PIX/ASA 7.x/FWSM 3.x: Vertaal meerdere mondiale IP-adressen aan één lokaal IP-adres met behulp van Static Policy NAT

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het in kaart brengen van één lokaal IP-adres naar twee of meer wereldwijde IP-adressen door middel van op beleid gebaseerde statische netwerkadresomzetting (NAT) in de software van PIX/Adaptieve security (ASA) 7.x.

Voorwaarden

Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereiste worden voldaan:

- Zorg ervoor dat u over een werkkennis van de PIX/ASA 7.x CLI en eerdere ervaring hebt met het configureren van toegangslijsten en statische NAT.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit specifieke voorbeeld maakt gebruik van een ASA 5520. Maar NAT-configuraties werken ook aan elk PIX- of ASA-apparaat dat 7.x draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

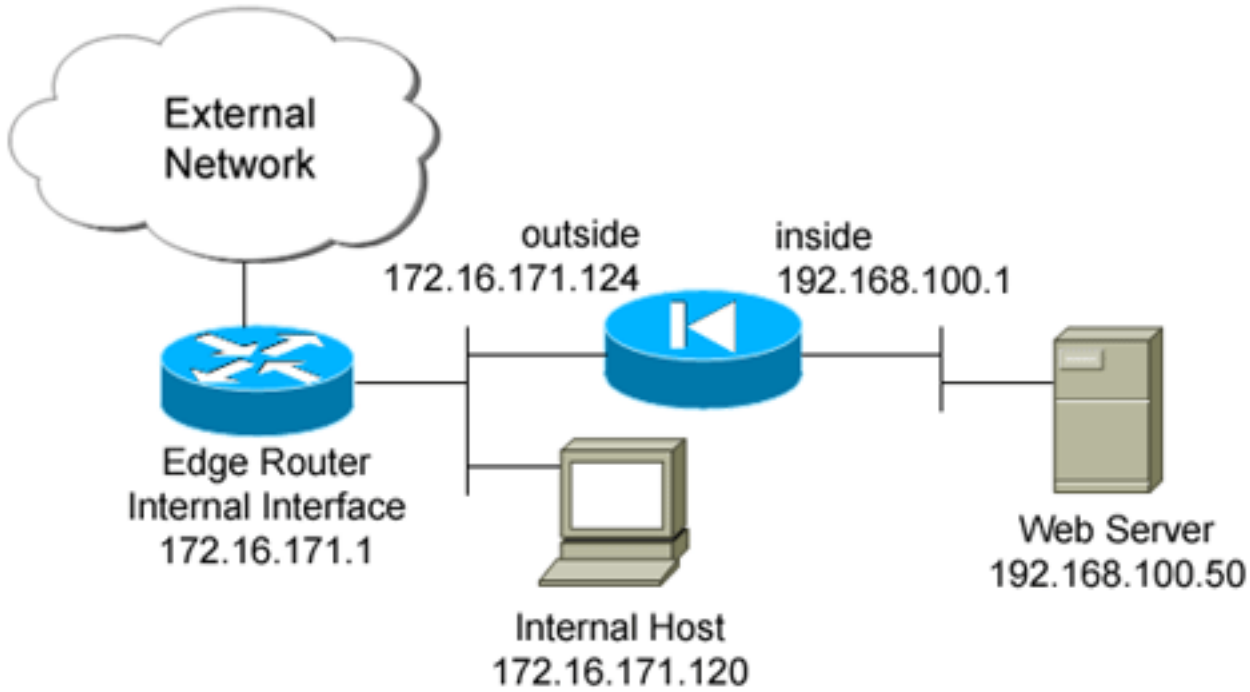
Configureren

Dit configuratievoorbeeld heeft een interne webserver op 192.168.100.50, die achter de ASA ligt. Het vereiste is dat de server toegankelijk moet zijn voor de externe netwerkinterface door zijn interne IP-adres van 192.168.100.50 en zijn externe adres van 172.16.171.125. Er is ook een beveiligingsbeleidvereiste dat het privé-IP-adres van 192.168.100. 50 is alleen toegankelijk via het 172.16.171.0/24 netwerk. Bovendien zijn het Internet Control Message Protocol (ICMP) en het Port 80-verkeer de enige protocollen die binnenkomend op de interne webserver zijn toegestaan. Aangezien er twee globale IP adressen zijn die aan één lokaal IP adres in kaart worden gebracht, moet u beleid NAT gebruiken. Anders wijst PIX/ASA de twee één-op-één statcs met een overlappende adresfout af.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd



Configuratie

Dit document gebruikt deze configuratie.

```
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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

1. Op upstream IOS® router 172.16.17.1.1, controleer of u beide globale IP adressen van de webserver kunt bereiken via de **ping** opdracht.

```
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. Controleer op de ASA of u de vertalingen ziet die in de vertaal- (verlooptabel) zijn ingebouwd.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Als uw ping of verbinding niet succesvol is, probeer dan om syslogs te gebruiken om te bepalen of er problemen met de vertaalconfiguratie zijn. Op een licht gebruikt netwerk (zoals een labomgeving) is de grootte van de houtkapbuffer meestal toereikend om het probleem op te lossen. Anders moet u de syslogs naar een externe syslogserver doorsturen. Schakel loggen in op de buffer op niveau 6 om te zien of de configuratie juist is in deze syslig-items.

```
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)
```

Als u vertaalfouten in het logbestand ziet, dubbelcontroleert u de NAT-configuraties. Als u geen systemen waarneemt, gebruikt u de **opnamefunctie** van de ASA om het verkeer op de interface op te nemen. Om een opname in te stellen, moet u eerst een toegangslijst specificeren om op een specifiek type verkeer of TCP-stroom te matchen. Daarna moet u deze opname op een of meer interfaces toepassen om te beginnen met het opnemen van pakketten.

```
!--- 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
```

Gerelateerde informatie

- ASA 7.2 opdrachtreferentie
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems