Expedición del puerto de la Versión de ASA 9.x de la configuración con el NAT

Contenido

Introducción

Este documento explica cómo configurar la redirección de puerto (expedición) y las características de la traducción (NAT) de la dirección de red externa en la versión de software adaptante 9.x del dispositivo de seguridad (ASA), con el uso del CLI o del Administrador de dispositivos de seguridad adaptante (ASDM).

Refiera a la guía de Configuración de ASDM del Firewall de la serie de Cisco ASA para la información adicional.

Prerrequisitos

Requisitos

Refiera a configurar el Acceso de 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

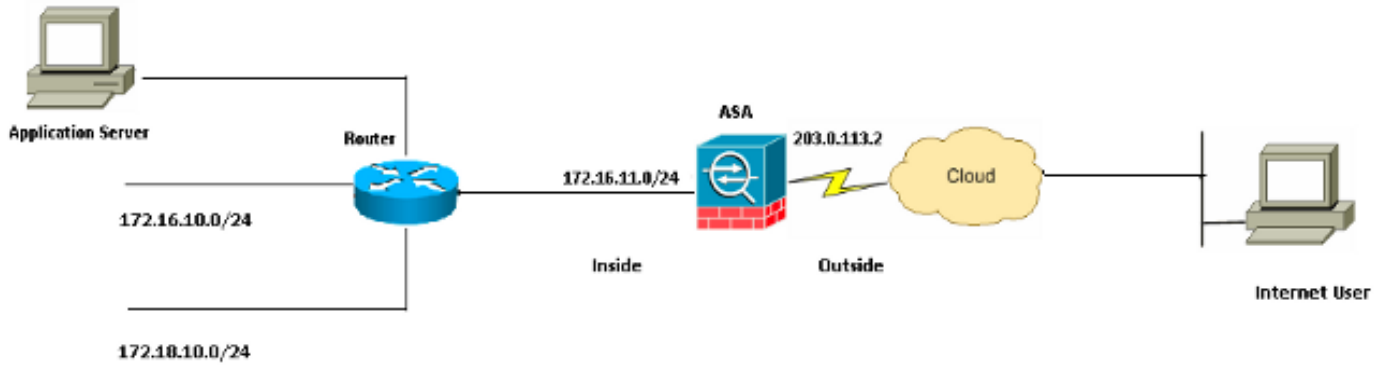
hardware.

- Versión de software 9.x del dispositivo de seguridad de las 5525 Series de Cisco ASA y posterior
- Versión 7.x y posterior del ASDM

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Diagrama de la red



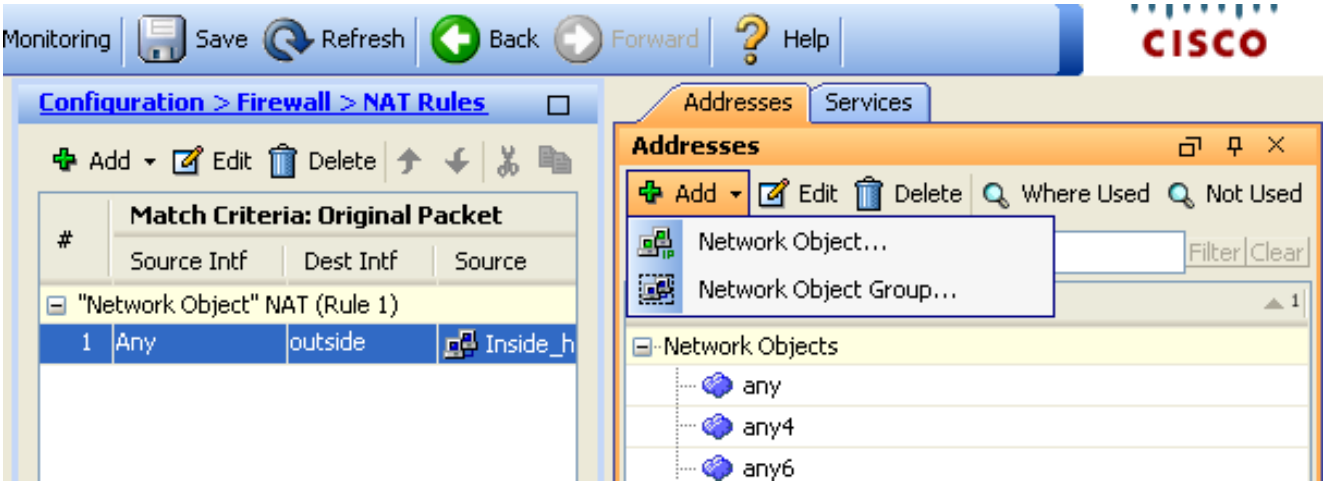
Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

No prohiba a host interiores el acceso a las redes externas con la PALMADITA

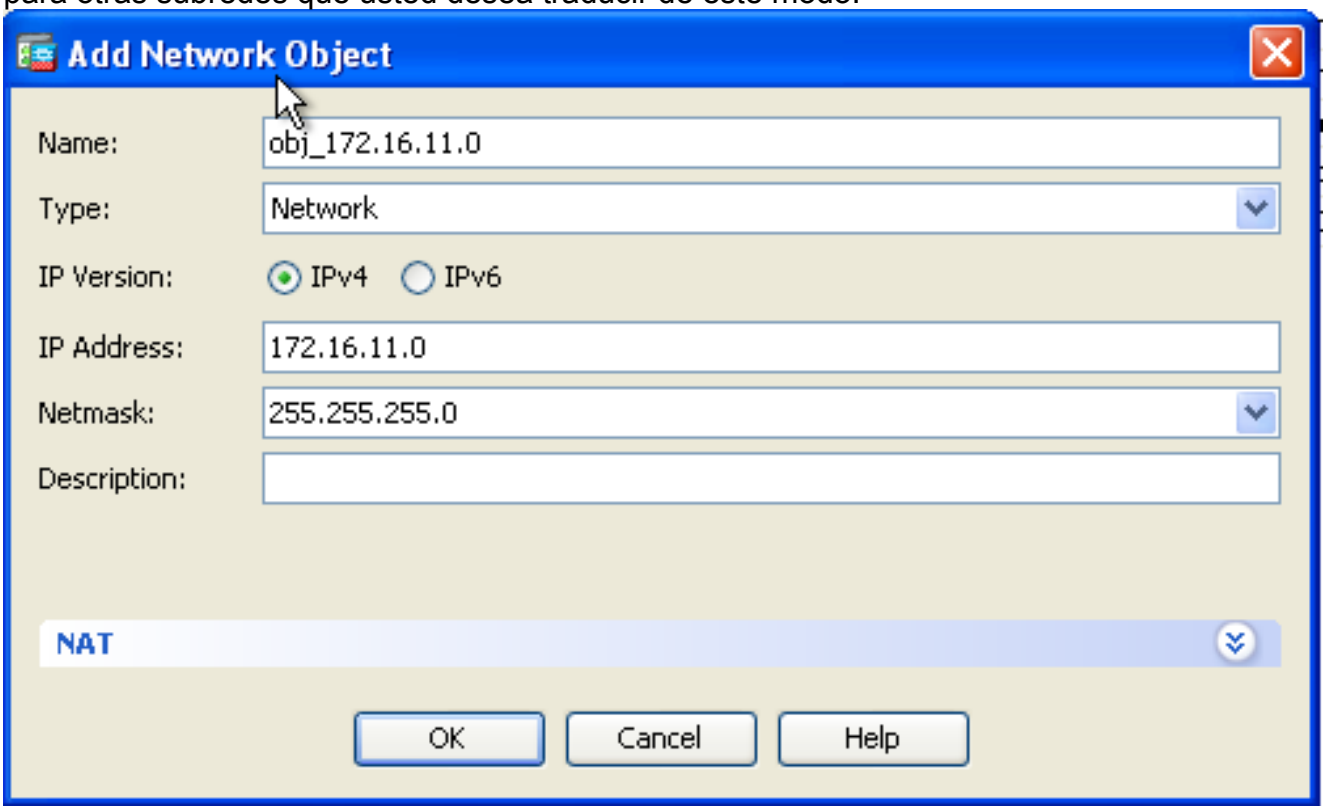
Si usted quisiera que los host interiores compartieran a una sola dirección pública para la traducción, utilice el Port Address Translation (PAT). Una de las configuraciones más simples de la PALMADITA implica la traducción de todos los host internos para parecer la dirección IP de la interfaz exterior. Ésta es la configuración típica de la PALMADITA se utiliza que cuando el número de IP Address ruteables disponible desde el ISP se limita solamente a algunos, o quizás apenas uno.

Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con la PALMADITA:

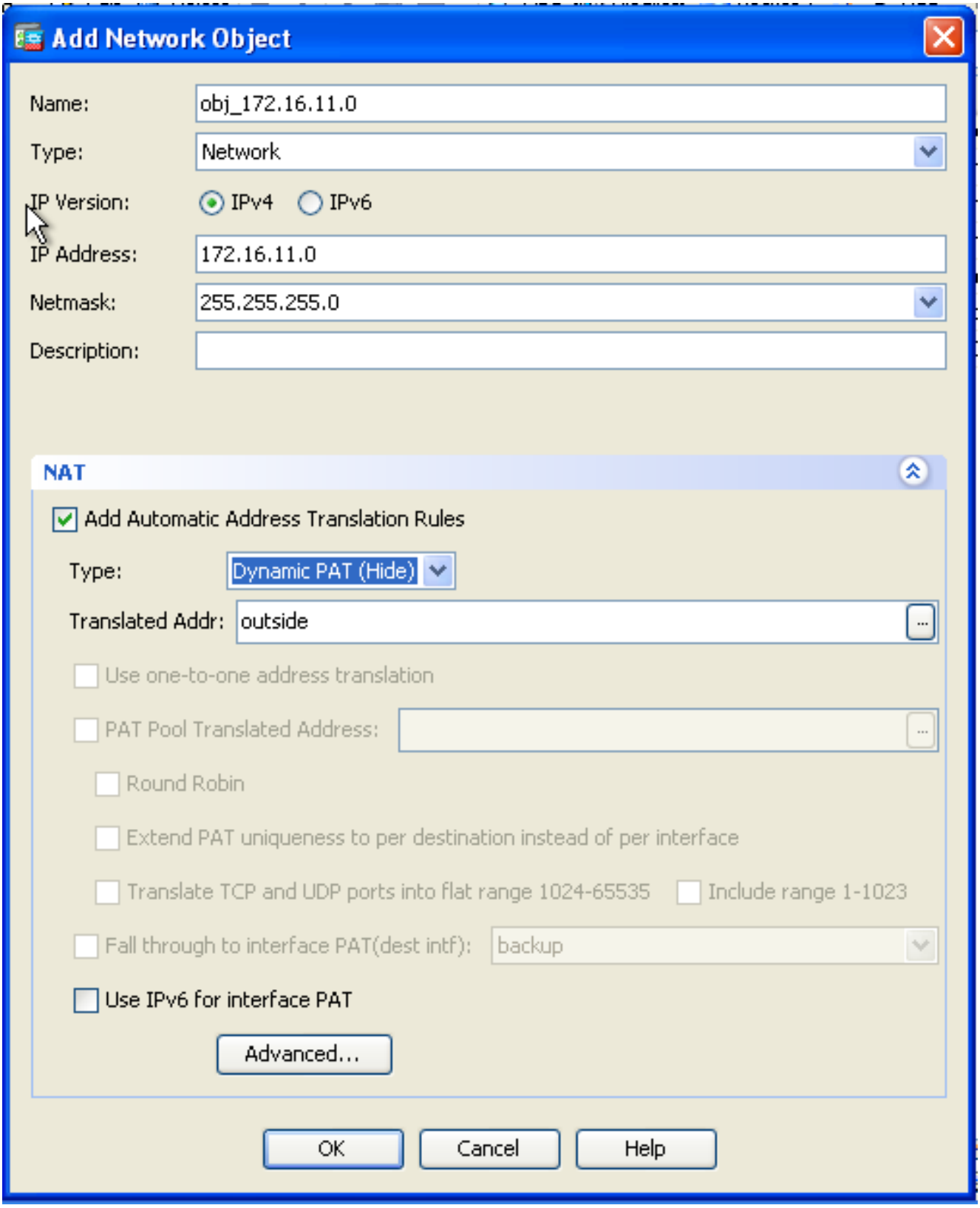
1. Elija la **configuración** > el **Firewall** > las **reglas NAT**. El tecleo **agrega** y después elige el **objeto de red** para configurar una regla dinámica NAT.



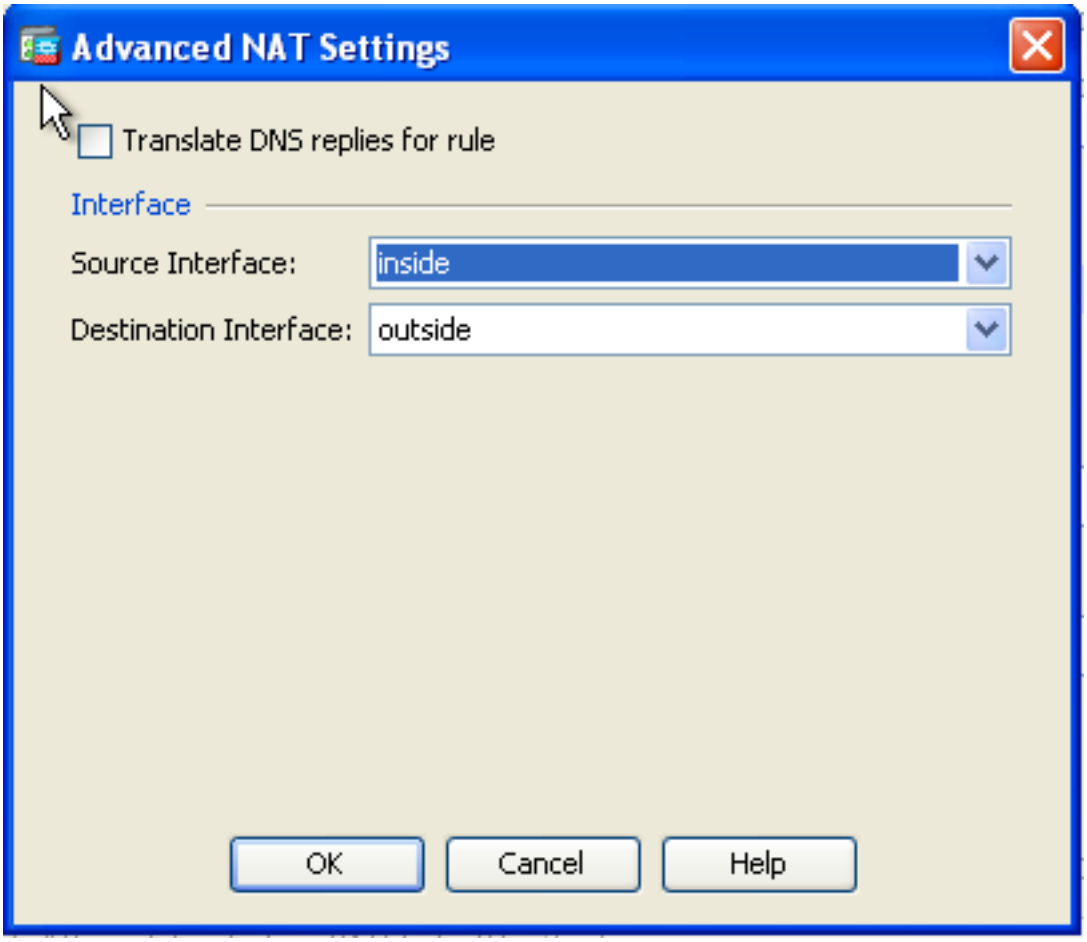
2. Configure la red/el host/el rango para el cual se requiere la **PALMADITA dinámica**. En este ejemplo, una de las subredes interiores se ha seleccionado. Este proceso se puede relanzar para otras subredes que usted desea traducir de este modo.



3. Amplíe el NAT. Marque la casilla de verificación **automática de las reglas de traducción de la dirección del agregar**. En la lista desplegable del tipo, elija la **PALMADITA dinámica (piel)**. En el campo **traducido del addr**, elija la opción para reflejar la interfaz exterior. Haga clic en **Advanced**.



4. En las listas desplegables de la interfaz de origen y de la interfaz de destino, elija las interfaces apropiadas. El Haga Click en OK y el tecleo **solicitan los** cambios para tomar el efecto.



Éste es el CLI equivalente hecho salir para esta configuración de la PALMADITA:

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

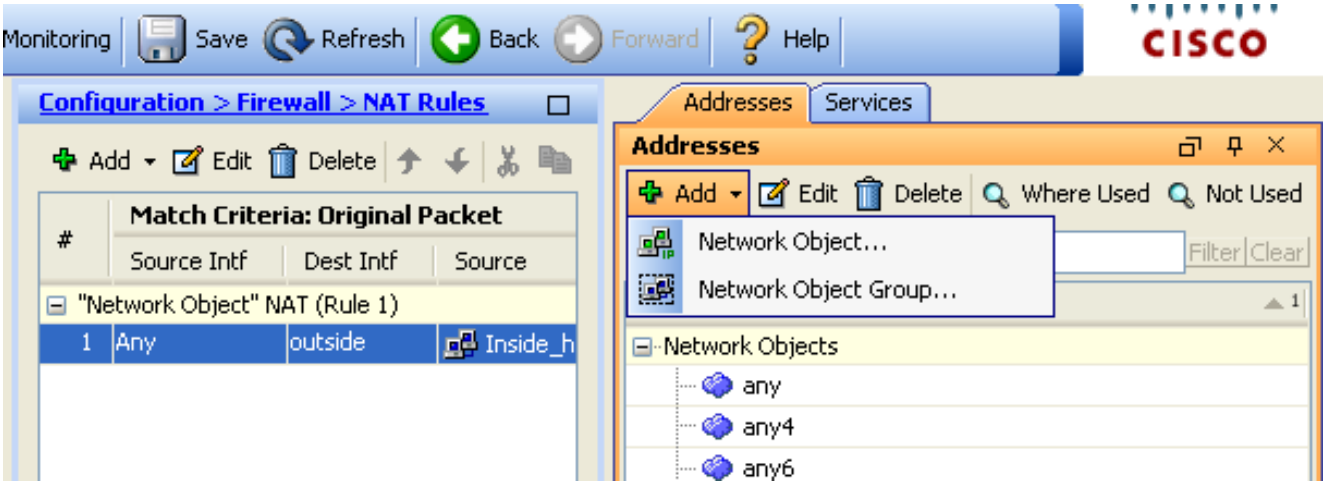
Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT

Usted podría permitir que un grupo de host interiores/de redes acceda el mundo exterior con la configuración de las reglas dinámicas NAT. A diferencia de la PALMADITA, el NAT dinámico afecta un aparato a las direcciones traducidas de una agrupación de direcciones. Como consecuencia, un host se asocia a su propia dirección IP traducida y dos host no pueden compartir la misma dirección IP traducida.

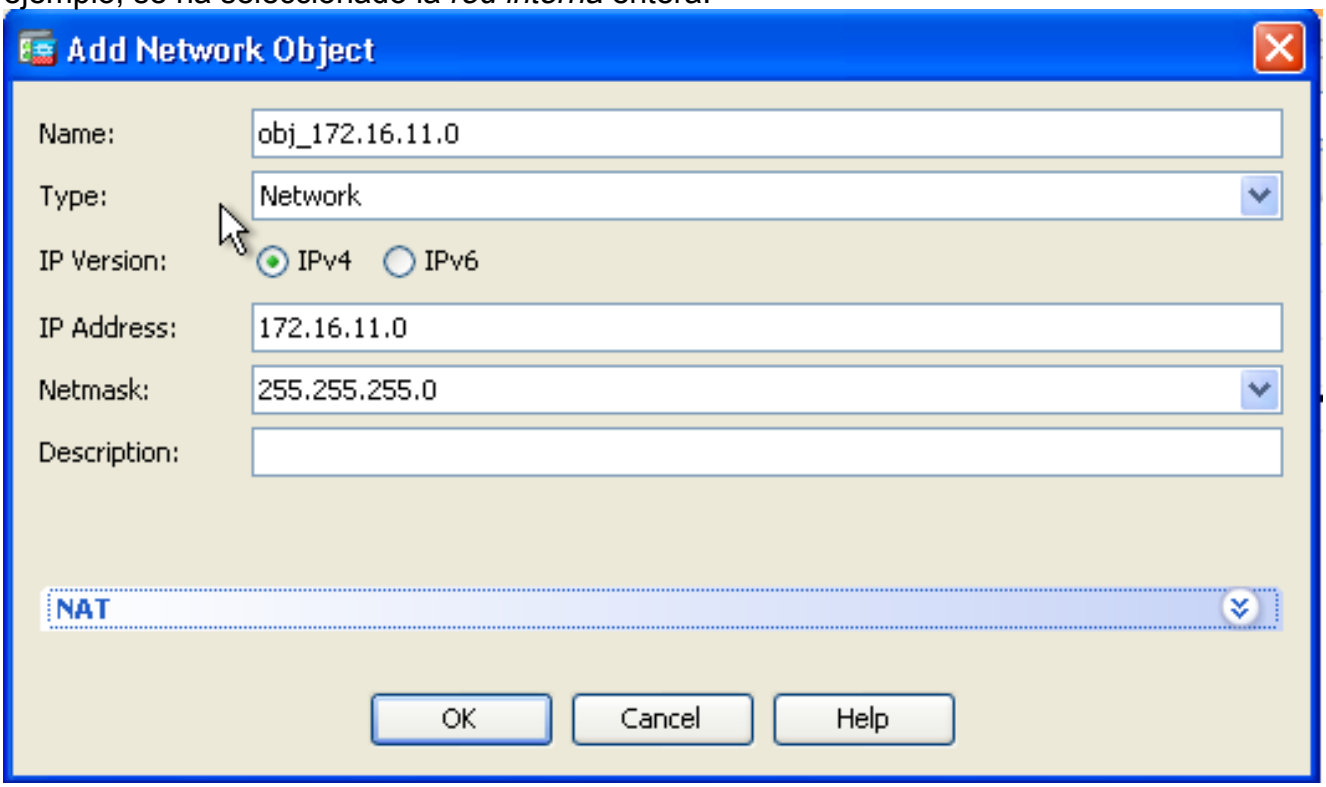
Para lograr esto, usted necesita seleccionar a la dirección real de los host/de las redes para ser dados el acceso y entonces tienen que ser asociados a un pool de los IP Addresses traducidos.

Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con el NAT:

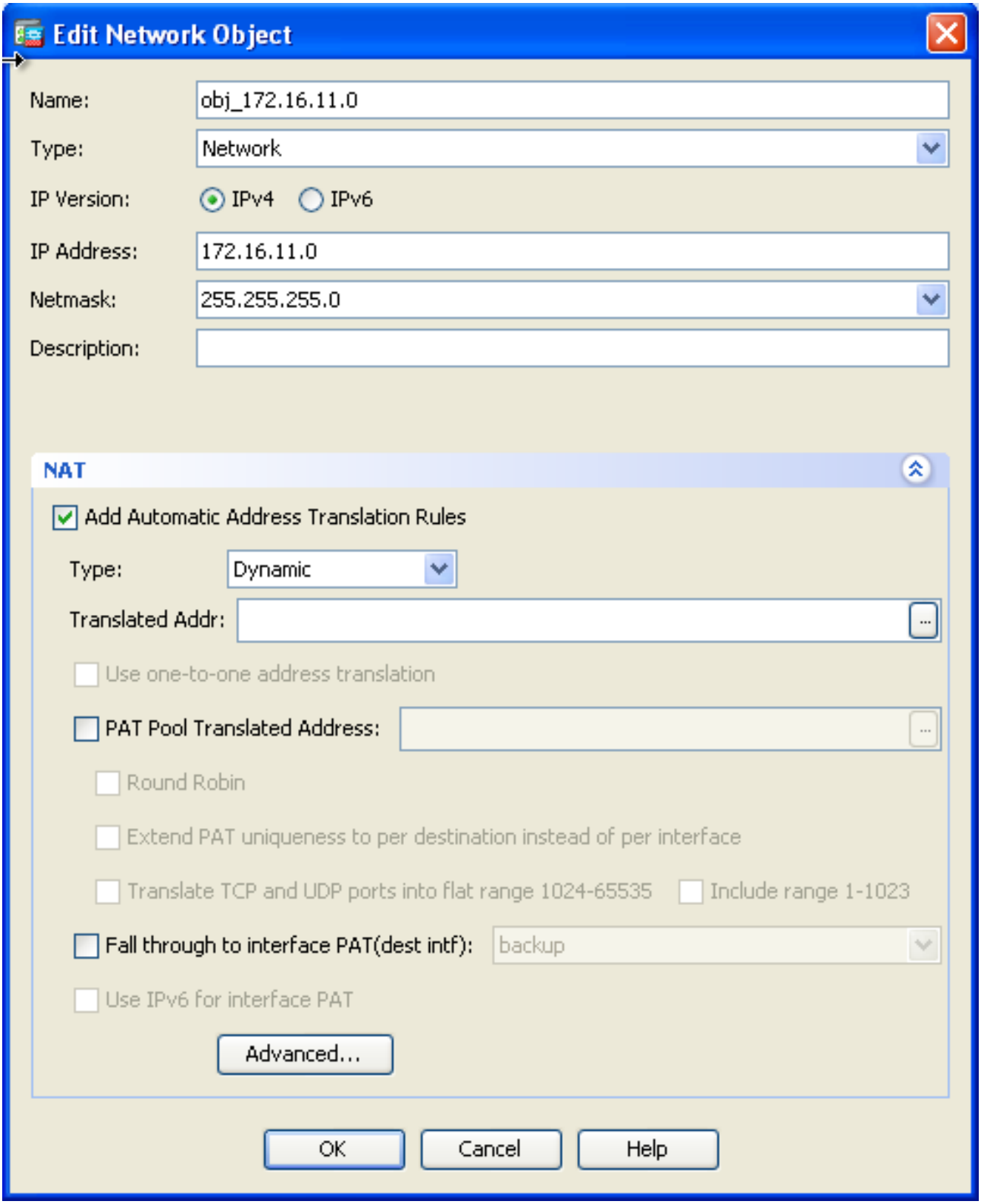
1. Elija la **configuración** > el **Firewall** > las **reglas NAT**. El tecleo **agrega** y después elige el **objeto de red** para configurar una regla dinámica NAT.



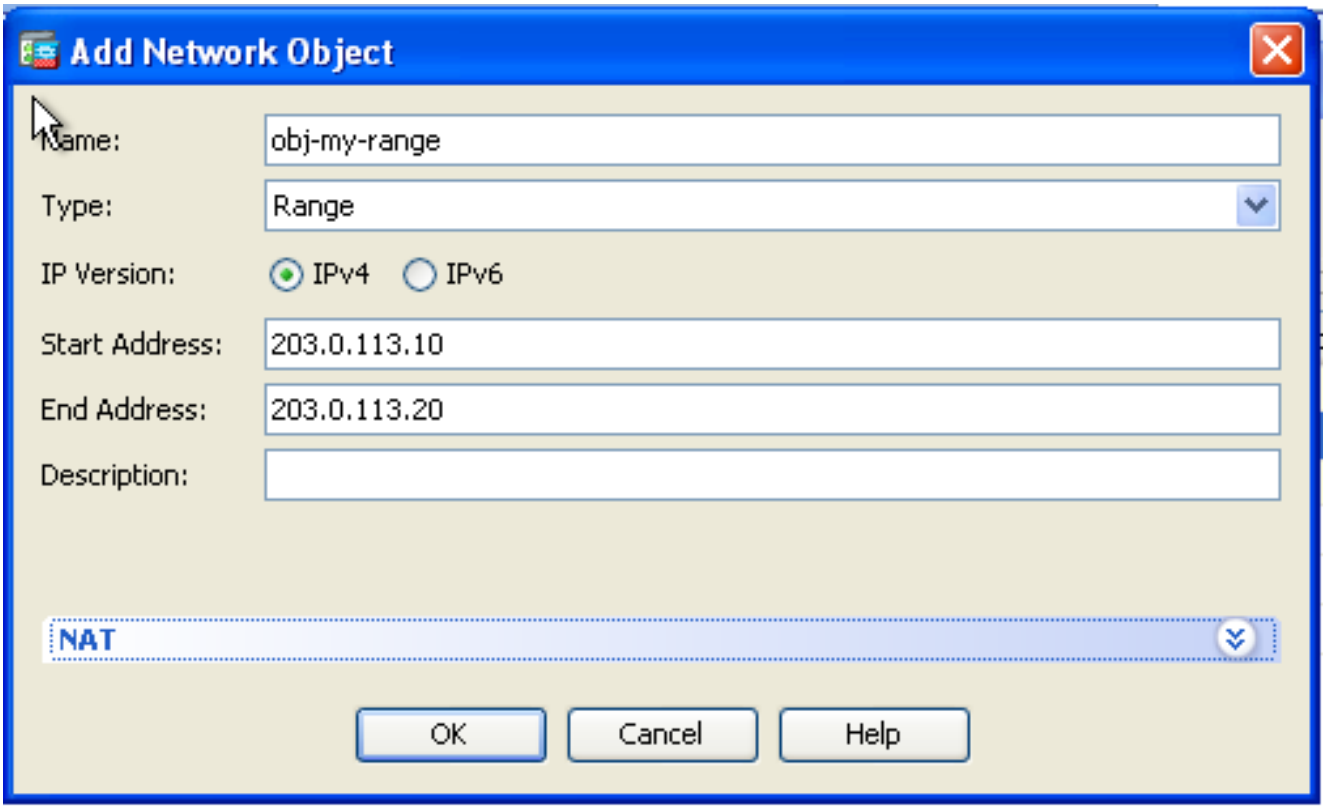
2. Configure la red/el host/el rango para el cual se requiere la PALMADITA dinámica. En este ejemplo, se ha seleccionado la *red interna* entera.



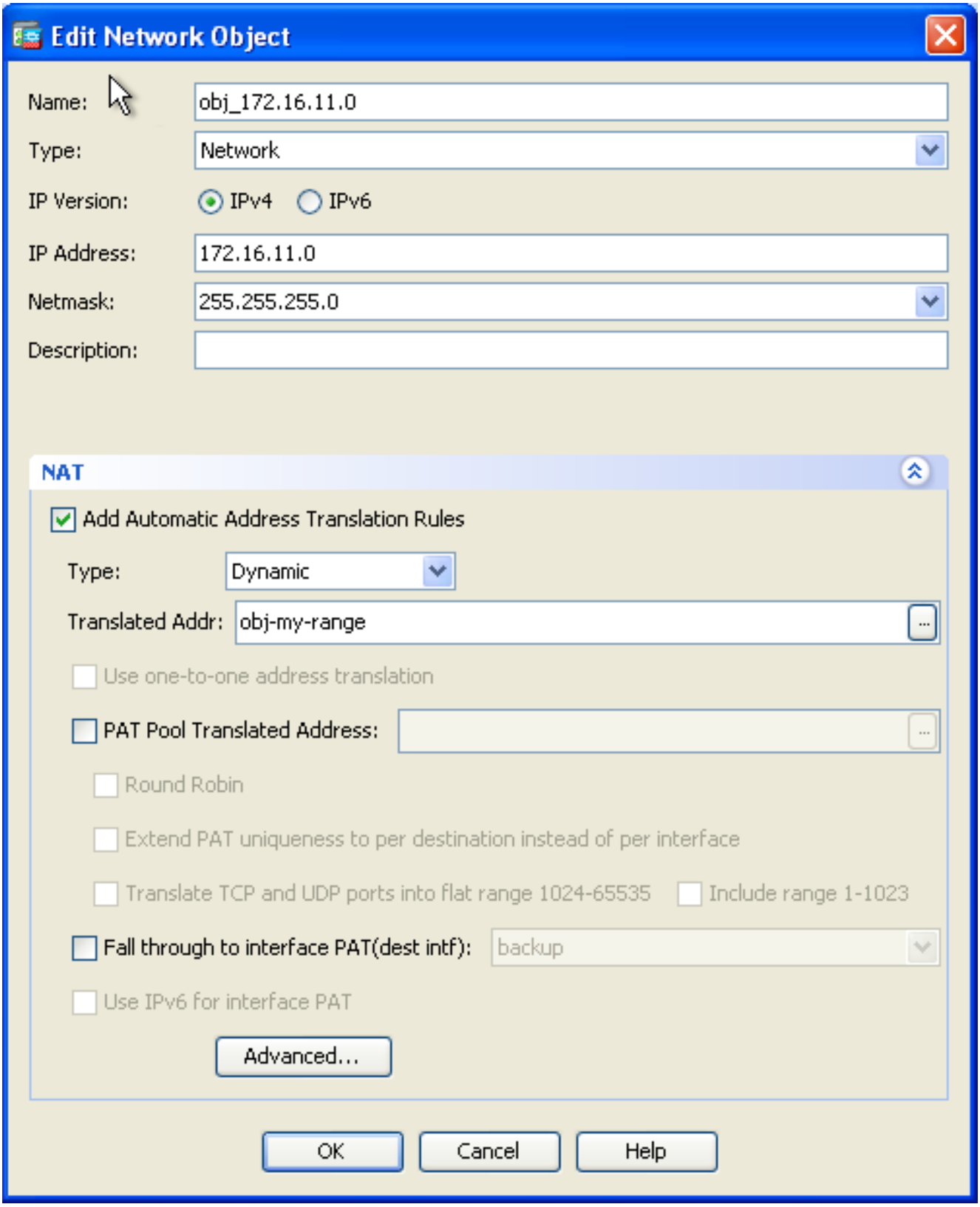
3. Amplíe el NAT. Marque la casilla de verificación **automática de las reglas de traducción de la dirección del agregar**. En la lista desplegable del tipo, elija **dinámico**. En el campo traducido del addr, elija la selección apropiada. Haga clic en **Advanced**.



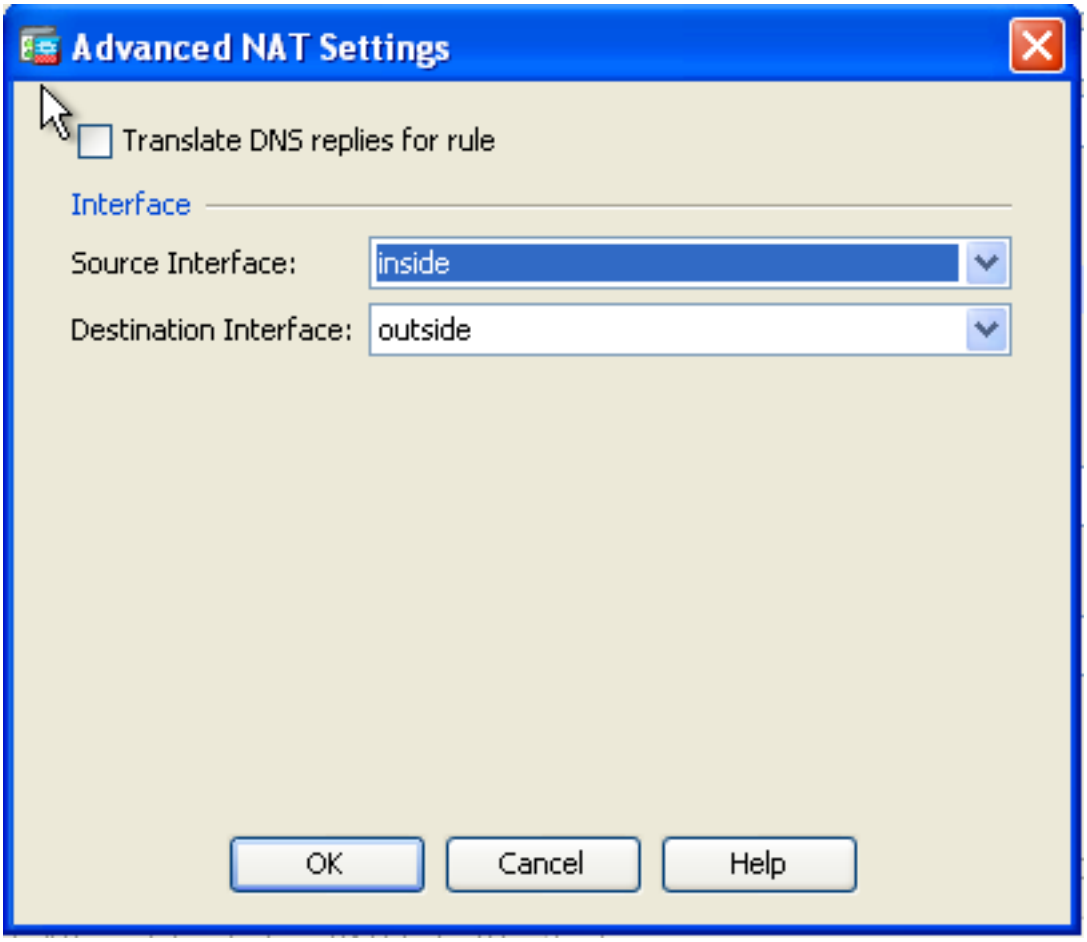
4. El tecleo **agrega** para agregar el objeto de red. En la lista desplegable del tipo, elija el **rango**. En los campos de dirección de la Dirección de inicio y del extremo, ingrese los IP Addresses de la PALMADITA que comienzan y de terminaciones. Haga clic en OK.



5. En el campo traducido del addr, elija el objeto del direccionamiento. Haga clic **avanzado** para seleccionar la fuente y las interfaces de destino.



6. En las listas desplegables de la interfaz de origen y de la interfaz de destino, elija las interfaces apropiadas. El Haga Click en OK y el tecleo **solicitan los** cambios para tomar el efecto.

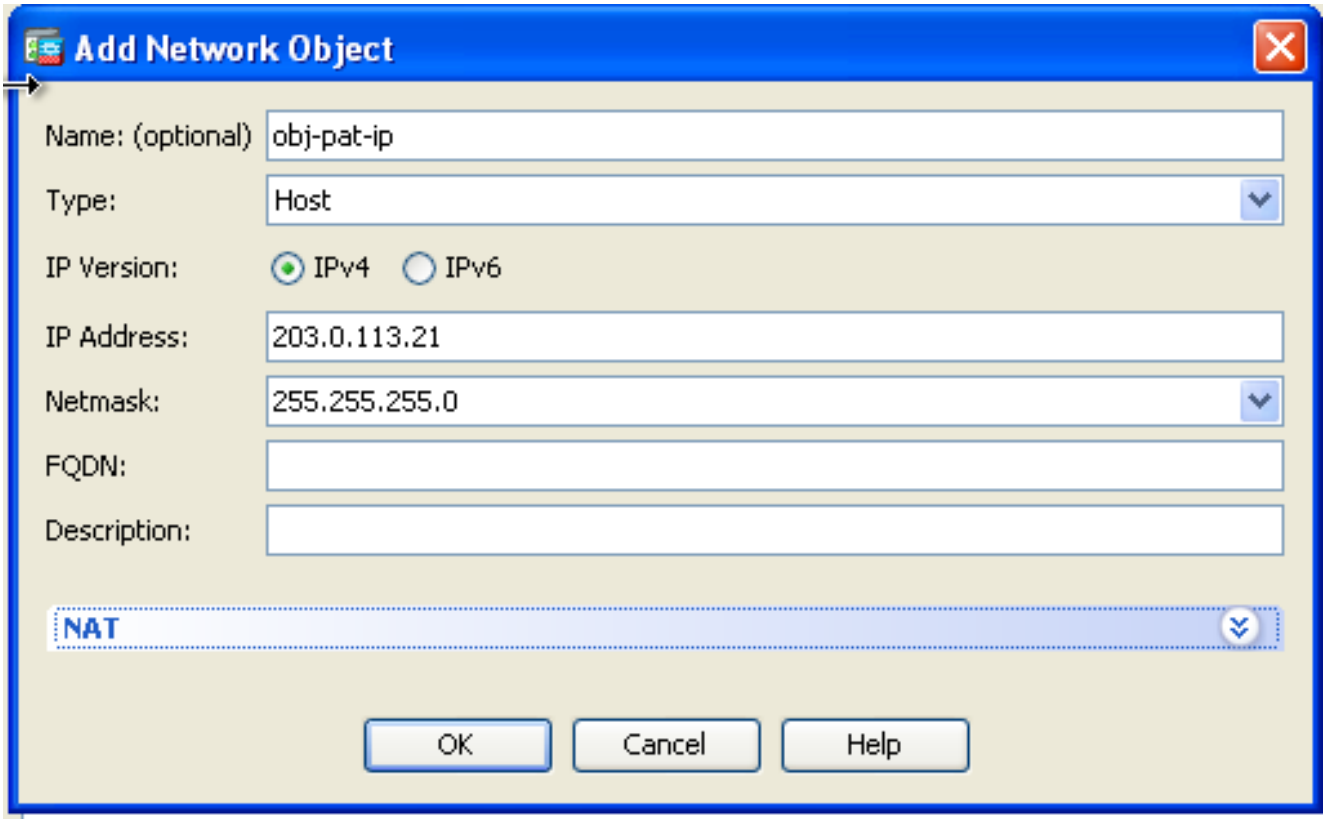


Éste es el CLI equivalente hecho salir para esta Configuración de ASDM:

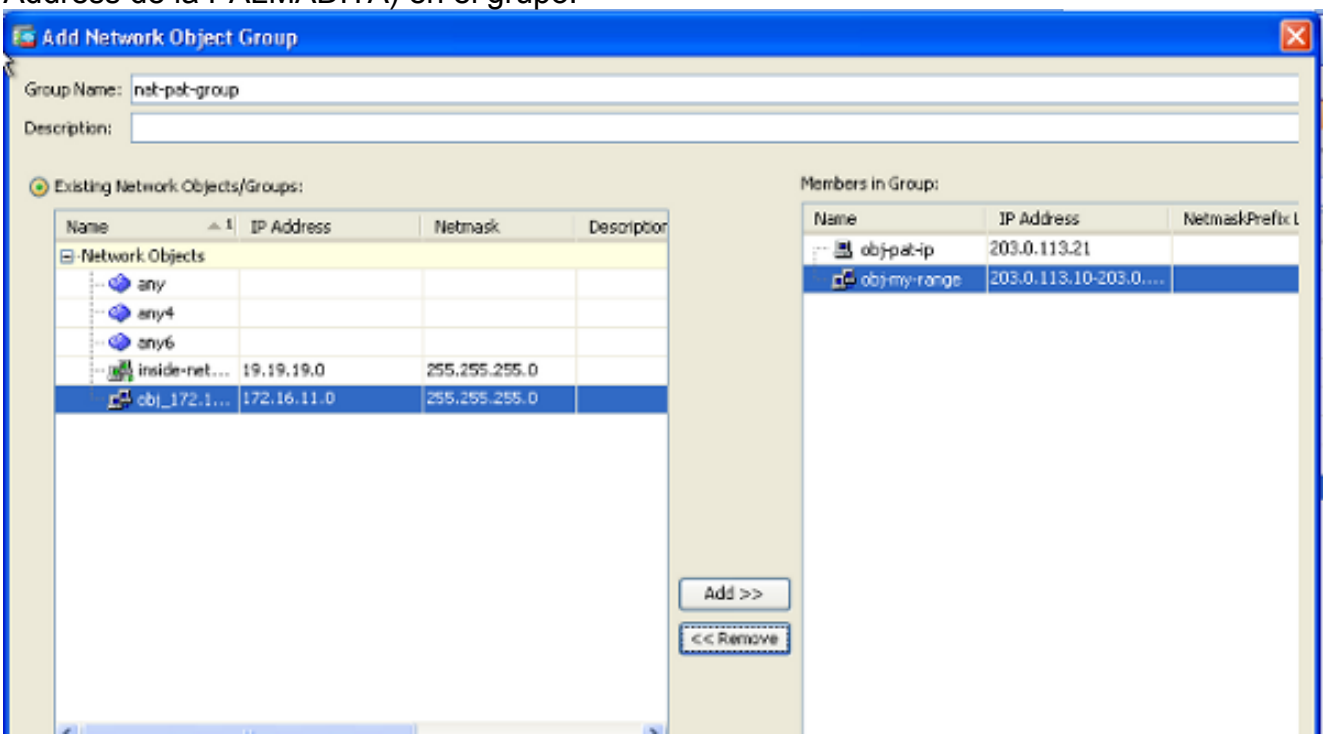
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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 host en la red de 172.16.11.0 conseguirán traducidos a cualquier dirección IP del agrupamiento NAT, 203.0.113.10 - 203.0.113.20. Si el pool asociado tiene menos direccionamientos que el grupo real, usted podría ejecutarse de los direccionamientos. Como consecuencia, usted podría intentar implementar el NAT dinámico con el respaldo dinámico de la PALMADITA o usted podría intentar ampliar el pool existente.

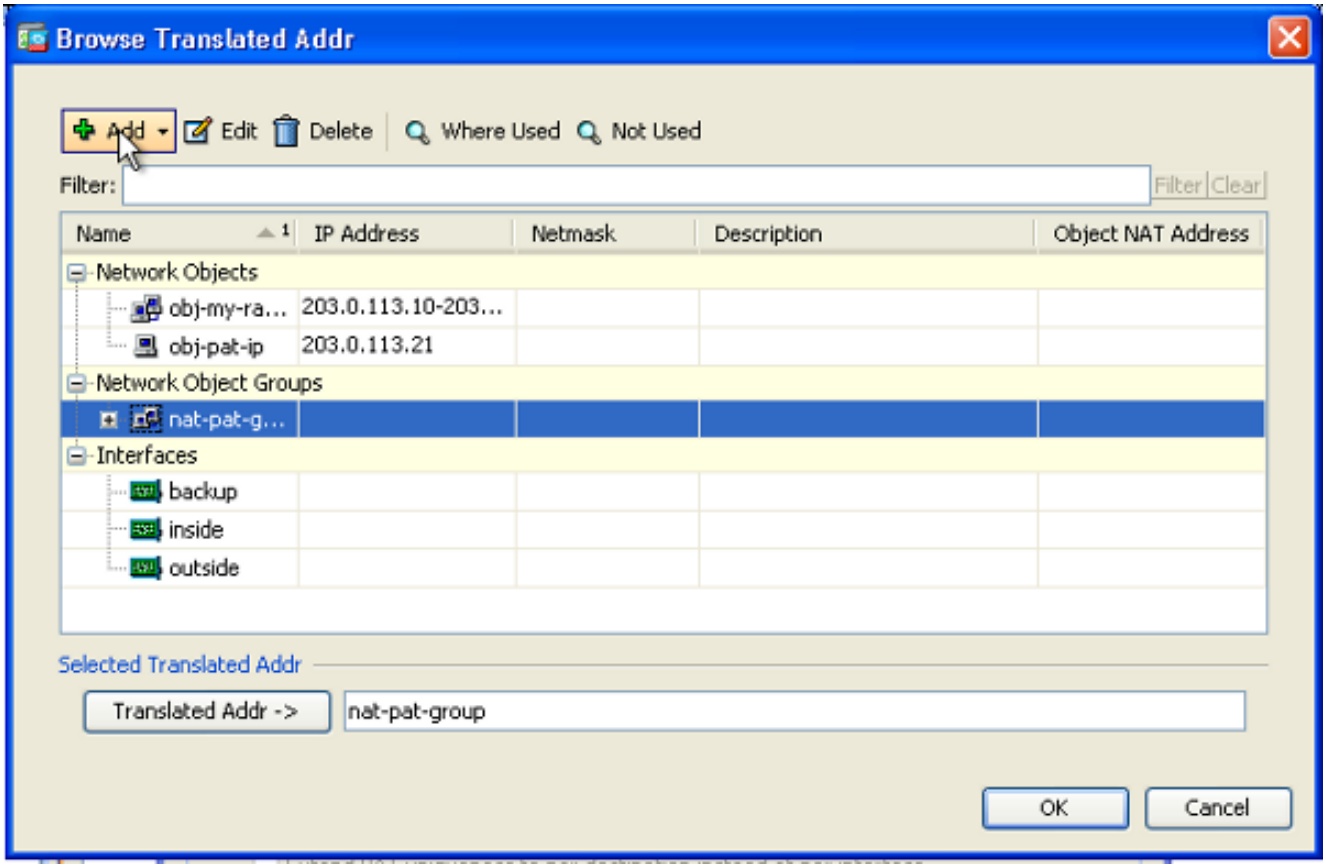
1. Relance los pasos 1 a 3 en la configuración previa y el tecleo **agrega** de nuevo para agregar un objeto de red. En la lista desplegable del tipo, elija el **host**. En el campo del IP Address, ingrese el IP Address del respaldo de la PALMADITA. Haga clic en OK.



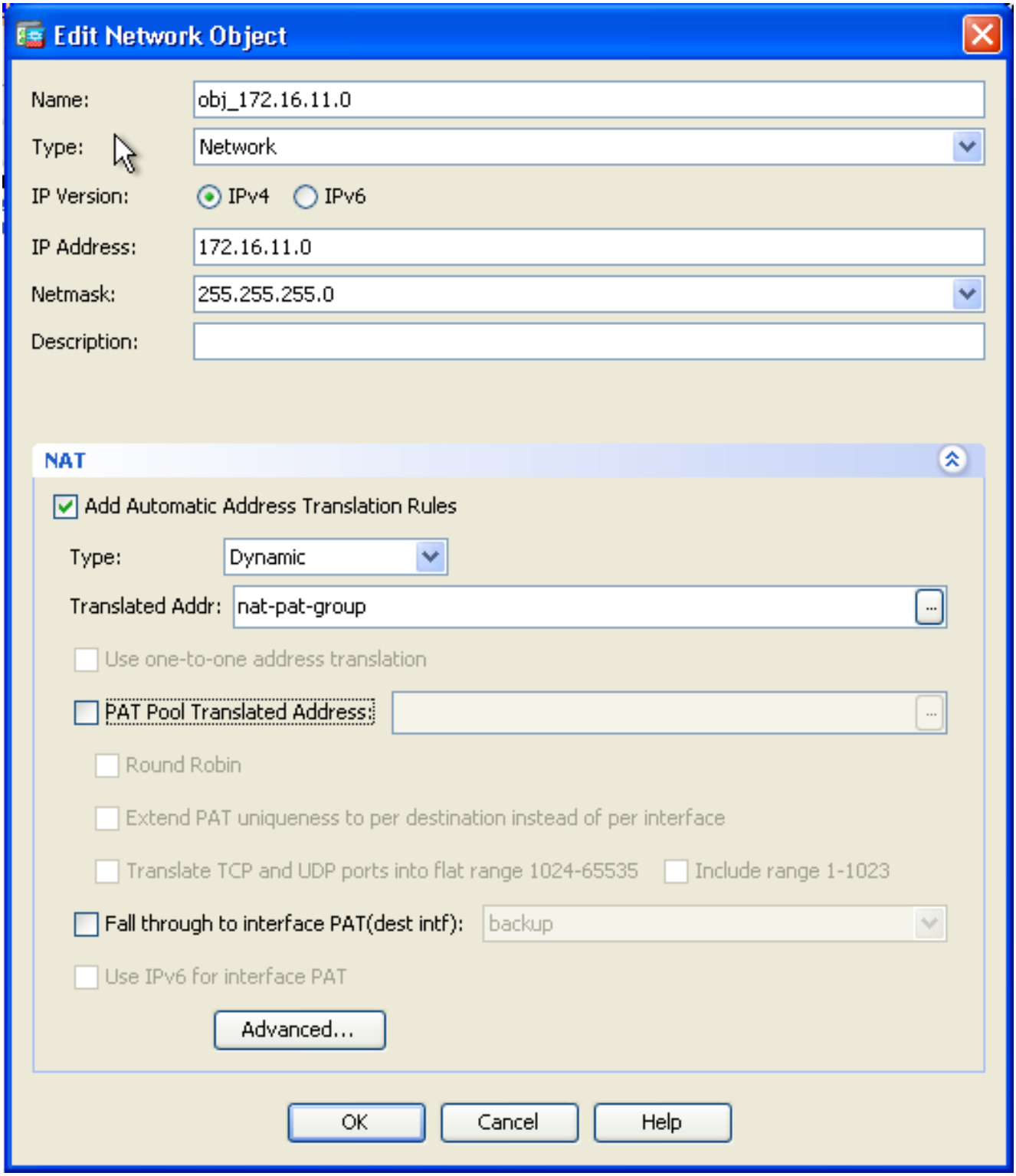
2. El tecleo **agrega** para agregar un grupo de objeto de red. En el campo de nombre del grupo, ingrese un nombre del grupo y **agregue** ambos objetos del direccionamiento (rango NAT y IP Address de la PALMADITA) en el grupo.



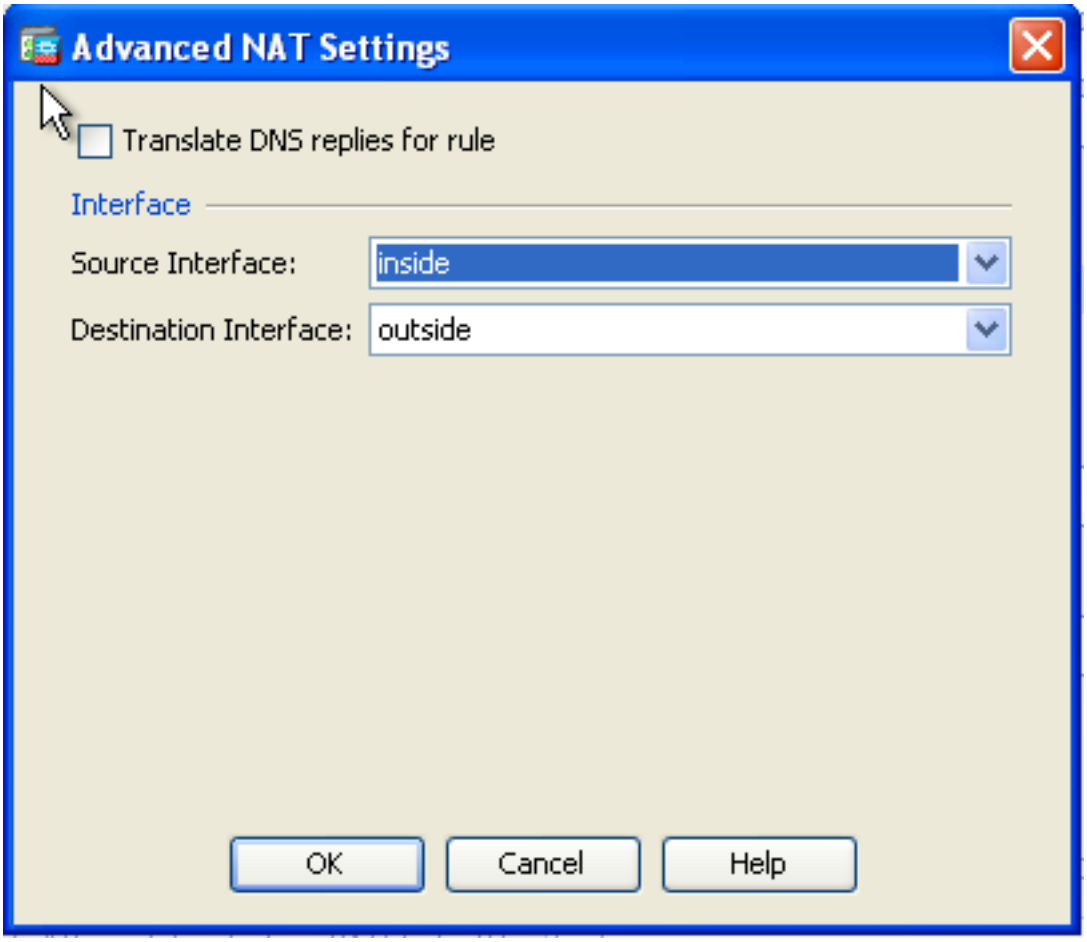
3. Elija la regla configurada NAT y cambie el addr traducido para ser “NAT-palmadita-grupo” del grupo nuevamente configurado (estaba previamente el “OBJ-mi-rango "). Haga clic en OK.



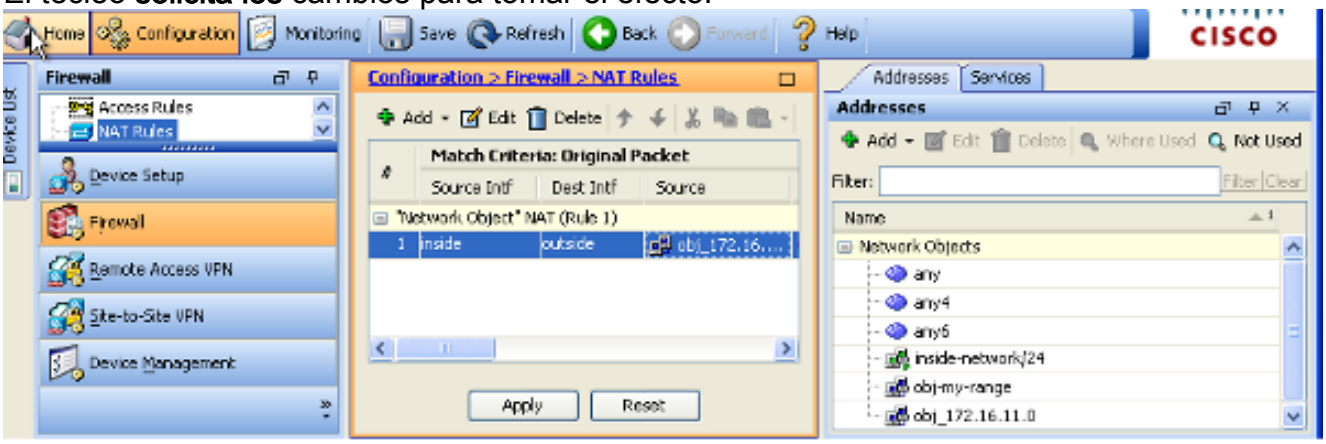
4. Haga Click en OK para agregar la regla NAT. El tecleo **avanzó** para seleccionar la fuente y las interfaces de destino.



5. En las listas desplegables de la interfaz de origen y de la interfaz de destino, elija las interfaces apropiadas. Haga clic en OK.



6. El tecleo **solicita los** cambios para tomar el efecto.



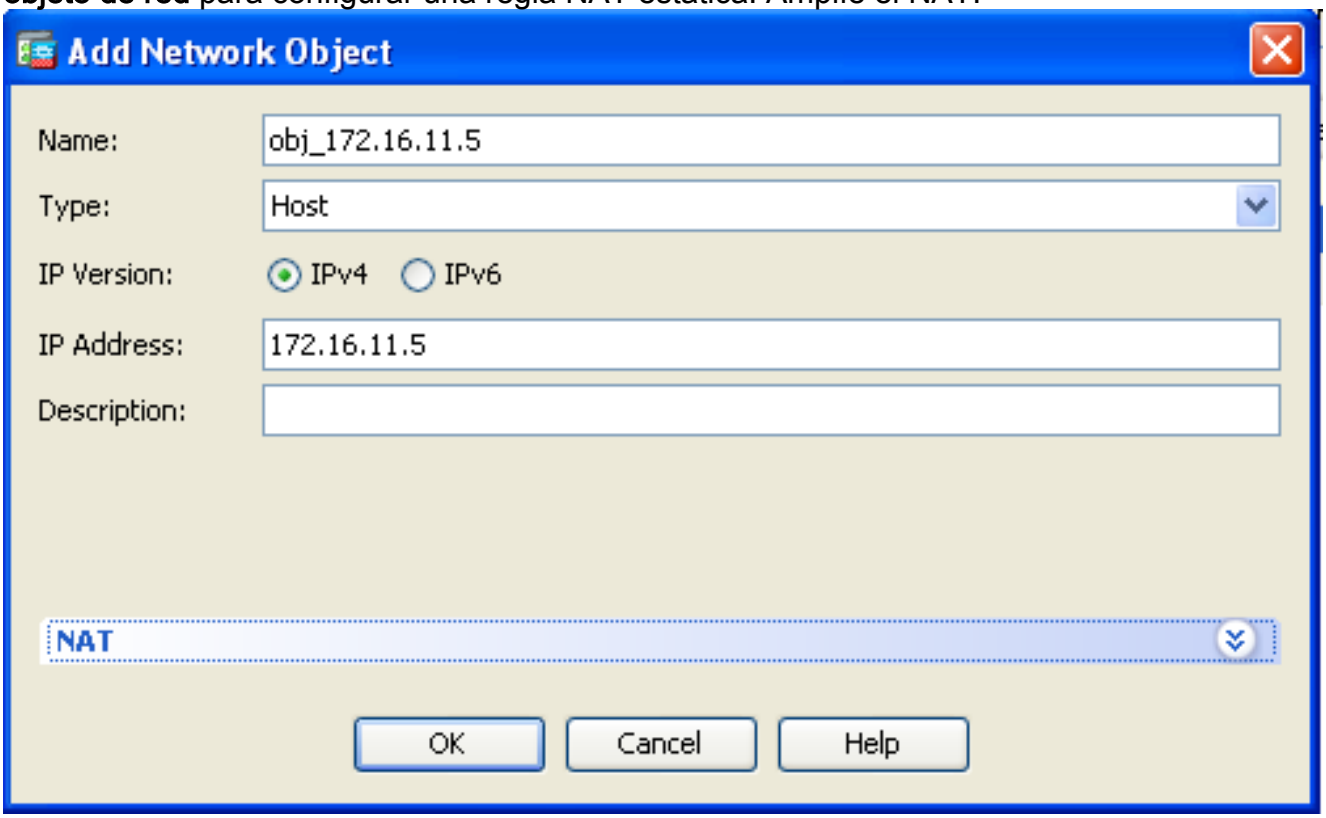
Éste es el CLI equivalente hecho salir para esta Configuración de ASDM:

```
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
```

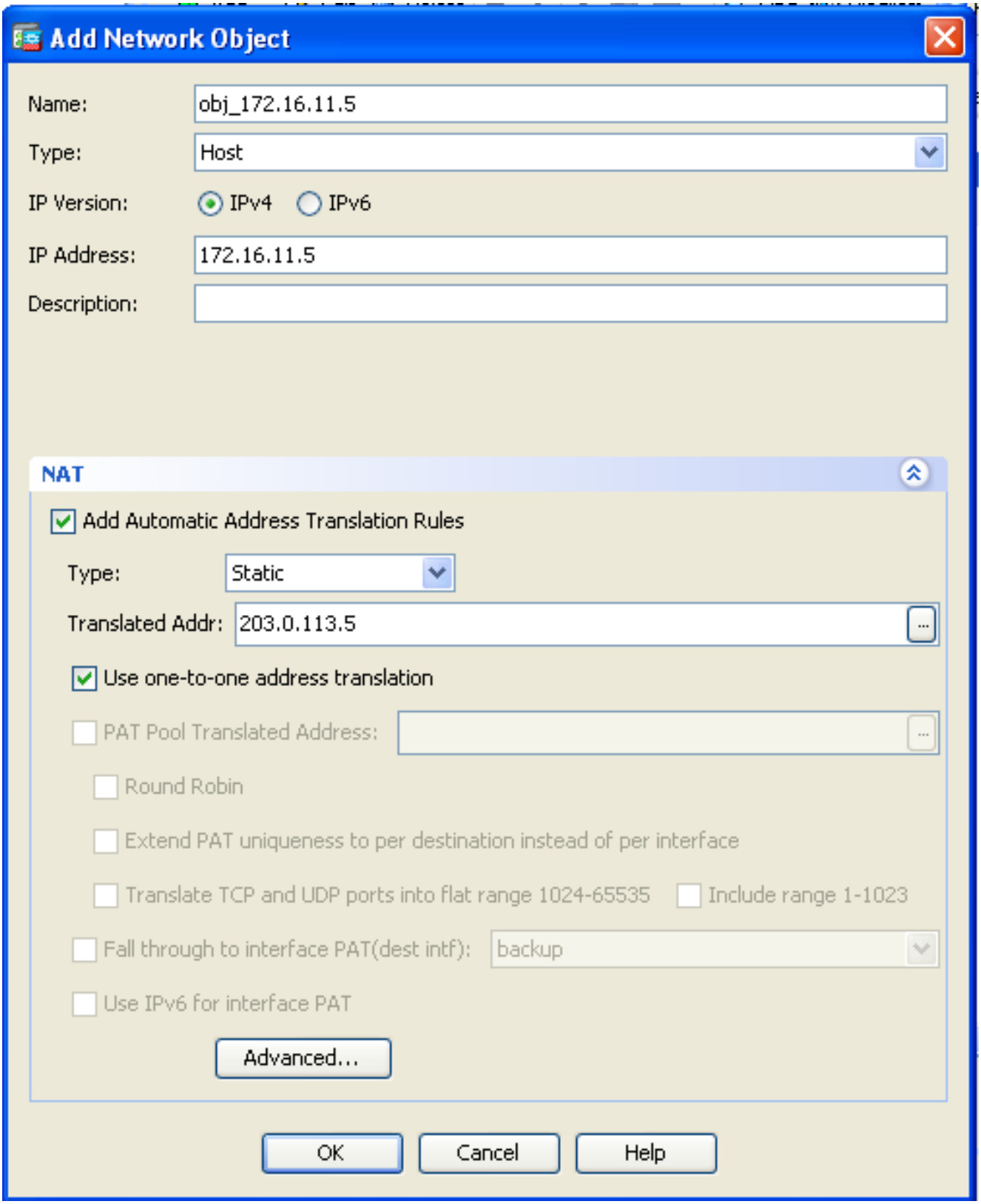
Permita el Acceso de los Hosts no Confiables a los Hosts de su Red de Confianza

Esto se puede alcanzar con la aplicación de una traducción NAT estática y de una regla de acceso de permitir esos host. Le requieren configurar esto siempre que un usuario externo quisiera acceder cualquier servidor que se siente en su red interna. El servidor en la red interna tendrá un IP Address privado que no sea routable en Internet. Como consecuencia, usted necesita traducir ese IP Address privado a un IP Address público con una regla NAT estática. Suponga que usted tiene un servidor interno (172.16.11.5). Para hacer este trabajo, usted necesita traducir este dirección IP del servidor privado a un IP Address público. Este ejemplo describe cómo implementar el NAT estático bidireccional para traducir 172.16.11.5 a 203.0.113.5.

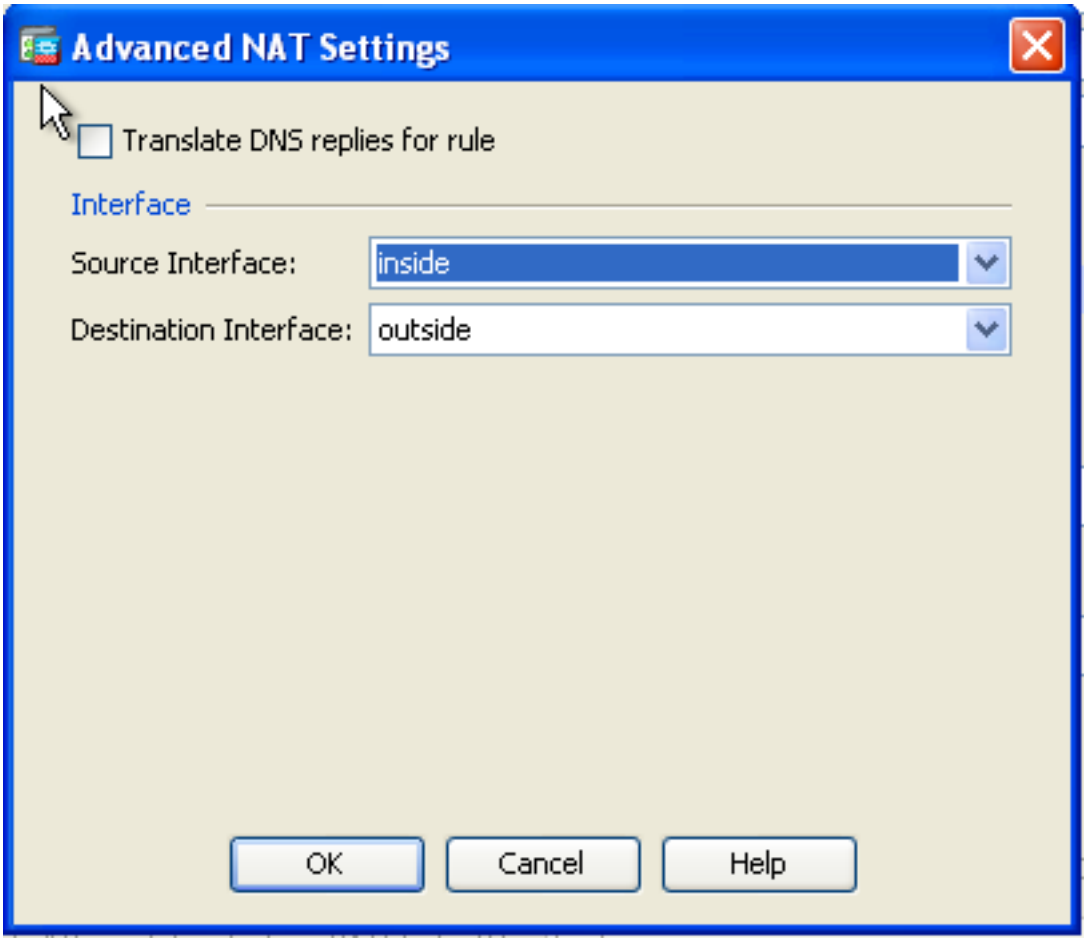
1. Elija la **configuración** > el **Firewall** > las **reglas NAT**. El tecleo **agrega** y después elige el **objeto de red** para configurar una regla NAT estática. Amplíe el NAT.



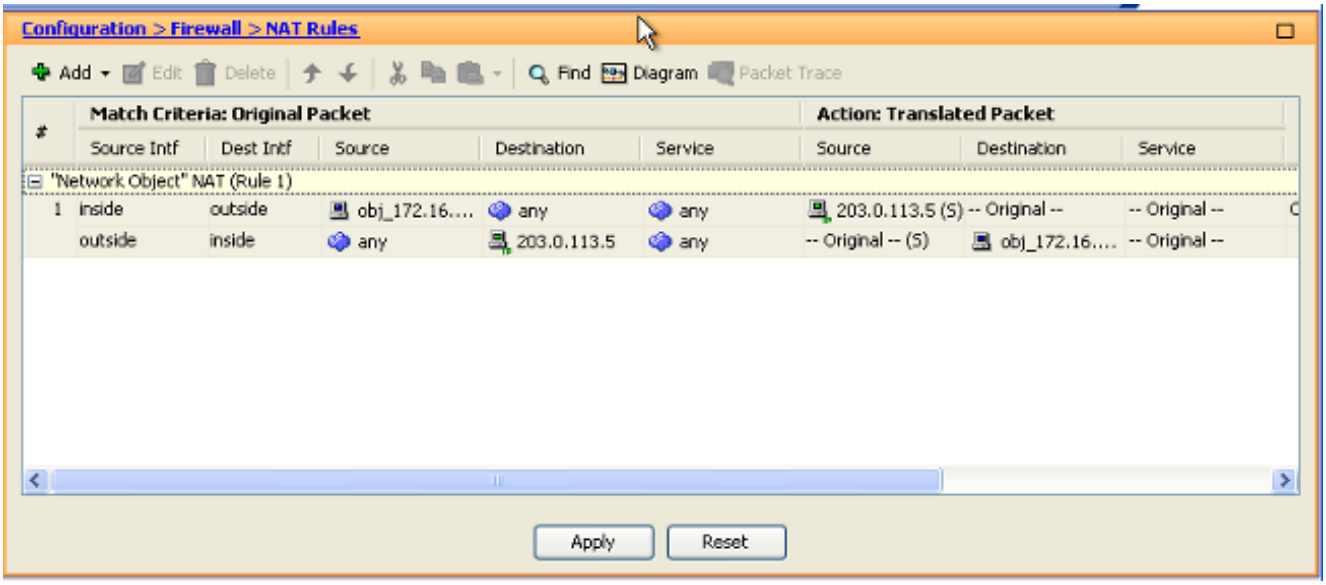
2. Marque la casilla de verificación **automática de las reglas de traducción de la dirección del agregar**. En la lista desplegable del tipo, elija los **parásitos atmosféricos.** En el campo traducido del addr, ingrese el IP Address. Haga clic **avanzado** para seleccionar la fuente y las interfaces de destino.



3. En las listas desplegables de la interfaz de origen y de la interfaz de destino, elija las interfaces apropiadas. Haga clic en OK.



4. Usted puede ver la entrada NAT estática configurada aquí. El tecleo **se aplica** para enviar esto al ASA.



Éste es el CLI equivalente hecho salir para esta configuración del NAT:

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

Identidad estática NAT

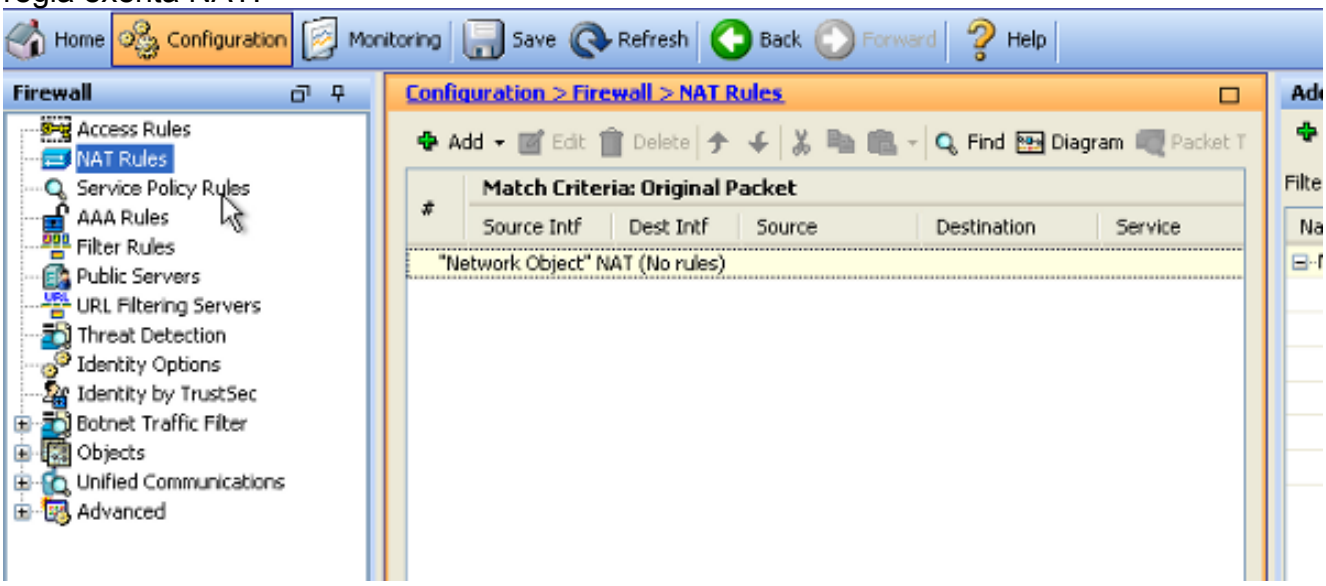
El NAT exento es una función útil donde los usuarios interiores intentan acceder un host/un servidor del telecontrol VPN o un poco de host/servidor recibido detrás de cualquier otra interfaz del ASA sin la realización de un NAT. Para alcanzar esto, el servidor interno, que tiene un IP

Address privado, será identidad traducida a sí mismo y se permite que a su vez acceder el destino que realiza un NAT.

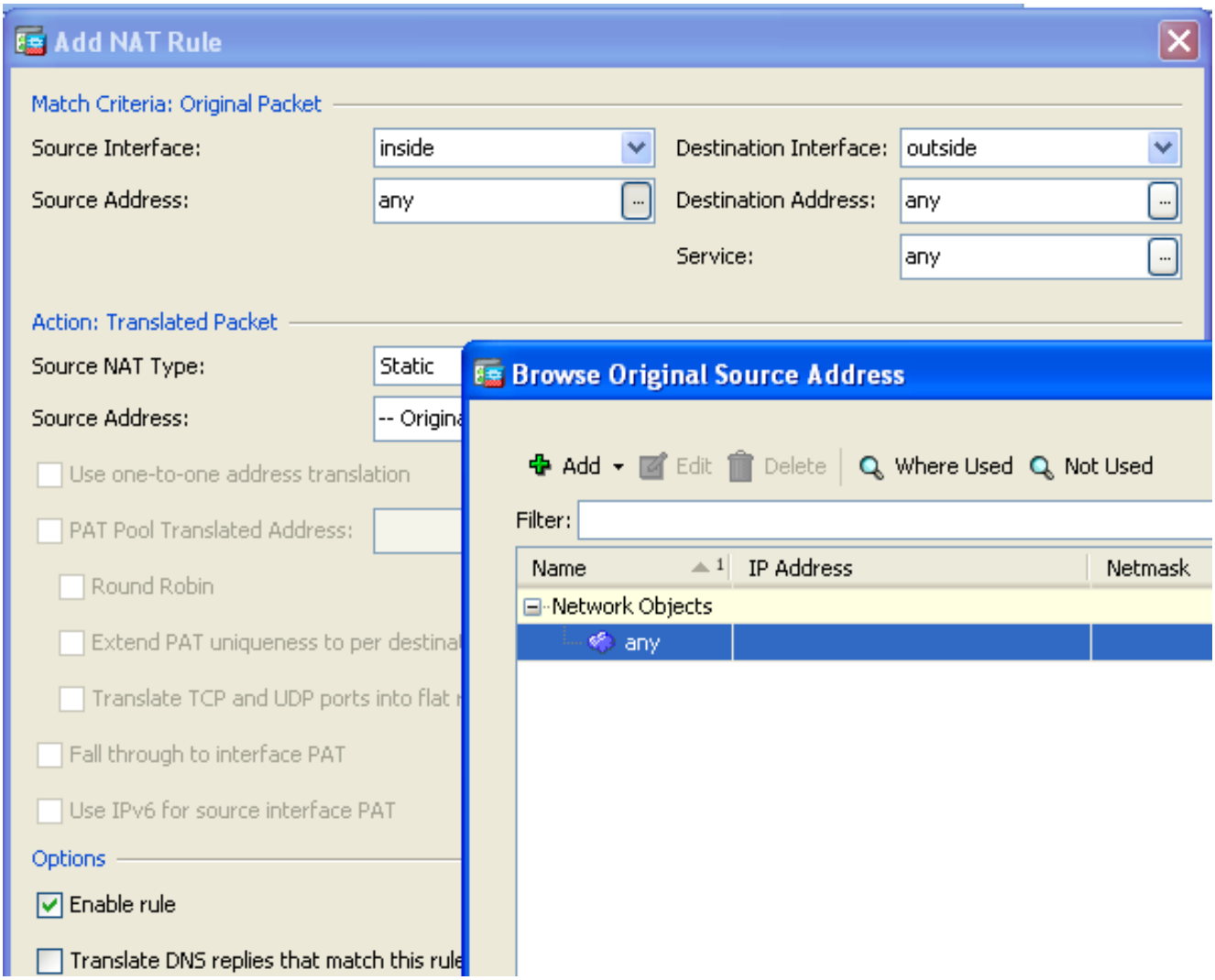
En este ejemplo, el host interior 172.16.11.15 necesita acceder al servidor VPN remoto 172.20.21.15.

Complete estos pasos para no prohibir a los host interiores el acceso a la red VPN remota con la realización de un NAT:

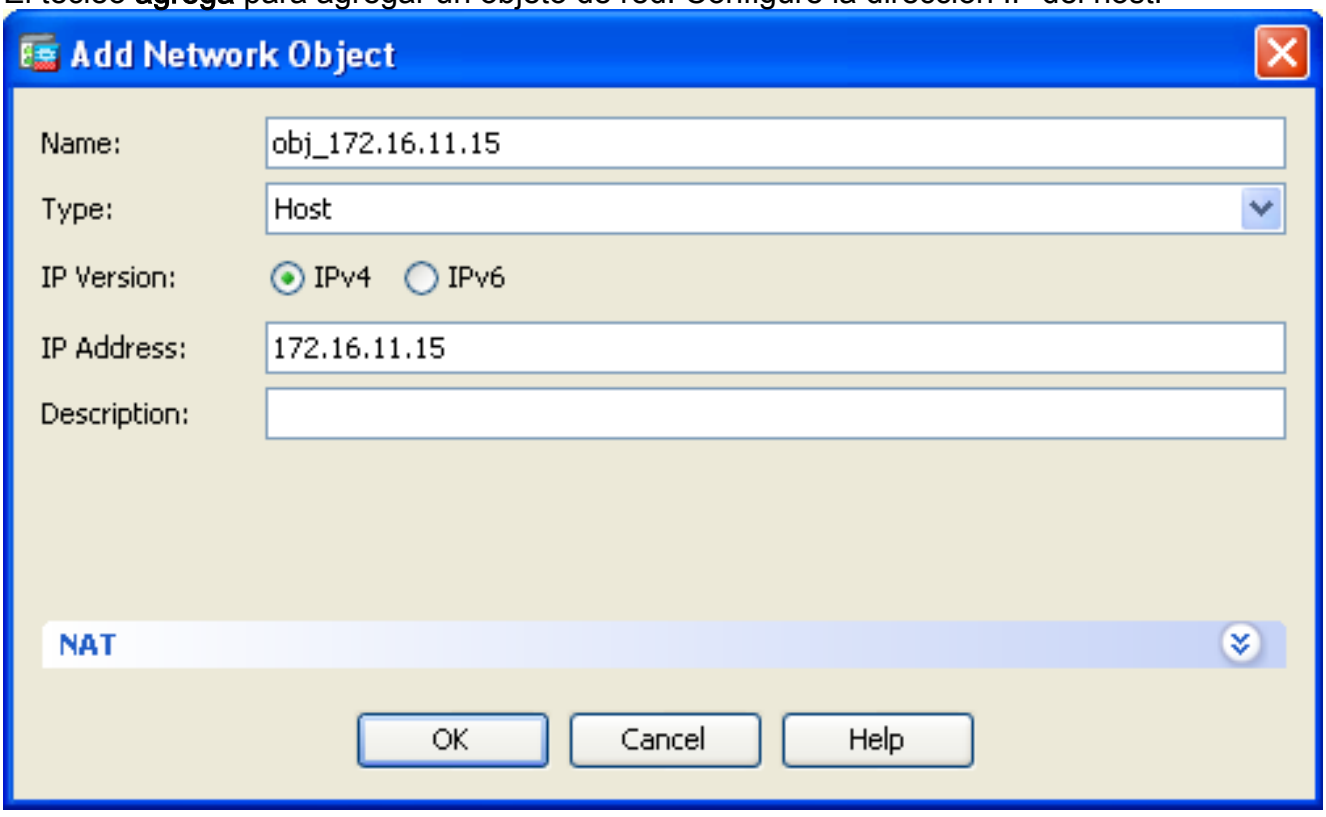
1. Elija la **configuración** > el **Firewall** > las **reglas NAT**. El tecleo **agrega** para configurar una regla exenta NAT.



2. En las listas desplegables de la interfaz de origen y de la interfaz de destino, elija las interfaces apropiadas. En el campo de dirección de origen, elija la entrada apropiada.

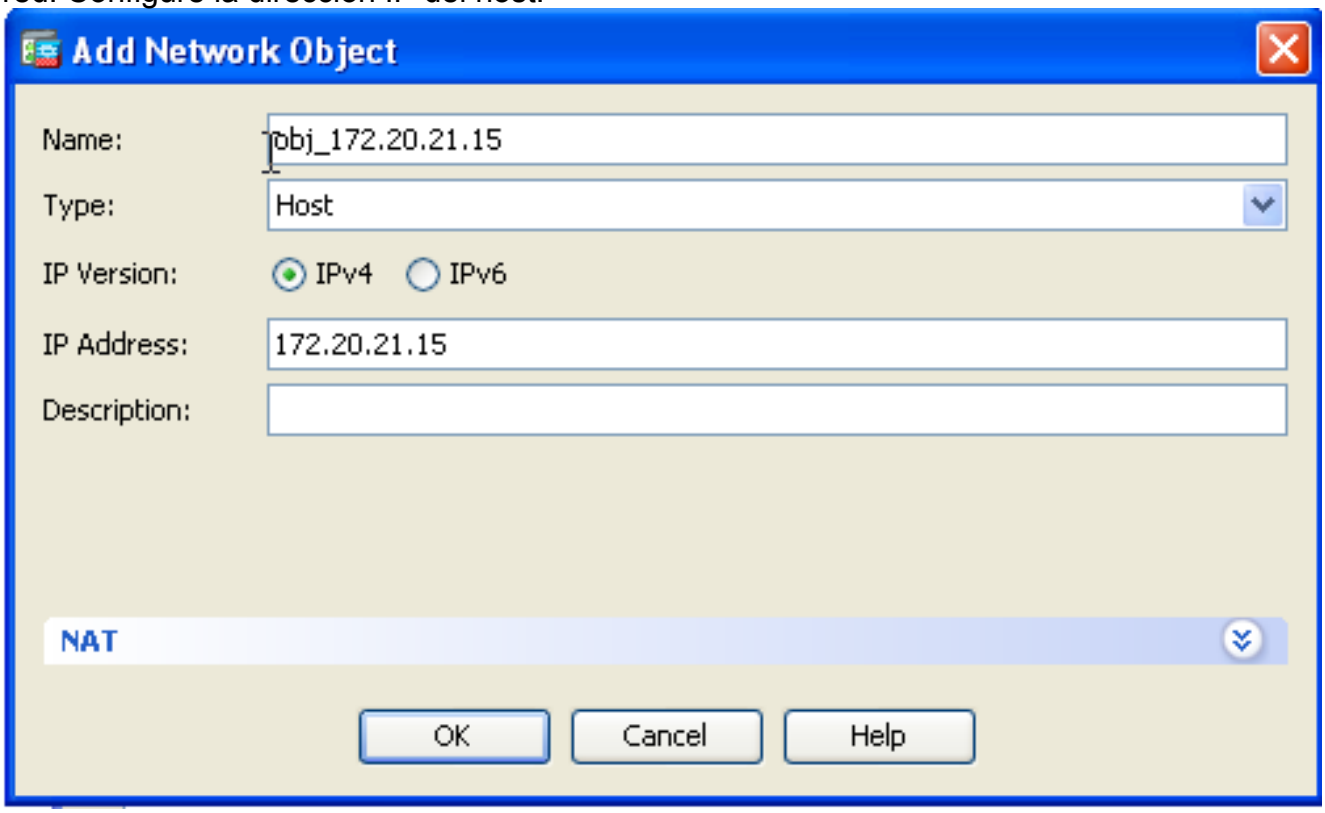


3. El tecleo **agrega** para agregar un objeto de red. Configure la dirección IP del host.

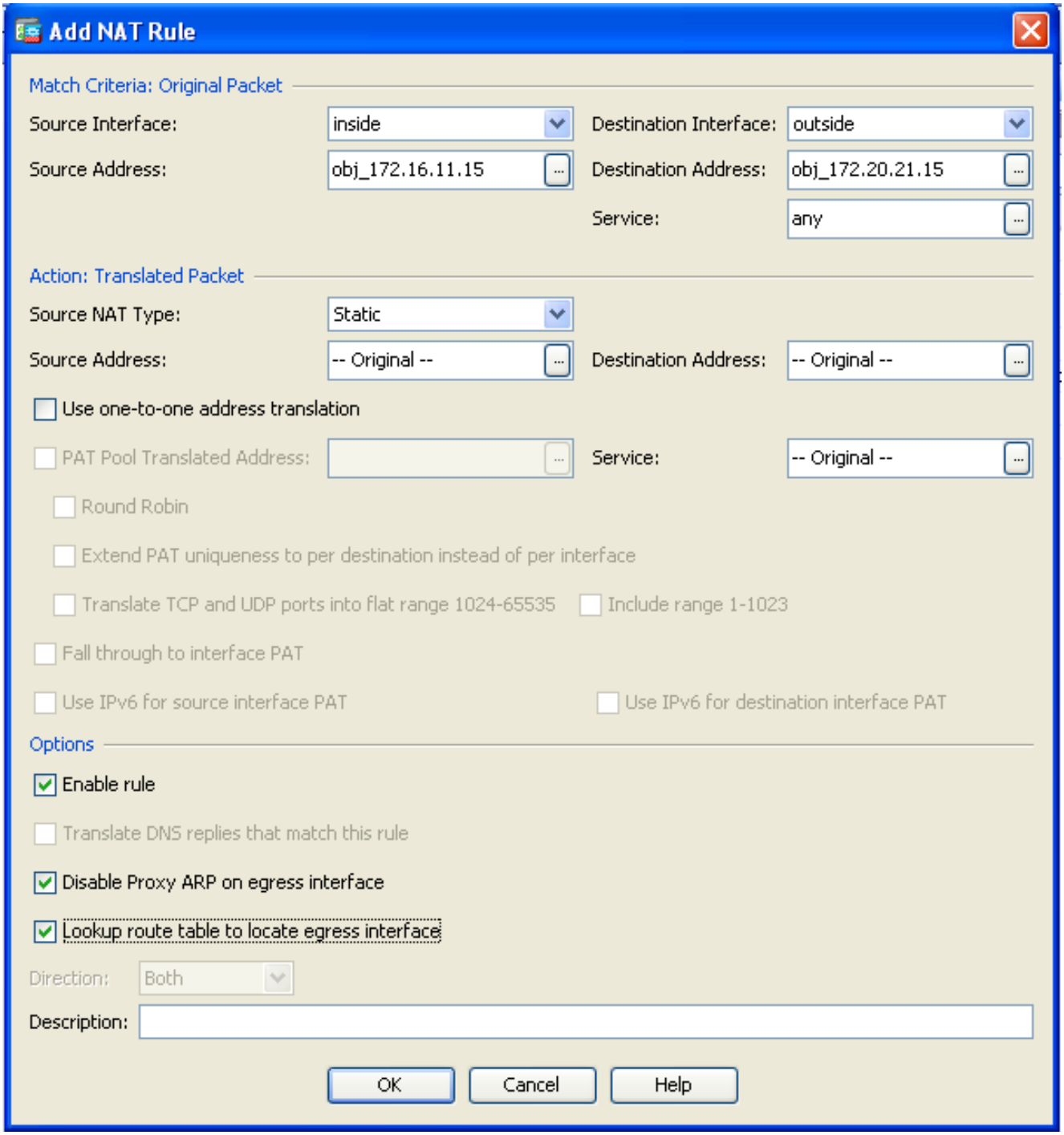


4. Semejantemente, hojee a la **dirección destino**. El tecleo **agrega** para agregar un objeto de

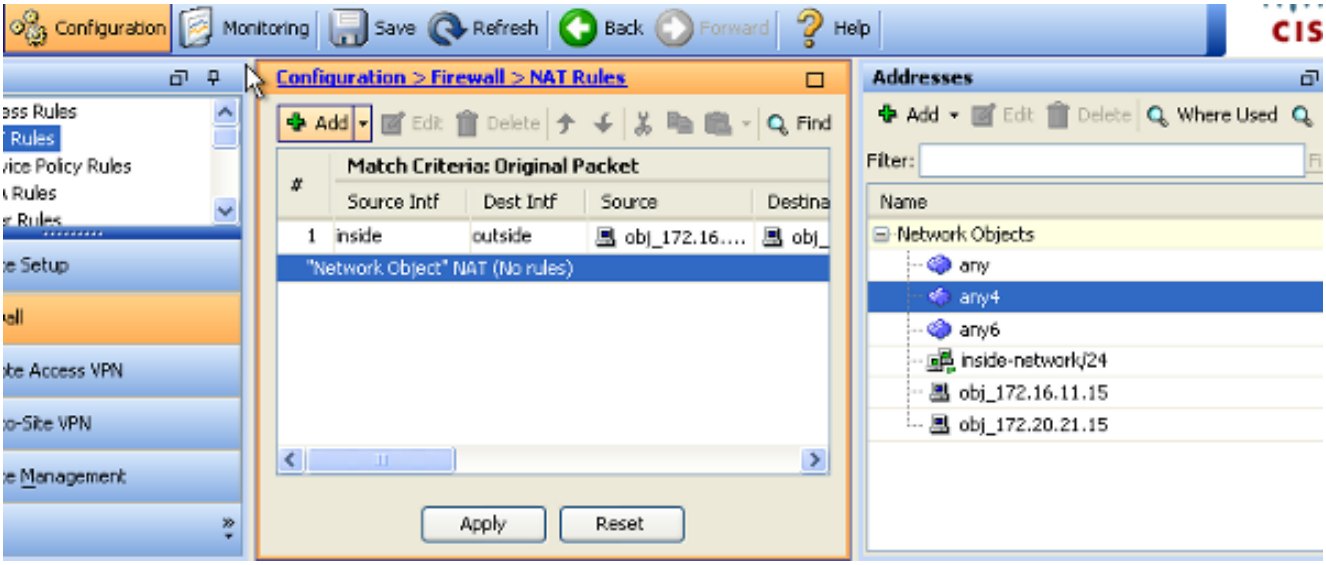
red. Configure la dirección IP del host.



5. Elija los objetos configurados de la dirección de origen y de la dirección destino. Marque el **proxy ARP de la neutralización en la interfaz de egreso** y la **tabla de ruta de las operaciones de búsqueda para localizar las** casillas de verificación de la **interfaz de egreso**. Haga clic en OK.



6. El tecleo **solicita los** cambios para tomar el efecto.



Éste es el CLI equivalente hecho salir para el NAT exento o la configuración del NAT de la 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 puerto (expedición) con los parásitos atmosféricos

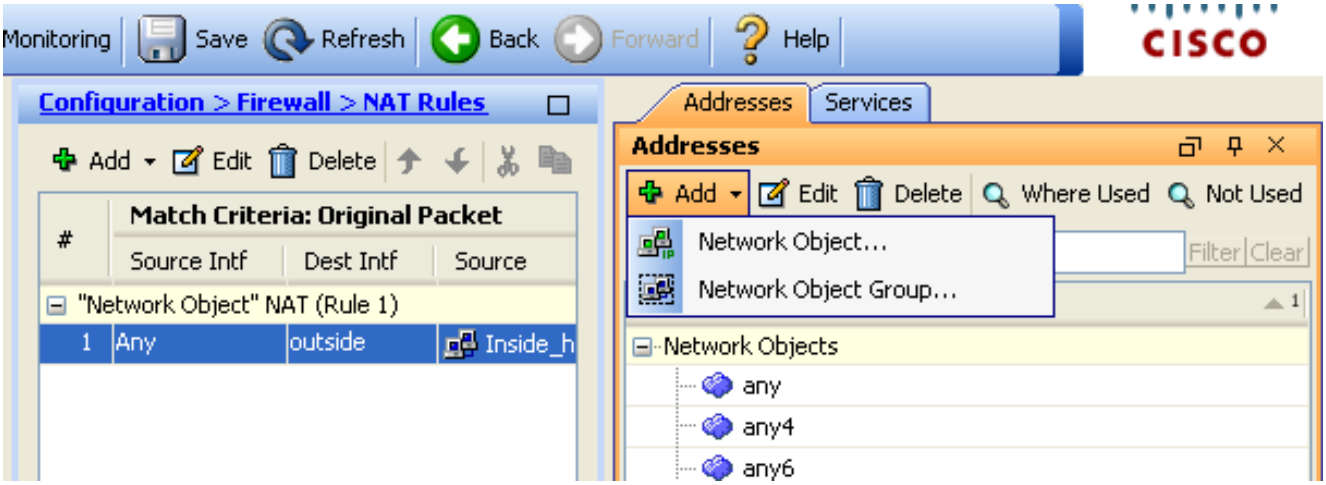
La expedición o la redirección de puerto del puerto es una función útil donde los usuarios externos intentan acceder a un servidor interno en un puerto específico. Para alcanzar esto, traducirán al servidor interno, que tiene un IP Address privado, a un IP Address público que a su vez no se prohiba el acceso para el puerto específico.

En este ejemplo, el usuario externo quiere acceder al servidor SMTP, 203.0.115.15 en el puerto 25. Esto se logra en dos pasos:

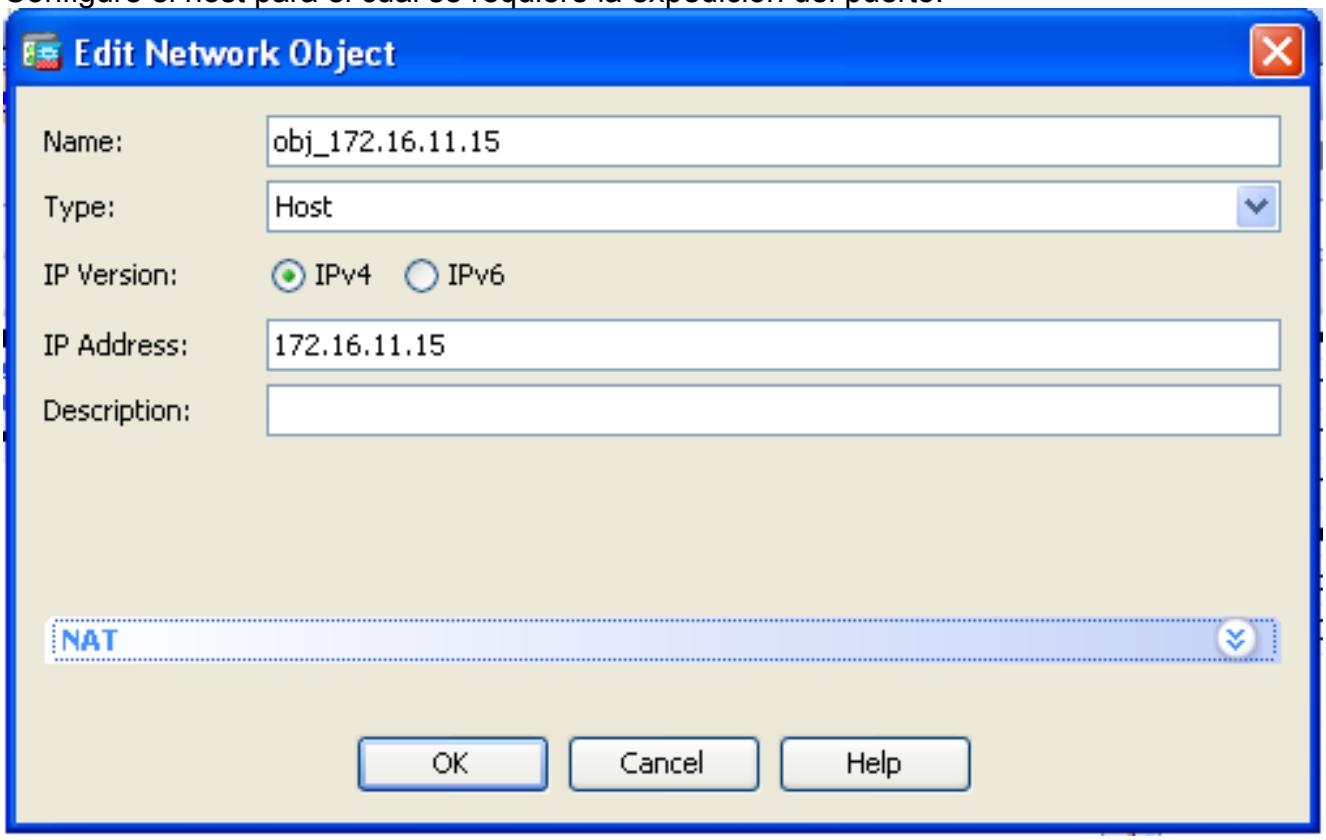
1. Traduzca al servidor de correo interno, 172.16.11.15 en el puerto 25, al IP Address público, 203.0.115.15 en el puerto 25.
2. Permita el acceso al mail server público, 203.0.115.15 en el puerto 25.

Cuando el usuario externo intenta acceder el servidor, 203.0.115.15 en el puerto 25, este tráfico se reorienta al servidor de correo interno, 172.16.11 15 en el puerto 25.

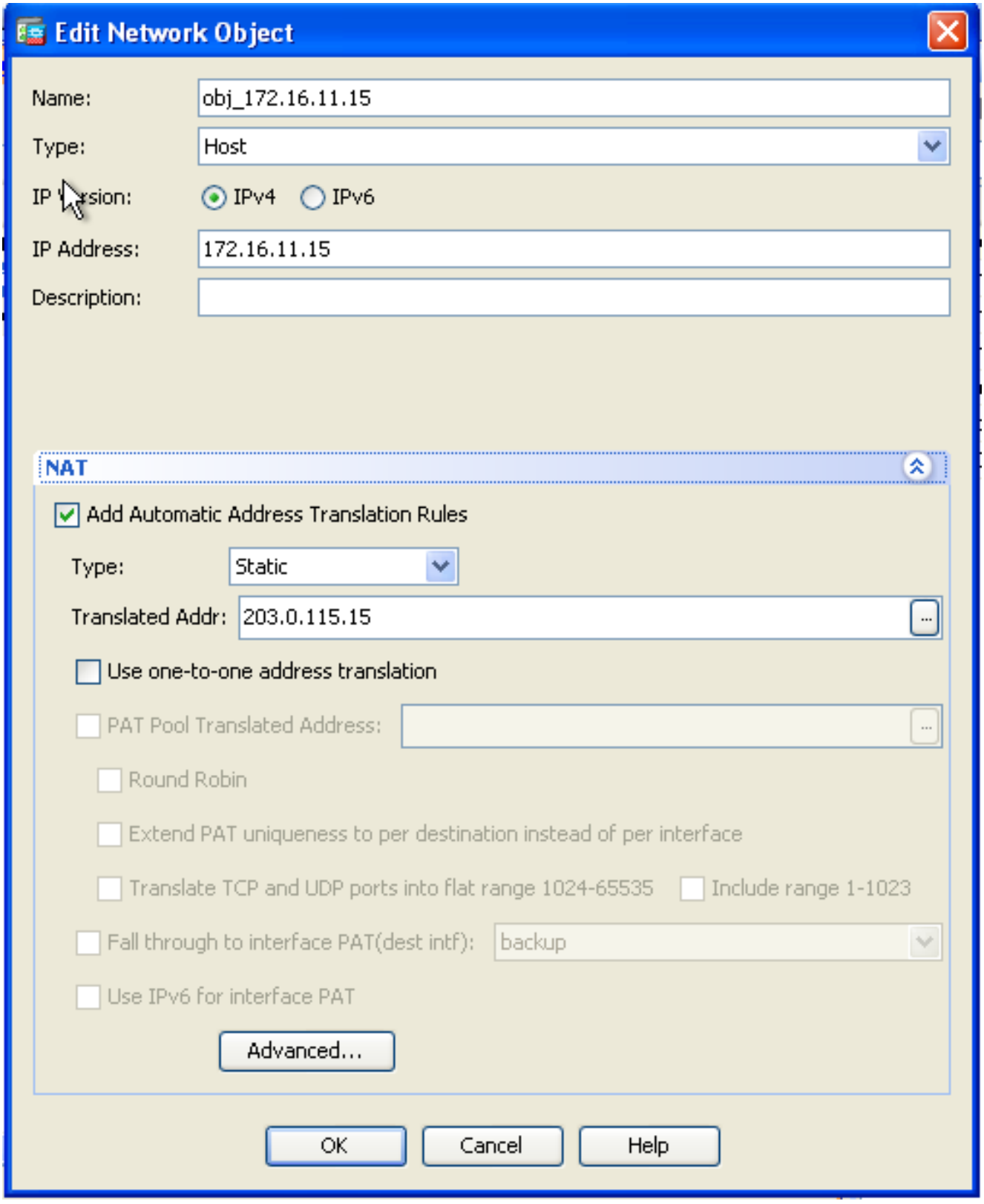
1. Elija la **configuración > el Firewall > las reglas NAT**. El tecleo **agrega** y después elige el **objeto de red** para configurar una regla NAT estática.



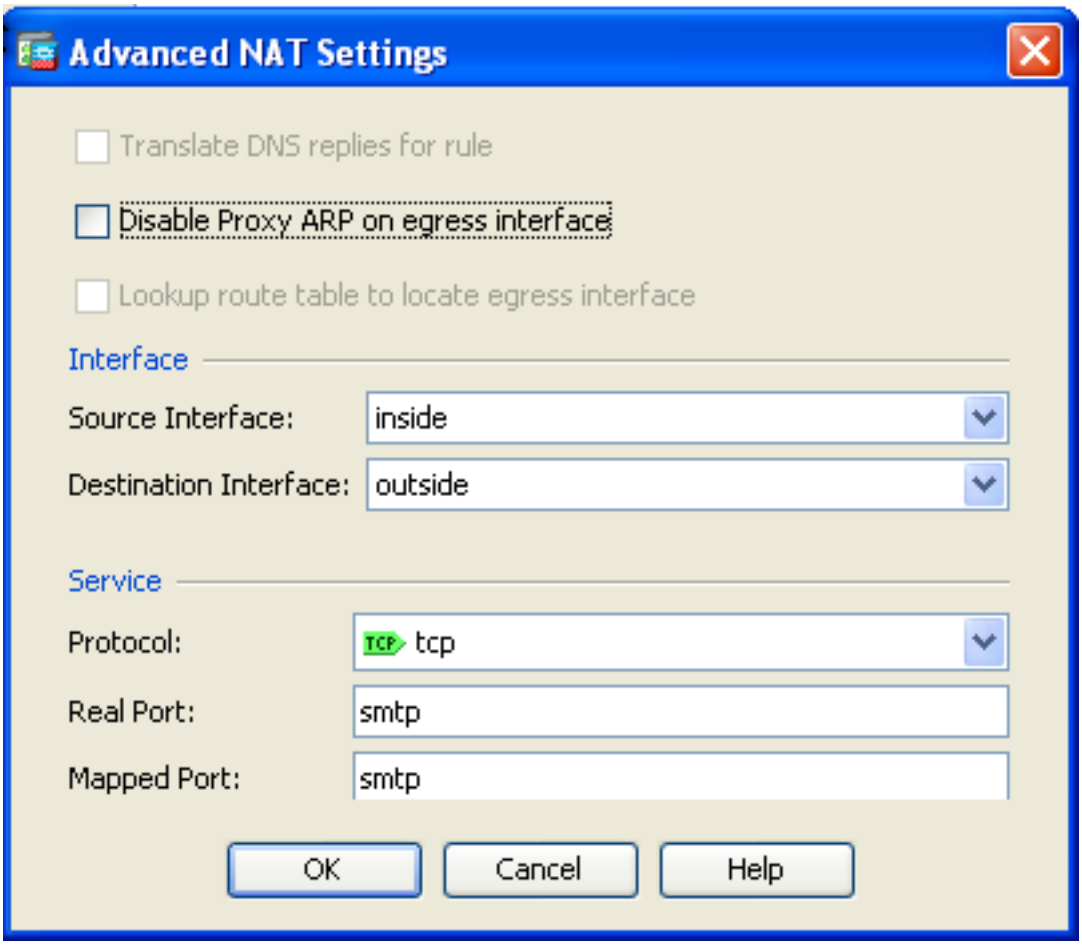
2. Configure el host para el cual se requiere la expedición del puerto.



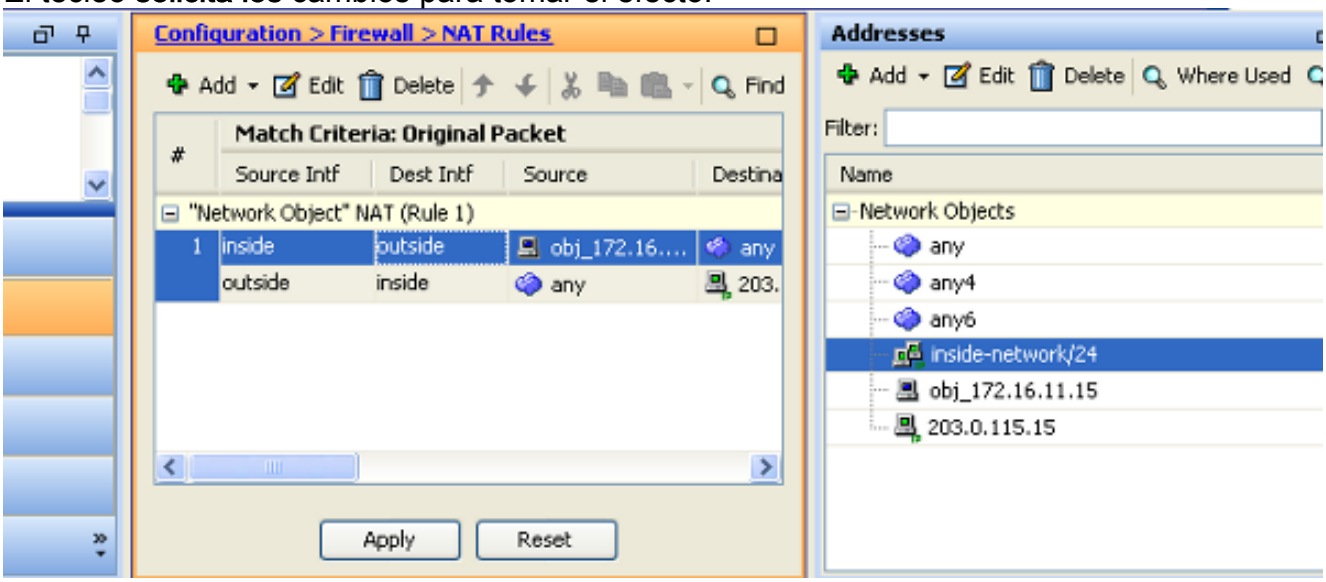
3. Amplíe el NAT. Marque la casilla de verificación **automática de las reglas de traducción de la dirección del agregar**. En la lista desplegable del tipo, elija los **parásitos atmosféricos**. En el campo traducido del addr, ingrese el IP Address. Haga clic **avanzado** para seleccionar el servicio y la fuente y las interfaces de destino.



4. En las listas desplegables de la interfaz de origen y de la interfaz de destino, elija las interfaces apropiadas. Configure el servicio. Haga clic en OK.



5. El tecleo **solicita los** cambios para tomar el efecto.



Éste es el CLI equivalente hecho salir para esta configuración del NAT:

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.115.15 service tcp smtp smtp
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El analizador del CLI de Cisco (clientes registrados solamente) apoya los ciertos comandos show. Utilice el analizador del CLI de Cisco para ver una análisis de la salida del comando show.

Acceda un sitio web vía el HTTP con un buscador Web. Este ejemplo utiliza un sitio que se reciba en 198.51.100.100. Si la conexión es acertada, esta salida se puede considerar en el ASA CLI.

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
```

El ASA es un escudo de protección con estado, y el tráfico de retorno del servidor Web se permite detrás con el Firewall porque hace juego una ***conexión*** en la tabla de conexiones del Firewall. Trafique que hace juego una conexión que preexista se permita con el Firewall sin el bloqueo por una interfaz ACL.

En la salida anterior, el cliente en la interfaz interior ha establecido una conexión al host de 198.51.100.100 apagado de la interfaz exterior. Esta conexión se hace con el protocolo TCP y ha estado ociosa por seis segundos. Los indicadores de la conexión indican al estado actual de esta conexión. Más información sobre los indicadores de la conexión se puede encontrar en los indicadores de la conexión TCP 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 ASA genera los Syslog durante el funcionamiento normal. Los Syslog se extienden en la verbosidad basada en la configuración de registro. La salida muestra dos Syslog que se vean en el nivel seis, o el nivel “informativo”.

En este ejemplo, hay dos Syslog generados. El primer es un mensaje del registro que indica que el Firewall ha construido una traducción, específicamente una traducción dinámica TCP (PALMADITA). Indica la dirección IP de origen y el puerto y la dirección IP y el puerto traducidos mientras que el tráfico atraviesa del interior a las interfaces exteriores.

El segundo Syslog indica que el Firewall ha construido una conexión en su tabla de conexiones para este tráfico específico entre el cliente y servidor. Si el Firewall fuera configurado para bloquear este intento de conexión, o un cierto otro factor inhibiera la creación de esta conexión (las restricciones de recursos o una posible configuración incorrecta), el Firewall no generaría un registro que indica que la conexión fue construida. En lugar registraría una razón de la conexión para ser negado o una indicación sobre qué factor inhibió la conexión de ser creado.

Trazalíneas del paquete

```
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
```

Las funciones del trazalíneas del paquete en el ASA permiten que usted especifique un paquete *simulado* y que considere todos los diversos pasos, controles, y funciones que el Firewall pasa por cuando procesa el tráfico. Con esta herramienta, es útil identificar un ejemplo del tráfico que usted cree *debe* ser permitido pasar con el Firewall, y utiliza que 5-tupple para simular el tráfico. En el ejemplo anterior, el trazalíneas del paquete se utiliza para simular un intento de conexión que cumpla estos criterios:

- El paquete simulado llega en el interior.
- El protocolo usado es TCP.
- El dirección IP del cliente simulado es 172.16.11.5.
- El cliente envía el tráfico originado del puerto 1234.
- El tráfico se destina a un servidor en la dirección IP 198.51.100.100.
- El tráfico se destina al puerto 80.

Note que no había mención de la interfaz afuera en el comando. Esto está por el diseño del trazalíneas del paquete. La herramienta le dice cómo los procesos del Firewall que la tentativa del tipo de conexión, que incluye de cómo la rutearía, y fuera de cuál interfaz. Más información sobre el trazalíneas del paquete se puede encontrar en los paquetes del seguimiento con el trazalíneas del paquete.

Captura

Aplique la 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 198.51.100.100ASA#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 32768ASA#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 ingresa o deja sus interfaces. Estas funciones de la captura son fantásticas porque pueden probar definitivo si el tráfico llega, o se van de, un Firewall. El ejemplo anterior mostró la configuración de dos capturas nombradas capin y capout en las interfaces interior y exterior respectivamente. Los comandos capture utilizaron la palabra clave de la coincidencia, que permite que usted sea específico sobre qué tráfico usted quiere capturar.

Para el capin de la captura, usted indicó que usted quiso hacer juego el tráfico visto en la interfaz

interior (ingreso o salida) ese host 198.51.100.100 de 172.16.11.5 del host TCP de las coincidencias. Es decir usted quiere capturar tráfico TCP que se envía del host 172.16.11.5 para recibir 198.51.100.100 o vice versa. El uso de la palabra clave de la coincidencia permite que el Firewall capture ese tráfico bidireccional. El comando capture definido para la interfaz exterior no se refiere a la dirección IP del cliente interno porque el Firewall conduce la PALMADITA en ese dirección IP del cliente. Como consecuencia, usted no puede hacer juego con ese dirección IP del cliente. En lugar, este ejemplo utiliza ningunos para indicar que todos los IP Addresses posibles harían juego esa condición.

Después de que usted configure las capturas, usted entonces intentaría establecer una conexión otra vez, y procede a ver las capturas con el comando del ***<capture_name> de la*** **captura de la demostración**. En este ejemplo, usted puede ver que el cliente podía conectar con el servidor como evidente por el apretón de manos de tres vías TCP visto en las capturas.

Troubleshooting

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

Información Relacionada

- Ejemplo de la configuración de syslog ASA
- Capturas de paquetes ASA con el CLI y el ejemplo de la Configuración de ASDM
- Soporte Técnico y Documentación - Cisco Systems