듀얼 내부 네트워크용 ASA 구성

목차

소개

이 문서에서는 두 내부 네트워크를 사용하기 위해 소프트웨어 버전 9.x를 실행하는 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 9.x를 실행하는 Cisco ASA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

ASA 방화벽 뒤에 두 번째 내부 네트워크를 추가할 때 다음 중요한 정보를 고려하십시오.

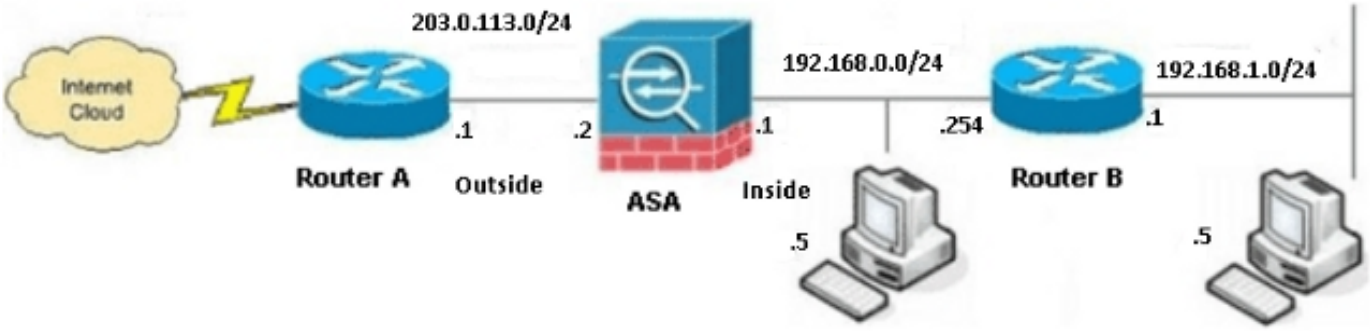
- ASA는 보조 주소 지정을 지원하지 않습니다.
- 현재 네트워크와 새로 추가된 네트워크 간의 라우팅을 수행하려면 ASA 뒤에 라우터를 사용해야 합니다.
- 모든 호스트의 기본 게이트웨이는 내부 라우터를 가리켜야 합니다.
- ASA를 가리키는 내부 라우터에 기본 경로를 추가해야 합니다.
- 내부 라우터에서 ARP(Address Resolution Protocol) 캐시를 지워야 합니다.

구성

ASA를 구성하려면 이 섹션에 설명된 정보를 사용합니다.

네트워크 다이어그램

다음은 이 문서의 예제에 사용되는 토폴로지입니다.



참고:이 컨피그레이션에서 사용되는 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용되는 RFC 1918 주소입니다.

ASA 9.x 구성

Cisco 디바이스에서 **write terminal** 명령의 출력이 있는 경우 Output Interpreter 툴(등록된 고객만 해당)을 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다.

다음은 소프트웨어 버전 9.x를 실행하는 ASA의 컨피그레이션입니다.

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
```

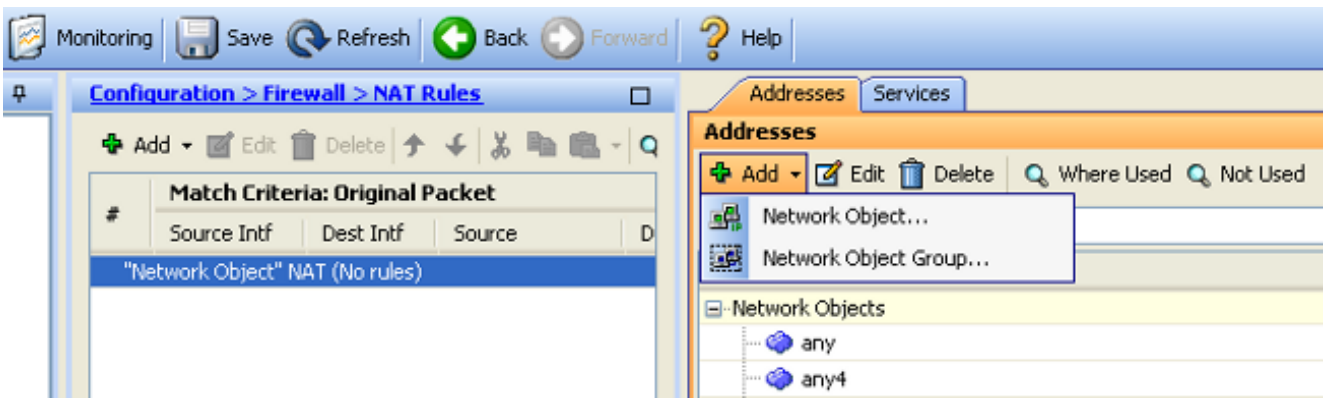
```
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

내부 호스트가 PAT를 사용하여 외부 네트워크에 액세스 허용

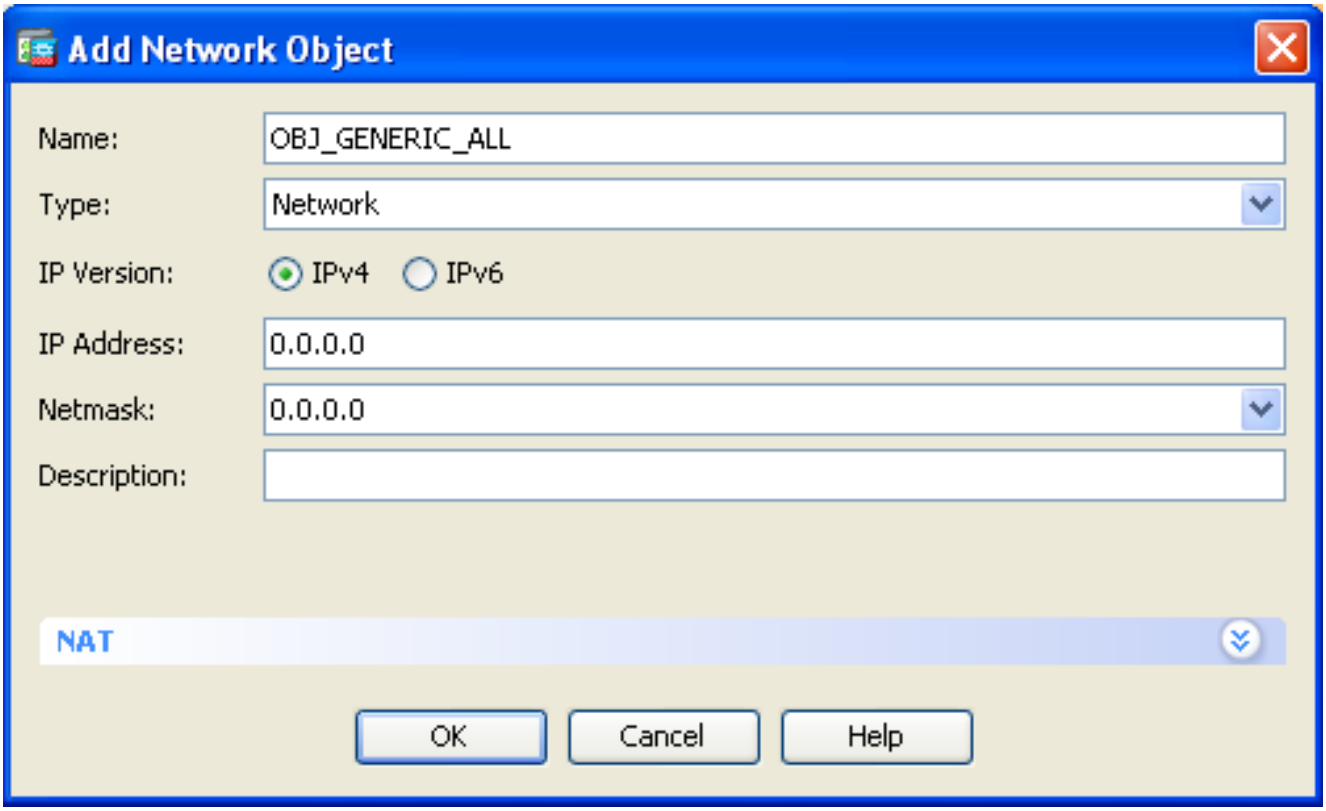
내부 호스트가 번역을 위해 단일 공용 주소를 공유하도록 하려면 PAT(Port Address Translation)를 사용합니다. 가장 간단한 PAT 컨피그레이션 중 하나는 모든 내부 호스트를 변환하여 외부 인터페이스 IP로 보이도록 합니다.이는 ISP에서 사용할 수 있는 라우팅 가능한 IP 주소 수가 몇 개 또는 한 개로 제한될 때 사용되는 일반적인 PAT 컨피그레이션입니다.

내부 호스트가 PAT를 사용하여 외부 네트워크에 액세스할 수 있도록 하려면 다음 단계를 완료합니다.

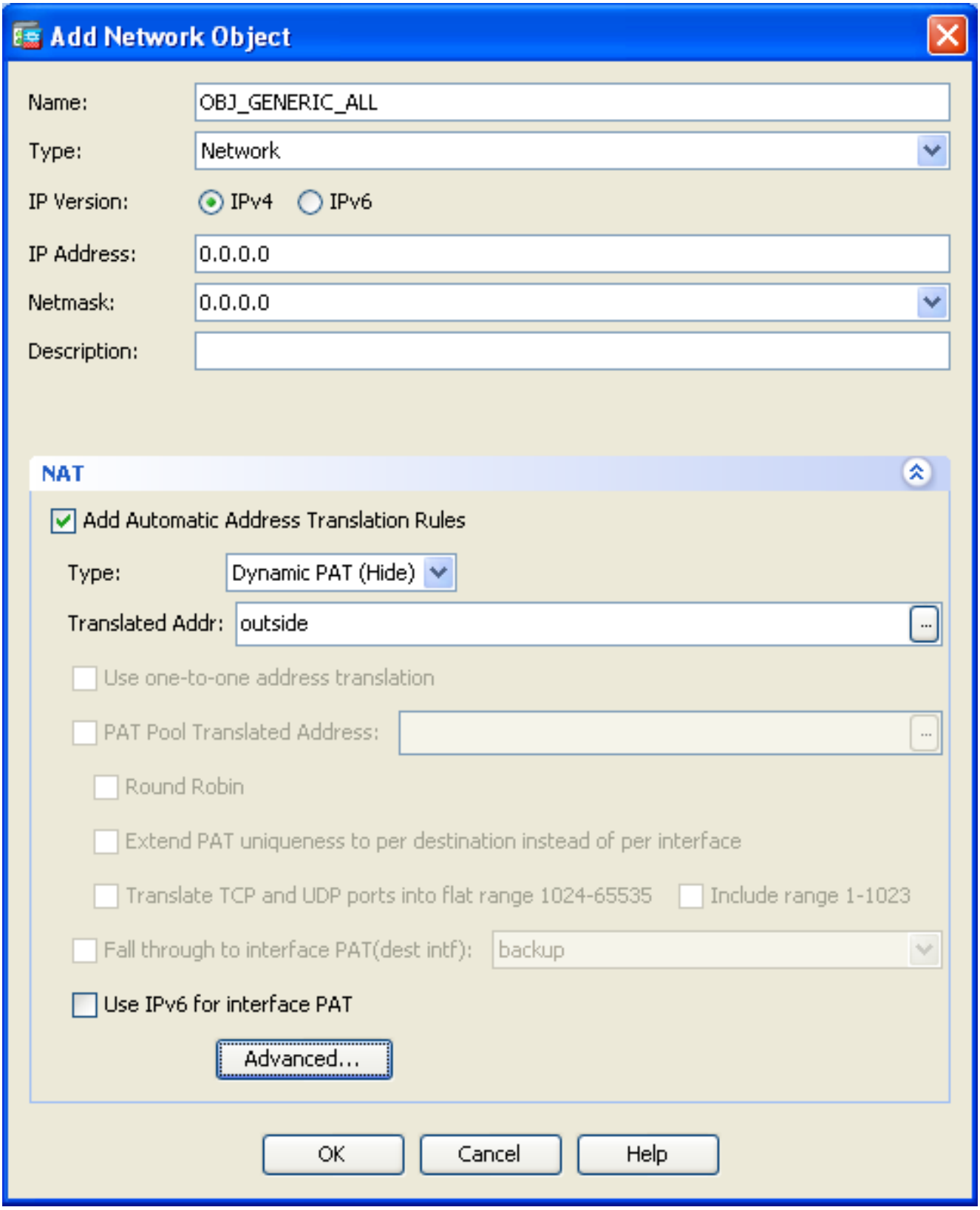
1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)로** 이동하고 **Add(추가)**를 클릭하고 **Network Object(네트워크 개체)를 선택하여 동적 NAT 규칙을 구성합니다.**



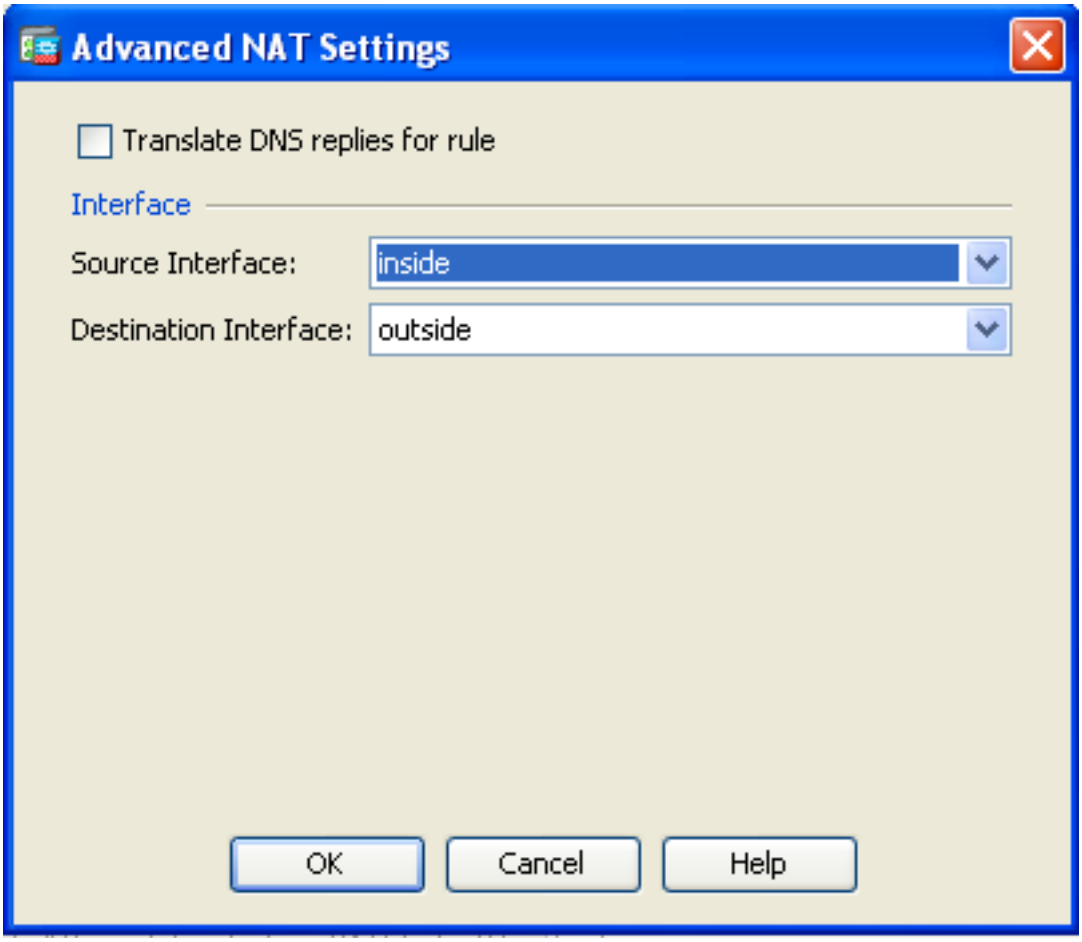
2. 동적 PAT가 필요한 네트워크/호스트/범위를 구성합니다.이 예에서는 모든 내부 서브넷을 선택했습니다.다음과 같이 변환하려는 특정 서브넷에 대해 이 프로세스를 반복해야 합니다.



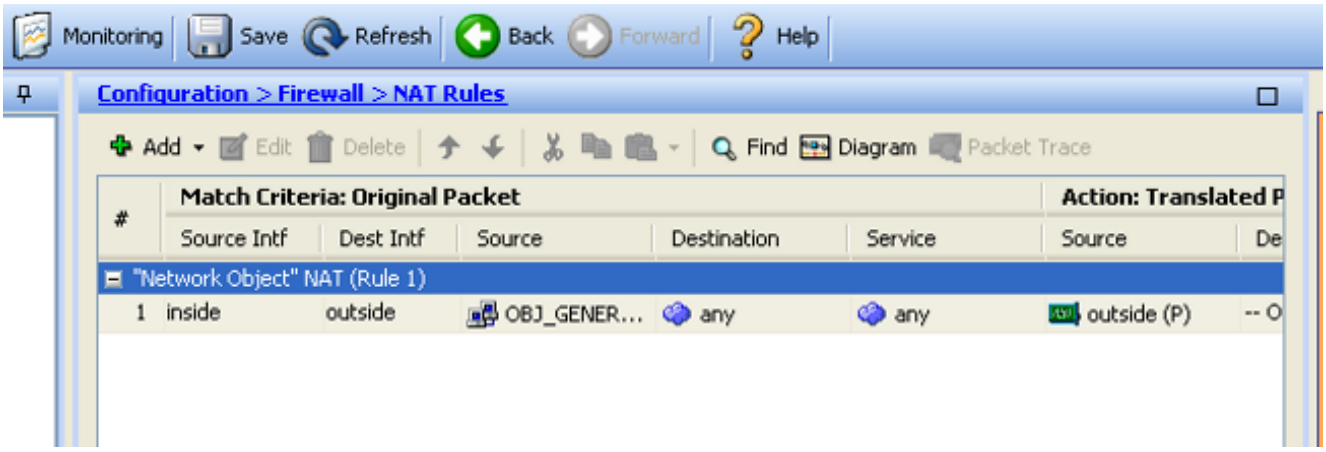
3. NAT를 클릭하고 **Add Automatic Address Translation Rule** 확인란을 선택하고 **Dynamic을** 입력한 다음 **Translated Addr 옵션을 설정하여 외부 인터페이스를 반영합니다.**줄임표 버튼을 클릭하면 외부 인터페이스와 같이 미리 구성된 객체를 선택할 수 있습니다.



4. 소스 및 대상 인터페이스를 선택하려면 Advanced를 클릭합니다.



5. 확인을 클릭한 다음 적용을 **클릭하여** 변경 사항을 적용합니다.완료되면 ASDM(Adaptive Security Device Manager)에 NAT 규칙이 표시됩니다.



라우터 B 컨피그레이션

다음은 라우터 B의 컨피그레이션입니다.

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하기 위해 웹 브라우저를 통해 HTTP를 통해 웹 사이트에 액세스합니다.

이 예에서는 IP 주소 *198.51.100.100에서 호스팅되는* 사이트를 사용합니다. 연결이 성공하면 다음 섹션에 제공된 출력을 ASA CLI에서 볼 수 있습니다.

연결

연결을 확인하려면 **show connection address** 명령을 입력합니다.

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
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 ACL(Access Control List)에 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.

> **참고:**연결 플래그에 대한 자세한 내용은 ASA TCP 연결 플래그(Connection Build-up 및 teardown) Cisco 문서를 참조하십시오.

문제 해결

컨피그레이션 문제를 해결하려면 이 섹션에 설명된 정보를 사용하십시오.

Syslog

syslogs를 보려면 show log 명령을 입력합니다.

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 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:192.168.1.5/58799 (203.0.113.2/58799)
```

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

이 예에서는 두 개의 syslog가 생성됩니다.첫 번째는 방화벽이 변환을 구축했음을 나타내는 로그 메시지입니다.특히 PAT(Dynamic TCP Translation)입니다. 트래픽이 내부에서 외부 인터페이스로 이동하는 동안 소스 IP 주소 및 포트, 변환된 IP 주소 및 포트를 나타냅니다.

두 번째 syslog는 방화벽이 클라이언트와 서버 간의 이 특정 트래픽에 대한 연결 테이블에 연결을 구축했음을 나타냅니다.이 연결 시도를 차단하도록 방화벽이 구성되었거나 이 연결의 생성을 방해하는 다른 요인(리소스 제약 조건 또는 컨피그레이션 오류 가능성)인 경우 방화벽은 연결이 구축되었음을 나타내는 로그를 생성하지 않습니다.대신 연결이 거부되는 이유 또는 연결을 만드는 것을 방해하는 요인에 대한 표시를 기록합니다.

패킷 추적기

패킷 추적기 기능을 활성화하려면 다음 명령을 입력합니다.

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

ASA의 패킷 추적기 기능을 사용하면 *시뮬레이션된* 패킷을 지정하고, 방화벽이 트래픽을 처리할 때 완료하는 다양한 단계, 검사 및 기능을 모두 볼 수 있습니다.이 툴을 사용하면 방화벽을 통과하도록 허용되어야 *한다고* 생각하는 트래픽의 예를 식별하고, 트래픽을 시뮬레이션하기 위해 5-튜플을 사용하는 것이 좋습니다.이전 예에서 패킷 추적기는 다음 조건을 충족하는 연결 시도를 시뮬레이션하기 위해 사용됩니다.

- 시뮬레이션된 패킷이 내부 인터페이스에 도착합니다.
- 사용되는 프로토콜은 TCP입니다.
- 시뮬레이션된 클라이언트 IP 주소는 192.168.1.5입니다.
- 클라이언트는 포트 1234에서 소싱된 트래픽을 전송합니다.
- 트래픽은 IP 주소 198.51.100.100의 서버로 전송됩니다.
- 트래픽은 포트 80으로 이동됩니다.

명령에 외부 인터페이스에 대한 언급이 없습니다.이는 패킷 추적기 설계 때문입니다.이 툴은 방화벽이 어떤 유형의 연결 시도를 어떻게 처리하는지, 여기에는 라우팅 방법과 어떤 인터페이스 밖으로 처리되는지 알려줍니다.

> **팁**:패킷 추적기 기능에 대한 자세한 내용은 *CLI, 8.4 및 8.6을 사용하여 Cisco ASA 5500 Series Configuration Guide*의 Tracing packets with Packet Tracer *섹션을* 참조하십시오.

캡처

캡처를 적용하려면 다음 명령을 입력합니다.

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
```

```
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA 방화벽은 인터페이스를 드나드는 트래픽을 캡처할 수 있습니다.이 캡처 기능은 트래픽이 방화벽에 도달하는지 또는 방화벽에서 출발하는지 확실하게 확인할 수 있으므로 환상적인 기능입니다 .위의 예에서는 내부 및 외부 인터페이스에서 capin 및 capout이라는 두 **캡처**의 컨피그레이션을 각각 보여줍니다.capture **명령**은 **match** 키워드를 사용하며, 이를 통해 캡처할 트래픽을 지정할 수 있습니다.

capin 캡처 예의 경우 *tcp 호스트 192.168.1.5 호스트 198.51.100.100과* 일치하는 내부 인터페이스(인그레스 또는 이그레스)에 표시되는 트래픽을 매칭하고자 합니다. 즉, 호스트 *192.168.1.5*에서 호스트1998.*01.5*01.5*50001호스트호스트에서 전송되는 모든 TCP 트래픽을 캡처하고자* 합니다 1.1.1.1.1.1.11111.11111011011001111111111 0.100 또는 그 반대입니다.**match** 키워드를 사용하면 방화벽에서 해당 트래픽을 양방향으로 캡처할 수 있습니다.외부 인터페이스에 대해 정의된 **capture** 명령은 방화벽이 해당 클라이언트 IP 주소에서 PAT를 수행하기 때문에 내부 클라이언트 IP 주소를 참조하지 않습니다.따라서 해당 클라이언트 IP 주소와 일치시킬 수 없습니다.대신 이 예에서는 **any를 사용하여** 가능한 모든 IP 주소가 해당 조건과 일치함을 나타냅니다.

캡처를 구성한 후 다시 연결을 설정하고 show capture***<capture_name>*** 명령을 사용하여 캡처를 볼 수 있습니다.이 예에서는 클라이언트가 캡처에서 볼 수 있는 TCP 3-way 핸드셰이크에 의해 분명하게 나타나듯이 서버에 연결할 수 있음을 확인할 수 있습니다.

관련 정보

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500-X Series 차세대 방화벽
- 의견 요청(RFC)
- Cisco ASA Series CLI 컨피그레이션 가이드, 9.0 정적 및 기본 경로 구성
- 기술 지원 및 문서 URL Cisco 시스템