Cisco Secure ASA 방화벽 컨피그레이션에서 NAT 및 PAT 문 사용 예시

목차

소개

이 문서에서는 Cisco ASA(Secure Adaptive Security Appliance) 방화벽의 기본 NAT(Network Address Translation) 및 PAT(Port Address Translation) 컨피그레이션의 예를 제공합니다.이 문서에서는 간소화된 네트워크 다이어그램도 제공합니다.자세한 내용은 ASA 소프트웨어 버전에 대한 ASA 설명서를 참조하십시오.

이 문서는 Cisco 장치에 대한 맞춤형 분석을 제공합니다.

자세한 내용은 ASA 5500/5500-X Series Security Appliances의 ASA에서 NAT 컨피그레이션을 참조하십시오.

사전 요구 사항

요구 사항

Cisco는 Cisco Secure ASA 방화벽에 대한 지식을 보유하고 있는 것이 좋습니다.

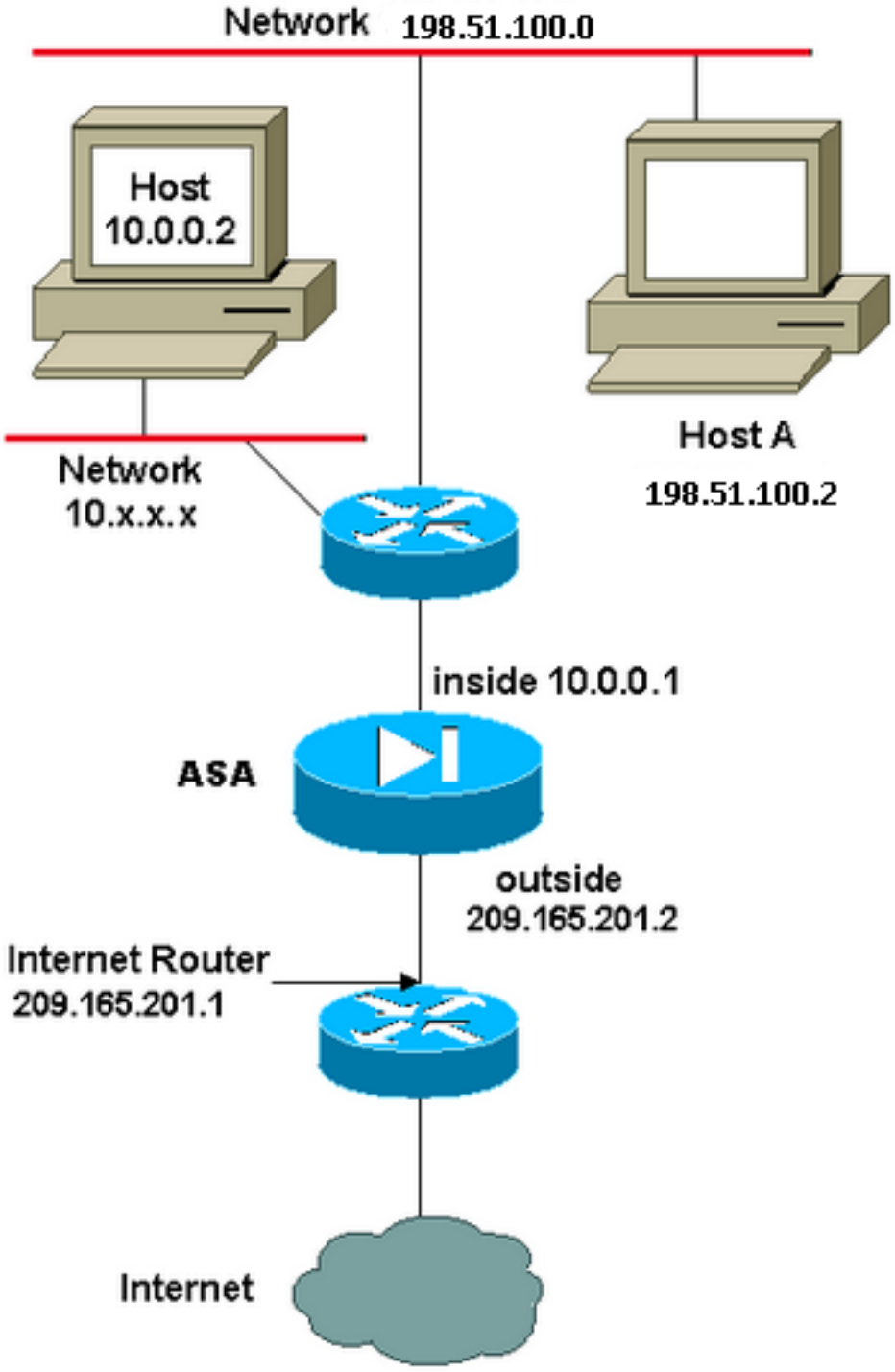
사용되는 구성 요소

이 문서의 정보는 Cisco Secure ASA Firewall Software 버전 8.4.2 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 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Configure(구성) - 수동 및 자동 NAT를 사용하는 다중 NAT 문

네트워크 다이어그램



이 예에서 ISP는 네트워크 관리자에게 209.165.201.1~209.165.201.30 범위의 IP 주소 블록 209.165.201.0/27을 제공합니다. 네트워크 관리자는 인터넷 라우터의 내부 인터페이스에 209.165.201.1을 할당하고 ASA의 외부 인터페이스에 209.165.201.2을 할당합니다.

네트워크 관리자는 198.51.100.0/24네트워크에 클래스 C 주소가 이미 할당되어 있으며 인터넷에 액세스하기 위해 이러한 주소를 사용하는 일부 워크스테이션이 있습니다.이 워크스테이션에는 유효한 주소가 이미 있으므로 주소 변환이 필요하지 않습니다.그러나 새 워크스테이션은 10.0.0.0/8 네트워크에 주소가 할당되며 번역할 필요가 있습니다. 10.x.x.x는 RFC 1918에 따라 라우팅 불가능한 주소 공간 중 하나이기 때문입니다.

이 네트워크 설계를 수용하려면 네트워크 관리자가 ASA 컨피그레이션에서 2개의 NAT 문과 1개의 전역 풀을 사용해야 합니다.

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
```

```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

이 컨피그레이션은 198.51.100.0/24 네트워크의 아웃바운드 트래픽의 소스 주소를 변환하지 않습니다.10.0.0.0/8 네트워크의 소스 주소를 209.165.201.3~209.165.201.30 범위의 주소로 변환합니다.

> **참고:**NAT 정책을 사용하는 인터페이스가 있고 다른 인터페이스에 전역 풀이 없는 경우 NAT 예외를 설정하려면 nat 0을 사용해야 합니다.

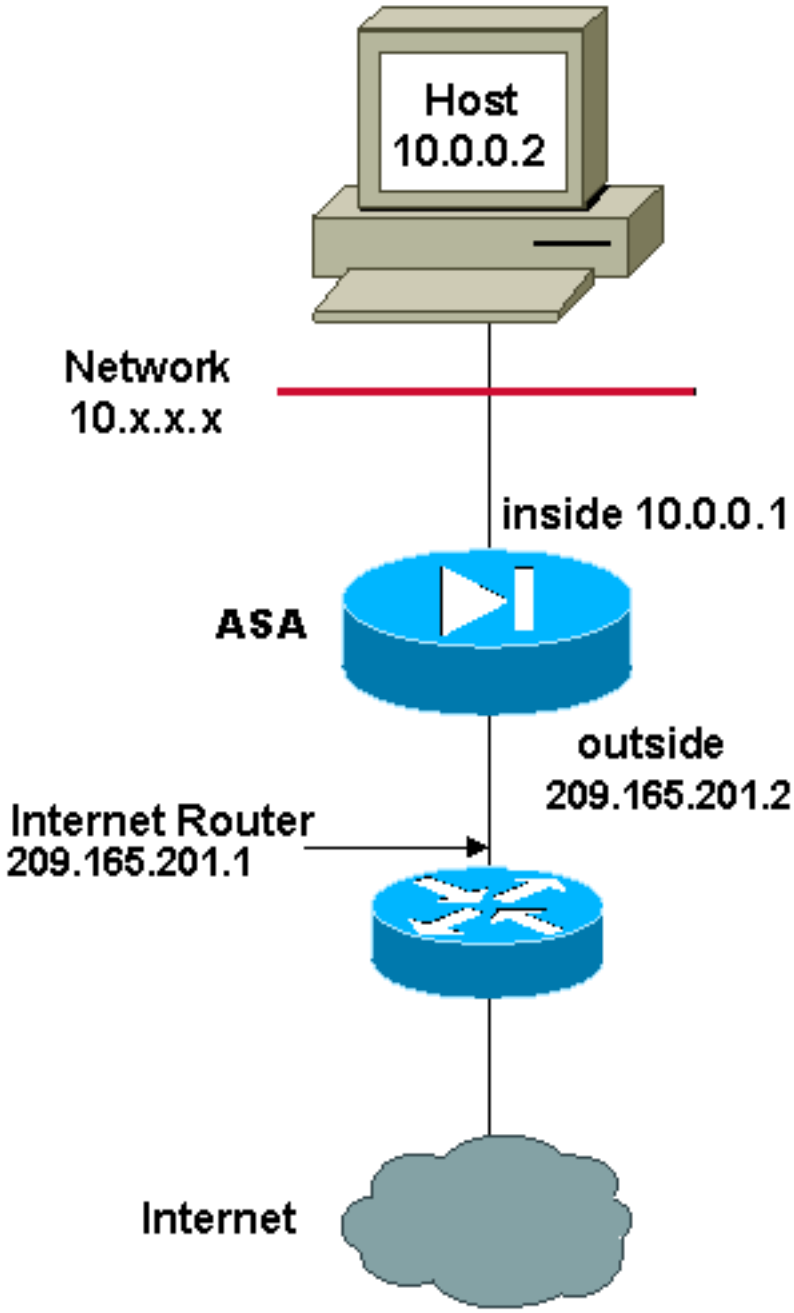
ASA 버전 8.3 이상

컨피그레이션은 다음과 같습니다.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

구성 - 여러 글로벌 풀

네트워크 다이어그램



이 예에서 네트워크 관리자는 인터넷에 등록된 두 개의 IP 주소 범위를 가집니다.네트워크 관리자는 10.0.0.0/8 범위에 있는 모든 내부 주소를 등록된 주소로 변환해야 합니다.네트워크 관리자가 사용해야 하는 IP 주소의 범위는 209.165.201.1~209.165.201.30 및 209.165.200.225~209.165.200.254입니다. 네트워크 관리자는 다음을 사용하여 이 작업을 수행할 수 있습니다.

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> **참고:**와일드카드 주소 지정 체계는 NAT 문에 사용됩니다.이 명령문은 ASA가 인터넷으로 나갈 때 내부 소스 주소를 변환하도록 지시합니다.이 명령의 주소는 원하는 경우 더 구체적일 수 있습니다.

ASA 버전 8.3 이상

컨피그레이션은 다음과 같습니다.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

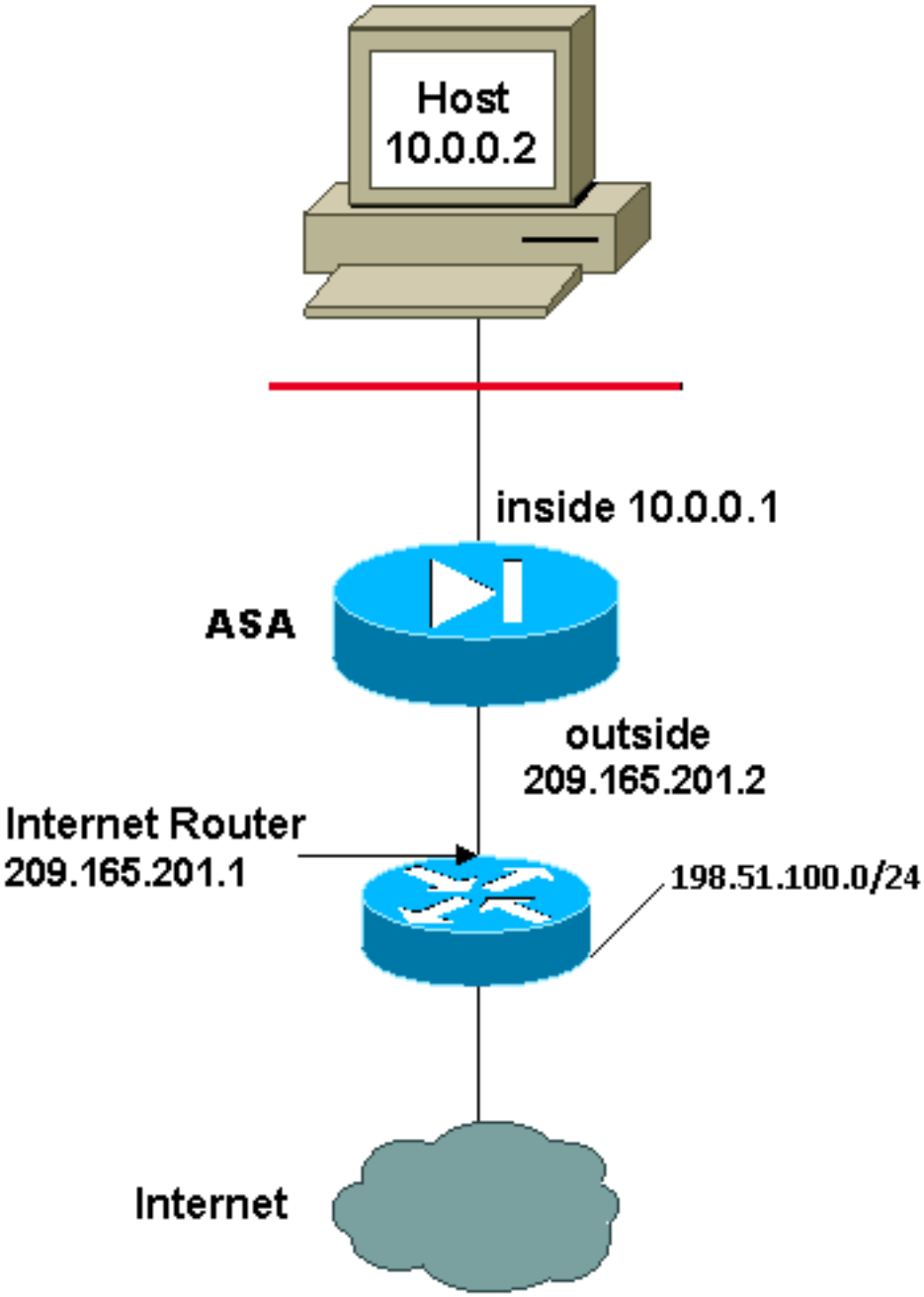
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

구성 - NAT와 PAT 문 혼합

네트워크 다이어그램



이 예에서 ISP는 네트워크 관리자에게 회사가 사용할 주소 범위를 209.165.201.1~209.165.201.30으로 제공합니다.네트워크 관리자는 인터넷 라우터의 내부 인터페이스에는 209.165.201.1을, ASA의 외부 인터페이스에는 209.165.201.2을 사용하기로 결정했습니다.그런 다음 NAT 풀에 사용할 209.165.201.3~209.165.201.30이 표시됩니다.그러나 네트워크 관리자는 ASA를 탈퇴하려는 사용자가 한 번에 28명 이상 있을 수 있음을 알고 있습니다.네트워크 관리자는 여러 사용자가 동시에 하나의 주소를 공유할 수 있도록 209.165.201.30을 가져와서 PAT 주소로 지정하기로 결정했습니다.

이러한 명령은 ASA에서 처음 27명의 내부 사용자가 ASA를 통과하도록 소스 주소를 209.165.201.3~209.165.201.29으로 변환하도록 지시합니다.이러한 주소가 모두 소진되면 ASA는 NAT 풀의 주소 중 하나가 사용 가능해질 때까지 모든 후속 소스 주소를 209.165.201.30으로 변환합니다.

참고:와일드카드 주소 지정 체계는 NAT 문에 사용됩니다.이 명령문은 ASA가 인터넷으로 나갈 때 내부 소스 주소를 변환하도록 지시합니다.이 명령의 주소는 원하는 경우 더 구체적일 수 있습니다.

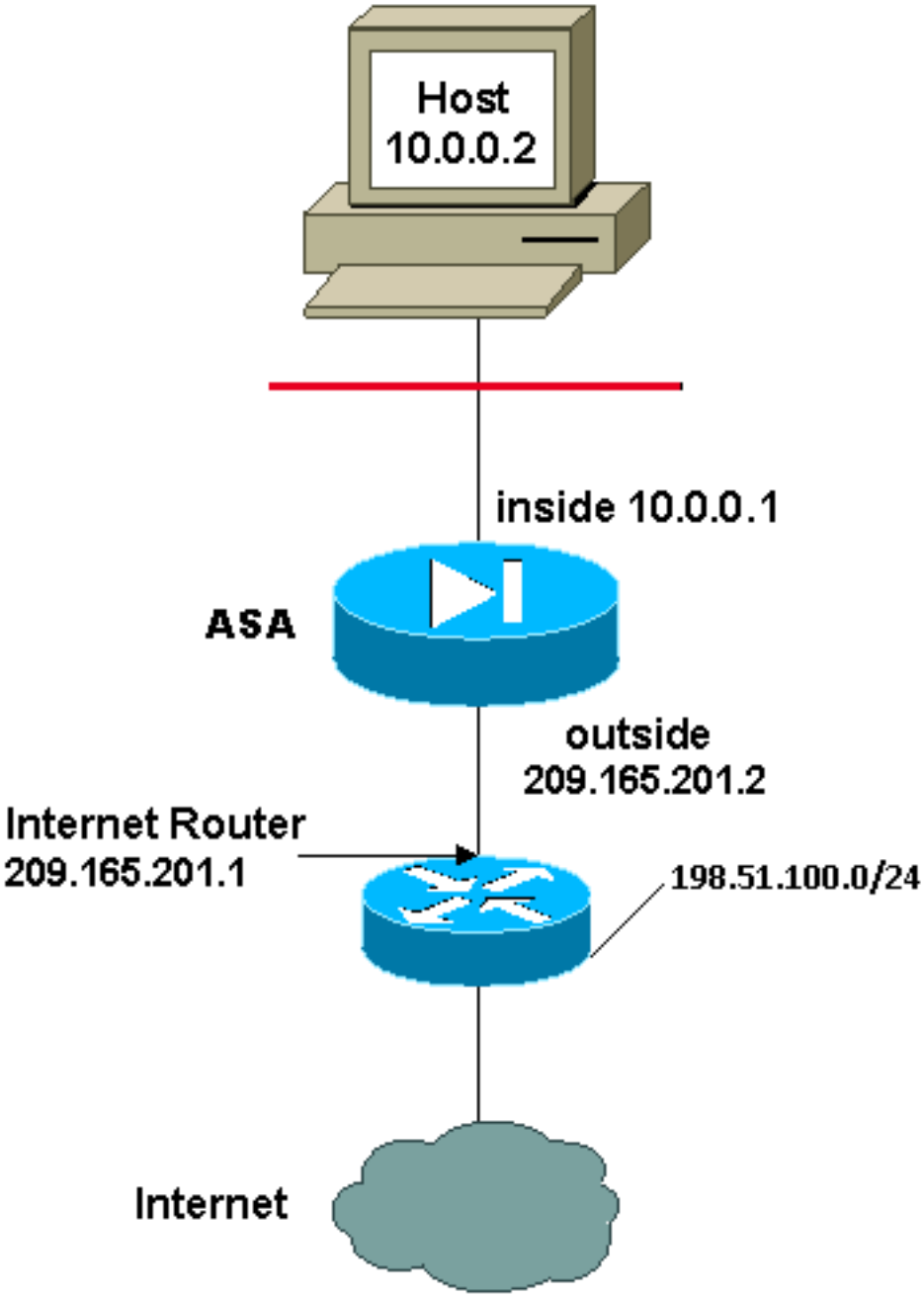
ASA 버전 8.3 이상

컨피그레이션은 다음과 같습니다.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configure(구성) - 수동 명령문이 있는 다중 NAT 문

네트워크 다이어그램



이 예에서 ISP는 다시 네트워크 관리자에게 209.165.201.1~209.165.201.30 범위의 주소를 제공합니다. 네트워크 관리자는 인터넷 라우터의 내부 인터페이스에 209.165.201.1을 할당하고 ASA의 외부 인터페이스209.165.201.2 할당합니다.

그러나 이 시나리오에서는 다른 프라이빗 LAN 세그먼트가 인터넷 라우터에서 분리됩니다.네트워크 관리자는 이 두 네트워크의 호스트가 서로 통신할 때 전역 풀의 주소를 낭비하지 않는 것을 선호합니다.네트워크 관리자는 인터넷으로 이동할 때 모든 내부 사용자(10.0.0.0/8)의 소스 주소를 변환해야 합니다.

이 컨피그레이션은 소스 주소가 10.0.0.0/8이고 대상 주소가 198.51.100.0/24인 주소를 변환하지 않습니다. 10.0.0.0/8 네트워크 내에서 시작된 트래픽에서 소스 주소를 변환하고 198.51.100.0/24 이외의 다른 위치로 향하는 트래픽을 209.165.201.3~209.165.201.30 범위의 주소로 변환합니다.

Cisco 디바이스에서 **write terminal** 명령의 출력이 있는 경우 Output Interpreter Tool(등록된 고객만 해당)을 사용할 수 있습니다.

ASA 버전 8.3 이상

컨피그레이션은 다음과 같습니다.

Using the Manual Nat statements:

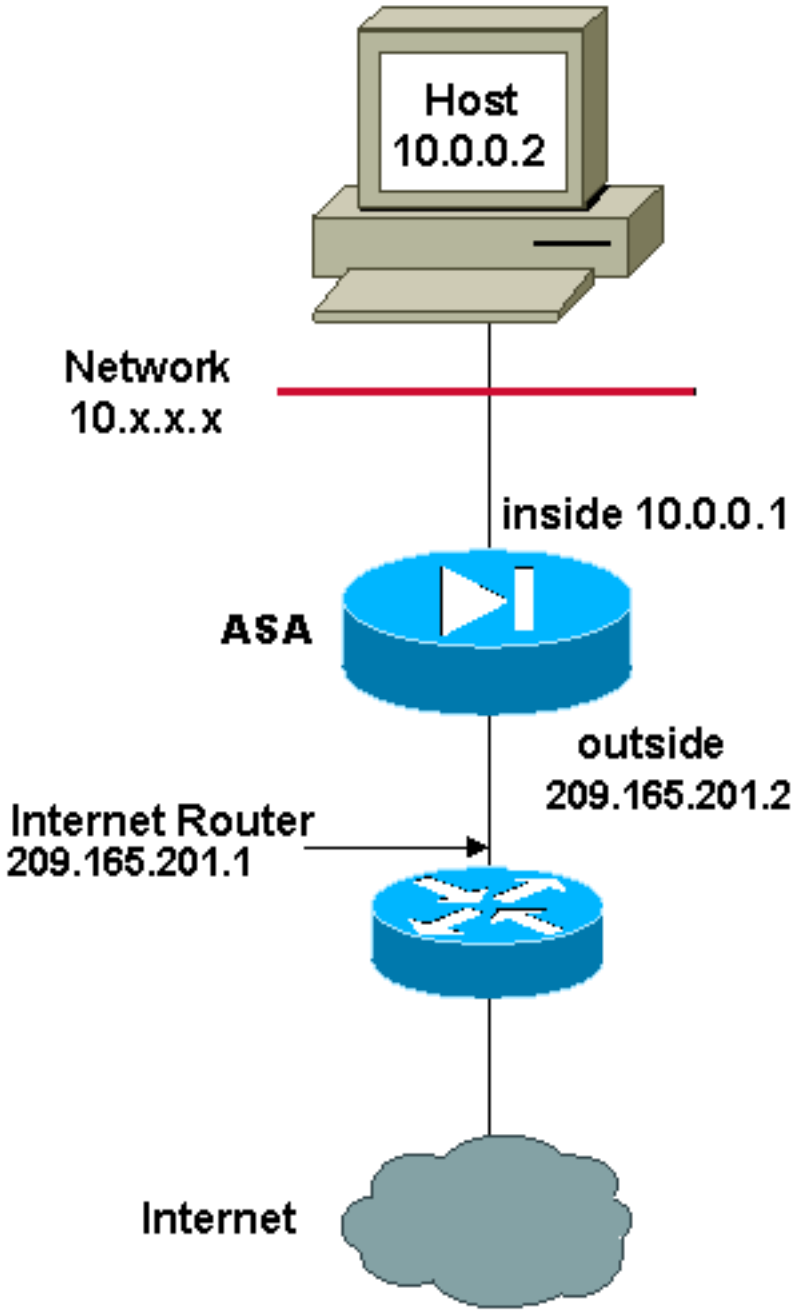
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

구성 - 정책 NAT 사용

네트워크 다이어그램



0 이외의 NAT ID에 대해 nat 명령과 함께 액세스 목록을 사용할 경우 정책 NAT를 활성화합니다.

정책 NAT를 사용하면 액세스 목록의 소스 및 대상 주소(또는 포트)의 사양에 따라 주소 변환에 대한 로컬 트래픽을 식별할 수 있습니다.일반 NAT는 소스 주소/포트만 사용합니다.정책 NAT는 소스 및 대상 주소/포트를 모두 사용합니다.

> **참고:**NAT 면제(nat 0 access-list)를 제외한 모든 유형의 NAT 지원 정책 NAT입니다.NAT 면제는 로컬 주소를 식별하기 위해 ACL(Access Control List)을 사용하지만 포트는 고려되지 않으므로 정책 NAT와는 다릅니다.

정책 NAT를 사용하면 소스/포트 및 대상/포트 조합이 각 문에 대해 고유한 경우 동일한 로컬 주소를 식별하는 여러 NAT 또는 고정 문을 생성할 수 있습니다.그런 다음 각 소스/포트 및 대상/포트 쌍에 서로 다른 전역 주소를 일치시킬 수 있습니다.

이 예에서 네트워크 관리자는 포트 80(웹) 및 포트 23(텔넷)에 대해 대상 IP 주소 172.30.1.11에 대한 액세스를 제공해야 하지만 두 개의 다른 IP 주소를 소스 주소로 사용해야 합니다 .209.165.201.3은 웹의 소스 주소로 사용되고 209.165.201.4은 텔넷에 사용되며 10.0.0.0/8 범위에

있는 모든 내부 주소를 변환해야 합니다.네트워크 관리자는 다음을 사용하여 이 작업을 수행할 수 있습니다.

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA 버전 8.3 이상

컨피그레이션은 다음과 같습니다.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> **참고:**ASA 버전 8.4에서 NAT 및 PAT 컨피그레이션에 대한 자세한 내용은 NAT 정보를 참조하십시오.
>
> ASA 버전 8.4의 액세스 목록 컨피그레이션에 대한 자세한 내용은 액세스 목록 정보를 참조하십시오.

다음을 확인합니다.

웹 브라우저를 사용하여 HTTP를 통해 웹 사이트에 액세스해 보십시오.이 예에서는 198.51.100.100에서 호스팅되는 사이트를 사용합니다. 연결이 성공하면 다음 섹션의 출력을 ASA CLI에서 볼 수 있습니다.

연결

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
flags UIO
```

ASA는 스테이트풀 방화벽이며, 방화벽 연결 테이블의 ***연결***과 일치하기 때문에 웹 서버의 반환 트래픽이 방화벽을 통해 다시 허용됩니다.존재하는 연결과 일치하는 트래픽은 인터페이스 ACL에 의해 차단되지 않고 방화벽을 통해 허용됩니다.

이전 출력에서 내부 인터페이스의 클라이언트는 외부 인터페이스의 198.51.100.100 호스트에 대한 연결을 설정했습니다.이 연결은 TCP 프로토콜로 이루어지며 6초 동안 유휴 상태가 되었습니다.연결 플래그는 이 연결의 현재 상태를 나타냅니다.연결 플래그에 대한 자세한 내용은 ASA TCP Connection Flags(ASA TCP 연결 플래그)를 참조하십시오.

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.0.0.2/57431 (209.165.201.3/57431)
```

ASA 방화벽은 정상 작동 중에 syslog를 생성합니다.syslogs는 로깅 컨피그레이션을 기반으로 자세한 범위를 제공합니다.출력은 레벨 6 또는 '정보' 레벨에서 보이는 두 개의 syslog**를** 보여줍니다.

이 예에서는 두 개의 syslog가 생성됩니다.첫 번째 메시지는 방화벽이 **변환**을 구축했음을 나타내는 로그 메시지, 특히 동적 TCP 변환(PAT)입니다. 트래픽이 내부에서 외부 인터페이스로 이동하는 동안 소스 IP 주소 및 포트와 변환된 IP 주소 및 포트를 나타냅니다.

두 번째 syslog는 방화벽이 클라이언트와 서버 간의 이 특정 트래픽에 대한 연결 테이블에 **연결**을 구축했음을 나타냅니다.이 연결 시도를 차단하도록 방화벽을 구성했거나 이 연결 생성을 방해하는 다른 요인(리소스 제약 조건 또는 잘못된 컨피그레이션)이 있는 경우 방화벽은 연결이 구축되었음을 나타내는 로그를 생성하지 않습니다.대신 연결이 거부되는 이유 또는 연결이 생성되는 것을 방해하는 요인에 대한 표시가 기록됩니다.

NAT 변환(Xlate)

```
ASA(config)# show xlate local 10.0.0.2
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

이 컨피그레이션의 일부로, 내부 호스트 IP 주소를 인터넷에서 라우팅 가능한 주소로 변환하기 위해 PAT가 구성됩니다.이러한 번역이 생성되었는지 확인하기 위해 xlate(translation) 테이블을 확인할 수 있습니다.명령 **show xlate는 local** 키워드 및 내부 호스트의 IP 주소와 결합되면 해당 호스트의 변환 테이블에 있는 모든 항목을 표시합니다.이전 출력에서는 내부 인터페이스와 외부 인터페이스

간에 이 호스트에 대해 현재 구축된 변환이 있음을 보여줍니다.내부 호스트 IP 및 포트는 컨피그레이션에 따라 10.165.200.226 주소로 변환됩니다.

나열된 플래그(**r i)는** 변환이 **동적** 및 포트맵임을 **나타냅니다**.서로 다른 NAT 컨피그레이션에 대한 자세한 내용은 NAT 정보를 참조하십시오.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.