

PIX/ASA 7.x: Vire Redirection(Forwarding) hacia el lado de babor con nacional, global, los parásitos atmosféricos y los comandos access-list

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configuración inicial](#)

[Permita el Acceso de Salida](#)

[Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT](#)

[Permita el Acceso de los Hosts interiores a las Redes Externas con el uso de PAT](#)

[Limita el acceso de los Hosts Interiores a las Redes Externas](#)

[Permita el Acceso de los Hosts no Confiables a los Hosts de su Red de Confianza](#)

[Use los ACL en el PIX Versiones 7.0 y posterior](#)

[Inhabilite NAT para los Hosts/Redes Específicos](#)

[Redirección \(Reenvío\) de Puerto con Estático](#)

[Diagrama de la Red - Redirección de Puertos \(Reenvío\)](#)

[Configuración parcial de PIX: redirección del puerto](#)

[Limite la Sesión TCP/UDP con Estático](#)

[Lista de Acceso Basada en el Tiempo](#)

[Información que debe Obtener si Abre un Caso de Soporte Técnico](#)

[Información Relacionada](#)

Introducción

Para maximizar la seguridad al implementar Cisco PIX Security Appliance version 7.0, es importante comprender cómo se transfieren los paquetes entre las interfaces de alta seguridad y las interfaces de baja seguridad cuando usa los comandos **nat-control**. Este documento explica las diferencias entre estos comandos y cómo configurar el puerto Redirección (reenvío) y las funciones de Traducción de Dirección de Red Externa (NAT) en PIX software version 7.x, con el uso de la interfaz de línea de comando o el Adaptive Security Device Manager (ASDM).

Nota: Algunas opciones en el ASDM 5.2 y posterior pueden aparecer diferentes en las opciones

en el ASDM 5.1. Consulte la [documentación ASDM](#) para obtener más información.

prerrequisitos

Requisitos

Consulte [Cómo Permitir Acceso HTTPS para ASDM](#) 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.

- Cisco PIX 500 Series Security Appliance Software version 7.0 y posterior
- ASDM version 5.x y posterior

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.

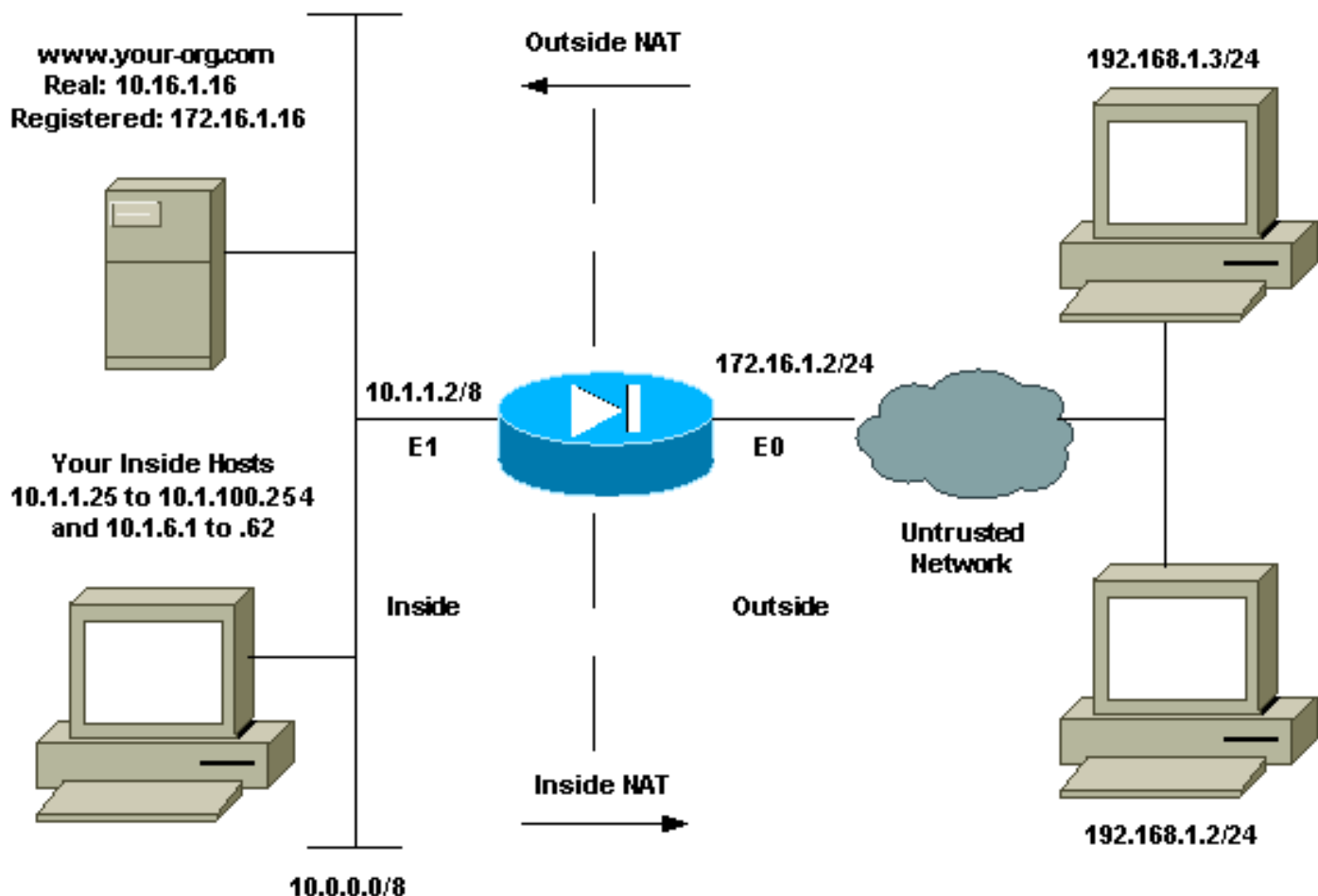
Productos Relacionados

También puede utilizar esta configuración con Cisco ASA Security Appliance

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

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.

[Configuración inicial](#)

Los nombres de la interfaz son:

- **interface ethernet 0** — nameif outside
- **interface ethernet 1** — nameif inside

Nota: Para encontrar la información adicional en los comandos usados en este documento, use la [Command Lookup Tool](#) ([clientes registrados solamente](#)).

[Permita el Acceso de Salida](#)

El acceso de salida describe las conexiones de una interfaz de mayor nivel de seguridad a una interfaz de menor nivel de seguridad. Esto incluye las conexiones desde el interior al exterior, interior hacia las zonas desmilitarizadas (DMZ) y DMZ hacia el exterior. Esto también puede incluir las conexiones de una DMZ a otra, mientras la interfaz de la fuente de conexión tiene un mayor nivel de seguridad que el destino. Revise la configuración "security-level" en las interfaces PIX para confirmar esto.

Este ejemplo muestra el nivel de seguridad y la configuración del nombre de la interfaz:

```
pix(config)#interface ethernet 0 pix(config-if)#security-level 0 pix(config-if)#nameif outside
```

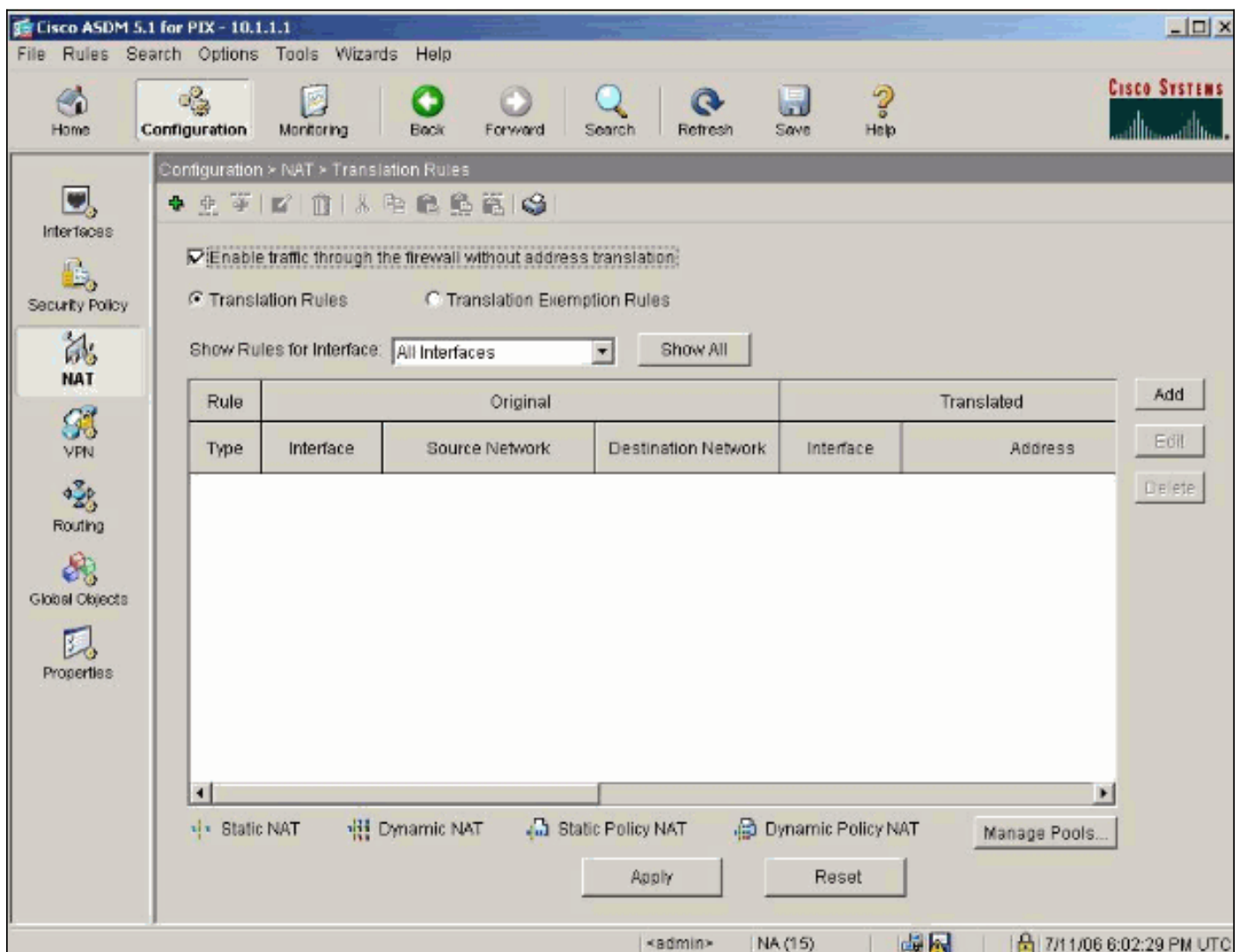
```
pix(config-if)#exit
```

El PIX 7.0 introduce el comando **nat-control**. Usted puede utilizar el comando **nat-control** en el modo de configuración para especificar si el NAT se requiere para las comunicaciones exteriores. Con el control de NAT habilitado, la configuración de las reglas NAT se requieren para permitir el tráfico saliente, como en el caso de las versiones anteriores del software PIX. Si el control NAT está inhabilitado (**no hay control nat**), los hosts interiores pueden comunicarse con las redes externas sin la configuración de una regla NAT. Sin embargo, si tiene host interiores que no tienen las direcciones públicas, todavía debe configurar el NAT para dichos hosts.

Para configurar el control NAT con el uso de ASDM, seleccione la pestaña de configuración de la ventana de inicio de ASDM y elija el **NAT** del menú de características.

Habilite el tráfico con el firewall sin la traducción: Esta opción fue introducida en la versión de PIX 7.0(1). Cuando esta opción está verificada, no se ejecuta ningún comando **nat-control** en la configuración. Este comando significa que no se requiere una traducción para atravesar el firewall. Esta opción se verifica generalmente solamente cuando los host internos tienen las direcciones IP públicas o la topología de red no requiere que los hosts internos se traduzcan a ninguna dirección IP.

Si los host internos tienen direcciones IP privadas, esta opción debe ser verificada de modo que los host internos puedan ser traducidos a una dirección IP pública y acceder a Internet.



Hay dos políticas que se requieren para permitir el acceso de salida con el control NAT. La primera es un método de traducción. Esto puede ser una traducción estática con el uso del

comando **static** , o una traducción dinámica con el uso de una regla **nacional/global**. No es necesario que el control NAT esté inhabilitado ni que sus host interiores tengan las direcciones públicas.

El otro requisito para el acceso de salida (que se aplica si el control NAT está habilitado o inhabilitado), es si hay una lista de control de acceso (ACL). Si hay una ACL, debe permitir el acceso de host de origen a la computadora principal de destino con el uso del protocolo y el puerto específicos. De forma predeterminada, no hay restricciones de acceso a las conexiones salientes a través del PIX. Esto significa que si no hay ACL configurada para la interfaz de origen, de forma predeterminada, se permite la conexión saliente si hay un método de traducción configurado.

[Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT](#)

Esta configuración le da a todos los hosts en el acceso de la subred 10.1.6.0/24 al exterior. Para lograr esto, utilice la **nat** y los **comandos globales** como lo muestra este procedimiento.

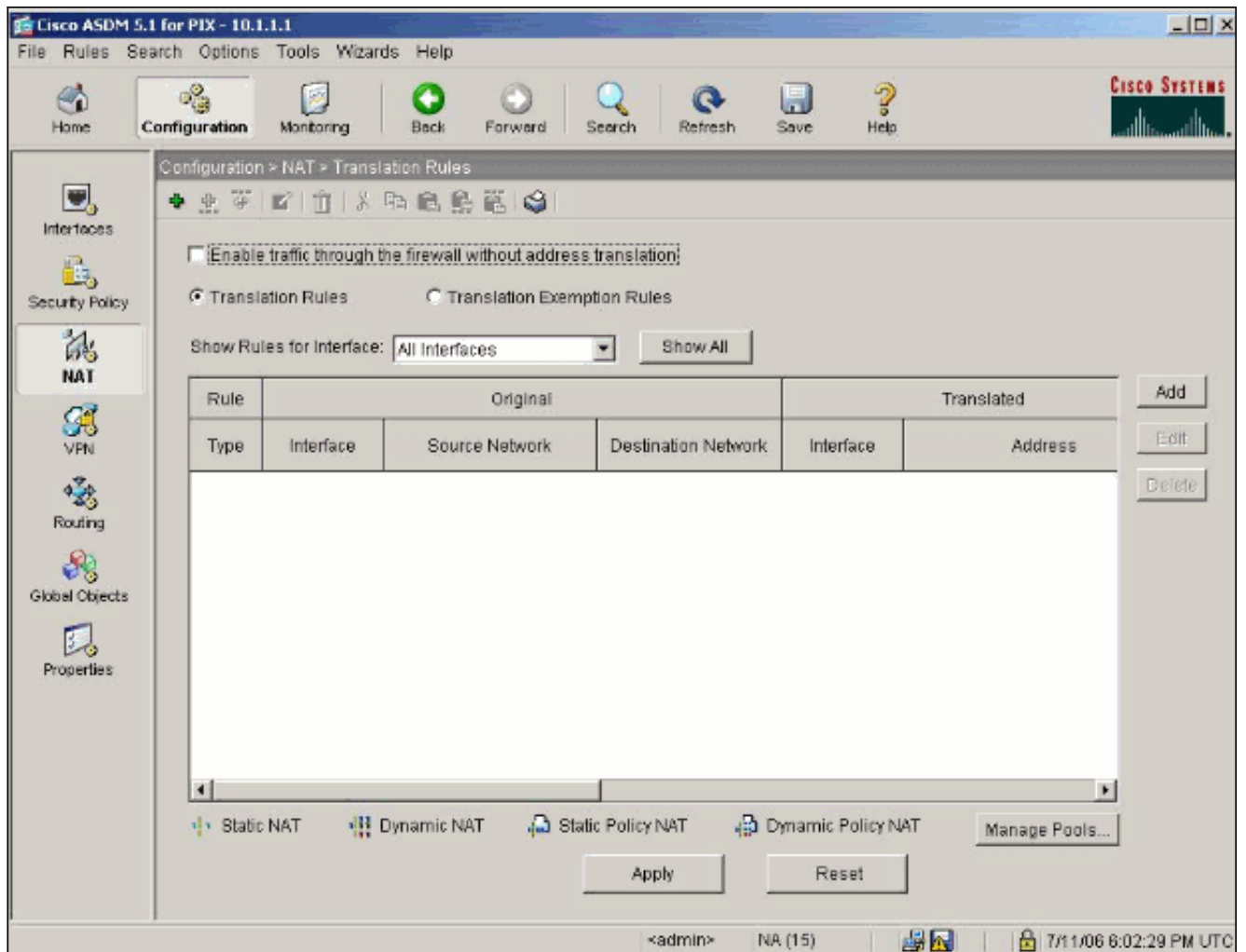
1. Defina al grupo interno que desea incluir para el NAT.

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. Especifique un grupo de direcciones en la interfaz exterior a la cual los hosts definidos en la sentencia NAT son traducidos.

```
global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
```

3. Use el ASDM para crear su grupo global de direcciones. Elija **Configuration > Features > NAT** y desmarque **Habilitar el tráfico con el firewall sin la traducción de la dirección**. Haga clic en **Agregar** para configurar la Regla NAT.



4. Haga clic en **Administrar Pools** para definir las direcciones del pool NAT.

Edit Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

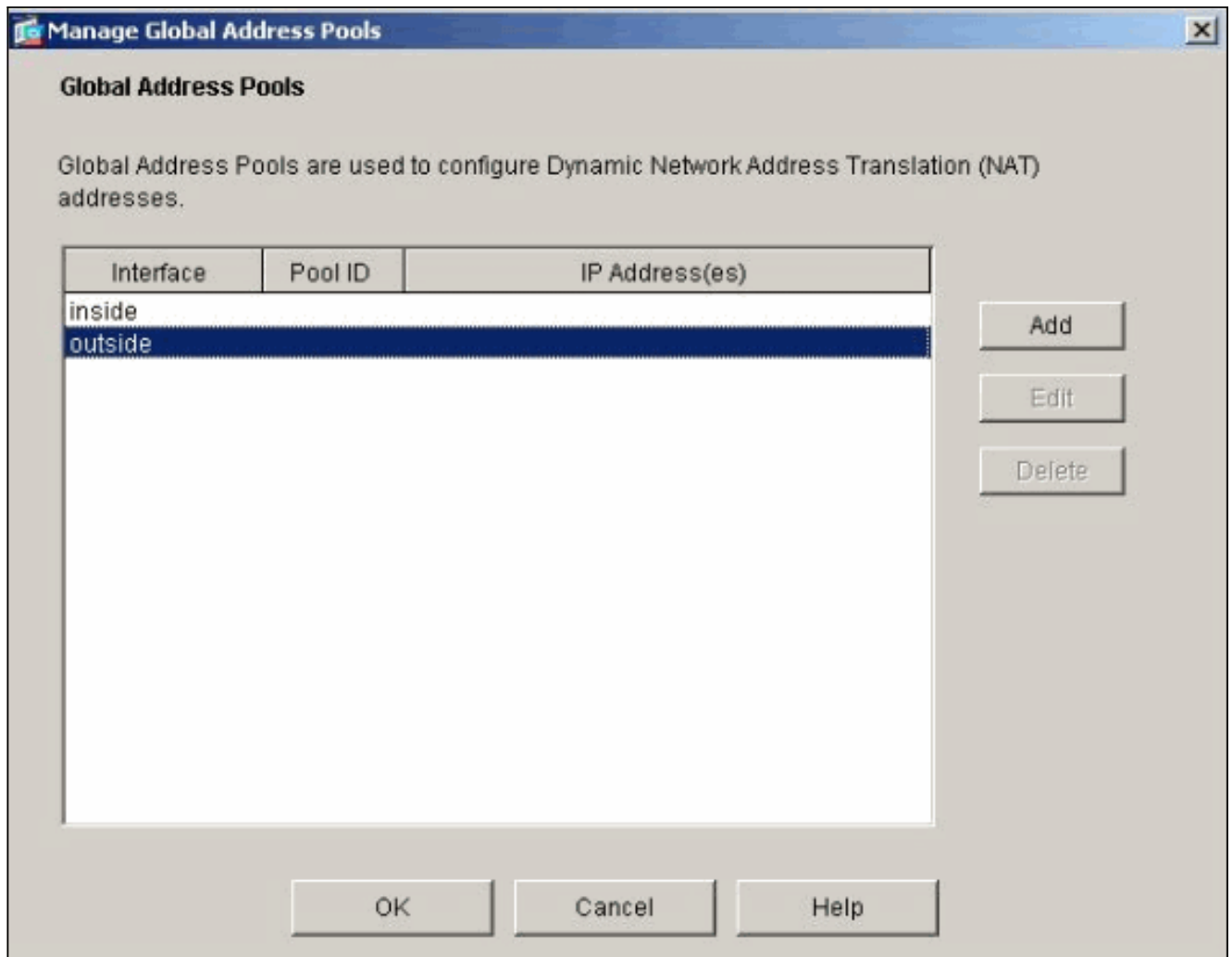
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

5. Elija **Outside > Add**, y elija un rango para especificar un pool de direcciones.



6. Ingrese su rango de direcciones, ingrese un pool ID, y haga clic en **Aceptar**.

Add Global Pool Item

Interface: Pool ID:

Range
 Port Address Translation (PAT)
 Port Address Translation (PAT) using the IP address of the interface

IP Address: —

Network Mask (optional):

7. Elija **Configuration > las Configuration > NAT > Translation Rules** para crear la regla de traducción.
8. Elija **Interior** como la Interfaz de Origen, e ingrese las direcciones que desea en la NAT.
9. Para Dirección de Traducción en la Interfaz, seleccione **Exterior**, elija **Dinámico**, y seleccione Pool de Direcciones que acaba de configurar.
10. Haga clic en **OK**.

Edit Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

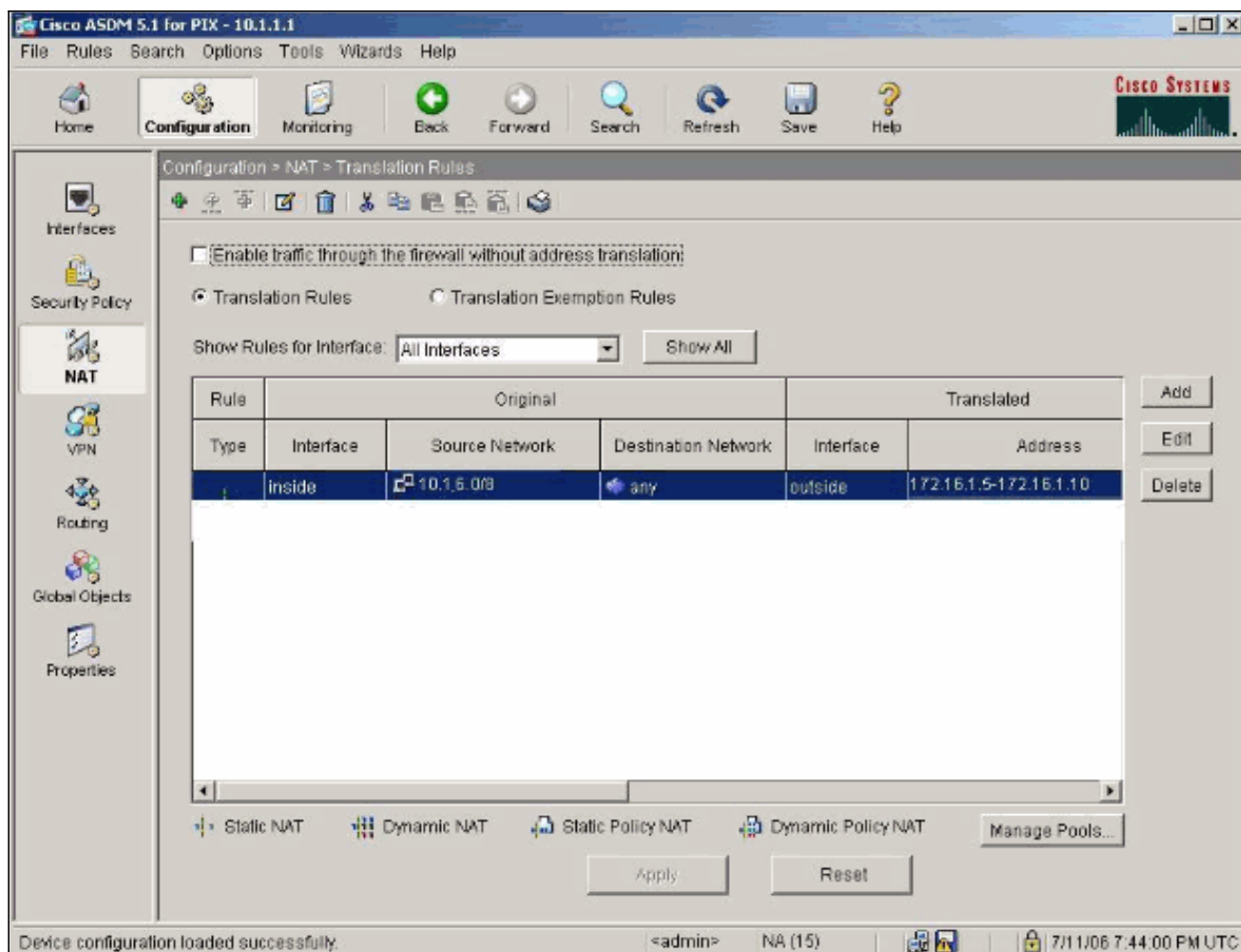
TCP Original port: Translated port:

 UDP

Dynamic Address Pool:

Pool ID	Address
1	172.16.1.5-172.16.1.10

11. La traducción aparece en las Reglas de Traducción en **Configuration > Features > NAT > Translation Rules**.



Ahora, los host internos pueden obtener acceso a redes externas. Cuando algunos hosts internos inician una conexión al exterior, son traducidos a una dirección del conjunto global. Las direcciones se asignan del pool global en función del orden y de la traducción, y comienza con la dirección más corta en el pool. Por ejemplo, si el host 10.1.6.25 es el primero en iniciar una conexión al exterior, recibe la dirección 172.16.1.5. El host siguiente hacia fuera recibe 172.16.1.6, y así sucesivamente. Éste no es una traducción estática, y los tiempos de traducción hacia fuera después de un período de inactividad según lo definido por el **timeout xlate hh: milímetro: comando ss**. Si hay más host interiores que direcciones en el pool, la dirección final en el pool se utiliza para la Traducción de Dirección de Puerto (PAT).

[Permita el Acceso de los Hosts interiores a las Redes Externas con el uso de PAT](#)

Si desea que los host internos compartan a una sola dirección pública para la traducción, use PAT. Si la **sentencia global** especifica una dirección, a esa dirección se le traduce el puerto. El PIX permite una traducción de puerto por interfaz y esa traducción admite hasta 65,535 objetos de traducción activos para una única traducción global. Complete estos pasos para permitir acceso de los hosts internos a las redes externas con el uso de PAT.

1. Defina el grupo interno que desea incluir para la PAT (cuando utiliza 0 0, seleccione todos los host interiores.)

```
nat (inside) 1 10.1.6.0 255.255.255.0
```
2. Especifique la dirección global que desea utilizar para PAT. Ésta puede ser la dirección de la interfaz.

```
global (outside) 1 172.16.1.4 netmask 255.255.255.0
```

3. En el ASDM, elija la **Configuration > Features > el NAT** y desmarque **Habilitar el tráfico a través de firewall sin la traducción de la dirección**.
4. Haga clic en **Agregar** para configurar la regla NAT.
5. Elija **Administrar Pools** para configurar su dirección PAT.
6. Elija **Outside > Add** y haga clic en **Traducción de Dirección de Puerto (PAT)** para configurar a una sola dirección para PAT.
7. Ingrese una dirección, un Pool ID, y haga clic en **Aceptar**.

The screenshot shows the 'Add Global Pool Item' dialog box. The 'Interface' dropdown is set to 'outside' and the 'Pool ID' text box contains '1'. There are three radio button options: 'Range', 'Port Address Translation (PAT)' (which is selected), and 'Port Address Translation (PAT) using the IP address of the interface'. Below these options, there is a section for IP address configuration. The 'IP Address' field contains '172.16.1.4' and the 'Network Mask (optional)' field contains '255.255.255.0'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

8. Elija **Configuration > las Configuration > NAT > Translation Rules** para crear la regla de traducción.
9. Seleccione el **interior** como la interfaz de origen, e ingrese las direcciones que desea NAT.
10. Para la Dirección de Traducción en la interfaz, seleccione **exterior**, elija **dinámico**, y seleccione la Dirección de Pool que acaba de configurar. Haga clic en **OK**.

Edit Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

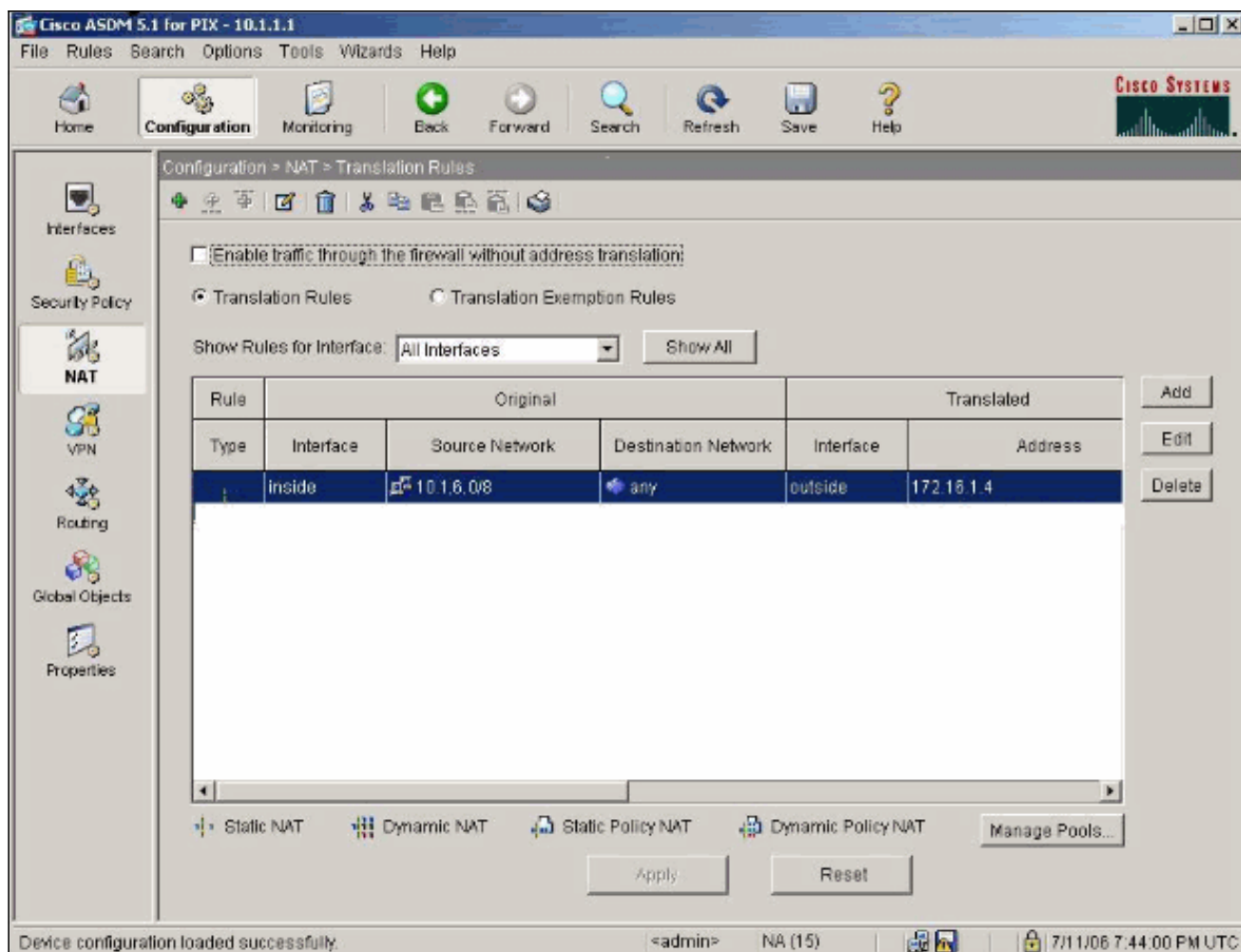
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
1	172.16.1.4

11. La traducción aparece en las Reglas de Traducción en **Configuration > Features > NAT > Translation Rules**.



Hay algunas cosas que debe considerar cuando utiliza el patente.

- Las direcciones IP que especifica para PAT no pueden estar en otro pool de dirección global.
- PAT no funciona con las aplicaciones H.323, servidores de nombre caché, y Point-to-Point Tunneling Protocol (PPTP). PAT funciona con Sistema de nombres de dominio (DNS), FTP y FTP pasivo, HTTP, correo, llamada de procedimiento remoto (RPC), rshell, Telnet, filtrado de URL y el traceroute de salida.
- No utilices PAT cuando necesita ejecutar las aplicaciones multimedia con el firewall. Las aplicaciones multimedia pueden estar en conflicto con las correlaciones de puertos que PAT proporciona.
- En el PIX software release 4.2(2), la función PAT no funciona con los paquetes de datos IP que llegan en orden inverso. PIX software release 4.2(3) corrige este problema.
- Las direcciones IP en el pool de direcciones globales especificadas con el **comando global** requieren las entradas de DNS inverso para asegurarse de que todas las direcciones de red externa sean accesibles con el PIX. Para crear las mappings de DNS inverso, use un Puntero DNS (PTR) en el archivo de mapping dirección-nombre para cada dirección global. Sin las entradas PTR, los sitios pueden sufrir una conectividad a Internet lenta o intermitente y los pedidos FTP pueden fallar constantemente. Por ejemplo, si una dirección IP global es 192.168.1.3 y el nombre de dominio para el dispositivo de seguridad PIX es pix.caguana.com, el registro PTR es:


```
3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
4.1.1.175.in-addr.arpa. IN PTR
pix4.caguana.com & so on.
```

[Limita el acceso de los Hosts Interiores a las Redes Externas](#)

Si hay un método de traducción válido definido para el host de origen, y ningún ACL definido para la interfaz PIX de origen, la conexión saliente se permite de forma predeterminada. Sin embargo, en algunos casos es necesario restringir el acceso de salida basado en la fuente, el destino, el protocolo, o el puerto. Para lograr esto, configure un ACL con el comando **access-list** y aplíquelo a la interfaz PIX de la fuente de conexión con el comando **access-group**. Usted puede aplicar PIX 7.0 ACL en las direcciones de entrada y de salida. Este procedimiento es un ejemplo que permite el acceso HTTP saliente para una subred, pero deniega el resto de los hosts el acceso HTTP al exterior, mientras que permite el resto del tráfico IP para cada uno.

1. Definir la ACL.

```
access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www access-list
```

```
acl_outbound deny tcp any any eq www access-list acl_outbound permit ip any any
```

Nota: El PIX ACL difiere de los ACL en los routers de Cisco IOS® en que el PIX no utiliza una máscara comodín como el Cisco IOS. Usa una máscara de subred regular en la definición ACL. Al igual que en los routers Cisco IOS, la ACL de PIX posee un “denegar todo” implícito al final de la ACL. **Nota:** Las nuevas entradas de lista de acceso serán añadidas al final del fichero al final de los ACE existentes. Si usted necesita ACE específico procesado primero, usted puede utilizar la *línea* palabra clave en la lista de acceso. Esto es un resumen del comando **example**:

```
access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any
```

2. Aplique el ACL a la interfaz interna.

```
access-group acl_outbound in interface inside
```

3. Use el ASDM para configurar la primera entrada de lista de acceso en el paso 1 para permitir el tráfico HTTP a partir del 10.1.6.0/24. Elija **Configuration > Features > Security Policy > Access Rules**.

4. Haga clic en **Agregar**, ingrese la información cuando esta ventana muestra, y haga clic en **Aceptar**.

Add Access Rule


Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Time Range
 Time Range:

Syslog
 Default Syslog

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 10.1.6.0/24 **inside** **outside** any
 Allow traffic

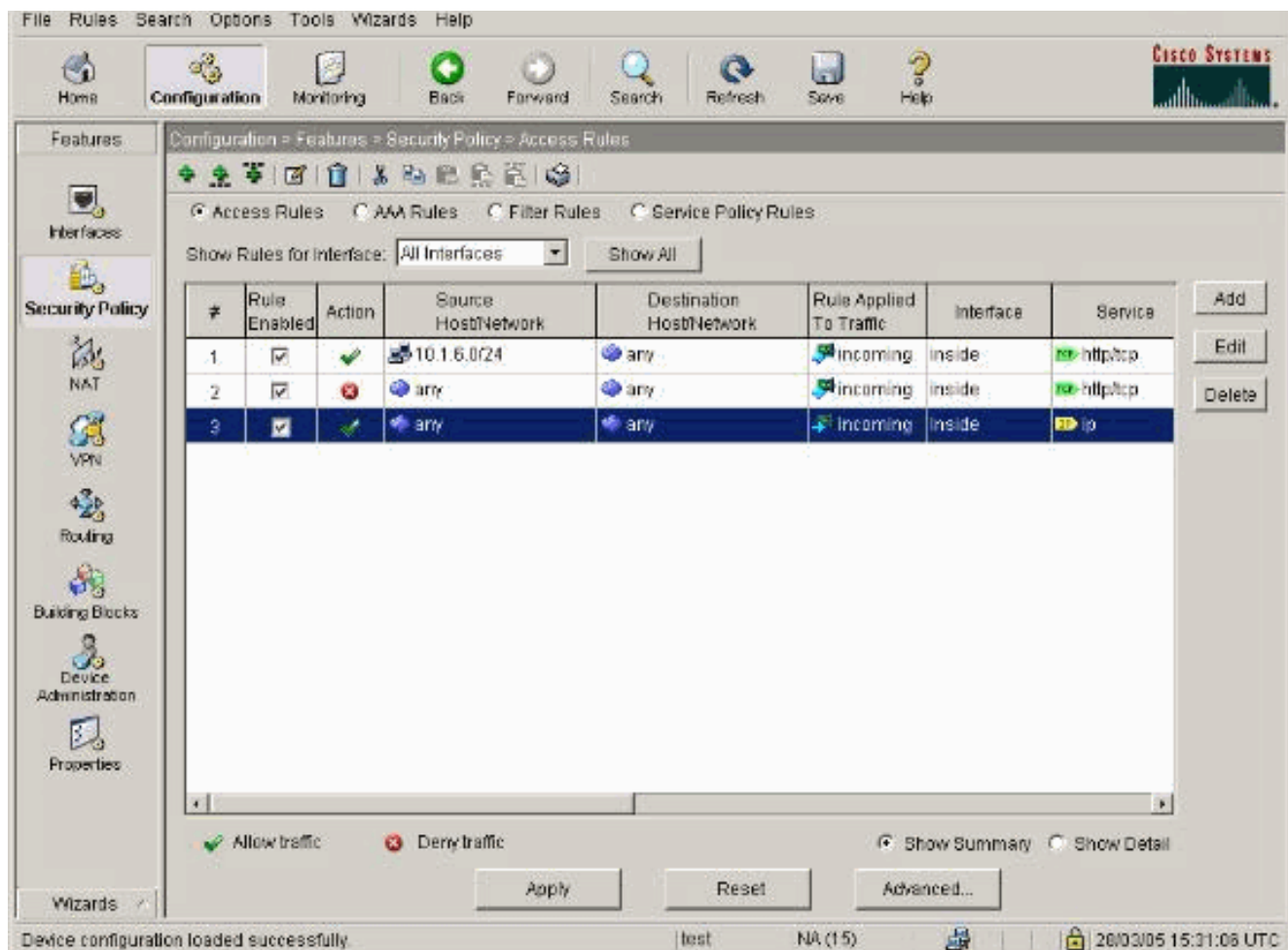
Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service = ...
 Service Group

Destination Port
 Service = ...
 Service Group

Please enter the description below (optional):

- Una vez que ingresó las tres entradas de lista de acceso, elija **Configuration > Feature > Security Policy > Access Rules** para mostrar estas reglas.



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

La mayoría de las organizaciones necesitan permitir el acceso de los hosts no confiables a los recursos en su red de confianza. Un ejemplo común es servidor Web interno. De forma predeterminada, el PIX niega las conexiones de los host exteriores a los host interiores. Para permitir esta conexión en el modo de control NAT, use el comando **static**, con los comandos **access-list** y **access-group**. Si el control NAT está inhabilitado, sólo se requieren los comandos **access-list** y **access-group**, si no se realiza ninguna traducción.

Aplique los ACL a las interfaces con un comando **access-group**. Este comando asocia el ACL a la interfaz para examinar el tráfico que fluye en una dirección particular.

A diferencia de **nat** y los comandos **global** que permiten los host interiores hacia fuera, el comando **static** crea una traducción bidireccional que permite los host interiores hacia fuera y los host exteriores adentro si agrega los ACL/a los grupos apropiados.

En los ejemplos de configuración de PAT que se muestran en este documento, si un host exterior intenta conectar con la dirección global, puede ser utilizado por los miles de hosts internos. El comando **static** crea un mapeo uno a uno. El comando de la **access-list** define qué tipo de conexión se requiere en un host interno y siempre se requiere cuando un host de menor seguridad conecta con un host de mayor seguridad. El comando **access-list** se basa en el puerto y protocolo y puede ser muy permisivo o muy restrictivo, sobre la base de lo que quiere el administrador de sistema alcanzar.

[El diagrama de la red](#) en este documento ilustra el uso de estos comandos para configurar el PIX para permitir que cualquier host no confiable conecte con el servidor Web interior, y permite el acceso del host no confiable 192.168.1.1 a un servicio FTP en el mismo equipo.

[Use los ACL en el PIX Versiones 7.0 y posterior](#)

Complete estos pasos para las versiones de software PIX 7.0 y posterior con el uso de los ACL.

1. Si se habilita el control NAT, defina una traducción de dirección estática para el servidor Web interior a una dirección externa/global.
`static (inside, outside) 172.16.1.16 10.16.1.16`
2. Defina qué hosts pueden conectar en qué puertos a su Web/servidor FTP.
`access-list 101 permit tcp any host 172.16.1.16 eq www access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp`
3. Aplique el ACL a la interfaz exterior.
`access-group 101 in interface outside`
4. Elija **Configuration > Features > NAT** y haga clic en **Agregar** para crear esta traducción estática con el uso de ASDM.
5. Seleccione **interior** como la interfaz de origen, ingrese la dirección interna para la que desea crear una traducción estática.
6. Elija **Static** e ingrese la dirección externa que desea traducir en al campo de dirección IP. Haga clic en OK.

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

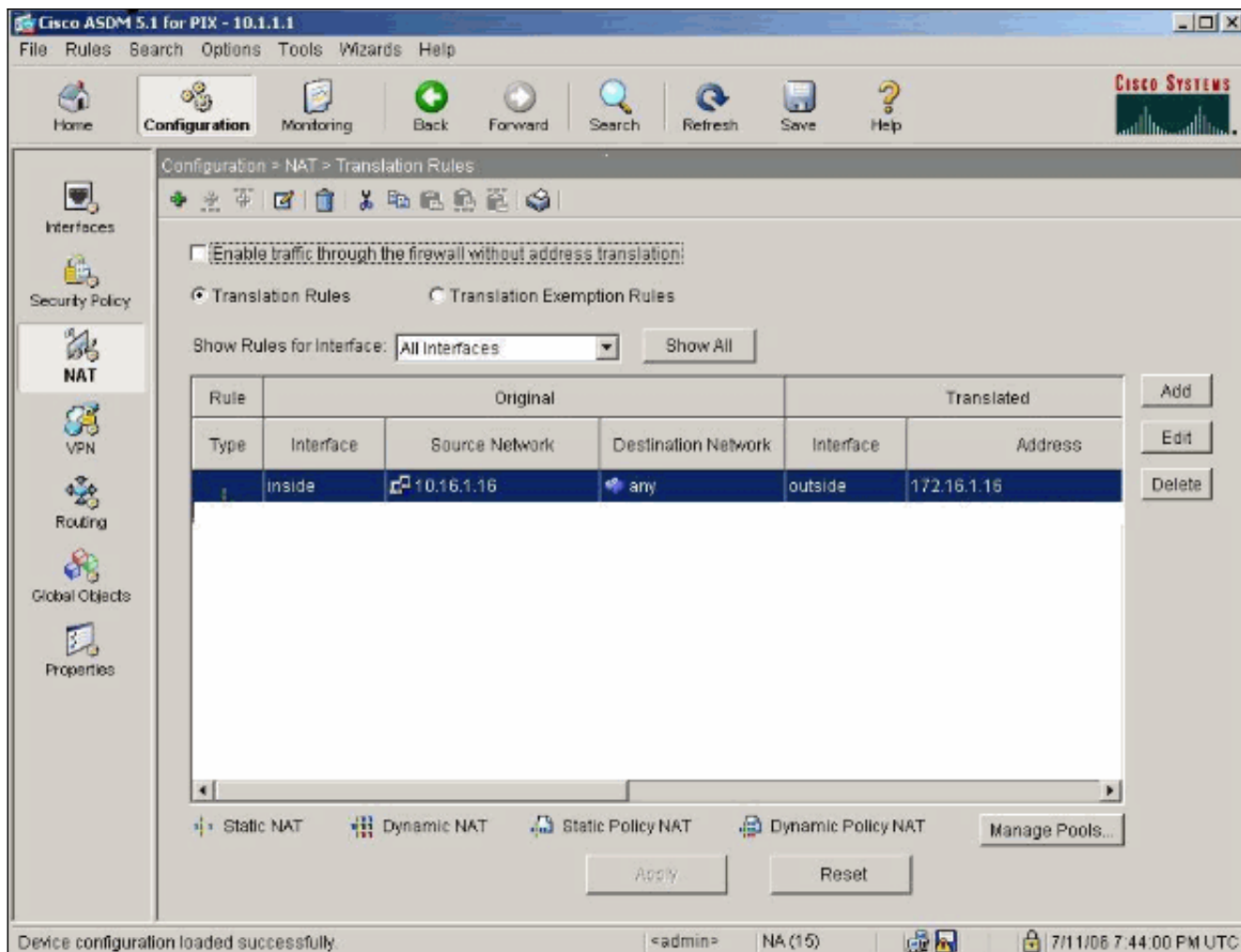
TCP Original port: Translated port:

UDP

 Dynamic Address Pool:

Pool ID	Address

7. La traducción aparece en las reglas de traducción cuando elige **Configuration > Features > NAT > Translation Rules**.



8. Use el procedimiento [Restringir Acceso de los Hosts Internos a las Redes Externas](#) para ingresar las entradas de **lista de acceso**. **Nota:** Tenga cuidado cuando implementa estos comandos. Si implementa el comando **access-list 101 permit ip any any**, cualquier host en la red no confiable puede acceder a cualquier host en la red de confianza con el uso de IP mientras haya una traducción activa.

[Inhabilite NAT para los Hosts/Redes Específicos](#)

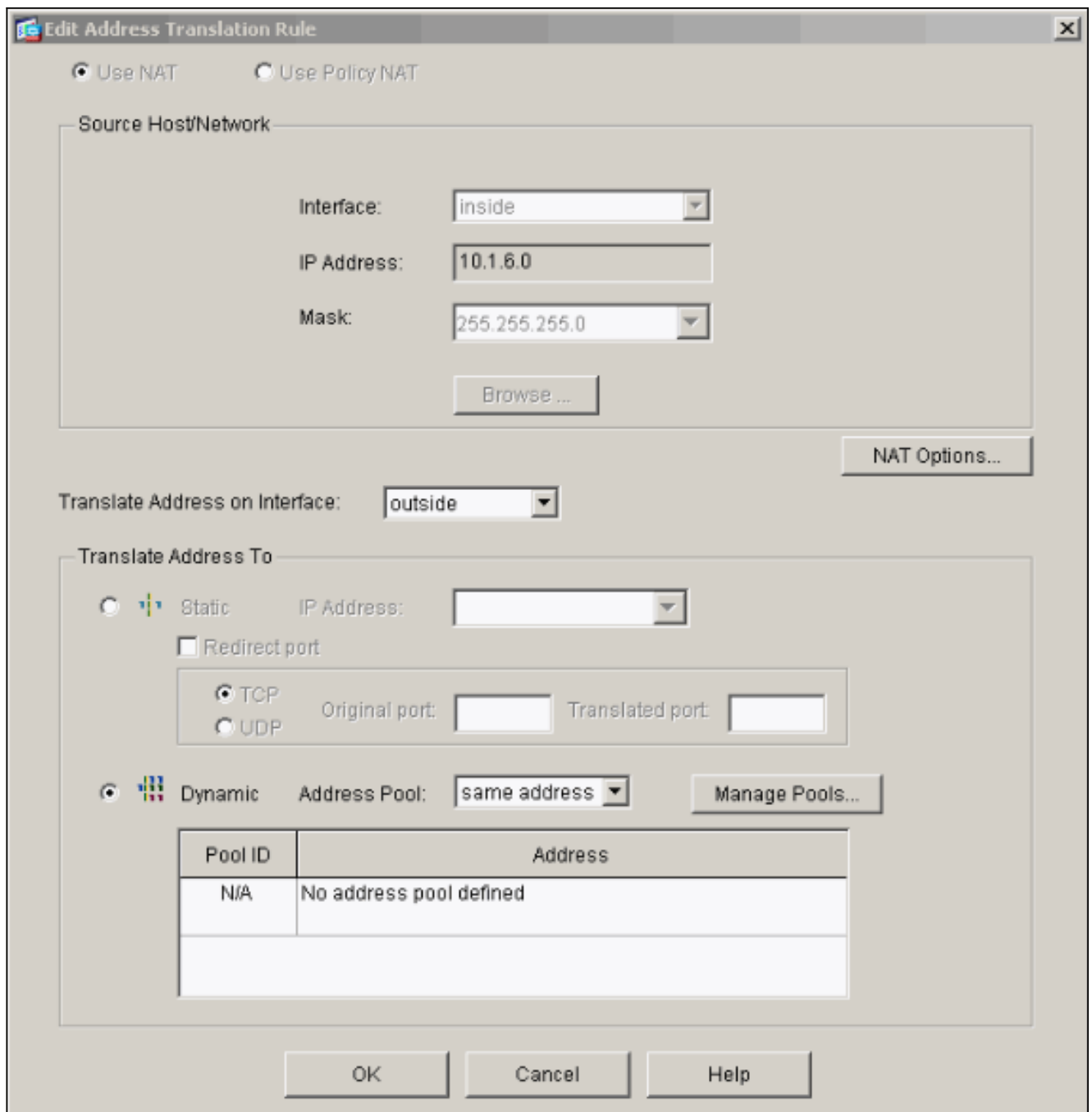
Si usa el control NAT y tiene direcciones públicas en la red interna, y desea que aquellos host interiores específicos salieran al exterior sin la traducción, puede invalidar el NAT para dichos hosts, con **nat 0** o los comandos **static**.

Éste es un ejemplo del comando **nat**:

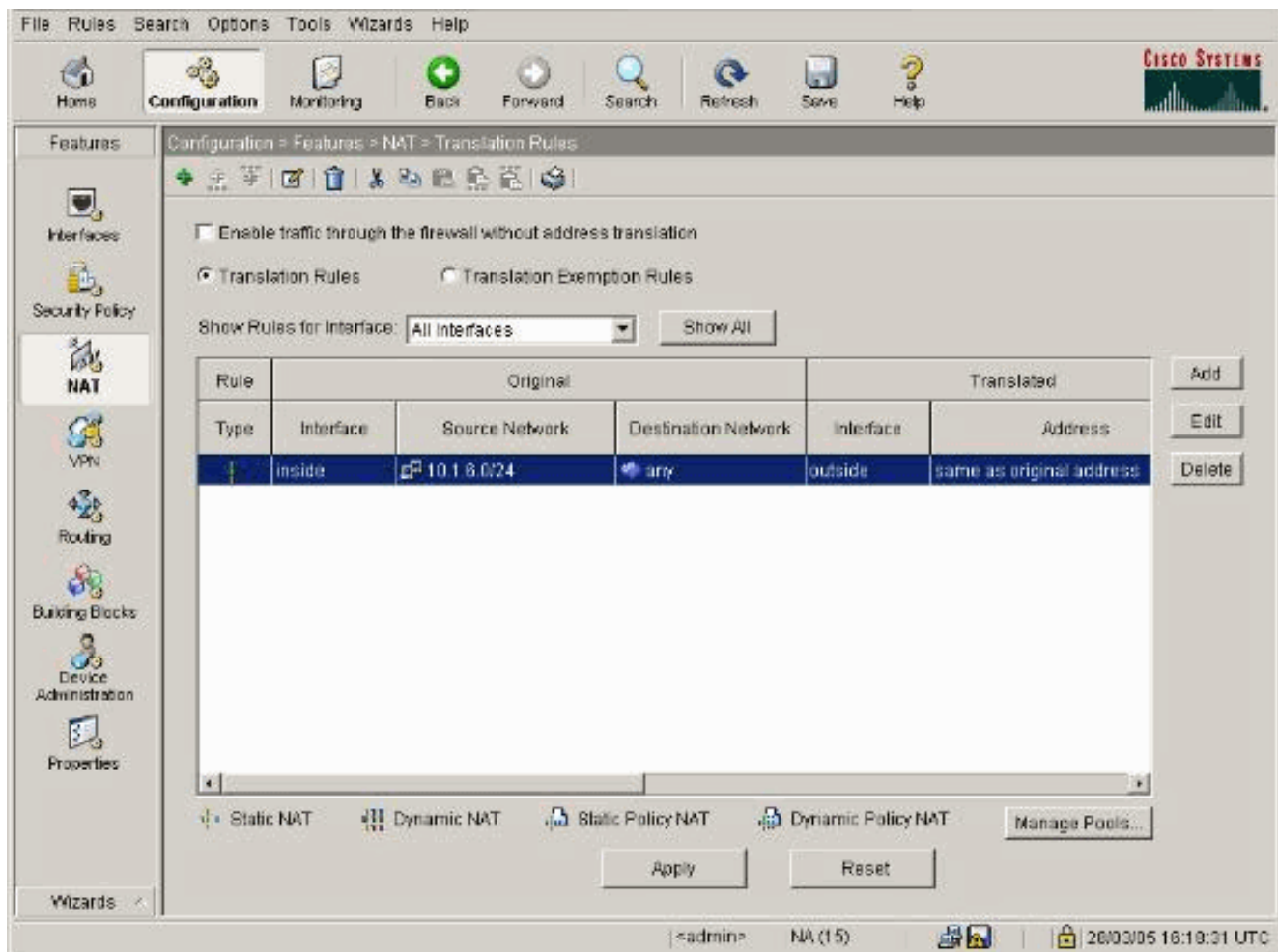
```
nat (inside) 0 10.1.6.0 255.255.255.0
```

Complete estos pasos para invalidar el NAT para los hosts/redes específicos con el uso de ASDM.

1. Elija la **Configuration > Features > NAT** y haga clic en **Agregar**
2. Elija **interior** como la interfaz de origen, e ingrese la dirección interna/la red para la cual desea crear una traducción estática.
3. Elija **Dinámico** y seleccione la misma dirección para el Pool de Direcciones. Haga clic en **OK**.

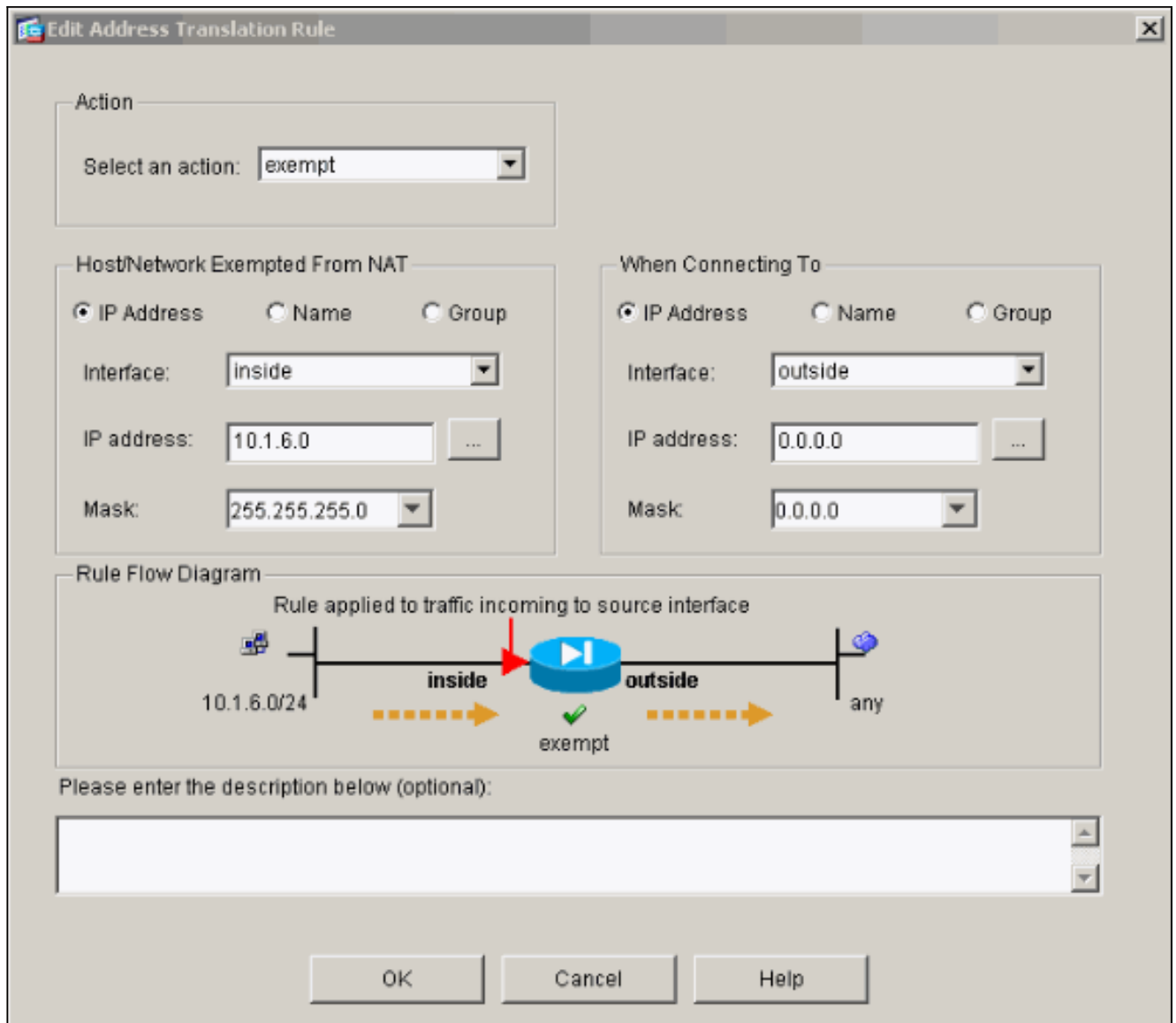


4. La nueva regla aparece en las Reglas de Traducción cuando elige la **Configuration > Features > el NAT > Translation Rules.**

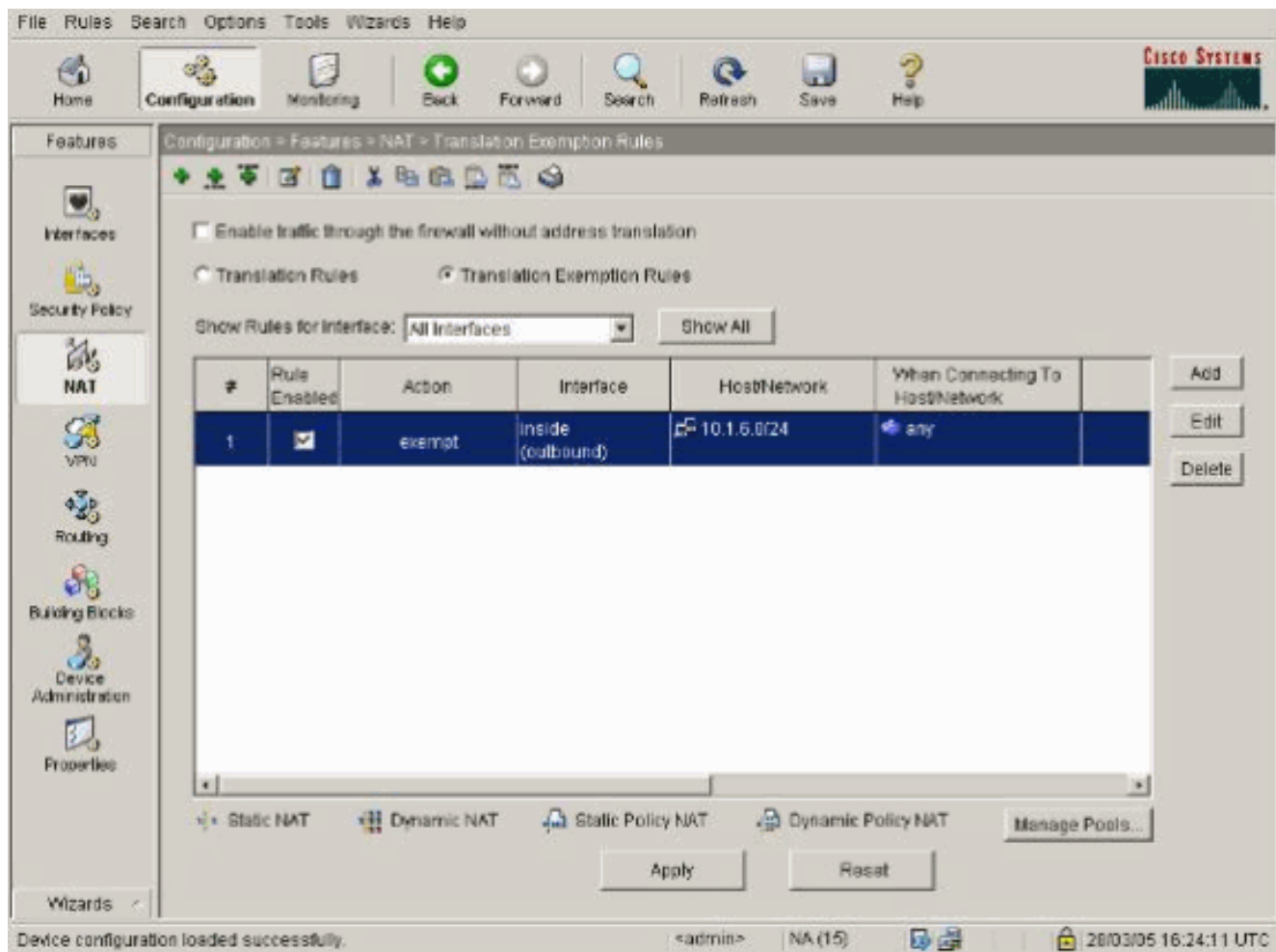


5. Si usa los ACL, que permiten un control más preciso del tráfico que no debe traducir (basado en la fuente/el destino), use estos comandos.

```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any nat (inside) 0 access-list 103
```
6. Use el ASDM y elija la **Configuration > Features > NAT > Translation Rules**.
7. Elija **Reglas de Exención de Traducción** y haga clic en Agregar. Este ejemplo muestra cómo eximir el tráfico de la red 10.1.6.0/24 a cualquier lugar de la traducción.



8. Elija **Configuration > Features > NAT > Translation Exemption Rules** para mostrar las nuevas reglas.



9. El comando **static** para el servidor Web cambia mientras que este ejemplo se muestra.
`static (inside, outside) 10.16.1.16 10.16.1.16`
10. De ASDM, elija **Configuration > Features > NAT > Translation Rules**.
11. Seleccione las **Reglas de Traducción** Ingrese la información de dirección de origen, y seleccione los **Estático**. Ingrese la misma dirección en el campo de Dirección IP.

Add Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:


Translate Address on Interface:

Translate Address To

 Static

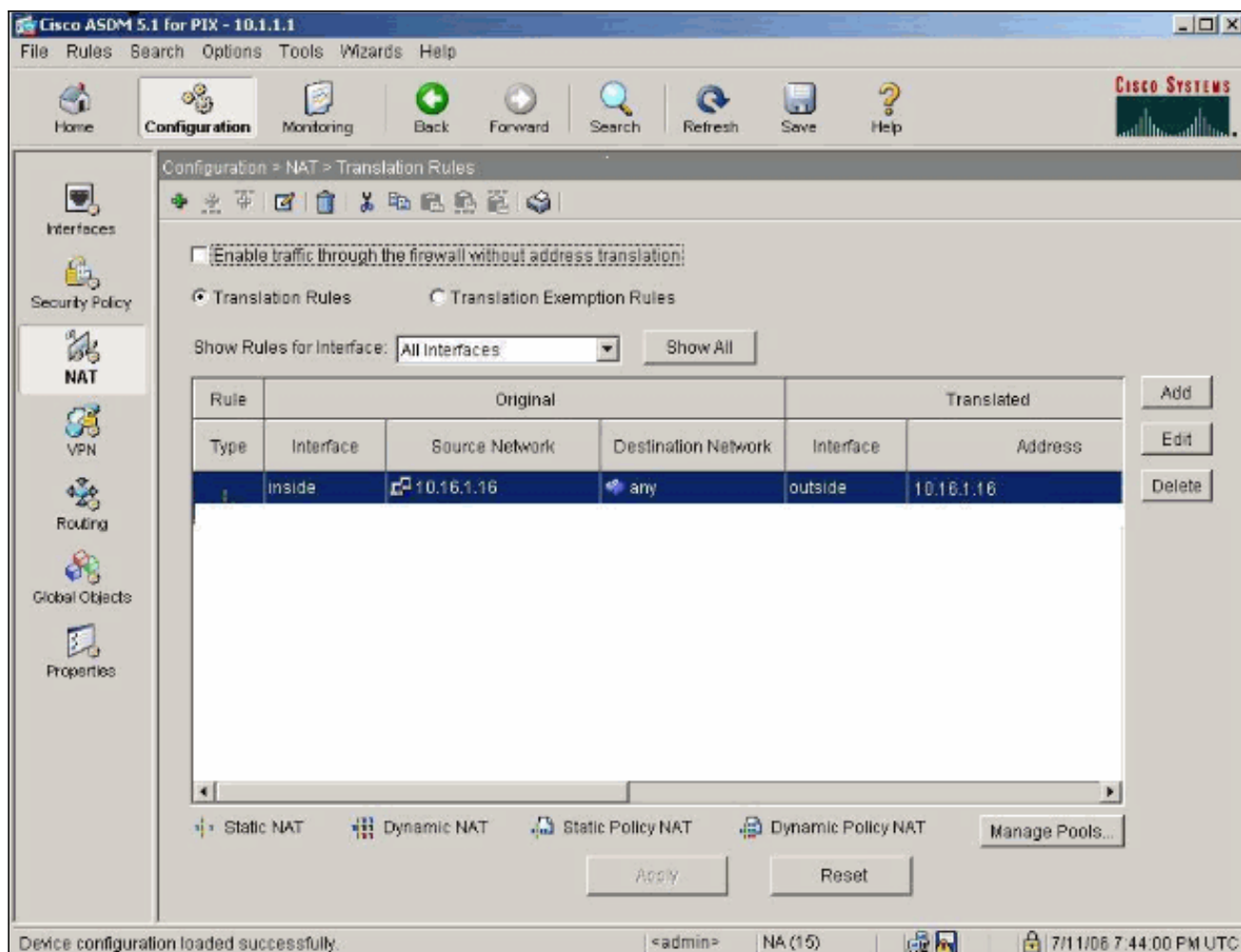
Redirect port

TCP
 Original port:
 Translated port:

 Dynamic

Pool ID	Address

12. La traducción aparece en las reglas de traducción cuando elige **Configuration > Features > NAT > Translation Rules**.



13. Si usa los ACL, use estos comandos.

`access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside` Consulte la sección [Restringir Acceso de Hosts Interiores a Redes Externas de](#) este documento para más información sobre la configuración de los ACL en el ASDM. Observe la diferencia entre el uso de `nat 0` cuando especificas la red/la máscara en comparación con ACL que utiliza una red/una máscara que permite la iniciación de la conexión desde adentro solamente. El uso de los ACL con `nat 0` permite la iniciación de la conexión por el tráfico de entrada o de salida. Las interfaces PIX deben estar en diversas subredes para evitar los problemas del alcance.

[Redirección \(Reenvío\) de Puerto con Estático](#)

En PIX 6.0, la función Redirección (reenvío) de Puertos se agregó para permitir que usuarios externos se conecten a una dirección particular IP/puerto y el PIX El comando **estático** fue modificado. La dirección compartida puede ser una dirección única, una dirección PAT de salida compartida, o compartida con la interfaz externa. Esta función está disponible en PIX 7.0.

Nota: Debido a las limitaciones de espacio, los comandos se muestran en dos líneas.

```
static [(internal_if_name, external_if_name)] {global_ip/interface}local_ip [netmask mask]
[max_conns [emb_limit [norandomseq]]] static [(internal_if_name, external_if_name)] {tcp/udp}
{global_ip/interface} global_port local_ip local_port [netmask mask] [max_conns [emb_limit
[norandomseq]]]
```

Nota: Si el NAT estático utiliza la dirección exterior del IP (global_IP) para traducir, ésta pudo causar una traducción. Por lo tanto, use la **interfaz de la palabra clave** en vez de la dirección IP en

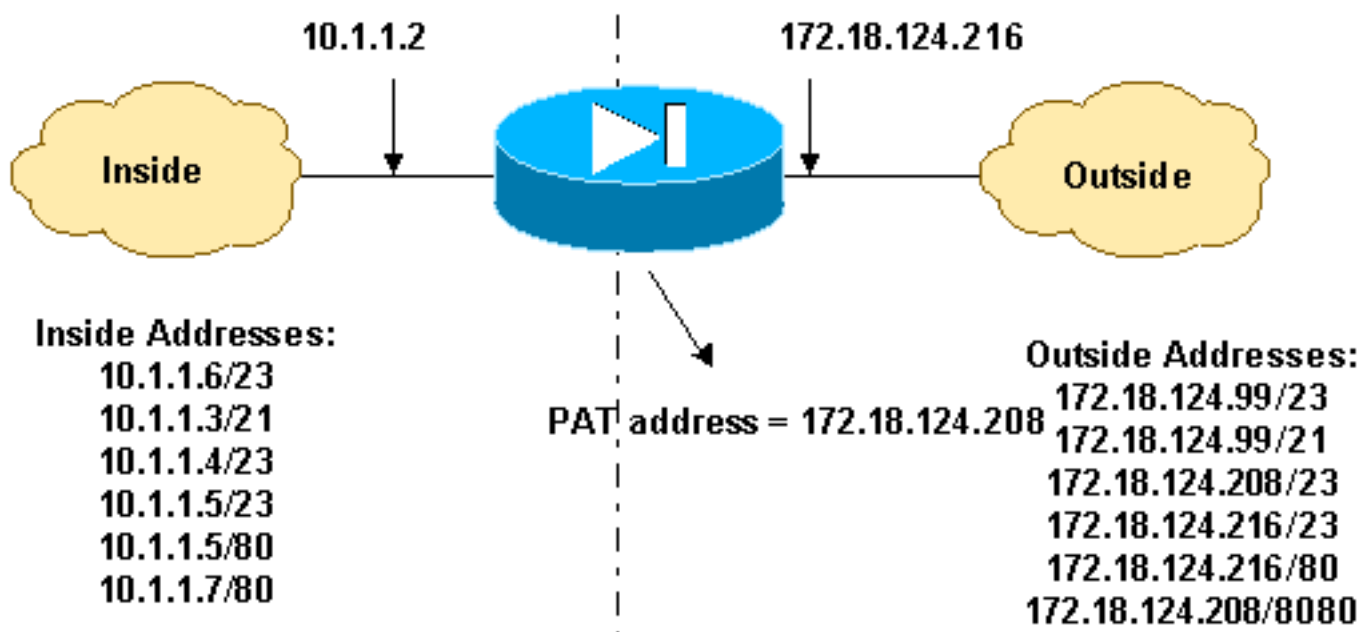
la traducción estática.

Estas Redirecciones (Reenvíos) de Puertos están en este ejemplo de red:

- Los usuarios externos dirigen las solicitudes de Telnet a la dirección IP única 172.18.124.99, que el PIX redirige a 10.1.1.6.
- Los usuarios externos dirigen las peticiones FTP a la dirección IP exclusiva 172.18.124.99, que PIX redirige a 10.1.1.3.
- Los usuarios externos dirigen las peticiones Telnet a la dirección PAT 172.18.124.208 y el PIX las redirige a 10.1.1.4.
- Los usuarios externos dirigen las peticiones Telnet a la dirección IP externa 172.18.124.216, que el PIX redirige a 10.1.1.5.
- Los usuarios externos dirigen la solicitud de HTTP a la dirección IP externa 172.18.124.216 PIX, que el PIX redirige a 10.1.1.5.
- Los usuarios externos direccionan las peticiones del puerto 8080 http a la dirección PAT 172.18.124.208 y el PIX las redirecciona a la 10.1.1.7 del puerto 80.

Este ejemplo también bloquea el acceso de algunos usuarios desde el interior al exterior con el ACL 100. Este paso es opcional. Sin el ACL implementado se permite todo el tráfico de salida.

Diagrama de la Red - Redirección de Puertos (Reenvío)



Configuración parcial de PIX: redirección del puerto

Esta configuración parcial ilustra el uso de la Redirección (reenvío) de Puerto Estático. Consulte el [diagrama de la red de Redirección \(Reenvío\) de Puertos](#).

Configuración parcial PIX 7.x - Redirección (Reenvío) de Puertos

```
fixup protocol ftp 21
!--- Use of an outbound ACL is optional. access-list 100
permit tcp 10.1.1.0 255.255.255.128 any eq www access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
```

```
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(inside,outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside
```

Nota: Si el PIX/ASA se configura con el **noproxyarp del sysopt fuera del** comando, después no permite que el Firewall haga el proxy ARP y las traducciones NAT estáticas en el PIX/ASA. Para resolver esto, quite el **noproxyarp del sysopt fuera del** comando en la configuración del PIX/ASA y después ponga al día las entradas ARP usando el ARP gratuito. Esto permite que las entradas NAT estáticas trabajen muy bien.

Este procedimiento es un ejemplo de cómo configurar la Redirección (Reenvío) de Puertos que permite a usuarios externos dirigir las solicitudes de Telnet directas a la dirección IP única 172.18.124.99, que el PIX redirige a 10.1.1.6.

1. Use el ASDM y elija la **Configuration > Features > NAT > Translation Rules**.
2. Seleccione las **Reglas de Traducción**
3. Para el Host Seguro / Red , ingrese la información para la dirección IP interior.
4. Para Dirección de Traducción a, seleccione los **Estático**, ingrese la dirección IP externa y verifique el **puerto Redirigir**.
5. Ingrese la información de puerto de la previa a la traducción y posterior a la traducción (este ejemplo mantiene el puerto 23). Haga clic en OK.

Add Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

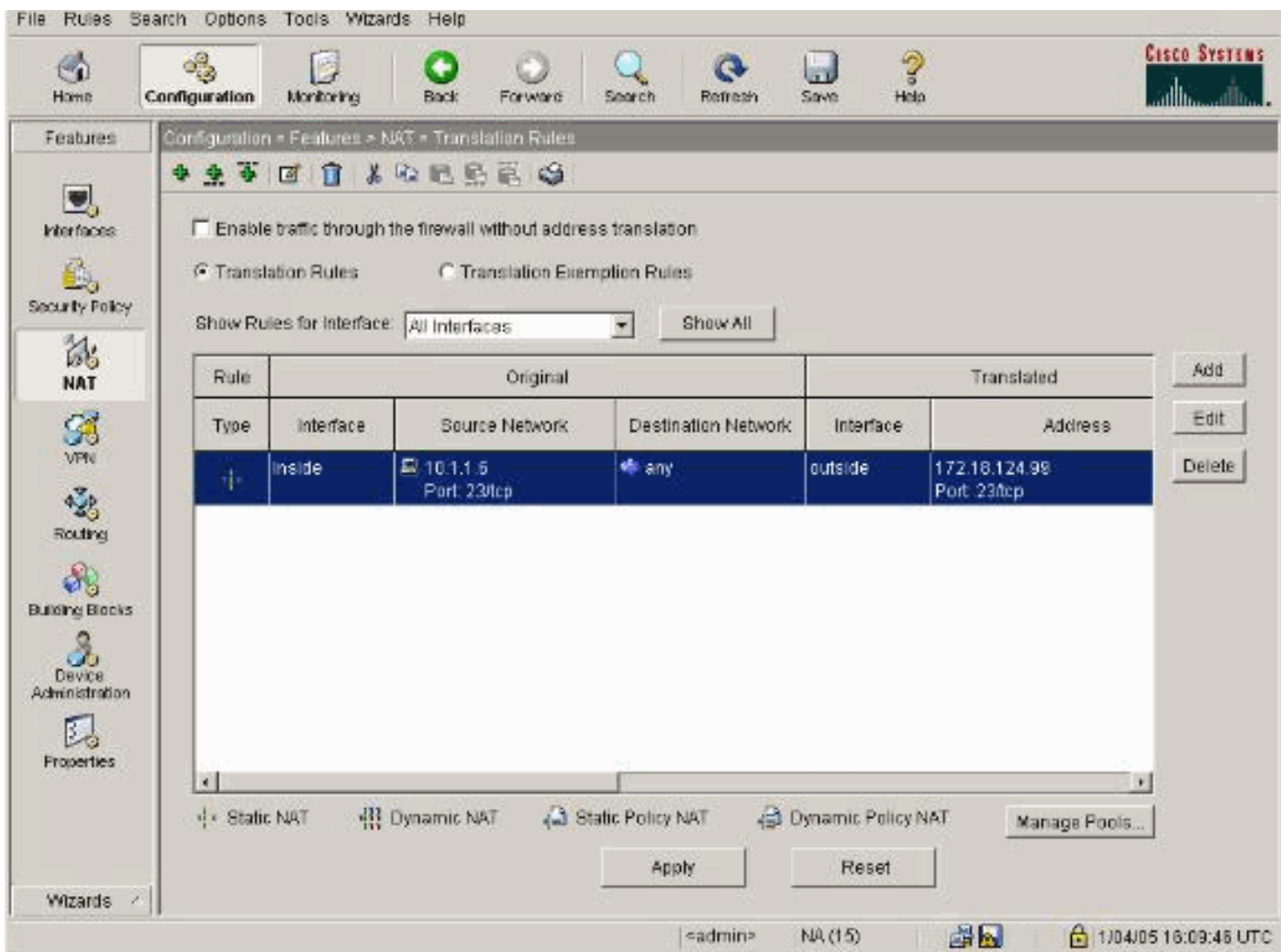
TCP Original port: Translated port:

 UDP

Dynamic Address Pool:

Pool ID	Address

La traducción aparece en las reglas de traducción cuando elige **Configuration > Features > NAT > Translation Rules**.



Limite la Sesión TCP/UDP con Estático

Si desea limitar las sesiones TCP o UDP al servidor interno colocado en PIX/ASA, use el comando **estático** .

Especifique el número máximo de TCP simultáneo y las conexiones UDP para la subred completa. El valor predeterminado es 0, lo que significa que conexiones ilimitadas (las conexiones inactivas se cierran después del tiempo de espera inactivo especificado por el comando **timeout conn.**). Esta opción no se aplica al NAT exterior. El dispositivo de seguridad solamente rastrea las conexiones de una interfaz de mayor seguridad a una interfaz de menor seguridad.

Limitar el número de conexiones embrionarias lo protege contra un ataque DOS. El dispositivo de seguridad utiliza el límite embrionario para accionar la intercepción de TCP, que protege los sistemas interiores contra un ataque DOS perpetrado al inundar una interfaz con los paquetes SYN TCP. Una conexión embrionaria es una solicitud de conexión que no ha esperado el tiempo de espera de entrada en contacto necesario entre el origen y el destino. Esta opción no se aplica al NAT exterior. La función intercepción de TCP se aplica solamente a los hosts o a los servidores en un mayor nivel de seguridad. Si establece el límite embrionario para el NAT exterior, se ignora el límite embrionario.

Por ejemplo:

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100 !--- The maximum
number of simultaneous tcp connections the local IP !--- hosts are to allow is 500, default is 0
which means unlimited !--- connections. Idle connections are closed after the time specified !--
```

- by the `timeout conn` command !--- The maximum number of embryonic connections per host is 100.

%PIX-3-201002: Demasiadas conexiones encendidas {estático|xlate} global_address! econns nconns

Esto es un mensaje relacionado con la conexión. Este mensaje se registra cuando la cantidad máxima de conexiones a la dirección estática especificada fue satisfactoria. La variable de los econns es el número máximo de conexiones embrionarias y los nconns son la cantidad máxima de conexiones permitida para los static o xlate.

La acción recomendada es utilizar el comando **show static** para verificar el límite impuesto en las conexiones a una dirección estática. El límite es configurable.

%ASA-3-201011: El límite de la conexión excedió de 1000/1000 para el paquete de entrada a partir del 10.1.26.51/2393 a 10.0.86.155/135 en la interfaz afuera

Este mensaje de error es debido al Id. de bug Cisco [CSCsg52106](#) ([clientes registrados solamente](#)). Consulte este bug para obtener más información.

[Lista de Acceso Basada en el Tiempo](#)

La creación de un rango de tiempo no restringe el acceso al dispositivo. El comando **time-range** define el rango de tiempo solamente. Después de que se define rango de tiempo, puede asociarlo a las reglas de tráfico o a una acción.

Para implementar un ACL basado en el tiempo, use el comando **time-range** para definir momentos específicos del día y de la semana. Use con el comando **access-list extended time-range** para unir el rango de tiempo a una ACL.

El rango de tiempo confía en el reloj del sistema del dispositivo de seguridad. Sin embargo, la característica funciona mejor con la sincronización NTP.

Después de que haya creado un rango de tiempo e ingresado el modo de configuración del rango de tiempo, puede definir los parámetros del rango de tiempo con los comandos **absolutos** y **periódicos**. Para restablecer las configuraciones predeterminadas para las palabras clave periódicas y absolutas del comando de **rango de tiempo**, use el comando **predeterminado** en el modo de configuración `time-range`.

Para implementar un ACL basado en el tiempo, use el comando **time-range** para definir momentos específicos del día y de la semana. Entonces use **con el** comando **access-list extended** para unir el rango de tiempo a una ACL. El próximo ejemplo conecta una ACL denominada "Ventas" a un rango de tiempo denominado "Minuto de Nueva York":

Este ejemplo crea un rango de tiempo denominado "Minuto de Nueva York" e ingrese al modo de configuración del rango de tiempo:

```
hostname(config)#time-range New_York_Minute hostname(config-time-range)#periodic weekdays 07:00
to 19:00 hostname(config)#access-list Sales line 1 extended deny ip any any time-range
New_York_Minute hostname(config)#access-group Sales in interface inside
```

[Información que debe Obtener si Abre un Caso de Soporte Técnico](#)

Si aún necesita ayuda y desea abrir un caso con el Soporte Técnico de Cisco, asegúrese de incluir esta información para troubleshooting su dispositivo de seguridad PIX.

- Descripción de problemas y detalles relevantes de la topología.
- Pasos usados para resolver problemas antes de abrir el caso.
- Salida del comando **showtech-support**.
- Salida del comando **show log** después de que el comando **logging buffered debugging** se ejecute, o capturas de consola que demuestran el problema (si está disponible).

Adjunte los datos recopilados para su caso en un texto sin formato (.txt), sin compactar. Puede adjuntar la información a su caso en la [Herramienta de Solicitud de Servicio TAC \(clientes registrados solamente\)](#). Si no puede acceder a la [Herramienta de la Solicitud de Servicio TAC \(clientes registrados solamente\)](#), puede enviar la información en un archivo adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto del mensaje.

[Información Relacionada](#)

- [Páginas de Soporte de PIX Security Appliance](#)
- [Referencias de Comando PIX](#)
- [Alertas y Troubleshooting de Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)