PIX/ASA 7.x/FWSM 3.x: Traducir Varias Direcciones IP Globales a una Dirección IP Local Única Usando la Política Estática NAT

Contenido

Introducción

Este documento provee una configuración de ejemplo para asignar una dirección IP local a dos o más direcciones IP globales mediante Traducción de Dirección de Red (NAT) estática basada en políticas en el software PIX/Adaptive Security Appliance (ASA) 7.x.

Prerequisites

Requirements

Asegúrese de cumplir este requisito antes de intentar esta configuración:

- Asegúrese de tener un conocimiento funcional de la CLI de PIX/ASA 7.x y experiencia previa en la configuración de listas de acceso y NAT estática.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este ejemplo específico utiliza un ASA 5520. Sin embargo, las configuraciones de NAT de políticas funcionan en cualquier dispositivo PIX o ASA que ejecute 7.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

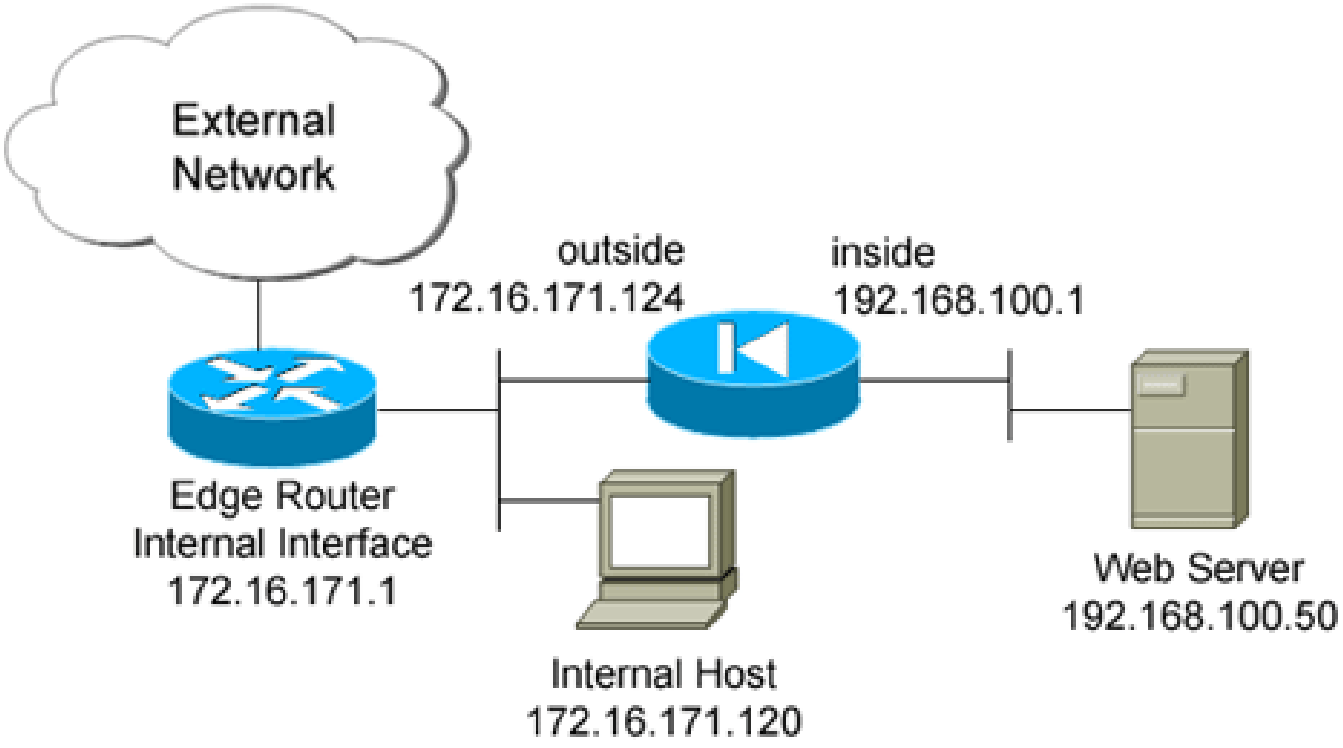
Configurar

Este ejemplo de configuración tiene un servidor web interno en 192.168.100.50, ubicado detrás del ASA. El requisito es que el servidor debe ser accesible a la interfaz de red externa por su dirección IP interna de 192.168.100.50 y su dirección externa de 172.16.171.125. También existe un requisito de política de seguridad que establece que la dirección IP privada 192.168.100.50 solo se puede acceder a través de la red 172.16.171.0/24. Además, el protocolo de mensajes de control de Internet (ICMP) y el tráfico del puerto 80 son los únicos protocolos permitidos de entrada al servidor web interno. Dado que hay dos direcciones IP globales asignadas a una dirección IP local, debe utilizar la política NAT. De lo contrario, el PIX/ASA rechaza las dos estáticas uno a uno con un error de dirección superpuesta.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red



Configuración

Este documento usa esta configuración.

```
<#root>

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 wa



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 a



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.



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.
```

```
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
```

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

1. En el router ascendente IOS® 172.16.171.1, verifique que puede alcanzar ambas direcciones IP globales del servidor web a través del comando ping.

```
<#root>

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. En ASA, verifique que vea las traducciones que se construyen en la tabla translation (xlate).

```
<#root>

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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de

configuración.

Si el ping o la conexión no son correctos, intente utilizar syslogs para determinar si hay algún problema con la configuración de traducción. En una red poco utilizada (como un entorno de laboratorio), el tamaño del búfer de registro suele ser suficiente para solucionar el problema. De lo contrario, debe enviar los syslogs a un servidor syslog externo. Habilite el registro en el buffer en el nivel 6 para ver si la configuración es correcta en estas entradas de syslog.

```
<#root>

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 !--- (172.16.171.12


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)
```

Si ve errores de traducción en el registro, vuelva a comprobar las configuraciones de NAT. Si no observa ningún syslog, utilice la función capture en ASA para intentar capturar el tráfico en la interfaz. Para configurar una captura, primero debe especificar una lista de acceso que coincida en un tipo específico de tráfico o flujo TCP. A continuación, debe aplicar esta captura a una o más interfaces para comenzar a capturar paquetes.

<#root>

!--- Create a capture access-list to match on port 80 traffic to !--- the external IP address of 172.16

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. Not

capture

!--- on the inside interface, in packet 2 you should see the server reply with !--- 192.168.100.50 as

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

Información Relacionada

- Referencia de Comandos de ASA 7.2
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).