PIX/ASA 7.x y FWSM: Declaraciones NAT y de la PALMADITA

Contenido

Introducción

Este documento proporciona ejemplos básicos Traducción de Dirección de Red (NAT) y configuraciones de Traducción de Dirección de Puerto (PAT) en los PIX/ASA Security Appliances de Cisco. Se suministran diagramas de red simplificados. Consulte la documentación de PIX/ASA para su versión de software PIX/ASA para obtener información detallada.

Consulte Uso de los comandos nat, global, static, conduit, y access-list y Redirección (Reenvío) de Puertos de PIX para obtener más información sobre los comandos **nat**, **global**, **static**, **conduit**, y access-list y Redirección (Reenvío) de Puertos en PIX 5.x y posterior

Consulte Uso de Sentencias NAT y PAT en Cisco Secure PIX Firewall para obtener más información sobre los ejemplos de configuraciones básicas NAT y PAT en Cisco Secure PIX Firewall.

Para más información sobre la configuración del NAT en la Versión de ASA 8.3 y posterior, refiera a la información sobre el NAT.

Nota: El NAT en el modo transparente es soportado a partir de la versión 8.x de PIX/ASA. Refiera al NAT en el modo transparente para más información.

prerrequisitos

Requisitos

Los lectores de este documento deben estar bien informados sobre el Cisco PIX/ASA Security Appliance de Cisco.

Componentes Utilizados

La información en este documento se basa en Cisco PIX 500 Series Security Appliance Software versión PIX 500 7.0 y posterior.

Nota: Este documento ha sido certificado nuevamente con la versión 8.x de PIX/ASA.

Nota: Los comandos usados en estos documentos son aplicables al Servicio de Firewall al Módulo (FWSM).

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.

Convenciones

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

Comando nat-control

El comando **nat-control** en el PIX/ASA especifica que todo el tráfico defirewall debe tener una entrada de traducción específica (**sentencia NAT** con la sentencia **global** o **estática correspondiente**) para que ese tráfico atraviese el firewall. El comando **nat-control** garantiza que el comportamiento de traducción sea igual a las versiones de firewall PIX anterior de 7.0. La configuración predeterminada de la versión 7.0 y posterior de PIX/ASA es la especificación del comando **no nat-control**. Con la versión 7.0 y posterior de PIX/ASA, puede cambiar este comportamiento cuando ejecuta el comando **nat-control**.

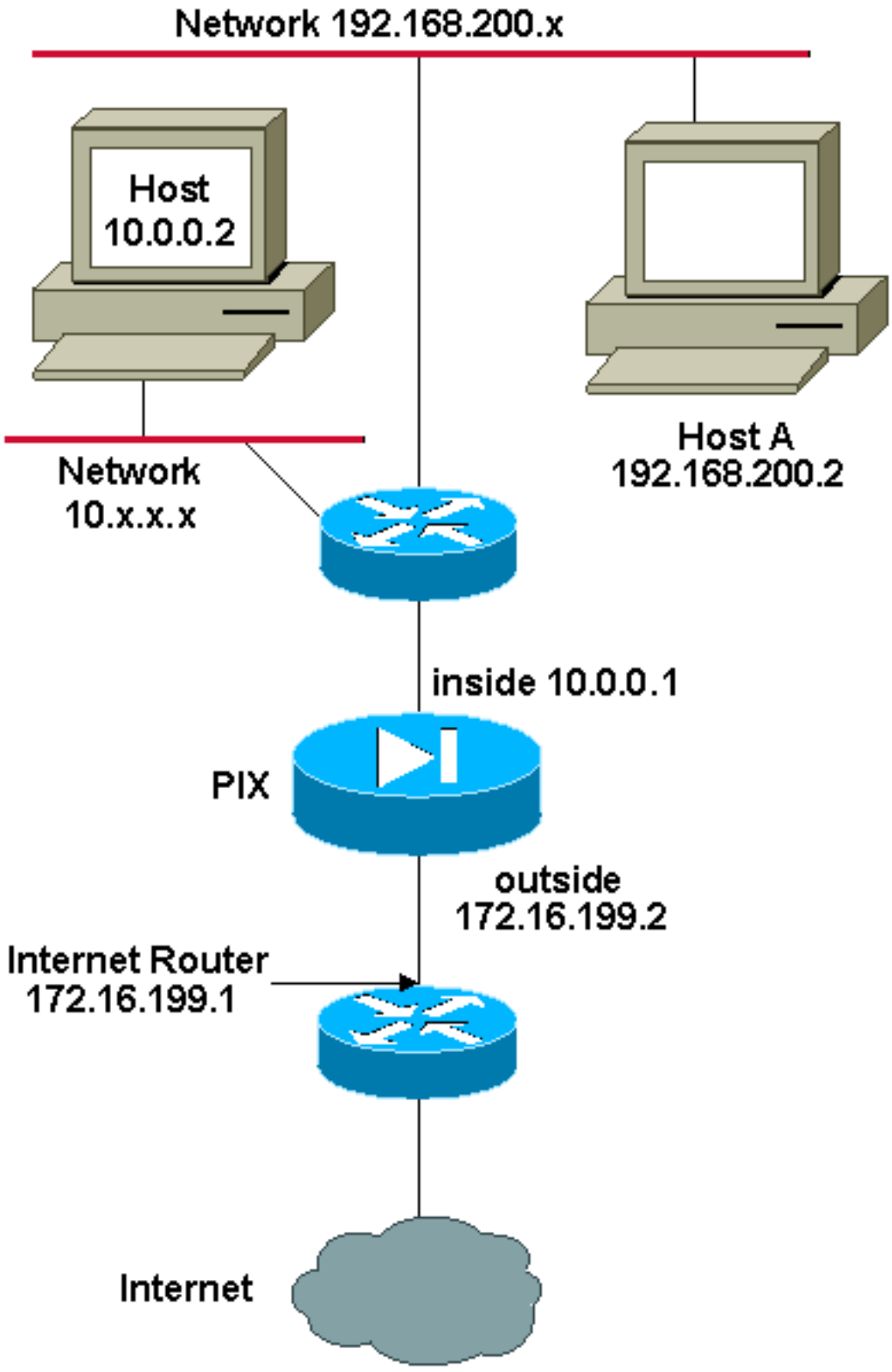
Con **nat-control** invalidado, el PIX/ASA reenvía los paquetes de una interfaz de la alta seguridad más baja sin una entrada de traducción específica en la configuración. Para pasar el tráfico de una interfaz de seguridad más baja a una de seguridad más alta, use las listas de acceso para

permitir el tráfico. El PIX/ASA entonces reenvía el tráfico. Este documento se centra en el comportamiento del dispositivo de seguridad de PIX/ASA con el comando **nat-control** habilitado.

Nota: Si desea quitar o invalidar la sentencia nat-control en el PIX/ASA, debe quitar todas las sentencias NAT del dispositivo de seguridad. En general debe quitar el NAT antes de apagar el control NAT. Debe configurar de nuevo la sentencia NAT en el PIX/ASA para que funcione según lo esperado.

Múltiples sentencias de NAT con NAT 0

Diagrama de la red



Nota: 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.

En este ejemplo, el ISP proporciona el administrador de la red con un rango de direcciones de 172.16.199.1 a 172.16.199.63. El administrador de la red decide asignar 172.16.199.1 a la interfaz interior en el router de Internet y 172.16.199.2 a la interfaz exterior del PIX/ASA.

El administrador de la red ya tienen una dirección de la clase C asignada a la red, 192.168.200.0/24, y tiene algunas estaciones de trabajo que utilizan estas direcciones para

acceder a Internet. Estas estaciones de trabajo no son direcciones traducidas. Sin embargo, las estaciones de trabajo nuevas reciben direcciones en la red 10.0.0.0/8, y deben ser traducidas.

Para adaptar este diseño de red, el administrador de la red debe utilizar dos sentencias NAT y un pool global en la configuración PIX/ASA mientras que esta salida muestra:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

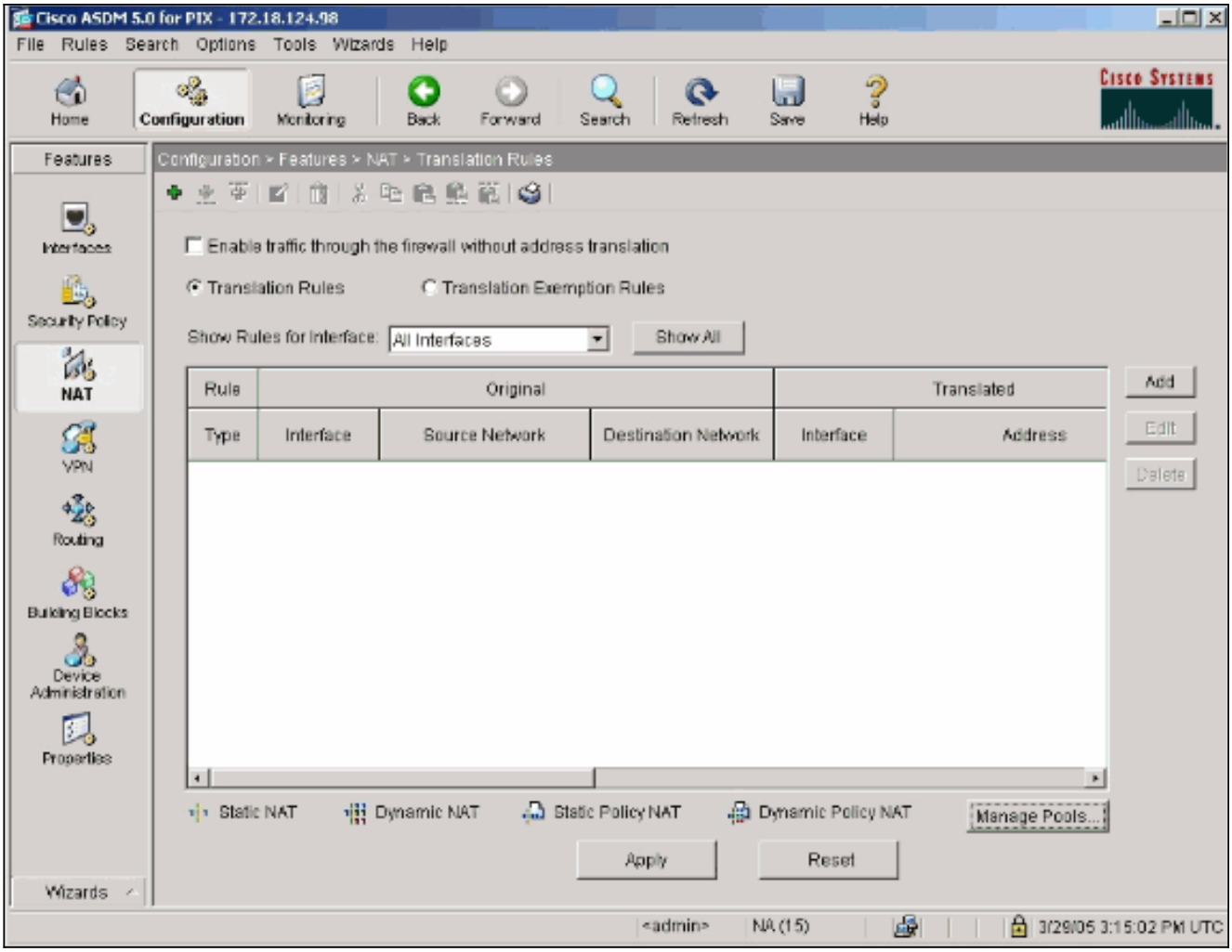
Esta configuración no traduce a la dirección de origen de ningún tráfico saliente de la red 192.168.200.0/24. Traduce a una dirección de origen en la red 10.0.0.0/8 a una dirección del rango 172.16.199.3 a 172.16.199.62.

Estos pasos proporcionan una explicación de cómo aplicar esta misma configuración con el uso del administrador de Adaptive Security Device Manager (ASDM).

Nota: Realice todos los cambios en las configuraciones con el CLI o ASDM. El uso de CLI y de ASDM para los cambios de configuraciones provoca una conducta muy errática en cuanto a lo aplicado por ASDM. Esto no es un bug, pero se produce debido al funcionamiento de ASDM.

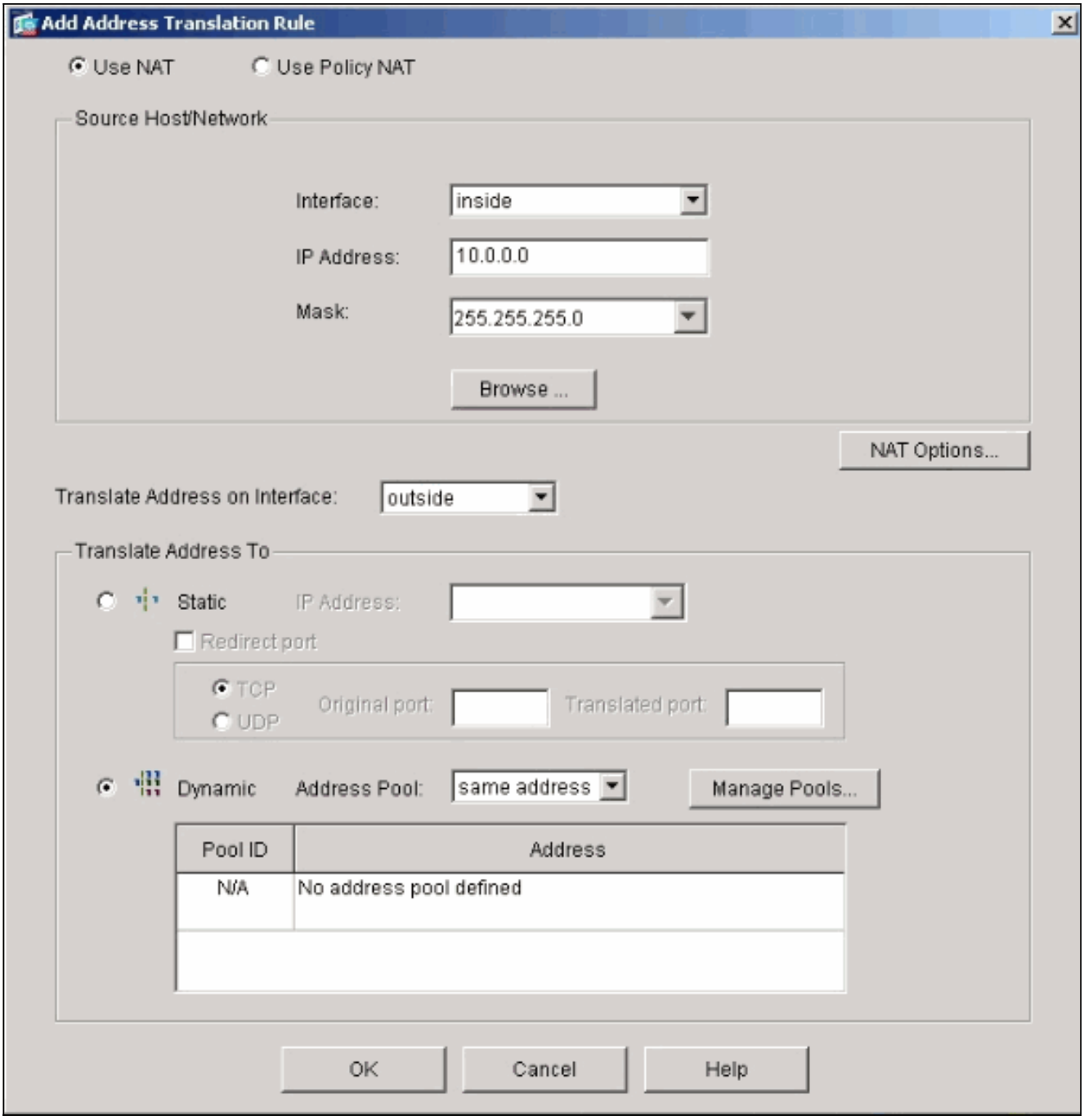
Nota: Cuando abre el ASDM, importa la configuración actual de PIX/ASA y funciona desde esa configuración cuando realiza y aplica los cambios. Si un cambio se realiza en el PIX/ASA con la sesión ASDM abierta, el ASDM ya no funciona con lo que considera que es la configuración actual de PIX/ASA. Asegúrese de cerrar todas las sesiones ASDM si realiza cambios en las configuraciones a través de CLI. Abre otra vez el ASDM cuando desee trabajar a través de GUI.

1. Inicie el ASDM, busque la pestaña Configuration, y haga clic en **NAT**.
2. Haga clic en **Agregar** para crear una nueva regla.

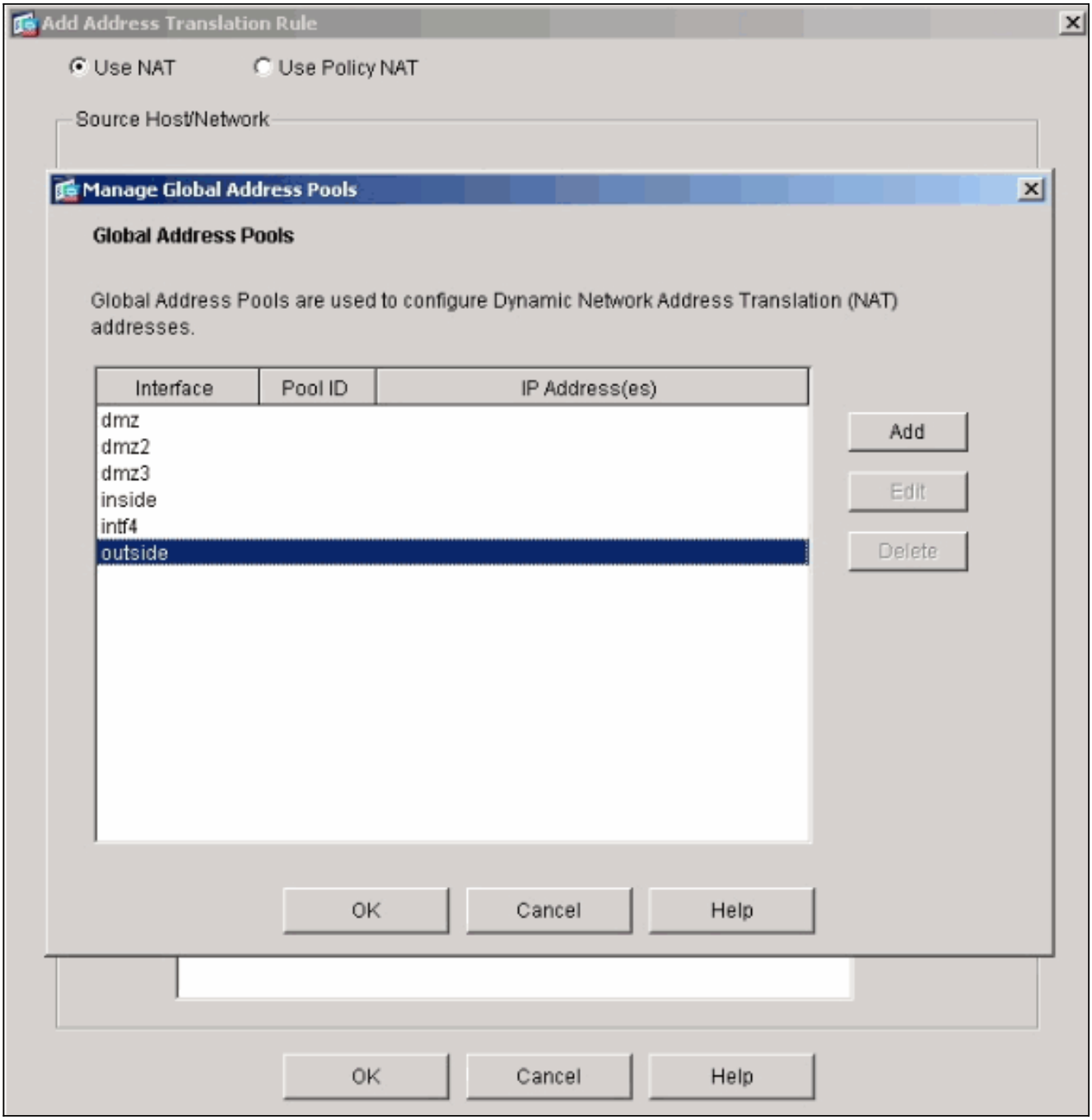


Una nueva ventana aparece que permite que el usuario cambie las opciones NAT para esta entrada de NAT. Por este ejemplo, realice los paquetes NAT que llegan en la interfaz interior que proviene de la red específica 10.0.0.0/24.El PIX/ASA traduce estos paquetes a un pool de IP dinámica en la interfaz exterior. Después de que ingrese la información que describe qué tráfico a NAT, defina un pool de las direcciones IP para el tráfico traducido.

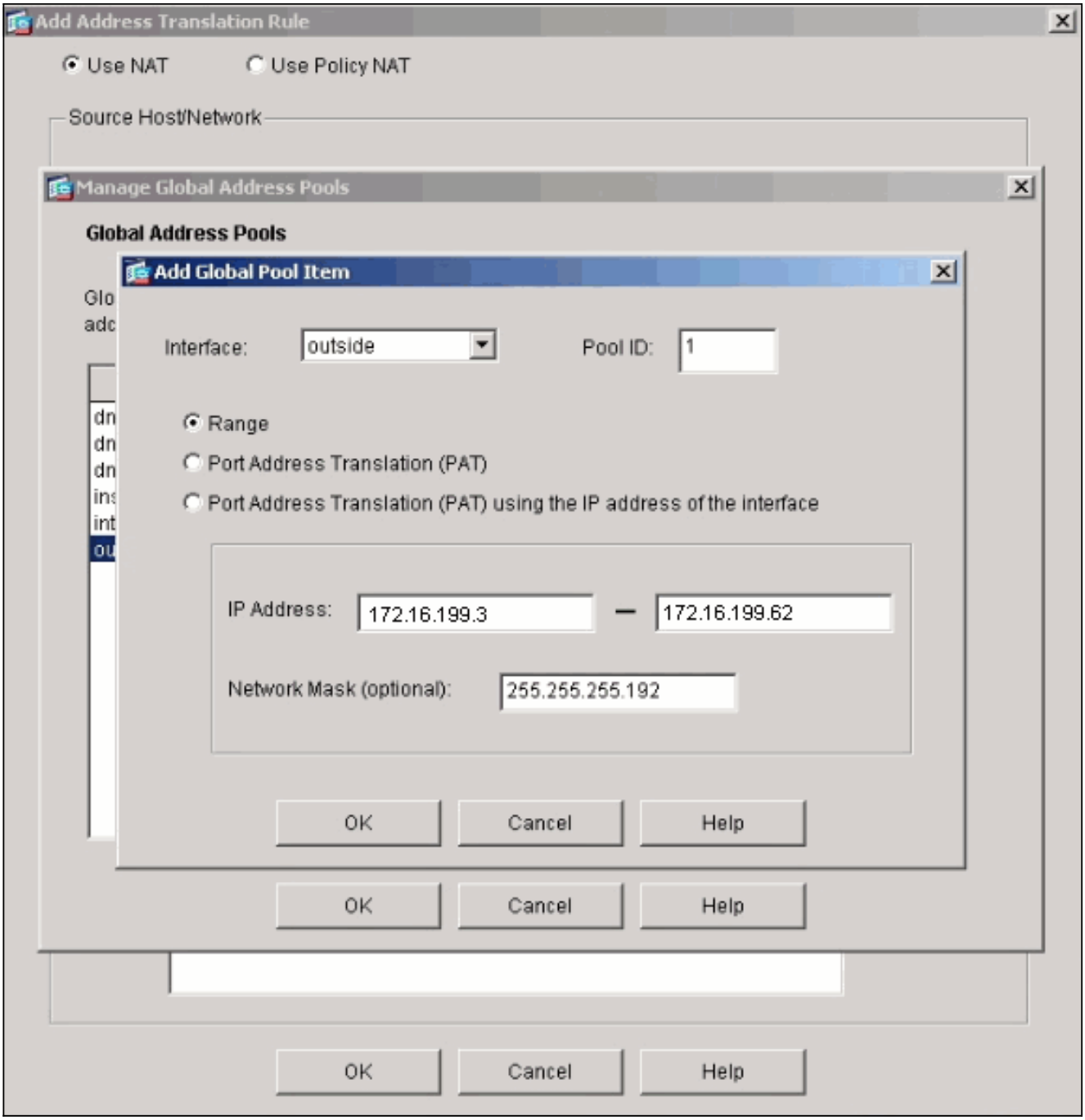
3. Haga clic en**Administrar los pools** para agregar un nuevo pool IP.



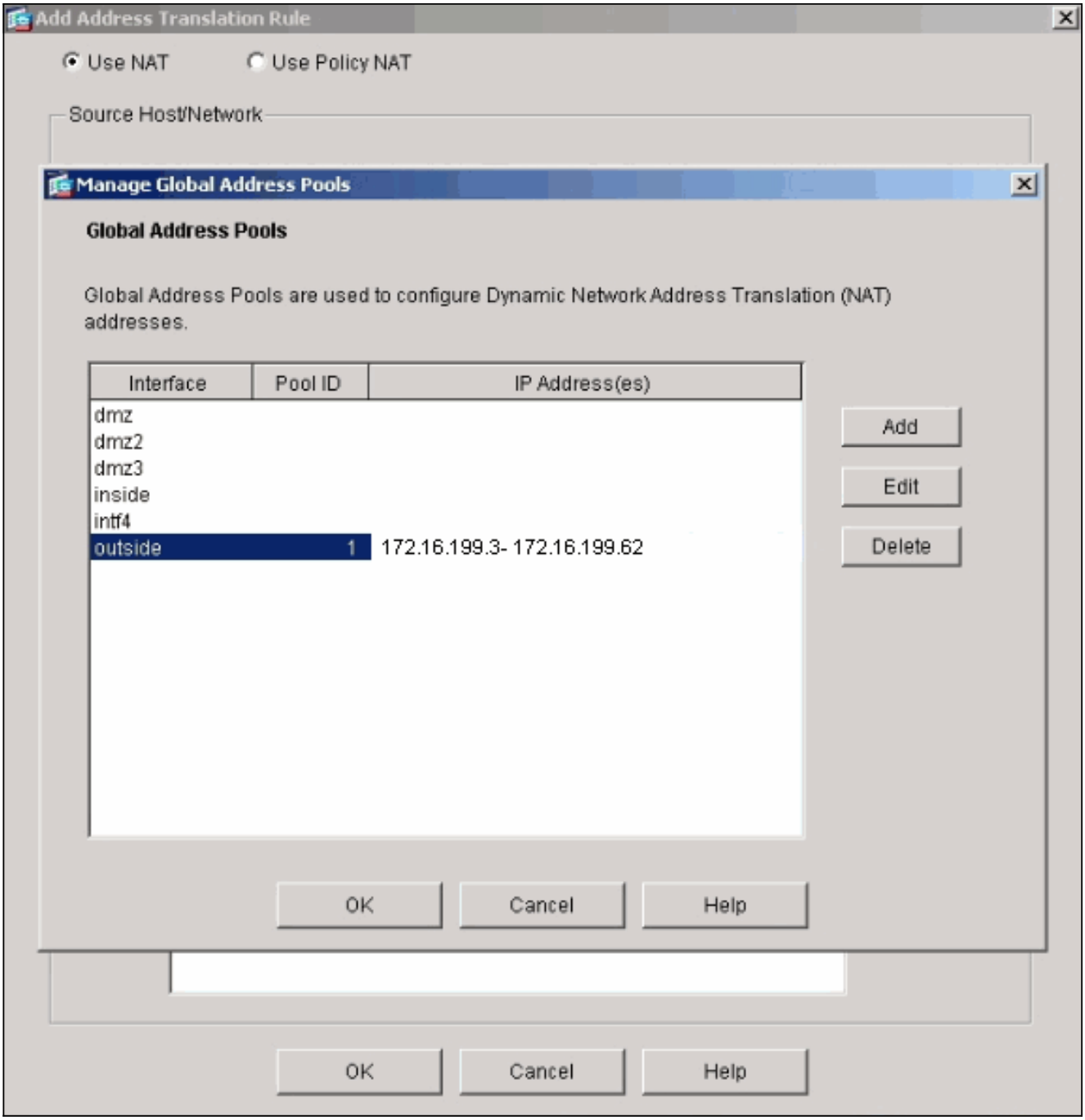
4. Elija **hacia el exterior**, y haga clic en Agregar



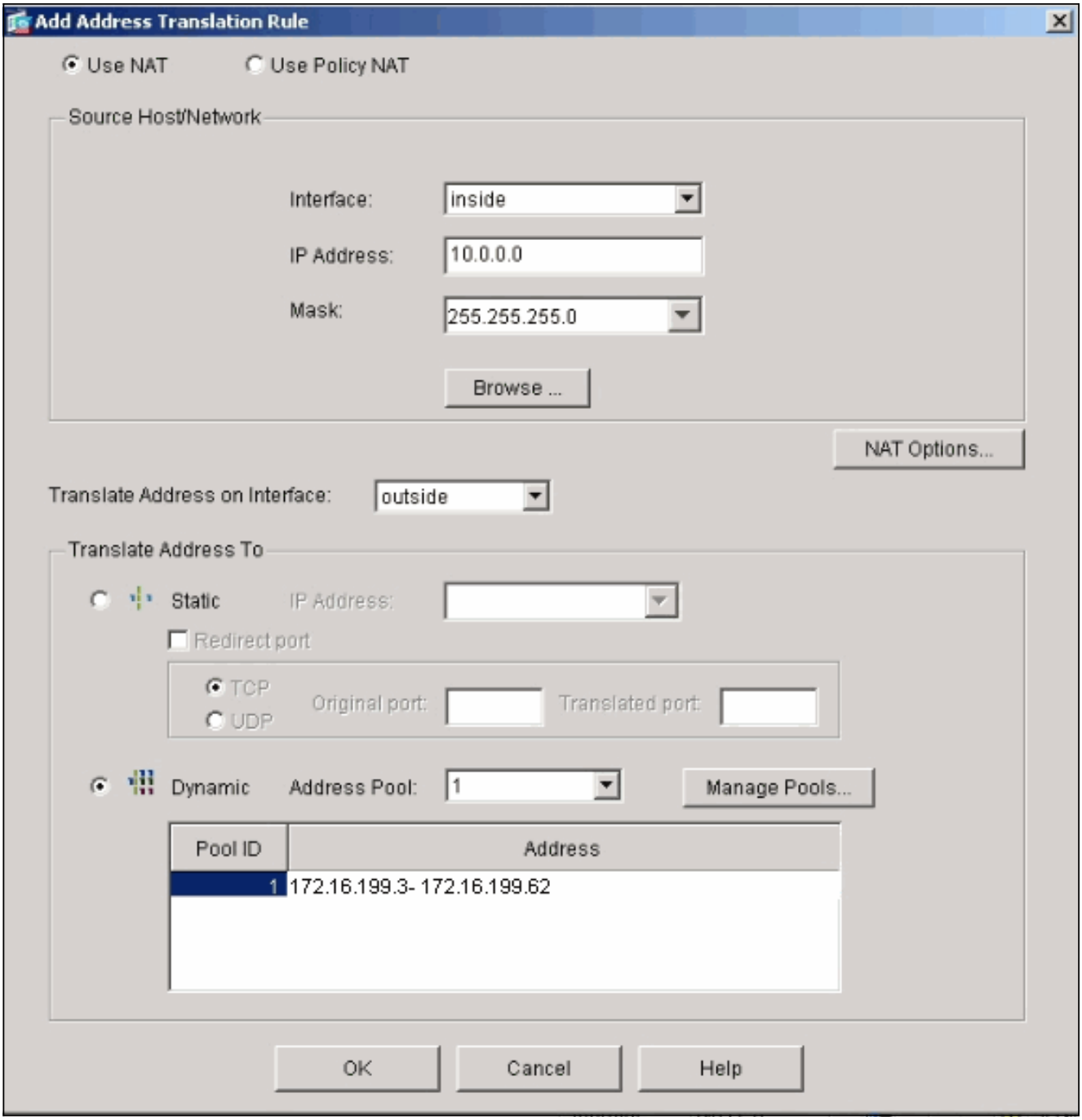
5. Especifique el rango de IP para el pool, y proporcione a pool un número de ID entero exclusivo.



6. Ingrese los valores adecuados, y haga clic en **Aceptar**.El nuevo pool se define para la interfaz
exterior.

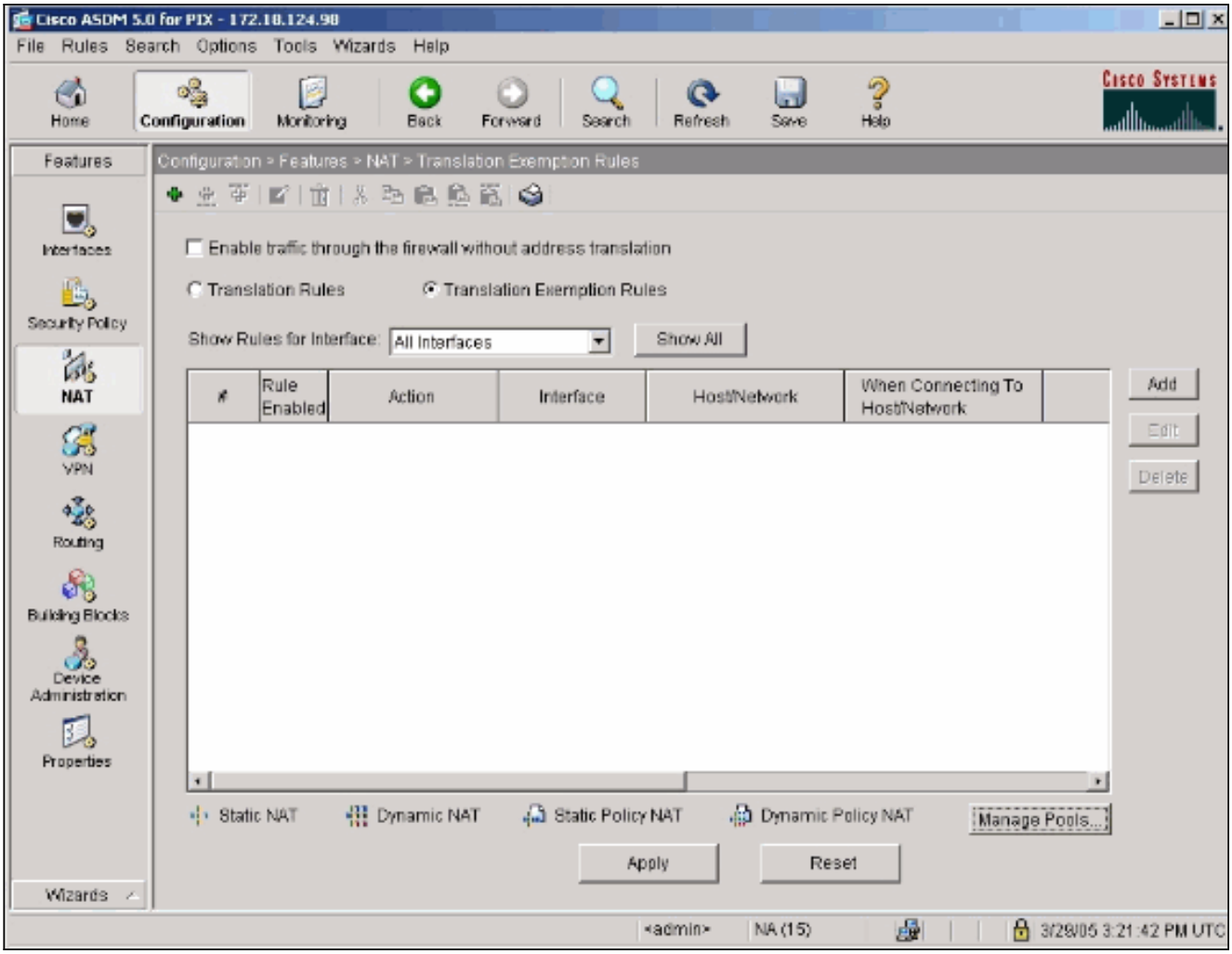


7. Después de que defina el pool, haga clic en **Aceptar** para volver a la ventana de configuración de la regla NAT.Asegúrese de elegir el pool correcto que acaba de crear conforme a la lista desplegable del Pool de Direcciones.

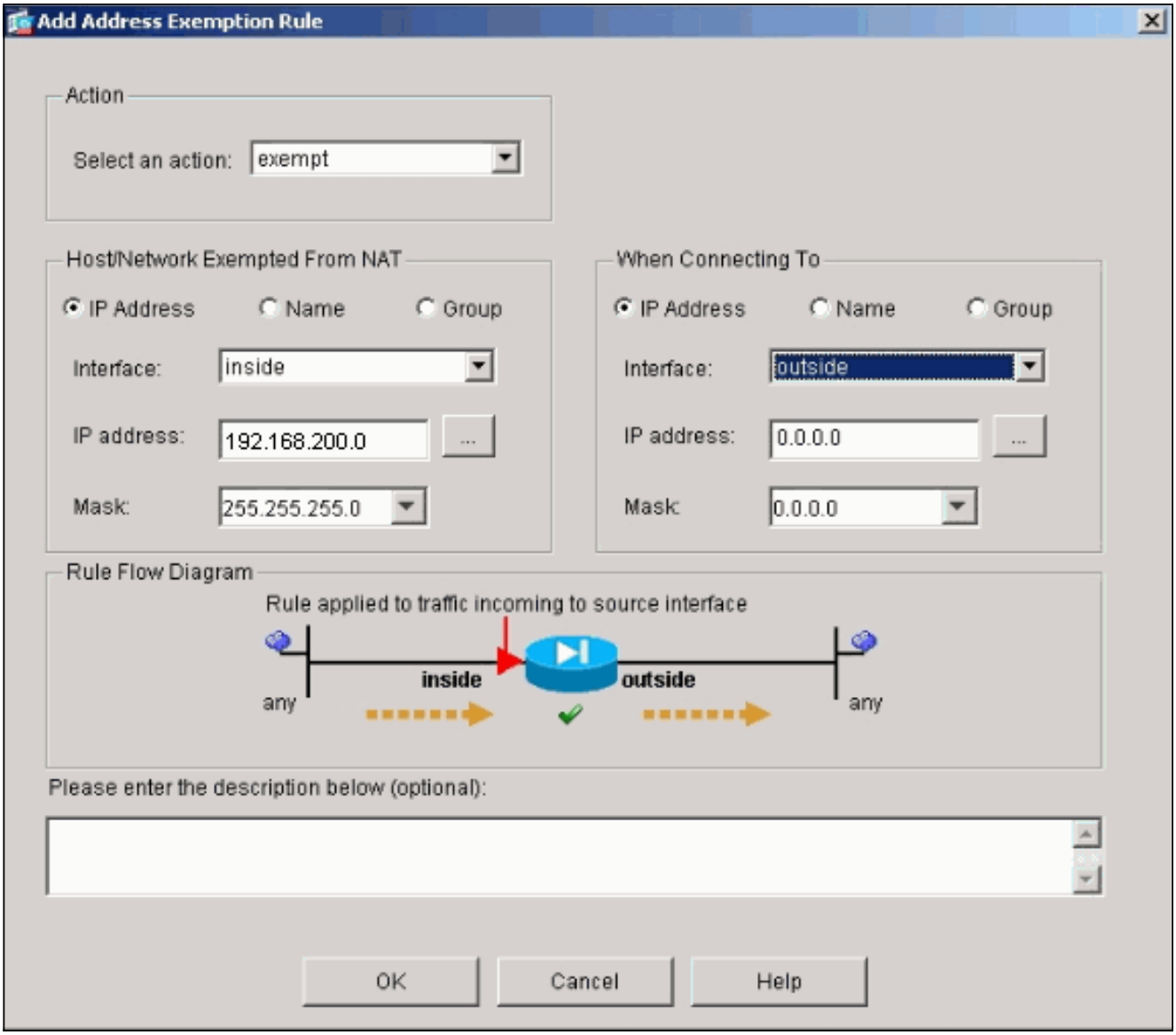


Ahora ha creado una traducción de NAT a través del dispositivo de seguridad. Sin embargo, todavía necesita crear la entrada de NAT que especifica qué tráfico no será traducido con NAT.

8. Haga clic en las **Reglas de la Exención de la Traducción** situadas en la parte superior de la ventana, y después haga clic **Agregar** para crear una nueva regla.



9. Elija la *interfaz interior* como la fuente, y especifique la subred **192.168.200.0/24**. Deje los valores predeterminados de "Durante la conexión".



Las reglas NAT ahora se definen.

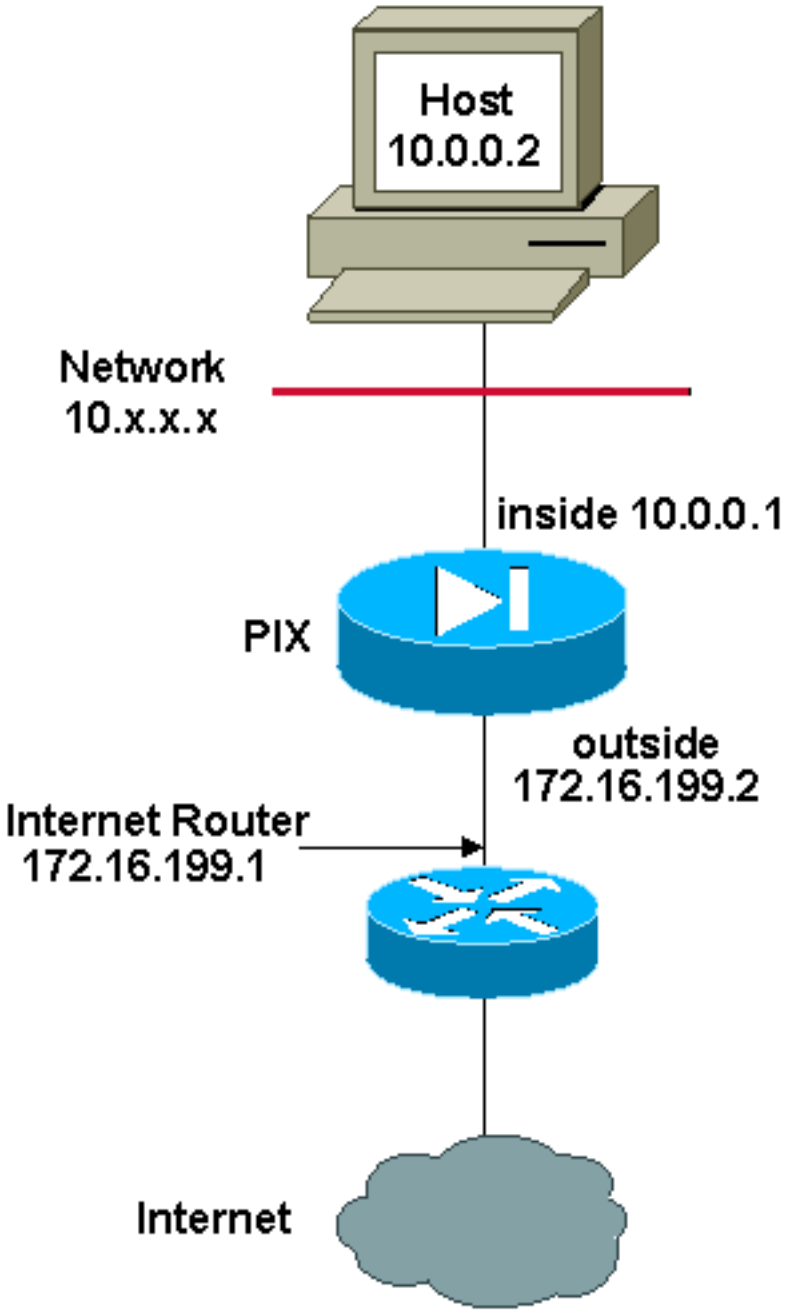
10. Haga clic en **Aplicar** para aplicar los cambios a la configuración actual de ejecución del dispositivo de seguridad.Esta salida muestra los agregados reales que se aplican a la configuración del PIX/ASA. Son levemente diferentes de los comandos ingresados con el método manual, pero son iguales.`access-list inside_nat0_outbound extended permit ip 192.168.200.0 255.255.255.0 any`

    `global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192`

    `nat (inside) 0 access-list inside_nat0_outbound`
    `nat (inside) 1 10.0.0.0 255.255.255.0`

Conjuntos globales múltiples

Diagrama de la red



Nota: 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.

En este ejemplo, el administrador de la red tiene dos rangos de direcciones IP que se registran en el Internet. El administrador de la red debe convertir todas las direcciones internas, que están en el rango 10.0.0.0/8, en direcciones registradas. Los rangos de las direcciones IP que el administrador de la red debe utilizar son 172.16.199.1 con 172.16.199.62 y 192.168.150.1 a 192.168.150.254. El administrador de la red puede hacer esto con:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

En el NAT dinámico, la sentencia más específica es la que tiene prioridad cuando utiliza la misma interfaz en global.

```
nat (inside) 1 10.0.0.0 255.0.0.0
```

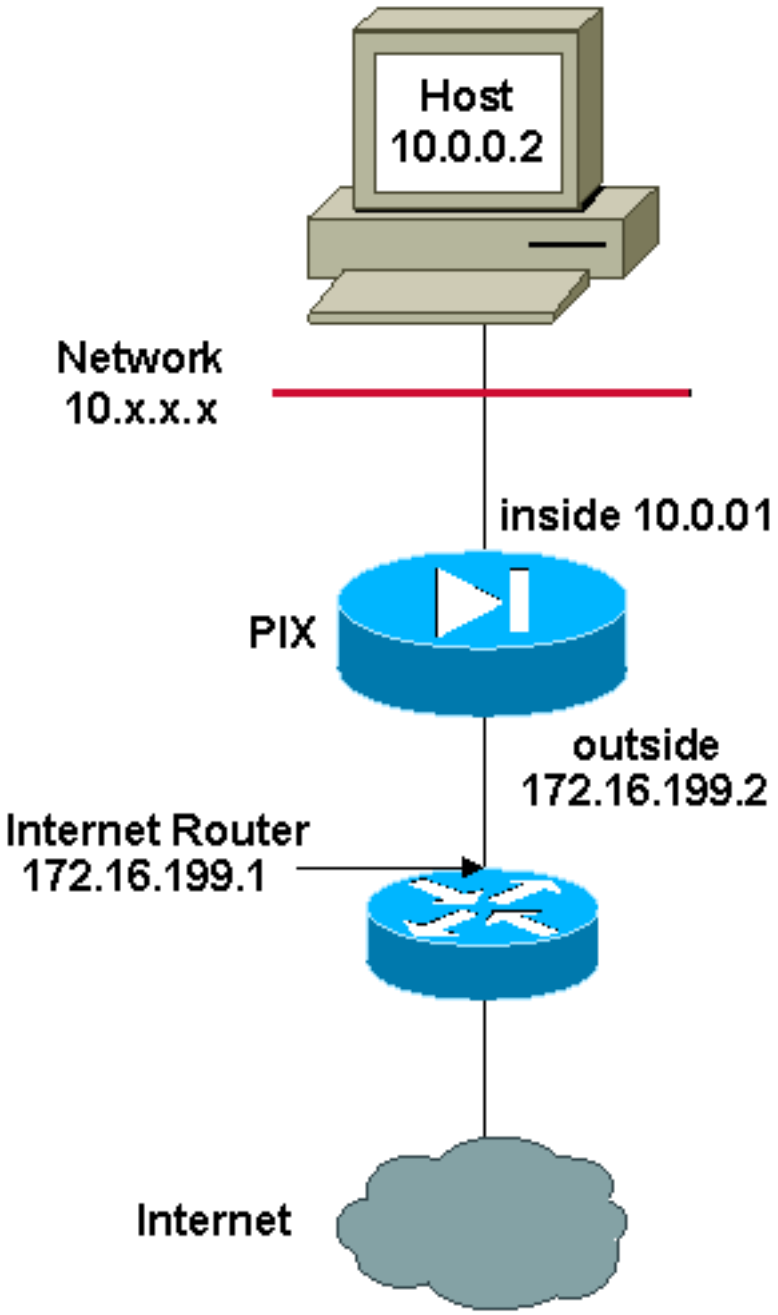
```
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Si tiene la red interna como 10.1.0.0, la NAT global 2 tiene prioridad sobre la 1 ya que es más específica para la traducción.

Nota: Un esquema de direccionamiento comodín se utiliza en la sentencia NAT. Esta sentencia le ordena al PIX/ASA traducir cualquier dirección de origen interna cuando sale de Internet. La dirección de este comando puede ser más específica si se lo desea.

Sentencias NAT y PAT Globales Mixtas

Diagrama de la red



Nota: 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.

En este ejemplo, el ISP proporciona al administrador de la red un rango de direcciones de 172.16.199.1 con 172.16.199.63 para el uso de la compañía. El administrador de la red decide utilizar 172.16.199.1 para la interfaz interior en el router de Internet y 172.16.199.2 para la interfaz exterior en el PIX/ASA. Le queda 172.16.199.3 a 172.16.199.62 para utilizar para el pool de NAT. Sin embargo, el administrador de la red sabe que, en cualquier momento, puede haber más de sesenta personas intentanto salir dePIX/ASA. Por lo tanto, el administrador de la red decide tomar 172.16.199.62 y convertirla en una dirección PAT de modo que los usuarios múltiples puedan compartir una dirección al mismo tiempo.

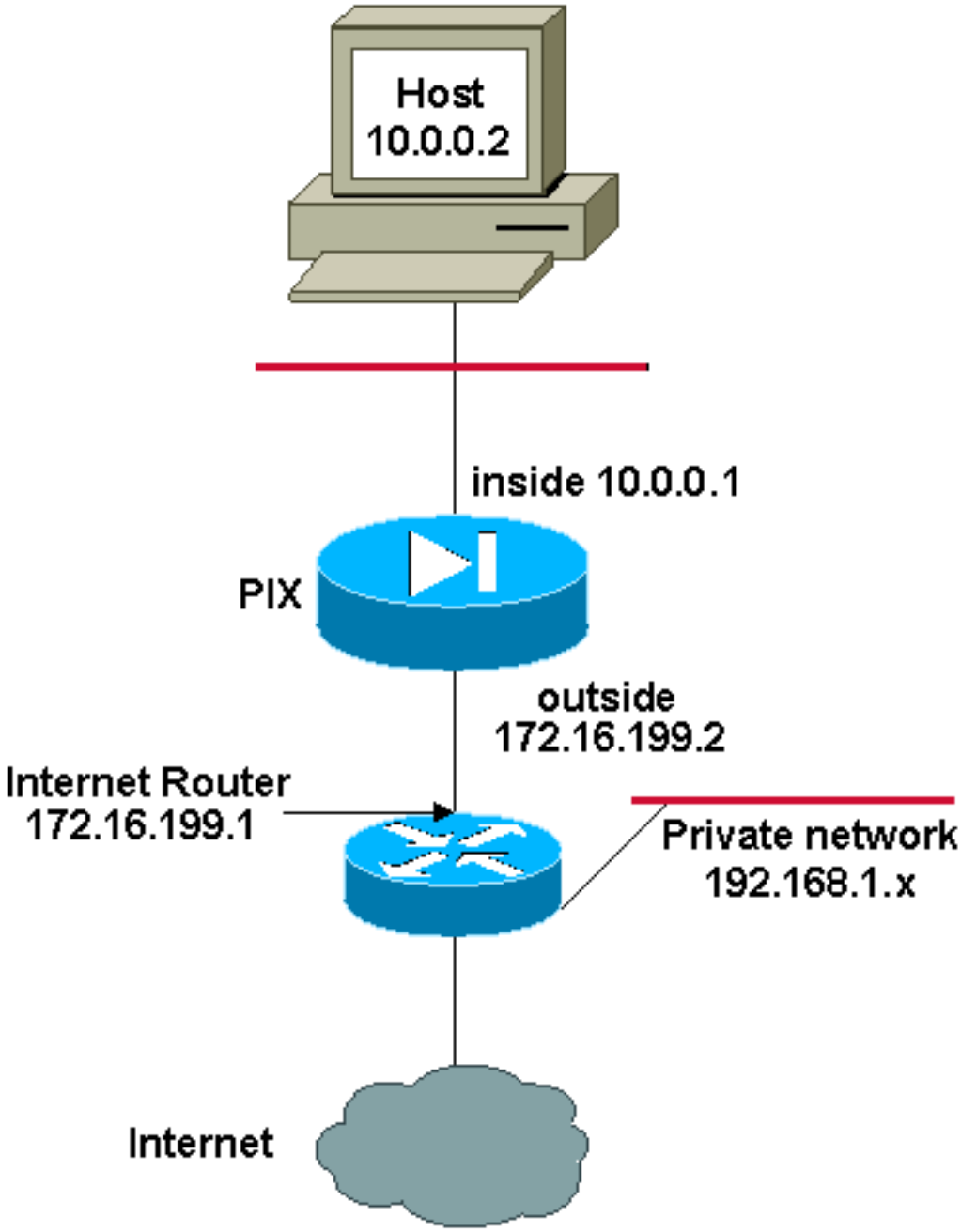
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Estos comandos dan instrucciones al PIX/ASA para traducir a la dirección de origen a 172.16.199.3 con 172.16.199.61 para que los primeros cincuenta y nueve usuarios internos pasen a través del PIX/ASA. Después de que se agoten estas direcciones, el PIX traduce todas las direcciones de origen posteriores a 172.16.199.62 hasta que una de las direcciones en el pool de NAT queda libre.

Nota: Un esquema de direccionamiento comodín se utiliza en la sentencia NAT. Esta sentencia le ordena al PIX/ASA traducir cualquier dirección de origen interna cuando sale de Internet. La dirección en este comando puede ser más específica si lo desea.

Múltiples sentencias de NAT con NAT 0 Access-List

Diagrama de la red



Nota: 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.

En este ejemplo, el ISP proporciona al administrador de la red un rango de direcciones de 172.16.199.1 a 172.16.199.63. El administrador de la red decide asignar 172.16.199.1 a la interfaz interior en el router de Internet y 172.16.199.2 a la interfaz exterior del PIX/ASA.

Sin embargo, en este escenario otro segmento de LAN privado se coloca fuera del router de Internet. El administrador de la red prefiere no usar las direcciones del pool global cuando los hosts de estas dos redes se comunican. El administrador de la red todavía necesita traducir a la dirección de origen para todos los usuarios internos (10.0.0.0/8) cuando salen a Internet.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list 101
```

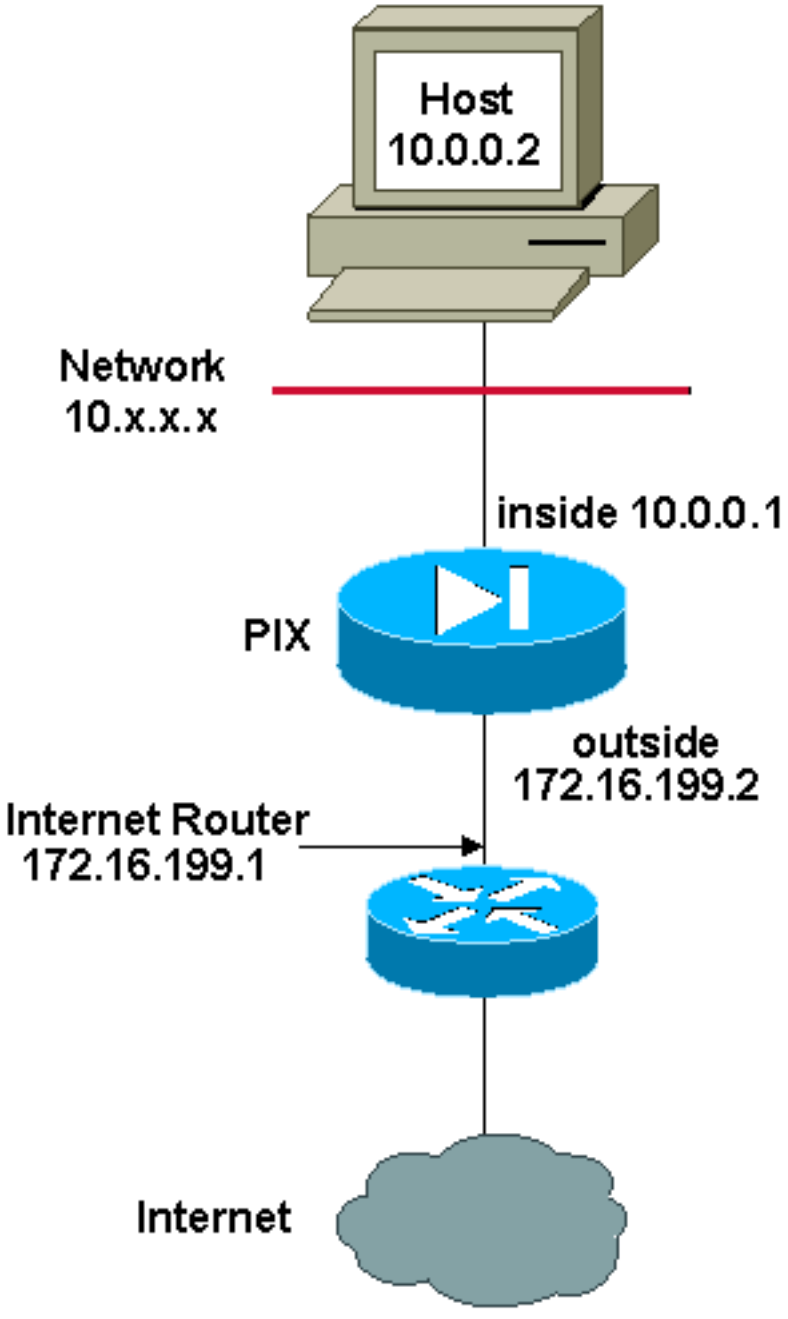
```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Esta configuración no traduce las direcciones con una dirección de origen de 10.0.0.0/8 y una dirección de destino de 192.168.1.0/24. Traduce la dirección de origen de cualquier tráfico iniciado dentro de la red 10.0.0.0/8 y destinado para cualquier lugar con excepción de 192.168.1.0/24 en una dirección del rango 172.16.199.3 con 172.16.199.62.

Si tiene la salida de un comando **write terminal** de su dispositivo Cisco, puede utilizar Output Interpreter Tool (**clientes registrados solamente**).

Utilice la Política NAT

Diagrama de la red



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

Cuando utiliza una lista de acceso con el comando **nat** para cualquier ID de NAT con excepción de 0, debe habilitar la política NAT.

Nota: La política NAT fue introducida en la versión 6.3.2.

La política NAT permite que identifique el tráfico local para la traducción de la dirección cuando especifica las direcciones de origen y de destino (o los puertos) en una lista de acceso. El NAT habitual utiliza las direcciones de origen/los puertos solamente, mientras que la política NAT utiliza las direcciones de origen y de destino/los puertos.

Nota: Todos los tipos de política de soporte NAT a excepción de la exención de NAT (**nat 0 access-list**). La exención de NAT utiliza una lista de control de acceso para identificar las direcciones locales, pero difiere de la política NAT en la que los puertos no están considerados.

Con la política NAT, puede crear múltiple NAT o sentencias estáticas que identifican la misma dirección local siempre que las combinaciones origen /puerto y destino /puerto sean únicas para cada sentencia. Puede hacer coincidir diversas direcciones globales a cada par origen /puerto y destino /puerto.

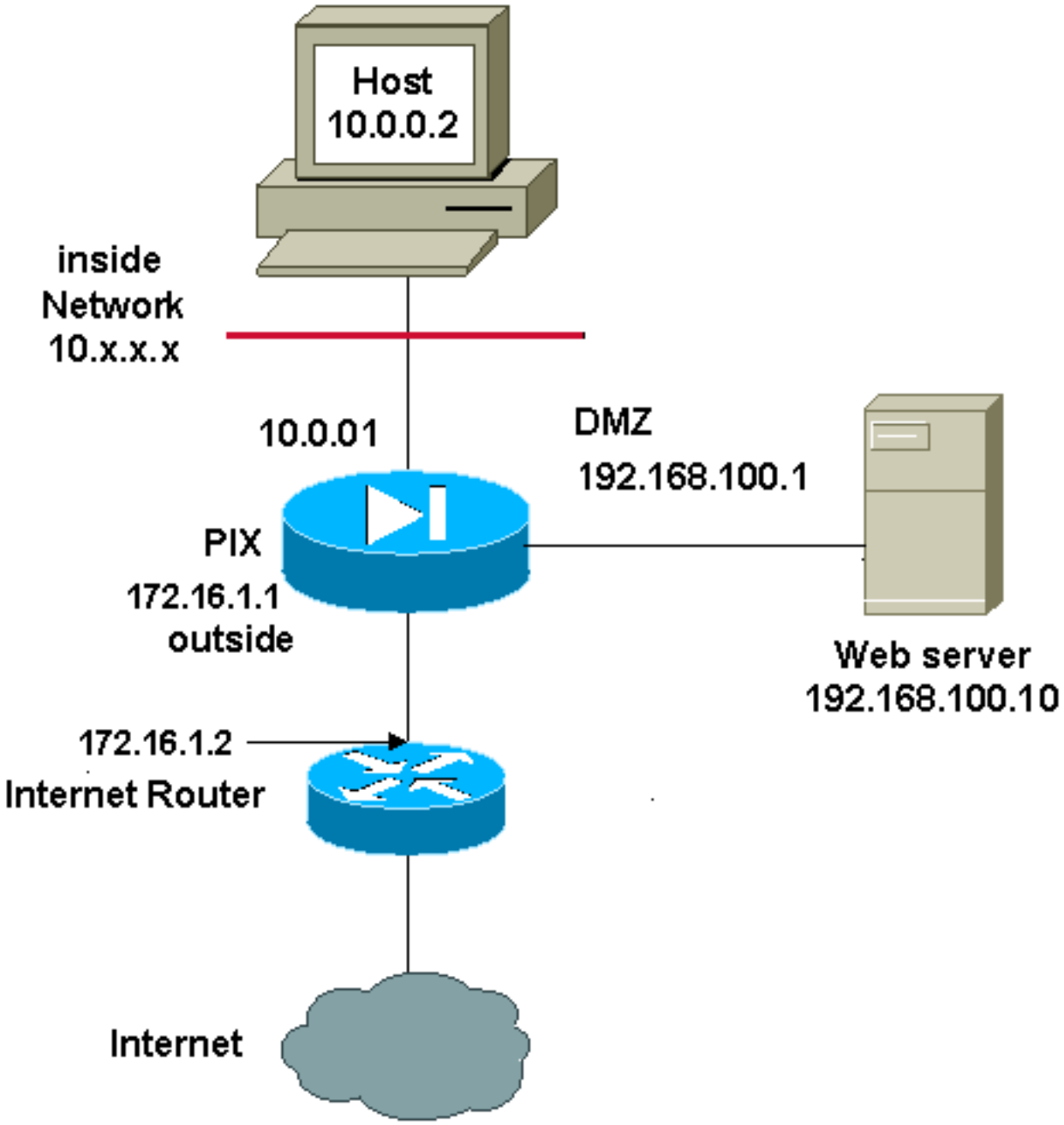
En este ejemplo, el administrador de la red proporciona el acceso para la dirección IP de destino 192.168.201.11 para el puerto 80 (Web) y el puerto 23 (telnet), pero debe utilizar dos direcciones IP de destino como dirección de origen. La dirección IP 172.16.199.3 se usa la dirección de origen para la web. La dirección IP 172.16.199.4 se usa para Telnet, y debe convertir todas las direcciones internas, que son se encuentran dentro del rango 10.0.0.0/8. El administrador de la red puede hacer esto con:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Puede utilizar la Output Interpreter Tool (clientes registrados solamente) para visualizar los problemas potenciales y las soluciones.

NAT estática

Diagrama de la red



Nota: 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.

Una configuración NAT estática crea un mapping uno a uno y traduce a una dirección específica a otra dirección. Este tipo de configuración crea una entrada permanente en la tabla NAT siempre que la configuración esté presente y habilita los hosts internos y externos para iniciar la conexión. Esto es sobre todo útil para los hosts que proporcionan los servicios de aplicación como el correo, la Web, el FTP y otros. En este ejemplo, las sentencias de NAT estática se configuran para permitir que los usuarios en el interior y los usuarios en el exterior accedan al servidor Web en el DMZ.

Esta salida muestra cómo se construye una sentencia estática. Observe la solicitud de las direccionesIP reales y mapeadas.

`static (`*`real_interface`*`,`*`mapped_interface`*`) `*`mapped_ip real_ip`* `netmask `*`mask`*

Aquí se encuentra la traducción estática creada para proporcionar a los usuarios en la interfaz

interna acceso al servidor en la DMZ. Crea un mapping entre una dirección en el interior y la dirección del servidor en la DMZ. Los usuarios en el interior pueden acceder al servidor en la DMZ a través de la dirección interna.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

La siguiente es la traducción estática creada para proporcionar a los usuarios en acceso de la interfaz exterior al servidor en la DMZ. Crea un mapping entre una dirección en el exterior y la dirección del servidor en la DMZ. Los usuarios en el exterior pueden acceder el servidor en la DMZ vía la dirección externa.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

Nota: Debido a que la interfaz exterior tiene un nivel de seguridad más bajo que la DMZ, también debe crearse una lista de acceso para permitir a los usuarios de afuera acceso al servidor DMZ. La lista de acceso debe garantizar a los usuarios el acceso la **dirección mapeada** en la traducción estática. Se recomienda que esta lista de acceso es lo más específica posible. En este caso, a cualquier host se le permite acceso solamente a los puertos 80 (WWW/HTTP) y 443 (https) en el servidor Web.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

La lista de acceso se debe aplicar a la interfaz exterior.

```
access-group OUTSIDE in interface outside
```

Consulte access-list extended y access-group para obtener más información sobre los comandos **access-list** y **access-group** .

Cómo Evitar NAT

Esta sección describe cómo desviar el NAT. Quizá desee desviar el NAT cuando habilite el control NAT. Puede utilizar la identidad NAT, la identidad estática NAT, o la exención de NAT para desviar el NAT.

Configure Identificación NAT

La identidad NAT traduce la dirección IP real a la misma dirección IP. Solamente los hosts “traducidos” pueden crear las traducciones de NAT, y se permite el tráfico de respuesta nuevamente.

Nota: Si cambia la configuración del NAT, y no desea esperar las traducciones existentes para medir el tiempo hacia fuera antes de que se utilice la nueva información NAT, use el comando **clear xlate** para borrar la tabla de traducción. Sin embargo, todas las conexiones actuales que utilizan las traducciones son desconectadas cuando borra la tabla de traducción.

Para configurar la identidad NAT, ingrese este comando:

```
hostname(config)#nat (real_interface) 0 real_ip [mask [dns] [outside] [norandomseq] [[tcp]
tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

Por ejemplo, para utilizar la identidad NAT para la red del interior 10.1.1.0/24, ingrese este comando:

```
hostname(config)#nat (inside) 0 10.1.1.0 255.255.255.0
```

Consulte Cisco Security Appliance Command Reference, versión 7.2 para más información sobre

el comando **nat**.

Configure Identificación Estática NAT

La identidad estática NAT traduce la dirección IP real a la misma dirección IP. La traducción está siempre activa, y los hosts “traducidos” y host remotos pueden originar las conexiones. La identidad estática NAT le permite usar NAT habitual o la política NAT. La política NAT lo deja identificar las direcciones de destino al determinar las direcciones reales para traducir (consulte la sección de la política NAT del uso para más información sobre la política NAT). Por ejemplo, puede utilizar la identidad estática NAT de la política para una dirección interna cuando acceda a la interfaz exterior y el destino es el servidor A, sino utilizar una traducción normal al acceder el servidor exterior B.

Nota: Si quita un comando estático, las conexiones actuales que utilizan la traducción no son afectadas. Para quitar estas conexiones, ingrese el comando **clear local-host**. No puede borrar traducciones estáticas desde la tabla de traducción con el comando **clear xlate**; debe quitar el comando static en lugar de otro. Solamente las traducciones dinámicas creadas por los comandos nat y global se pueden quitar con el comando clear xlate.

Para configurar la identidad estática NAT de la política, ingrese este comando:

```
hostname(config)#static (real_interface,mapped_interface) real_ip access-list acl_id [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

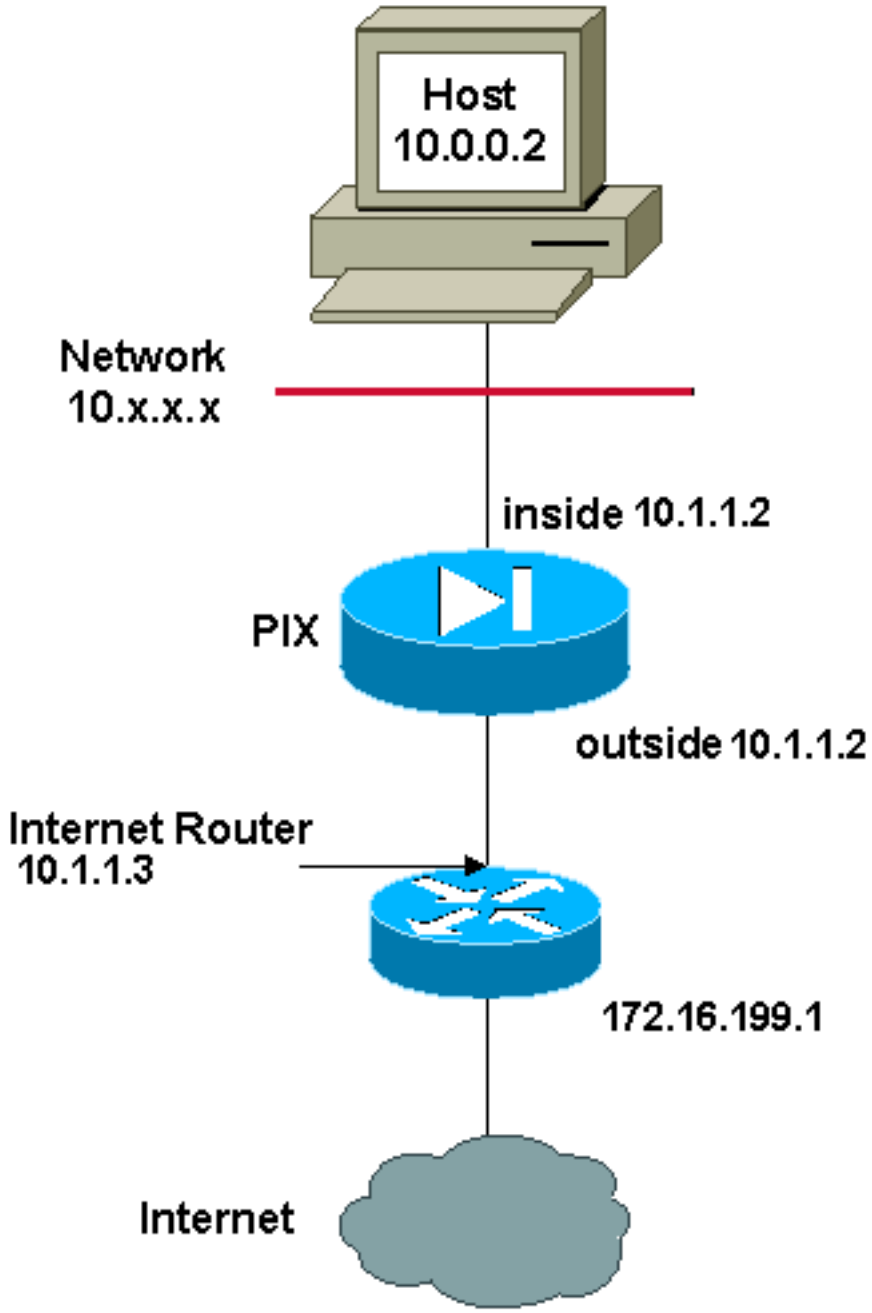
Use el comando **access-list extended** para crear la lista de acceso ampliada. Esta lista de acceso debe incluir solamente el permiso ACE. Asegúrese de que la dirección de origen en la lista de acceso coincida con real_ip en este comando. La política NAT no considera las palabras claves inactivas o el rango de tiempo; todos los ACE se consideran activos para la configuración del NAT de la política. Consulte sección Uso de la política NAT para más información.

Para configurar la identidad estática regular NAT, ingrese este comando:

```
hostname(config)#static (real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

Especifique la misma dirección IP para ambos argumentos de real_ip.

Diagrama de la red



Nota: 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.

Por ejemplo, este comando utiliza la identidad estática NAT para una dirección IP interior (10.1.1.2) al acceder por el exterior:

```
hostname(config)#static (inside,outside) 10.1.1.2 10.1.1.2 netmask 255.255.255.255
```

Consulte Cisco Security Appliance Command Reference, versión 7.2 para más información sobre el comando **static**.

Este comando utiliza la identidad estática NAT para una dirección externa (172.16.199.1) al acceder por el interior:

```
hostname(config)#static (outside,inside) 172.16.199.1 172.16.199.1 netmask 255.255.255.255
```

Este comando mapea estáticamente una subred completa:

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2 netmask 255.255.255.0
```

Este ejemplo de NAT estático de la política de identidad muestra una sola dirección real que utiliza la identidad NAT al acceder a una dirección de destino y una traducción al acceder a otra:

```
hostname(config)#access-list NET1 permit ip host 10.1.1.3 172.16.199.0 255.255.255.224
hostname(config)#access-list NET2 permit ip host 10.1.1.3 172.16.199.224 255.255.255.224
hostname(config)#static (inside,outside) 10.1.1.3 access-list NET1 hostname(config)#static
(inside,outside) 172.16.199.1 access-list NET2
```

Nota: Para más información sobre el comando **static**, consulte la CiscoASA 5580 Adaptive Security Appliance Command Reference, versión 8.1.

Nota: Para más información sobre las listas de acceso, consulte Cisco ASA 5580 Adaptive Security Appliance Command LineConfiguration Guide versión 8.1.

Configure Exención de NAT

La exención de NAT exime las direcciones de la traducción y permite que loshost remotos los reales originen las conexiones. La exención de NAT le permite especificar las direcciones de destino al determinar el tráfico real para eximir (similar a la política NAT), por lo que tiene un mayor control usando la exención de NAT que la identidad NAT. Sin embargo a diferencia de la política NAT, la exención de NAT no considera los puertos en la lista de acceso. Utiliza la identidad estática NAT para considerar los puertos en la lista de acceso.

Nota: Si quita una configuración de la exención de NAT, las conexiones existentes que utilizan la exención de NAT no son afectadas. Para quitar estas conexiones, ingrese el comando clear host local.

Para configurar la exención de NAT, ingrese este comando:

```
hostname(config)#nat (real_interface) 0 access-list acl_name [outside]
```

Cree la lista de acceso ampliada usando el comando **access-list extended**. Esta lista de acceso puede incluir el permiso ACE y negar los ACE. No especifique los puertos reales y de destino en la lista de acceso; La exención de NAT no considera los puertos. La exención de NAT tampoco considera las palabras claves inactivas o el rango de tiempo; Los ACE se consideran activos para la configuración de la exención de NAT.

De forma predeterminada, este comando exime el tráfico desde adentro al exterior. Si desea que el tráfico del exterior al interior desvía el NAT, después agregue el comando adicional **nat** e ingrese afuera para identificar el caso NAT como NAT exterior. Quizá desee utilizar la exención de NAT exterior si configura el NAT dinámico para la interfaz exterior y desea eximir el otro tráfico.

Por ejemplo, para eximir una red interna al acceder a cualquier dirección de destino, ingrese este comando:

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0 255.255.255.0 any hostname(config)#nat
(inside) 0 access-list EXEMPT
```

Para utilizar el NAT exterior dinámico para una red DMZ, y eximir otra red DMZ, ingrese este comando:

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0 outside dns hostname(config)#global
(inside) 1 10.1.1.2 hostname(config)#access-list EXEMPT permit ip 10.1.1.0 255.255.255.0 any
hostname(config)#nat (dmz) 0 access-list EXEMPT
```

Para eximir a una dirección interna al acceder a dos direcciones de destino diferentes, ingrese estos comandos:

```
hostname(config)#access-list NET1 permit ip 10.1.1.0 255.255.255.0 172.16.199.0 255.255.255.224
hostname(config)#access-list NET1 permit ip 10.1.1.0 255.255.255.0 172.16.199.224
255.255.255.224 hostname(config)#nat (inside) 0 access-list NET1
```

Verificación

El tráfico que fluye a través del dispositivo de seguridad por lo general se somete a NAT. Consulte PIX/ASA: Monitoreo y Troubleshooting de Problemas de Rendimiento para verificar las traducciones que están funcionando en el dispositivo de seguridad.

El comando **show del xlate count** muestra el número máximo actual de traducciones con el PIX. Una traducción es un mapping de una dirección interna a una dirección externa y puede ser un mapping uno a uno, como NAT, o un mapping de varios a uno, por ejemplo PAT. Este comando es un subgrupo del comando show xlate, que envía cada traducción a través de PIX. La salida de comando muestra las traducciones “funcionando,” que se refiere al número de traducciones activas en el PIX cuando se publica el comando; “más usado” se refiere a las traducciones máximas que se han visto en el PIX desde que fue encendido.

Troubleshooting

Mensaje de error recibido al agregar un PAT estático para el puerto 443

Problema

Usted recibe este mensaje de error cuando usted agrega un PAT estático para el puerto 443:

```
(DENTRO, AFUERA) netmask [ERROR] estático 255.255.255.255 tcp 0 de 192.168.1.87 443 de la
interfaz 443 tcp 0 UDP 0

incapaz de reservar el puerto 443 para el PAT estático

ERROR: incapaz de descargar la directiva
```

Solución

Este mensaje de error ocurre cuando el ASDM o el WEBVPN se está ejecutando en el puerto 443. Para resolver este problema, inicie sesión al Firewall, y complete uno de estos pasos:

- Para cambiar el puerto del ASDM cualquier cosa con excepción de 443, funcione con estos comandos:`ASA(config)#no http server enable ASA(config)#http server enable 8080`
- Para cambiar el puerto del WEBVPN cualquier cosa con excepción de 443, funcione con estos comandos:`ASA(config)#webvpn ASA(config-webvpn)#enable outside ASA(config-webvpn)#port 65010`

Después de que usted funcione con estos comandos, usted debe poder agregar un NAT/PAT en el puerto 443 a otro servidor. Cuando usted intenta utilizar el ASDM para manejar el ASA en el futuro, especifique el nuevo puerto como 8080.

ERROR: conflicto del asociar-direccionamiento con los parásitos atmosféricos existentes

Problema

Usted recibe este error cuando usted agrega un enunciado estático en el ASA:

```
ERROR: conflicto del asociar-direccionamiento con los parásitos atmosféricos existentes
```

Solución

Verifique que una entrada no exista ya para la fuente estática que usted quiere agregar.

Información Relacionada

- Página de Soporte de PIX
- Referencias de Comando PIX
- Páginas de Soporte ASA
- Referencias de Comandos ASA
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems