잭션은 통과시킵니다(그림 1). 모든 공격 행위를 폭 넓게 파악하도록 설계된 직관적인 그래픽 인터페이스와 여러 수준의 광범위한 모니터링 및 리포팅 기능을 지닌 Cisco Anomaly Guard Module 은 가장 광범위한 DDoS 방어 성능을 제공하여 비즈니스 운영을 보호합니다.

그림 1. Cisco Anomaly Guard Module MVP 아키텍처



작동 방식

Cisco Anomaly Guard Module 은 DDoS 공격으로부터 대기업, 정부 기관, 호스팅 센터 및 서비스 제공업체를 보호해주는 시스코 시스템즈의 완벽한 탐지 및 완화 솔루션 중 일부분에 지나지 않습니다. Cisco Anomaly Guard Module 은 호스팅 및 서비스 제공업체가 유용한 DDoS 공격 보호 서비스를 가입자에게 제공하는 데 사용할 수 있는 강력한 확장형 솔루션입니다. Cisco Traffic Anomaly Detector Module(또는 DDoS 공격여부를 탐지하는 타사의 경보 시스템)과 함께 Anomaly Guard Module 을 사용하여 상세한 공격 분석, 식별 및 차단 서비스를 수행함으로써 공격으로 인한 네트워크와 데이터 센터 운영의 중단을 예방할 수 있습니다.

Traffic Anomaly Detector Module 이 잠재적인 공격을 식별하면 Anomaly Guard Module 에게 동적인 우회를 시작하라고 알립니다. 이 우회 기능은 대상 리소스로 향하는 트래픽을 검사하고 정화하기 위해 트래픽 방향을 우회시킵니다. 다른 모든 트래픽은 원하는 목적지로 바로 전송되므로 Cisco Anomaly Guard Module 은 영향을 최소화하고 안정성이 높으며 경제적이고 설치가 쉬운 솔루션입니다.

우회된 트래픽은 Anomaly Guard Module 을 통해 재라우팅되며 여러 검사 레이어를 거쳐"악성"트래픽과 합법적인 트랜잭션을 식별하고 구분합니다. 특정 공격 패킷을 식별하여 제거하고"정상적인"트래픽은 원래의 목적지로 포워딩되므로, 올바른 사용자와 트랜잭션만이 전달되어 가용성이 극대화됩니다.

구성 및 배치 옵션

Cisco Anomaly 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 Cisco Anomaly Guard Module 이 설치됩니다. 공격이 탐지되면, 수상한 트래픽이 Cisco Catalyst 백플레인을 통해 Anomaly Guard Module 에 동적으로 우회되어 분석과 치료를 거칩니다. 분석과 치료를 거친 트래픽은 그 다음에 있는 정상적인 다운스트림 장치로 포워딩됩니다.

전용 모드에서는 Cisco Catalyst 6500 Series 스위치 또는 7600 Series 라우터에 Anomaly Guard Module 이 설치됩니다. 예를 들어, 고용량의 보호 성능을 위해"Scrubbing Center"에서 여러 개의 Cisco Anomaly Guard

Module 을 클러스터로 구성할 수 있습니다. 전용 모드에서 공격이 탐지되면 지원되는 Cisco IOS® Software 라우팅 프로토콜을 사용하여 감염 트래픽이 업스트림 스위치나 라우터에서 전용 Cisco Catalyst 스위치로 우회됩니다. 전용 섀시 내에서 Cisco Anomaly Guard Module 은 수퍼바이저 엔진의 라우팅 프로세스가 포워딩한 우회된 트래픽의 다음 경유지가 됩니다. 여기에서 트래픽이 정화되고 악성 트래픽이 제거됩니다.

Anomaly Guard Module 이 합법적인 트래픽을 네트워크로 되돌려 보내면, 이 곳에서 트래픽은 원래의 목적지로 계속 진행합니다. 또한 통합 또는 전용 모드에서 Cisco Traffic Anomaly Detector Module 을 설치하면 1 단계 또는 2 단계 패킷 캡처 프로세스를 사용하여 모니터링용으로 트래픽의 사본을 받아볼 수 있습니다.
통합 모드나 전용 모드에서 공격이 탐지되면 일반적으로 Anomaly Guard Module 이 활성화 시에 우회 프로세스를 시작하도록 설정됩니다. 이를 위해 Anomaly Guard Module 은 Cisco Catalyst 섀시 내에 Cisco RHI(Route Health Injection) 프로토콜을 사용하여 Anomaly Guard Module 을 다음 번 경유지로 만드는 수퍼바이저 엔진의 라우팅 업데이트를 동적으로 삽입합니다. 전용 모드에서 수퍼바이저 엔진의 라우팅 프로세스는 일반적으로 경로 업데이트를 업스트림 장치로 재분배하도록 구성됩니다. 기타 우회 옵션으로는 운영자 입력 경로 업데이트나 영구 정적 경로가 있습니다.

애플리케이션

Cisco DDoS 이상 탐지 및 완화 솔루션은 기업 및 서비스 제공업체 환경에 서비스를 제공하는 다양한 토폴로지에 배치될 수 있습니다
(그림 2-4).

그림 2. 기업 또는 호스팅 데이터 센터에서의 Cisco DDoS 이상 탐지 및 완화

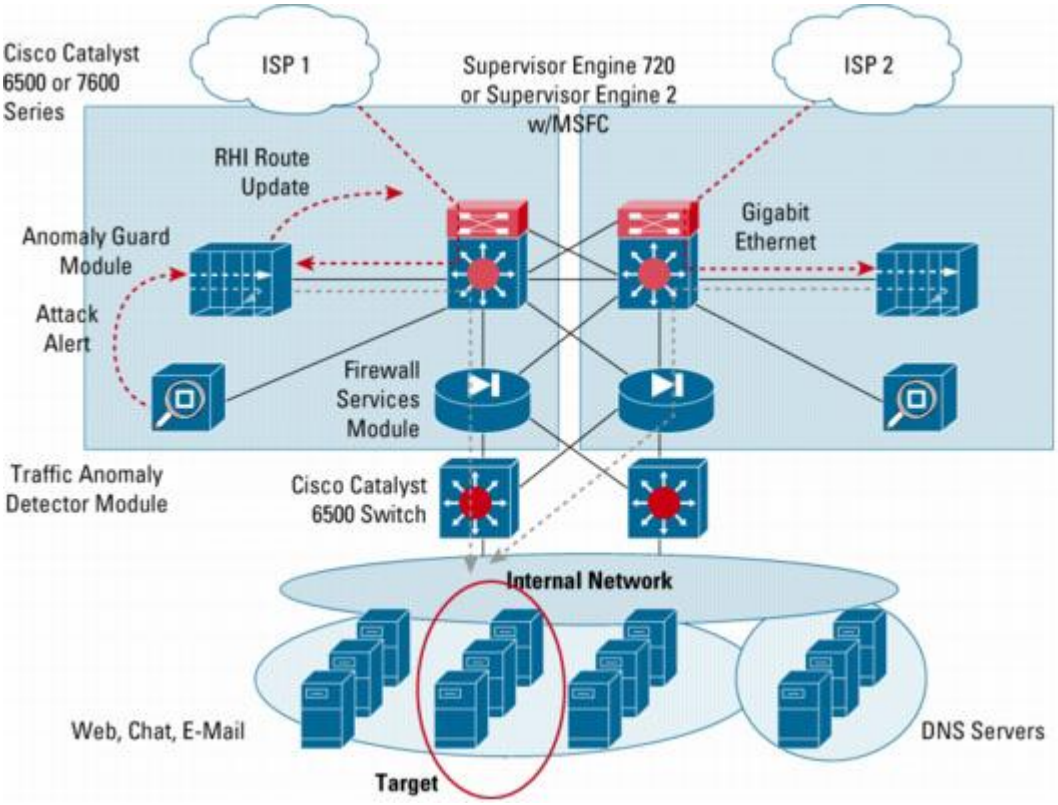


그림 3. 서비스 제공업체 환경에서의 Cisco DDoS 분산형 종단 보호

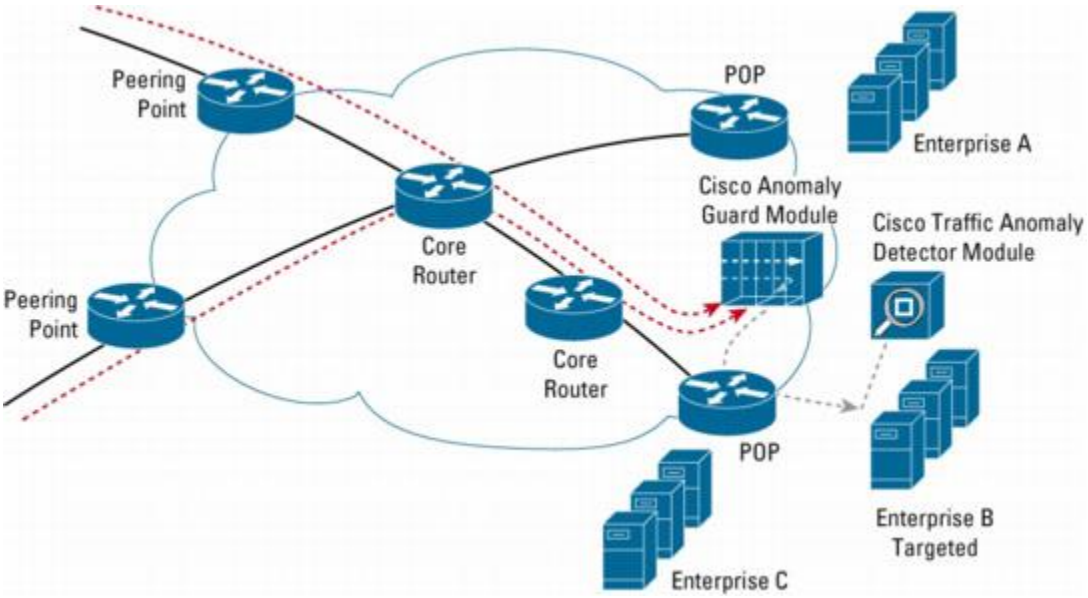
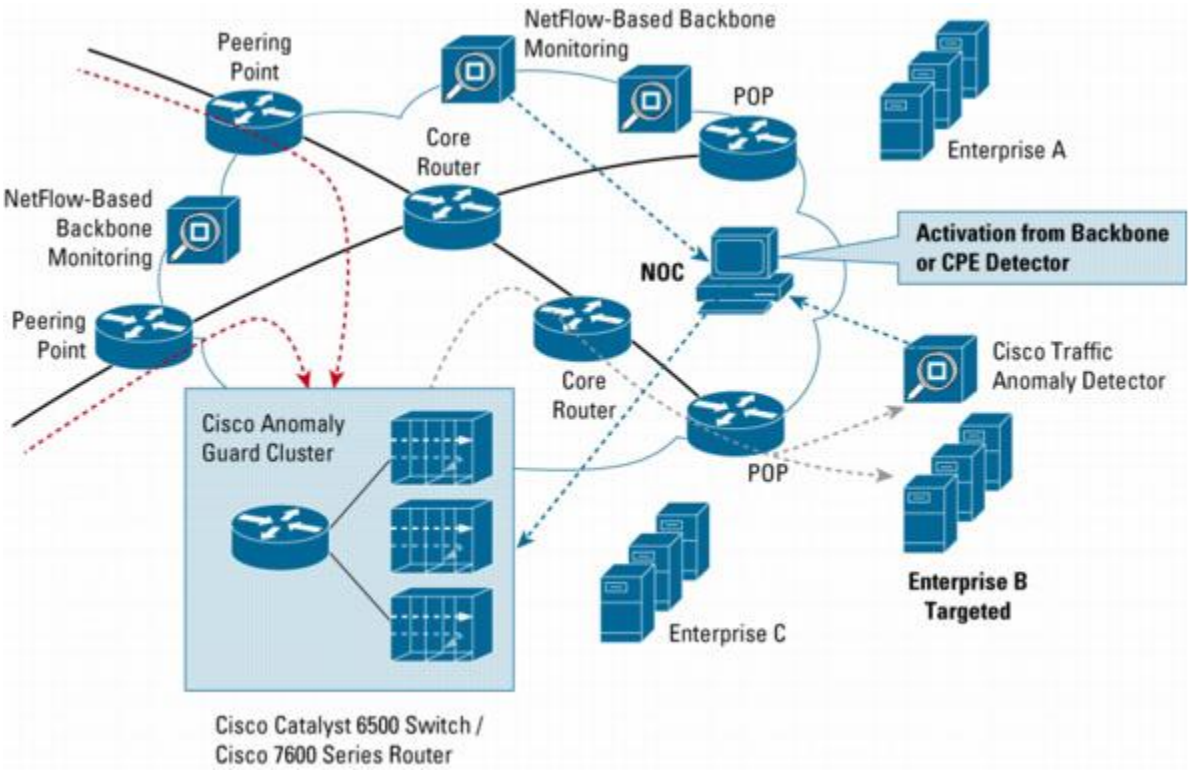


그림 4. 중앙 Scrubbing Center 에서의 Cisco DDoS 이상 탐지 및 완화



기능 및 이점

다단계 검사

Anomaly Guard Module 의 혁신적인 차단 기술은 시스코 고유의 MVP 아키텍처를 기반으로 합니다. 이 아키텍처에서는 모든 종류의 공격을 매우 정확하게 식별하고 차단하는 여러 쌍방향 레이어의 차단 기능을 제공합니다. 통합된 동적 필터링과 효과적인 검사 기술, 고급 프로필 기반의 이상 탐지 엔진을 통해 모든 종류의 공격(Day Zero 공격 포함)을 자동으로 신속하게 차단할 수 있습니다. Anomaly Guard Module 은 정교한 플로우별 분석 및 차단을 수행하여 뛰어난 정확성으로 공격 트래픽을 차단하고 합법적인 트랜잭션은 그대로 전달합니다. 이상 탐지 엔진은 일반적인 동작 기준(완벽한 플로우별 프로필 포함)을 사용하여 각 보호 리소스에 해당하는 정상 동작이나 예상 동작을 정의합니다. 사용자가 원하는 경우, 개별 장치나 구역에 맞게 프로필을 커스터마이즈하는 자동 사이트 인식 기능을 통해 기본 프로필을 향상시킬 수도 있습니다.

추가된 속도 제한 기능은 또 다른 완화 방법을 제공할 뿐만 아니라, 갑작스런 트래픽 홍수를 차단해줍니다. Berkeley Packet Filter 기반의 정적 필터인 Flex 필터를 사용하여 정밀 패킷 검사 필터를 만들 수 있으며 바이패스"화이트 리스트"필터도 사용할 수 있습니다. 또한 Anomaly Guard Module 은 모든 종류와 규모의 공격을 차단하는"좀비 킬러"성능을 제공합니다. 이러한 공격에는 좀비라고 불리는 감염된 컴퓨터에서 개시되는 공격이 포함됩니다. 이 공격은 오늘날 가장 만연하고 차단이 어려운 DDoS 공격 소스입니다. 클러스터 구성으로 Anomaly Guard Module 을 배치하면 수십 만 개의 개별 좀비를
식별하고 차단하여 최상의 보호 수준을 제공함으로써 대규모의 botnet 공격도 막을 수 있습니다.

멀티기가비트 성능

각 Cisco Anomaly Guard Module 에는 완전한 기가비트 회선 속도로 공격 분석 및 치료를 지원하는 전용 네트워크 프로세서가 있습니다. 이를 통해 감염된 좀비 호스트와 같은 대규모 분산 공격자가 개시하는 공격을 비롯한 대규모의 DDoS 공격을 차단할 수 있습니다.
여러 개의 Cisco Anomaly Guard Module 을 단일 섀시에 설치하여 초 당 패킷 속도 및 좀비 차단 성능을 점차적으로 확장할 수 있습니다. 이러한 확장을 통해 가장 심각한 위협으로부터 대기업과 서비스 제공업체 환경을 충분히 보호할 수 있습니다. 또한 여러 모듈을 클러스터로 구성하면 특별한 로드 밸런싱이 없이도 단일 리소스나 구역을 보호할 수 있습니다.

동적 우회

Cisco Anomaly Guard Module 에서는 강력한 동적 정화(on-demand Scrubbing) 모델을 사용합니다. Cisco Anomaly Guard Module 은 기존의 인라인 장치와 같은 정상적인 데이터 경로에는 삽입되지 않으며 오히려 공격을 받은 특정 리소스나 구역으로 향하는 트래픽을 자동으로 우회시켜서 추가적인 정화를 수행합니다. 공격이 탐지되면, Cisco Anomaly Guard Module 은 Cisco RHI 프로토콜을 사용하여 라우팅 업데이트를 수퍼바이저 엔진 라우팅 테이블에 삽입하여, 대상 리소스로 향하는 특정 트래픽의 다음 번 경유지로 Anomaly Guard Module 을 만듭니다.
대상 장치나 구역으로 향하는 트래픽이 정화되고 악성 패킷이 차단되면, 합법적인 트랜잭션이 원래의 목적지로 계속해서 포워딩되므로, 중요한 요청이손실될 염려가 없습니다. Cisco Anomaly Guard Module 은 현재 공격을 받고 있는 리소스나 구역으로 향하는 플로우로만 트래픽 우회를 제한하므로, 최적의 리소스 사용성, 투명성 및 안정성을 확장형 솔루션에 제공하여 대기업과 서비스 제공업체 환경의 수요를 충족시킬 수 있습니다. 또한 이 L3 장비상에 삽입함으로써 설치를 단순화하고 설치 시 영향을 줄일 수 있으며, 운영상의 유지보수와 문제 해결을 원활하게 수행할 수 있습니다.

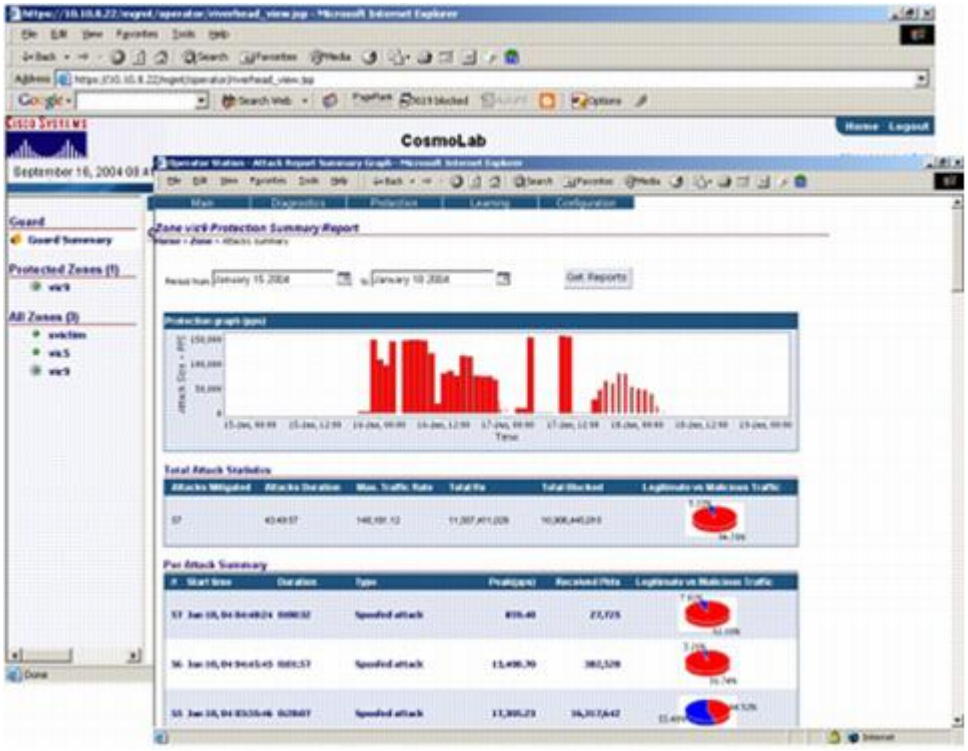
여러 수준의 모니터링 및 리포팅

Cisco Anomaly Guard Module 에는 정책 정의, 운영 모니터링 및 보고서 생성 프로세스를 단순화해 주는 직관적인 웹 기반 GUI 가 있습니다.

여러 수준의 모니터링 및 리포팅은 네트워크 운영자, 보안 관리자 및 고객에게 상세한 실시간 정보를 제공합니다(그림 5). 공격 리포트는 공격 특성, 식별된 좀비 목록 및 사용된 시행 작업을 비롯하여 개별 공격에 관련된 정보를 제공하기 때문에 보안 전문가가 Cisco Anomaly Guard Module 보안 정책을 검토하고 조정할 수 있습니다.

한편, 고객 수준의 정보 요약을 통해 서비스 제공업체가 공격 유형, 지속 시간 및 규모에 대해 쉽게 보고할 수 있습니다. 또한, 쌍방향 모드를 통해 사용자가 권장 작업과 정책을 검토하고 승인한 후에 활성화할 수 있으므로, 필요한 경우 공격 대응을 수동으로 제어할 수도 있습니다.

그림 5. 여러 수준의 모니터링 및 리포팅을 통해 상세한 실시간 성능 정보 제공



통합의 이점

배치의 유연성

Cisco Catalyst 6500 Series 스위치나 Cisco 7600 Series 라우터 내에 설치되는 Cisco Anomaly Guard Module 은 완벽한 DDoS 보호 기능을 네트워크 인프라에 통합합니다. 기존의 스위치나 라우터에 모듈을 쉽게 설치할 수 있으므로, 때와 장소에 상관없이 인터페이스 포트를 사용하지 않고도 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 정화 장치나 멀티서비스 보안 스위치를 배치할 수 있습니다. 호환되는 라인 카드는

미디어의 유연성을 보장해줍니다. 우회는 완전히 섀시 내에서만 일어나거나 수퍼바이저 엔진의 Cisco IOS Software 라우팅 및 터널링 프로토콜 지원을 사용하여 여러 장치상에서 일어날 수 있습니다.

확장성

고용량의 보호가 필요한 경우 8 개의 모듈을 단일 스위치에 설치하여 급속하게 확장되는 대규모 환경을 지원할 수 있습니다. 또한, Cisco Anomaly Guard Module 의 멀티프로세서 아키텍처와 멀티기가비트 백플레인 인터페이스가 향후에 라이센스 소프트웨어 업그레이드를 지원하므로 모듈 당 수 기가비트의 성능이 가능합니다.

안정성 및 고가용성

Cisco Anomaly Guard Module 은 강력한 장애 복구 보호 기능이 있는 라우팅 기반의 동적 우회를 통해 강력한 주문형 정화 아키텍처를 유지합니다. 이러한 성능은 완화 기능을 활성화하는 데 필요한 기존의 인라인 솔루션이 제공하지 못하는 설치의 용이성, 운영상의 안정성 및 투명성을 제공합니다. 또한, Cisco Catalyst 6500 Series 스위치와 Cisco 7600 Series 라우터가 DDoS 차단 및 고가용성 옵션을 위해 CPP(Control Plane Policing)를 제공합니다.

관리 운용 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. 또한 애플리케이션 소프트웨어가 장치 애플리케이션 소프트웨어와 유사하므로 교육 비용이 최소화됩니다.

요약

서비스 제공업체, 호스팅 센터 및 온라인 엔터프라이즈용으로 설계된 Cisco Anomaly Guard Module 은 다른 DDoS 완화 솔루션이 수행할 수 없는 최상의 성능을 제공합니다. 즉, 가장 심각한 공격에서도 비즈니스 운영이 중단되는 것을 막아줍니다. 이러한 중요한 경쟁 우위를 통해 소중한 비즈니스 자산의 가용성을 완벽하게 보장하고 보호할 수 있습니다.

시스템 요구사항

• Cisco Anomaly Guard Module MVP-OS Software Release 4.0 이상.
• MSFC2(Multilayer Switch Feature Card 2)가 포함된 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).
• Supervisor Engine 2 에서 1 Gbps 이상의 트래픽을 처리하기 위해서 SFM(Switch Fabric Module) 필요.
• VPN Routing Forwarding(VRF)에 합법적인 트래픽을 전달하기 위해서 필요한 MPLS(Multiprotocol Label Switching)(WS-SUP720-3B 또는 WS-SUP720-3BXL)를 지원하는 Supervisor Engine 720 모듈.
• 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 됩니다.
• Cisco Catalyst 6500 Series 스위치 또는 Cisco 7600 Series 라우터에서 슬롯 1 개 점유.
• 최대 8 개의 Cisco Anomaly Guard Module 을 단일 섀시에 배치하여 로드 공유 모드에서 동일한 목적지나 다른 목적지를 보호할 수 있습니다.
Cisco Anomaly Guard 모듈과 Cisco Traffic Anomaly Detector 모듈을 동일한 섀시에 배치하는 경우 총 8 개의 모듈을 조합하여 설치할 수 있습니다.
비표준 설치에 대해서는 릴리스 노트를 참조하거나 시스코 기술 지원 대리점에 문의하십시오.
• 고가용 수퍼바이저 엔진은 SSO(Stateful Switchover) 모드를 지원하는 NSF(Nonstop Forwarding)가 사용되어야

합니다(RPR[Route Processor
Redundancy] 또는 RPR+가 아님).

호환성

최초 제품 소개(FCS) 시에 동일한 스위치나 라우터에서 Cisco Anomaly Guard Module 이 다음과 같은 장치와 호환되도록 인증됩니다.

- 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 Anomaly Guard Module 의 기능을 나타냅니다.

표 1. Cisco Anomaly Guard Module 기능

부품번호	설명
용량	• 1Gbps 인터페이스 1 개 • 최대 150,000 개의 동적 필터 • 150 만개의 동시 연결 • 1 ms 미만의 지연 시간 및 지터
클러스터링	• 동일한 비용의 다중 경로 라우팅 사용 • 특별한 로드 밸런싱 장치가 필요 없음
다중 보안 컨텍스트	• 다른 정책과 기준을 정의할 수 있는 500 개의 구역 • 동시에 우회시키고 정화할 수 있는 최대 30 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(Simple Network Management Protocol) 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 Syslogging 및 이벤트
공격 보호	• 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 Anomaly Guard Module 의 제품 사양을 나타냅니다.

표 2. 제품 사양

부품번호	설명
메모리	7 GB DDRAM, 1 GB 컴팩트 플래시
중량	• 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	116.34 인치(415 cm)
동작 온도	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+ • 시스로그
인증	• UL-승인 • CE • FCC Rules Part 15 호환

주문 정보

표 3 은 Cisco Anomaly Guard Module 의 주문 정보를 나타냅니다.

표 3. 주문 정보

제품명	부품번호	SMARTnet 번호
Cisco Catalyst 6500/Cisco 7600 Router Anomaly Guard Module	WS-SVC-AGM-1-K9	CON-SNT-WSAGMK9
Cisco Catalyst 6500/7600 Router Anomaly Guard Module MVP-OS R4.0 Software	SC-AGM-4.0-K9	

<업데이트: 2005 년 6 월 16 일>