웹 사이트 보안 및 DoS(Denial-of-Service) 공격 방지

배경

성공적인 공공 웹 사이트가 되려면 사이트로의 액세스를 장려하는 동시에 바람직하지 못한 또는 치명적인 트래픽을 제거하고 사이트의 성능이나 확장성을 제한하지 않으면서 필요한 수준의 보안을 충분히 제공해야 합니다.

DoS(denial-of-service) 공격으로 인한 서비스 중단은 포털, 전자 상거래 사이트 등 웹 중심의 기업에게는 그야말로 "죽음의 키스(kiss of death)"입니다. 1999년 실시한 컴퓨터 범죄 및 보안 상태 조사(Computer Crime and Security Survey)에 의하면 외부인에 의한 침입을 보고한 응답자의 비율이 30%로, 외부인에 의한 시스템 침입이 3년 연속 증가한 것으로 나타났습니다. 인터넷 연결을 빈번한 공격 지점으로 보고한 사람들의 비율은 1996년 전체 응답자의 37%에서 1999년 57%로 3년간 줄곧 상승세를 보였습니다.

대부분의 웹 사이트의 경우 DoS 공격을 방지하는 것이 중요합니다. 특히 이러한 공격은 정상적인 웹 트래픽처럼 보이도록 하는 방법을 이용하여 웹 사이트 작동을 중단시키기 때문에 이미 손을 쓸 수 없는 상황에서야 이를 알게 됩니다. 웹 사이트 관리자는 기본적으로 IP 라우터에서 패킷 필터링 기능을 사용하여 액세스를 제어해 왔지만, 이 경우 라우터 성능이 지나칠 정도로 저하될 수 있으며 일반적인 유형의 많은 DoS 공격을 제거하지 못합니다.

기존의 방화벽은 NAT(Network Address Translation)를 사용하고, 특정 TCP 포트를 사용하는 트래픽을 제한하여 DoS를 방지하고, 특정 네트워크 주소로부터 수신되는 트래픽을 제한하거나 트래픽을 스캐닝하여 바이러스나 바람직하지 않은 애플리케이션이 있는지 확인하는 등 IP 주소의 경계 역할을 할 수 있습니다. 그러나 이런 솔루션은 시스템에 대한 액세스 방지라는, 오늘날의 웹에는 맞지 않는 개념을 바탕으로 설계되었습니다. 뿐만 아니라 기존의 방화벽은 트래픽 용량이 극도로 증가하는 오늘날의 웹 환경에 맞게 확장할 수 없습니다.

Cisco CSS 11000 시리즈 컨텐트 서비스 스위치는 확장성이나 성능을 손상시키지 않으면서 적절한 수준의 보안을 제공하도록 설계된 광범위한 웹 사이트 및 백엔드 시스템 보안 기능을 제공합니다. 여기에는 다음과 같은 보안 기능이 포함됩니다(그림 1 참조).

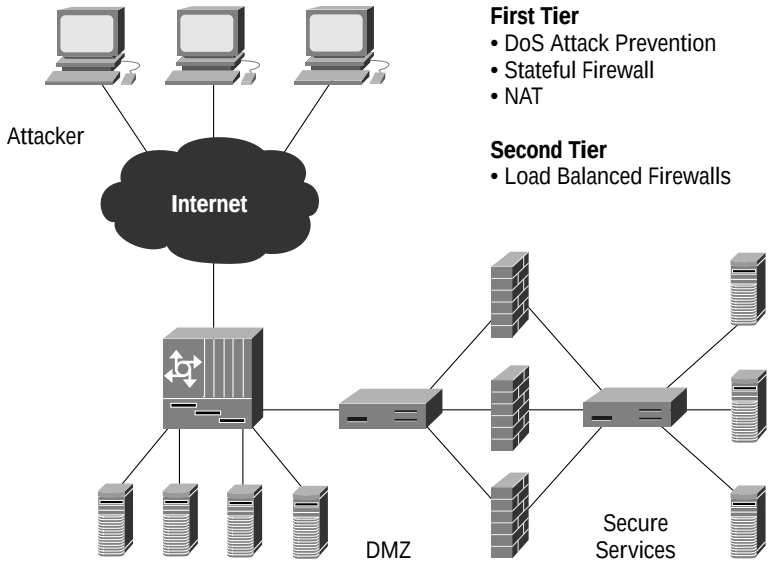
사이트 수준 보안

- ***DoS 공격 방지*** – 시스코 CSS 웹 스위치는 초기 플로우 셋업 시 모든 세션 플로우를 확인하여 시스코 CSS 웹 스위치의 성능에는 영향을 주지 않으면서 연결 기반의 모든 DoS 공격과 기타 시도된 치명적 또는 비정상적 연결을 제거합니다.
- ***FlowWall 보안*** – 시스코 CSS 웹 스위치는 IP 주소, TCP 포트, 호스트 태그, 전체 URL 또는 파일 유형별로 특정 컨텐트 요청을 차단하는 고속 ACL(Access Control List)을 포함하여 방화벽 서비스를 제공합니다.
- ***NAT(Network Address Translation)*** – 시스코 CSS 웹 스위치에서 유선 속도의 NAT 기능은 웹 서버, 캐시 등 웹 스위치 뒤에 위치한 모든 장치의 IP 주소를 숨겨 해커가 명시적 IP 주소를 사용하여 서버를 직접 공격하지 못하도록 합니다.

백엔드 시스템에 대한 보안

- ***방화벽 로드 밸런싱*** – 인터넷 경로에서 또는 핵심적인 백엔드 시스템이나 네트워크를 보호하기 위해 완벽한 방화벽 보안이 필요한 경우 Cisco CSS 11000 시리즈 스위치는 병목현상을 방지할 수 있으며, 여러 개의 로드 밸런싱된 방화벽 간에 트래픽을 분산하여 단일 장애 지점을 제거할 수 있습니다.

그림 1: 웹 사이트 보안 DoS 공격



- ***DoS 공격*** – 일반적으로 DoS 공격은 대상 웹 서버를 과부하 상태로 만들어 무력화시킬 목적으로 표준 프로토콜 또는 연결 프로세스를 악용합니다.
- ***TCP SYN 쇄도*** – 이 공격은 요청이 완료되지 않아도 반복적으로 TCP 연결 요청을 전송하여 대상 시스템이 자원을 모두 소모할 때까지 TCP 제어 블록을 할당하도록 합니다.
- ***"Smurf" 및 "fraggle" 공격*** – 이 공격은 대상 서버의 원본 주소를 위조하여 다수의 ICMP(Internet Control Message Protocol) 에코(핑) 메시지를 IP 브로드캐스트 주소로 전송합니다. 해당 브로드캐스트 주소로 트래픽을 전달하는 라우팅 장치가 레이어 2 브로드캐스트 기능에 대해 IP 브로드캐스트를 수행하기 때문에 대부분의 네트워크 호스트는 각각 ICMP 에코 요청을 받아들여 에코 응답을 발행하게 되므로 응답 중인 호스트 수에 비례하여 트래픽이 증가합니다. Fraggle은 UDP(User Datagram Protocol) 에코 메시지를 사용한다는 점을 제외하곤 smurf와 유사합니다. 멀티액세스 브로드캐스트 네트워크에서는 잠재적으로 수백 대의 시스템이 각 패킷에 응답할 수 있습니다.
- ***UNIX 프로세스 테이블 DoS 공격*** – 이 공격에서는 UNIX 서버로 개방형 연결 요청을 반복적으로 전송합니다. 모든 연결에 자동으로 응답하고 요청을 실행하도록 서브프로그램(Internet Daemon, Secure Shell Daemon, Internet Message Access Protocol Daemon 등)이 작성됩니다. 그러나 요청 없이 연결이 시작되는 경우 대부분의 디먼은 회선을 열어 둔 채로 동시에 600 – 1500개의 작업을 처리할 수 있는 서버 프로세스 테이블의 자원을 사용합니다. 연결이 반복되면 프로세스 테이블이 금방 과부하 상태가 되어 서버가 작동을 멈출 수 있습니다.
- ***Finger of death*** – 이 공격은 핑거 요청을 특정 컴퓨터로 매분마다 전송하지만 결코 연결이 끊어지지 않습니다. 프로그램 장애로 연결을 종료하지 못하면 UNIX 서버 "프로세스 테이블"이 금방 과부하 상태가 되어 ISP(Internet Service Provider)의 서비스가 몇 시간 동안 중단될 수 있습니다.

Cisco CSS 11000 시리즈 스위치는 웹 스위치 자체에는 아무런 영향을 주지 않으면서 스위치 통과를 시도하는 악성 연결 요청은 물론 앞서 설명한 모든 DoS 공격을 제거합니다.

모든 트래픽에 대한 일반 보호

Cisco CSS 11000 시리즈 스위치는 다음 경우에 프레임을 폐기합니다.

- 프레임 길이가 너무 짧은 경우
- 프레임이 단편화된 경우
- 소스 IP 주소 = IP 수신지(LAND attack)
- 소스 주소 = 시스코 주소 또는 소스가 서브넷 브로드캐스트인 경우
- 소스 주소가 유니캐스트 주소가 아닌 경우
- 소스 IP 주소가 루프백 주소인 경우
- 수신 IP 주소가 루프백 주소인 경우
- 수신 주소가 유효한 유니캐스트 또는 멀티캐스트 주소가 아닌 경우

레이어 4 및 5의 경우

스위치에서 레이어 5 규칙을 사용하여 VIP〔Virtual IP〕 주소로 전달된 HTTP(Hypertext Transfer Protocol) 플로우의 경우, 웹 스위치는 플로우가 시작되고 16초 이내에 유효한 컨텐트 프레임을 수신해야 합니다. 그렇지 못할 경우 프레임을 폐기하고 플로우를 중단합니다. 웹 스위치가 유효한 컨텐트 프레임을 수신할 때까지 서버 연결은 이루어지지 않습니다. 따라서 Cisco CSS 11000 시리즈 스위치에 의해 종료된 TCP 상태 블록이 서버 프론트에 남게 될 위험은 없습니다.

스위치에서 레이어 4 규칙을 사용하여 VIP로 전달된 TCP 플로우의 경우, 웹 스위치는 16초 이내에 3-way ACK 핸드쉐이크에 대해 리턴 ACK를 수신해야 합니다. 그렇지 못할 경우 해당 TCP 흐름을 중단합니다. 따라서 서버로 개방형 연결 요청을 반복적으로 시도하는 프로세스 테이블 DoS 공격이 제거됩니다.

8번 이상 초기 SYN을 시도한 플로우의 경우에는 웹 스위치가 플로우를 없애고(kill) 초기 시퀀스 번호, 소스 및 수신 주소와 포트 쌍이 동일한 해당 소스에서 보낸 SYS를 더 이상 처리하지 않습니다. 따라서 SYN 쇄도 DoS 공격이 제거됩니다.

NAT(Network Address Translation)

NAT는 스위치 뒤에 위치한 모든 장치의 IP 주소를 숨겨 수천 개의 사설 IP 주소(10.xxx.xxx.xxx)를 무제한으로 사용하여 전세계적으로 고유하게 할당된 IP 주소를 토대로 하나 이상의 외부 VIP에 맵핑할 수 있도록 합니다. NAT는 기존의 할당된 IP 주소, 희귀 자원을 관리하는 데도 중요하며 네트워크가 확장됨에 따라 추가로 주소를 많이 획득하지 않아도 됩니다.

NAT는 RFC 1631에 기술된 업계 표준 구현을 바탕으로 하지만 모든 포트에서 유선 속도로 완벽한 양방향 NAT를 제공할 수 있는 스위치는 Cisco CSS 11000 시리즈 스위치뿐입니다. 이 스위치는 소스 그룹 NAT도 지원하는데, 이 NAT는 서버에서 시작되어 다시 클라이언트로 이동하는 플로우(포트 기반 동적 FTP〔File Transfer Protocol〕) 또는 서버에서 시작되어 클라이언트 이외의 다른 위치로 이동하는 플로우에 NAT를 제공합니다. 따라서 사이트 성능을 저하시키지 않고 보안을 향상시킬 수 있습니다.

FlowWall 보안

신규 플로우가 감지됨과 동시에 ACL과 플로우 승인 제어를 비롯한 웹 스위치 방화벽 규칙이 호출됩니다. 모든 트래픽은 이러한 정책들이 플로우 설정의 일부로 검증된 후에 해당 플로우가 지속되는 동안 유선 속도로 스위칭됩니다. 시스코는 Cisco PIX Firewall에 필적하는 기능을 보다 빠른 속도로 제공하지만 모든 패킷을 검사하는 기존의 소프트웨어 기반 방화벽을 대체하지는 않습니다. 예를 들어, FlowWall은 인터넷에서는 일반적이지만 보안 엔터프라이즈 네트워크에서는 허용되지 않는 Java 및 Active-X 트래픽을 스캐닝하지 않습니다.

몇 가지 중요한 일반 방화벽 규칙 외에 특정 도메인 이름이나 URL(Universal Resource Locator)에 대한 정책에 맞게 웹 스위치를 구성할 수도 있습니다. 실제로 Cisco CSS 11000 시리즈 스위치는 다음 중 일부 또는 모두에 일치하는 요청에 대해 액션(포함/우회/차단)을 지정하도록 ACL을 구성할 수 있습니다.

- 소스 IP 주소
- 수신 IP 주소
- TCP 포트
- 호스트 태그
- URL
- 파일 확장명

"차단(blocking)" 규칙은 특정 컨텐트에 대한 요청이 원래 서버나 캐시로 이동하지 못하도록 합니다. PoP(Point of Presence) 또는 케이블 헤드엔드(headend)에 위치한 프론트 엔딩 캐시 서버인 스위치에서 이 기능을 사용하여 인터넷에서 특정 컨텐트에 대한 액세스를 차단할 수 있습니다.

ACL을 통해 고급 투명 캐싱 정책을 사용할 수도 있는데 예를 들면 다음과 같습니다.

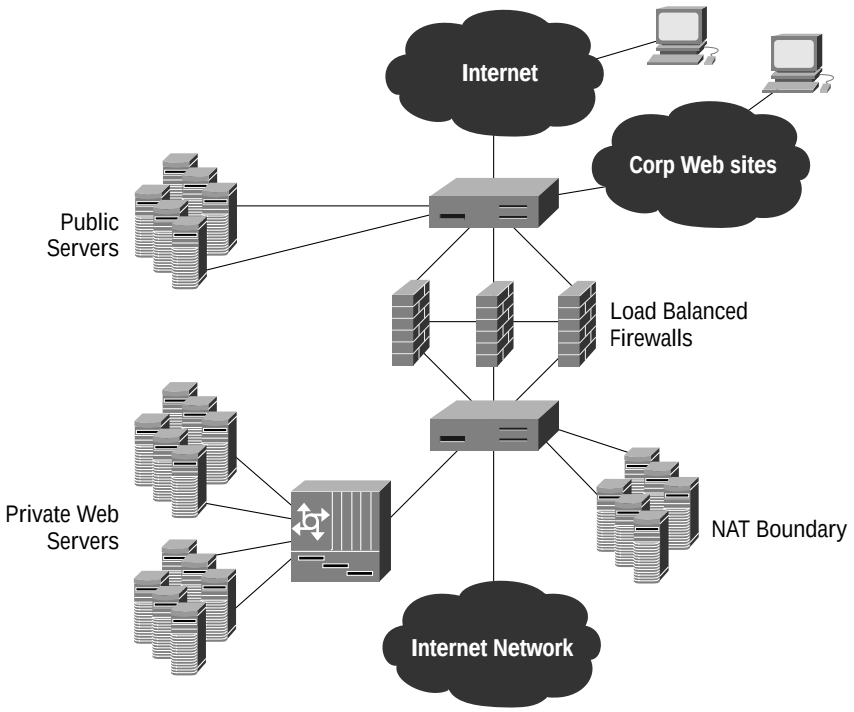
- "포함" 규칙을 사용하여 특정 컨텐트에 대한 모든 요청을 캐시로 전달하고 그 밖의 요청에 대해서는 캐시를 우회하여 특정 고객 컨텐트 공급을 최적화할 수 있습니다.
- 우회 규칙을 사용하여 특정 컨텐트에 대한 모든 요청에 대해 캐시를 우회하고 그 밖의 요청은 캐시로 전달할 수 있습니다. 기술적, 법적, 철학적 이유로 트래픽을 캐싱하는 고객들이 있는데, 이 기능을 사용하면 특정 고객의 컨텐트 중 일부 또는 전부가 캐시로 전달되지 않도록 세밀하게 제어할 수 있습니다.

방화벽 로드 밸런싱

Cisco CSS 11000 시리즈 스위치는 여러 개의 방화벽 간에 트래픽을 로드 밸런싱하여 성능 병목현상과 단일 장애점을 없애 웹 사이트, 백엔드 데이터베이스, 네트워크 또는 기타 자원에 대한 보안을 유지합니다.

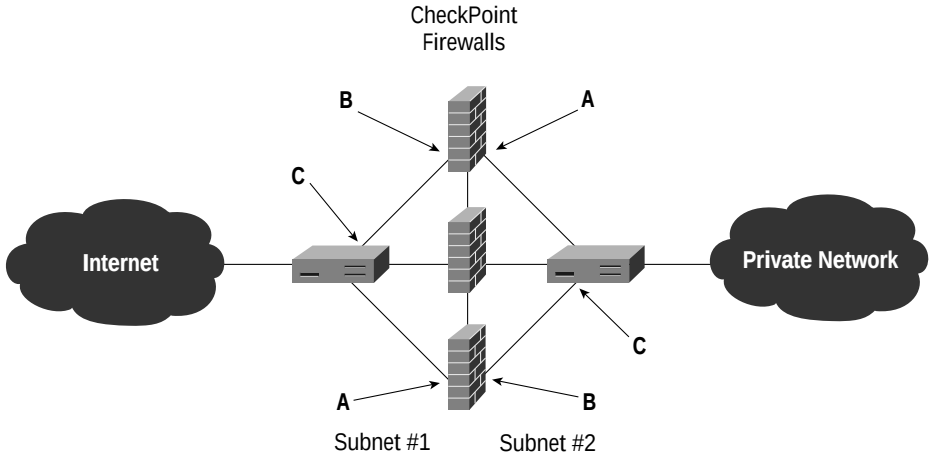
Cisco CSS 11000 시리즈 스위치는 로드 밸런싱이 이루어지고 있는 방화벽 앞, 뒤에 설치할 수 있습니다. 그림 2에서와 같이 방화벽 로드 밸런싱에 사용되지 않는 각 스위치에서 포트를 다른 용도로 구성할 수는 있지만 실제로 고유 스위치는 방화벽 양쪽에 설치됩니다.

그림 2: 엔터프라이즈 방화벽 로드 밸런싱 예



시스코 방화벽 로드 밸런싱은 고유 IP 주소를 갖고 있는 상태 저장(stateful) 방화벽 간에 트래픽을 분산하도록 설계되었습니다.

그림 3: 로드 밸런싱된 방화벽 구성

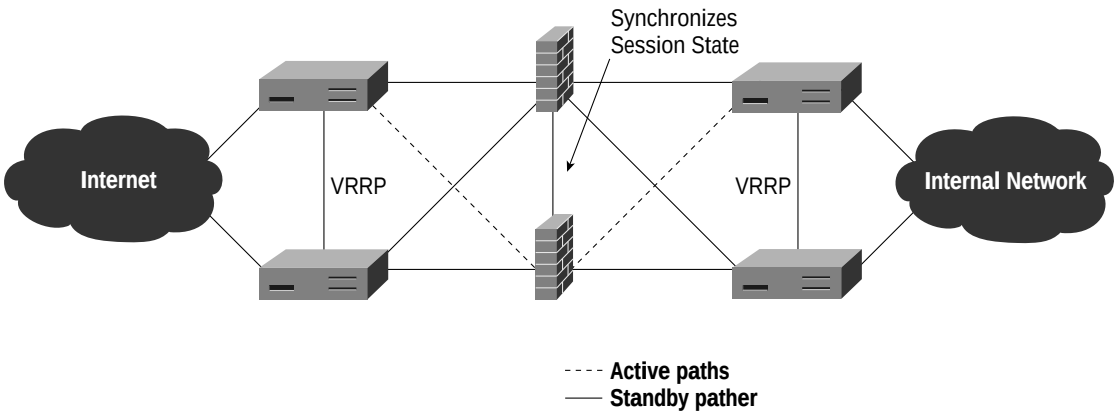


Cisco CSS 11000 시리즈 스위치는 한 쌍의 IP 주소 사이의 특정 웹 플로우에 대한 모든 트래픽이 어느 방향으로든 동일한 방화벽을 통과하도록 보장합니다. 그림 3에서와 같이 인접 방화벽 포트의 IP 주소(A), 원격 방화벽 포트의 IP 주소(B), 원격 웹 스위치 포트의 IP 주소(C)를 사용하여 각 스위치에서 정적 IP 경로를 구성하면 됩니다. 또한 로드 밸런싱된 방화벽 양쪽의 모든 포트는 서로 다른 IP 서브넷 주소를 활용하고 있습니다. 이 구성에서는 NAT를 수행하도록 방화벽을 구성할 수 없습니다. 모든 NAT 처리는 방화벽의 사설 네트워크 측에 있는 웹 스위치에서 수행됩니다.

Cisco CSS 11000 시리즈 웹 스위치는 각각 상태 검사를 사용하여 경로의 각 단계가 응답하고 있는지 확인함으로써 방화벽을 통해 인접 방화벽 포트, 원격 방화벽 포트, 원격 웹 스위치 포트 등 경로를 보안합니다. 일부 경로를 사용할 수 없는 경우, 웹 스위치는 생존 경로를 통해 모든 트래픽을 다시 라우팅합니다. 경보를 전송하거나 이벤트를 기록하여 시스템 관리자에게 장애를 알리도록 Cisco CSS 11000 시리즈 스위치를 구성할 수 있습니다. 세션 상태 정보를 공유하고 실제로 서로 연결되도록 방화벽이 구성되어 있으면 경로나 방화벽에 장애가 발생한 경우에도 사용자 세션이 중단되지 않습니다.

리던던시를 추가로 제공하기 위해 활성/비활성 구성으로 로드 밸런싱이 이루어지고 있는 방화벽 양쪽에 Cisco CSS 11000 시리즈 스위치를 여러 개 설치할 수 있습니다. 이렇게 하면 그림 4에서와 같이 방화벽과 웹 스위치 모두의 단일 장애점이 제거됩니다. 이 구성에서 비활성 웹 스위치는 활성 Cisco CSS 11000 시리즈 스위치의 상태를 모니터링하고 스위치나 업링크 장애를 감지함과 동시에 VRRP(Virtual Router Redundancy Protocol)를 사용하여 비활성 스위치 쌍으로 제어를 전송합니다.

그림 4: 완벽한 이중 방화벽 로드 밸런싱 예



결론

Cisco CSS 11000 시리즈 스위치는 성능이나 확장성을 손상시키지 않고 모든 측면의 웹 사이트 보안을 위한 포괄적인 솔루션을 제공하도록 설계되었습니다. Cisco CSS 11000 시리즈 스위치는 정교한 DoS 공격을 제거할 수 있도록 내재된 지능을 각 웹 사이트별로 고객 보안 정책을 구성할 수 있는 유연성과 결합하여 실제 고객과 정당한 사용자가 사이트를 항상 사용할 수 있도록 보장합니다.