# PIX/ASA 7.x/FWSM 3.x:고정 정책 NAT를 사용하여 여러 글로벌 IP 주소를 단일 로컬 IP 주소로 변환

## 목차



## 소개

이 문서에서는 PIX/ASA(Adaptive Security Appliance) 7.x 소프트웨어의 정책 기반 고정 NAT(Network Address Translation)를 통해 하나 이상의 글로벌 IP 주소에 로컬 IP 주소를 매핑하기 위한 샘플 컨피그레이션을 제공합니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 이 요구 사항을 충족해야 합니다.

- PIX/ASA 7.x CLI에 대한 작업 지식 및 액세스 목록 및 고정 NAT를 구성하는 이전 경험이 있는지 확인합니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 구체적인 예에서는 ASA 5520을 사용합니다.그러나 정책 NAT 컨피그레이션은 7.x를 실행하는 PIX 또는 ASA 어플라이언스에서 작동합니다.

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.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

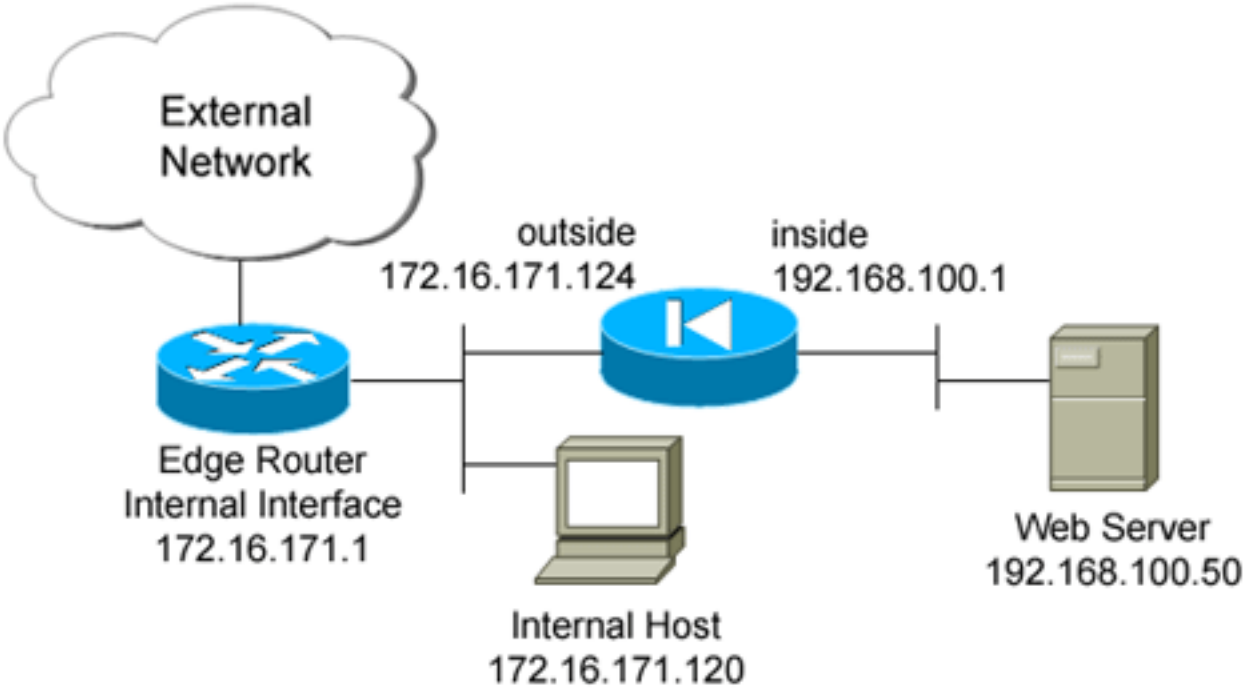
# 구성

이 컨피그레이션 예에서는 ASA 뒤에 있는 192.168.100.50에 내부 웹 서버가 있습니다.내부 IP 주소 192.168.100.50과 외부 주소 172.16.171.125을 통해 외부 네트워크 인터페이스에 액세스할 수 있어야 합니다. 또한 보안 정책 요구 사항192.168.100.50의 개인 IP 주소는 172.16.171.0/24 네트워크에서만 액세스할 수 있어야 합니다.또한 ICMP(Internet Control Message Protocol) 및 포트 80 트래픽은 내부 웹 서버로 인바운드를 허용하는 유일한 프로토콜입니다.하나의 로컬 IP 주소에 매핑된 2개의 전역 IP 주소가 있으므로 정책 NAT를 사용해야 합니다.그렇지 않으면 PIX/ASA는 겹치는 주소 오류가 있는 1대1 2의 통계를 거부합니다.

**참고:** 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

## 네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.




## 구성

이 문서에서는 이 구성을 사용합니다.

```
ciscoasa(config)#show run
: Saved
```

```
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.171.124 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- policy_nat_web1 and policy_nat_web2 are two access-
lists that match the source !--- address we want to
translate on. Two access-lists are required, though they
!--- can be exactly the same. access-list
policy_nat_web1 extended permit ip host 192.168.100.50
any
access-list policy_nat_web2 extended permit ip host
192.168.100.50 any

!--- The inbound_outside access-list defines the
security policy, as previously described. !--- This
access-list is applied inbound to the outside interface.
access-list inbound_outside extended permit tcp
172.16.171.0 255.255.255.0
   host 192.168.100.50 eq www
access-list inbound_outside extended permit icmp
172.16.171.0 255.255.255.0
   host 192.168.100.50 echo-reply
access-list inbound_outside extended permit icmp
172.16.171.0 255.255.255.0
   host 192.168.100.50 echo
access-list inbound_outside extended permit tcp any host
172.16.171.125 eq www
access-list inbound_outside extended permit icmp any
host 172.16.171.125 echo-reply
```

```
access-list inbound_outside extended permit icmp any
host 172.16.171.125 echo
pager lines 24
logging asdm informational
mtu management 1500
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!--- This first static allows users to reach the
translated global IP address of the !--- web server.
Since this static appears first in the configuration,
for connections !--- initiated outbound from the
internal web server, the ASA translates the source !---
address to 172.16.171.125. static (inside,outside)
172.16.171.125  access-list policy_nat_web1

!--- The second static allows networks to access the web
server by its private !--- IP address of 192.168.100.50.
static (inside,outside) 192.168.100.50  access-list
policy_nat_web2

!--- Apply the inbound_outside access-list to the
outside interface. access-group inbound_outside in
interface outside

route outside 0.0.0.0 0.0.0.0 172.16.171.1 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
http server enable
http 192.168.1.0 255.255.255.0 management
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 preset_dns_map
 parameters
  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
!
service-policy global_policy global
prompt hostname context
```

# 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

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

1. 업스트림 IOS® 라우터 172.16.171.1에서 ping 명령을 통해 웹 서버의 두 전역 IP 주소에 연결할 수 있는지 **확인합니다**.
   ```
   router#ping 172.16.171.125

   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 172.16.171.125, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
   router#ping 192.168.100.50

   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 192.168.100.50, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
   ```
2. ASA에서 xlate(translation) 테이블에 내장된 변환이 표시되는지 확인합니다.
   ```
   ciscoasa(config)#show xlate global 192.168.100.50
   2 in use, 28 most used
   Global 192.168.100.50 Local 192.168.100.50
   ciscoasa(config)#show xlate global 172.16.171.125
   2 in use, 28 most used
   Global 172.16.171.125 Local 192.168.100.50
   ```

# 문제 해결

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

ping 또는 연결에 실패하면 syslog를 사용하여 변환 컨피그레이션에 문제가 있는지 확인합니다.사용량이 적은 네트워크(예: 랩 환경)에서 로깅 버퍼 크기는 일반적으로 문제를 해결하는 데 충분합니다.그렇지 않으면 외부 syslog 서버로 syslog를 전송해야 합니다.이러한 syslog 항목에서 컨피그레이션이 올바른지 확인하려면 레벨 6의 버퍼에 대한 로깅을 활성화합니다.

```
ciscoasa(config)#logging buffered 6
ciscoasa(config)#logging on

!--- From 172.16.171.120, initiate a TCP connection to port 80 to both the external !---
(172.16.171.125) and internal addresses (192.168.100.50). ciscoasa(config)#show log
```

```
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 4223 messages logged
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level informational, 4032 messages logged
%ASA-5-111008: User 'enable_15' executed the 'clear logging buffer' command.
%ASA-7-609001: Built local-host outside:172.16.171.120
%ASA-7-609001: Built local-host inside:192.168.100.50
%ASA-6-302013: Built inbound TCP connection 67 for outside:172.16.171.120/33687
(172.16.171.120/33687) to inside:192.168.100.50/80 (172.16.171.125/80)
%ASA-6-302013: Built inbound TCP connection 72 for outside:172.16.171.120/33689
(172.16.171.120/33689) to inside:192.168.100.50/80 (192.168.100.50/80)
```

로그에 변환 오류가 표시되면 NAT 컨피그레이션을 다시 확인합니다.syslog를 관찰하지 않는 경우 ASA에서 **capture** 기능을 사용하여 인터페이스에서 트래픽을 캡처합니다.캡처를 설정하려면 먼저 특정 유형의 트래픽 또는 TCP 흐름에서 매칭할 액세스 목록을 지정해야 합니다.그런 다음 패킷을 캡처하기 시작하려면 하나 이상의 인터페이스에 이 캡처를 적용해야 합니다.

```
!--- Create a capture access-list to match on port 80 traffic to !--- the external IP address of
172.16.171.125. !--- Note: These commands are over two lines due to spatial reasons.


ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.120
     host 172.16.171.125 eq 80
ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.125
    eq 80 host 172.16.171.120
ciscoasa(config)#

!--- Apply the capture to the outside interface.


ciscoasa(config)#capture capout access-list acl_capout interface outside

!--- After you initiate the traffic, you see output similar to this when you view !--- the
capture. Note that packet 1 is the SYN packet from the client, while packet !--- 2 is the SYN-
ACK reply packet from the internal server. If you apply a capture !--- on the inside interface,
in packet 2 you should see the server reply with !--- 192.168.100.50 as its source address.

ciscoasa(config)#show capture capout
4 packets captured
   1: 13:17:59.157859 172.16.171.120.21505 > 172.16.171.125.80: S
      2696120951:2696120951(0) win 4128 <mss 1460>
   2: 13:17:59.159446 172.16.171.125.80 > 172.16.171.120.21505: S
      1512093091:1512093091(0) ack 2696120952 win 4128 <mss 536>
   3: 13:17:59.159629 172.16.171.120.21505 > 172.16.171.125.80: .
      ack 1512093092 win 4128
   4: 13:17:59.159873 172.16.171.120.21505 > 172.16.171.125.80: .
      ack 1512093092 win 4128
```

## 관련 정보

- ASA 7.2 명령 참조
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems