PIX/ASA:static 명령 및 2개의 NAT 인터페이스 컨피그레이션으로 DNS Doctoring 수행 예

목차

소개

이 문서에서는 고정 NAT(Network Address Translation) 문을 사용하여 ASA 5500 Series Adaptive Security Appliance 또는 PIX 500 Series Security Appliance에서 DNS(Domain Name System) 설명서를 수행하기 위한 샘플 컨피그레이션을 제공합니다.DNS Doctoring을 사용하면 보안 어플라이언스에서 DNS A 레코드를 다시 작성할 수 있습니다.

DNS 재작성은 두 가지 기능을 수행합니다.

- DNS 클라이언트가 사설 인터페이스에 있을 때 DNS 회신의 공용 주소(라우팅 가능 또는 매핑된 주소)를 사설 주소(실제 주소)로 변환합니다.
- DNS 클라이언트가 공용 인터페이스에 있을 때 사설 주소를 공용 주소로 변환합니다.

참고: 이 문서의 컨피그레이션에는 두 개의 NAT 인터페이스가 있습니다.내부 및 외부.스태틱스 및 3개의 NAT 인터페이스(내부, 외부 및 dmz)를 사용하는 DNS 도킹의 예는 PIX/ASA를 참조하십시오.static 명령 및 3개의 NAT 인터페이스 컨피그레이션 예를 사용하여 DNS Doctoring을 수행합니다.

보안 어플라이언스에서 NAT를 사용하는 방법에 대한 자세한 내용은 PIX/ASA 7.x NAT 및 PAT 문을 참조하고 PIX에서 nat, global, static, pattern 및 access-list Commands and Port Redirection (Forwarding) on PIX를 참조하십시오.

사전 요구 사항

요구 사항

보안 어플라이언스에서 DNS 인증을 수행하려면 DNS 검사를 활성화해야 합니다.DNS 검사는 기본적으로 켜져 있습니다.꺼진 경우 이 문서의 뒷부분에서 DNS 검사 구성 섹션을 참조하여 다시 활성화합니다.DNS 검사가 활성화되면 보안 어플라이언스는 다음 작업을 수행합니다.

- static 및 nat 명령(DNS 재작성)을 사용하여 완료된 컨피그레이션을 기반으로 DNS 레코드를 변환합니다. 변환은 DNS 회신의 A 레코드에만 적용됩니다.따라서 PTR 레코드를 요청하는 역방향 조회는 DNS 재작성의 영향을 받지 않습니다.**참고:** 여러 PAT 규칙이 각 A 레코드에 적용되며 사용할 PAT 규칙이 모호하기 때문에 DNS 재작성은 고정 PAT(Port Address Translation)와 호환되지 않습니다.
- 최대 DNS 메시지 길이를 적용합니다(기본값은 512바이트이고 최대 길이는 65535바이트). 재조립은 패킷 길이가 구성된 최대 길이보다 작은지 확인하기 위해 필요한 만큼 수행됩니다.패킷이 최대 길이를 초과하면 삭제됩니다.**참고:** maximum-length 옵션 없이 inspect dns 명령을 실행하면 DNS 패킷 크기가 검사되지 않습니다.
- 255바이트의 도메인 이름 길이와 63바이트의 레이블 길이를 적용합니다.
- DNS 메시지에서 압축 포인터가 발견되는 경우 포인터에서 참조하는 도메인 이름의 무결성을 확인합니다.
- 압축 포인터 루프가 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 ASA 5500 Series Security Appliance 버전 7.2(1)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 컨피그레이션은 Cisco PIX 500 Series Security Appliance 버전 6.2 이상에서도 사용할 수 있습니다.

참고: Cisco ASDM(Adaptive Security Device Manager) 구성은 버전 7.x에만 적용됩니다.

표기 규칙

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

배경 정보

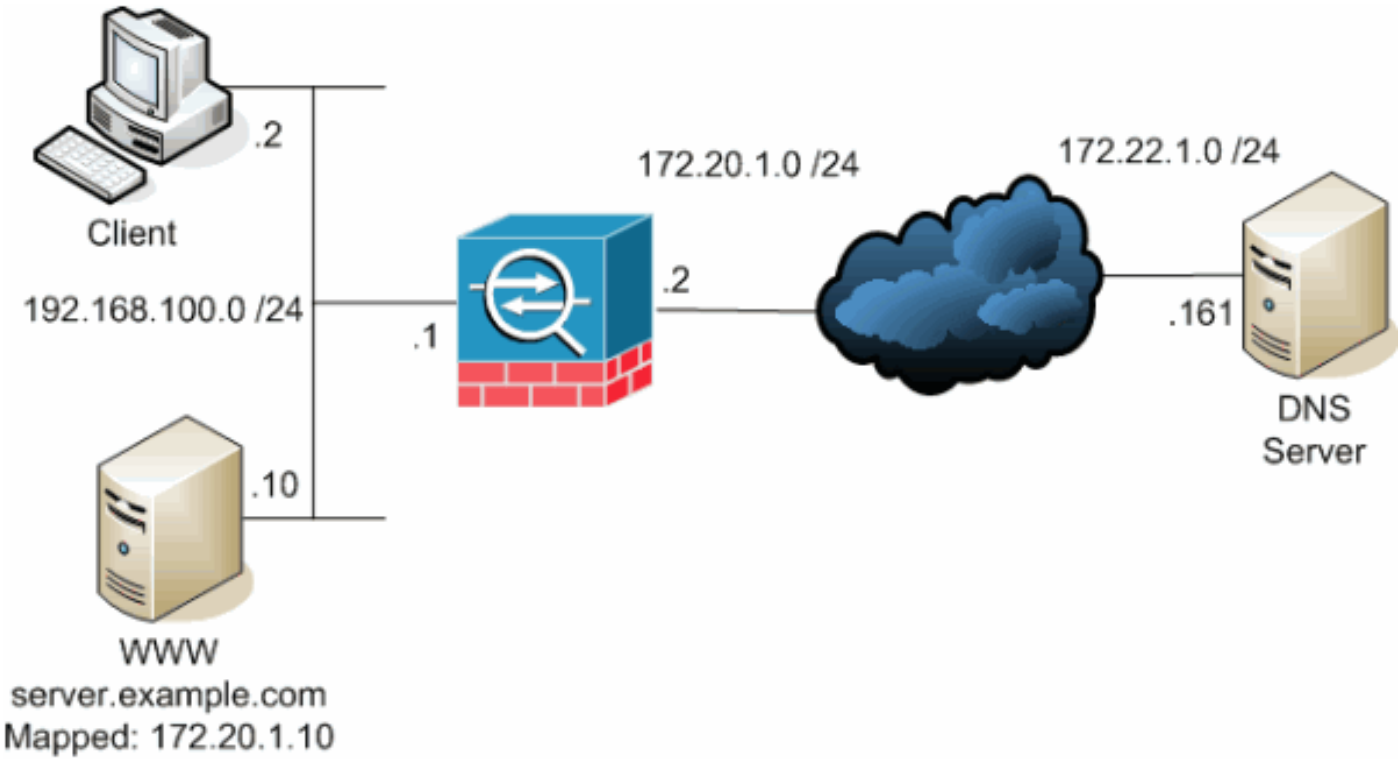
일반적인 DNS 교환에서는 클라이언트가 해당 호스트의 IP 주소를 확인하기 위해 DNS 서버에 URL

또는 호스트 이름을 전송합니다.DNS 서버가 요청을 수신하고 해당 호스트에 대한 이름-IP 주소 매핑을 찾은 다음 A-record에 IP 주소를 제공합니다.이 절차는 많은 상황에서 잘 작동하지만 문제가 발생할 수 있습니다.이러한 문제는 클라이언트와 클라이언트가 연결하려는 호스트가 모두 NAT 뒤의 동일한 사설 네트워크에 있지만 클라이언트에서 사용하는 DNS 서버가 다른 공용 네트워크에 있을 때 발생할 수 있습니다.

시나리오:2개의 NAT 인터페이스(내부, 외부)

토폴로지

이 시나리오에서는 클라이언트가 연결하려는 클라이언트와 WWW 서버가 모두 ASA의 내부 인터페이스에 있습니다.동적 PAT는 클라이언트가 인터넷에 액세스할 수 있도록 구성됩니다.access-list가 있는 고정 NAT는 서버가 인터넷에 액세스할 수 있도록 허용하며 인터넷 호스트가 WWW 서버에 액세스할 수 있도록 구성됩니다.



이 다이어그램은 이러한 상황의 예입니다.이 경우 192.168.100.2의 클라이언트는 **server.example.com** URL을 사용하여 192.168.100.10의 WWW 서버에 액세스하려고 합니다. 클라이언트에 대한 DNS 서비스는 172.22.1.161의 외부 DNS 서버에서 제공합니다. DNS 서버는 다른 공용 네트워크에 있으므로 WWW 서버의 개인 IP 주소를 모르는 것입니다.대신 WWW 서버의 매핑된 주소 172.20.1.10을 알고 있습니다. 따라서 DNS 서버에는 **server.example.com**의 IP 주소-이름 매핑이 **172.20.1.10**에 포함됩니다.

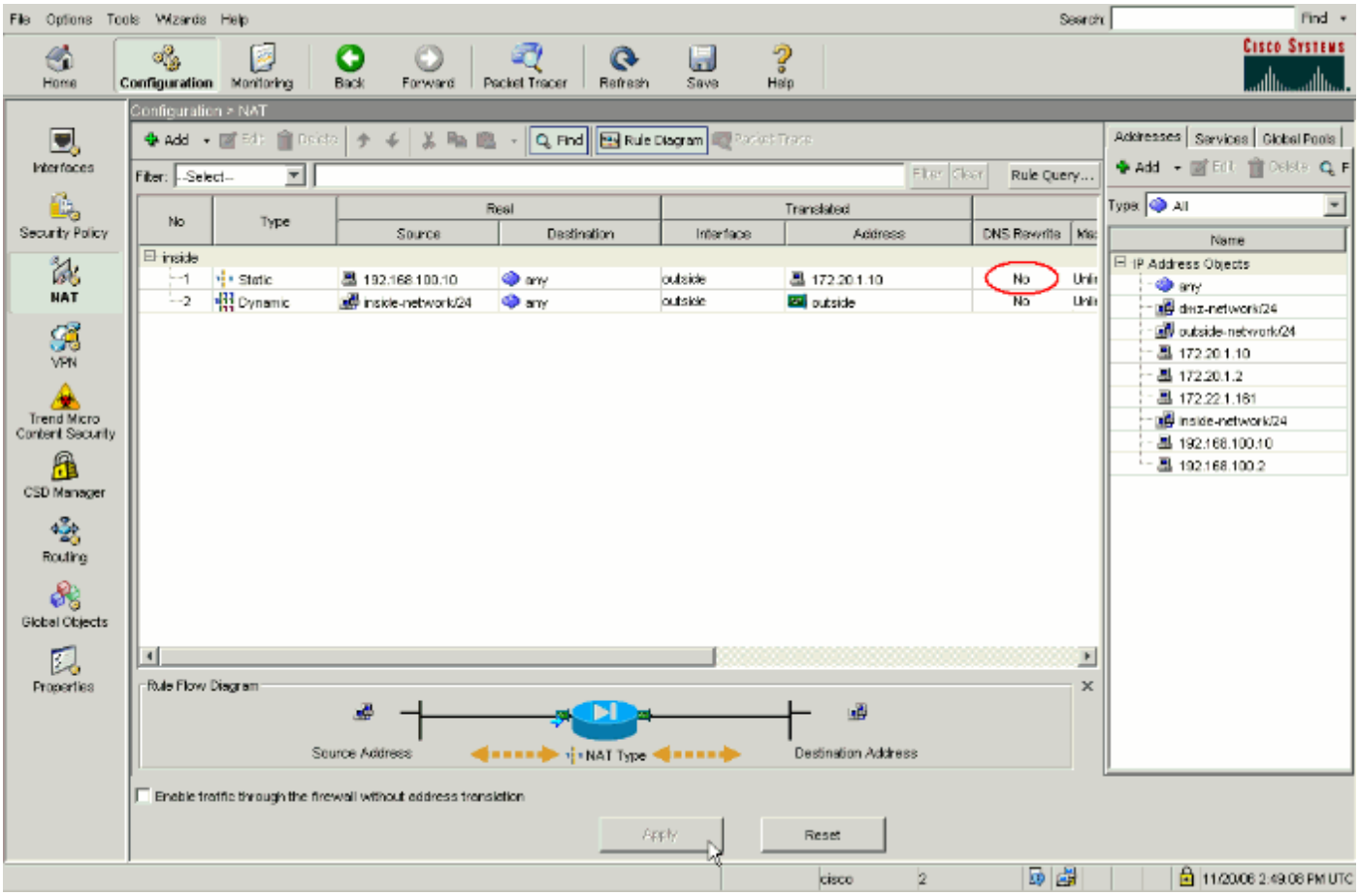
문제/장애:클라이언트가 WWW 서버에 액세스할 수 없음

이 상황에서 DNS 설명서나 다른 솔루션이 활성화되지 않은 경우 클라이언트가 server.example.com의 IP 주소에 대한 DNS 요청을 보내는 경우 WWW 서버에 액세스할 수 없습니다.클라이언트가 매핑된 공용 주소를 포함하는 A 레코드를 수신하기 때문입니다.172.20.1.10.클라이언트가 이 IP 주소에 액세스하려고 하면 보안 어플라이언스는 동일한 인터페이스에서 패킷 리디렉션을 허용하지 않으므로 패킷을 삭제합니다.다음은 DNS 문서가 활성화되지 않은 경우 컨피그레이션의 NAT 부분이 어떻게 나타나는지 보여줍니다.

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 access-group OUTSIDE
in interface outside !--- Output suppressed.
```

다음은 DNS 인증이 활성화되지 않은 경우 ASDM에서 표시되는 컨피그레이션입니다.



다음은 DNS 인증이 활성화되지 않은 경우 이벤트의 패킷 캡처입니다.

1. 클라이언트가 DNS 쿼리를 보냅니다.

```
No.     Time       Source           Destination      Protocol Info
1       0.000000   192.168.100.2    172.22.1.161     DNS      Standard query
                                                              A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x0004
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
```

```
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

2. PAT는 ASA에서 DNS 쿼리에 대해 수행되며 쿼리가 전달됩니다.패킷의 소스 주소가 ASA의 외부 인터페이스로 변경되었습니다.

```
No.     Time      Source           Destination         Protocol Info
1       0.000000  172.20.1.2       172.22.1.161        DNS      Standard query
                                                               A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x0004
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

3. DNS 서버는 WWW 서버의 매핑된 주소로 응답합니다.

```
No.     Time      Source           Destination       Protocol Info
2       0.005005  172.22.1.161     172.20.1.2        DNS      Standard query response
                                                               A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.005005000 seconds]
    Transaction ID: 0x0004
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 172.20.1.10
            Name: server.example.com
            Type: A (Host address)
```

```
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. ASA는 DNS 응답의 목적지 주소 변환을 취소하고 패킷을 클라이언트에 전달합니다.DNS Doctoring이 활성화되지 않은 경우 응답의 **Addr**은 여전히 WWW 서버의 매핑된 주소입니다.

```
No.     Time       Source          Destination         Protocol Info
2       0.005264   172.22.1.161    192.168.100.2       DNS      Standard query response
                                                               A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.005264000 seconds]
    Transaction ID: 0x0004
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 172.20.1.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 172.20.1.10
```

5. 이 시점에서 클라이언트는 172.20.1.10의 WWW 서버에 액세스를 시도합니다. ASA는 이 통신에 대한 연결 항목을 생성합니다.그러나 트래픽이 내부에서 외부로 외부로 이동하는 것을 허용하지 않으므로 연결이 시간 초과됩니다.ASA 로그에는 다음이 표시됩니다.

```
%ASA-6-302013: Built outbound TCP connection 54175 for
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)

%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80 to
inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

해결책:"dns" 키워드

"dns" 키워드와 함께 DNS Doctoring

dns 키워드를 사용한 DNS 설명에서는 보안 어플라이언스에서 클라이언트에 대한 DNS 서버 회신의 내용을 가로채고 재작성할 수 있습니다.올바르게 구성된 경우 보안 어플라이언스는 A 레코드를 변경하여 문제에서 설명한 시나리오에서 클라이언트를 허용할 수 있습니다.클라이언트가 연결할

WWW 서버 섹션에 액세스할 수 없습니다.이 경우 DNS doctoring이 활성화되면 보안 어플라이언스는 A-record를 다시 작성하여 클라이언트가 **172.20.1.10** 대신 **192.168.100.10으로** 리디렉션합니다. DNS doctoring은 고정 NAT 문에 dns 키워드를 추가할 때 활성화됩니다.다음은 DNS 인증이 활성화될 때 컨피그레이션의 NAT 부분입니다.

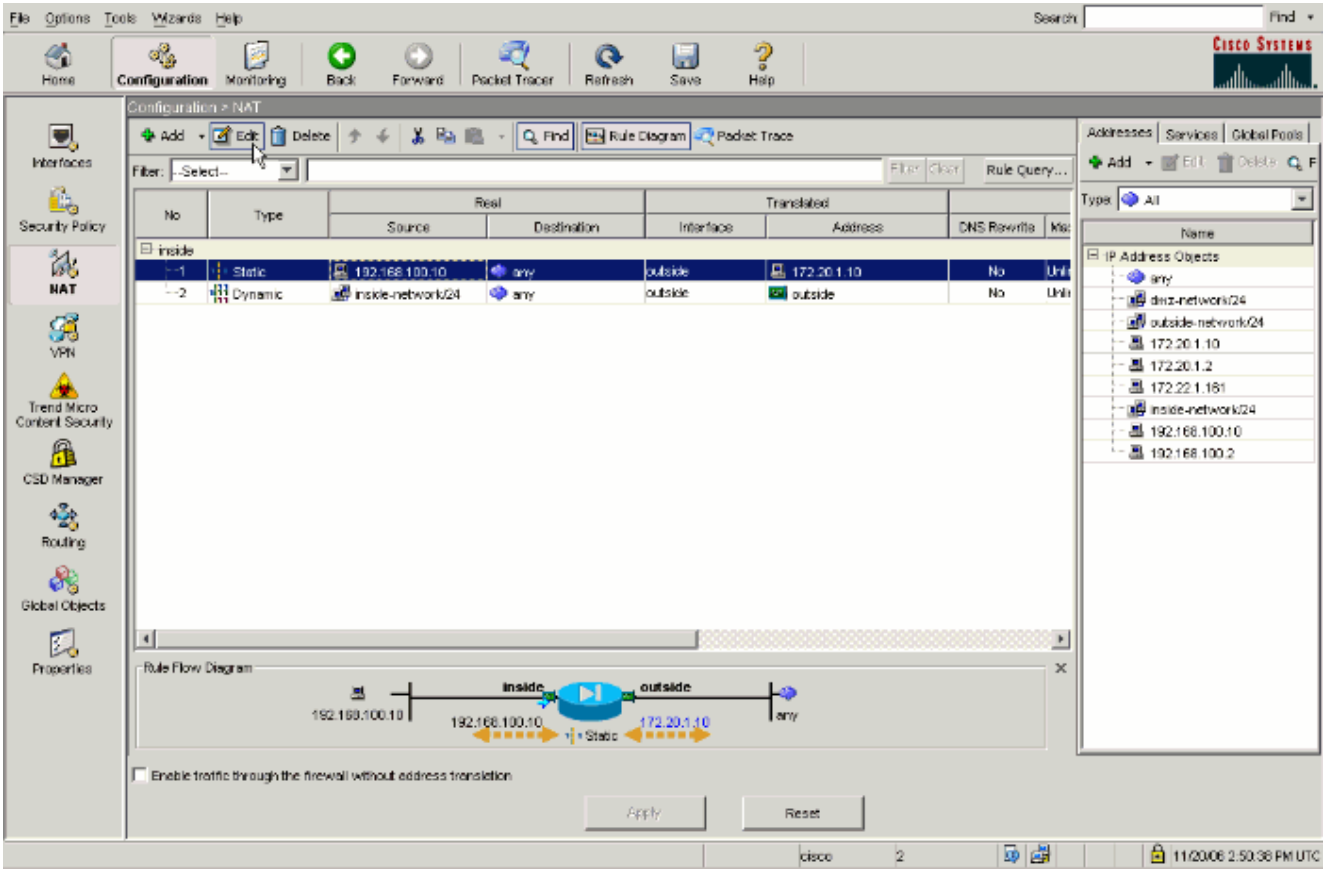
```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns
!--- The "dns" keyword is added to instruct the security appliance to modify !--- DNS records
related to this entry. access-group OUTSIDE in interface outside !--- Output suppressed.
```

ASDM에서 DNS 설명서를 구성하려면 다음 단계를 완료합니다.

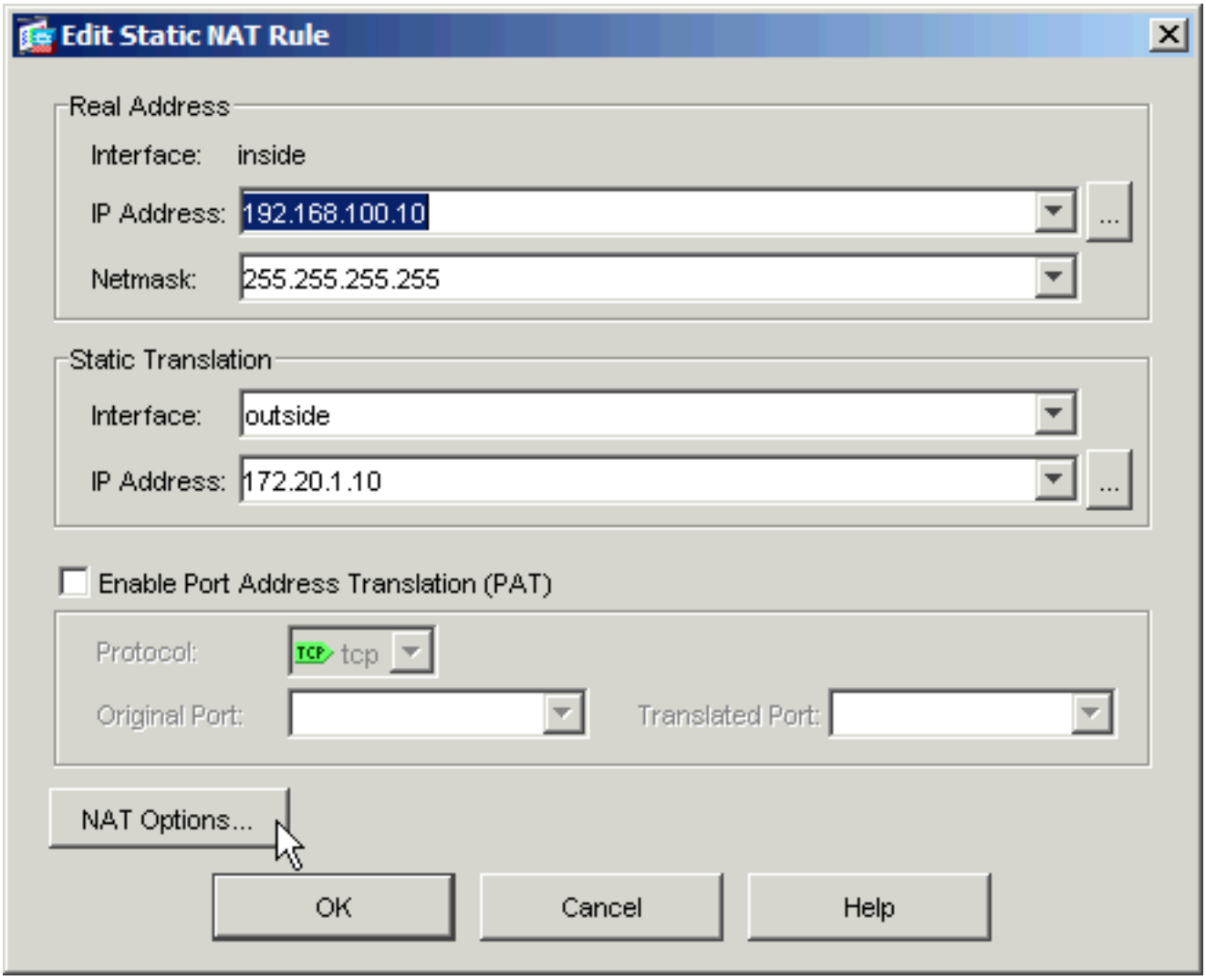
1. Configuration(컨피그레이션) **> NAT**로 이동하고 수정할 고정 NAT 규칙을 선택합니다.Edit를 **클릭합니다**

.

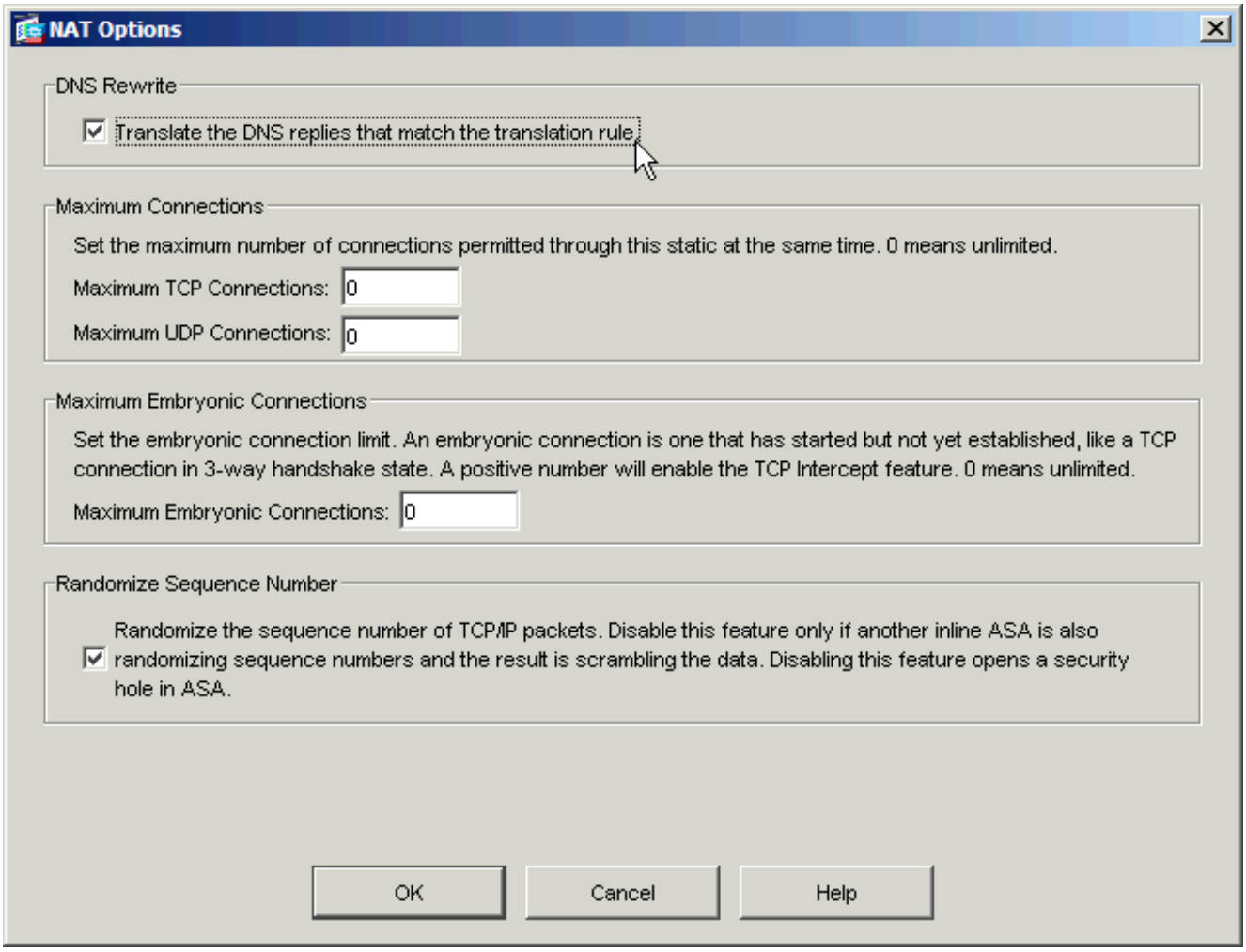


2. NAT **옵션...을 클릭합니다**

..



3. Translation **DNS replies that match the translation rule** 확인란을 선택합니다
.



4. **OK**를 클릭하여 NAT Options 창을 종료합니다.**OK**를 클릭하여 Edit Static NAT Rule(고정 NAT 규칙 수정) 창을 종료합니다.Apply(**적용**)를 클릭하여 컨피그레이션을 보안 어플라이언스에 전송합니다.

다음은 DNS 인증이 활성화된 경우 이벤트의 패킷 캡처입니다.

1. 클라이언트가 DNS 쿼리를 보냅니다.

```
No.     Time       Source           Destination        Protocol Info
1       0.000000   192.168.100.2    172.22.1.161       DNS      Standard query
                                                       A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x000c
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

2. PAT는 ASA에서 DNS 쿼리에 대해 수행되며 쿼리가 전달됩니다.패킷의 소스 주소가 ASA의 외부 인터페이스로 변경되었습니다.

```
No.     Time      Source          Destination        Protocol Info
1       0.000000  172.20.1.2      172.22.1.161       DNS      Standard query
                                                              A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x000c
    Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
```

3. DNS 서버는 WWW 서버의 매핑된 주소로 응답합니다.

```
No.     Time      Source          Destination       Protocol Info
2       0.000992  172.22.1.161    172.20.1.2        DNS      Standard query response
                                                             A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.000992000 seconds]
    Transaction ID: 0x000c
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 172.20.1.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 172.20.1.10
```

4. ASA는 DNS 응답의 목적지 주소 변환을 취소하고 패킷을 클라이언트에 전달합니다.DNS Doctoring이 활성화되면 응답의 Addr이 WWW 서버의 실제 주소로 재작성됩니다.

```
No.     Time      Source          Destination       Protocol Info
```

```
2       0.001251  172.22.1.161    192.168.100.2       DNS      Standard query response
                                                               A 192.168.100.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 52985 (52985)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.001251000 seconds]
    Transaction ID: 0x000c
    Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        server.example.com: type A, class IN
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        server.example.com: type A, class IN, addr 192.168.100.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 192.168.100.10
!--- 172.20.1.10 has been rewritten to be 192.168.100.10.
```

5. 이 시점에서 클라이언트는 192.168.100.10의 WWW 서버에 액세스하려고 시도합니다. 연결이 성공합니다.클라이언트와 서버가 동일한 서브넷에 있으므로 ASA에서 트래픽이 캡처되지 않습니다.

"dns" 키워드를 사용한 최종 구성

dns 키워드와 2개의 NAT 인터페이스를 사용하여 DNS 설명서를 수행하기 위한 ASA의 최종 컨피그레이션입니다.

최종 ASA 7.2(1) 컨피그레이션

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
```

```
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10
netmask 255.255.255.255 dns
!--- PAT and static NAT configuration. The DNS keyword
instructs !--- the security appliance to rewrite DNS
records related to this entry. access-group OUTSIDE in
interface outside
!--- The Access Control List (ACL) that permits HTTP
access !--- to the WWW server is applied to the outside
interface. route outside 0.0.0.0 0.0.0.0 172.20.1.1 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 uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns MY_DNS_INSPECT_MAP
 parameters
  message-length maximum 512
!--- DNS inspection map. policy-map global_policy class
inspection_default 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 dns
MY_DNS_INSPECT_MAP
!--- DNS inspection is enabled using the configured map.
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:a4a38088109887c3ceb481efab3dcf32
: end
```

대체 솔루션:헤어피닝

고정 NAT를 사용한 헤어피닝

주의: 고정 NAT를 사용하는 헤어피닝은 보안 어플라이언스를 통해 클라이언트와 WWW 서버 간에 모든 트래픽을 전송합니다.이 솔루션을 구현하기 전에 예상되는 트래픽 양과 보안 어플라이언스의 기능을 신중하게 고려하십시오.

헤어피닝은 트래픽이 도착한 인터페이스와 동일한 인터페이스로 다시 전송되는 프로세스입니다.이 기능은 보안 어플라이언스 소프트웨어 버전 7.0에 도입되었습니다. 7.2(1) 이전 버전의 경우, 헤어핀 트래픽(인바운드 또는 아웃바운드) 중 하나 이상을 암호화해야 합니다.7.2(1) 이상에서 이 요구 사항은 더 이상 존재하지 않습니다.7.2(1)를 사용할 경우 인바운드 트래픽과 아웃바운드 트래픽 모두 암호화되지 않을 수 있습니다.

고정 NAT 문과 함께 헤어피닝을 사용하여 DNS doctoring과 동일한 효과를 얻을 수 있습니다.이 메서드는 DNS 서버에서 클라이언트로 반환되는 DNS A 레코드의 내용을 변경하지 않습니다.대신 이 문서에서 설명한 시나리오와 같이 헤어피닝을 사용할 경우 클라이언트는 연결하기 위해 DNS 서버에서 반환한 **172.20.1.10** 주소를 사용할 수 있습니다.

다음은 DNS doctoring 효과를 얻기 위해 헤어피닝 및 고정 NAT를 사용할 때 컨피그레이션의 관련 부분입니다.굵게 표시된 명령은 이 출력 끝에 더 자세히 설명되어 있습니다.

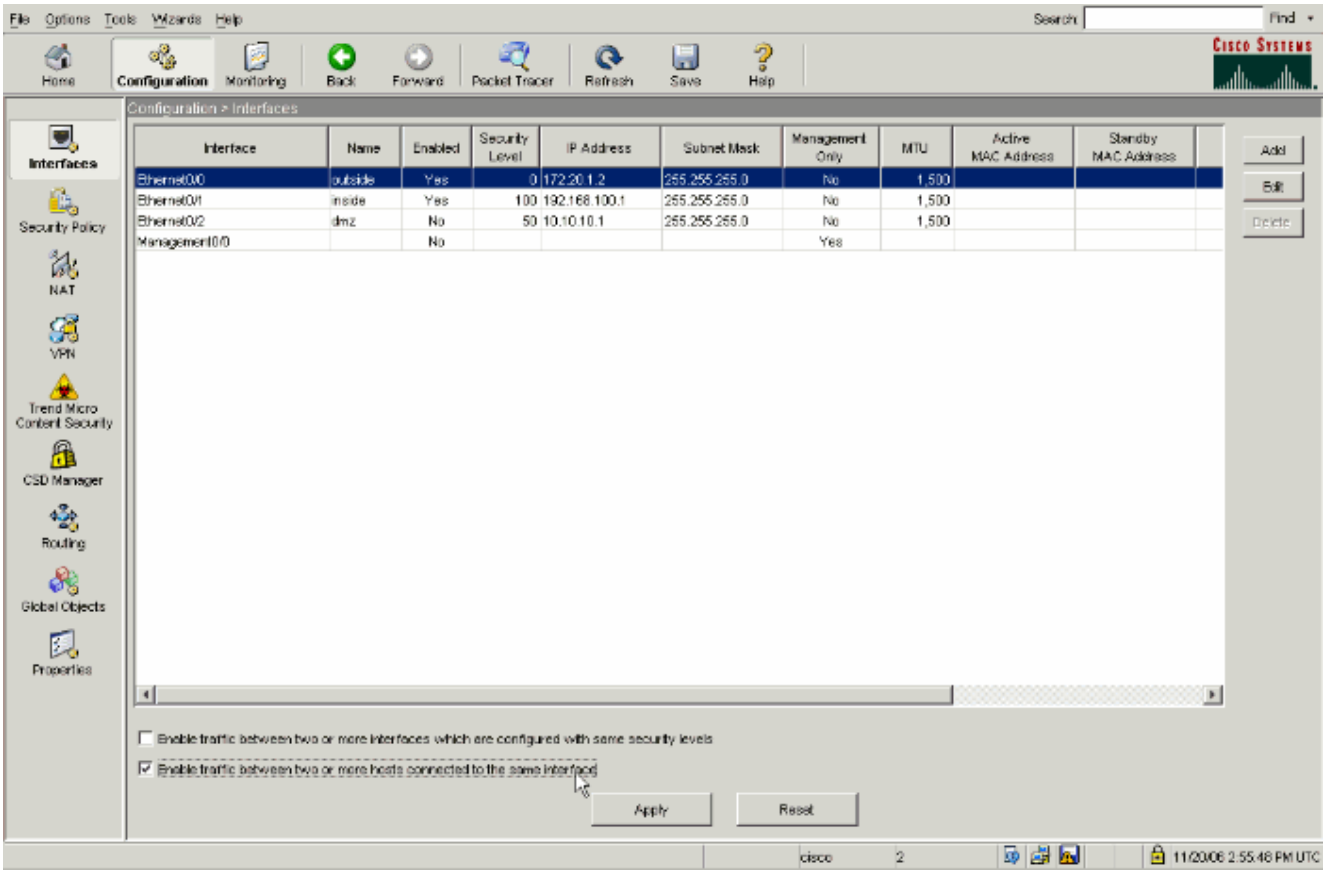
```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
!--- Output suppressed. same-security-traffic permit intra-interface
!--- Enable hairpinning. global (outside) 1 interface !--- Global statement for client access to
the Internet. global (inside) 1 interface
!--- Global statment for hairpinned client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should be
natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real
address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255
!--- Static NAT statment mapping requests for the public IP address of !--- the WWW server that
appear on the inside interface to the WWW server's !--- real address of 192.168.100.10.
```

- **same-security-traffic**—이 명령을 사용하면 보안 어플라이언스를 전송할 동일한 보안 수준의 트래픽을 사용할 수 있습니다.permit intra-**interface** 키워드는 same-security-traffic이 동일한 인터페이스에 들어오고 나가도록 허용하므로 헤어피닝이 활성화됩니다.**참고:** 헤어피닝 및 **same-security-traffic** 명령에 대한 자세한 내용은 same-security-traffic을 참조하십시오.
- **global (inside) 1 interface** - 보안 어플라이언스를 통과하는 모든 트래픽은 NAT를 거쳐야 합니다.이 명령은 내부 인터페이스로 들어오는 트래픽이 내부 인터페이스에서 헤어피닝될 때 PAT를 거치도록 하기 위해 보안 어플라이언스의 내부 인터페이스 주소를 사용합니다.
- **static (inside,inside) 172.20.1.10 192.168.100.10 넷마스크 255.255.255.255**—이 고정 NAT 항목은 WWW 서버의 공용 IP 주소에 대한 두 번째 매핑을 생성합니다.그러나 첫 번째 고정 NAT 항목과 달리 이번에는 주소 172.20.1.10이 보안 어플라이언스의 내부 인터페이스에 매핑됩니다.그러면 보안 어플라이언스가 내부 인터페이스에서 이 주소에 대해 표시되는 요청에 응답할 수 있습니다.그런 다음 해당 요청을 WWW 서버의 실제 주소로 직접 리디렉션합니다.

ASDM에서 고정 NAT로 헤어피닝을 구성하려면 다음 단계를 완료합니다.

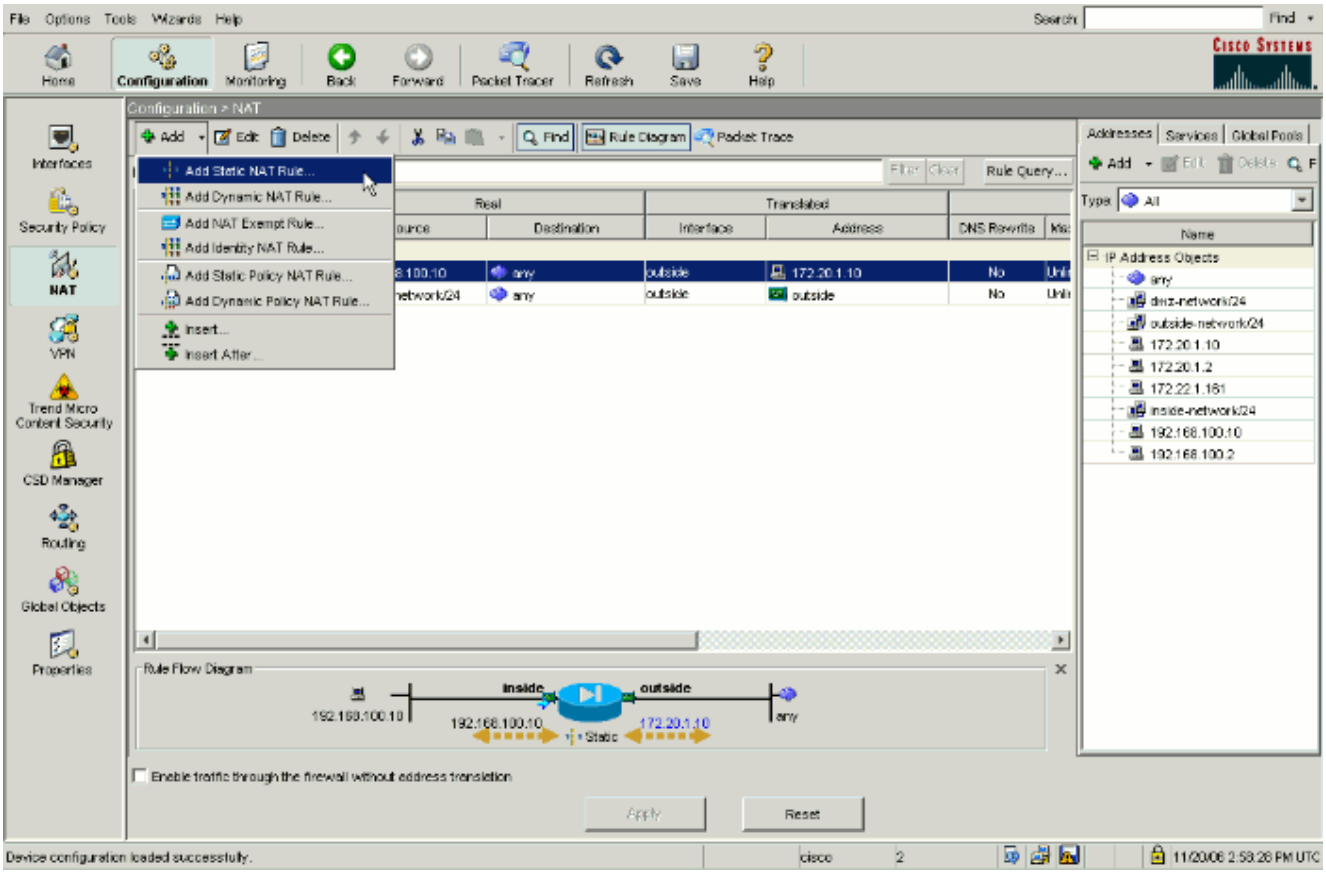
1. Configuration(컨피그레이션) **> Interfaces(인터페이스)로 이동합니다**.
2. 창 하단에서 **Enable traffic between two or more hosts connected to the same interface** 확인란을 선택합니다

.



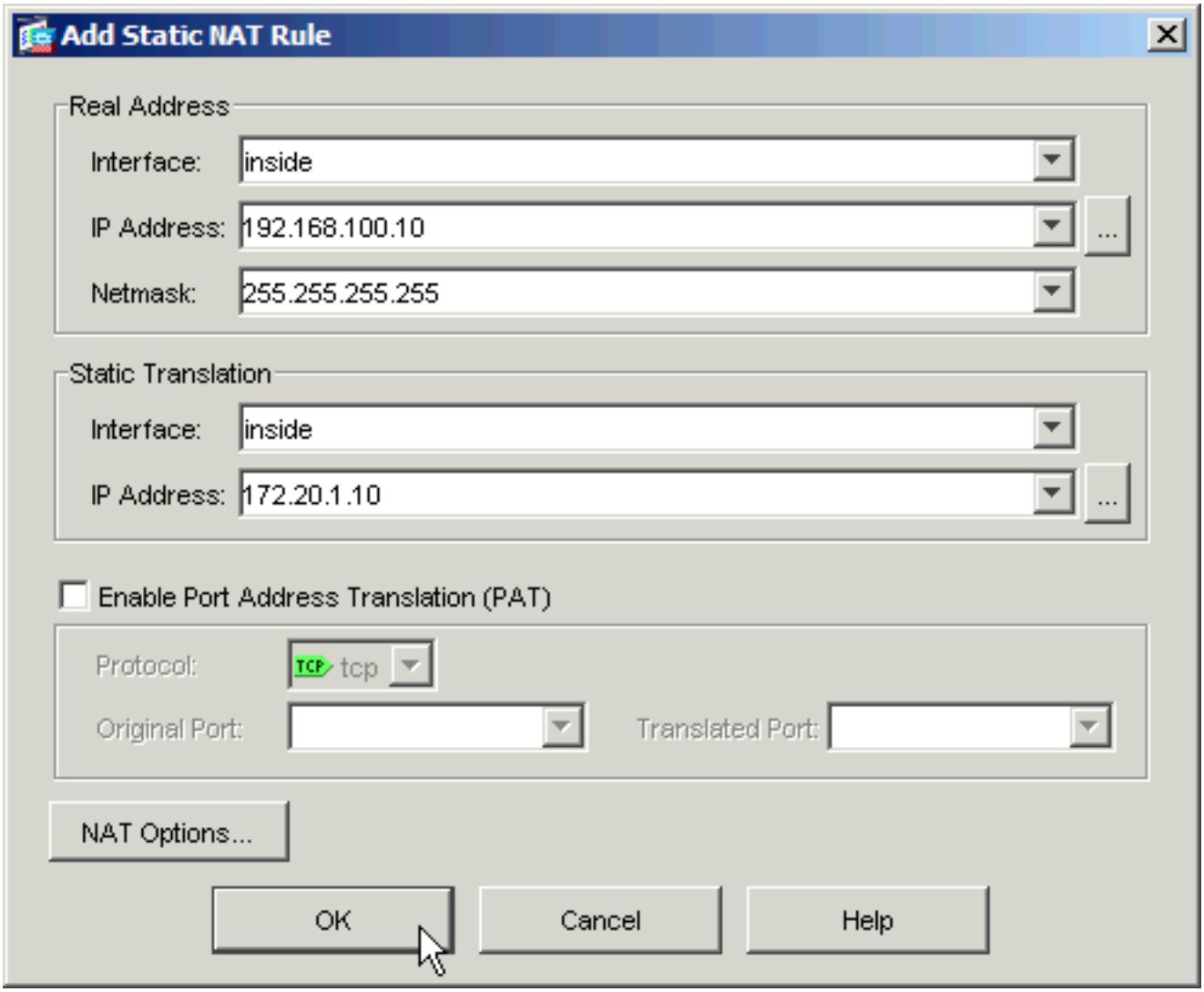
3. Apply를 **클릭합니다**.
4. Configuration(컨피그레이션) **> NAT(NAT)**로 이동하고 **Add(추가) > Add Static NAT Rule(고정 NAT 규칙 추가)을** 선택합니다

..



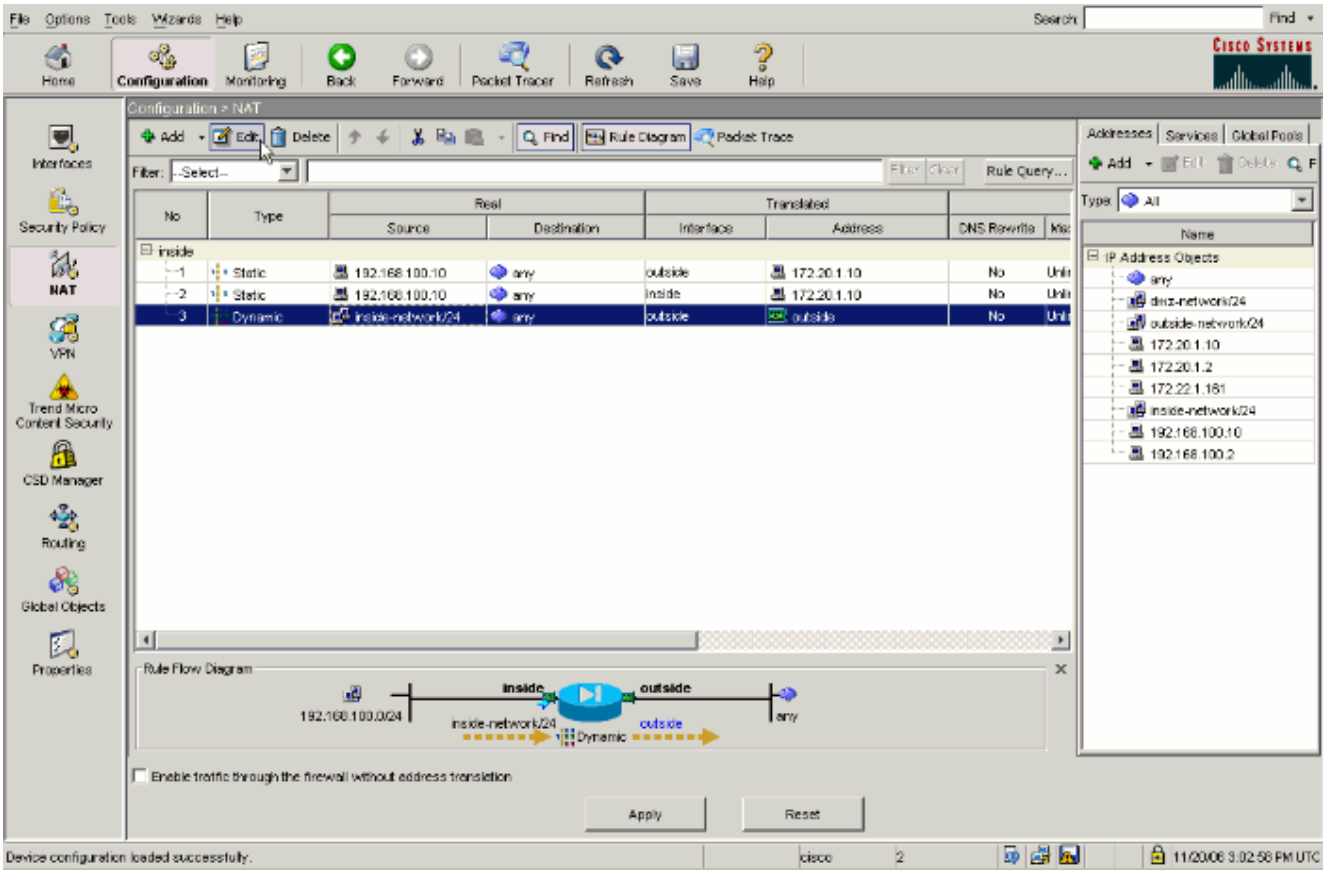
5. 새 고정 변환의 컨피그레이션을 채웁니다.Real **Address(실제 주소)** 영역을 WWW 서버 정보로 채웁니다.Static **Translation** 영역을 WWW 서버를 매핑할 주소와 인터페이스로 채웁니다.이 경우 내부 인터페이스의 호스트가 매핑된 주소 172.20.1.10을 통해 WWW 서버에 액세스하도록 내부 인터페이스를 선택합니다

.

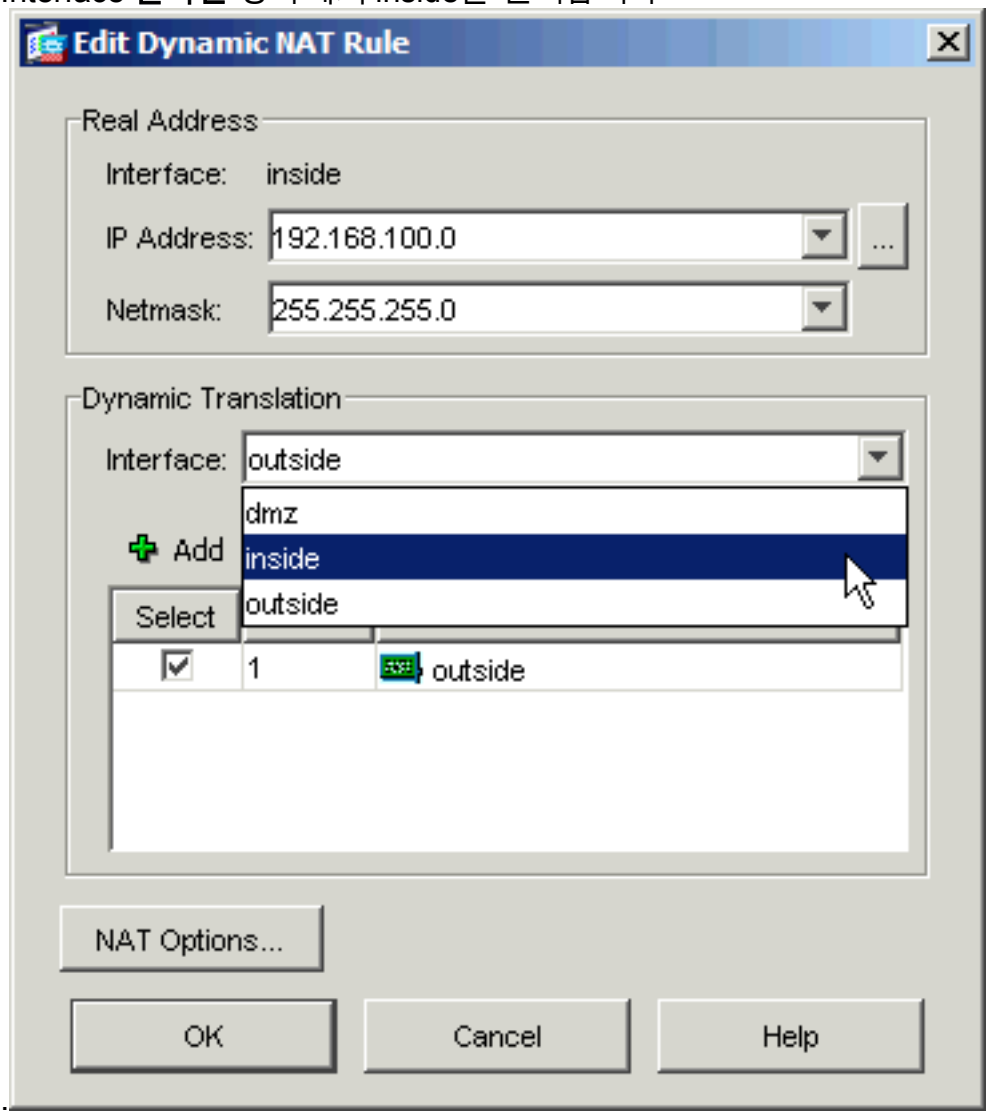


6. OK를 클릭하여 Add Static NAT Rule(고정 NAT 규칙 추가) 창을 종료합니다.
7. 기존 동적 PAT 변환을 선택하고 Edit를 **클릭합니다**

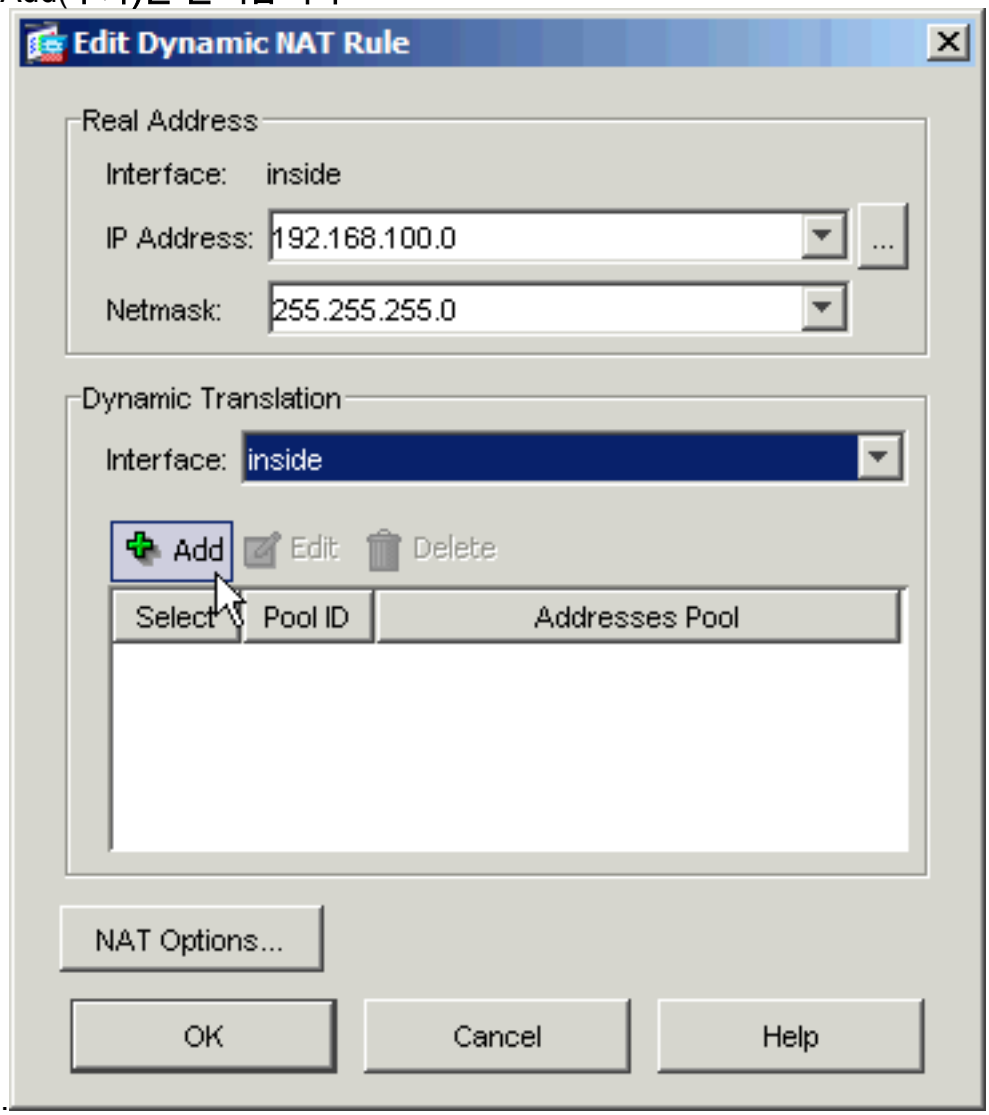
.



8. Interface **풀다운** 상자에서 inside를 선택합니다



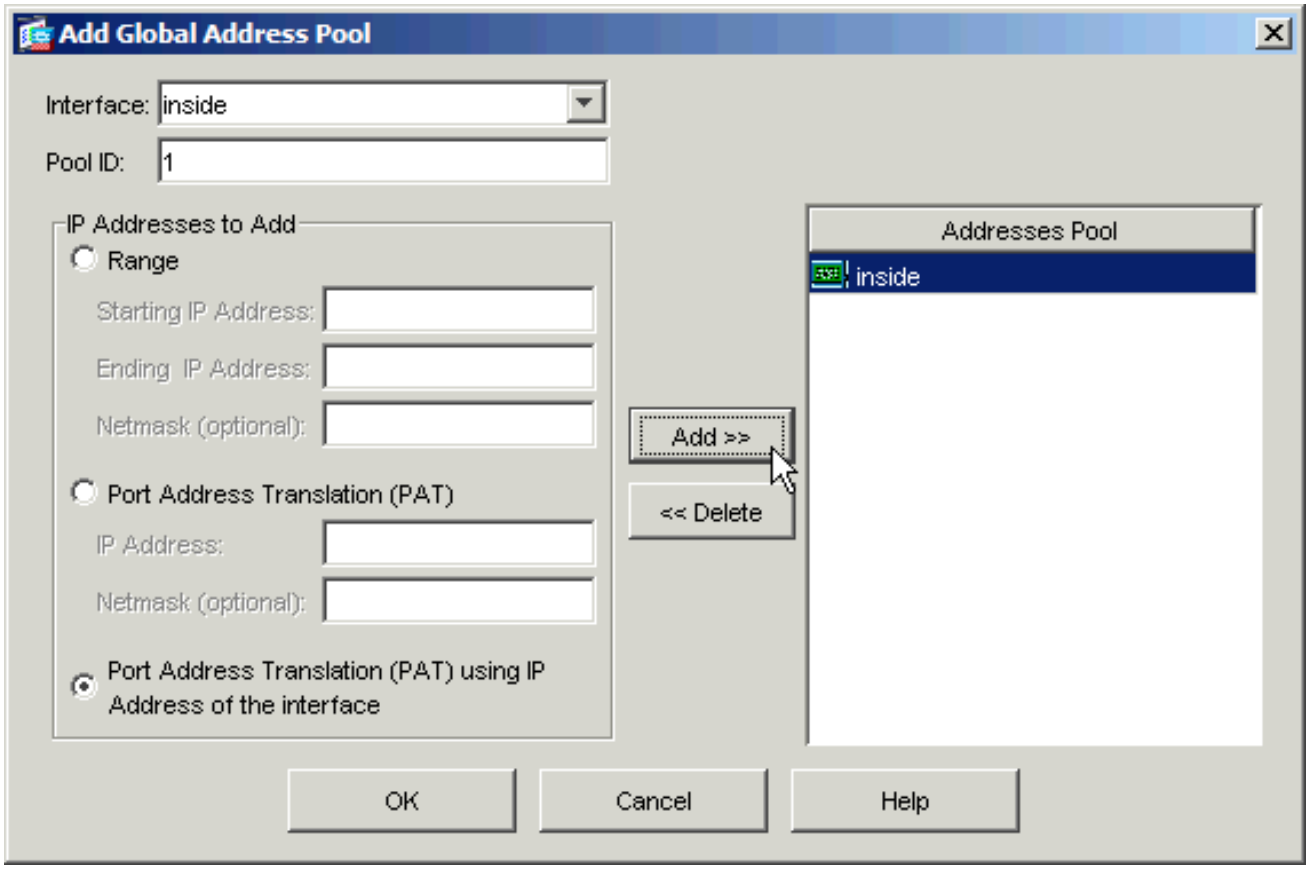
9. Add(**추가)를 클릭합니다**



.

10. **인터페이스**의 **IP 주소를 사용하여 PAT(Port Address Translation)로 표시된** 라디오 버튼을 **선택합니다**.Add(**추가)를 클릭합니다**

.



11. OK(**확인**)를 클릭하여 Add Global Address Pool(전역 주소 풀 추가) 창을 종료합니다.OK(**확인**)를 클릭하여 Edit Dynamic NAT Rule(동적 NAT 규칙 수정) 창을 종료합니다.Apply(**적용**)를 클릭하여 컨피그레이션을 보안 어플라이언스에 전송합니다.

다음은 헤어피닝이 구성될 때 발생하는 이벤트의 시퀀스입니다.클라이언트가 이미 DNS 서버를 쿼리하고 WWW 서버 주소에 대한 **172.20.1.10**의 응답을 받았다고 가정합니다.

1. 클라이언트가 WWW 서버(172.20.1.10)에 연결을 시도합니다.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. 보안 어플라이언스는 요청을 확인하고 WWW 서버가 192.168.100.10에 있음을 인식합니다.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.10
   ```
3. 보안 어플라이언스는 클라이언트에 대한 동적 PAT 변환을 생성합니다.클라이언트 트래픽의 소스가 이제 보안 어플라이언스의 내부 인터페이스입니다.192.168.100.1.
   ```
   %ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to
   inside:192.168.100.1/1026
   ```

4. 보안 어플라이언스는 클라이언트를 통해 WWW 서버와 TCP 연결을 생성합니다.각 호스트의 매핑된 주소를 괄호로 표시합니다.
   ```
   %ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012
   (192.168.100.1/1026) to inside:192.168.100.10/80 (172.20.1.10/80)
   ```

5. 보안 어플라이언스의 **show xlate** 명령은 클라이언트 트래픽이 보안 어플라이언스를 통해 변환되는지 확인합니다.
   ```
   ciscoasa(config)#show xlate
   3 in use, 9 most used
   Global 172.20.1.10 Local 192.168.100.10
   Global 172.20.1.10 Local 192.168.100.10
   PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)
   ```

6. 보안 어플라이언스의 **show conn** 명령은 보안 어플라이언스와 WWW 서버 간에 클라이언트 대신 연결이 성공했는지 확인합니다.클라이언트의 실제 주소를 괄호로 표시합니다.
   ```
   ciscoasa#show conn
   ```

```
TCP out 192.168.100.1(192.168.100.2):11019 in 192.168.100.10:80
idle 0:00:03 bytes 1120 flags UIOB
```

헤어피닝 및 고정 NAT를 사용한 최종 컨피그레이션

이것은 헤어피닝 및 고정 NAT를 사용하여 2개의 NAT 인터페이스와 함께 DNS doctoring 효과를 얻는 ASA의 최종 컨피그레이션입니다.

최종 ASA 7.2(1) 컨피그레이션

```
ciscoasa(config-if)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface
access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface !--- Global statement for client access to the
Internet. global (inside) 1 interface !--- Global
statment for hairpinned client access through !--- the
security appliance. nat (inside) 1 192.168.100.0
255.255.255.0 !--- The NAT statement defines which
traffic should be natted. !--- The whole inside subnet
in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT
```

```
statement mapping the WWW server's real address to a
public !--- address on the outside interface. static
(inside,inside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 !--- Static NAT statement mapping
requests for the public IP address of the !--- WWW
server that appear on the inside interface to the WWW
server's real address !--- of 192.168.100.10. access-
group OUTSIDE in interface outside !--- The ACL that
permits HTTP access to the WWW server is applied !--- to
the outside interface. route outside 0.0.0.0 0.0.0.0
172.20.1.1 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 uauth
0:05:00 absolute username cisco password
ffIRPGpDSOJh9YLq encrypted http server enable no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
MY_DNS_INSPECT_MAP parameters message-length maximum 512
policy-map global_policy class inspection_default
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 dns MY_DNS_INSPECT_MAP
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:7c9b4e3aff085ba90ee194e079111e1d
: end
```

참고: Cisco ASA (등록된 고객만 해당)에 대한 헤어피닝, 이 비디오를 참조하여 헤어피닝 기능을 사용할 수 있는 다양한 시나리오에 대한 자세한 정보를 확인하십시오.

DNS 검사 구성

DNS 검사를 활성화하려면(이전에 비활성화된 경우) 다음 단계를 수행합니다.이 예에서 DNS 검사는 기본 전역 검사 정책에 추가되며, 이는 ASA가 기본 컨피그레이션으로 시작된 것처럼 **service-policy** 명령에 의해 전역적으로 적용됩니다.서비스 정책 및 검사에 대한 자세한 내용은 Using Modular Policy Framework를 참조하십시오.

1. DNS에 대한 검사 정책 맵을 만듭니다.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```

2. policy-map 컨피그레이션 모드에서 매개변수 컨피그레이션 모드를 입력하여 검사 엔진에 대한 매개변수를 지정합니다.
   ```
   ciscoasa(config-pmap)#parameters
   ```

3. policy-map 매개변수 컨피그레이션 모드에서 DNS 메시지의 최대 메시지 길이를 512로 지정합니다.
   ```
   ciscoasa(config-pmap-p)#message-length maximum 512
   ```

4. policy-map 매개변수 컨피그레이션 모드 및 policy-map 컨피그레이션 모드를 종료합니다.
   ```
   ciscoasa(config-pmap-p)#exit
   ```

```
ciscoasa(config-pmap)#exit
```

5. 원하는 대로 검사 정책 맵이 생성되었는지 확인합니다.
```
ciscoasa(config)#show run policy-map type inspect dns
!
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
  message-length maximum 512
!
```
6. global_policy에 대한 policy-map 컨피그레이션 모드를 입력합니다.
```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```
7. 정책 맵 컨피그레이션 모드에서 기본 레이어 3/4 클래스 맵인 inspection_default를 지정합니다.
```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```
8. 정책 맵 클래스 컨피그레이션 모드에서 1-3단계에서 생성한 검사 정책 맵을 사용하여 DNS를 검사하도록 지정합니다.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```

9. policy-map 클래스 컨피그레이션 모드 및 policy-map 컨피그레이션 모드를 종료합니다.
```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

10. global_policy policy-map이 원하는 대로 구성되었는지 확인합니다.
```
ciscoasa(config)#show run policy-map
!
!--- The configured DNS inspection policy map. policy-map type inspect dns
MY_DNS_INSPECT_MAP parameters message-length maximum 512 policy-map global_policy class
inspection_default 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 dns MY_DNS_INSPECT_MAP
!--- DNS application inspection enabled. !
```
11. global_policy가 서비스 정책에 의해 전역으로 적용되는지 확인합니다.
```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

스플릿-DNS 컨피그레이션

스플릿 터널을 통해 확인할 도메인 목록을 입력하려면 group-policy 컨피그레이션 모드에서 split-dns 명령을 실행합니다.목록을 삭제하려면 이 명령의 no 형식을 사용합니다.

스플릿 터널링 도메인 목록이 없는 경우 사용자는 기본 그룹 정책에 있는 항목을 상속합니다.스플릿 터널링 도메인 목록의 상속을 방지하려면 split-dns none 명령을 실행합니다.

도메인 목록에서 각 항목을 구분하려면 단일 공간을 사용합니다.항목 수에 제한이 없지만 전체 문자열은 255자를 초과할 수 없습니다.영숫자, 하이픈(-) 및 마침표(.)만 사용할 수 있습니다. 인수 없이 no split-dns 명령을 사용하면 모든 현재 값이 삭제되며, split-dns none 명령을 실행할 때 생성된 null 값이 포함됩니다.

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 스플릿 터널링을 통해 확인할 도메인 Domain1, Domain2, Domain3 및 Domain4를 구성하는 방법을 보여 줍니다.

```
hostname(config)#group-policy FirstGroup attributes
```

```
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

DNS 트래픽 캡처

보안 어플라이언스가 DNS 레코드를 올바르게 재작성하는지 확인하는 한 가지 방법은 이전 예에 설명된 대로 문제의 패킷을 캡처하는 것입니다.ASA에서 트래픽을 캡처하려면 다음 단계를 완료합니다.

1. 생성할 각 캡처 인스턴스에 대한 액세스 목록을 생성합니다.ACL은 캡처할 트래픽을 지정해야 합니다.이 예에서는 2개의 ACL이 생성되었습니다.외부 인터페이스의 트래픽에 대한 ACL:
   ```
   access-list DNSOUTCAP extended permit ip host 172.22.1.161 host 172.20.1.2
   !--- All traffic between the DNS server and the ASA. access-list DNSOUTCAP extended permit
   ip host 172.20.1.2 host 172.22.1.161 !--- All traffic between the ASA and the DNS server.
   ```
   내부 인터페이스의 트래픽에 대한 ACL:
   ```
   access-list DNSINCAP extended permit ip host 192.168.100.2 host 172.22.1.161
   !--- All traffic between the client and the DNS server. access-list DNSINCAP extended
   permit ip host 172.22.1.161 host 192.168.100.2 !--- All traffic between the DNS server and
   the client.
   ```
2. 캡처 인스턴스를 생성합니다.
   ```
   ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface outside
   !--- This capture collects traffic on the outside interface that matches !--- the ACL
   DNSOUTCAP. ciscoasa#capture DNSINSIDE access-list DNSINCAP interface inside
   !--- This capture collects traffic on the inside interface that matches !--- the ACL
   DNSINCAP.
   ```
3. 캡처를 봅니다.다음은 몇 가지 DNS 트래픽이 전달된 후 캡쳐되는 예입니다.
   ```
   ciscoasa#show capture DNSOUTSIDE
   2 packets captured
      1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53:  udp 36
      2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025:  udp 93
   2 packets shown
   ciscoasa#show capture DNSINSIDE
   2 packets captured
      1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53:  udp 36
      2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225:  udp 93
   2 packets shown
   ```
4. (선택 사항) 캡처를 다른 애플리케이션에서 분석할 수 있도록 pcap 형식으로 TFTP 서버에 복사합니다.pcap 형식을 구문 분석할 수 있는 애플리케이션은 DNS A 레코드의 이름 및 IP 주소와 같은 추가 세부 정보를 표시할 수 있습니다.
   ```
   ciscoasa#copy /pcap capture:DNSINSIDE tftp
   ...
   ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
   ```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

DNS 재작성이 수행되지 않음

보안 어플라이언스에 DNS 검사가 구성되어 있는지 확인합니다.DNS 검사 구성 섹션을 참조하십시오.

번역 생성 실패

클라이언트와 WWW 서버 간에 연결을 생성할 수 없는 경우 NAT 컨피그레이션 오류 때문일 수 있습니다.보안 어플라이언스를 통한 변환을 프로토콜이 생성하지 못했음을 나타내는 메시지에 대한 보안 어플라이언스 로그를 확인합니다.이러한 메시지가 나타나면 원하는 트래픽에 대해 NAT가 구성되었는지, 잘못된 주소가 없는지 확인합니다.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst dmz:10.10.10.10/23
```

xlate 항목을 지운 다음 NAT 문을 제거 및 다시 적용하여 이 오류를 해결합니다.

UDP DNS 회신 삭제

DNS 패킷 삭제로 인해 이 오류 메시지가 표시될 수 있습니다.

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

이 문제를 해결하려면 DNS 패킷 길이를 512-65535 사이로 늘리십시오.

예:

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림
- RFC(Request for Comments)
- Cisco ASA의 헤어핀
- Cisco ASA 5500 Series Adaptive Security Appliance