ASA NAT(Network Address Translation) 컨피그레이션 문제 해결

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 플랫폼에서 NAT(Network Address Translation) 컨피그레이션의 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

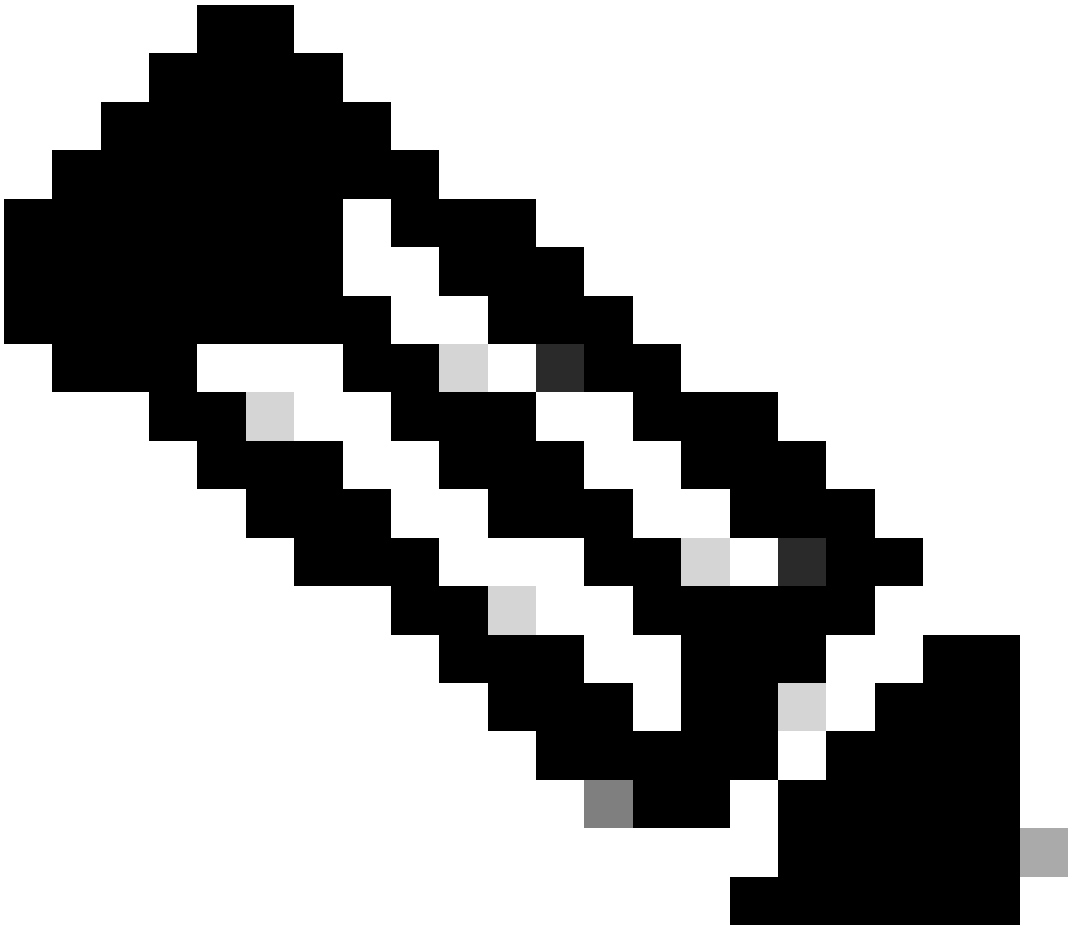
이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 ASA 버전 8.3 이상을 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.

ASA에서 NAT 컨피그레이션 문제 해결



참고: 기본 NAT 컨피그레이션을 보여주는 비디오가 포함된 NAT 컨피그레이션의 몇 가지 기본 예는 이 문서 하단의 Related Information 섹션을 참조하십시오.

NAT 컨피그레이션의 문제를 해결할 때 ASA의 NAT 컨피그레이션이 NAT 정책 테이블을 구축하는 데 어떻게 사용되는지 이해하는 것이 중요합니다.

이러한 컨피그레이션 오류는 ASA 관리자가 발생하는 NAT 문제의 대부분을 차지합니다.

- NAT 컨피그레이션 규칙이 잘못되었습니다. 예를 들어 수동 NAT 규칙이 NAT 테이블의 맨 위에 배치되므로 NAT 테이블 아래에 더 많이 배치된 특정 규칙은 절대 맞지 않습니다.
- NAT 컨피그레이션에 사용되는 네트워크 객체가 너무 광범위하므로 트래픽이 실수로 이러한 NAT 규칙과 일치하게 되고 더 구체적인 NAT 규칙을 놓치게 됩니다.

패킷 추적기 유틸리티는 ASA에서 대부분의 NAT 관련 문제를 진단하는 데 사용할 수 있습니다. NAT 컨피그레이션을 사용하여 NAT 정책 테이블을 작성하는 방법 및 특정 NAT 문제를 해결하고

해결하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오.

또한 show nat detail 명령을 사용하여 어떤 NAT 규칙이 새 연결에 의해 도달하는지 파악할 수 있습니다.

ASA 컨피그레이션을 사용하여 NAT 정책 테이블을 작성하는 방법

ASA에서 처리된 모든 패킷은 NAT 테이블을 기준으로 평가됩니다. 이 평가는 맨 위(섹션 1)에서 시작하며 NAT 규칙이 일치할 때까지 작동합니다.

일반적으로 NAT 규칙이 일치하면 해당 NAT 규칙이 연결에 적용되고 패킷에 대해 더 이상 NAT 정책이 점검되지 않지만 다음에 설명하는 몇 가지 주의 사항이 있습니다.

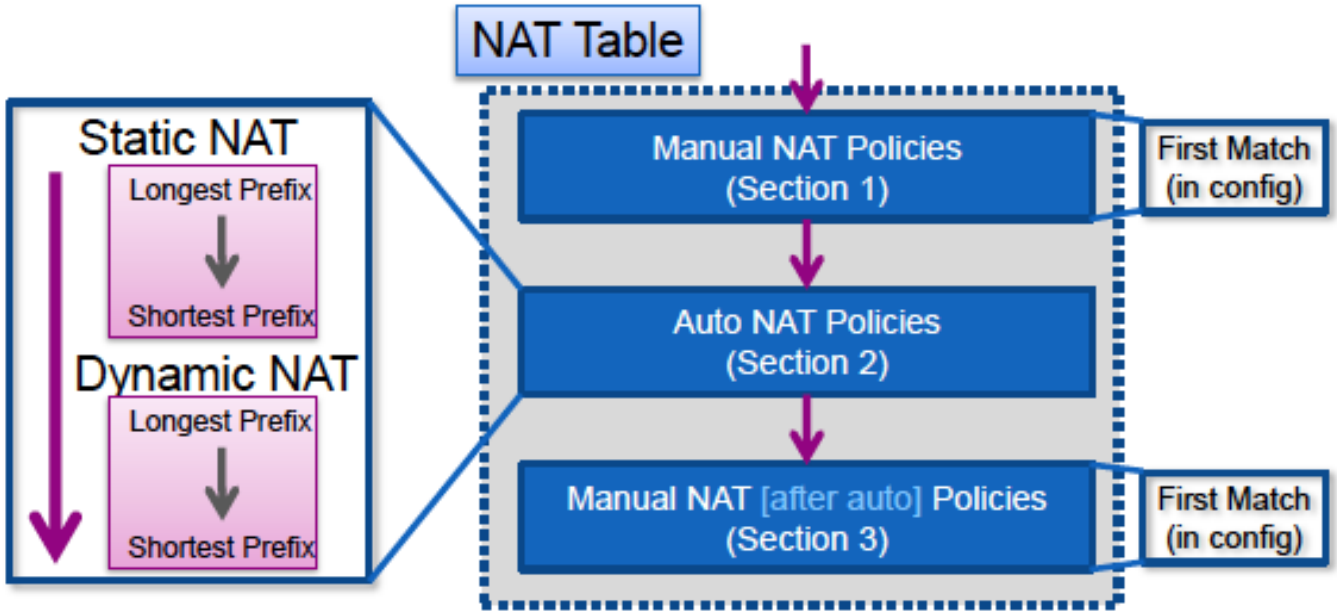
NAT 정책 테이블

ASA의 NAT 정책은 NAT 컨피그레이션에서 구축됩니다.

ASA NAT 테이블의 세 섹션은 다음과 같습니다.

섹션 1	수동 NAT 정책 이는 컨피그레이션에 나타나는 순서대로 처리됩니다.
섹션 2	자동 NAT 정책 NAT 유형(정적 또는 동적) 및 개체의 접두사(서브넷 마스크) 길이를 기반으로 처리됩니다.
섹션 3	자동 이후 수동 NAT 정책 이는 컨피그레이션에 나타나는 순서대로 처리됩니다.

이 다이어그램은 여러 NAT 섹션 및 이러한 섹션의 순서를 보여줍니다.



NAT 규칙 일치

섹션 1

- 흐름은 첫 번째 규칙으로 시작되는 NAT 테이블의 섹션 1에 대해 먼저 평가됩니다.
  - 패킷의 소스 및 목적지 IP가 수동 NAT 규칙의 매개변수와 일치하면 변환이 적용되고 프로세스가 중지되며 어떤 섹션에서도 추가 NAT 규칙이 평가되지 않습니다.
  - 일치하는 NAT 규칙이 없는 경우 NAT 테이블의 섹션 2에 대해 플로우가 평가됩니다.

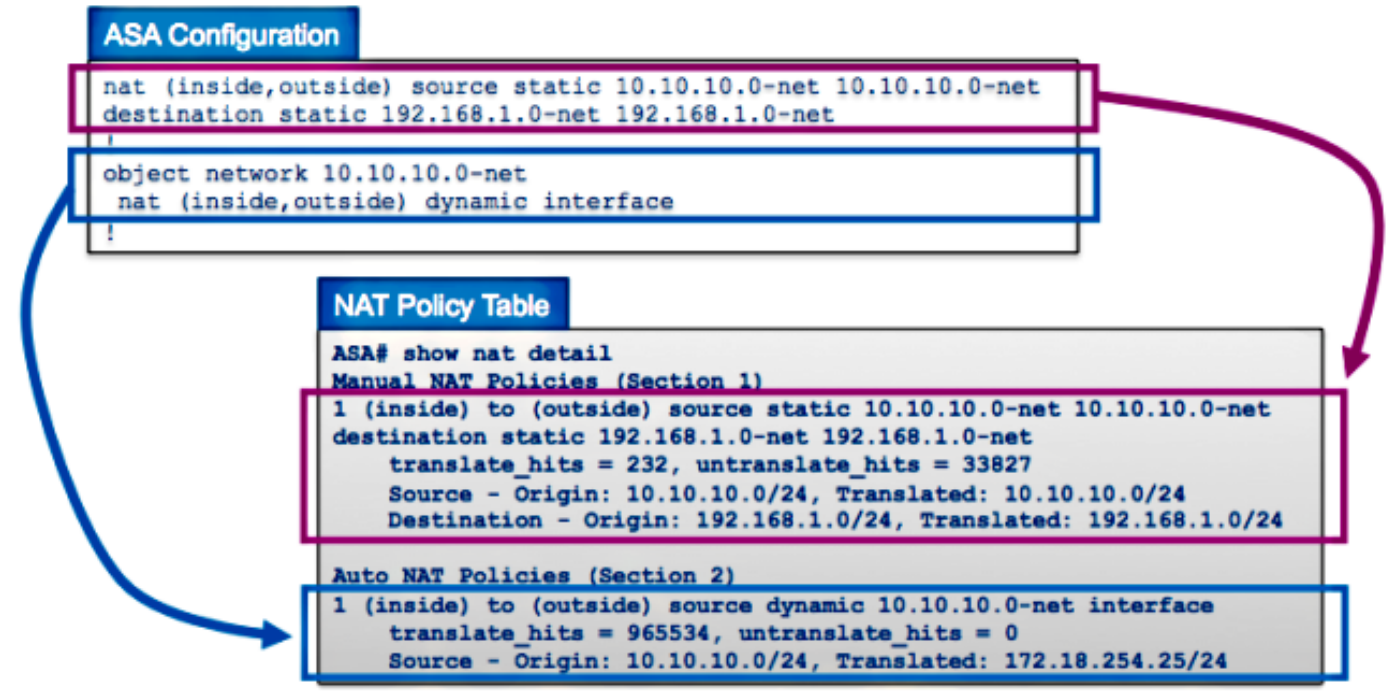
섹션 2

- 흐름은 앞에서 지정한 순서대로 섹션 2 NAT 규칙에 대해 평가되며, 먼저 고정 NAT 규칙을 거쳐 동적 NAT 규칙을 차례로 거칩니다.
  - 변환 규칙이 흐름의 소스 또는 대상 IP와 일치하면 변환을 적용하고 나머지 규칙을 계속 평가하여 흐름의 다른 IP와 일치하는지 확인할 수 있습니다. 예를 들어, 하나의 auto-NAT 규칙은 소스 IP를, 또 다른 auto-NAT 규칙은 목적지를 변환할 수 있습니다.
  - 플로우가 자동 NAT 규칙과 일치하면, 섹션 2의 끝에 도달하면 NAT 조회가 중지되고 섹션 3의 규칙이 평가되지 않습니다.
  - 섹션 2의 NAT 규칙이 플로우에 대해 매칭되지 않으면 조회가 섹션 3으로 진행됩니다

섹션 3

- 섹션 3의 과정은 본질적으로 섹션 1과 동일하다. 패킷의 소스 및 목적지 IP가 수동 NAT 규칙의 매개변수와 일치하면 변환이 적용되고 프로세스가 중지되며 어떤 섹션에서도 추가 NAT 규칙이 평가되지 않습니다.

다음 예에서는 두 개의 규칙(하나의 수동 NAT 문과 하나의 자동 NAT 컨피그레이션)이 있는 ASA NAT 컨피그레이션이 NAT 테이블에 표시되는 방법을 보여 줍니다.



NAT 문제 해결 방법

Packet Tracer 유틸리티 사용

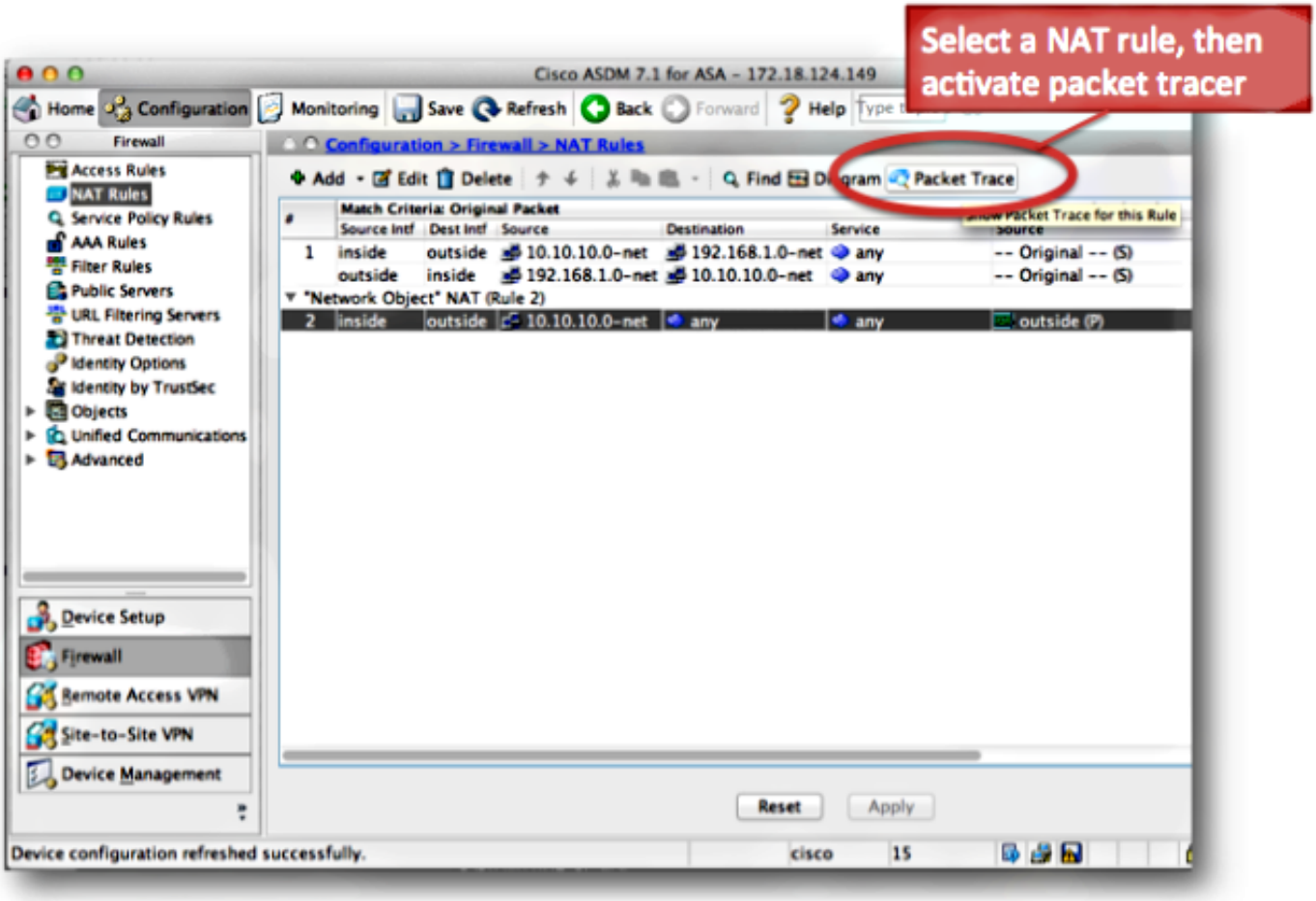
NAT 컨피그레이션 문제를 해결하려면 패킷 추적기 유틸리티를 사용하여 패킷이 NAT 정책에 도달

하는지 확인합니다. 패킷 추적기를 사용하면 ASA에 들어가는 샘플 패킷을 지정할 수 있으며, ASA는 패킷에 어떤 컨피그레이션이 적용되는지 그리고 허용되는지 여부를 나타냅니다.

다음 예에서는 내부 인터페이스로 들어가서 인터넷의 호스트로 향하는 샘플 TCP 패킷이 제공됩니다. 패킷 추적기 유틸리티는 패킷이 동적 NAT 규칙과 일치하고 외부 IP 주소 172.16.123.4로 변환됨을 보여줍니다.

```
<#root>

ASA#

packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80



...(output omitted)...

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:

object network 10.10.10.0-net
 nat (inside,outside) dynamic interface


Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up

Action: allow



ASA#
```

Cisco ASDM(Adaptive Security Device Manager)에서 패킷 추적기를 활성화하려면 NAT 규칙을 선택하고 Packet Trace를 클릭합니다. NAT 규칙에 지정된 IP 주소를 패킷 추적기 툴에 대한 입력으로 사용합니다.

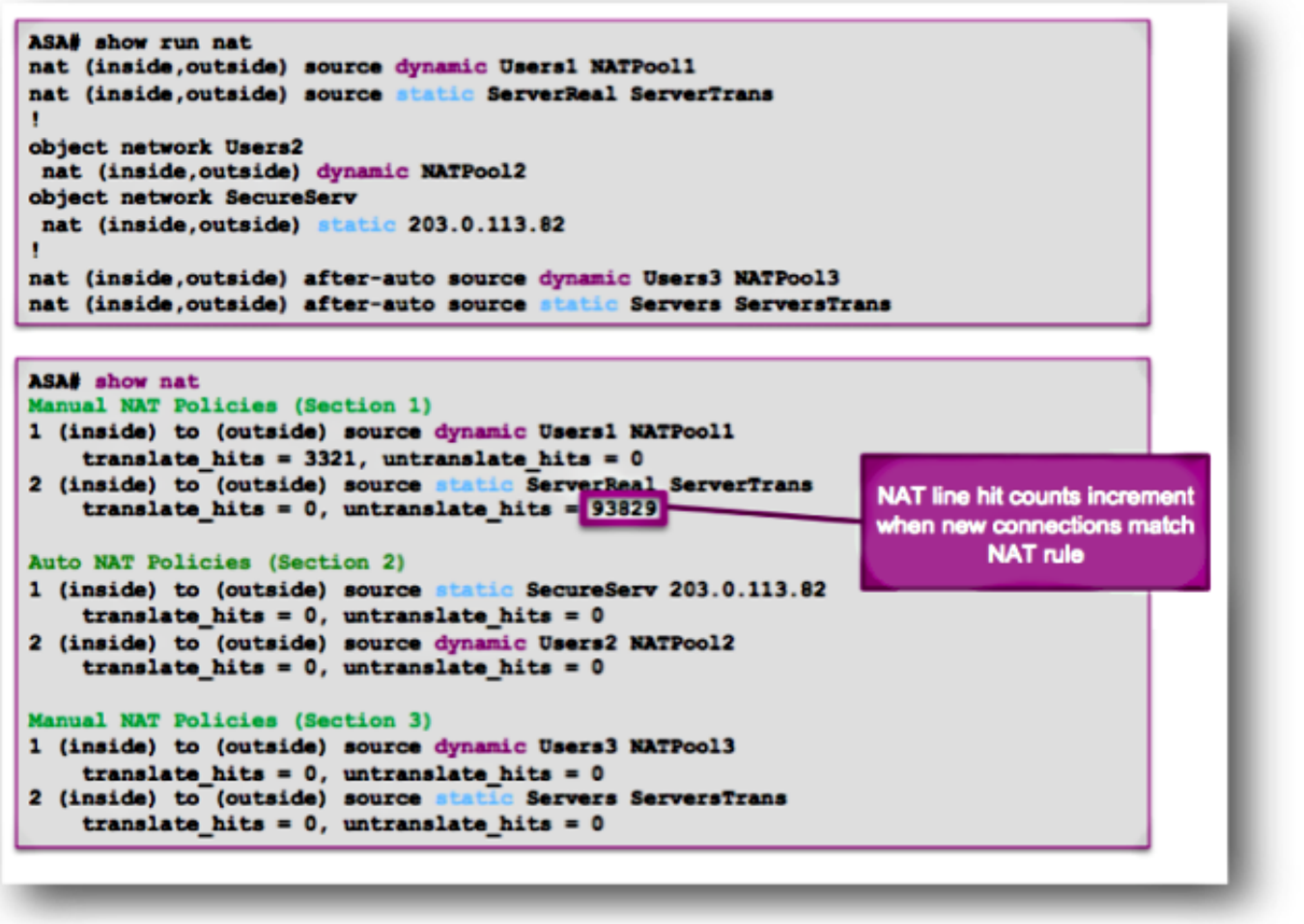


Show Nat 명령의 출력 보기

NAT 정책 테이블을 보기 위해 show nat detail 명령의 출력을 사용할 수 있습니다. 특히, translate_hits 및 untranslate_hits 카운터를 사용하여 ASA에서 어떤 NAT 엔트리를 사용할지 결정할 수 있습니다.

새 NAT 규칙에 translate_hits 또는 untranslate_hits가 없는 경우 트래픽이 ASA에 도착하지 않거나 NAT 테이블에서 우선순위가 더 높은 다른 규칙이 트래픽과 일치함을 의미합니다.

다음은 다른 ASA 컨피그레이션의 NAT 컨피그레이션 및 NAT 정책 테이블입니다.



앞의 예에서는 이 ASA에 구성된 6개의 NAT 규칙이 있습니다. show nat 출력은 각 규칙에 대한 translate_hits 및 untranslate_hits의 수뿐만 아니라 NAT 정책 테이블을 작성하는 데 이 규칙이 어떻게 사용되는지 보여줍니다.

이러한 적중 카운터는 연결당 한 번만 증가합니다. ASA를 통해 연결이 구축되면 현재 연결과 일치하는 후속 패킷은 NAT 행을 증가시키지 않습니다(ASA에서 access-list 적중 횟수가 작동하는 방식과 비슷함).

Translate_hits: 전달 방향의 NAT 규칙과 일치하는 새 연결 수입니다.

"전달 방향"은 NAT 규칙에 지정된 인터페이스 방향으로 ASA를 통해 연결이 구축되었음을 의미합니다.

내부 서버가 외부 인터페이스로 변환되도록 NAT 규칙이 지정된 경우 NAT 규칙의 인터페이스 순서는 "nat (inside,outside)..."입니다. 서버가 외부의 호스트에 대한 새 연결을 시작하는 경우 translate_hit 카운터가 증가합니다.

Untranslate_hits: NAT 규칙과 역방향으로 일치하는 새 연결 수입니다.

NAT 규칙에서 내부 서버가 외부 인터페이스로 변환되도록 지정하는 경우 NAT 규칙의 인터페이스 순서는 "nat (inside,outside)..."입니다. ASA 외부의 클라이언트가 내부의 서버에 대한 새 연결을 시작하는 경우 untranslate_hit 카운터가 증가합니다.

새 NAT 규칙에 translate_hits 또는 untranslate_hits가 없는 경우 트래픽이 ASA에 도착하지 않거나 NAT 테이블에서 우선순위가 더 높은 다른 규칙이 트래픽과 일치함을 의미합니다.

NAT 문제 해결 방법론

샘플 패킷이 ASA의 적절한 NAT 컨피그레이션 규칙과 일치하는지 확인하려면 패킷 추적기를 사용합니다. 적중되는 NAT 정책 규칙을 파악하려면 show nat detail 명령을 사용합니다. 연결이 예상과 다른 NAT 컨피그레이션과 일치하면 다음 질문에 대한 트러블슈팅을 수행합니다.

- 트래픽을 처리하려는 NAT 규칙보다 우선하는 다른 NAT 규칙이 있습니까?
- 개체 정의가 너무 광범위하고(서브넷 마스크가 너무 짧음, 예: 255.0.0.0) 이 트래픽이 잘못된 규칙과 일치하게 하는 다른 NAT 규칙이 있습니까?
- 수동 NAT 정책의 순서가 잘못되어 패킷이 잘못된 규칙과 일치합니까?
- NAT 규칙이 잘못 구성되어 규칙이 트래픽과 일치하지 않습니까?

샘플 문제 및 해결 방법은 다음 섹션을 참조하십시오.

NAT 컨피그레이션의 일반적인 문제

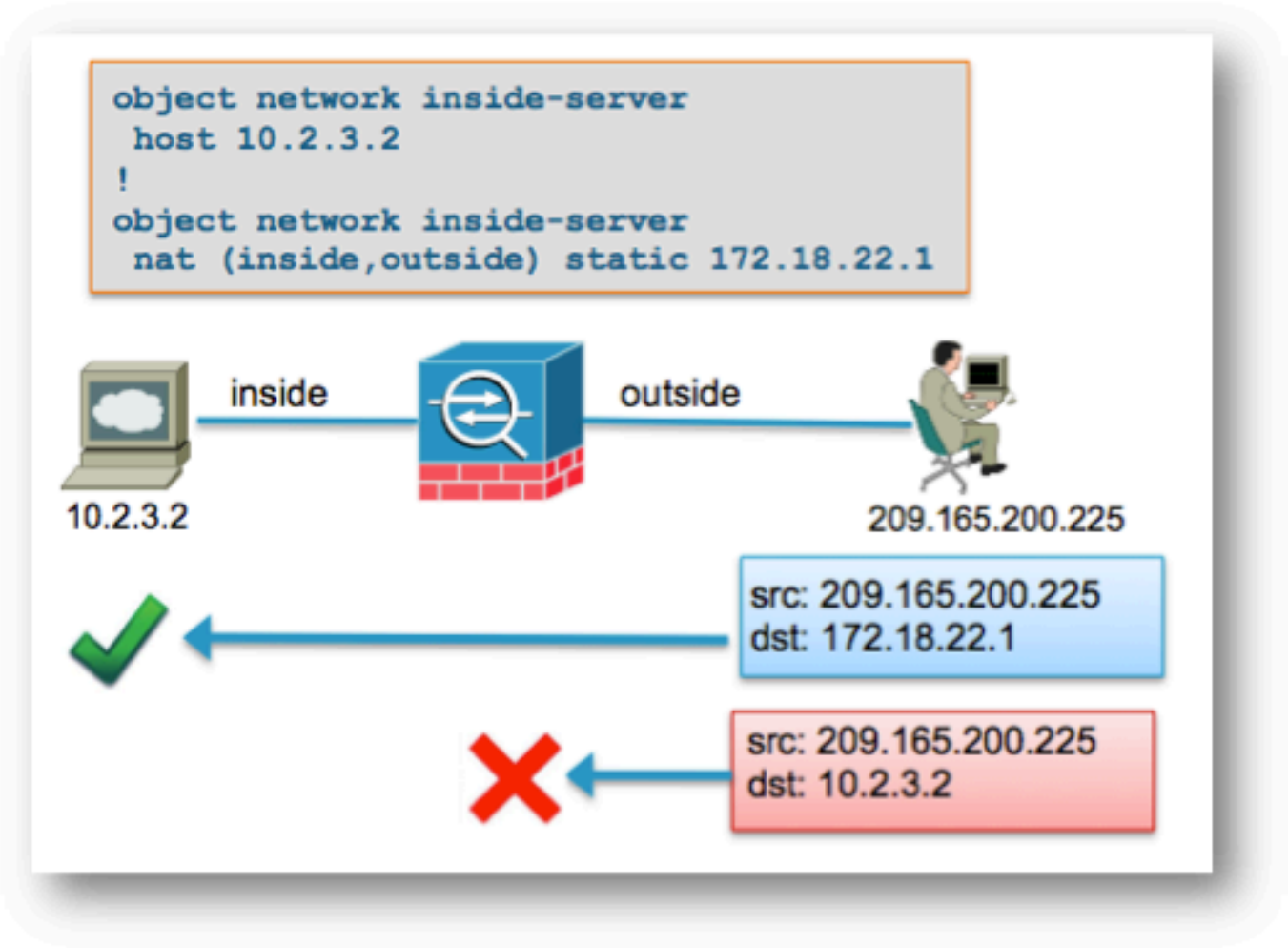
다음은 ASA에서 NAT를 구성할 때 흔히 발생하는 몇 가지 문제입니다.

문제: NAT RPF(Reverse Path Failure)로 인해 트래픽이 실패함 오류: 순방향 및 역방향 흐름에 대해 비대칭 NAT 규칙이 일치함

NAT RPF 검사는 ASA에서 TCP 동기화(SYN)와 같이 전달 방향으로 변환되는 연결이 TCP SYN/승인(ACK)과 같은 동일한 NAT 규칙에 의해 반대 방향으로 변환되도록 합니다.

가장 일반적으로 이 문제는 NAT 문의 로컬(변환되지 않은) 주소로 향하는 인바운드 연결에 의해 발생합니다. 기본 레벨에서 NAT RPF는 서버에서 클라이언트로의 역방향 연결이 동일한 NAT 규칙과 일치하는지 확인합니다. 일치하지 않으면 NAT RPF 확인에 실패합니다.

예: 209.165.200.225



192.168.200.225의 외부 호스트가 로컬(변환되지 않은) IP 주소 10.2.3.2로 직접 목적지인 패킷을 전송하면, ASA는 패킷을 삭제하고 이 syslog를 로깅합니다.

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

해결책:

먼저 호스트가 올바른 전역 NAT 주소로 데이터를 전송해야 합니다. 호스트가 올바른 주소로 향하는 패킷을 전송하는 경우, 연결에서 적중된 NAT 규칙을 확인하십시오.

NAT 규칙이 올바르게 정의되었는지, 그리고 NAT 규칙에서 참조하는 개체가 올바른지 확인하십시오. 또한 NAT 규칙의 순서가 적절한지 확인합니다.

거부된 패킷의 세부사항을 지정하려면 packet tracer 유틸리티를 사용합니다. 패킷 추적기는 RPF 검사 실패로 인해 삭제된 패킷을 표시해야 합니다.

다음으로, NAT 단계 및 NAT-RPF 단계에서 적중되는 NAT 규칙을 확인하기 위해 패킷 추적기의 출력을 확인합니다.

패킷이 NAT RPF-check 단계의 NAT 규칙과 일치하면(역방향 흐름이 NAT 변환에 도달함을 나타냄), NAT 단계의 규칙과 일치하지 않으면(순방향 흐름이 NAT 규칙에 도달하지 않음을 나타냄) 패킷이 삭제됩니다.

이 출력은 이전 다이어그램에 표시된 시나리오와 일치합니다. 여기서 외부 호스트는 전역(변환된) IP 주소가 아닌 서버의 로컬 IP 주소로 트래픽을 잘못 전송합니다.

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80



    .....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

패킷이 올바른 매핑된 IP 주소인 172.18.22.1로 갈 경우, 패킷은 전달 방향의 UN-NAT 단계에서 올바른 NAT 규칙을 매칭하고, NAT RPF-check 단계에서 동일한 규칙을 매칭합니다.

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
```

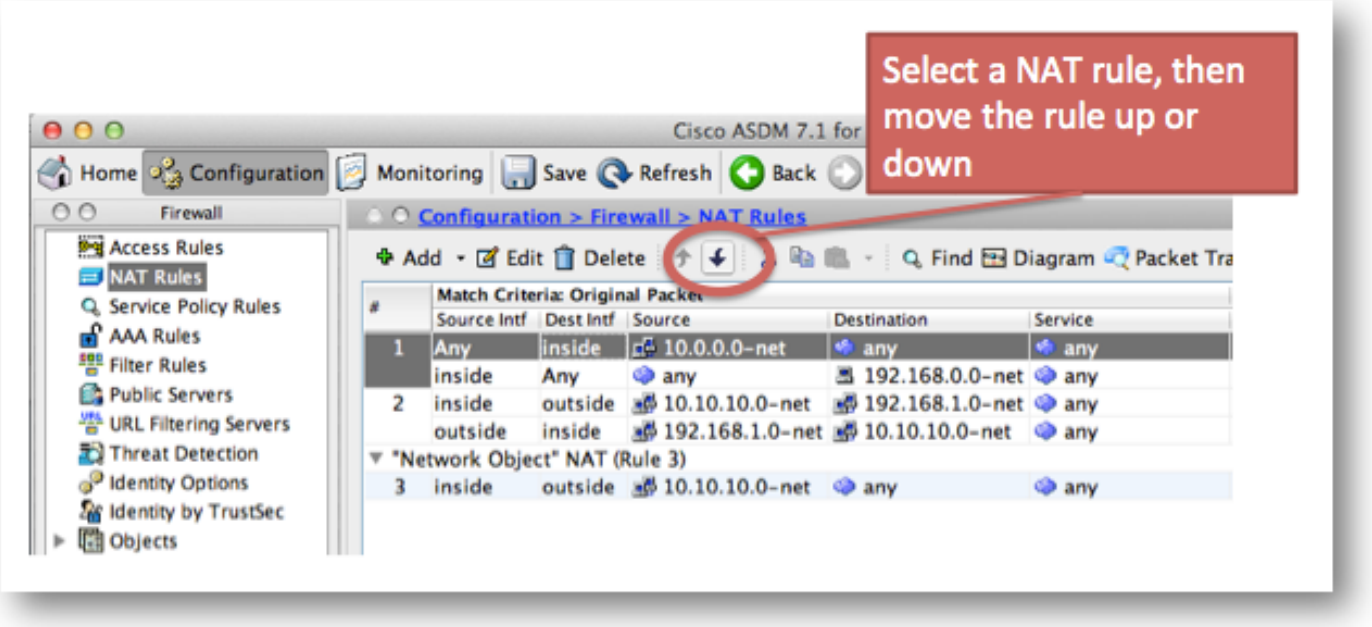
```
Subtype: rpf-check
Result:

ALLOW


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

문제: 수동 NAT 규칙의 순서가 잘못되어 잘못된 패킷 일치가 발생합니다.

수동 NAT 규칙은 컨피그레이션에서의 모양을 기반으로 처리됩니다. 매우 광범위한 NAT 규칙이 컨피그레이션에서 첫 번째로 나열되는 경우 NAT 테이블에서 좀 더 아래에 있는 또 다른 좀 더 구체적인 규칙을 재정의할 수 있습니다. 어떤 NAT 규칙이 트래픽에 도달하는지 확인하려면 패킷 추적기를 사용합니다. 수동 NAT 항목을 다른 순서로 재배열해야 할 수 있습니다.

해결책:

ASDM을 사용하여 NAT 규칙의 순서를 조정합니다.



해결책:

규칙을 제거하고 특정 라인 번호에 다시 삽입하는 경우 NAT 규칙은 CLI와 함께 순서를 변경할 수 있습니다. 특정 라인에 새 규칙을 삽입하려면 인터페이스가 지정된 직후 라인 번호를 입력합니다.

예:

```
ASA(config)#

nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net
```

문제

NAT 규칙이 너무 광범위하며 일부 트래픽을 실수로 매칭합니다. 너무 광범위한 객체를 사용하는 NAT 규칙이 생성되는 경우가 있습니다. 이러한 규칙이 NAT 테이블의 상단 근처에 있는 경우(예: 섹션 1의 상단), 의도한 것보다 더 많은 트래픽을 매칭할 수 있으며, NAT 규칙이 테이블 아래쪽으로 더 멀리 떨어지면 결코 히트가 발생하지 않습니다.

솔루션

트래픽이 너무 광범위한 객체 정의를 가진 규칙과 일치하는지 확인하려면 packet tracer를 사용합니다. 이 경우, 해당 객체의 범위를 줄이거나 NAT 테이블 아래로 더 멀리 규칙을 이동하거나 NAT 테이블의 after-auto 섹션(섹션 3)으로 규칙을 이동해야 합니다.

문제

NAT 규칙은 잘못된 인터페이스로 트래픽을 전환합니다. NAT 규칙은 패킷이 ASA를 이그레스(egress)하는 인터페이스를 결정할 때 라우팅 테이블보다 우선할 수 있습니다. 인바운드 패킷이 NAT 문에서 변환된 IP 주소와 일치하는 경우 이그레스 인터페이스를 결정하기 위해 NAT 규칙이 사용됩니다.

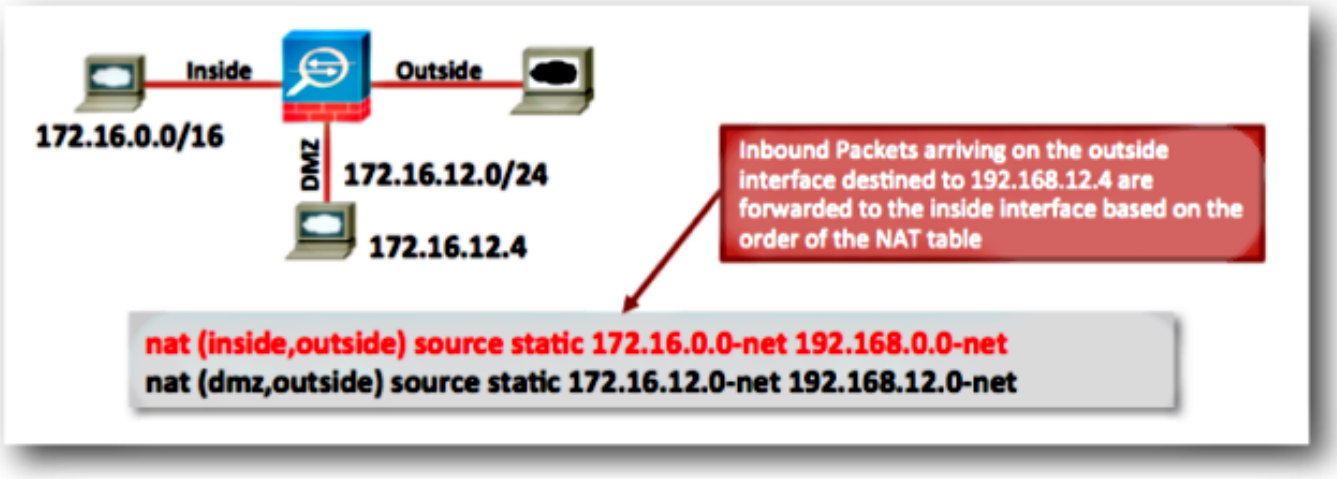
NAT 전환 확인(라우팅 테이블을 재정의할 수 있는 것)은 인터페이스에 도착하는 인바운드 패킷에 대한 목적지 주소 변환을 지정하는 NAT 규칙이 있는지 확인합니다.

해당 패킷 대상 IP 주소를 변환하는 방법을 명시적으로 지정하는 규칙이 없는 경우 전역 라우팅 테이블을 참조하여 이그레스 인터페이스를 결정합니다.

패킷 대상 IP 주소를 변환하는 방법을 명시적으로 지정하는 규칙이 있는 경우, NAT 규칙은 패킷을 변환의 다른 인터페이스로 가져오며 전역 라우팅 테이블은 효과적으로 우회됩니다.

이 문제는 외부 인터페이스에 도착하는 인바운드 트래픽에서 가장 자주 나타나며, 일반적으로 의도하지 않은 인터페이스로 트래픽을 전환하는 비순차적 NAT 규칙 때문입니다.

예:



솔루션:

이 문제는 다음 작업 중 하나로 해결할 수 있습니다.

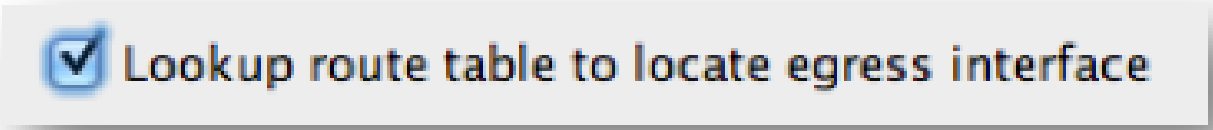
- 더 구체적인 항목이 먼저 나열되도록 NAT 테이블의 순서를 조정합니다.
- NAT 문에 겹치지 않는 전역 IP 주소 범위를 사용합니다.

NAT 규칙이 ID 규칙인 경우(즉, IP 주소가 규칙에 의해 변경되지 않음) route-lookup 키워드를 사용할 수 있습니다(NAT 규칙이 ID 규칙이 아니므로 이 키워드는 이전 예에 적용할 수 없음).

route-lookup 키워드는 ASA가 NAT 규칙과 매칭할 때 추가 검사를 수행하도록 합니다. ASA의 라우팅 테이블이 이 NAT 컨피그레이션이 패킷을 우회하는 것과 동일한 이그레스 인터페이스로 패킷을 전달하는지 확인합니다.

라우팅 테이블 이그레스 인터페이스가 NAT 전환 인터페이스와 일치하지 않으면 NAT 규칙이 일치하지 않고(규칙이 생략됨) 패킷이 NAT 테이블을 아래로 계속 내려가 이후 NAT 규칙에 의해 처리됩니다.

route-lookup 옵션은 NAT 규칙이 ID NAT 규칙인 경우에만 사용할 수 있습니다. 즉, IP 주소가 규칙에 의해 변경되지 않습니다. NAT 라인 끝에 route-lookup을 추가하거나 ASDM의 NAT 규칙 컨피그레이션에서 Lookup route table to locate egress interface 확인란을 선택하는 경우 NAT 규칙당 route-lookup 옵션을 활성화할 수 있습니다.



문제: NAT 규칙을 사용하면 ASA에서 매핑된 인터페이스의 트래픽에 대해 ARP(Address Resolution Protocol)를 프록시합니다

전역 인터페이스의 NAT 문에서 전역 IP 주소 범위에 대한 ASA 프록시 ARP. NAT 문에 no-proxy-arp 키워드를 추가하면 NAT별 규칙에 따라 이 프록시 ARP 기능을 비활성화할 수 있습니다.

이 문제는 글로벌 주소 서브넷이 의도한 것보다 훨씬 더 크게 의도하지 않게 생성된 경우에도 나타납니다.

솔루션

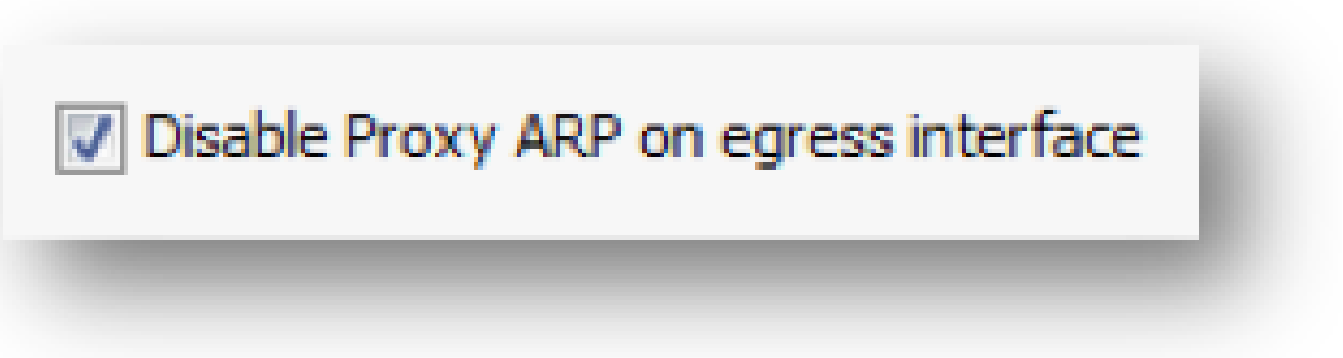
가능한 경우 no-proxy-arp 키워드를 NAT 라인에 추가합니다.

예:

<#root>

```
ASA(config)#

object network inside-server

ASA(config-network-object)#

nat (inside,outside) static 172.18.22.1 no-proxy-arp

ASA(config-network-object)#

end

ASA#
  ASA#

 show run nat

object network inside-server
 nat (inside,outside) static 172.18.22.1

no-proxy-arp

ASA#
```

이 작업은 ASDM에서도 수행할 수 있습니다. NAT 규칙 내에서 Disable Proxy ARP on egress interface 확인란을 선택합니다.



.

관련 정보

- 비디오: DMZ 서버 액세스를 위한 ASA 포트 전달(버전 8.3 및 8.4)
- 기본 ASA NAT 컨피그레이션: ASA 버전 8.3 이상의 DMZ에 있는 웹 서버
- 책 2: Cisco ASA Series 방화벽 CLI 컨피그레이션 가이드, 9.1
- 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.