Configurar el ASA para redes internas dobles

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuración de ASA 9.x](#)
[Permita que los hosts internos accedan a las redes externas con PAT](#)
[Configuración del Router B](#)
[Verificación](#)
[Conexión](#)
[Troubleshoot](#)
[Registros del sistema](#)
[Rastreadores de paquetes](#)
[Captura](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo configurar un dispositivo de seguridad adaptable de Cisco (ASA) que ejecuta la versión de software 9.x para el uso de dos redes internas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el Cisco ASA que ejecuta software versión 9.x.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. 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.

Antecedentes

Cuando agrega una segunda red interna detrás de un firewall ASA, tenga en cuenta esta información importante:

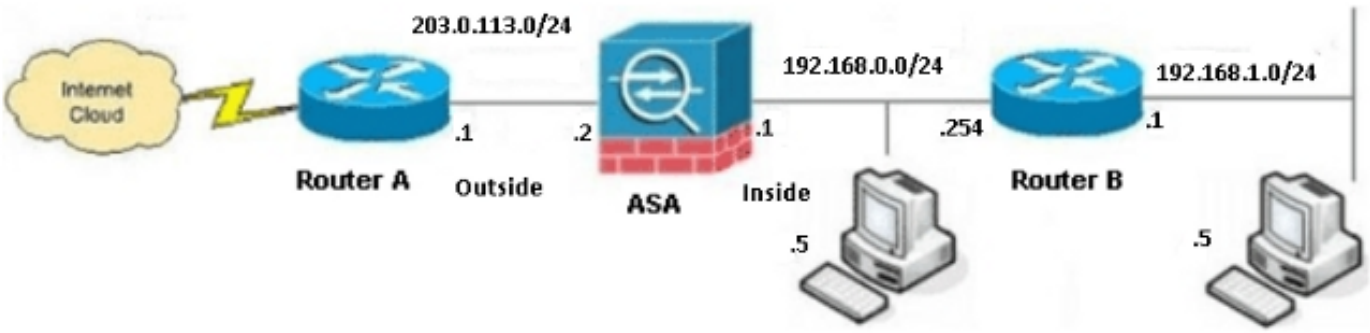
- ASA no admite direccionamiento secundario.
- Debe usarse un router detrás del ASA para lograr el enrutamiento entre la red actual y la red recién agregada.
- La puerta de enlace predeterminada para todos los hosts debe apuntar al router interno.
- Debe agregar una ruta predeterminada en el router interno que apunte a la ASA.
- Debe vaciar el caché del Protocolo de resolución de direcciones (ARP) del router interno.

Configurar

Use la información que se describe en esta sección para configurar la ASA.

Diagrama de la red

Aquí se presenta la topología que se usa para los ejemplos de todo el documento:



Nota: Los esquemas de direcciones IP que se usan en esta configuración no pueden enrutarse legalmente a Internet. Son [direcciones RFC 1918 que se usan en un entorno de laboratorio.]

Configuración de ASA 9.x

Si tiene la salida del **comando de terminal de escritura del dispositivo de Cisco, puede usar la herramienta** Output Interpreter (solo para clientes registrados) a fin de ver posibles problemas y soluciones.

Esta es la configuración para el ASA que ejecuta la versión de software 9.x:

```
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
```

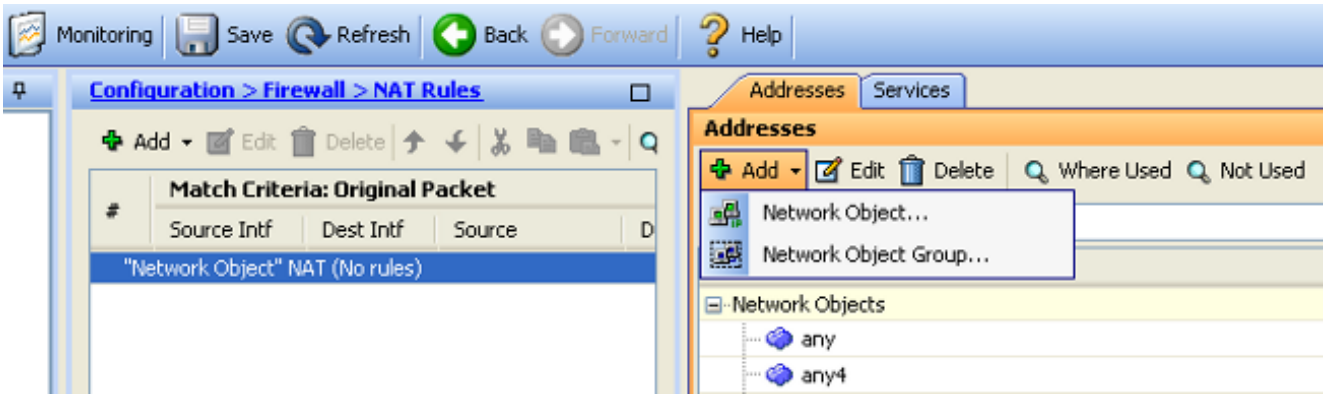
```
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map 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
```

Permita que los hosts internos accedan a las redes externas con PAT

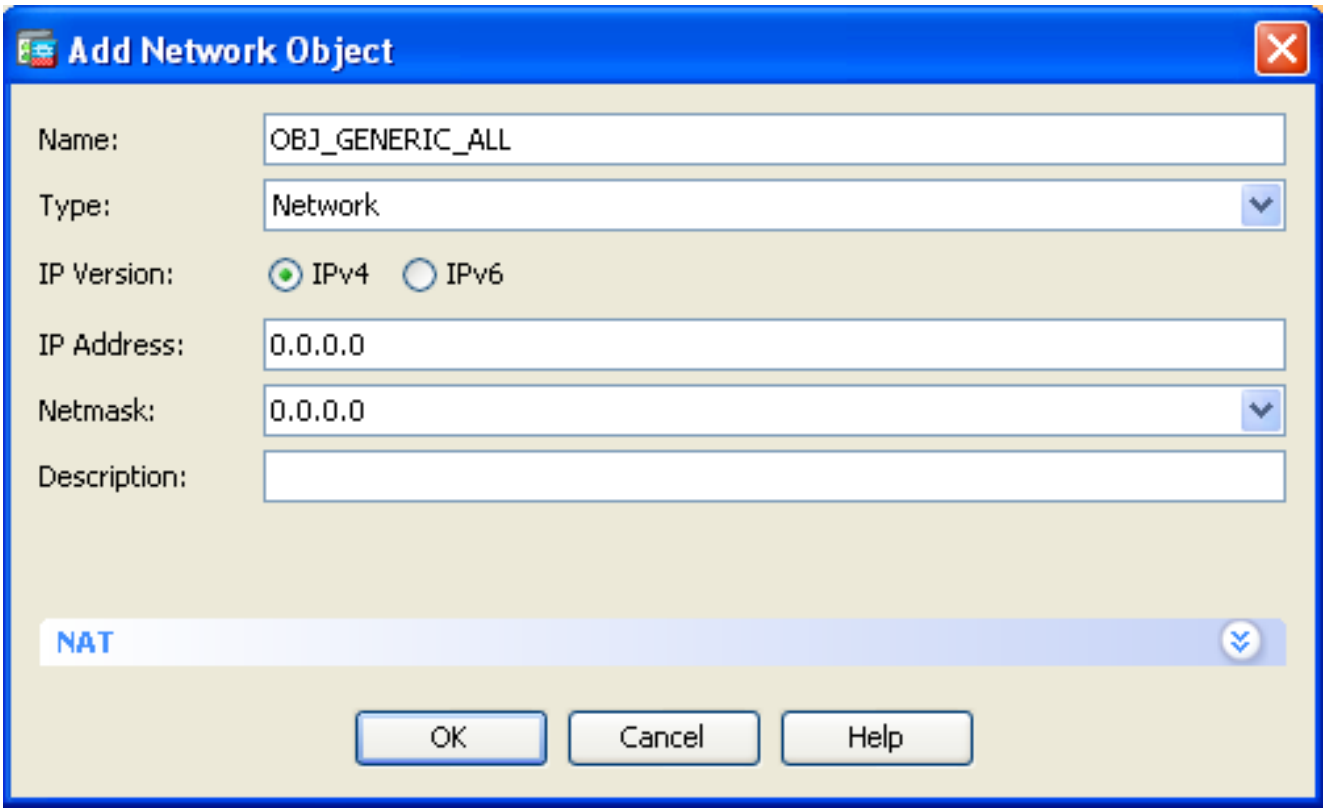
Si desea que los hosts internos compartan una única dirección pública para la traducción, utilice la traducción de direcciones de puerto (PAT). Una de las configuraciones de PAT más simples implica la traducción de todos los hosts internos para que parezcan ser la IP de la interfaz externa. Esta es la configuración típica de PAT que se usa cuando la cantidad de direcciones IP enrutables que están disponibles del ISP se limita a solo algunas, o solo a una.

Complete estos pasos para permitir que los hosts internos accedan a las redes externas con PAT:

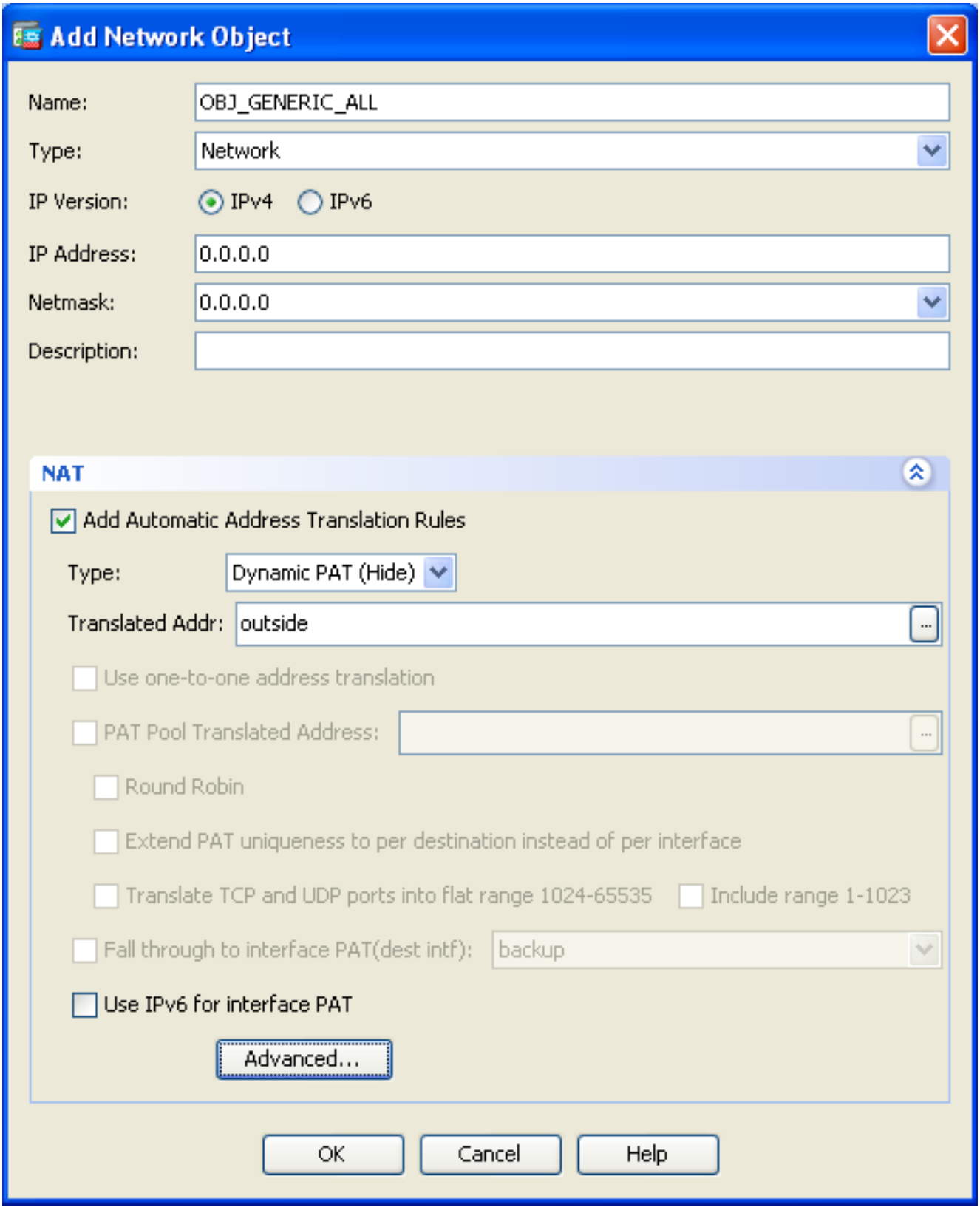
1. Vaya a **Configuración> Firewall> Reglas NAT**, haga clic en **Agregar** y elija **Objeto de red para configurar una regla de NAT dinámica:**



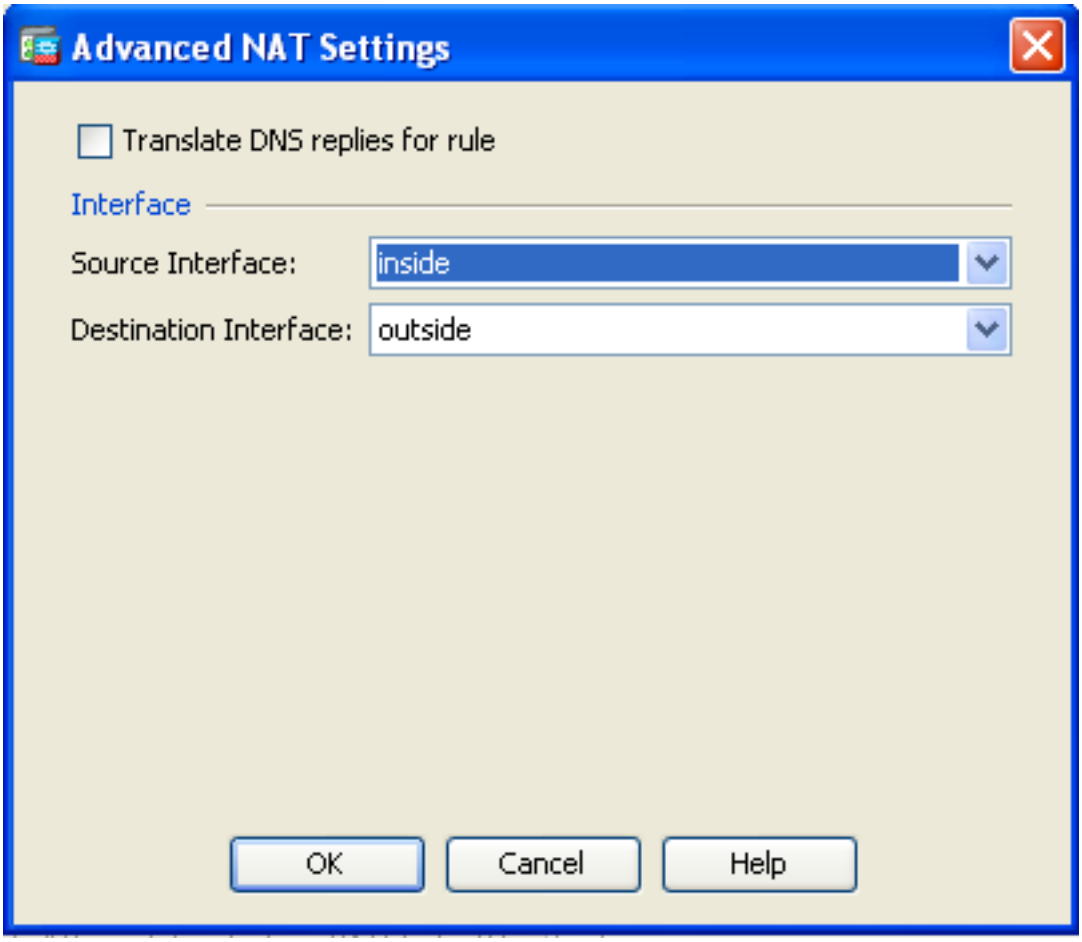
2. Configure la red/el host/el alcance para el que se requiere la PAT dinámica. En este ejemplo, se seleccionaron todas las subredes internas. Este proceso debe repetirse para las subredes específicas que desea traducir de esta manera:



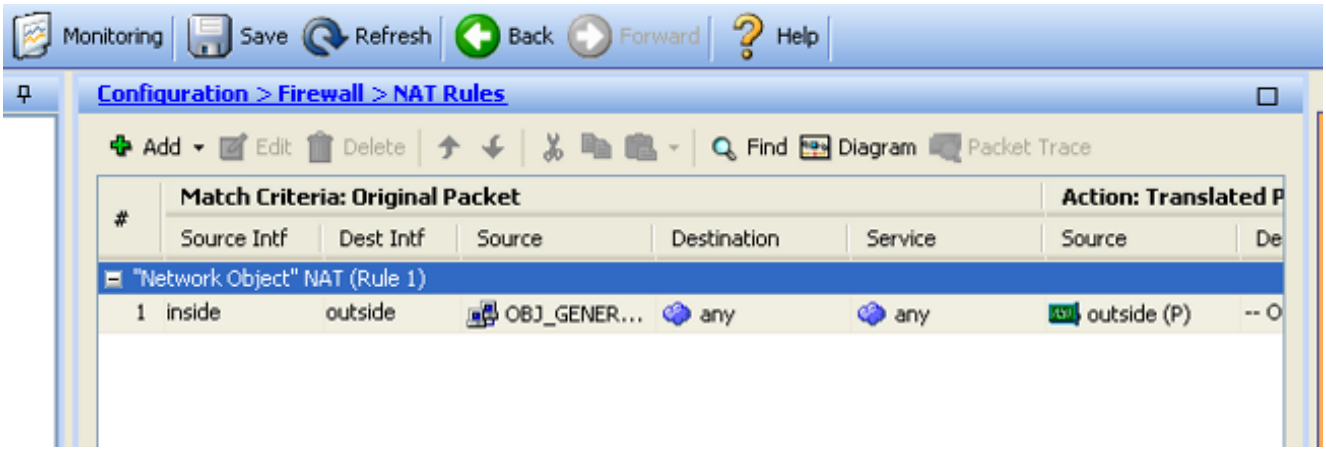
3. Haga clic en NAT, marque la casilla de verificación **Agregar regla de traducción automática de direcciones, ingrese Dinámico** y establezca la opción **Dirección traducida** para que refleje la interfaz externa. Si hace clic en el botón de puntos suspensivos, lo ayuda a elegir un objeto preconfigurado, como la interfaz externa:



4. Haga clic en **Avanzado para seleccionar una interfaz de origen y de destino:**



5. Haga clic en Aceptar y luego en **Aplicar para aplicar los cambios.** Una vez completado, el administrador de dispositivos de seguridad adaptable (ASDM) muestra la regla de NAT:



Configuración del Router B

A continuación se muestra la configuración de Router B:

```
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
```

Verificación

Acceda a un sitio web por HTTP desde un navegador web para verificar que la configuración funcione correctamente.

En este ejemplo se usa un sitio que está alojado en la dirección IP 198.51.100.100. Si la conexión se realiza correctamente, las salidas que se proporcionan en las siguientes secciones se pueden ver en la CLI de ASA.

Conexión

Ingrese el comando **show connection address para verificar la conexión:**

```
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
```

El ASA es un firewall con estado, y el tráfico de retorno del servidor web puede regresar por el firewall porque coincide con una conexión de la tabla de conexiones del firewall. Al tráfico que coincide con una conexión que ya existe se le permite pasar por el firewall sin bloquearse con una lista de control de acceso (ACL) de interfaz.

En la salida anterior, el cliente de la interfaz interna estableció una conexión con el host 198.51.100.100 fuera de la interfaz externa. Esta conexión se realiza con el protocolo TCP y ha estado inactiva durante seis segundos. Los indicadores de conexión indican el estado actual de esta conexión.

> **Nota:** Consulte el documento de Cisco Indicadores de conexión de TCP de ASA (conexión y desconexión) para obtener más información sobre los indicadores de conexión.

Troubleshoot

Use la información descrita en esta sección para solucionar los problemas de configuración.

Registros del sistema

Ingrese el comando **show log para ver los syslogs:**

```
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)
```

El firewall de ASA genera syslogs durante el funcionamiento normal. El nivel de detalle de los syslogs depende de la configuración de registro. El resultado muestra dos syslog que se ven en el nivel seis, o el *nivel de la información.*

En este ejemplo, se generan dos syslogs. El primero es un mensaje de registro para indicar que el firewall ha creado una traducción; específicamente, una traducción de TCP dinámica (PAT). Indica la dirección IP y el puerto de origen, así como la dirección IP y el puerto traducidos, a medida que el tráfico atraviesa las interfaces internas hacia las externas.

El segundo syslog indica que el firewall ha creado una conexión en su tabla de conexiones para este tráfico específico entre el cliente y el servidor. Si el firewall se configuró para bloquear este intento de conexión, o algún otro factor impidió establecer esta conexión (restricciones de recursos o una posible configuración incorrecta), el firewall no genera un registro para indicar que se creó la conexión. En cambio, registra un motivo para denegar la conexión o una indicación con

respecto al factor que impidió que se estableciera dicha conexión.

Rastreadores de paquetes

Ingrese este comando para habilitar la función de rastreador de paquetes:

```
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
```

La función de rastreador de paquetes en el ASA permite especificar un paquete *simulado y ver toda la diversidad de pasos, comprobaciones y funciones que el firewall realiza cuando procesa el tráfico.* Con esta herramienta, es útil identificar un ejemplo del tráfico que usted cree que *debe* poder pasar por el firewall y utilizar esa tupla de 5 para simular el tráfico. En el ejemplo anterior, se utiliza el rastreador de paquetes para simular un intento de conexión que cumpla con estos criterios:

- El paquete simulado llega a la interfaz interna.
- El protocolo que se usa es TCP.
- La dirección IP del cliente simulado es 192.168.1.5.
- El cliente envía el tráfico que se origina en el puerto 1234.
- El tráfico se destina a un servidor en la dirección IP 198.51.100.100.
- El tráfico está destinado al puerto 80.

Observe que no se mencionó la interfaz externa en el comando. Esto se debe al diseño del rastreador de paquetes. La herramienta le indica cómo el firewall procesa ese tipo de intento de conexión, lo que incluye cómo lo enrutaría y desde qué interfaz.

> **Consejo:** Para obtener más información sobre la función de rastreador de paquetes, consulte la sección Rastreo de paquetes con Packet Tracer de la *Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6*.

Captura

Ingrese estos comandos para aplicar una captura:

```
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>
```

El firewall de ASA puede capturar el tráfico que ingresa o sale de sus interfaces. Esta función de captura es fantástica porque puede probar definitivamente si el tráfico llega o sale de un firewall. El ejemplo anterior muestra la configuración de dos capturas denominadas **capin y capout en las interfaces internas y externas, respectivamente.** Los **comandos de captura utilizan la palabra clave match, que le permite especificar el tráfico que desea capturar.**

Para el ejemplo de captura de *capin, se indica que desea hacer coincidir el tráfico que se ve en la interfaz interna (ingreso o egreso) que coincide con el host tcp 192.168.1.5 host 198.51.100.100*. En otras palabras, desea capturar cualquier tráfico TCP que se envíe del host *192.168.1.5 al host 198.51.100.100*, o viceversa. El uso de la palabra clave match permite que el firewall capture ese tráfico bidireccionalmente. El comando **capture que se define para la interfaz externa no hace referencia a la dirección IP interna del cliente porque el firewall realiza PAT en esa dirección IP del cliente.** Como resultado, no puede coincidir con esa dirección IP de cliente. En cambio, este ejemplo usa **any** para indicar que todas las direcciones IP posibles coincidirían con esa condición.

Después de configurar las capturas, puede intentar establecer una conexión nuevamente y proceder a ver las capturas con el comando **show capture*<capture_name>*** . En este ejemplo, puede ver que el cliente puede conectarse al servidor, como lo demuestra el protocolo TCP de enlace de tres vías que se ve en las capturas.

Información Relacionada

- Cisco Adaptive Security Device Manager
- Firewalls de próxima generación Cisco ASA Serie 5500-X
- Peticiones de comentarios (RFC)
- Guía de configuración de CLI de la serie Cisco ASA, 9.0 âÂÂ Configuración de rutas estáticas

y predeterminadas

- Asistencia técnica y documentación âÂ Â Cisco Systems