ASA 성능 문제 모니터링 및 문제 해결

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)의 성능을 모니터링하고 문제를 해결하는 데 사용할 명령에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 버전 8.3 이상을 실행하는 Cisco 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

성능 문제 해결

성능 문제를 해결하려면 이 섹션에 설명된 기본 영역을 확인하십시오.

참고: show Cisco 디바이스의 명령 출력이 있는 경우 Cisco CLI Analyzer를 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다. Cisco CLI Analyzer는 특정 명령을 show 지원합니다. Cisco CLI Analyzer를 사용하는 경우 등록된 Cisco 사용자여야 하며, Cisco 계정에 로그인해야 하며, 브라우저에서 JavaScript를 활성화해야 합니다.

속도 및 이중 설정

보안 어플라이언스는 인터페이스에서 속도 및 듀플렉스 설정을 자동으로 탐지하도록 사전 구성되어 있습니다. 그러나 자동 협상 프로세스가 실패하여 속도 또는 이중 불일치(및 성능 문제)가 발생할 수 있는 몇 가지 상황이 있습니다. 미션 크리티컬 네트워크 인프라의 경우, Cisco는 각 인터페이스의 속도와 듀플렉스를 수동으로 하드코딩하므로 오류가 발생할 가능성이 없습니다. 이러한 디바이스는 일반적으로 이동하지 않으므로 올바르게 구성하면 변경할 필요가 없습니다.

모든 네트워크 디바이스에서 링크 속도를 감지할 수 있지만 이중 모드를 협상해야 합니다. 두 네트워크 디바이스가 속도와 듀플렉스를 자동으로 협상하도록 구성된 경우, 속도 및 듀플렉스 기능을 알리는 프레임(FLP(Fast Link Pulse)이라고 함)을 교환합니다. 인지하지 못하는 링크 파트너를 위해 이러한 펄스는 일반 10Mbps 프레임과 유사합니다. 펄스를 디코딩할 수 있는 링크 파트너를 위해 FLP에는 링크 파트너가 제공할 수 있는 모든 속도 및 이중 설정이 포함되어 있습니다. FLP를 수신하는 스테이션은 프레임을 승인하며, 각 디바이스는 각각 달성할 수 있는 최고 속도 및 양방향 설정에 대해 상호 동의합니다. 한 디바이스에서 자동 협상을 지원하지 않는 경우 다른 디바이스는 FLP를 수신하고 병렬 탐지 모드로 전환합니다. 장치는 파트너의 속도를 감지하기 위해 펄스의 길이를 듣고, 그 길이를 기반으로 속도를 설정한다. 듀플렉스 설정에서는 문제가 발생합니다. 듀플렉스는 협상해야 하므로 자동 협상으로 설정된 디바이스는 다른 디바이스의 설정을 결정할 수 없으므로 IEEE 802.3u 표준에 명시된 대로 기본적으로 하프 듀플렉스로 설정됩니다.

예를 들어 자동 협상을 위해 ASA 인터페이스를 구성하고 이를 100Mbps 및 전이중으로 하드코딩되는 스위치에 연결할 경우 ASA는 FLP를 전송합니다. 그러나 스위치는 속도와 양방향을 위해 하드코딩되어 있고 자동 협상에 참여하지 않기 때문에 응답하지 않습니다. 스위치로부터 응답을 수신하지 않으므로 ASA는 병렬 탐지 모드로 전환되고 스위치가 보내는 프레임의 펄스 길이를 감지합니다. 즉, ASA는 스위치가 100Mbps로 설정되었음을 감지하므로 이를 기반으로 인터페이스 속도를 설정합니다. 그러나 스위치가 FLP를 교환하지 않으므로 ASA는 스위치가 전이중으로 실행할 수 있는지 여부를 감지할 수 없으므로 ASA는 IEEE 803.2u 표준에 명시된 대로 인터페이스 양방향을 반이중으로 설정합니다. 스위치가 100Mbps 및 전이중으로 하드코딩되고 ASA가 100Mbps 및 반이중으로 자동 협상되었기 때문에(그와 마찬가지로) 듀플렉스 불일치로 인해 심각한 성능 문제가 발생할 수 있습니다.

속도 또는 이중 불일치는 문제의 인터페이스의 오류 카운터가 증가할 때 가장 자주 나타납니다. 가장 일반적인 오류는 프레임, CRC(Cyclic Redundancy Check) 및 런트입니다. 인터페이스에서 이 값이 증가하면 속도/이중 불일치 또는 케이블 문제가 발생합니다. 계속하려면 이 문제를 해결해야 합니다.

예

<#root>

Interface GigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), A

157 runts

, 0 giants

379 input errors, 107 CRC, 273 frame

, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 121 packets output, 774

CPU 사용률

CPU 사용률이 높다는 것을 알게 된 경우 다음 단계를 완료하여 문제를 해결하십시오.

- 의 연결 수가 show xlate count 낮은지 확인합니다.
- 메모리 블록이 정상인지 확인합니다.
- ACL 수가 더 많은지 확인합니다.
- 명령을 show memory detail 실행하고 ASA에서 사용하는 메모리가 정상 사용인지 확인합니다.
- 의 개수와show processes cpu-hog 개수show processes memory가 정상인지 확인합니다.
- 보안 어플라이언스 내부 또는 외부에 있는 모든 호스트는 브로드캐스트/멀티캐스트 트래픽일 수 있고 CPU 사용률이 높은 악성 트래픽 또는 대량 트래픽을 생성할 수 있습니다. 이 문제를 해결하려면 액세스 목록을 구성하여 호스트 간(엔드 투 엔드) 트래픽을 거부하고 사용량을 확인합니다.
- ASA 인터페이스의 듀플렉스 및 속도 설정을 확인합니다. 원격 인터페이스와의 불일치 설정은 CPU 사용률을 높일 수 있습니다.

이 예에서는 속도 불일치로 인한 입력 오류 및 오버런 수가 더 많음을 보여줍니다. 오류를 show interface 확인하려면 다음 명령을 사용합니다.

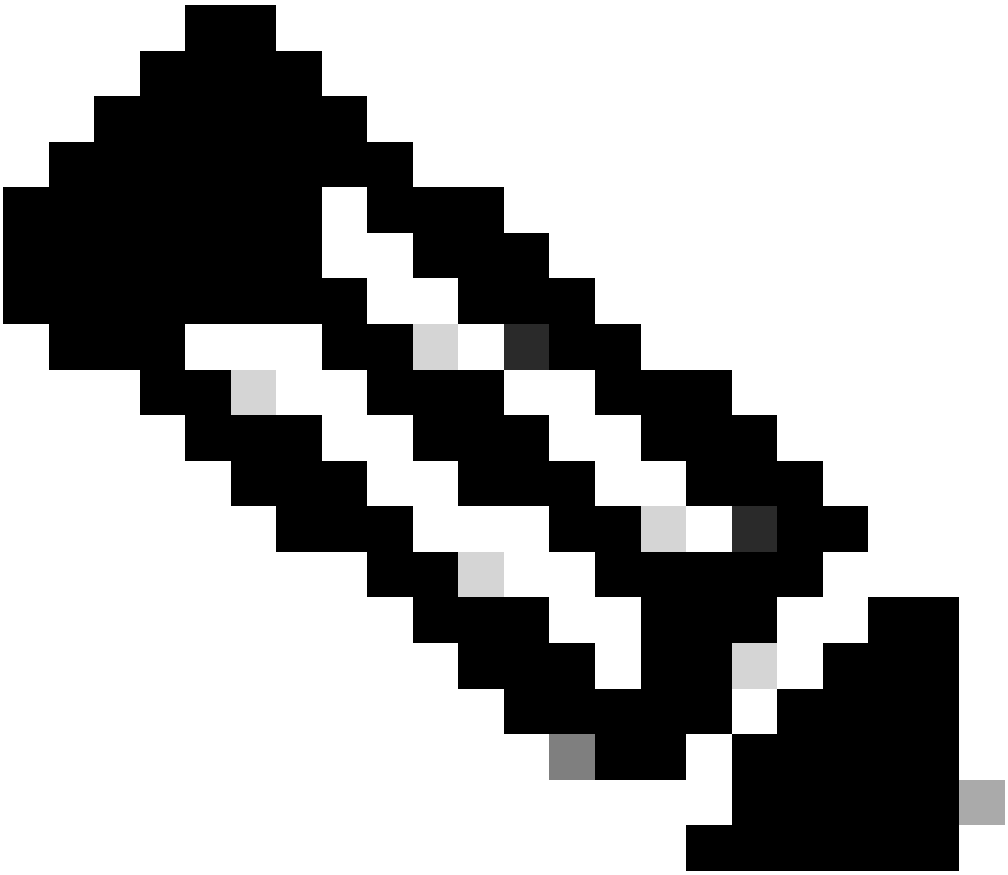
<#root>

Ciscoasa#

sh int GigabitEthernet0/1

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants



7186 input errors, 0 CRC, 0 frame, 7186 overrun



, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

이 문제를 해결하려면 해당 인터페이스에 속도를 auto로 설정합니다.

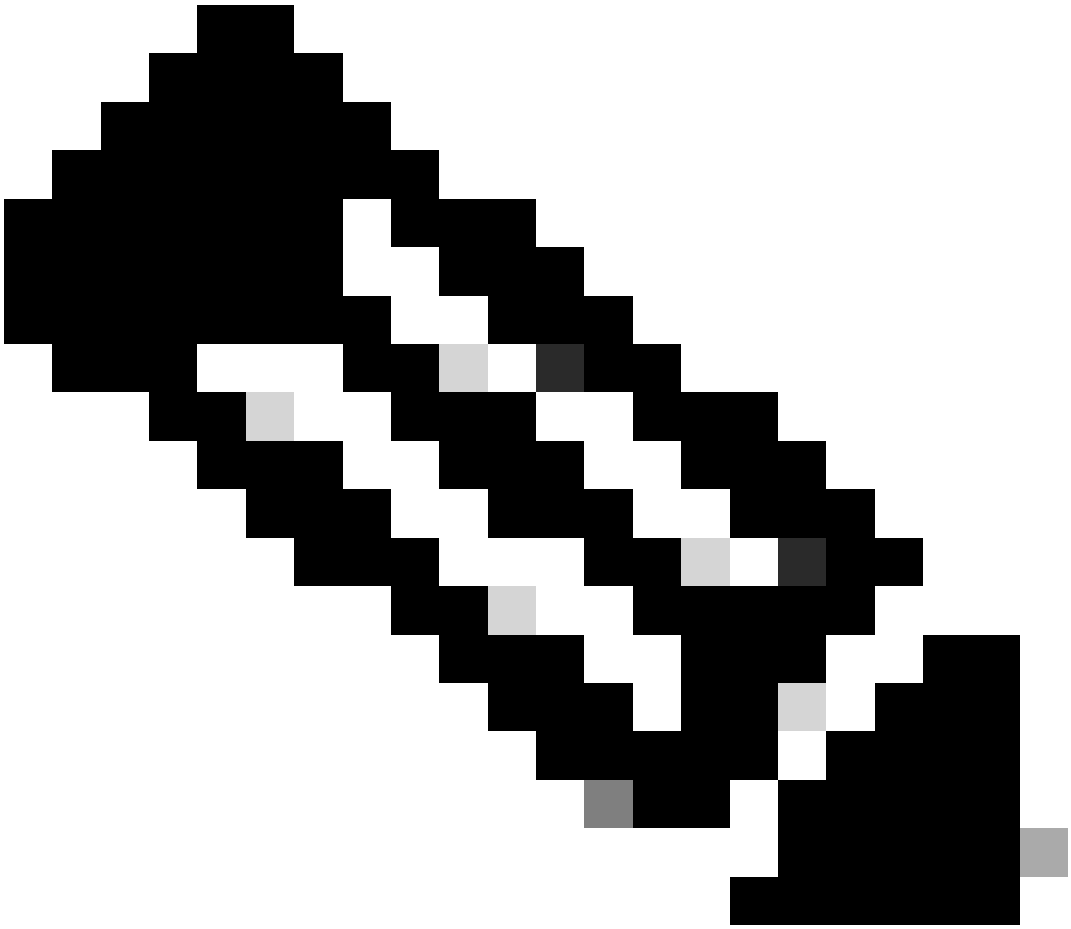


참고: Cisco에서는 모든 인터페이스에서 명령을ip verify reverse-path interface 활성화하는 것이 좋습니다. 그러면 유효한 소스 주소가 없는 패킷이 삭제되고 CPU 사용량이 줄어듭니다. 이는 FWSM이 높은 CPU 문제에 직면할 때 적용됩니다.

• CPU 사용량이 많은 또 다른 이유는 멀티캐스트 경로가 너무 많기 때문일 수 있습니다. ASA에서show mroute 멀티캐스트 경로를 너무 많이 수신하는지 확인하려면 명령을 실행합니다.

• 네트워크에서 show local-host 바이러스 공격을 나타낼 수 있는 서비스 거부(denial-of-service) 공격이 있는지 확인하려면 명령을 사용합니다.

- Cisco 버그 ID CSCsq48636으로 인해 높은 CPU가 발생할 수 있습니다. 자세한 내용은 Cisco 버그 ID CSCsq48636을 참조하십시오.



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 버그 정보에 액세스할 수 있습니다.

참고: 이전에 제공된 솔루션으로 문제가 해결되지 않을 경우 요구 사항에 따라 ASA 플랫폼을 업그레이드하십시오. Adaptive Security Appliance Platform 기능 및 용량에 대한 자세한 내용은 Cisco Security Modules for Security Appliances를 참조하십시오. 자세한 내용은 TAC(Cisco 기술 지원)에 문의하십시오.

높은 메모리 사용률

다음은 높은 메모리 사용률에 대한 몇 가지 가능한 원인 및 해결 방법입니다.

- **이벤트 로깅:** 이벤트 로깅은 많은 양의 메모리를 사용할 수 있습니다. 이 문제를 해결하려면 모든 이벤트를 설치하고 syslog 서버와 같은 외부 서버에 기록합니다.

- **메모리 누수:** 보안 어플라이언스 소프트웨어의 알려진 문제로 인해 메모리 소비가 증가할 수 있습니다. 이 문제를 해결하려면 보안 어플라이언스 소프트웨어를 업그레이드하십시오.

- **디버깅 사용:** 디버깅은 대량의 메모리를 사용할 수 있습니다. 이 문제를 해결하려면 undebug all 명령을 사용하여 디버깅을 비활성화합니다.

- **포트 차단:** 보안 어플라이언스의 외부 인터페이스에서 포트를 차단하면 보안 어플라이언스는 지정된 포트를 통해 패킷을 차단하기 위해 많은 양의 메모리를 사용합니다. 이 문제를 해결하려면 ISP 쪽에서 문제가 되는 트래픽을 차단합니다.

- **위협 탐지:** 위협 탐지 기능은 다양한 위협에 대해 수집되는 다양한 레벨의 통계와 호스트가 스캔을 수행할 시기를 결정하는 스캔된 위협 탐지로 구성됩니다. 메모리 **사용량**을 줄이려면 이 기능을 끕니다.

PortFast, 채널링 및 트렁킹

기본적으로 Catalyst OS(운영 체제)를 실행하는 Cisco 스위치와 같은 많은 스위치는 플러그 앤 플레이 장치로 설계되었습니다. 따라서 ASA가 스위치에 연결된 경우 대부분의 기본 포트 매개 변수는 바람직하지 않습니다. 예를 들어 Catalyst OS를 실행하는 스위치에서 기본 채널링은 Auto로, 트렁킹은 Auto로, PortFast는 Disabled로 설정됩니다. Catalyst OS를 실행하는 스위치에 ASA를 연결하는 경우 채널링을 비활성화하고 트렁킹을 비활성화하며 PortFast를 활성화합니다.

채널링은 Fast EtherChannel 또는 Giga EtherChannel이라고도 하며, 링크 전반의 전체 처리량을 높이기 위해 논리 그룹에서 둘 이상의 물리적 포트를 바인딩하는 데 사용됩니다. 포트가 자동 채널링에 대해 구성된 경우, 링크가 활성화되어 채널의 일부인지 확인하기 위해 PAgP(Port Aggregation Protocol) 프레임을 보냅니다. 다른 디바이스가 링크의 속도와 듀플렉스를 자동으로 협상하려고 할 경우 이러한 프레임으로 인해 문제가 발생할 수 있습니다. 포트의 채널링이 Auto(자동)로 설정된 경우, 링크가 가동된 후 포트가 트래픽 전달을 시작하기 전에 약 3초의 추가 지연도 발생합니다.

참고: Catalyst XL Series 스위치에서 채널링은 기본적으로 Auto로 설정되지 않습니다. 따라서 ASA에 연결되는 스위치 포트에서 채널링을 비활성화해야 합니다.

공통 트렁킹 프로토콜인 ISL(Inter-Switch Link) 또는 Dot1q로도 알려진 트렁킹은 단일 포트(또는 링크)에서 여러 가상 LAN(VLAN)을 결합합니다. 트렁킹은 일반적으로 두 스위치에 둘 이상의 VLAN이 정의된 경우 두 스위치 간에 사용됩니다. 자동 트렁킹을 위해 포트를 구성하면 연결된 포트가 트렁크를 원하는지 확인하기 위해 링크가 시작될 때 DTP(Dynamic Trunking Protocol) 프레임을 보냅니다. 이러한 DTP 프레임은 링크의 자동 협상 문제를 일으킬 수 있습니다. 스위치 포트에서 트렁킹이 Auto로 설정된 경우 링크가 가동된 후 포트가 트래픽 전달을 시작하기 전에 약 15초의 추가 지연이 발생합니다.

PortFast(Fast Start라고도 함)는 레이어 3 디바이스가 스위치 포트 외부에 연결되었음을 스위치에 알리는 옵션입니다. 포트는 기본값인 30초(수신 대기 15초, 학습 15초)를 기다리지 않습니다. 대신 이 작업을 수행하면 링크가 시작된 직후에 스위치가 포트를 전달 상태로 전환합니다. PortFast를 활성화하면 스패닝 트리가 비활성화되지 않습니다. 스패닝 트리가 해당 포트에서 여전히 활성 상태입니다. PortFast를 활성화하면 링크의 다른 쪽 끝에 연결된 다른 스위치나 허브(레이어 2 전용 디바이스)가 없다는 알림만 스위치에 전달됩니다. 스위치는 일반적인 30초 지연을 우회하면서 해당 포트를 가동할 경우 레이어 2 루프가 발생하는지 확인합니다. 링크가 시작된 후에도 스패닝 트리에 계속 참여합니다. 포트에서 BPDU(bridge packet data unit)를 전송하고, 스위치에서 해당 포트의 BPDU를 계속 수신 대기합니다. 이러한 이유로 인해 ASA에 연결되는 모든 스위치 포트에서 PortFast를 활성화하는 것이 좋습니다.

참고: Catalyst OS 릴리스 5.4 이상에는 단일 명령을 사용하여 채널링을set port host <mod>/<port> 비활성화하고 트렁킹을 비활성화하며 PortFast를 활성화할 수 있는 명령이 포함됩니다.

NAT(Network Address Translation)

각 NAT 또는 PAT(NAT Overload) 세션에는 xlate라는 변환 슬롯이 할당됩니다. 이러한 xlate는 NAT 규칙을 변경하여 영향을 준 후에도 지속될 수 있습니다. 이는 변환을 거치는 트래픽에 의해 변환 슬롯이 고갈되거나 예상치 못한 동작 또는 둘 다를 초래할 수 있습니다. 이 섹션에서는 보안 어플라이언스에서 xlate를 보고 지우는 방법에 대해 설명합니다.

주의: 보안 어플라이언스에서 xlate를 전역적으로 지우면 디바이스를 통과하는 모든 트래픽의 흐름이 일시적으로 중단될 수 있습니다.

외부 인터페이스 IP 주소를 사용하는 PAT의 샘플 ASA 컨피그레이션:

object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

보안 어플라이언스를 통과하는 트래픽은 NAT를 거칠 가능성이 높습니다. 보안 어플라이언스에서 사용 중인 변환을 보려면 다음 명령을show xlate 실행합니다.

<#root>

Ciscoasa#

show xlate

```
 5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice NA
```

변환 슬롯은 키 변경 후에도 유지될 수 있습니다. 보안 어플라이언스에서 현재 변환 슬롯을 지우려면 다음 명령을clear xlate 실행합니다.

<#root>

Ciscoasa#

clear xlate

<#root>

Ciscoasa#

show xlate

0 in use, 1 most used

이 clear xlate 명령은 xlate 테이블에서 모든 현재 동적 변환을 지웁니다. 특정 IP 변환을 지우려면 키워드와 함께 명령clear xlate을 사용할 수 global [ip address] 있습니다.

다음은 NAT를 위한 샘플 ASA 컨피그레이션입니다.

object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 10.10.10.10 10.10.10.100 nat (inside,outside) source dynamic inside

내부 show xlate 10.2.2.2에서 외부 글로벌 10.10.10으로의 변환에 대한 출력을 확인합니다.

<#root>

Ciscoasa#

show xlate

2 in use, 2 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri idle 62:33:57 timeout 0:00:30

TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30

10.10.10.10 글로벌 IP 주소에 대한 변환을 지웁니다.

<#root>

Ciscoasa# clear xlate global 10.10.10.10

이 예에서는 내부 10.2.2.2에서 외부 전역 10.10.10.10으로의 변환이 사라졌습니다.

<#root>

Ciscoasa#

show xlate

1 in use, 2 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30

Syslog

Syslog를 사용하면 ASA에서 문제를 해결할 수 있습니다. Cisco는 ASA Firewall Syslog Server(PFSS)라는 Windows NT용 무료 syslog 서버를 제공합니다. Cisco Technical Support & Downloads에서 PFSS를 다운로드할 수 있습니다.

다른 여러 공급업체(예: Windows 2000 및 Windows XP 등 다양한 Windows 플랫폼용 syslog 서버)도 제공합니다. 대부분의 UNIX 및 Linux 시스템에는 기본적으로 syslog 서버가 설치되어 있습니다.

syslog 서버를 설정할 때 로그를 전송하도록 ASA를 구성합니다.

예를 들면 다음과 같습니다.

<#root>

logging on logging host <ip_address_of_syslog_server> logging trap debugging

참고: 이 예에서는 디버깅(레벨 7) 및 더 중요한 syslog를 syslog 서버로 전송하도록 ASA를 구성합니다. 이러한 ASA 로그는 가장 자세한 정보이므로 문제를 해결할 때만 사용하십시오. 정상 작동의 경우 로깅 레벨을 Warning(경고)(레벨 4) 또는 Error(오류)(레벨 3)로 구성합니다.

성능 저하 문제가 발생하면 텍스트 파일에서 syslog를 열고 성능 문제와 관련된 소스 IP 주소를 검색합니다. (UNIX를 사용하는 경우 소스 IP 주소에 대해 syslog를 통해 grep할 수 있습니다.) 외부 서버가 TCP 포트 113(ID 프로토콜 또는 Ident용)의 내부 IP 주소에 액세스하려고 했으나 ASA가 패킷을 거부했음을 나타내는 메시지를 확인합니다. 메시지는 다음 예와 유사해야 합니다.

%ASA-2-106001: Inbound TCP connection denied from 10.64.10.2/35969 to 192.168.110.179/113 flags SYN

이 메시지를 받으면 ASA에 service resetinbound명령을 실행합니다. ASA는 패킷을 자동으로 삭제하지 않습니다. 대신 이 명령을 사용하면 ASA에서 보안 정책에 의해 거부된 모든 인바운드 연결을 즉시 재설정합니다. 서버는 Ident 패킷이 TCP 연결을 시간 초과하기까지 기다리지 않습니다. 대신 재설정 패킷을 즉시 수신합니다.

SNMP

엔터프라이즈 구축에 권장되는 방법은 Cisco ASA with SNMP의 성능을 모니터링하는 것입니다. Cisco ASA는 SNMP 버전 1, 2c 및 3에서 이를 지원합니다.

NMS(Network Management Server)에 트랩을 전송하도록 보안 어플라이언스를 구성하거나, NMS를 사용하여 보안 어플라이언스에서 MIB를 찾아볼 수 있습니다. MIB는 정의의 모음이며 보안 어플라이언스는 각 정의에 대한 값 데이터베이스를 유지 관리합니다. 이에 대한 자세한 내용은 Cisco ASA 5500 Series Configuration Guide with the CLI, 8.4 and 8.6을 참조하십시오.

Cisco ASA에 대해 지원되는 모든 MIB는 ASA MIB Support List(ASA MIB 지원 목록)에서 확인할 수 있습니다. 이 목록에서 다음 MIB는 성능을 모니터링할 때 유용합니다.

- CISCO-FIREWALL-MIB ----은 장애 조치에 유용한 개체를 포함합니다.

- CISCO-PROCESS-MIB ----은 CPU 사용률에 유용한 객체를 포함합니다.

- CISCO-MEMORY-POOL-MIB ----은 메모리 개체에 유용한 개체를 포함합니다.

역방향 DNS 조회

ASA에서 성능이 저하된 경우, ASA에서 사용하는 외부 주소에 대한 권한 있는 DNS 서버에 DNS PTR(Domain Name System Pointer) 레코드(Reverse DNS Lookup records라고도 함)가 있는지 확인합니다. 여기에는 전역 NAT(Network Address Translation) 풀의 모든 주소(또는 인터페이스에서 오버로드되는 경우 ASA 외부 인터페이스), 고정 주소 및 내부 주소(NAT를 함께 사용하지 않는 경우)가 포함됩니다. FTP(File Transfer Protocol) 및 텔넷 서버와 같은 일부 애플리케이션에서는 역방향 DNS 조회를 사용하여 사용자의 출처와 유효한 호스트 여부를 확인할 수 있습니다. 역방향 DNS 조회가 확인되지 않으면 요청 시간이 초과됨에 따라 성능이 저하됩니다.

이러한 호스트에 대해 PTR 레코드가 존재하도록 하려면 PC 또는nslookup UNIX 시스템에서 명령을 실행합니다. 인터넷에 연결하는 데 사용하는 전역 IP 주소를 포함합니다.

예

<#root>

```
% nslookup 192.168.219.25

 10.219.133.198.in-addr.arpa name = www.cisco.com.
```

해당 IP 주소에 할당된 디바이스의 DNS 이름으로 응답을 다시 받아야 합니다. 응답을 받지 못한 경우 각 글로벌 IP 주소에 대한 PTR 레코드 추가를 요청하기 위해 DNS를 제어하는 담당자에게 문의하십시오.

인터페이스에서 오버런

트래픽 버스트가 있는 경우, 버스트가 NIC의 FIFO 버퍼 및 수신 링 버퍼의 버퍼링 용량을 초과하면 삭제된 패킷이 발생할 수 있습니다. 흐름 제어를 위해 일시 중지 프레임을 활성화하면 이 문제를 완화할 수 있습니다. 일시 중지(XOFF) 및 XON 프레임은 FIFO 버퍼 사용량을 기준으로 NIC 하드웨어에 의해 자동으로 생성됩니다. 일시 중지 프레임은 버퍼 사용량이 최고 수위를 넘을 때 전송됩니다. 흐름 제어를 위해 일시 중지(XOFF) 프레임을 활성화하려면 다음 명령을 사용합니다.

<#root>

hostname(config)#

interface tengigabitethernet 1/0

hostname(config-if)#

flowcontrol send on

명령 표시

CPU 사용량 표시

이 show cpu usage 명령은 ASA CPU에 배치된 트래픽 로드를 확인하는 데 사용됩니다. 트래픽 피크 시간, 네트워크 급증 또는 공격 중에는 CPU 사용량이 급증할 수 있습니다.

ASA에는 다양한 작업을 처리할 수 있는 단일 CPU가 있습니다. 예를 들어, 패킷을 처리하고 디버그 메시지를 콘솔에 인쇄합니다. 각 프로세스는 고유의 목적을 가지고 있으며, 일부 프로세스는 다른 프로세스보다 더 많은 CPU 시간을 필요로 한다. 암호화는 아마도 CPU를 가장 많이 사용하는 프로세스일 것입니다. 따라서 ASA가 암호화된 터널을 통해 많은 트래픽을 전달할 경우 VPN 3000과 같은 전용 VPN Concentrator인 더 빠른 ASA를 고려해야 합니다. VAC는 ASA CPU에서 암호화 및 암호 해독을 오프로드하고 카드의 하드웨어에서 수행합니다. 이를 통해 ASA는 3DES(168비트 암호화)로 100Mbps의 트래픽을 암호화하고 해독할 수 있습니다.

로깅은 많은 양의 시스템 리소스를 사용할 수 있는 또 다른 프로세스입니다. 따라서 ASA에서 콘솔, 모니터 및 버퍼 로깅을 비활성화하는 것이 좋습니다. 문제를 해결할 때 이러한 프로세스를 활성화하지만, 특히 CPU 용량이 부족할 경우 일상적인 작업에 대해서는 비활성화할 수 있습니다. 또한 syslog 또는 SNMP(Simple Network Management Protocol) 로깅(로깅 기록)을 레벨 5(알림) 이하로 설정하는 것이 좋습니다. 또한 이 명령을 사용하여 특정 syslog 메시지 ID를 비활성화할 수 no logging message <syslog_id> 있습니다.

Cisco ASDM(Adaptive Security Device Manager)은 Monitoring 탭에 시간 경과에 따른 ASA의 CPU 사용량을 볼 수 있는 그래프도 제공

합니다. 이 그래프를 사용하여 ASA의 로드를 확인할 수 있습니다.

이 **show cpu usage** 명령을 사용하여 CPU 사용률 통계를 표시할 수 있습니다.

예

<#root>

Ciscoasa#

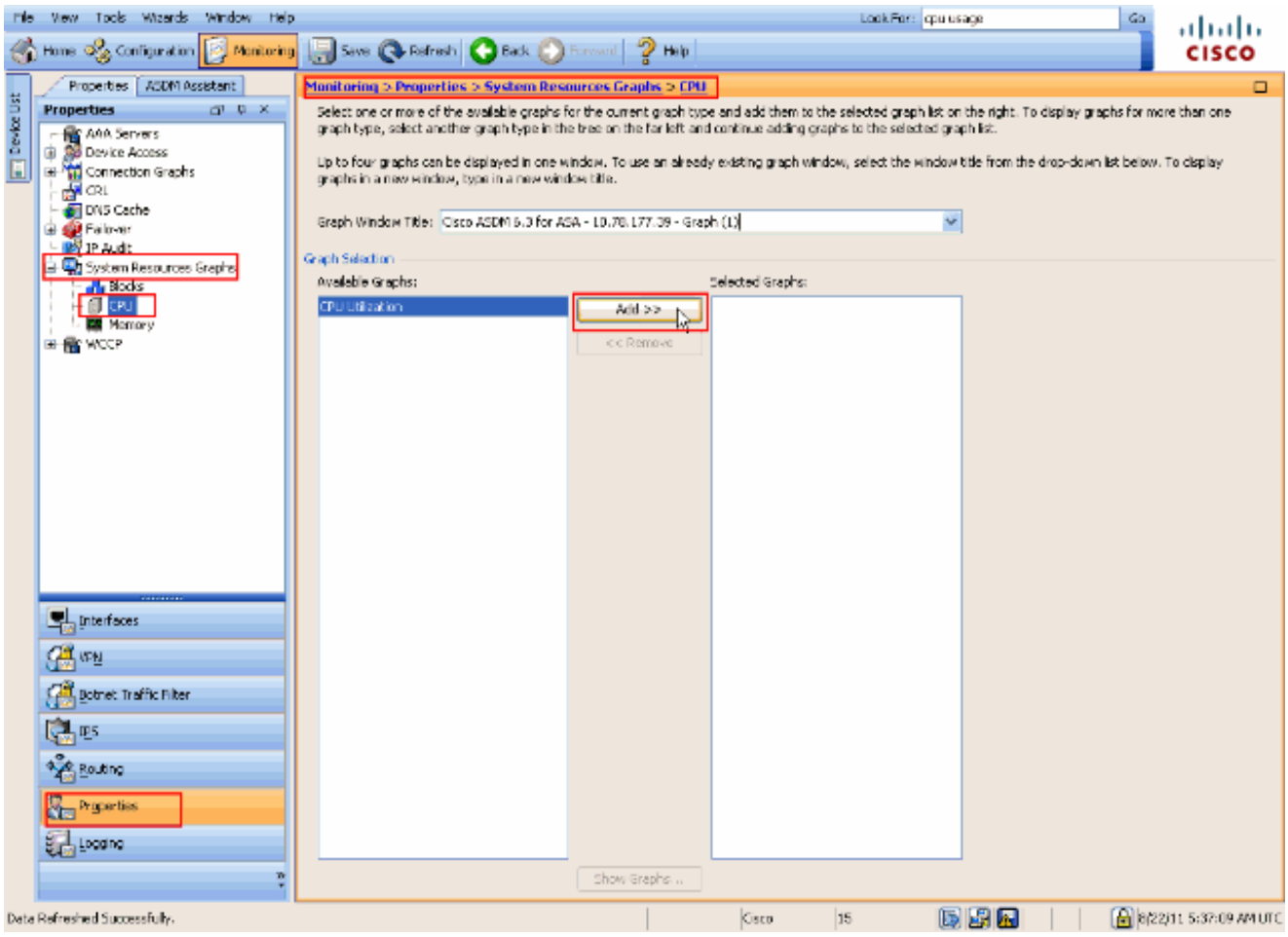
show cpu usage

```
 CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

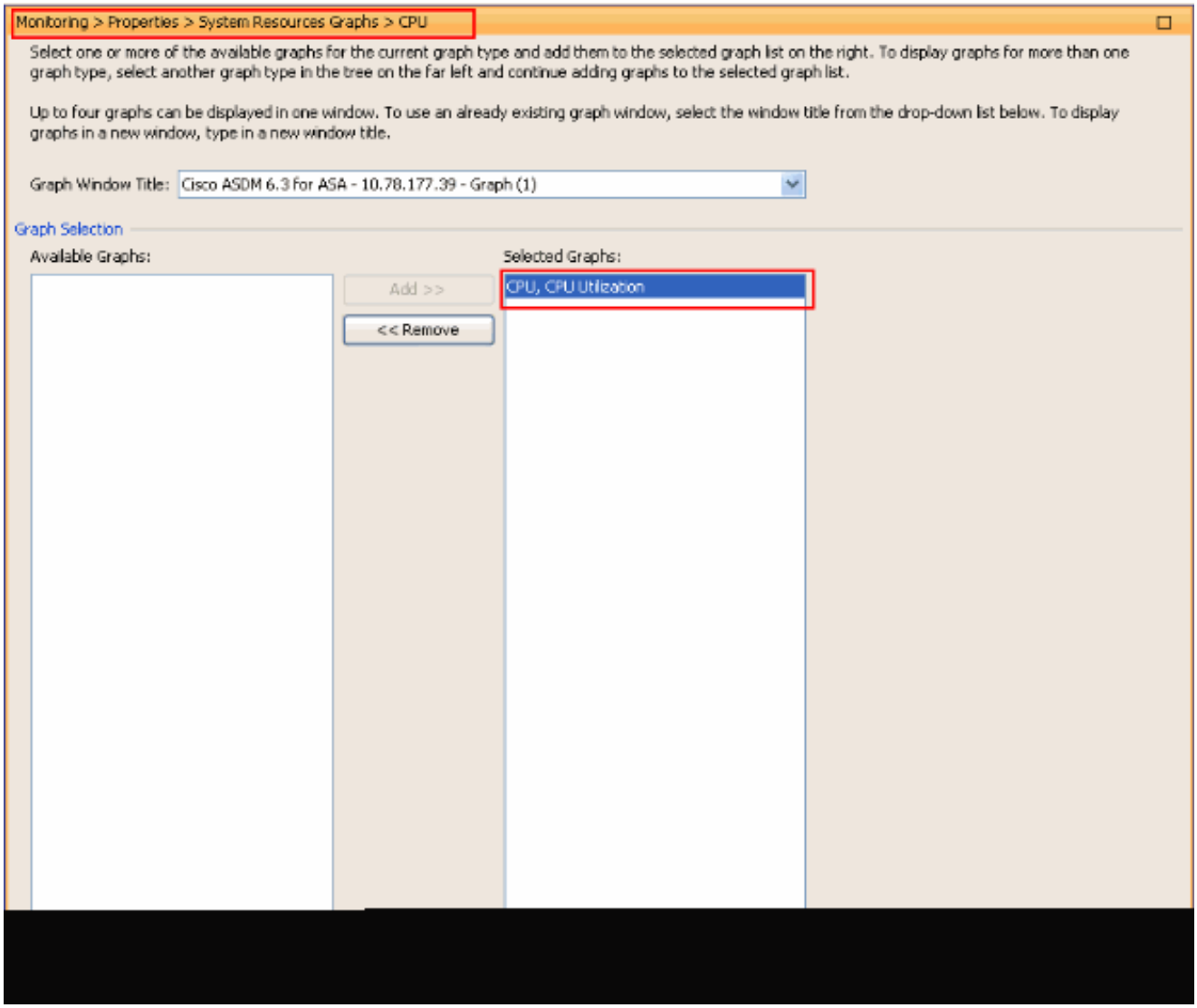
ASDM의 CPU 사용량 보기

ASDM에서 CPU 사용량을 보려면 다음 단계를 완료하십시오.

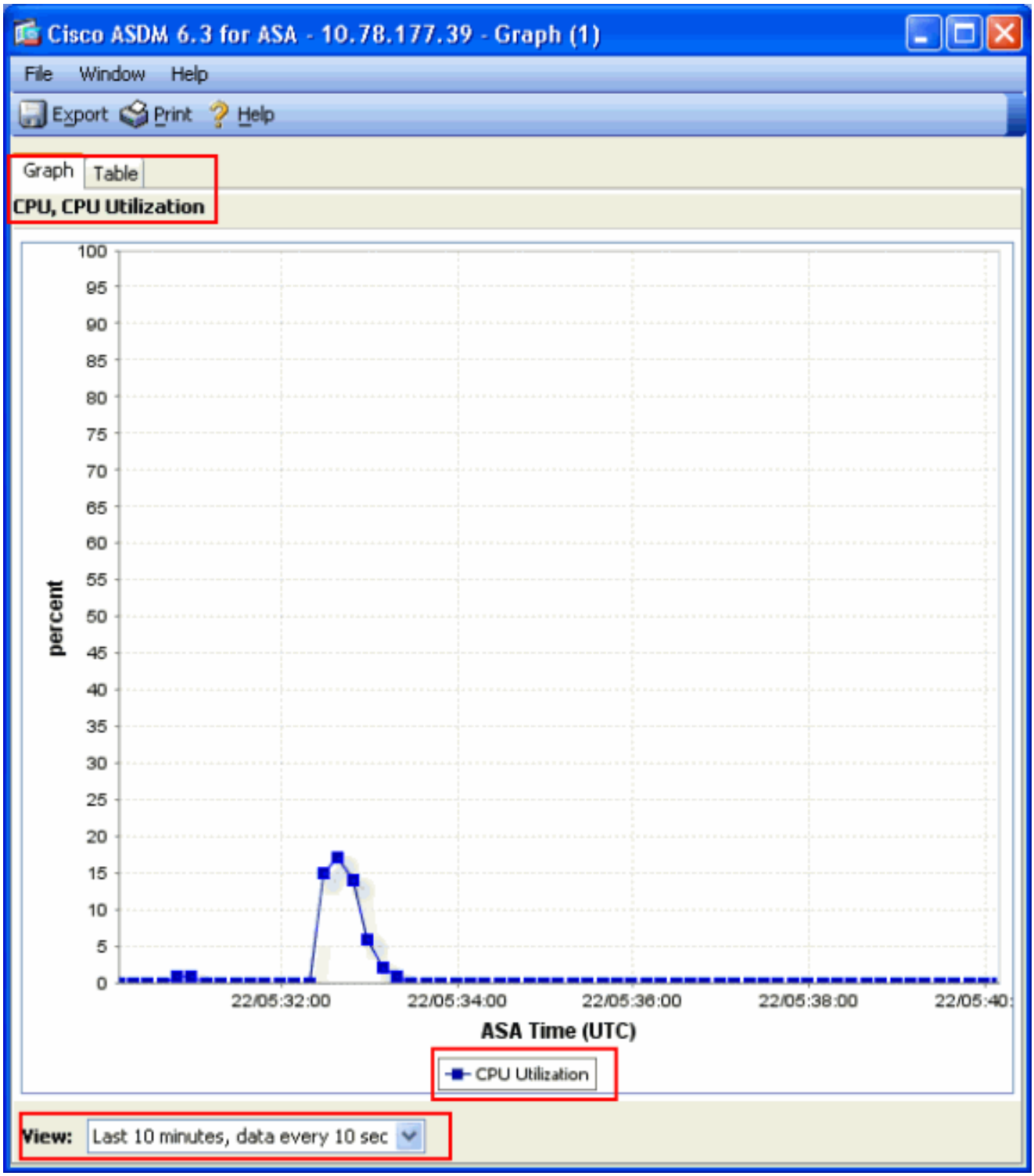
- ASDMMonitoring > Properties > System Resources Graphics > CPU 으로 이동하여 **Graph Window** Title(**그래프 창 제목)을 선택합니다**. 그런 다음 Available Graphs(사용 가능한 그래프) 목록에서 필요한 **그래프를** 선택하고 Add(**추가)**를 클릭합니다.



- **Selected Graphs** 섹션 아래에 필요한 그래프 이름이 추가되면 Show Graphs**를 클릭합니다**.



다음 그림에서는 ASDM의 **CPU Usage** 그래프를 보여줍니다. 이 그래프의 여러 뷰를 사용할 수 있으며, 뷰 드롭다운 목록의 뷰를 선택하면 이 뷰를 변경할 수 있습니다. 이 출력은 필요에 따라 인쇄하거나 컴퓨터에 저장할 수 있다.



출력 설명

이 표에서는 출력의 필드에 대해 **show cpu usage** 설명합니다.

필드	설명
5초 동안의 CPU 사용률	지난 5초 동안의 CPU 사용률
1분	지난 1분 동안 CPU 사용률 평균 5초 샘플
5분	지난 5분 동안 CPU 사용률 평균 5초 샘플

트래픽 표시

이 show traffic 명령은 지정된 기간 동안 ASA를 통과하는 트래픽의 양을 보여줍니다. 이 결과는 명령이 마지막으로 실행된 이후의 시간 간격을 기준으로 합니다. 정확한 결과를 얻으려면 명령을 **clear traffic** 먼저 실행한 다음 명령을 실행하기 전에 1-10분 정도 show traffic 기다리십시오. 명령을 show traffic 실행하고 1-10분 정도 기다렸다가 명령을 다시 실행할 수도 있지만, 두 번째 인스턴스의 출력만 유효합니다.

ASA를 show traffic통과하는 트래픽의 양을 확인하려면 명령을 사용할 수 있습니다. 여러 인터페이스가 있는 경우 이 명령을 사용하면 어떤 인터페이스에서 가장 많은 데이터를 보내고 받을지 결정할 수 있습니다. 두 개의 인터페이스가 있는 ASA 어플라이언스의 경우 외부 인터페이스의 인바운드 및 아웃바운드 트래픽 합계가 내부 인터페이스의 인바운드 및 아웃바운드 트래픽 합과 같아야 합니다.

예

<#root>

Ciscoasa#

show traffic

```
 outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370 pkts/sec 1341502 bytes/sec tra
```

인터페이스 중 하나에서 정격 처리량에 근접하거나 도달할 경우 더 빠른 인터페이스로 업그레이드하거나 해당 인터페이스로 드나드는 트래픽의 양을 제한해야 합니다. 이렇게 하지 않으면 패킷이 삭제될 수 있습니다. 이 섹션에서 설명한 **show interface**것처럼, 처리량에 대해 알아보려면 인터페이스 카운터를 검사할 수 있습니다.

성능 표시

이 show perfmon 명령은 ASA에서 검사하는 트래픽의 양과 유형을 모니터링하는 데 사용됩니다. 이 명령은 초당 변환(xlate) 및 연결(conn) 수를 결정하는 유일한 방법입니다. 연결은 TCP 및 UDP(User Datagram Protocol) 연결로 세분화됩니다. 이 **명령이 생성하는** 출력에 대한 설명은 출력 설명을 참조하십시오.

예

PERFMON STATS Current Average Xlates 18/s 19/s Connections 75/s 79/s TCP Conns 44/s 49/s UDP Conns 31/s 30/s URL Access 27/s 30/s URL Serve

출력 설명

이 표에서는 출력의 필드에 대해 show perfmon 설명합니다.

필드	설명
Xlates	초당 작성된 번역
연결	초당 설정된 연결 수
TCP Conn	초당 TCP 연결 수
UDP Conn	초당 UDP 연결 수
URL 액세스	초당 액세스된 URL(웹 사이트)
URL 서버 요청	초당 Websense 및 N2H2로 전송된 요청(filter 명령 필요)

TCP 수정	ASA에서 초당 전달하는 TCP 패킷의 수
TCPI상호 개념	고정에서 설정된 초기 제한을 초과한 초당 SYN 패킷 수입니다.
HTTP 수정	초당 포트 80이 목적지인 패킷 수(명령 필요fixup protocol http)
FTP 수정	초당 검사된 FTP 명령
AAA 아우텐	초당 인증 요청 수
AAA 작성자	초당 권한 부여 요청 수
AAA 계정	초당 계정 관리 요청

블록 표시

이 명령과 함께 show cpu usage 이 명령을 사용하여 ASAshow blocks가 오버로드되었는지 여부를 확인할 수 있습니다.

패킷 블록(1550바이트 및 16384바이트)

ASA 인터페이스로 들어오면 패킷이 입력 인터페이스 대기열에 배치되고 OS로 전달되어 블록에 배치됩니다. 이더넷 패킷의 경우 1550바이트 블록이 사용됩니다. 패킷이 66MHz 기가비트 이더넷 카드에 있는 경우 16384바이트 블록이 사용됩니다. ASA는 ASA(Adaptive Security Algorithm)를 기반으로 패킷의 허용 또는 거부 여부를 결정하고 아웃바운드 인터페이스의 출력 대기열을 통과하도록 패킷을 처리합니다. ASA에서 트래픽 로드를 지원할 수 없는 경우, 사용 가능한 1550바이트 블록(또는 66MHz GE의 경우 16384바이트 블록)의 수는 0에 가깝게 유지됩니다(명령 출력의 CNT 열에 표시됨). CNT 열이 0에 도달하면 ASA는 최대 8192개까지 더 많은 블록을 할당하려고 시도합니다. 사용 가능한 블록이 더 이상 없으면 ASA에서 패킷을 삭제합니다.

장애 조치 및 Syslog 블록(256바이트)

256바이트 블록은 주로 스테이트풀 장애 조치 메시지에 사용됩니다. 활성 ASA는 변환 및 연결 테이블을 업데이트하기 위해 패킷을 생성하여 대기 ASA로 전송합니다. 높은 연결 비율이 생성되거나 해제되는 과부하 트래픽 기간에는 사용 가능한 256바이트 블록의

수가 0으로 감소할 수 있습니다. 이 삭제는 하나 이상의 연결이 대기 ASA로 업데이트되지 않았음을 나타냅니다. 이는 일반적으로 다음 번에 상태 저장 장애 조치 프로토콜에서 xlate 또는 연결이 손실될 때 포착되기 때문에 허용됩니다. 그러나 256바이트 블록의 CNT 열이 오랜 시간 동안 0에 머물거나 그 근처에 있을 경우 ASA에서 처리하는 초당 연결 수 때문에 ASA에서 동기화된 변환 및 연결 테이블을 따라잡을 수 없습니다. 이러한 상황이 지속적으로 발생하면 ASA를 더 빠른 모델로 업그레이드하십시오.

ASA에서 전송된 Syslog 메시지는 256바이트 블록을 사용하지만, 일반적으로 256바이트 블록 풀이 고갈될 만큼 릴리스되지는 않습니다. CNT 열에 256바이트 블록 수가 0에 가까운 것으로 표시되면 Debugging(수준 7)에서 syslog 서버에 로그인하지 않아야 합니다. 이는 ASA 컨피그레이션의 로깅 트랩 줄에 표시됩니다. 디버깅을 위해 추가 정보가 필요한 경우가 아니면 로깅을 Notification(레벨 5) 이하로 설정하는 것이 좋습니다.

예

<#root>

Ciscoasa#

show blocks

```
 SIZE MAX LOW CNT 4 1600 1597 1600 80 400 399 400 256 500 495 499 1550 1444 1170 1188 16384 2048 1532 1
```

출력 설명

이 표에서는 출력의 열에 대해 show blocks 설명합니다.

열	설명
크기	E 블록 풀의 크기(바이트)입니다. 각 크기는 특정 유형을 나타냅니다
최대	지정된 바이트 블록 풀에 사용할 수 있는 최대 블록 수입니다. 최대 블록 수는 부팅 시 메모리에서 제거됩니다. 일반적으로 최대 블록 수는 변경되지 않습니다. 단, 256바이트 및 1550바이트 블록에서는 Adaptive Security Appliance에서 필요할 때 최대 8192개까지 동적으로 더 많이 생성할 수 있습니다.

낮음	최저 수위 표시. 이 숫자는 Adaptive Security Appliance의 전원이 켜진 이후 또는 블록을 마지막으로 지운 이후(clear blocks 명령 사용) 사용 가능한 이 크기의 블록 중 가장 낮은 수를 나타냅니다. LOW 열의 0은 메모리가 가득 찬 이전 이벤트를 나타냅니다.
CNT	해당 특정 크기의 블록 풀에 사용할 수 있는 현재 블록 수입니다. CNT 열의 0은 메모리가 현재 가득 찼음을 의미합니다.

이 표에서는 출력의 SIZE 행 값에 대해 show blocks 설명합니다.

크기 값	설명
0	dupb 블록에서 사용됩니다.
4	DNS, ISAKMP, URL 필터링, uauth, TFTP, TCP 모듈과 같은 애플리케이션의 기존 블록을 복제합니다. 또한 이 크기의 블록은 일반적으로 코드를 통해 드라이버에 패킷을 전송하는 등 사용할 수 있습니다.
80	TCP 가로채기에서 승인 패킷을 생성하고 장애 조치 hello 메시지에 사용됩니다.
256	상태 기반 장애 조치 업데이트, syslog 로깅 및 기타 TCP 기능에 사용됩니다. 이러한 블록은 주로 스테이트풀 장애 조치 메시지에 사용됩니다. 활성 ASA는 변환 및 연결 테이블을 업데이트하기 위해 대기 ASA에 패킷을 생성하고 전송합니다. 높은 연결 비율이 생성되거나 해제되는 과부하 트래픽에서는 사용 가능한 블록 수가 0으로 감소할 수 있습니다. 이 상황은 하나 이상의 연결이 대기 Adaptive Security Appliance에 업데이트되지 않았음을 나타냅니다. 상태 기반 장애 조치 프로토콜은 손실된 변환 또는 연결을 다음에 catch합니다. 256바이트 블록에 대한 CNT 열이 오랜 시간 동안 0에 머물거나 거의 0에 머무를 경우, Adaptive Security Appliance는 Adaptive Security Appliance에서 처리하는 초당 연결 수 때문에 변환 및 연결 테이블의 동기화를 유지하는 데 어려움을 겪습니다. Adaptive Security Appliance에서 전송되는 Syslog 메시지는 256바이트 블록을 사용하지만, 일반적으로 256바이트 블록 풀의 고갈을 야기하는 이러한 수량으로 릴리스되지 않습니다. CNT 열에 256바이트 블록 수가 0에 가까운 것으로 표시되는 경우 Debugging(수준 7)에서 syslog 서버에 로깅하지 않아야 합니다. 이는 Adaptive Security Appliance 컨피그레이션의 로깅 트랩 줄에 표시됩니다. 디버깅을 위해 추가 정보가 필요한 경우가 아니면 Notification(레벨 5) 이하에서 로깅을 설정하는 것이 좋습니다.
1550	Adaptive Security Appliance를 통해 처리할 이더넷 패킷을 저장하는 데 사용됩니다. 패킷이

	Adaptive Security Appliance 인터페이스에 진입하면 입력 인터페이스 대기열에 배치되고 운영 체제로 전달되며 블록에 배치됩니다. Adaptive Security Appliance는 보안 정책에 따라 패킷을 허용할지 아니면 거부할지 결정하고 아웃바운드 인터페이스의 출력 대기열을 통과하도록 패킷을 처리합니다. Adaptive Security Appliance가 트래픽 로드를 따라가는 데 어려움을 겪는 경우, 사용 가능한 블록 수는 0에 가깝게 호버링할 수 있습니다(명령 출력의 CNT 열에 표시됨). CNT 열이 0이면 Adaptive Security Appliance는 최대 8192개까지 더 많은 블록을 할당하려고 시도합니다. 사용 가능한 블록이 더 이상 없으면 Adaptive Security Appliance에서 패킷을 삭제합니다.
16384	64비트 66MHz 기가비트 이더넷 카드(i82543)에만 사용됩니다. 이더넷 패킷에 대한 자세한 내용은 1550의 설명을 참조하십시오.
2048	컨트롤 업데이트에 사용되는 컨트롤 또는 안내식 프레임입니다.

메모리 표시

이 show memory 명령은 현재 사용 가능한 바이트 수와 함께 ASA의 총 물리적 메모리(또는 RAM)를 표시합니다. 이 정보를 사용하려면 먼저 ASA에서 메모리를 사용하는 방법을 이해해야 합니다. ASA가 부팅되면 플래시의 OS를 RAM으로 복사하고 RAM에서 OS를 실행합니다(라우터와 동일). 그런 다음 ASA는 플래시에서 시작 컨피그레이션을 복사하여 RAM에 넣습니다. 마지막으로, ASA는 섹션에서 설명하는 블록 풀을 생성하기 위해 RAM을 show blocks 할당합니다. 이 할당이 완료되면 컨피그레이션의 크기가 증가하는 경우에만 ASA에 추가 RAM이 필요합니다. 또한 ASA는 변환 및 연결 항목을 RAM에 저장합니다.

정상 작동 중에는 ASA의 사용 가능한 메모리가 거의 변하지 않아야 합니다. 일반적으로 메모리가 부족하면 공격을 받고 수십만 개의 연결이 ASA를 통과하는 경우뿐입니다. 연결을 확인하려면 ASA를show conn count 통한 현재 및 최대 연결 수를 표시하는 명령을 실행합니다. ASA의 메모리가 부족하면 결국 충돌합니다. 충돌 전에 syslog(%ASA-3-211001)에서 메모리 할당 실패 메시지를 확인할 수 있습니다.

공격을 받아 메모리가 부족한 경우 Cisco 기술 지원 팀에 문의하십시오.

예

<#root>

Ciscoasa#

show memory

```
 Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) ------------- ---------------- T
```

Xlate 표시

이 show xlate count 명령은 ASA를 통한 현재 및 최대 변환 수를 표시합니다. 변환은 내부 주소를 외부 주소에 매핑하는 것으로, NAT(Network Address Translation)와 같은 일대일 매핑 또는 PAT(Port Address Translation)와 같은 다대일 매핑이 될 수 있습니다. 이 명령은 ASA를show xlate 통해 각 변환을 출력하는 명령의 하위 집합입니다. 명령 출력에는 "사용 중" 번역이 표시되며, 이는 명령이 실행될 때 ASA에서 활성화된 번역의 수를 나타냅니다. "가장 많이 사용됨"은 전원이 켜진 후 ASA에서 관찰된 최대 번역을 나타냅니다.

참고: 단일 호스트는 여러 대상에 대한 여러 연결을 가질 수 있지만 하나의 변환만 가능합니다. xlate 수가 내부 네트워크의 호스트 수보다 훨씬 큰 경우 내부 호스트 중 하나가 손상되었을 수 있습니다. 내부 호스트가 손상된 경우 소스 주소를 스푸핑하고 ASA에서 패킷을 전송합니다.

참고: vpnclient 컨피그레이션이 활성화되어 있고 내부 호스트가 DNS 요청을 전송하면 이 명령은 고정 변환에show xlate 대한 여러 xlate를 나열할 수 있습니다.

예

<#root>

Ciscoasa#

show xlate count

```
 84 in use, 218 most used
```

<#root>

Ciscoasa(config)#

show xlate

```
 3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside,
TCP PAT from inside:10.1.1.15/1026 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

UDP PAT from 10.1.1.15/1028 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

ICMP PAT from inside:10.1.1.15/21505 to outside:192.168.49.1/0 flags ri idle 62:33:57 timeout 0:00:30
```

첫 번째 항목은 내부 네트워크의 호스트 포트(10.1.1.15, 1026)에서 외부 네트워크의 호스트 포트(192.168.49.1, 1024)로의 TCP 포트 주소 변환입니다. "r" 플래그는 변환이 포트 주소 변환임을 나타냅니다. "i" 플래그는 변환이 내부 주소 포트에 적용됨을 나타냅니다.

두 번째 항목은 내부 네트워크의 호스트 포트(10.1.1.15, 1028)에서 외부 네트워크의 호스트 포트(192.168.49.1, 1024)로의 UDP 포트 주소 변환입니다. "r" 플래그는 변환이 포트 주소 변환임을 나타냅니다. "i" 플래그는 변환이 내부 주소 포트에 적용됨을 나타냅니다.

세 번째 항목은 내부 네트워크의 host-ICMP-id(10.1.1.15, 21505)에서 외부 네트워크의 host-ICMP-id(192.168.49.1, 0)로의 ICMP 포트 주소 변환입니다. "r" 플래그는 변환이 포트 주소 변환임을 나타냅니다. "i" 플래그는 변환이 내부 주소-ICMP-id에 적용됨을 나타냅니다.

내부 주소 필드는 보안 수준이 더 높은 인터페이스에서 보안 수준이 더 낮은 인터페이스로 이동하는 패킷에서 소스 주소로 표시됩니다. 반대로, 보안 수준이 낮은 인터페이스에서 보안 수준이 높은 인터페이스로 이동하는 패킷에서는 대상 주소로 표시됩니다.

연결 수 표시

이 show conn count 명령은 ASA를 통한 현재 및 최대 연결 수를 표시합니다. 연결은 내부 주소에서 외부 주소로의 레이어 4 정보 매핑입니다. ASA가 TCP 세션에 대한 SYN 패킷을 받거나 UDP 세션의 첫 번째 패킷이 도착하면 연결이 생성됩니다. ASA가 최종 ACK 패킷을 수신하면 연결이 해제됩니다. 이 패킷은 TCP 세션 핸드셰이크가 닫힐 때 또는 UDP 세션에서 시간 초과가 만료될 때 발생합니다.

연결 수가 매우 많으면(정상 50~100배) 공격을 받을 가능성이 있습니다. 높은 연결 수로 인해 ASA의 메모리가 부족해지지 않도록 하려면 명령을 show memory실행합니다. 공격을 받는 경우 고정 항목당 최대 연결 수를 제한하고 미발달 연결의 최대 수도 제한할 수 있습니다. 이 작업은 내부 서버를 보호하므로 과부하가 발생하지 않습니다. 자세한 내용은 CLI, 8.4 및 8.6과 함께 Cisco ASA 5500 Series 컨피그레이션 가이드를 참조하십시오.

예

<#root>

Ciscoasa#

show conn count

```
 2289 in use, 44729 most used
```

인터페이스 표시

show interface 명령은 듀플렉스 불일치 문제 및 케이블 문제를 확인하는 데 도움이 될 수 있습니다. 또한 인터페이스가 오버런되는지 여부에 대한 추가 통찰력을 제공할 수 있습니다. ASA의 CPU 용량이 부족할 경우 1550바이트 블록 수가 0에 가깝습니다(66MHz Gig 카드의 16384바이트 블록 참조). 또 다른 지표는 인터페이스에 "버퍼 없음"이 증가하는 것입니다. no buffers(버퍼 없음) 메시지는 패킷에 사용 가능한 블록이 없고 패킷이 삭제되었기 때문에 인터페이스에서 ASA OS에 패킷을 전송할 수 없음을 나타냅니다. 버퍼 레벨이 정기적으로 증가하지 않으면 명령을 실행하여 ASA의show proc cpu CPU 사용량을 확인합니다. 트래픽 로드가 많아 CPU 사용량이 많은 경우, 로드를 처리할 수 있는 더 강력한 ASA로 업그레이드합니다.

패킷이 처음 인터페이스에 진입하면 입력 하드웨어 대기열에 배치됩니다. 입력 하드웨어 대기열이 가득 차면 패킷이 입력 소프트웨어 대기열에 배치됩니다. 패킷은 입력 대기열에서 전달되어 1550바이트 블록(또는 66MHz 기가비트 이더넷 인터페이스의 16384바이트 블록)에 배치됩니다. 그런 다음 ASA는 패킷에 대한 출력 인터페이스를 결정하고 패킷을 적절한 하드웨어 대기열에 배치합니다. 하드웨어 대기열이 가득 차면 패킷이 출력 소프트웨어 대기열에 배치됩니다. 소프트웨어 대기열 중 하나의 최대 블록이 큰 경우 인터페이스가 오버런됩니다. 예를 들어, ASA에 200Mbps가 유입되고 모두 단일 100Mbps 인터페이스로 나갈 경우 출력 소프트웨어 대기열은 아웃바운드 인터페이스의 높은 숫자를 표시하는데, 이는 인터페이스에서 트래픽 볼륨을 처리할 수 없음을 나타냅니다. 이러한 상황이 발생하면 더 빠른 인터페이스로 업그레이드하십시오.

예

<#root>

Ciscoasa#

show interface

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000
```

또한 인터페이스에 오류가 있는지 확인해야 합니다. Runts, 입력 오류, CRC 또는 프레임 오류를 받으면 이중 불일치가 발생할 수 있습니다. 케이블에도 문제가 생길 수 있습니다. 듀플렉스 문제에 대한 자세한 내용은 속도 및 듀플렉스 설정을 참조하십시오. 각 오류 카운터는 해당 특정 오류로 인해 삭제된 패킷 수를 나타냅니다. 정기적으로 증가하는 특정 카운터가 표시되면 ASA의 성능이 저하될 가능성이 높으므로 문제의 근본 원인을 찾아야 합니다.

인터페이스 카운터를 검사할 때 인터페이스가 전이중으로 설정된 경우 충돌, 지연 충돌 또는 지연된 패킷을 경험해서는 안 됩니다. 반대로 인터페이스가 반이중으로 설정된 경우 충돌, 일부 늦은 충돌 및 일부 지연된 패킷을 수신해야 합니다. 총 충돌, 늦은 충돌 및 지연된 패킷 수는 입력 및 출력 패킷 카운터 합계의 10%를 초과해서는 안 됩니다. 충돌이 전체 트래픽의 10%를 초과할 경우 링크가 과다 사용되므로 전이중 또는 더 빠른 속도(10Mbps~100Mbps)로 업그레이드해야 합니다. 10%의 충돌은 ASA가 해당 인터페이스를 통과하는 패킷의 10%를 삭제한다는 것을 의미합니다. 이러한 패킷 각각은 재전송되어야 합니다.

인터페이스 카운터에 대한 자세한 interface 내용은 Cisco ASA 5500 Series Adaptive Security Appliances 명령 참조의 명령을 참조하십시오.

프로세스 표시

ASA**show processes** 명령은 명령이 실행될 때 ASA에서 실행되는 모든 활성 프로세스를 표시합니다. 이 정보는 어떤 프로세스가 너무 많은 CPU 시간을 수신하고 어떤 프로세스가 CPU 시간을 수신하지 않는지 확인하는 데 유용합니다. 이 정보를 얻으려면 명령을 두 번 **show processes** 실행합니다. 각 인스턴스 간에 약 1분 정도 기다립니다. 해당 프로세스의 경우 첫 번째 출력에 표시된 런타임 값에서 두 번째 출력에 표시된 런타임 값을 뺍니다. 이 결과는 해당 시간 간격 동안 프로세스가 받은 CPU 시간(밀리초)을 보여줍니다. 일부 프로세스는 특정 간격으로 실행되도록 스케줄링되며, 일부 프로세스는 처리할 정보가 있을 때만 실행됩니다. 577poll 프로세스는 모든 프로세스 중 Runtime 값이 가장 클 수 있습니다. 이는 577poll 프로세스가 처리해야 하는 데이터가 있는지 확인하기 위해 이더넷 인터페이스를 폴링하기 때문에 정상입니다.

참고: 각 ASA 프로세스에 대한 검토는 이 문서의 범위에 포함되지 않지만 완결성을 위해 간략하게 언급되어 있습니다. ASA 프로세스에 대한 자세한 내용은 ASA 8.3 이상: 성능 문제 모니터링 및 문제 해결을 참조하십시오.

명령 요약

요약하면, show cpu usage ASA가 사용 중인 로드를 식별하려면 명령을 사용합니다. 출력은 실행 평균입니다. ASA는 CPU 사용량이 급증할 수 있으며, 이는 실행 평균으로 마스킹됩니다. ASA가 CPU 사용량의 80%에 도달하면 ASA를 통한 레이턴시는 CPU 사용량의 약 90%로 서서히 증가합니다. CPU 사용량이 90%를 초과하면 ASA에서 패킷 삭제를 시작합니다.

CPU 사용량이 많은 경우 이 명령을 **show processes** 사용하여 CPU 시간을 가장 많이 사용하는 프로세스를 식별합니다. 이 정보를 사용하여 집약적인 프로세스(예: 로깅)에 소요되는 시간을 줄일 수 있습니다.

CPU가 핫(hot)으로 실행되지 않지만 패킷이 계속 삭제된다고 생각되면 ASA 인터페이스에서show interface 이중 불일치로 인한 버퍼와 충돌이 없는지 확인하려면 명령을 사용합니다. 버퍼 수가 증가하지 않지만 CPU 사용량이 낮지 않으면 인터페이스에서 이를 통과하는 트래픽을 지원할 수 없습니다.

버퍼가 괜찮은 경우 블록을 확인합니다. 1550바이트 블록(66MHz Gig 카드의show blocks 경우 16384바이트 블록)에서 출력의 현재 CNT 열이 0에 가까우면 ASA는 사용량이 너무 많아 이더넷 패킷을 삭제할 가능성이 높습니다. 이 경우 CPU가 급증합니다.

ASA를 통해 새 연결을 설정할 때 문제가 발생하면 ASA를 show conn count 통한 현재 연결 수를 확인하려면 명령을 사용합니다.

현재 카운트가 높은 경우 ASA에show memory 메모리가 부족하지 않도록 출력을 확인합니다. 메모리가 부족한 경우 네트워크가 서비스 거부 공격을 경험하지 않았는지 확인하기 위해 show conn show local-host 또는 명령을 사용하여 연결의 소스를 조사합니다.

ASA를 통과하는 트래픽의 양을 측정하기 위해 다른 명령을 사용할 수 있습니다. 이 **show traffic** 명령은 인터페이스당 총 패킷 및 바이트를 표시하고 는 show perfmon 트래픽을 ASA에서 검사하는 여러 유형으로 나눕니다.

관련 정보

- Cisco ASA 5500-X Series 방화벽
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.