Configuración del reenvío de puertos de ASA versión 9 con NAT

Contenido

Introducción

Este documento describe cómo configurar las funciones de redirección de puertos (reenvío) y traducción de direcciones de red (NAT) externa en la versión 9.x del software Adaptive Security Appliance (ASA), con el uso de CLI o Adaptive Security Device Manager (ASDM).

Consulte la Guía de Configuración de ASDM del Firewall de la Serie ASA de Cisco para obtener información adicional.

Prerequisites

Requirements

Consulte Configuración del Acceso a la Administración para permitir que el dispositivo sea configurado por el ASDM.

Componentes Utilizados

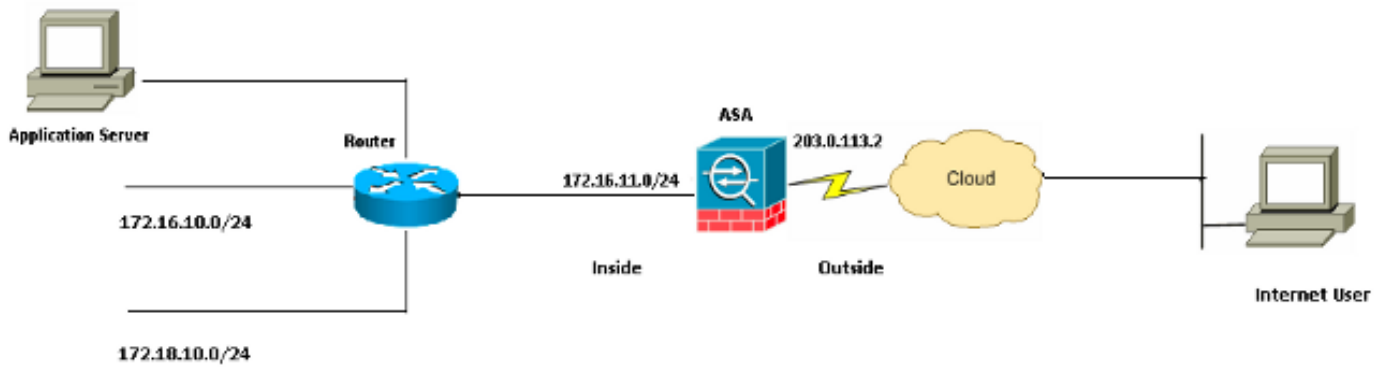
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco ASA 5525 Series Security Appliance versión 9.x y posteriores
- ASDM versión 7.x y posterior

"La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

Configurar

Diagrama de la red



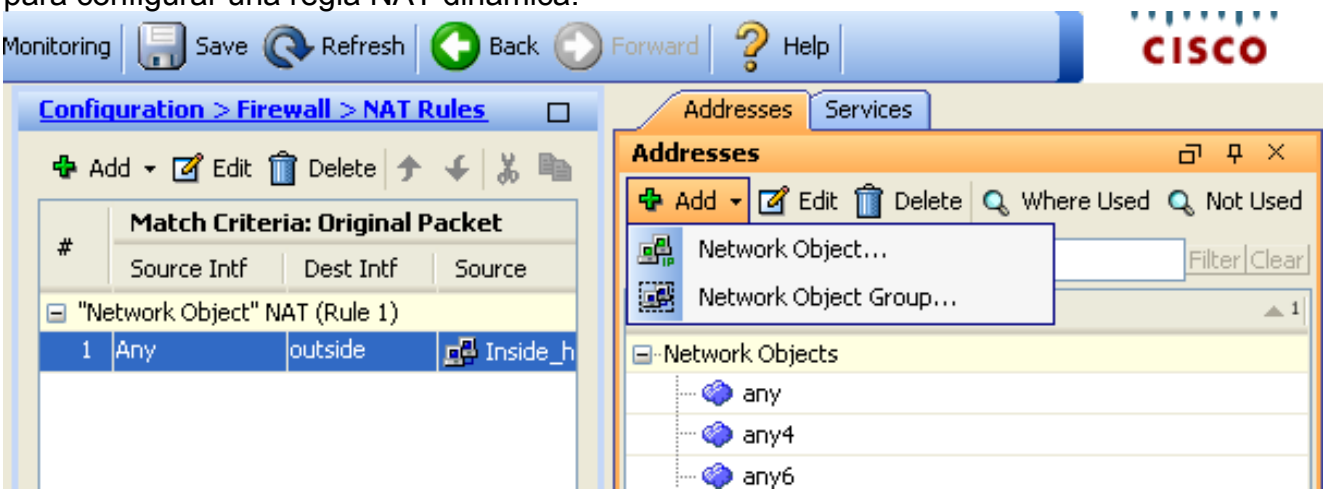
Los esquemas de dirección IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

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

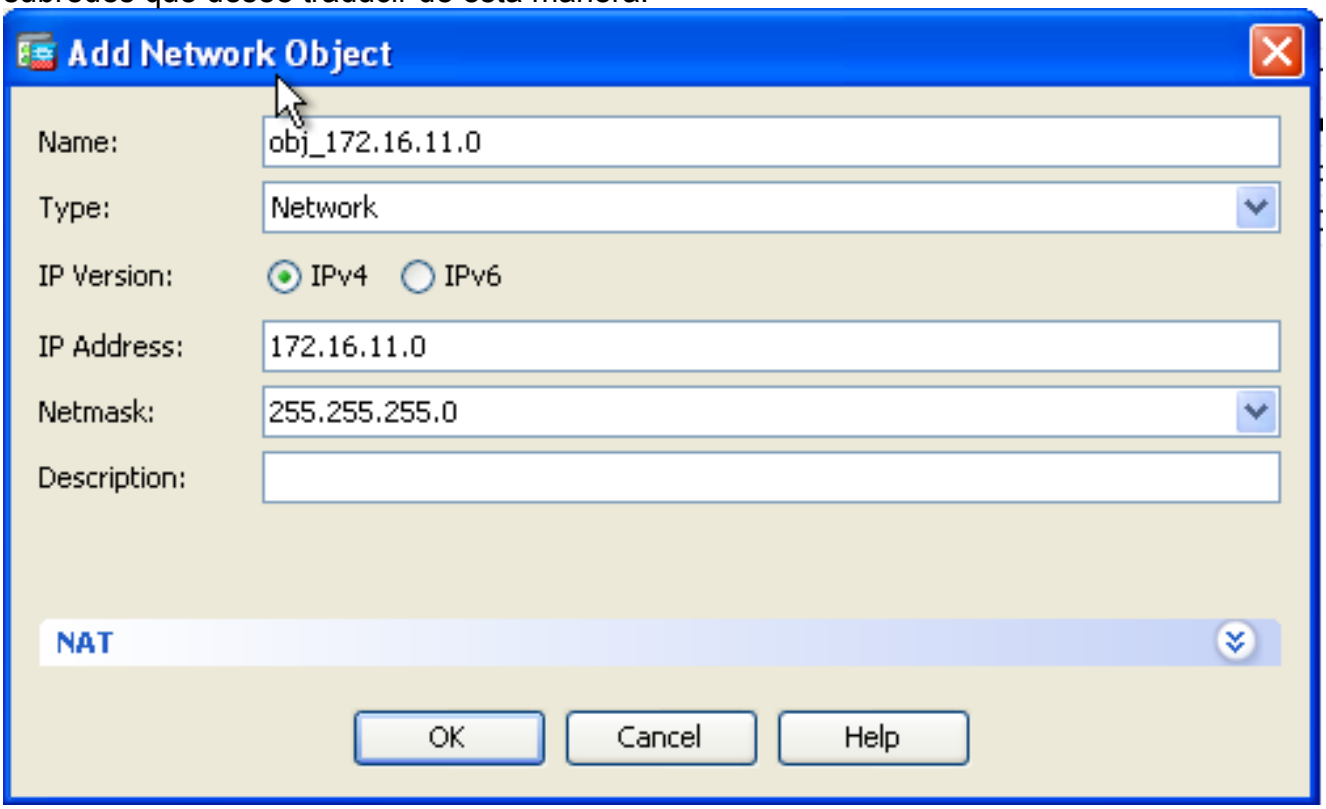
Si desea que los hosts internos compartan una única dirección pública para la traducción, utilice la Traducción de direcciones de puerto (PAT). Una de las configuraciones PAT más simples implica la traducción de todos los hosts internos para que se vean como la dirección IP de la interfaz externa. Ésta es la configuración PAT típica que se utiliza cuando el número de direcciones IP enrutables disponibles desde el ISP está limitado a sólo unas pocas, o quizás sólo una.

Complete estos pasos para permitir el acceso de los hosts internos a las redes externas con PAT:

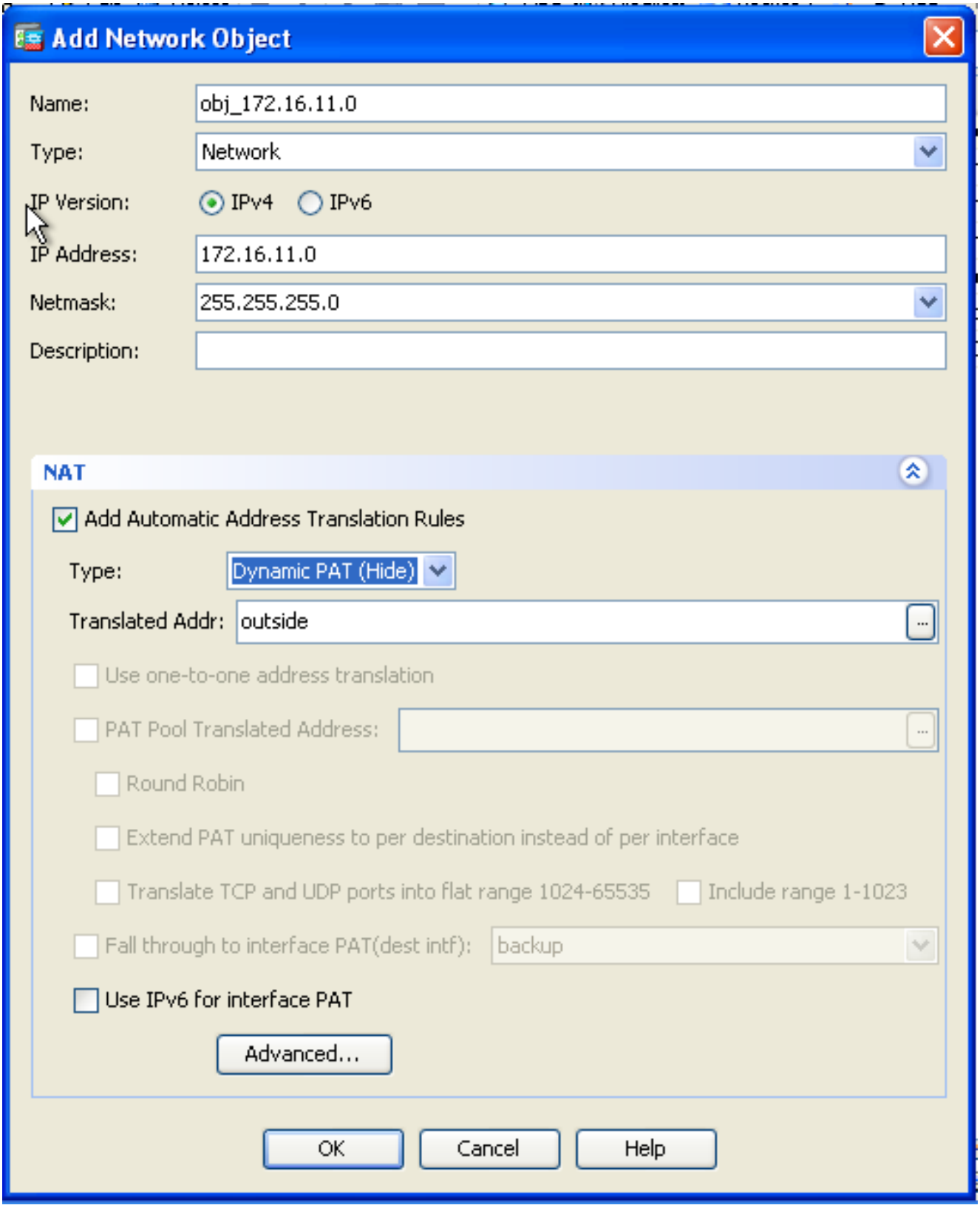
1. Elija **Configuration > Firewall > NAT Rules**. Haga clic en **Add** y luego elija **Network Object** para configurar una regla NAT dinámica.



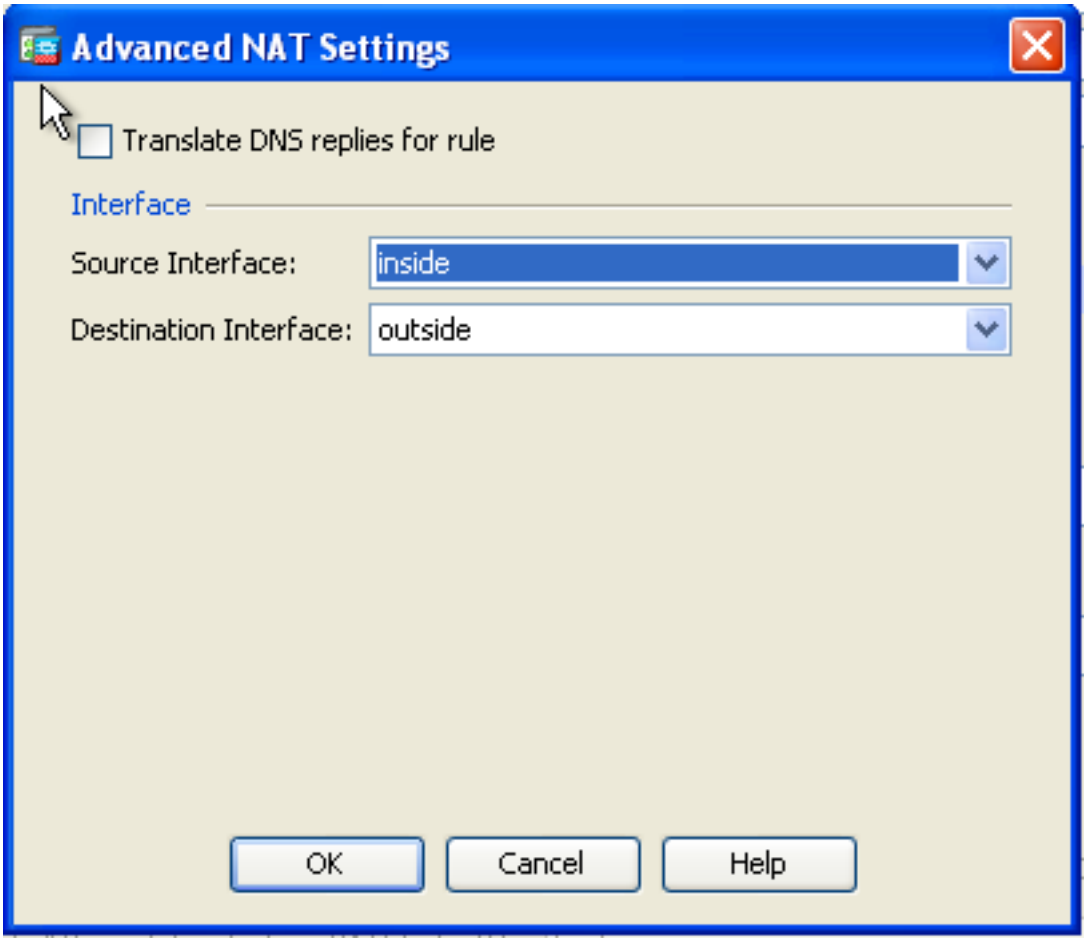
2. Configure la red/Host/Rango para el que se requiere **PAT dinámica**. En este ejemplo, se ha seleccionado una de las subredes internas. Este proceso se puede repetir para otras subredes que desee traducir de esta manera.



3. Expanda NAT. Marque la casilla de verificación **Agregar reglas de traducción automática de direcciones**. En la lista desplegable Tipo, seleccione **PAT dinámica (Ocultar)**. En el campo **Translated Addr**, elija la opción para reflejar la interfaz externa. Haga clic en **Advanced**.



4. En las listas desplegables Interfaz de origen e Interfaz de destino, elija las interfaces apropiadas. Haga clic en **Aceptar** y haga clic en **Aplicar** para que los cambios surtan efecto.



Este es el resultado CLI equivalente para esta configuración PAT:

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

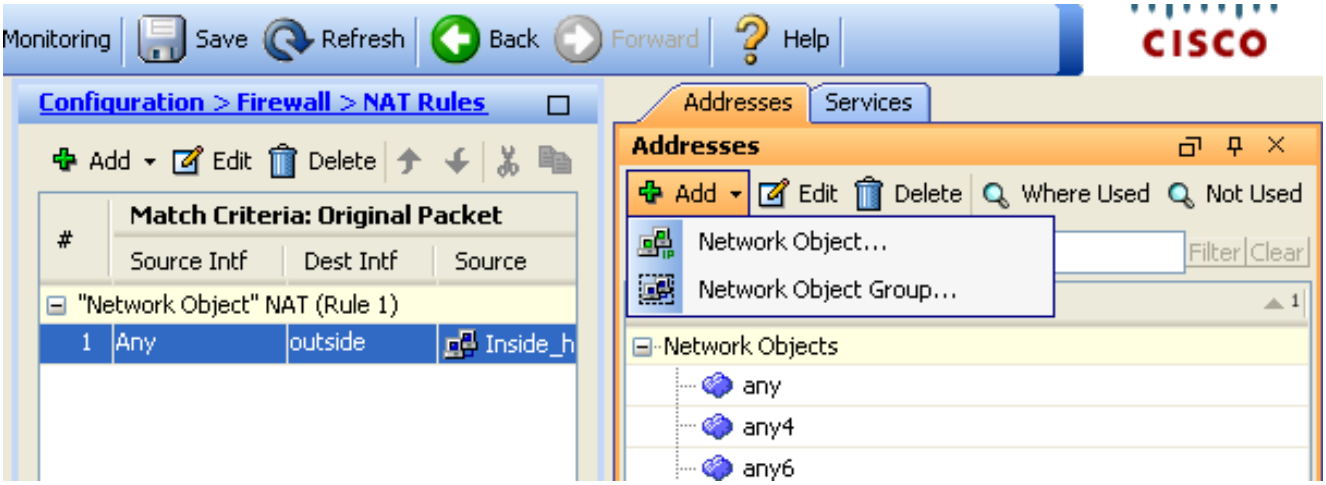
Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT

Puede permitir que un grupo de hosts/redes internas acceda al mundo exterior con la configuración de las reglas NAT dinámicas. A diferencia de PAT, NAT dinámica asigna direcciones traducidas de un conjunto de direcciones. Como resultado, un host se asigna a su propia dirección IP traducida y dos hosts no pueden compartir la misma dirección IP traducida.

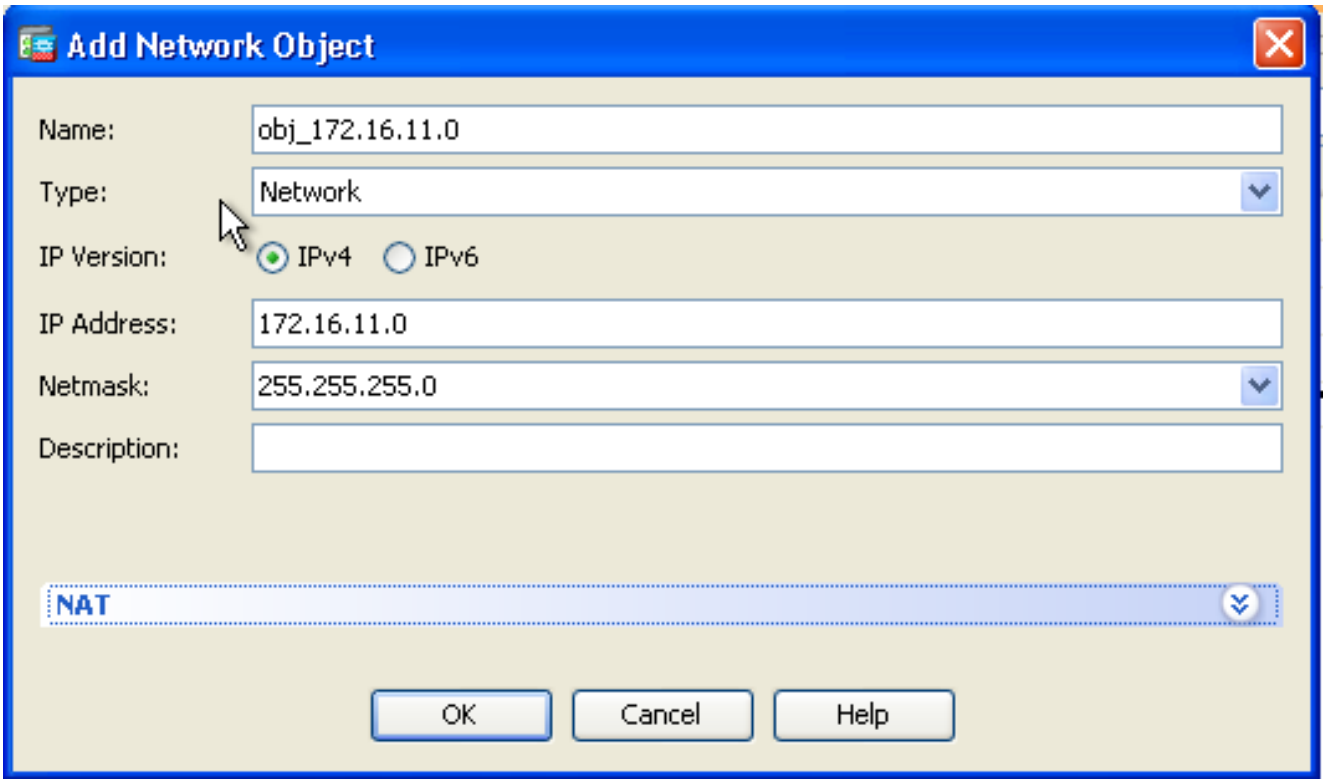
Para lograr esto, debe seleccionar la dirección real de los hosts/redes a los que se les dará acceso y luego deben ser mapeados a un conjunto de direcciones IP traducidas.

Complete estos pasos para permitir el acceso de los hosts internos a las redes externas con NAT:

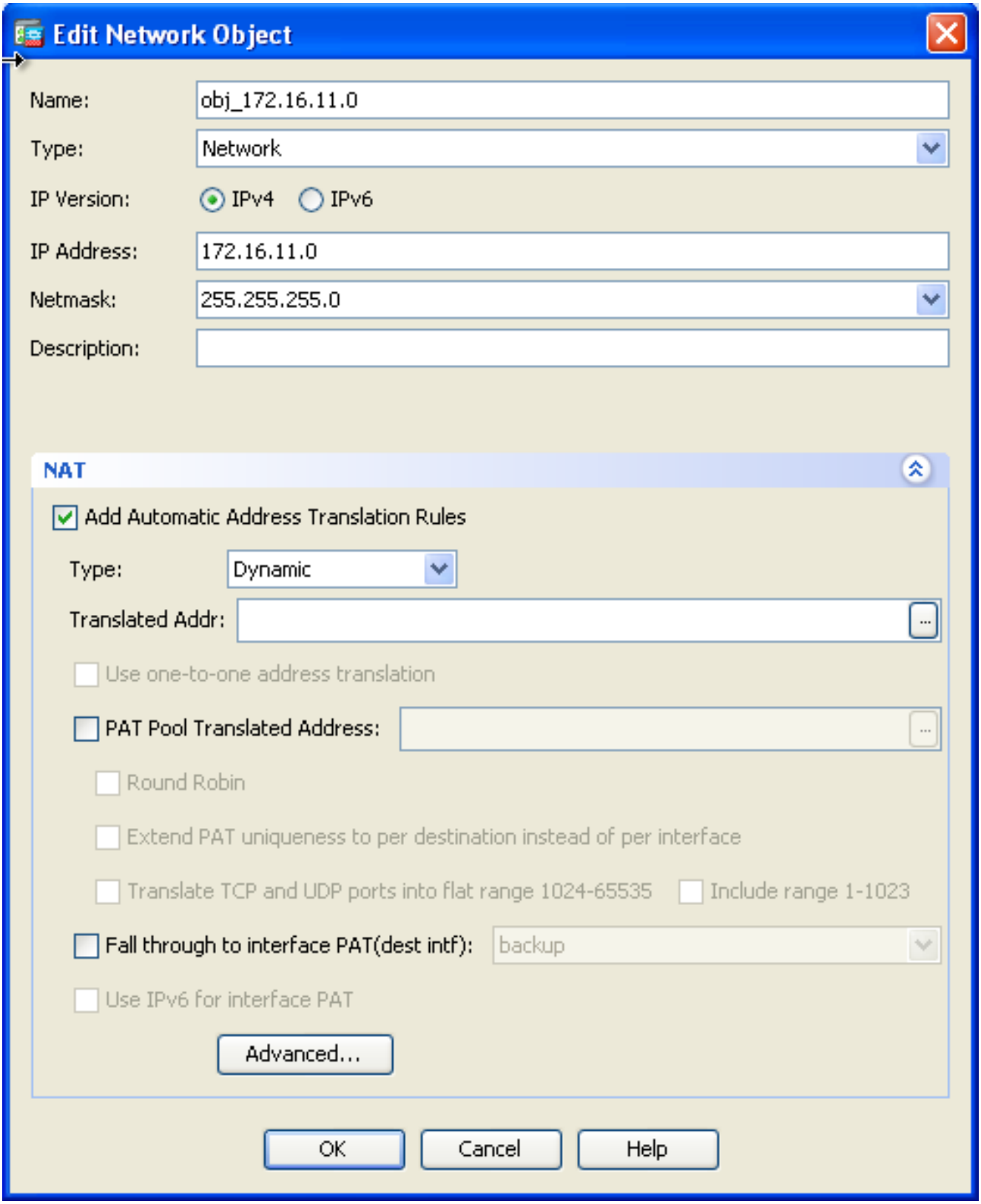
1. Elija **Configuration > Firewall > NAT Rules**. Haga clic en **Add** y luego elija **Network Object** para configurar una regla NAT dinámica.



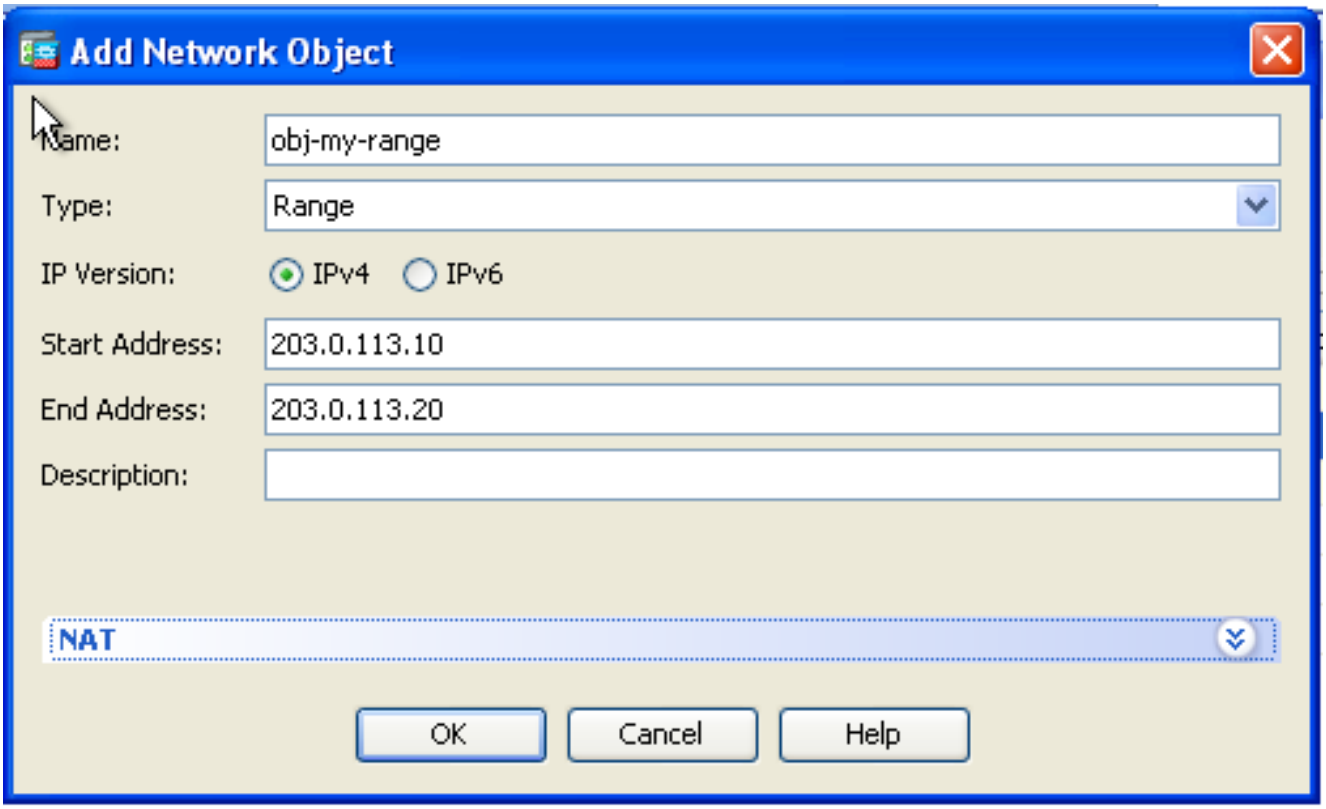
2. Configure la red/host/rango para el que se requiere PAT dinámica. En este ejemplo, se ha seleccionado toda la *red interna*.



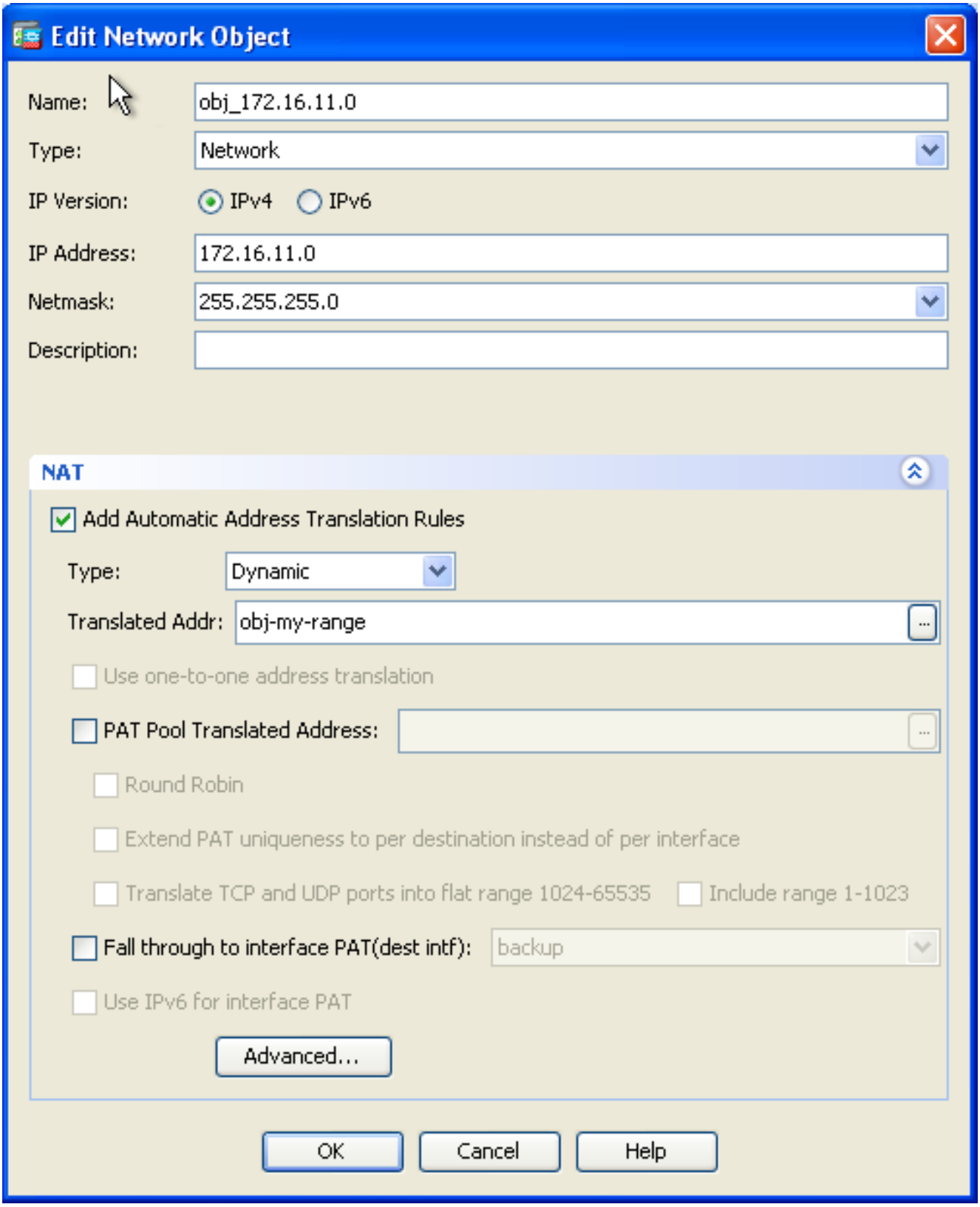
3. Expanda NAT. Marque la casilla de verificación **Agregar reglas de traducción automática de direcciones**. En la lista desplegable Tipo, elija **Dinámico**. En el campo Dirección traducida, seleccione la selección adecuada. Haga clic en **Advanced**.



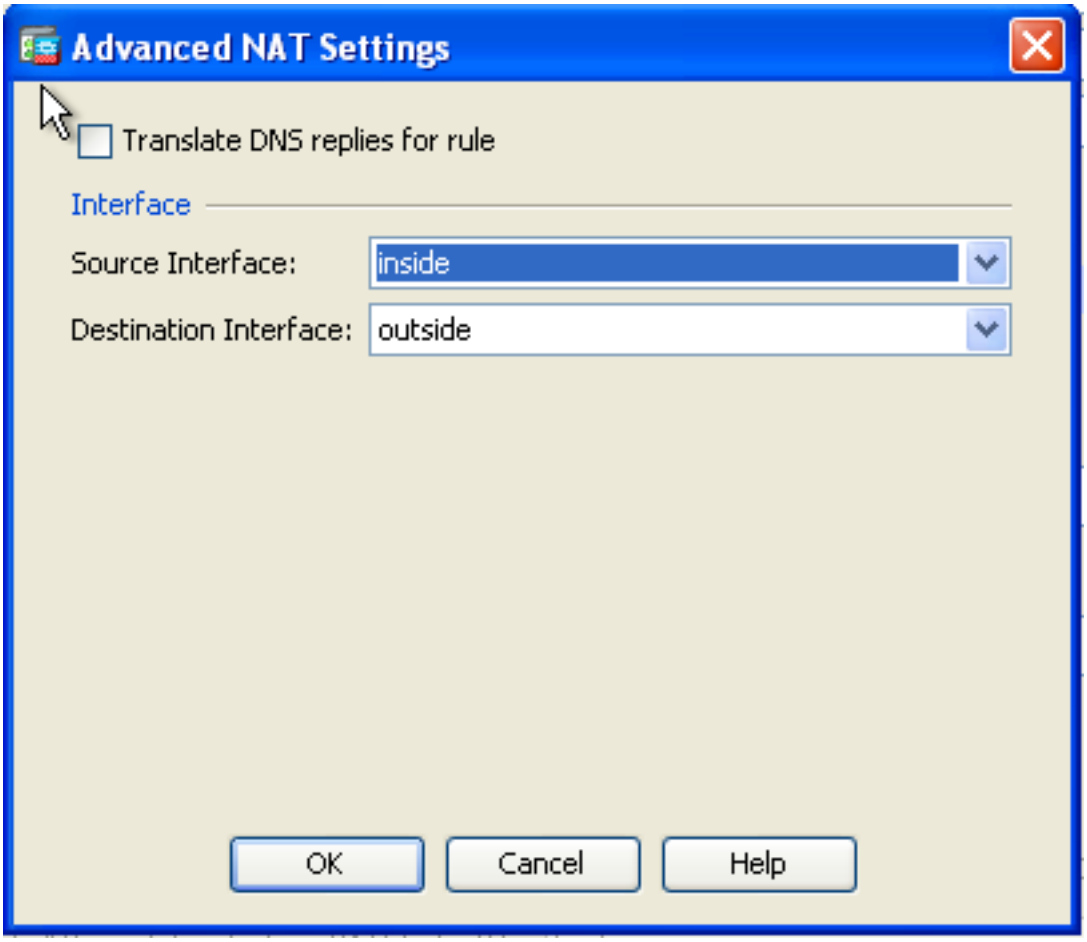
4. Haga clic en **Agregar** para agregar el objeto de red. En la lista desplegable Tipo, elija **Intervalo**. En los campos Dirección inicial y Dirección final, introduzca las direcciones IP iniciales y finales de PAT. Click OK.



5. En el campo Dirección traducida, elija el objeto de dirección. Haga clic en **Advanced** para seleccionar las interfaces de origen y destino.



6. En las listas desplegables Interfaz de origen e Interfaz de destino, elija las interfaces apropiadas. Haga clic en **Aceptar** y haga clic en **Aplicar** para que los cambios surtan efecto.

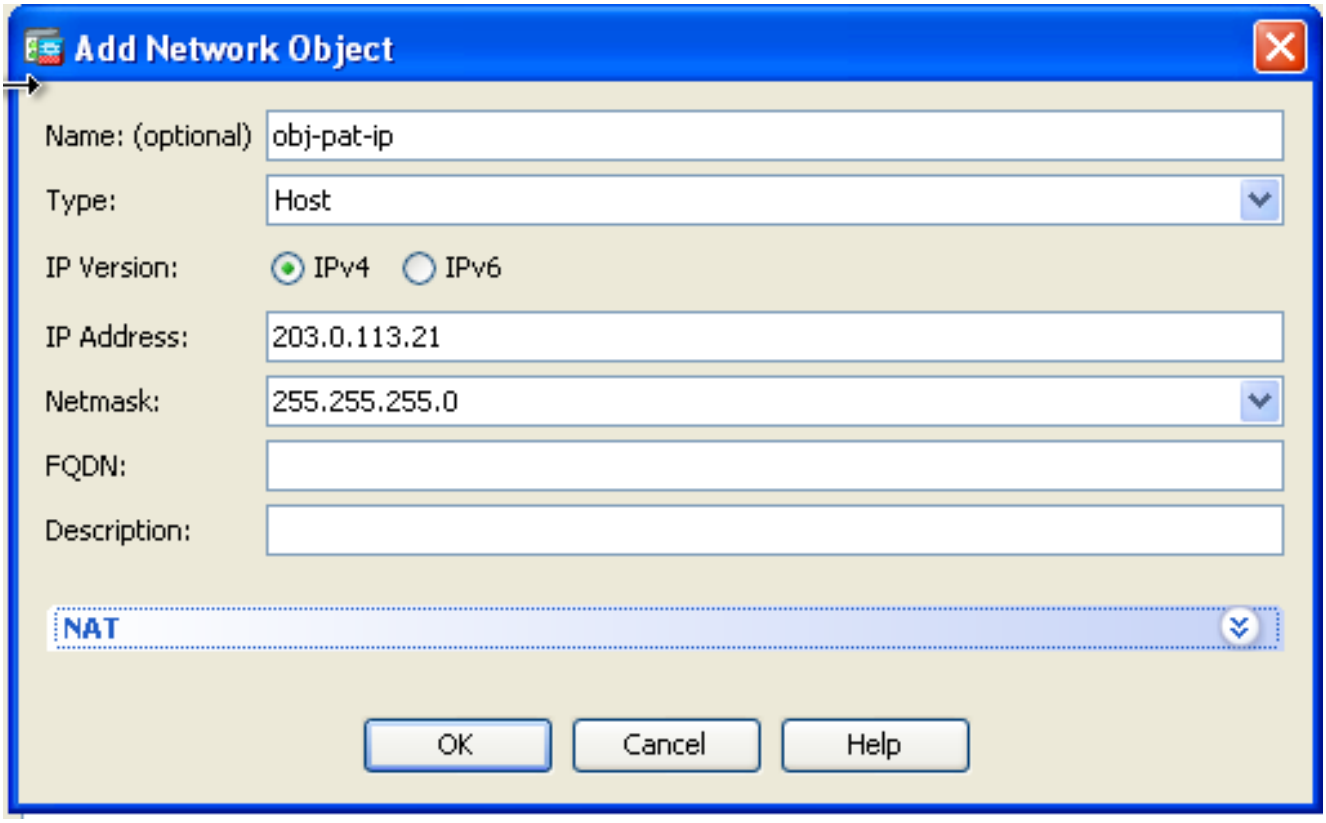


Este es el resultado CLI equivalente para esta configuración ASDM:

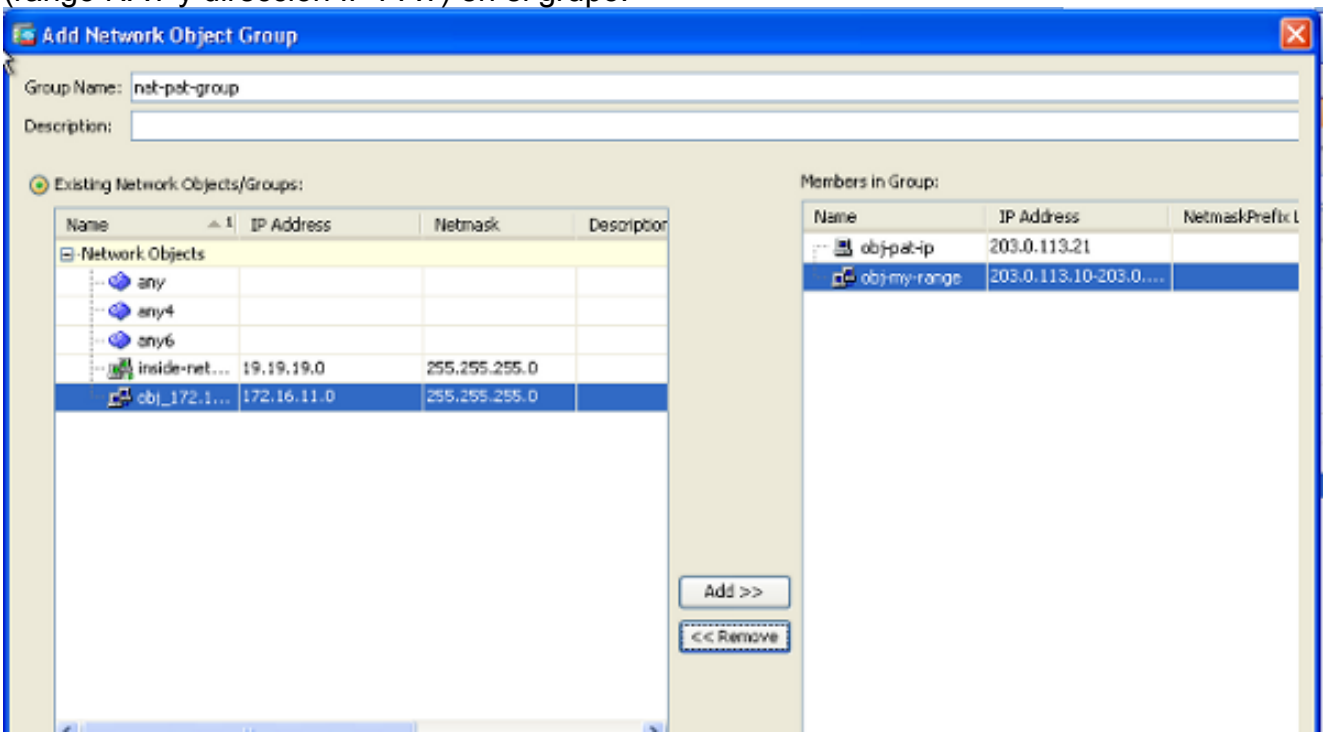
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat(inside,outside) dynamic obj-my-range
```

Según esta configuración, los hosts en la red 172.16.11.0 se traducen a cualquier dirección IP del conjunto NAT, 203.0.113.10 - 203.0.113.20. Si el conjunto asignado tiene menos direcciones que el grupo real, podría quedarse sin direcciones. Como resultado, puede intentar implementar NAT dinámica con respaldo PAT dinámico o puede intentar expandir el conjunto actual.

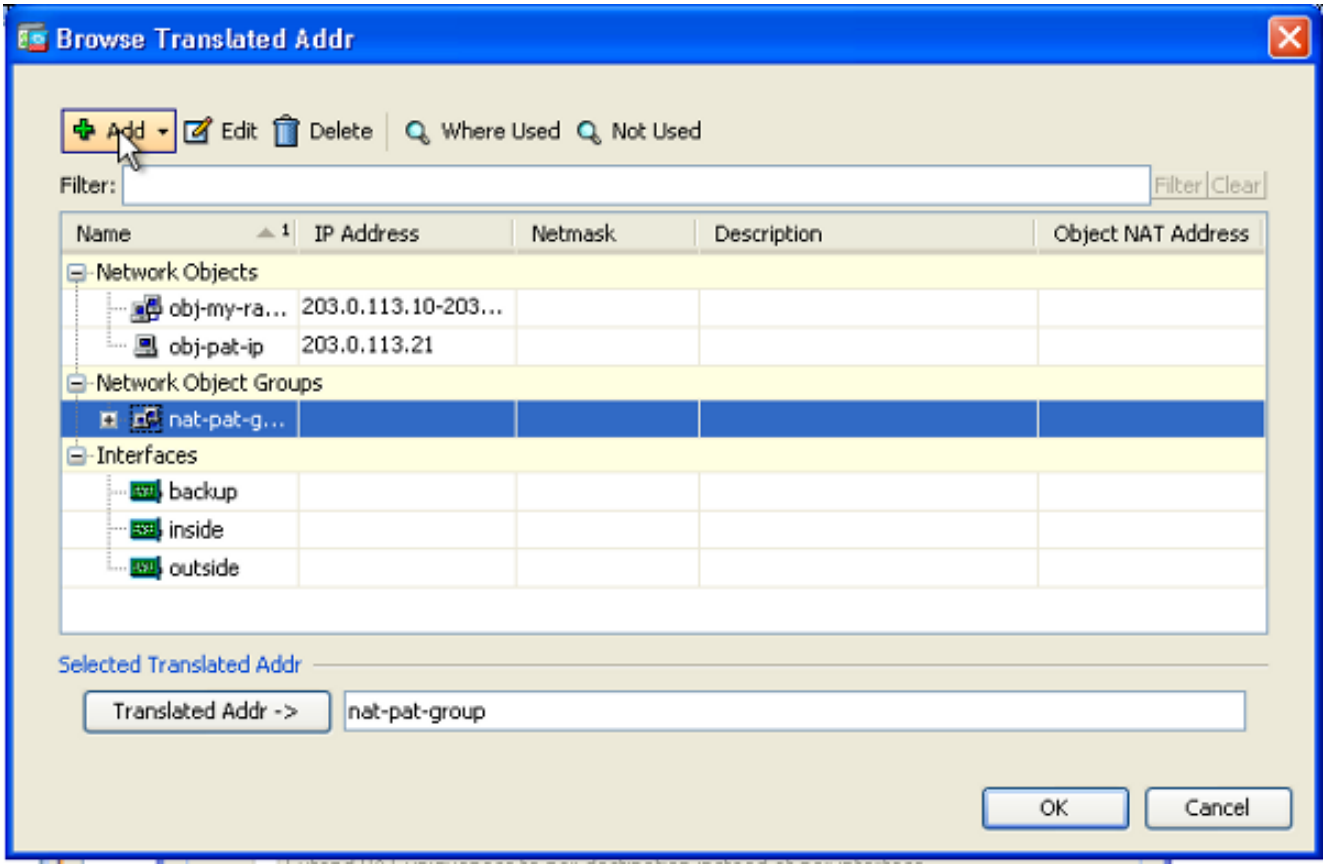
1. Repita los pasos 1 a 3 en la configuración anterior y haga clic en **Add** una vez más para agregar un objeto de red. En la lista desplegable Tipo, elija **Host**. En el campo Dirección IP, introduzca la dirección IP de copia de seguridad de PAT. Click OK.



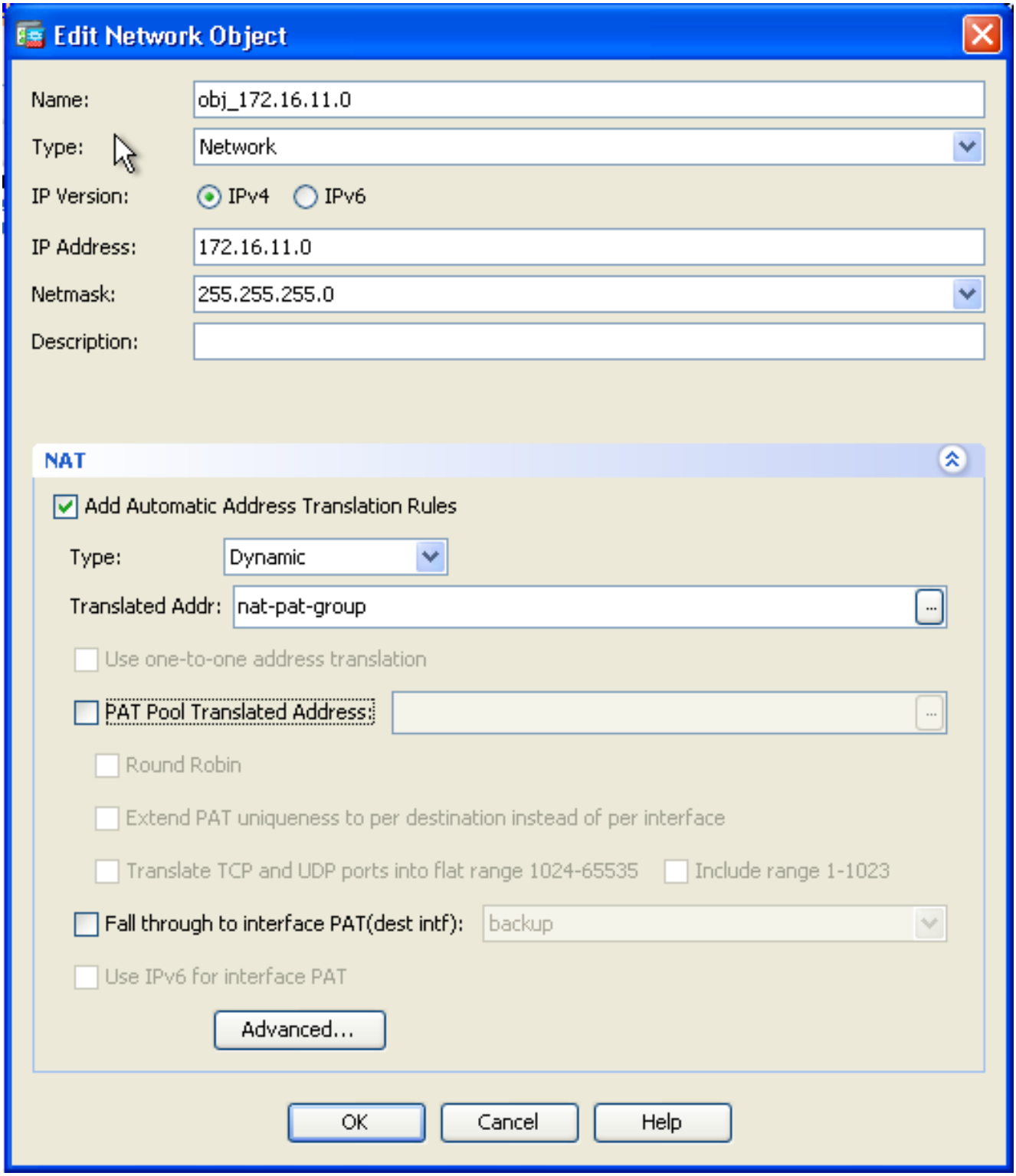
2. Haga clic en **Agregar** para agregar un grupo de objetos de red. En el campo Group Name (Nombre de grupo), introduzca un nombre de grupo y **añada** ambos objetos de dirección (rango NAT y dirección IP PAT) en el grupo.



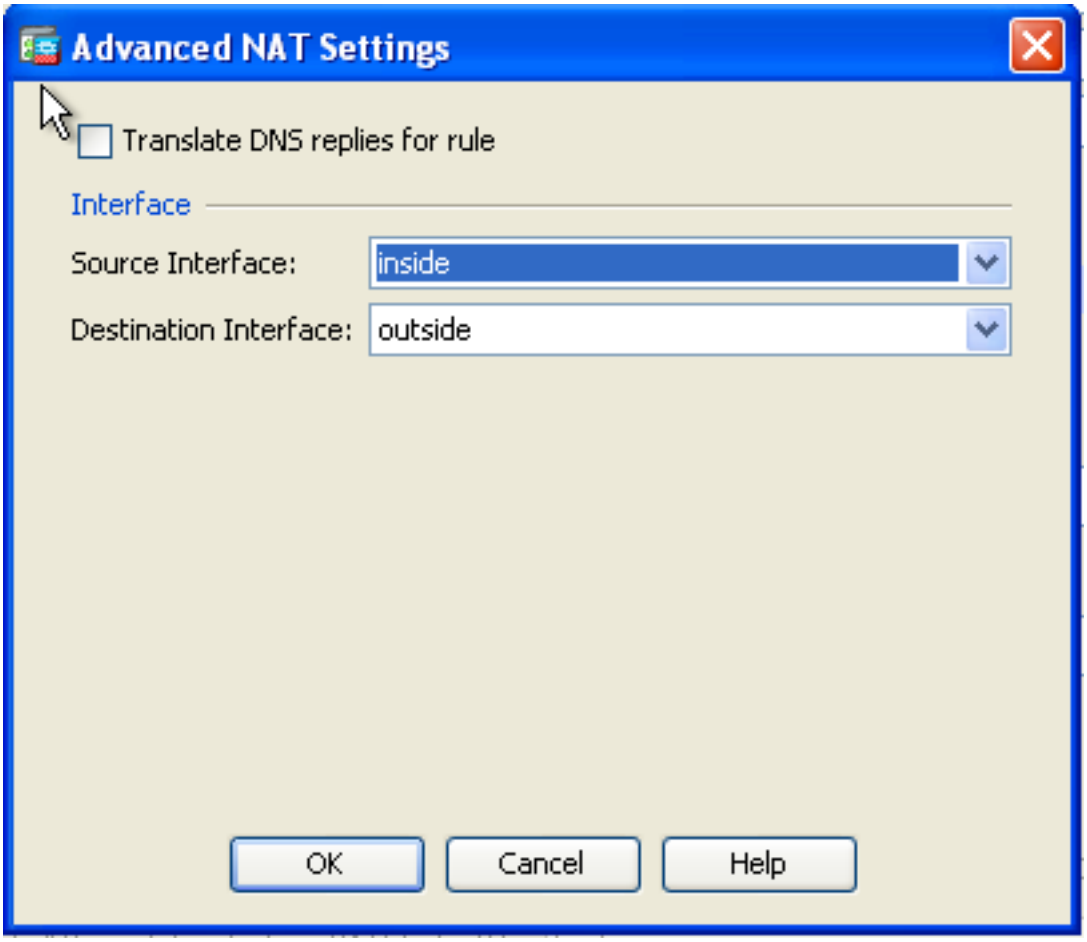
3. Elija la regla NAT configurada y cambie la dirección traducida para que sea el grupo recién configurado 'nat-pat-group' (anteriormente era 'obj-my-range'). Click OK.



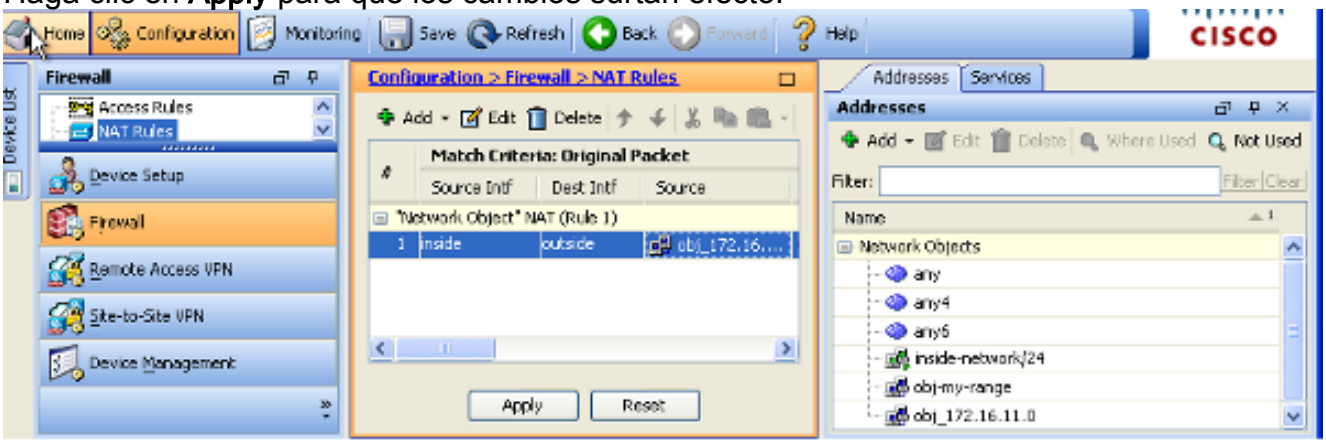
4. Haga clic en **Aceptar** para agregar la regla NAT. Haga clic en **Advanced** para seleccionar las interfaces de origen y destino.



5. En las listas desplegables Interfaz de origen e Interfaz de destino, elija las interfaces apropiadas. Click OK.



6. Haga clic en **Apply** para que los cambios surtan efecto.



Este es el resultado CLI equivalente para esta configuración ASDM:

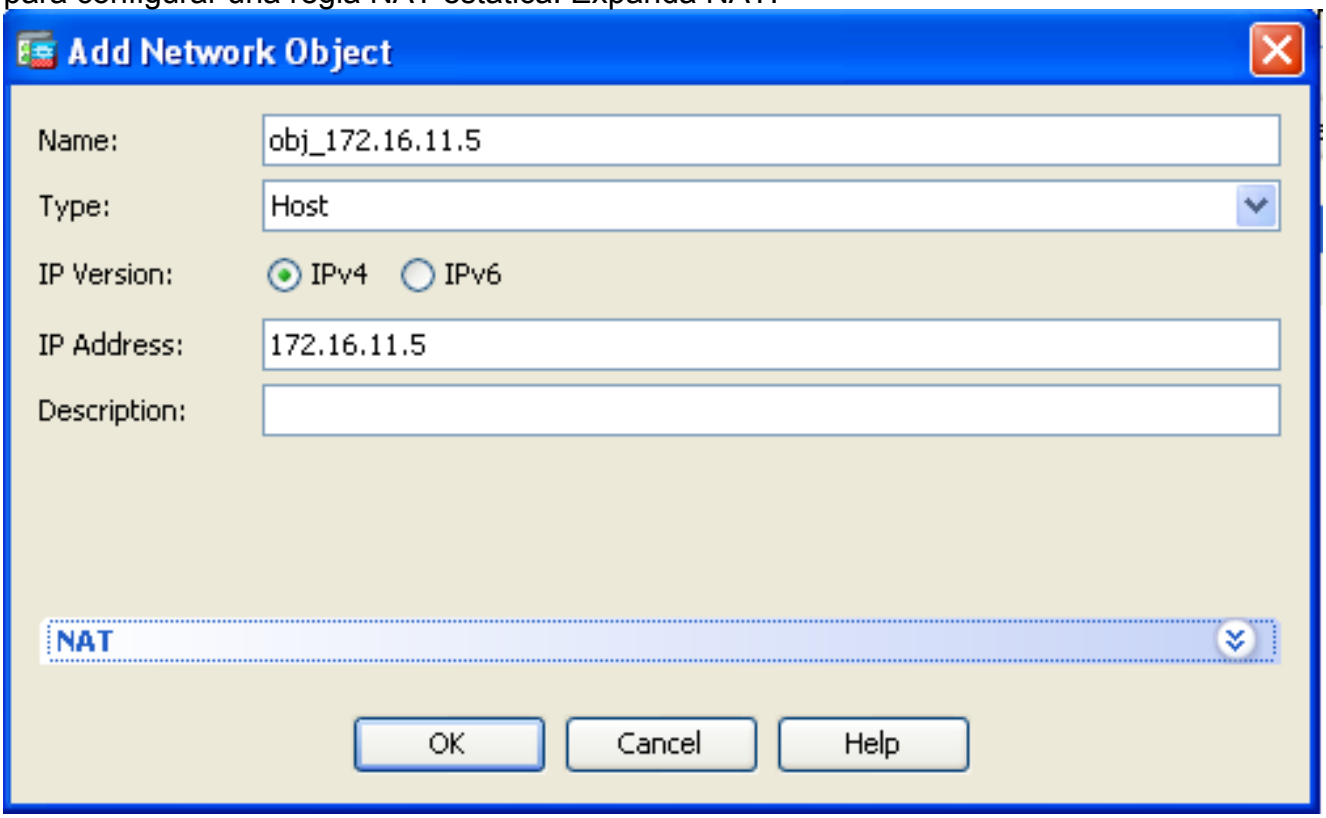
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

object network obj-pat-ip
host 203.0.113.21

object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

```
nat (inside,outside) dynamic nat-pat-group
```

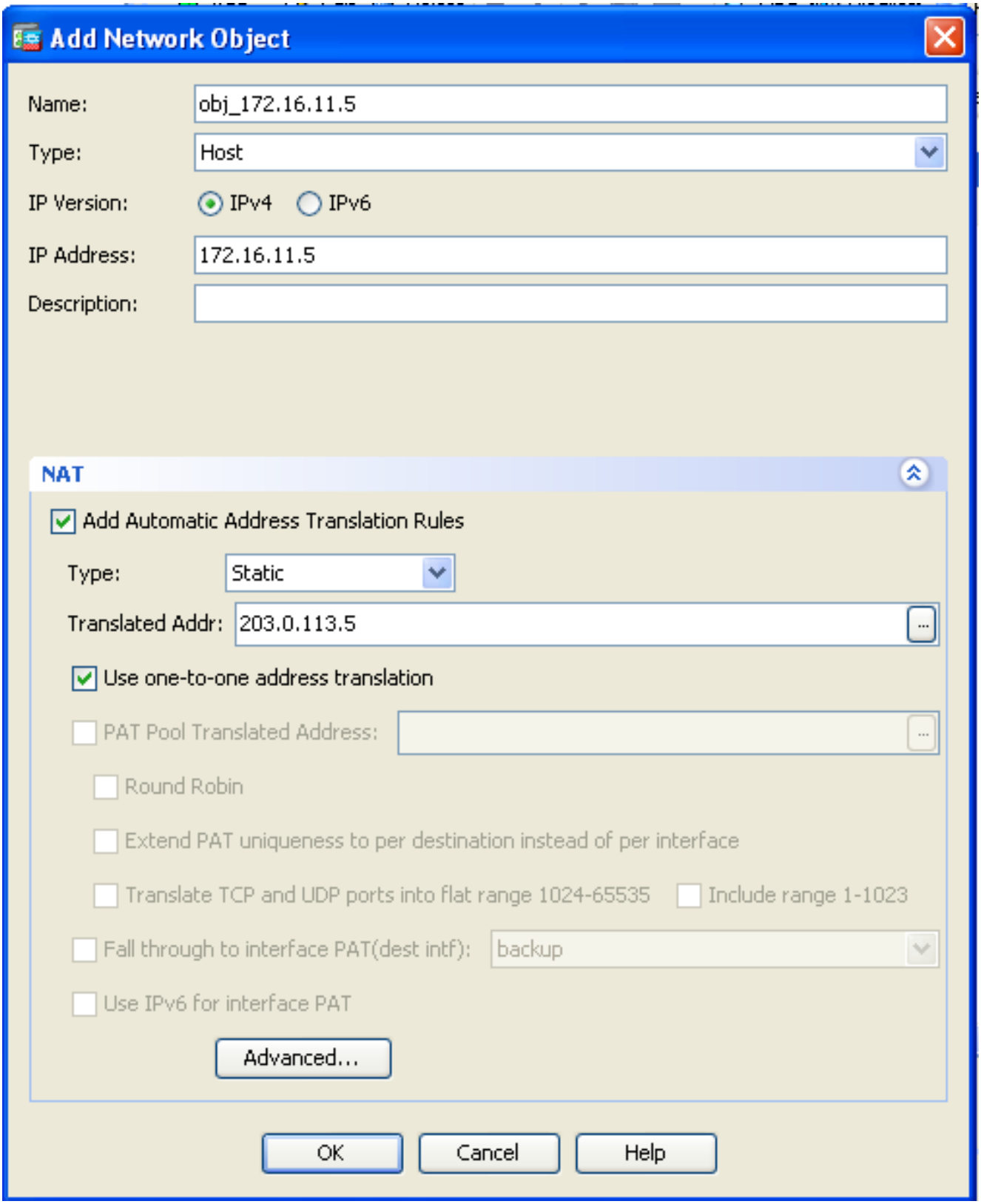
Permita el Acceso de los Hosts no Confiables a los Hosts de su Red de Confianza

Esto se puede lograr mediante la aplicación de una traducción NAT estática y una regla de acceso para permitir esos hosts. Debe configurarlo siempre que un usuario externo desee acceder a cualquier servidor que se encuentre en su red interna. El servidor de la red interna puede tener una dirección IP privada que no es enrutable en Internet. Como resultado, necesita traducir esa dirección IP privada a una dirección IP pública a través de una regla NAT estática. Suponga que tiene un servidor interno (172.16.11.5). Para que esto funcione, debe traducir esta dirección IP del servidor privado a una dirección IP pública. Este ejemplo describe cómo implementar la NAT estática bidireccional para traducir 172.16.11.5 a 203.0.113.5.

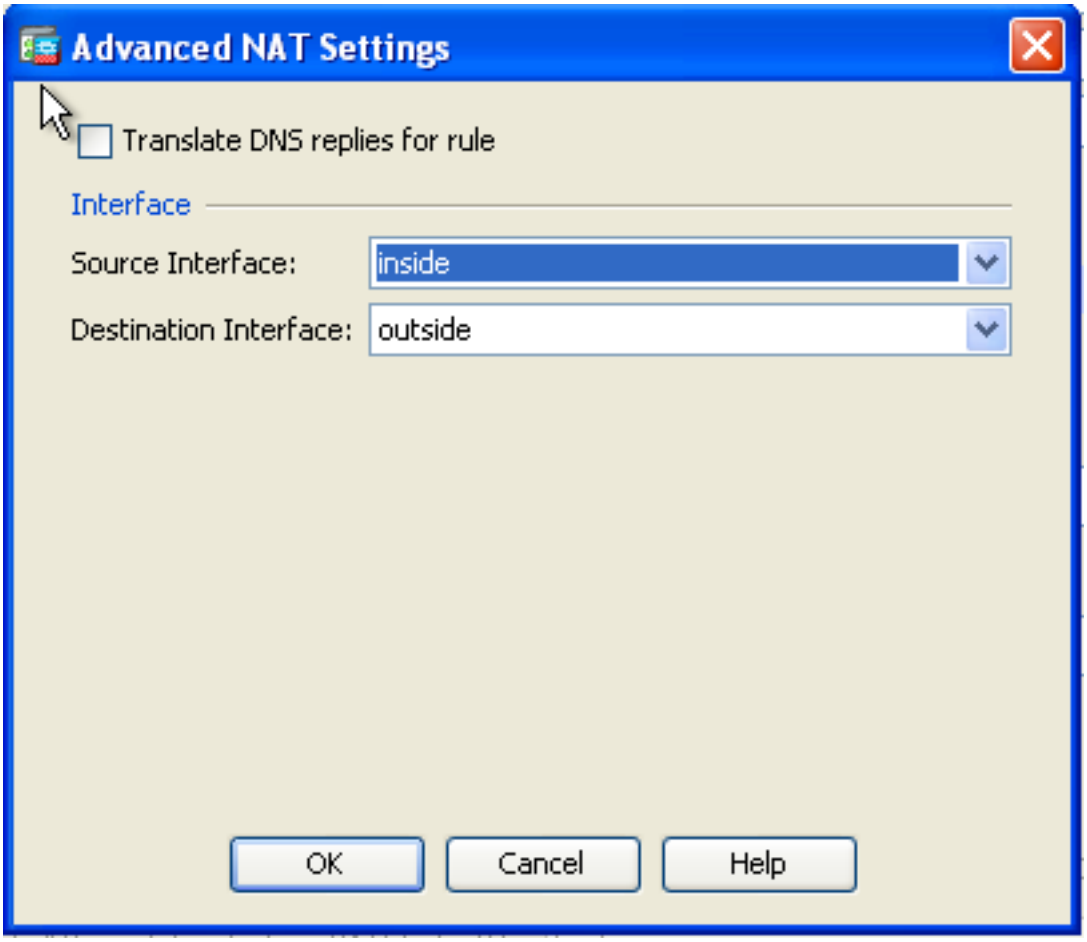
1. Elija **Configuration > Firewall > NAT Rules**. Haga clic en **Add** y luego elija **Network Object** para configurar una regla NAT estática. Expanda NAT.



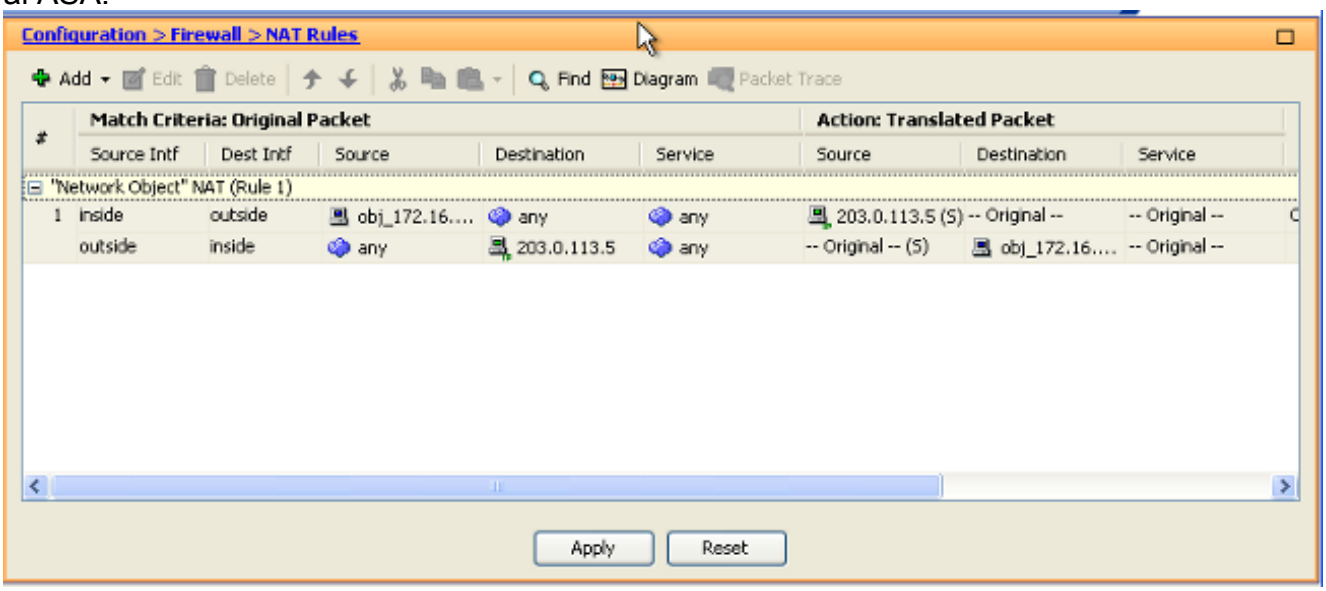
2. Marque la casilla de verificación **Agregar reglas de traducción automática de direcciones**. En la lista desplegable Tipo, seleccione **Estático.** En el campo Dirección traducida, introduzca la dirección IP. Haga clic en **Advanced** para seleccionar las interfaces de origen y destino.



3. En las listas desplegables Interfaz de origen e Interfaz de destino, elija las interfaces apropiadas. Click OK.



4. Puede ver la entrada de NAT estática configurada aquí. Haga clic en **Apply** para enviar esto al ASA.



Este es el resultado CLI equivalente para esta configuración NAT:

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

Identidad estática NAT

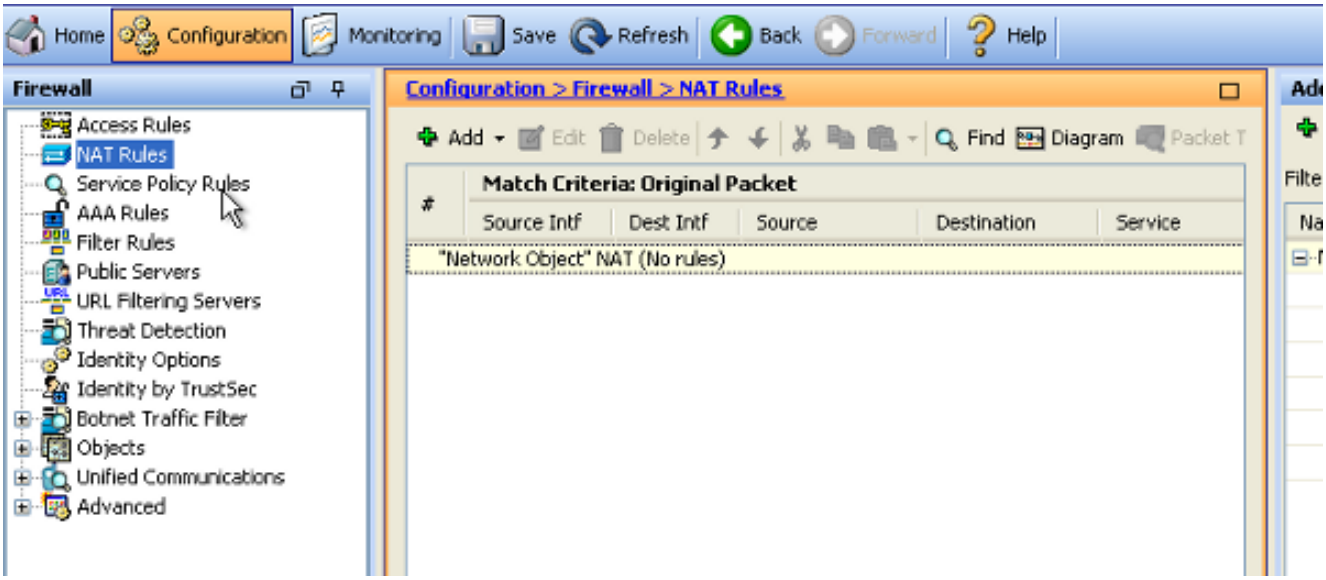
La exención de NAT es una función útil en la que los usuarios internos intentan acceder a un host/servidor VPN remoto o a algún host/servidor alojado detrás de cualquier otra interfaz del ASA

sin completar una NAT. Para lograr esto, el servidor interno, que tiene una dirección IP privada, puede ser la identidad traducida a sí mismo y que a su vez se le permite acceder al destino que realiza una NAT.

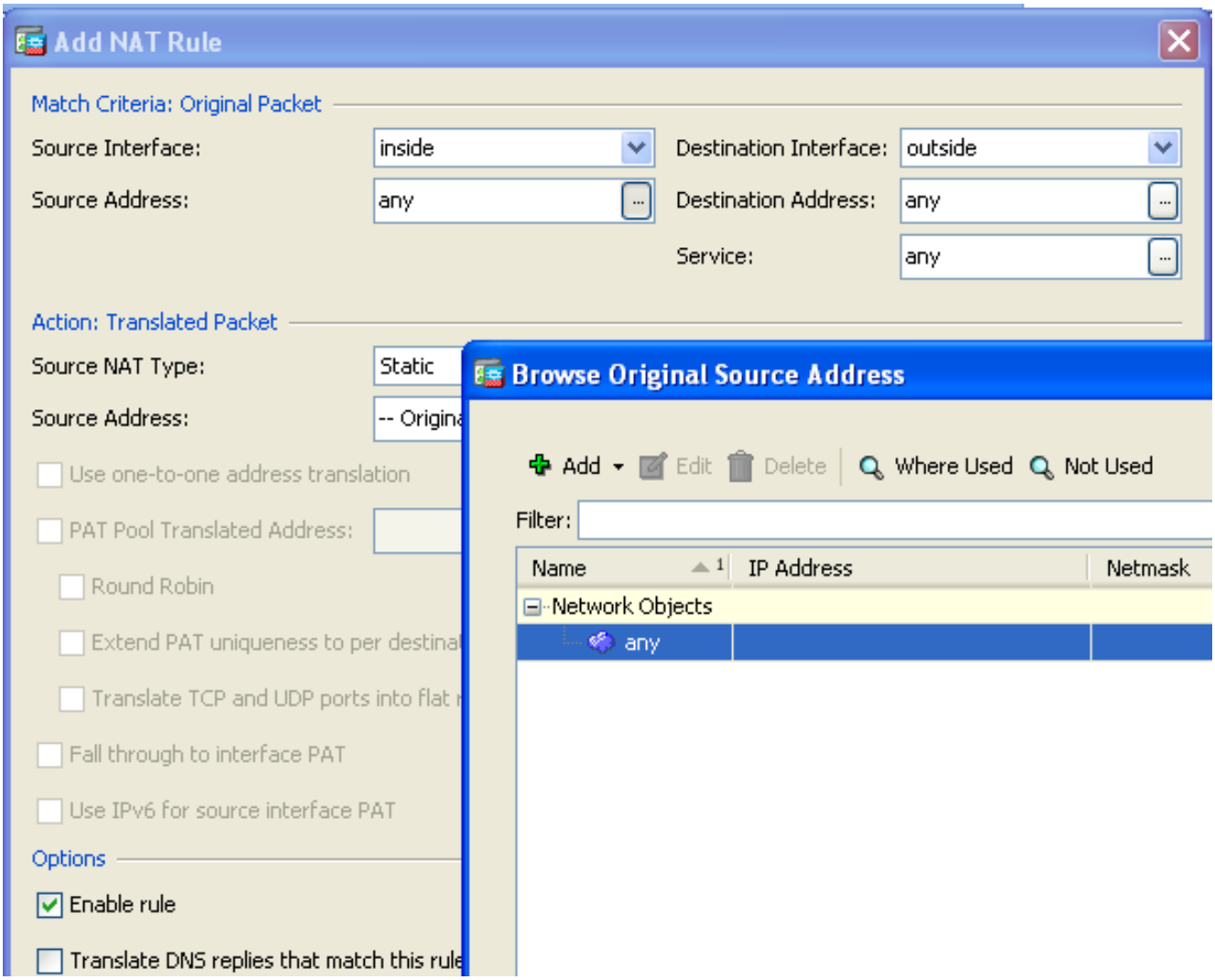
En este ejemplo, el host interno 172.16.11.15 necesita acceder al servidor VPN remoto 172.20.21.15.

Complete estos pasos para permitir el acceso de los hosts internos a la red VPN remota con la terminación de una NAT:

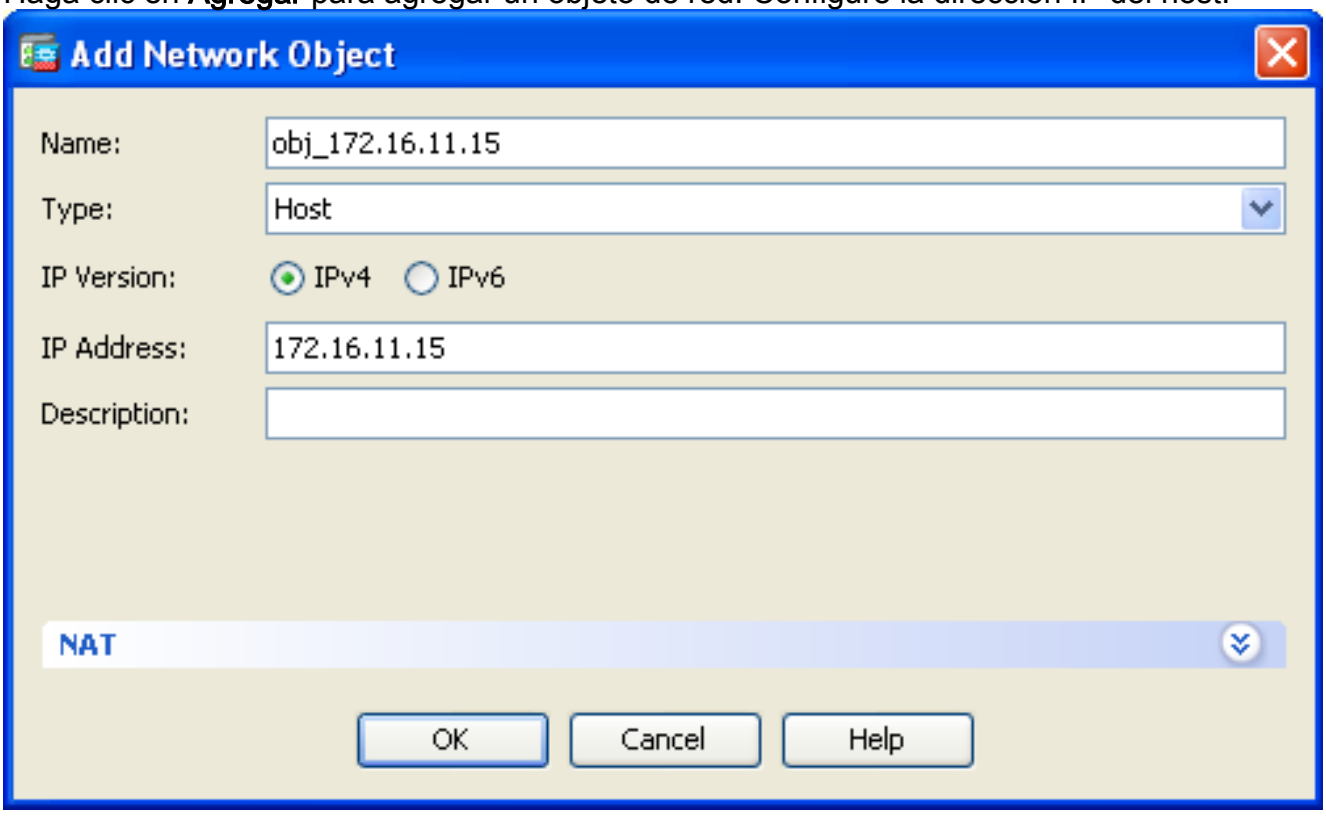
1. Elija **Configuration > Firewall > NAT Rules**. Haga clic en **Agregar** para configurar una regla de exención de NAT.



2. En las listas desplegables Interfaz de origen e Interfaz de destino, elija las interfaces apropiadas. En el campo Dirección de Origen, elija la entrada correspondiente.

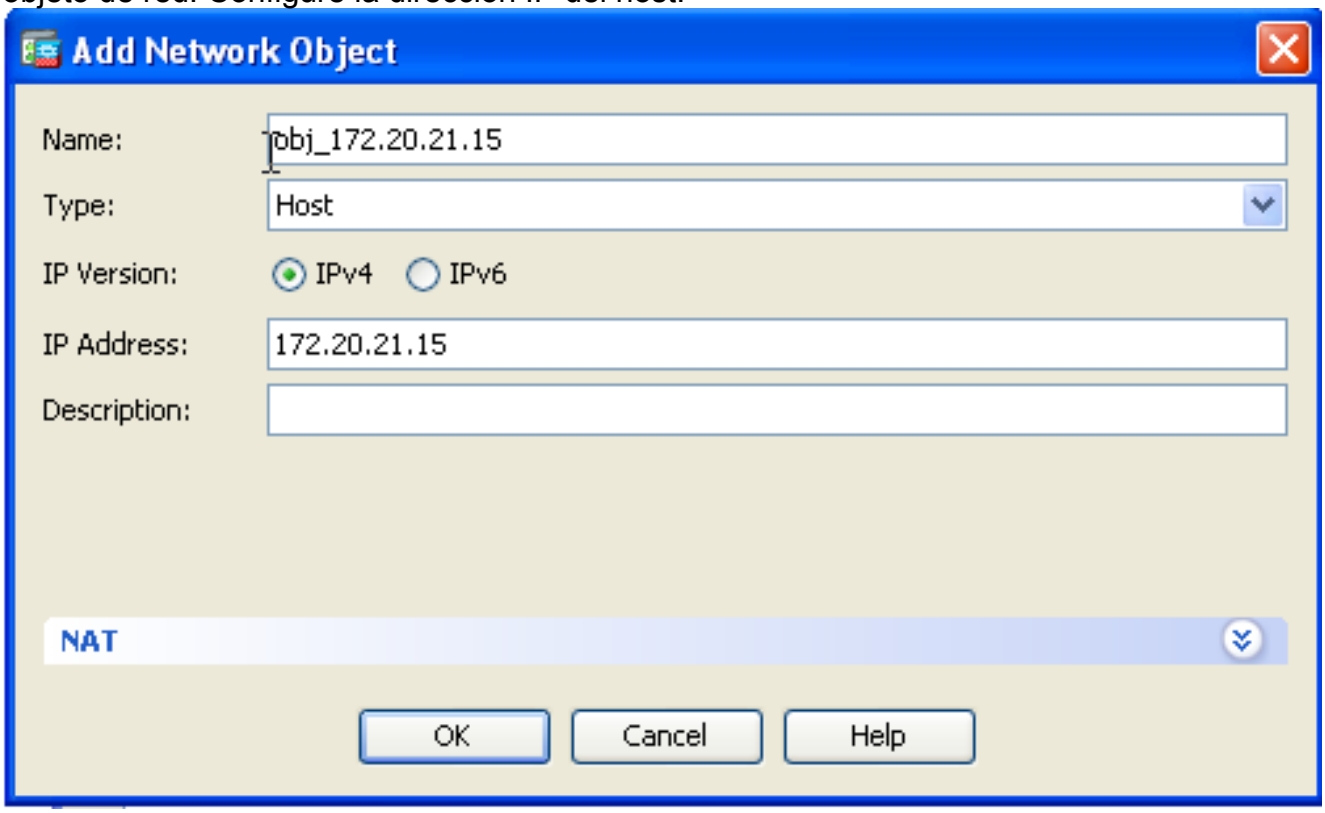


3. Haga clic en **Agregar** para agregar un objeto de red. Configure la dirección IP del host.

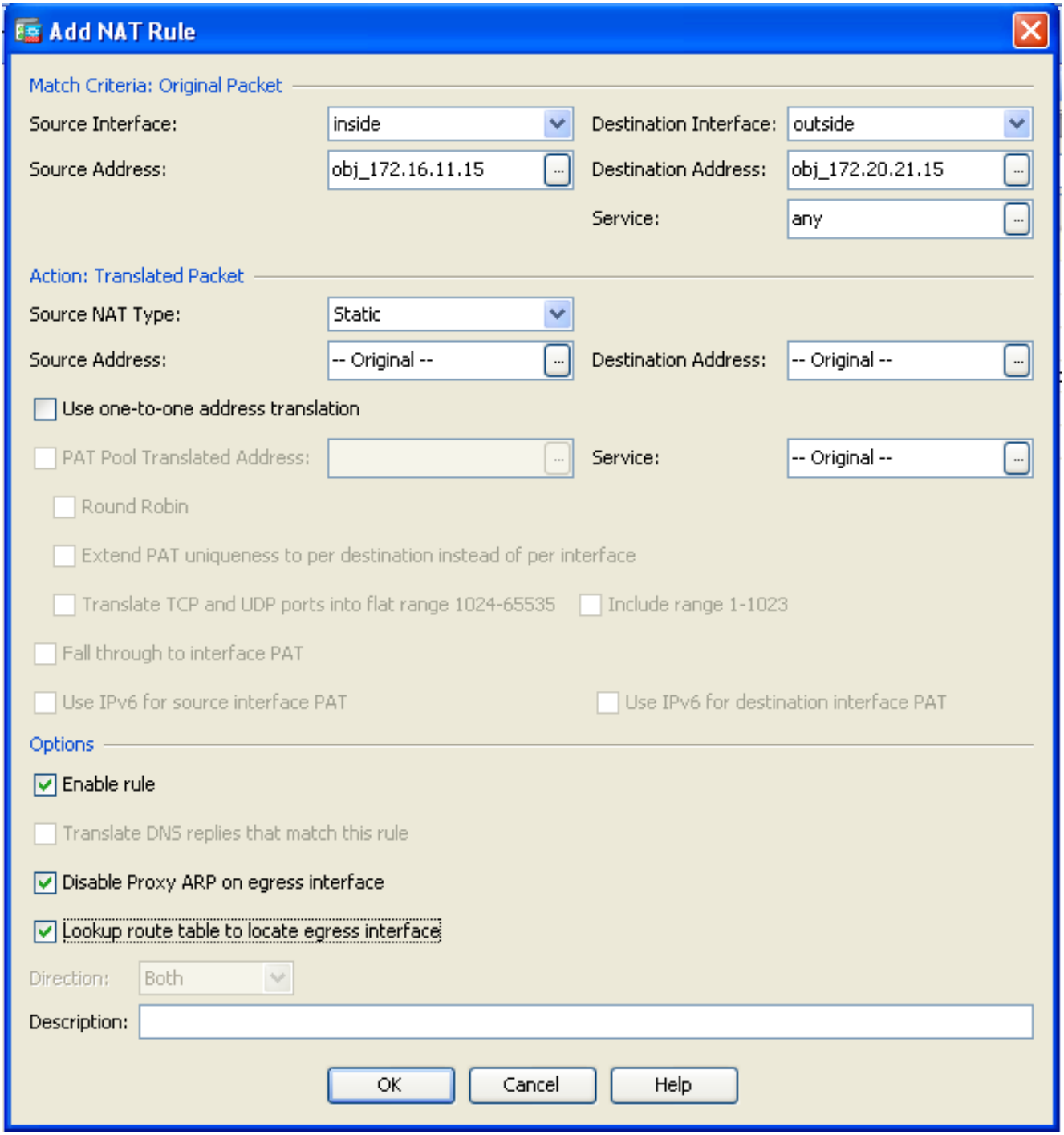


4. De manera similar, busque la **dirección de destino**. Haga clic en **Agregar** para agregar un

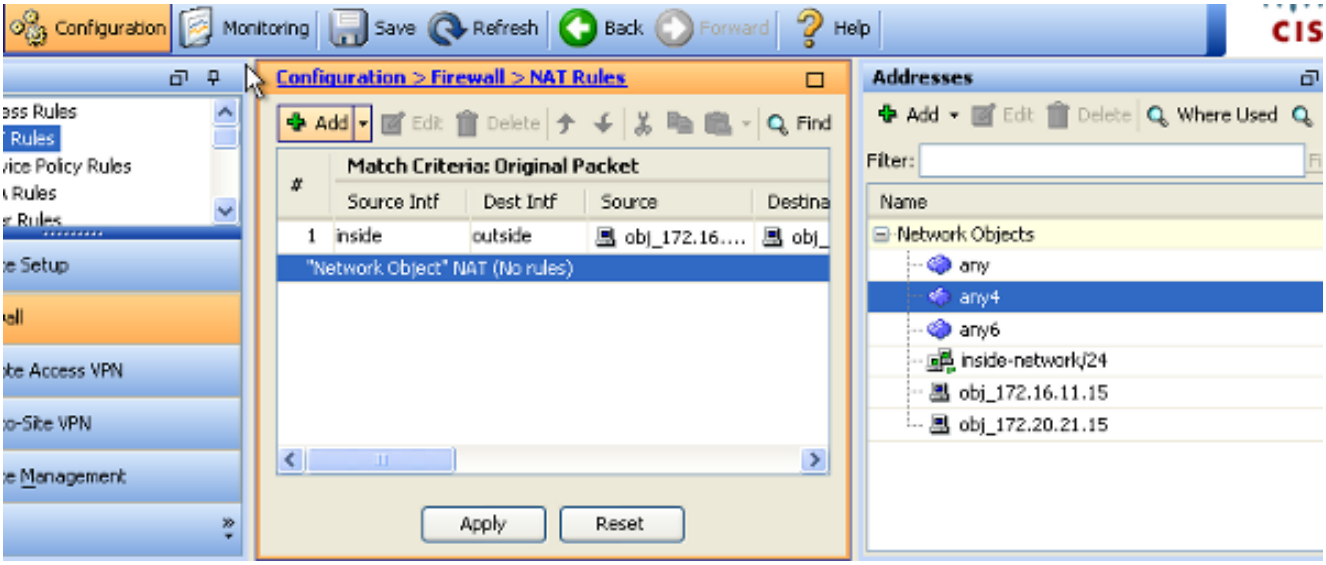
objeto de red. Configure la dirección IP del host.



5. Elija los objetos Dirección de origen y Dirección de destino configurados. Marque las casillas de verificación **Disable Proxy ARP on egress interface** y **Lookup route table to locate egress interface**. Click OK.



6. Haga clic en **Apply** para que los cambios surtan efecto.



Ésta es la salida CLI equivalente para la configuración NAT Exenta de NAT o NAT de identidad:

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15

nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

Redirección de puertos (reenvío) con estática

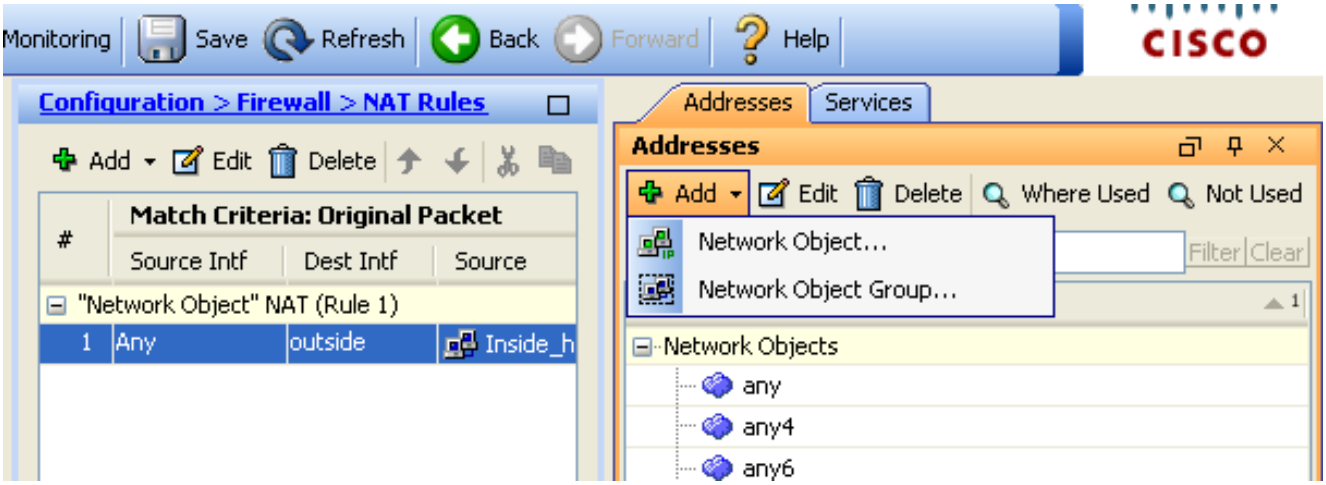
El reenvío de puertos o la redirección de puertos es una función útil en la que los usuarios externos intentan acceder a un servidor interno en un puerto específico. Para lograr esto, el servidor interno, que tiene una dirección IP privada, se puede traducir a una dirección IP pública que, a su vez, tiene permiso de acceso para el puerto específico.

En este ejemplo, el usuario externo desea acceder al servidor SMTP, 203.0.113.15 en el puerto 25. Esto se logra en dos pasos:

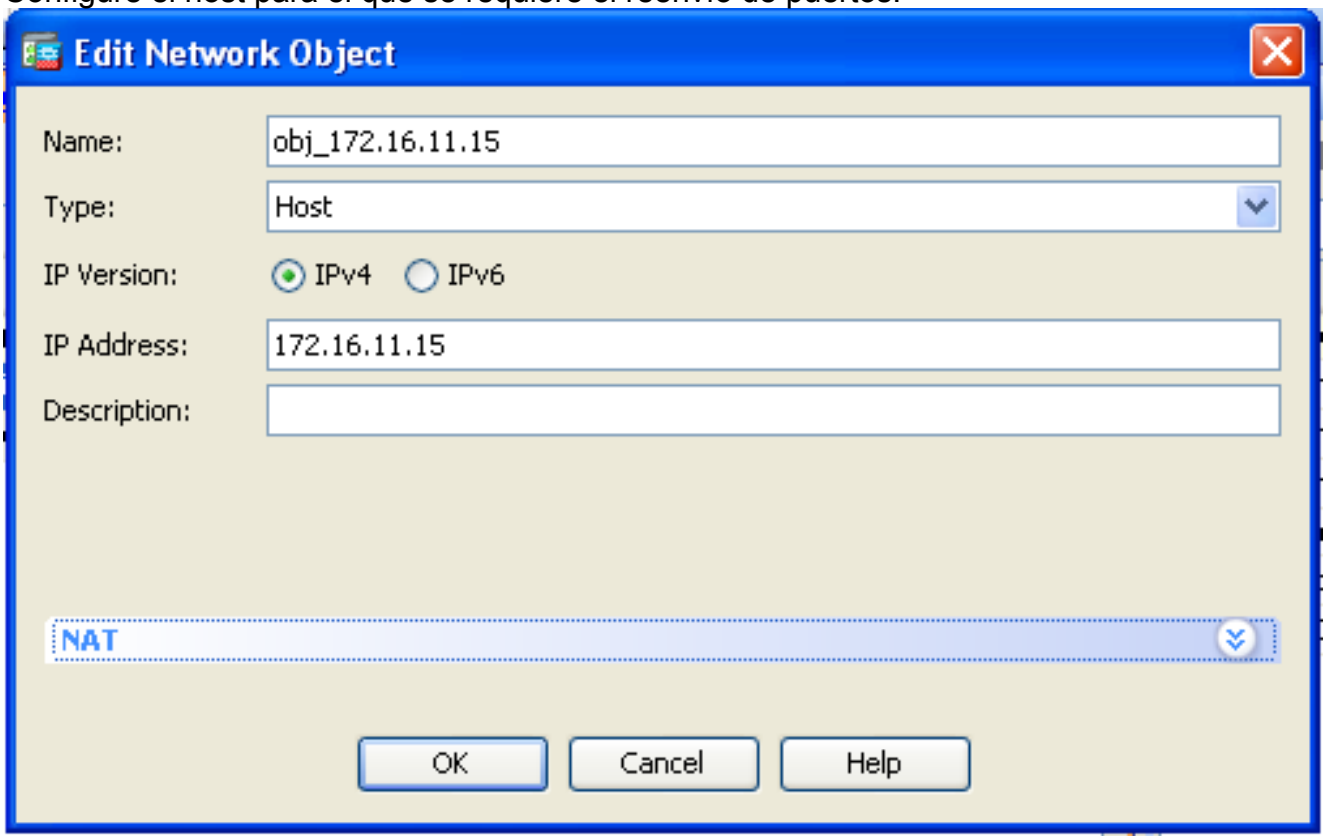
1. Traduzca el servidor de correo interno, 172.16.11.15 en el puerto 25, a la dirección IP pública, 203.0.113.15 en el puerto 25.
2. Permita el acceso al servidor de correo público, 203.0.113.15 en el puerto 25.

Cuando el usuario externo intenta acceder al servidor, 203.0.113.15 en el puerto 25, este tráfico se redirige al servidor de correo interno, 172.16.11.15 en el puerto 25.

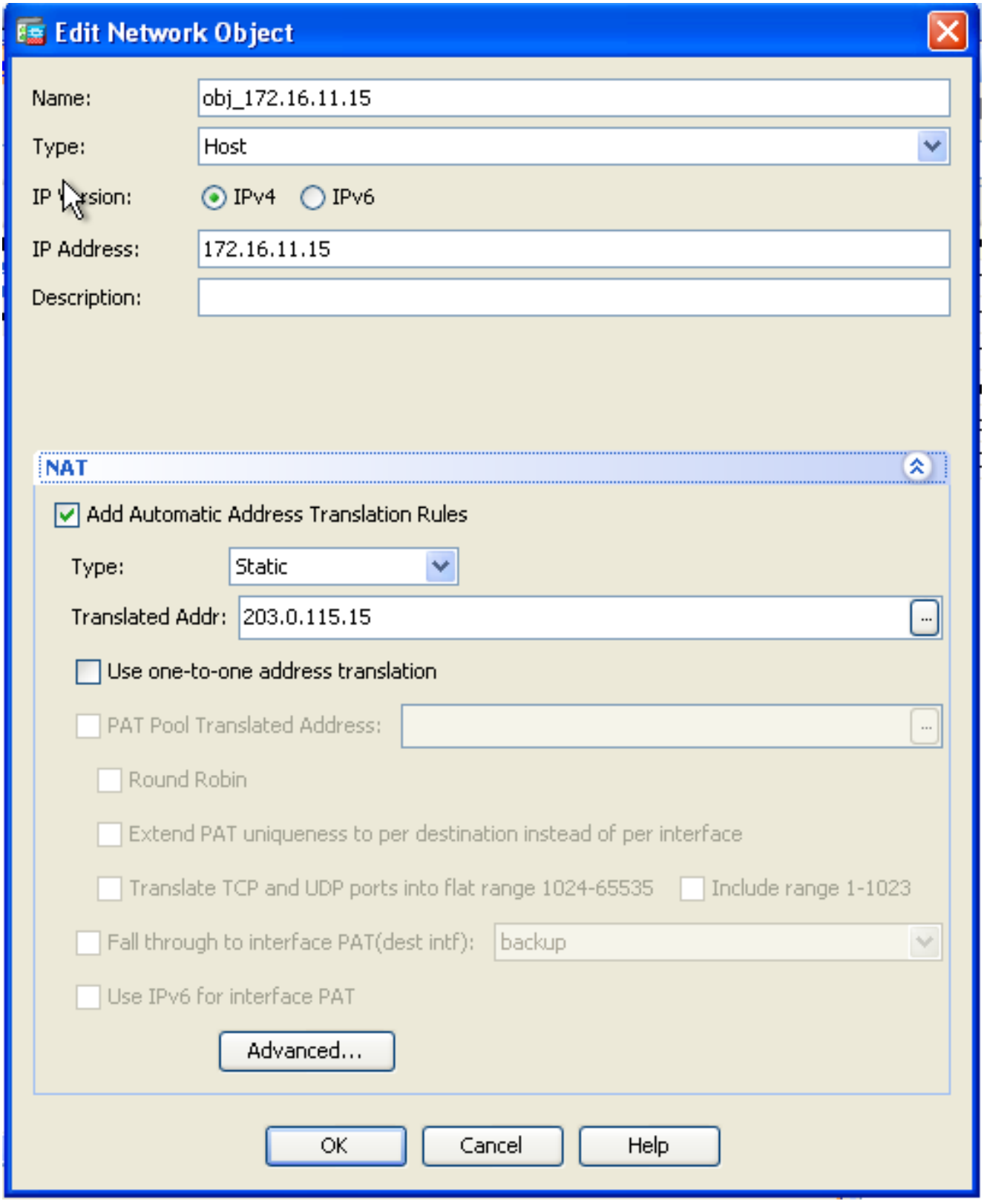
1. Elija **Configuration > Firewall > NAT Rules**. Haga clic en **Add** y luego elija **Network Object** para configurar una regla NAT estática.



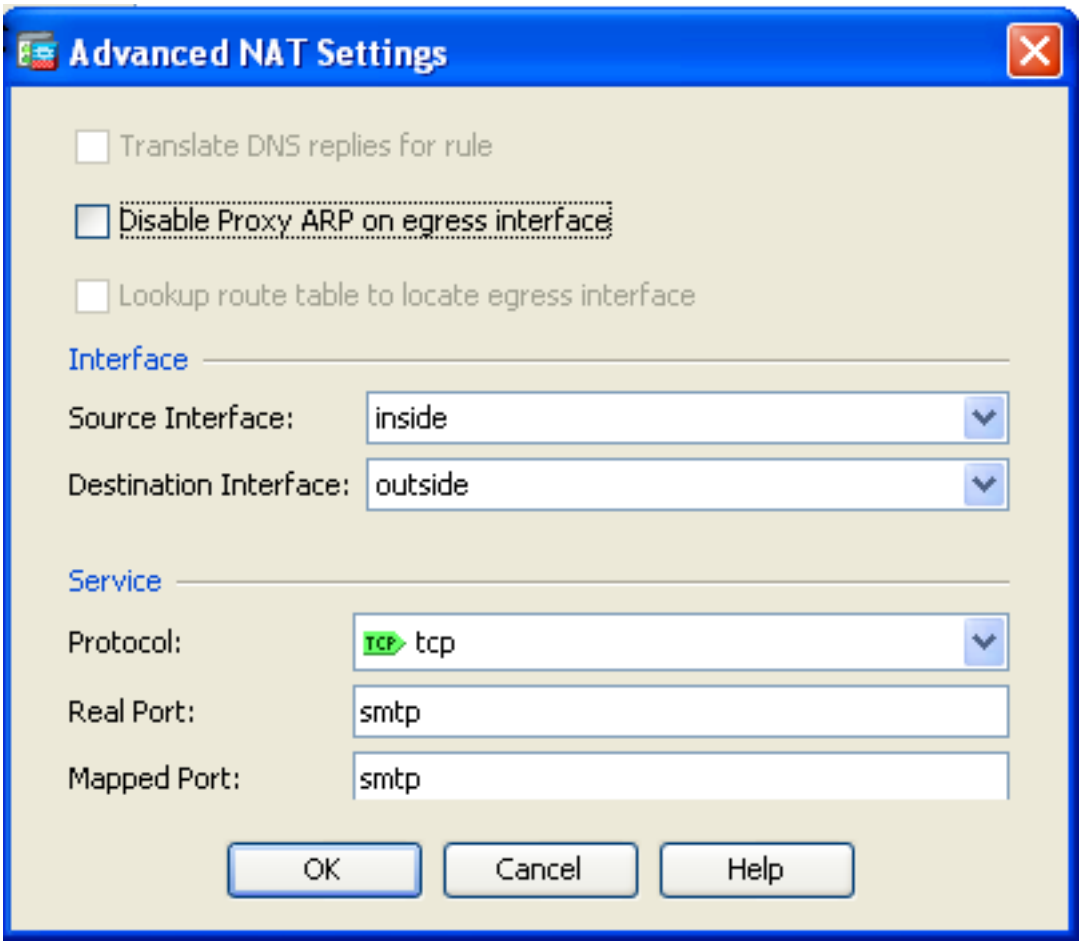
2. Configure el host para el que se requiere el reenvío de puertos.



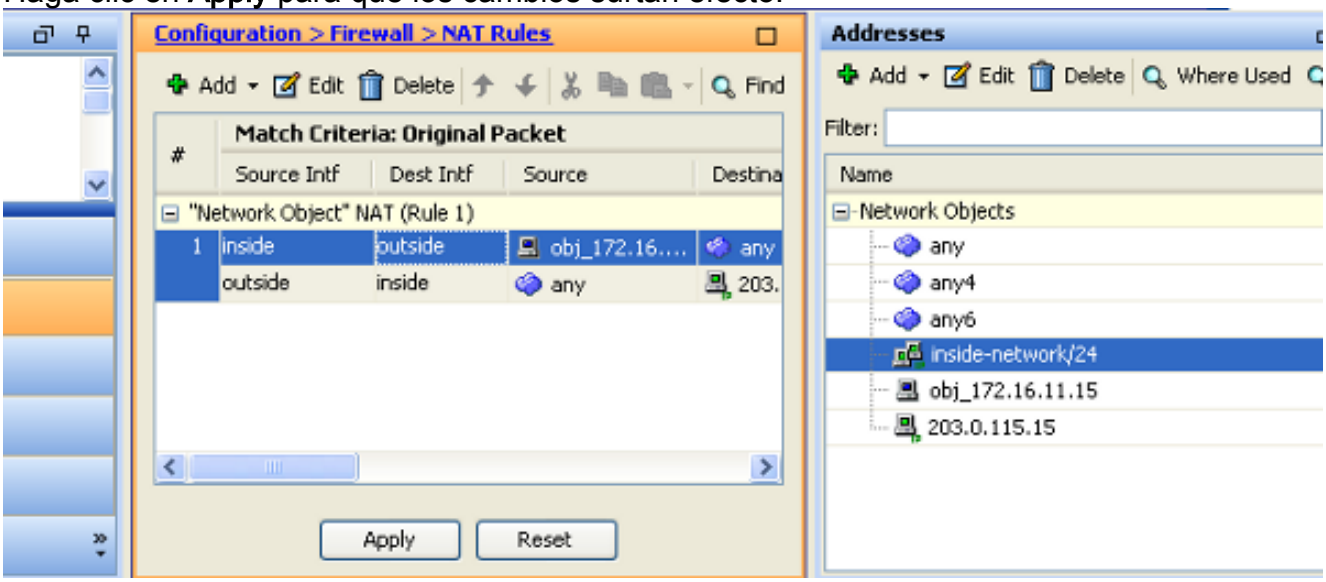
3. Expanda NAT. Marque la casilla de verificación **Agregar reglas de traducción automática de direcciones**. En la lista desplegable Tipo, elija **Estático**. En el campo Dirección traducida, introduzca la dirección IP. Haga clic en **Advanced** para seleccionar el servicio y las interfaces de origen y destino.



4. En las listas desplegables Interfaz de origen e Interfaz de destino, elija las interfaces apropiadas. Configure el servicio. Click OK.



5. Haga clic en **Apply** para que los cambios surtan efecto.



Este es el resultado CLI equivalente para esta configuración NAT:

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show.

Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

Acceder a un sitio Web a través de HTTP con un explorador Web. En este ejemplo se utiliza un sitio alojado en 198.51.100.100. Si la conexión es correcta, este resultado se puede ver en la CLI de ASA.

Conexión

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA es un firewall con estado y se permite el tráfico de retorno del servidor web a través del firewall porque coincide con una ***conexión de*** la tabla de conexiones del firewall. El tráfico que coincide con una conexión preexistente se permite a través del firewall sin ser bloqueado por una 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. Puede encontrar más información sobre los indicadores de conexión en Indicadores de conexión TCP de ASA.

Syslog

```
ASA(config)# show log | in 172.16.11.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 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:172.16.11.5/58799 (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 syslogs que se ven en el nivel seis, o el nivel 'informativo'.

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

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 inhibió la creación de esta conexión (restricciones de recursos o un posible error de configuración), el firewall no generaría un registro que indique que la conexión fue construida. En su lugar, registraría un motivo para denegar la conexión o una indicación sobre el factor que impedía la creación de la conexión.

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 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 funcionalidad de rastreo de paquetes en ASA le permite especificar un paquete *simulado* y ver todos los diversos pasos, verificaciones y funciones por los que pasa el firewall cuando procesa el tráfico. Con esta herramienta, es útil identificar un ejemplo de tráfico que cree que se *puede* permitir que pase a través del firewall, y utilizar ese 5-tupla para simular 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 al interior.
- El protocolo utilizado es TCP.
- La dirección IP del cliente simulado es 172.16.11.5.
- El cliente envía tráfico originado 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 realiza mediante el diseño del trazador 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. Puede encontrar más información sobre Packet Tracer en Rastreo de Paquetes con Packet Tracer.

Captura

Aplicar captura

```
ASA# capture capin interface inside match tcp host 172.16.11.5 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 172.16.11.5.58799 > 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 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 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 ASA puede capturar el tráfico que entra o sale de sus interfaces. Esta función de captura es fantástica, ya que puede demostrar definitivamente si el tráfico llega o sale de un firewall. El ejemplo anterior mostró la configuración de dos capturas denominadas capin y capout en las interfaces interna y externa respectivamente. Los comandos capture utilizan la palabra clave match, que permite ser específico sobre el tráfico que desea capturar.

Para la captura**,** indicó que quería hacer coincidir el tráfico visto en la interfaz interna (ingreso o egreso) que coincide con el host TCP 172.16.11.5 host 198.51.100.100. En otras palabras, desea capturar cualquier tráfico TCP que se envíe desde el host 172.16.11.5 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 definido para la interfaz externa no hace referencia a la dirección IP del cliente interno porque el firewall conduce 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, debería 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 fue capaz de conectarse al servidor como lo demuestra el protocolo de enlace TCP de 3 vías que se ve en las capturas.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Ejemplo de configuración de Syslog de ASA
- Ejemplo de Configuración de Capturas de Paquetes ASA con CLI y ASDM
- 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).