ASA/PIX 7.x 이상:네트워크 공격 완화

목차

소개

이 문서에서는 DoS(Denial-of-Services) 등 Cisco Security Appliance(ASA/PIX)를 사용하여 다양한 네트워크 공격을 완화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 7.0 이상을 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 소프트웨어 버전 7.0 이상을 실행하는 Cisco 500 Series PIX와 함께 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

SYN 공격으로부터 보호

ASA/PIX에 대한 SYN(Transmission Control Protocol) 동기화/시작(SYN) 공격을 어떻게 완화합니까?

TCP SYN 공격

TCP SYN 공격은 발신자가 완료할 수 없는 연결 볼륨을 전송하는 DoS 공격의 유형입니다.그러면 연결 큐가 채워져 합법적인 TCP 사용자에 대한 서비스가 거부됩니다.

일반 TCP 연결이 시작되면 대상 호스트가 소스 호스트에서 SYN 패킷을 수신하고 동기화 승인(SYN ACK)을 다시 전송합니다. 그런 다음 대상 호스트에서 SYN ACK의 ACK를 수신해야 연결이 설정됩니다.이를 TCP 3방향 핸드셰이크라고 합니다.

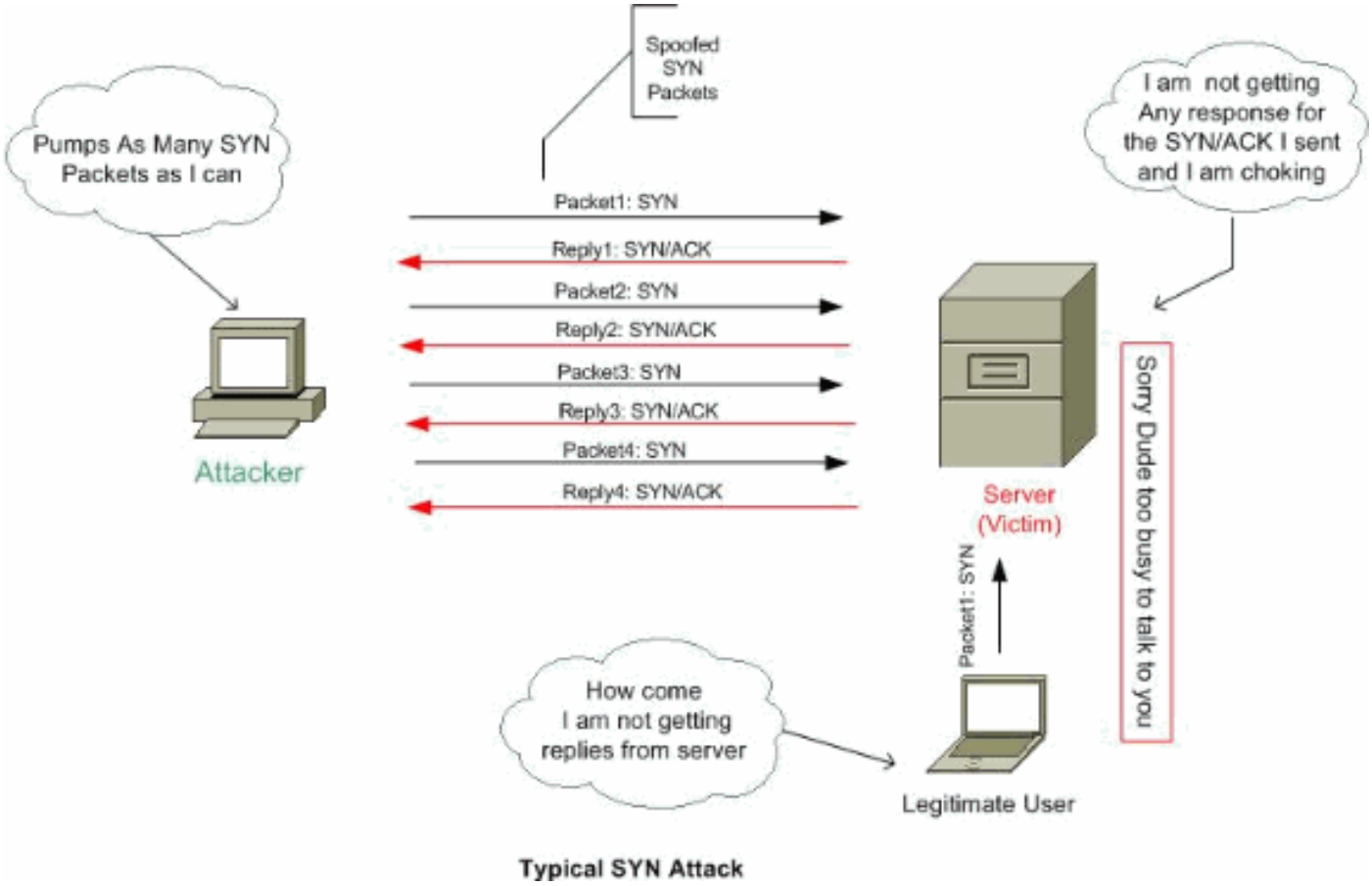
SYN ACK에 대한 ACK를 기다리는 동안 목적지 호스트의 제한된 크기의 연결 대기열이 완료되기를 기다리는 연결을 추적합니다.SYN ACK가 몇 밀리초 후에 도착할 것으로 예상되기 때문에 이 대기열은 일반적으로 빠르게 비워집니다.

TCP SYN 공격은 공격 소스 호스트가 임의의 소스 주소가 있는 TCP SYN 패킷을 피해자 호스트에 생성하도록 함으로써 이 설계를 악용합니다.피해자 대상 호스트는 SYN ACK를 임의의 소스 주소로 다시 전송하고 연결 대기열에 항목을 추가합니다.SYN ACK는 부정확하거나 존재하지 않는 호스트를 대상으로 하므로 "3방향 핸드셰이크"의 마지막 부분은 완료되지 않으며 타이머가 만료될 때까지 일반적으로 약 1분 동안 연결 대기열에 남아 있습니다.랜덤 IP 주소에서 신속하게 거짓 TCP SYN 패킷을 생성함으로써 연결 대기열을 채우고 합법적인 사용자에게 TCP 서비스(예: 이메일, 파일 전송 또는 WWW)를 거부할 수 있습니다.

소스의 IP 주소가 위조되므로 공격의 발신자를 쉽게 추적할 수 없습니다.

문제의 외부 매니페스트션에는 전자 메일을 받을 수 없거나, WWW 또는 FTP 서비스에 대한 연결을 수락할 수 없거나, SYN_RCVD 상태의 호스트에서 많은 수의 TCP 연결이 포함됩니다.

TCP SYN 공격에 대한 자세한 내용은 TCP SYN 플러딩 공격에 대한 방어를 참조하십시오.



Typical SYN Attack

완화

이 섹션에서는 최대 TCP 및 UDP(User Datagram Protocol) 연결, 최대 원시 연결 수, 연결 시간 제한 및 TCP 시퀀스 임의 지정을 비활성화하여 SYN 공격을 완화하는 방법에 대해 설명합니다.

원시 연결 제한에 도달하면 보안 어플라이언스는 SYN+ACK를 사용하여 서버로 전송되는 모든 SYN 패킷에 응답하고 SYN 패킷을 내부 서버로 전달하지 않습니다.외부 디바이스가 ACK 패킷으로 응답할 경우 보안 어플라이언스는 유효한 요청임을 알고 있으며(잠재적 SYN 공격의 일부가 아님) 그런 다음 보안 어플라이언스가 서버와의 연결을 설정하고 연결을 함께 조인합니다.보안 어플라이언스가 서버에서 ACK를 다시 가져오지 않으면 해당 초기 연결을 적극적으로 시간 초과하게 됩니다 .

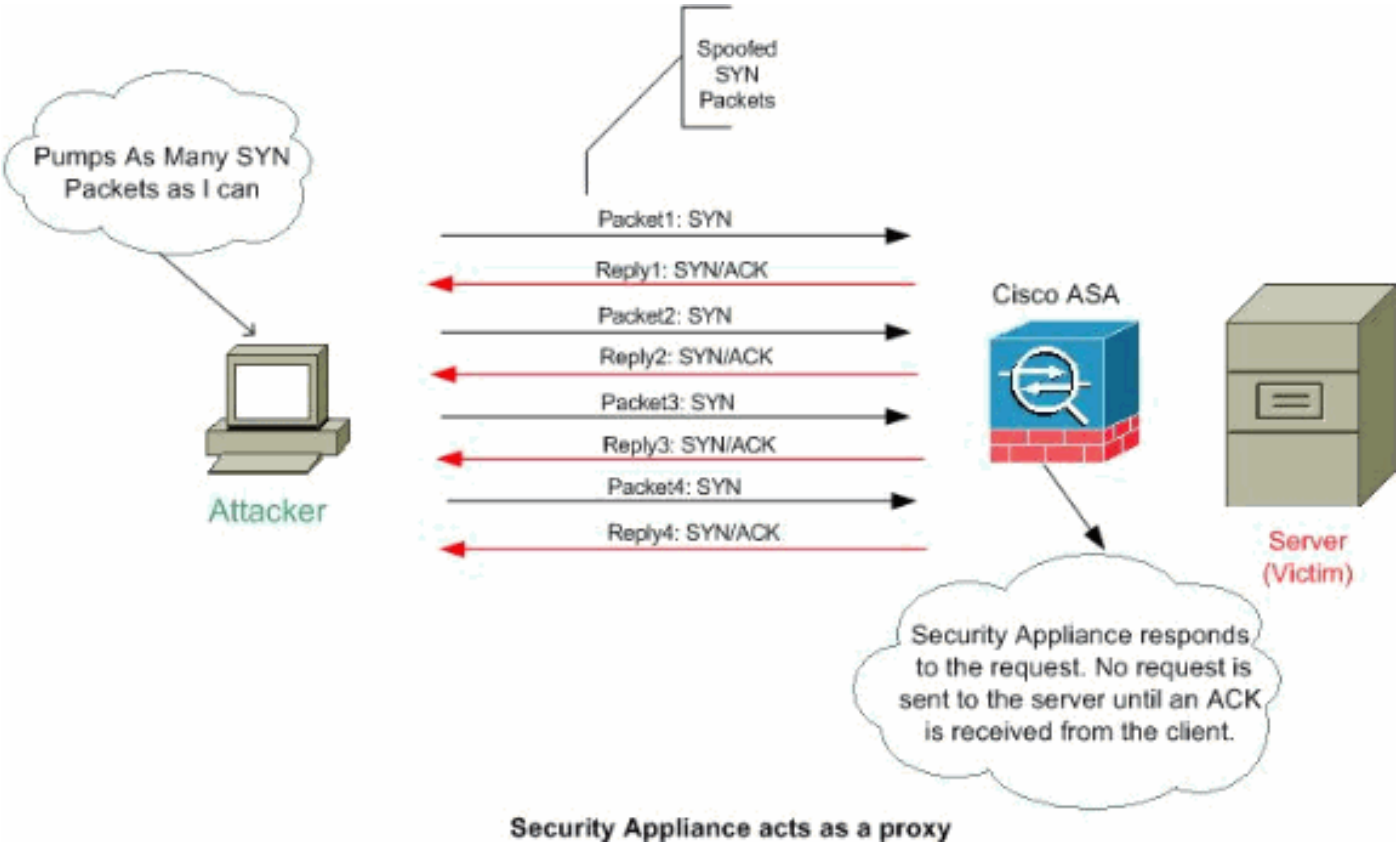
각 TCP 연결에는 두 개의 ISN(Initial Sequence Number)이 있습니다.하나는 클라이언트에 의해 생성되고 하나는 서버에 의해 생성됩니다.보안 어플라이언스는 인바운드 및 아웃바운드 방향 모두에서 전달되는 TCP SYN의 ISN을 임의로 지정합니다.

보호된 호스트의 ISN을 임의로 지정하면 공격자가 새 연결에 대한 다음 ISN을 예측하지 못하고 잠재적으로 새 세션을 가로채지 못합니다.

필요한 경우 TCP 초기 시퀀스 번호 임의 설정을 비활성화할 수 있습니다.예를 들면 다음과 같습니다.

- 또 다른 인라인 방화벽이 초기 시퀀스 번호도 임의로 지정하는 경우 두 방화벽 모두 이 작업을 수행할 필요가 없습니다. 이 작업은 트래픽에 영향을 미치지 않습니다.
- 보안 어플라이언스를 통해 eBGP(external BGP) 멀티홉을 사용하고 eBGP 피어가 MD5를 사용하는 경우 임의 설정은 MD5 체크섬을 해제합니다.
- 보안 어플라이언스가 연결의 시퀀스 번호를 임의로 지정하지 않도록 요구하는 WAAS(Wide Area Application Services) 디바이스를 사용합니다.

참고: NAT 컨피그레이션에서 최대 연결, 최대 미발달 연결 및 TCP 시퀀스 임의 설정을 구성할 수도 있습니다.두 방법을 모두 사용하여 동일한 트래픽에 대해 이러한 설정을 구성하는 경우 보안 어플라이언스는 더 낮은 제한을 사용합니다.TCP 시퀀스 임의 지정의 경우, 두 방법 중 하나를 사용하여 비활성화된 경우 보안 어플라이언스는 TCP 시퀀스 임의 지정을 비활성화합니다.



Security Appliance acts as a proxy

연결 제한을 설정하려면 다음 단계를 완료하십시오.

1. 트래픽을 식별하려면 Modular Policy Framework 사용에 따라 **class-map** 명령을 사용하여 클래스 맵을 추가합니다.
2. 클래스 맵 트래픽과 함께 수행할 작업을 설정하는 **정책 맵**을 추가하거나 편집하려면 다음 명령을 입력합니다.
   ```
   hostname(config)#policy-map name
   ```
3. 작업을 할당할 클래스 맵(1단계)을 식별하려면 다음 명령을 입력합니다.
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. 최대 연결(TCP와 UDP 모두), 최대 원시 연결 수, per-client-embryonic-max, per-client-max 또는 TCP 시퀀스 임의 지정을 비활성화할지 여부를 설정하려면 다음 명령을 입력합니다.
   ```
   hostname(config-pmap-c)#set connection {[conn-max number]
   [embryonic-conn-max number] [per-client-embryonic-max number]
   [per-client-max number][random-sequence-number {enable |
   disable}}
   ```
   여기서 number는 0에서 65535 사이의 정수입니다. 기본값은 0이며, 이는 연결의 제한을 의미하지 않습니다.한 줄에 모두 이 명령을 입력하거나(임의의 순서로) 각 특성을 별도의 명령으로 입력할 수 있습니다.이 명령은 실행 중인 컨피그레이션에서 한 줄로 결합됩니다.
5. 연결, 미발달 연결(절반이 열린) 및 절반이 닫힌 연결에 대한 시간 제한을 설정하려면 다음 명령을 입력합니다.
   ```
   hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
   [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
   ```
   여기서 **embryonic hh**[:mm[:ss]는 0:0:5에서 1192:59:59 사이의 시간입니다. 기본값은

0:0:30입니다. 이 값을 0으로 설정할 수도 있습니다. 즉 연결이 시간 초과되지 않습니다.**half-closed hh**[:mm[:ss] 및 **tcp** hh[:mm[:ss] 값은 0:5:0에서 1192:59:59 사이의 시간입니다. **half-closed의** 기본값은 0:10:0이고 tcp의 기본값은 1:0:0입니다. 이 값을 0으로 설정할 수도 있습니다. 즉, 연결이 시간 초과되지 않음을 의미합니다.한 줄에 모두 이 명령을 입력하거나(임의의 순서로) 각 특성을 별도의 명령으로 입력할 수 있습니다.이 명령은 실행 중인 컨피그레이션에서 한 줄로 결합됩니다.**Embryonic(Half-opened) connection** - 원시 연결은 소스와 대상 간의 필요한 핸드셰이크를 완료하지 않은 TCP 연결 요청입니다.**Half-closed connection(절반이 닫힌 연결) -** 절반이 닫힌 연결은 FIN을 전송하여 한 방향으로만 연결이 닫힌 경우입니다.그러나 TCP 세션은 피어에서 계속 유지됩니다.**Per-client-embryonic-max**—클라이언트당 허용되는 최대 동시 원시 연결 수(0~65535). 기본값은 0이며 무제한 연결을 허용합니다.**Per-client-max**—클라이언트당 허용되는 최대 동시 연결 수(0~65535)입니다. 기본값은 0이며 무제한 연결을 허용합니다.

6. 하나 이상의 인터페이스에서 정책 맵을 활성화하려면 다음 명령을 입력합니다.
   hostname(config)#**service-policy policymap_name** *{global | interface interface_name}*

   여기서 **global**은 모든 인터페이스에 정책 맵을 적용하고 **인터페이스**는 하나의 인터페이스에 정책을 적용합니다.하나의 전역 정책만 허용됩니다.해당 인터페이스에 서비스 정책을 적용하여 인터페이스에서 전역 정책을 재정의할 수 있습니다.각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

예:

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

참고: 특정 호스트에 대한 총 절반이 열린 세션 수를 확인하려면 다음 명령을 사용합니다.

```
ASA-5510-8x# show local-host all

Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
Interface xx: 0 active, 0 maximum active, 0 denied
Interface inside: 7 active, 18 maximum active, 0 denied

local host: <10.78.167.69>,

    TCP flow count/limit = 2/unlimited

    TCP embryonic count to host = 0

    TCP intercept watermark = unlimited
```

```
UDP flow count/limit = 0/unlimited
```

참고: `TCP` 수의 회선은 절반이 열린 세션 수를 표시합니다.

IP 스푸핑 공격으로부터 보호

PIX/ASA가 IP 스푸핑 공격을 차단할 수 있습니까?

IP 스푸핑

액세스를 얻기 위해 침입자는 스푸핑된 소스 IP 주소를 사용하여 패킷을 생성합니다.이 기능은 IP 주소를 기반으로 인증을 사용하는 애플리케이션을 악용하여 인증되지 않은 사용자 및 대상 시스템의 루트 액세스를 유도합니다.예를 들면 rsh 및 rlogin 서비스가 있습니다.

소스 주소가 로컬 도메인에 있는 수신 패킷을 필터링하도록 구성되지 않은 경우 필터링 라우터 방화벽을 통해 패킷을 라우팅할 수 있습니다.설명한 공격은 응답 패킷이 공격자에게 도달할 수 없더라도 가능합니다.

잠재적으로 취약한 구성의 예는 다음과 같습니다.

- 프록시 애플리케이션에서 인증에 소스 IP 주소를 사용하는 프록시 방화벽
- 여러 내부 인터페이스를 지원하는 외부 네트워크에 대한 라우터
- 내부 네트워크에서 서브넷을 지원하는 두 개의 인터페이스가 있는 라우터

완화

uRPF(Unicast Reverse Path Forwarding)는 라우팅 테이블에 따라 올바른 소스 인터페이스와 일치하는 소스 IP 주소가 모든 패킷에 있는지 확인하여 IP 스푸핑(패킷은 잘못된 소스 IP 주소를 사용하여 진정한 소스를 가려냅니다)을 차단합니다.

일반적으로 보안 어플라이언스는 패킷을 전달할 위치를 결정할 때 목적지 주소만 확인합니다.유니캐스트 RPF는 보안 어플라이언스에 소스 주소도 확인하도록 지시합니다.따라서 Reverse Path Forwarding이라고 **합니다**.보안 어플라이언스를 통해 허용하려는 트래픽의 경우 보안 어플라이언스 라우팅 테이블에 소스 주소로 돌아가는 경로가 포함되어야 합니다.자세한 내용은 RFC 2267 을 참조하십시오.

참고: `- %PIX-1-106021:reverse path check int_name` 로그 메시지 `src_addr dest_addr`까지의 프로토콜 을 거부할 수 있습니다.이 문제를 해결하려면 **no ip verify reverse-path interface (interface name)** 명령을 사용하여 reverse path check를 비활성화합니다.

`no ip verify reverse-path interface (interface name)`

예를 들어 외부 트래픽의 경우 보안 어플라이언스는 기본 경로를 사용하여 유니캐스트 RPF 보호를 충족할 수 있습니다.외부 인터페이스에서 트래픽이 들어오고 소스 주소를 라우팅 테이블에 알지 못하는 경우 보안 어플라이언스는 기본 경로를 사용하여 외부 인터페이스를 소스 인터페이스로 올바르게 식별합니다.

트래픽이 라우팅 테이블에 알려진 주소에서 외부 인터페이스로 진입하지만 내부 인터페이스와 연결된 경우 보안 어플라이언스는 패킷을 삭제합니다.마찬가지로, 트래픽이 알 수 없는 소스 주소에서 내부 인터페이스로 들어가면 일치하는 경로(기본 경로)가 외부 인터페이스를 나타내므로 보안

어플라이언스가 패킷을 삭제합니다.

유니캐스트 RPF는 다음과 같이 구현됩니다.

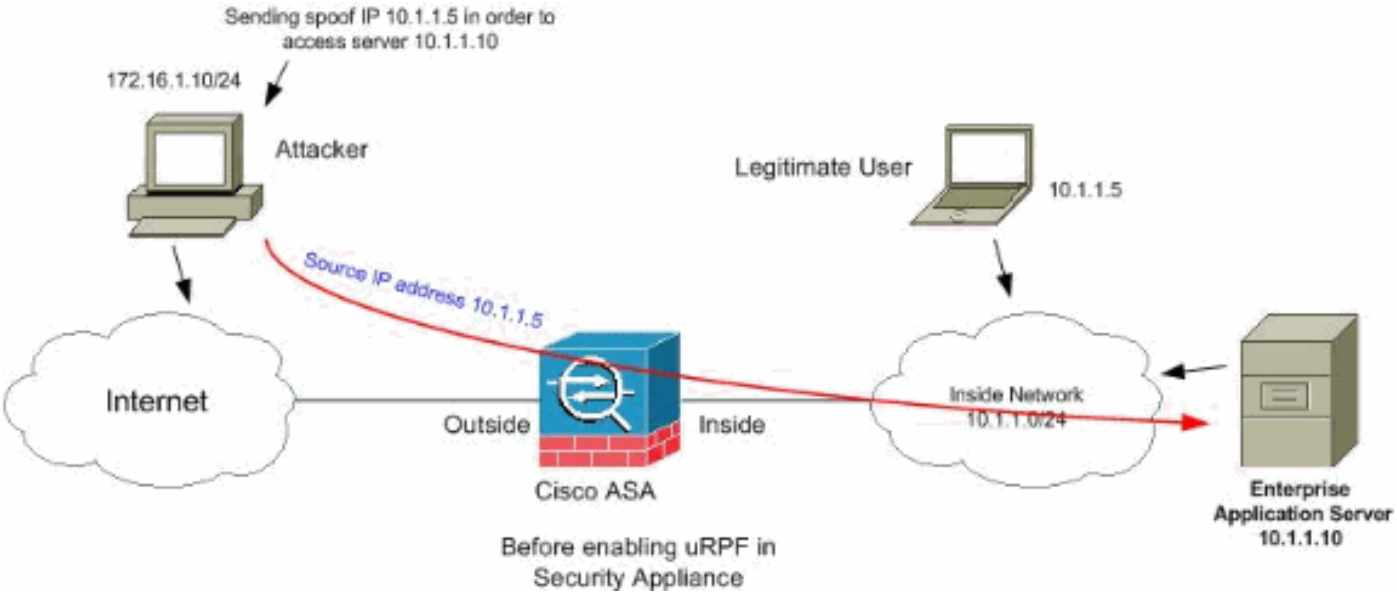
- ICMP 패킷에는 세션이 없으므로 각 패킷이 검사됩니다.
- UDP 및 TCP에는 세션이 있으므로 초기 패킷에는 역방향 경로 조회가 필요합니다.세션 중에 도착하는 후속 패킷은 세션의 일부로 유지되는 기존 상태를 사용하여 점검됩니다.초기 패킷이 아닌 패킷이 초기 패킷에서 사용하는 동일한 인터페이스에 도착했는지 확인합니다.

유니캐스트 RPF를 활성화하려면 다음 명령을 입력합니다.

```
hostname(config)#ip verify reverse-path interface interface_name
```

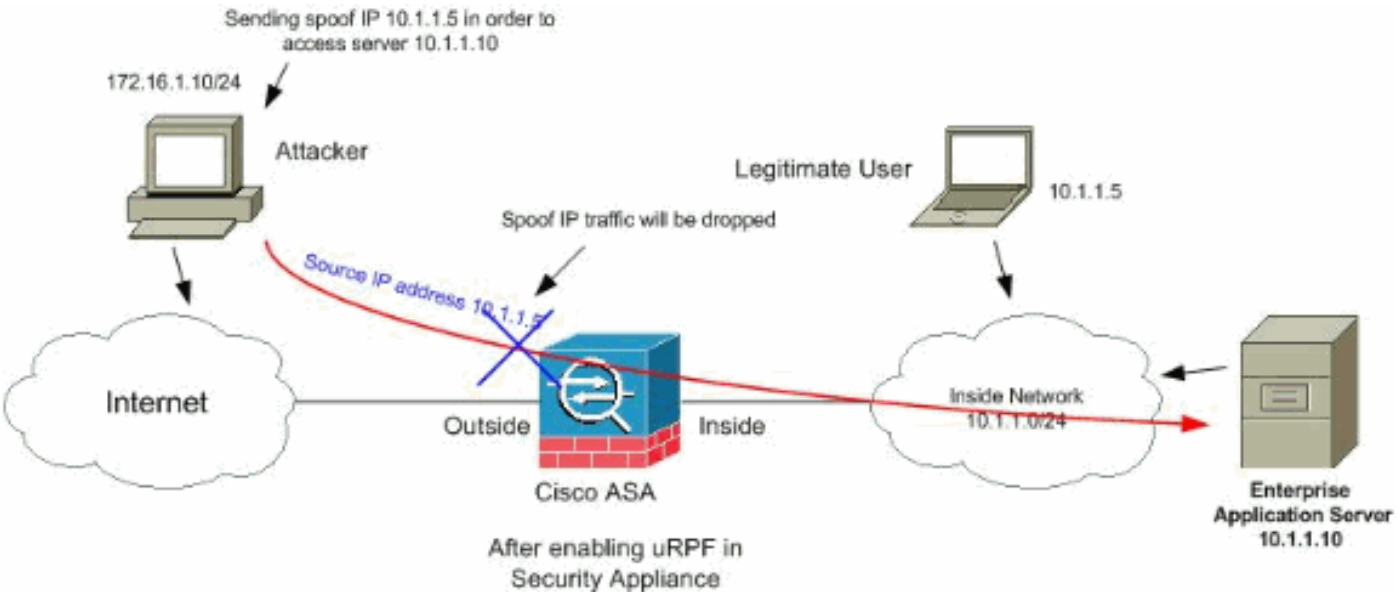
예:

이 그림에서 볼 수 있듯이 공격자 PC는 위조된 소스 IP 주소가 10.1.1.5/24인 패킷을 전송하여 애플리케이션 서버 10.1.1.10에 대한 요청을 시작하고 서버는 요청에 대한 응답으로 실제 IP 주소 10.1.1.5/24으로 패킷을 전송합니다.이러한 유형의 불법 패킷은 내부 네트워크의 애플리케이션 서버와 합법적인 사용자 모두를 공격합니다.



유니캐스트 RPF는 소스 주소 스푸핑을 기반으로 공격을 방지할 수 있습니다.다음과 같이 ASA의 외부 인터페이스에서 uRPF를 구성해야 합니다.

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Syslog 메시지를 사용하여 스푸핑 식별

보안 어플라이언스는 표시된 대로 계속해서 syslog 오류 메시지를 수신합니다.이는 스푸핑된 패킷을 사용하거나 비대칭 라우팅으로 인해 트리거될 수 있는 잠재적인 공격을 나타냅니다.

1.

%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name

설명연결 관련 메시지입니다.이 메시지는 지정된 트래픽 유형에 대해 정의된 보안 정책에서 내부 주소에 연결하려는 시도가 거부될 때 발생합니다.가능한 *tcp_flags* 값은 연결이 거부되었을 때 있었던 TCP 헤더의 플래그에 해당합니다.예를 들어 보안 어플라이언스에 연결 상태가 없는 TCP 패킷이 도착하여 삭제되었습니다.이 패킷의 *tcp_flags*는 FIN 및 ACK입니다 .tcp_*flags*는 다음과 같습니다.ACK - 승인 번호가 수신되었습니다.FIN - 데이터가 전송되었습니다.PSH - 수신자가 애플리케이션에 데이터를 전달했습니다.RST - 연결이 재설정되었습니다.SYN - 연결을 시작하기 위해 시퀀스 번호가 동기화되었습니다.URG - 긴급 포인터가 유효한 것으로 선언되었습니다.PIX/ASA에서 정적 변환이 실패하는 데에는 여러 가지 이유가 있습니다.그러나 일반적인 이유는 DMZ(demilitarized zone) 인터페이스가 외부 인터페이스와 동일한 보안 레벨(0)으로 구성된 경우입니다.이 문제를 해결하려면 모든 인터페이스에 다른 보안 수준을 할당하십시오.자세한 내용은 인터페이스 매개변수 구성을 참조하십시오.이 오류 메시지는 외부 디바이스가 PIX 방화벽에 의해 삭제된 내부 클라이언트로 IDENT 패킷을 전송하는 경우에도 나타납니다.자세한 내용은 IDENT 프로토콜로 인해 발생한 PIX 성능 문제를 참조하십시오.

2.

%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}

설명연결 관련 메시지입니다.이 메시지는 아웃바운드 **deny** 명령으로 인해 지정된 연결이 실패하는 경우 표시됩니다.프로토콜 변수는 ICMP, TCP 또는 UDP일 수 있습니다.**권장 작업:**아웃바운드 **목록을** 확인하려면 show outbound 명령을 사용합니다.

3.

%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)

설명보안 어플라이언스가 인바운드 ICMP 패킷 액세스를 거부했습니다.기본적으로 모든 ICMP 패킷은 특별히 허용되지 않는 한 액세스가 거부됩니다.

4.
```
%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on
interface interface_name.
```
설명이 메시지는 패킷이 보안 어플라이언스 인터페이스의 대상 IP 주소 0.0.0.0 및 대상 MAC 주소가 있는 보안 어플라이언스 인터페이스에 도착하면 생성됩니다.또한 이 메시지는 보안 어플라이언스가 다음 중 하나 또는 일부 잘못된 다른 주소를 포함할 수 있는 잘못된 소스 주소의 패킷을 폐기한 경우 생성됩니다.루프백 네트워크(127.0.0.0)브로드캐스트(제한적, net-directed, subnet-directed, all-subnets-directed)대상 호스트(land.c)스푸핑 패킷 탐지를 더욱 개선하려면 **icmp** 명령을 사용하여 보안 어플라이언스가 내부 네트워크에 속하는 소스 주소가 있는 패킷을 삭제하도록 구성합니다.**access-list** 명령은 더 이상 사용되지 않으며 제대로 작동하지 않을 수 있기 때문입니다.**권장 작업:**외부 사용자가 보호된 네트워크를 손상하려고 하는지 확인합니다.잘못 구성된 클라이언트를 확인합니다.

5.
```
%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to
IP_address
```
설명보안 어플라이언스가 IP 소스 주소가 IP 대상과 같고 대상 포트가 소스 포트와 같은 패킷을 받았습니다.이 메시지는 시스템을 공격하도록 설계된 스푸핑된 패킷을 나타냅니다.이 공격을 "토지 공격"이라고 합니다.**권장 작업:**이 메시지가 지속되면 공격이 진행 중일 수 있습니다.패킷이 공격이 발생한 위치를 확인할 수 있는 충분한 정보를 제공하지 않습니다.

6.
```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```
설명공격이 진행 중입니다.누군가 인바운드 연결에서 IP 주소를 스푸핑하려고 합니다.역방향 경로 조회라고도 하는 유니캐스트 RPF는 라우트로 표시되는 소스 주소가 없는 패킷을 탐지했으며 보안 어플라이언스에 대한 공격의 일부라고 가정합니다.이 메시지는 **ip verify reverse-path** 명령으로 유니캐스트 RPF를 활성화한 경우 나타납니다.이 기능은 인터페이스에 대한 패킷 입력에서 작동합니다.외부에 구성된 경우 보안 어플라이언스는 외부에서 도착하는 패킷을 확인합니다.보안 어플라이언스는 소스 주소를 기반으로 경로를 찾습니다.항목을 찾을 수 없고 경로가 정의되지 않은 경우 이 시스템 로그 메시지가 나타나고 연결이 삭제됩니다.경로가 있는 경우 보안 어플라이언스는 해당하는 인터페이스를 확인합니다.패킷이 다른 인터페이스에 도착한 경우 스푸프이거나 대상에 대한 경로가 둘 이상인 비대칭 라우팅 환경이 있습니다.보안 어플라이언스는 비대칭 라우팅을 지원하지 않습니다.보안 어플라이언스가 내부 인터페이스에 구성된 경우 고정 **route** 명령문 또는 RIP를 확인합니다.소스 주소를 찾을 수 없으면 내부 사용자가 주소를 스푸핑하고 있습니다.**권장 작업:**공격이 진행 중이지만 이 기능이 활성화된 경우 사용자 작업이 필요하지 않습니다.보안 어플라이언스가 공격을 대응합니다.**참고:** show asp **drop** 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로(asp)에서 삭제한 패킷 또는 연결을 표시합니다.또한 asp drop 카운터가 마지막으로 지워진 시간을 나타냅니다.인터페이스에 **ip verify reverse-path**가 구성되고 보안 어플라이언스에서 소스 IP의 경로 조회가 패킷을 수신한 것과 동일한 인터페이스를 산출하지 않은 패킷을 수신하면 카운터가 증가되는 **show asp drop rpf-violated** 명령을 사용합니다.
```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                       2
```
참고: 권장 사항:다음 시스템 메시지에 인쇄된 소스 IP를 기반으로 트래픽의 소스를 추적하고 스푸핑된 트래픽을 보내는 이유를 조사합니다.**참고: 시스템 로그 메시지:**106021

7.
```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```
설명연결과 일치하는 패킷이 연결이 시작된 인터페이스와는 다른 인터페이스에 도착합니다

.예를 들어 사용자가 내부 인터페이스에서 연결을 시작하지만 보안 어플라이언스가 경계 인터페이스에 도달하는 동일한 연결을 탐지하면 보안 어플라이언스는 대상에 대한 경로가 두 개 이상 있습니다.이를 비대칭 라우팅이라고 하며 보안 어플라이언스에서 지원되지 않습니다.또한 공격자는 보안 어플라이언스에 침입하는 방법으로 한 연결에서 다른 연결로 패킷을 추가하려고 시도할 수 있습니다.두 경우 모두 보안 어플라이언스가 이 메시지를 표시하고 연결을 삭제합니다.**권장 조치:**이 메시지는 **ip verify reverse-path** 명령이 구성되지 않은 경우 나타납니다.라우팅이 비대칭적이지 않은지 확인합니다.

8.
```
%PIX|ASA-4-106023: Deny protocol src
[interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by
access_group acl_ID
```
설명ACL에서 IP 패킷을 거부했습니다.ACL에 대해 **log** 옵션이 활성화되지 않은 경우에도 이 메시지가 표시됩니다.**권장 조치:**메시지가 동일한 소스 주소에서 계속 전송될 경우, 발판 또는 포트 검사 시도를 나타내는 메시지가 표시될 수 있습니다.원격 호스트 관리자에게 문의하십시오.

9.
```
%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet
from sip/sport to dip/dport on interface if_name.
```
10.
```
%ASA-4-419002: Received duplicate TCP SYN from
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
different initial sequence number.
```
설명이 시스템 로그 메시지는 방화벽 디바이스를 통해 새 연결을 설정하면 구성된 최대 연결 제한 중 하나 이상을 초과하게 됩니다.시스템 로그 메시지는 static 명령을 사용하여 구성된 연결 제한 또는 Cisco Modular Policy Framework를 사용하여 구성된 연결 제한에 모두 적용됩니다.기존 연결 중 하나가 해제될 때까지 방화벽 디바이스를 통해 새 연결이 허용되지 않으므로 현재 연결 수가 구성된 최대 연결 수 이하로 설정됩니다.*cnt* - 현재 연결 수*limit* - 구성된 연결 제한*dir* - 트래픽, 인바운드 또는 아웃바운드 방향*sip* - 소스 IP 주소*sport* - 소스 포트*dip* - 대상 IP 주소*dport* - 대상 포트*if_name*—트래픽 유닛이 수신되는 인터페이스의 이름(Primary 또는 Secondary)입니다.**권장 조치:**연결 제한은 적절한 이유로 구성되므로 이 시스템 로그 메시지는 가능한 DoS 공격을 나타낼 수 있습니다. 이 경우 트래픽의 소스가 스푸핑된 IP 주소일 수 있습니다.소스 IP 주소가 완전히 무작위가 아닌 경우, 소스를 식별하여 액세스 목록을 사용하여 차단하는 것이 도움이 될 수 있습니다.다른 경우에는 스니퍼 추적을 가져오고 트래픽의 소스를 분석하면 원치 않는 트래픽을 합법적인 트래픽에서 격리하는 데 도움이 됩니다.

ASA 8.x의 기본 위협 탐지 기능

Cisco Security Appliance ASA/PIX는 소프트웨어 버전 8.0 이상에서 위협 탐지라는 기능을 지원합니다.보안 어플라이언스는 기본 위협 탐지를 사용하여 다음과 같은 이유로 인해 삭제된 패킷 및 보안 이벤트의 속도를 모니터링합니다.

- 액세스 목록에 의한 거부
- 잘못된 패킷 형식(예: invalid-ip-header 또는 invalid-tcp-hdr-length)
- 연결 제한 초과(시스템 차원의 리소스 제한 및 구성에 설정된 제한 모두)
- DoS 공격 감지(예: 잘못된 SPI, 상태 저장 방화벽 확인 실패)
- 기본 방화벽 검사 실패(이 옵션은 이 글머리 기호 목록의 모든 방화벽 관련 패킷 삭제를 포함하는 결합된 속도입니다.여기에는 인터페이스 오버로드, 애플리케이션 검사에서 실패한 패킷, 탐지된 스캔 공격 등 방화벽과 관련 없는 삭제는 포함되지 않습니다.)
- 의심스러운 ICMP 패킷 감지

- 애플리케이션 검사에 실패한 패킷
- 인터페이스 오버로드
- 스캔 공격 감지(이 옵션은 스캔 공격을 모니터링합니다.예를 들어 첫 번째 TCP 패킷이 SYN 패킷이 아니거나 TCP 연결이 3방향 핸드셰이크에 실패했습니다.전체 스캐닝 위협 탐지(자세한 내용은 스캐닝 위협 탐지 구성 참조)는 이 스캐닝 공격 속도 정보를 가져와 호스트를 공격자로 분류하고 자동으로 차단하는 등의 방식으로 수행합니다.
- TCP SYN 공격 감지 또는 데이터 UDP 세션 공격 감지 등과 같은 불완전한 세션 감지

보안 어플라이언스가 위협을 탐지하면 즉시 시스템 로그 메시지(730100)를 전송합니다.

기본 위협 감지는 중단이나 잠재적 위협이 있는 경우에만 성능에 영향을 미칩니다.이 시나리오에서도 성능에 미치는 영향은 미미합니다.

보안 어플라이언스에 **로그인했을** 때 잠재적 공격을 식별하기 위해 show threat-detection rate 명령을 사용합니다.

```
ciscoasa#show threat-detection rate
                          Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                0               0       0                16
  1-hour ACL  drop:                0               0       0               112
  1-hour SYN attck:                5               0       2             21438
  10-min  Scanning:                0               0      29               193
  1-hour  Scanning:              106               0      10            384776
  1-hour Bad  pkts:               76               0       2            274690
  10-min  Firewall:                0               0       3                22
  1-hour  Firewall:               76               0       2            274844
  10-min DoS attck:                0               0       0                 6
  1-hour DoS attck:                0               0       0                42
  10-min Interface:                0               0       0               204
  1-hour Interface:               88               0       0            318225
```

컨피그레이션 부분에 대한 자세한 내용은 ASA 8.0 컨피그레이션 가이드의 기본 위협 탐지 구성 섹션을 참조하십시오.

Syslog 메시지 733100

오류 메시지:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
```

시스템 로그 메시지에 지정된 개체가 지정된 버스트 임계값 속도 또는 평균 임계값 속도를 초과했습니다.개체는 잠재적인 공격으로 인해 호스트, TCP/UDP 포트, IP 프로토콜 또는 다양한 삭제의 활동을 삭제할 수 있습니다.시스템이 잠재적인 공격 상태임을 나타냅니다.

참고: 이 오류 메시지는 ASA 8.0 이상에만 적용됩니다.

1. Object(개체) - 삭제 속도 카운트의 일반 또는 특정 소스(다음 항목이 포함될 수 있음).방화벽잘못된 패킷속도 제한DoS 공격ACL 삭제연결 제한ICMP 공격검사 중SYN 공격검사인터페이스
2. rate_ID - 초과 중인 구성된 비율입니다.대부분의 객체는 서로 다른 간격으로 최대 3개의 서로 다른 속도로 구성할 수 있습니다.
3. rate_val - 특정 비율 값입니다.
4. total_cnt - 개체를 만들거나 지운 이후의 총 수입니다.

다음 세 가지 예는 이러한 변수가 발생하는 방법을 보여줍니다.

- CPU 또는 버스 제한으로 인한 인터페이스 삭제:
```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
    second,
max configured rate is 8000; Current average rate is 2030 per second,
max configured rate is 2000; Cumulative total count is 3930654
```
- 잠재적 공격으로 인한 스캔 삭제:
```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
    second_
max configured rate is 10; Current average rate is 245 per second_
max configured rate is 5; Cumulative total count is 147409 (35 instances received)
```
- 잠재적인 공격으로 인한 불량 패킷의 경우:
```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
    second,
max configured rate is 400; Current average rate is 760 per second,
max configured rate is 100; Cumulative total count is 1938933
```

권장 작업:

메시지에 나타나는 지정된 객체 유형에 따라 다음 단계를 수행합니다.

1. syslog 메시지의 객체가 다음 중 하나인 경우방화벽잘못된 패킷속도 제한DoS 공격ACL 삭제 연결 제한ICMP 공격검사 중SYN 공격검사인터페이스실행 중인 환경에서 삭제 속도가 허용되는지 확인합니다.
2. **threat-detection rate** ***xxx*** 명령을 실행하여 특정 드롭의 임계값 속도**를** 적절한 값으로 조정합니다. 여기서 xxx는 다음 중 하나입니다.acl-dropbad packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-drop스캐닝 위협syn 공격
3. syslog 메시지의 객체가 TCP 또는 UDP 포트, IP 프로토콜 또는 호스트 삭제인 경우 실행 중인 환경에 대해 삭제 속도가 허용되는지 확인합니다.
4. **threat-detection rate bad-packet-drop** 명령을 실행하여 특정 드롭의 임계값 속도**를 적절한 값으로** 조정합니다.자세한 내용은 ASA 8.0 컨피그레이션 가이드의 Configuring Basic Threat Detection 섹션을 참조하십시오.

참고: 삭제 속도가 경고를 초과하지 않도록 하려면 no threat-**detection basic-threat** 명령을 실행하여 이를 비활성화할 수 있습니다.

관련 정보

- Cisco 5500 Series Adaptive Security Appliances 지원 페이지
- Cisco 500 Series PIX 지원 페이지
- TCP SYN 플러딩 공격에 대한 방어
- Cisco 적용 완화 게시판:Content Switching Module에서 Denial of Service Vulnerabilities 활용 식별 및 완화
- Cisco 적용 완화 게시판:Cisco PIX 및 ASA 어플라이언스 및 방화벽 서비스 모듈에서 여러 취약성 익스플로잇 식별 및 완화
- IP 스푸핑
- 기술 지원 및 문서 – Cisco Systems