ASA 8.2: Redirección de puerto (expedición) con nacional, global, estático, y comandos access-list que usan el ASDM

Contenido

Introducción

Este documento describe cómo funciona la redirección de puertos en Cisco Adaptive Security Appliance (ASA) mediante ASDM. Se ocupa del control de acceso del tráfico mediante el ASA y de cómo funcionan las reglas de traducción.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Descripción general de NAT
- PIX/ASA 7.X: Redirección de puerto

Componentes Utilizados

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

- Versión de ASA 8.2 de las Cisco 5500 Series
- Cisco ASDM versión 6.3

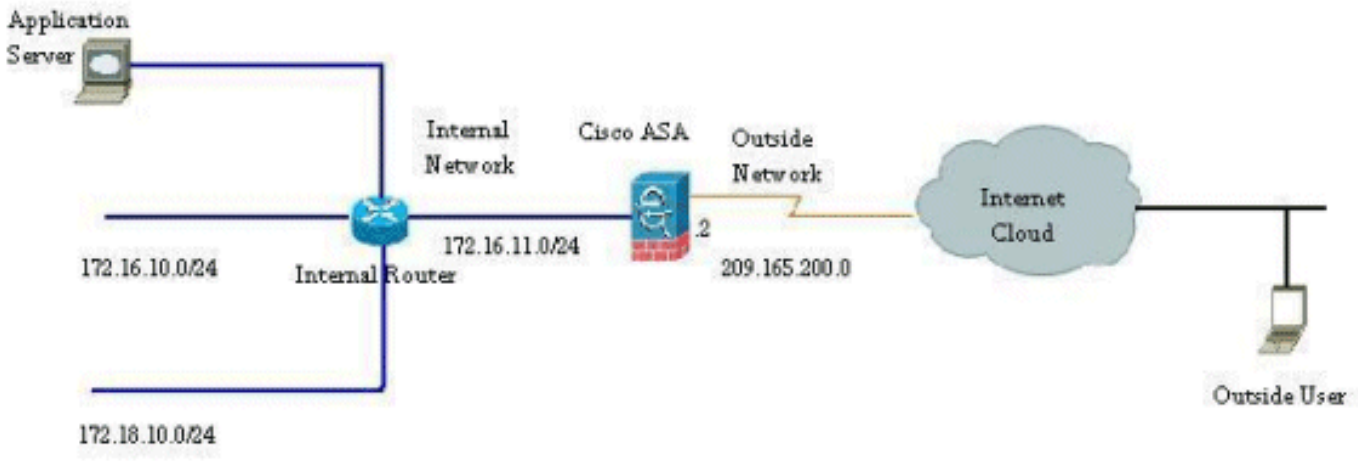
Nota: Esta configuración trabaja muy bien de la versión de software 8.0 a 8.2 de Cisco ASA solamente, porque no hay cambios importantes en la funcionalidad de NAT.

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Diagrama de la red



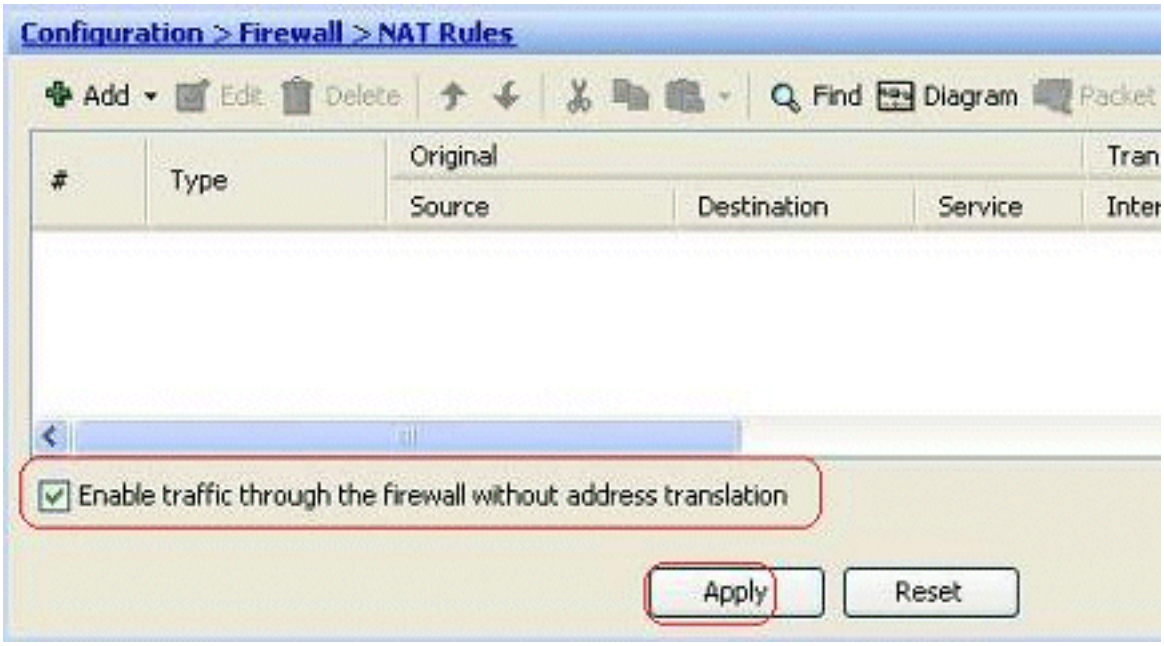
Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

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.

Ninguna conexión puede pasar a través del dispositivo de seguridad sin una regla de traducción configurada. Esta característica se llama NAT control. La imagen mostrada aquí representa cómo inhabilitar esto con el ASDM para permitir las conexiones con el ASA sin ninguna traducción de la dirección. Sin embargo, si usted hace cualquier regla de traducción configurar, después inhabilitar esta característica no sigue siendo válido para todo el tráfico y usted necesitará eximir

explícitamente las redes de la traducción de la dirección.

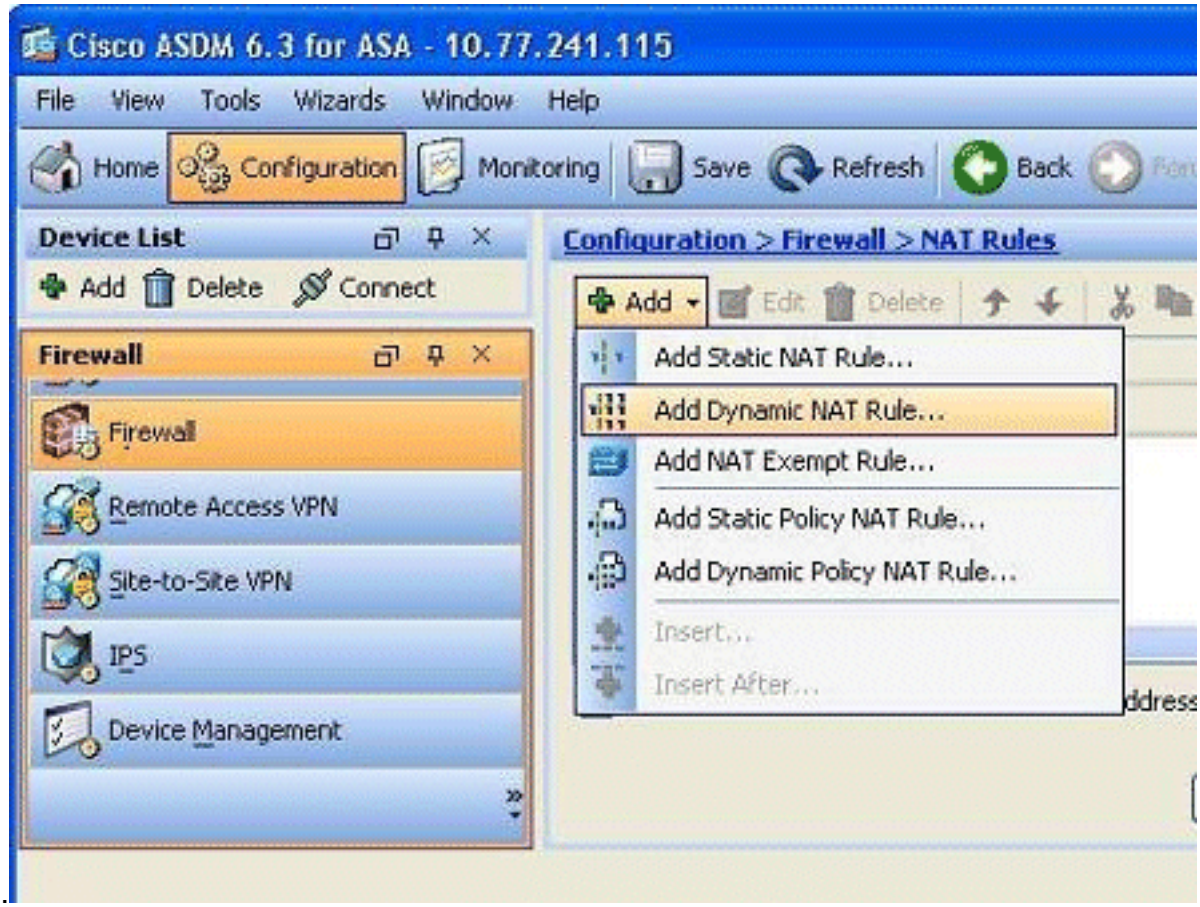


Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT

Usted podría permitir que un grupo de host interiores/de redes acceda el mundo exterior configurando las reglas dinámicas NAT. 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 asociadas a un pool de los IP Addresses traducidos.

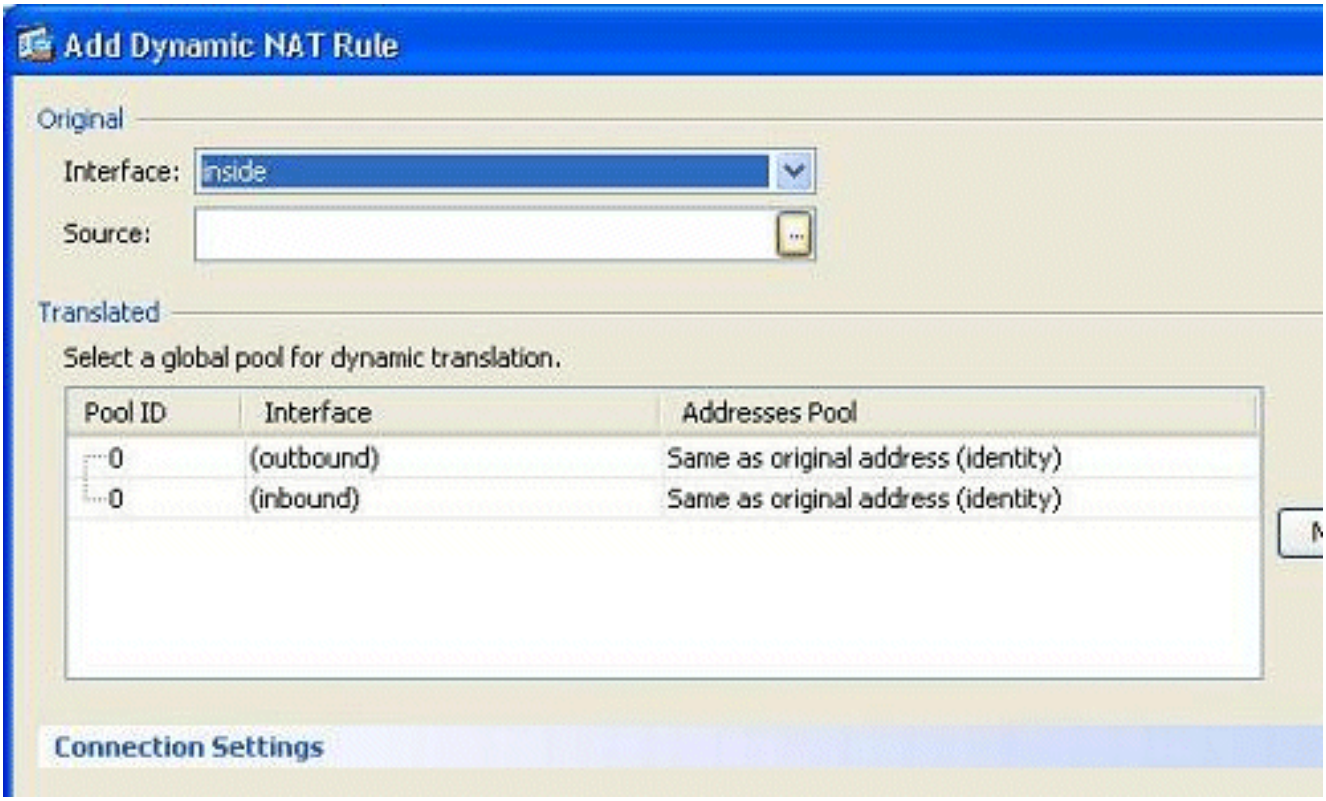
Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con el NAT:

1. Vaya a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y después elige la opción **dinámica de la regla del agregar NAT** para configurar una regla dinámica

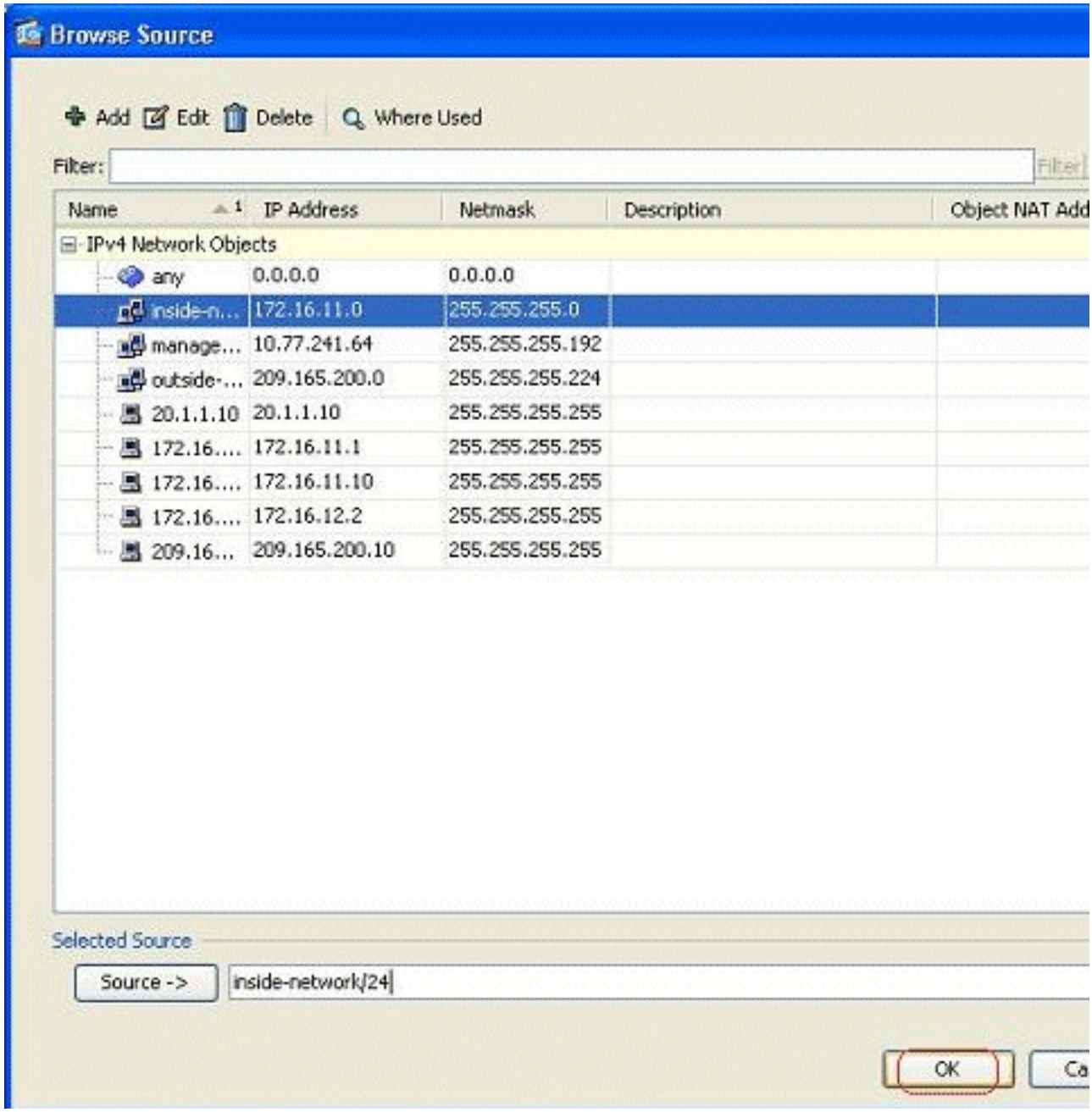


NAT.

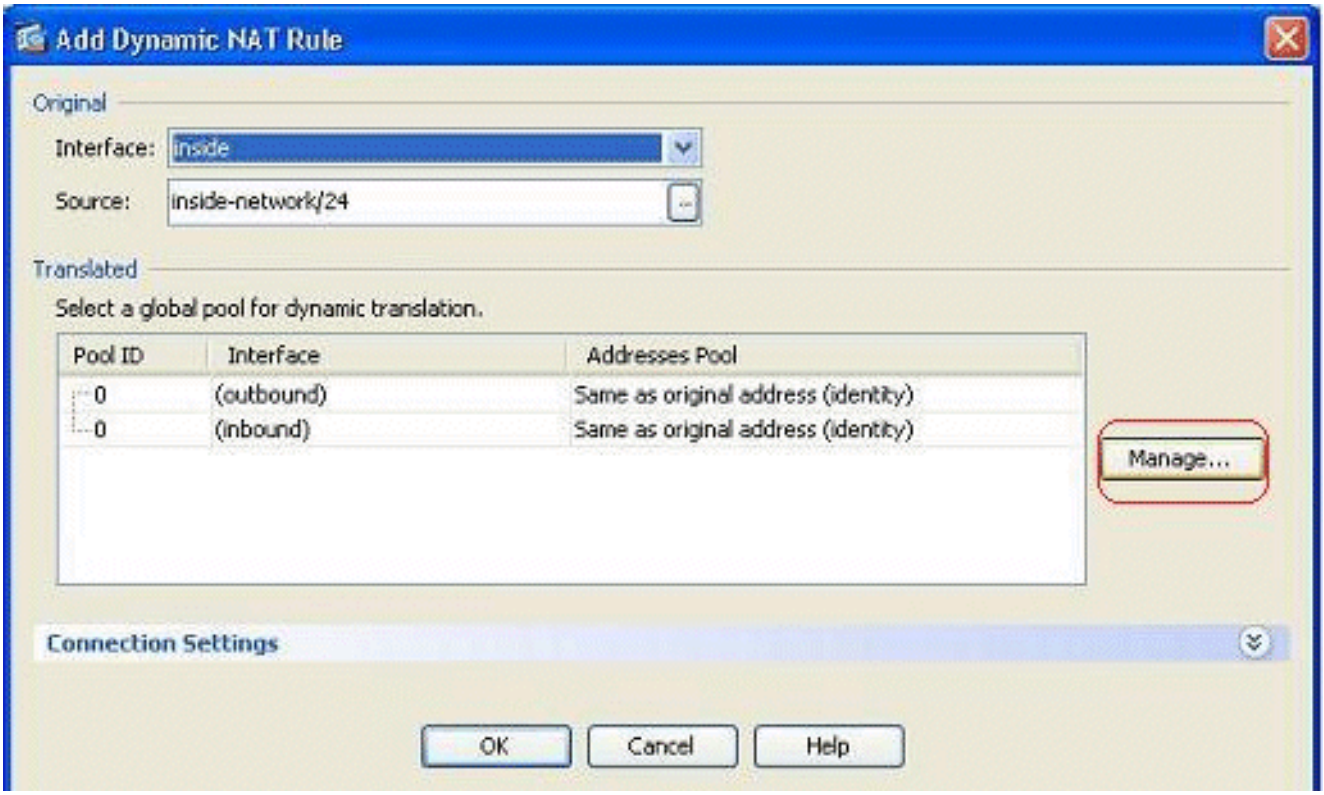
2. Elija el nombre de la interfaz con la cual los host reales están conectados. Elija el IP Address real de los host/de las redes usando el **botón Details Button** en el campo de **fuente**.



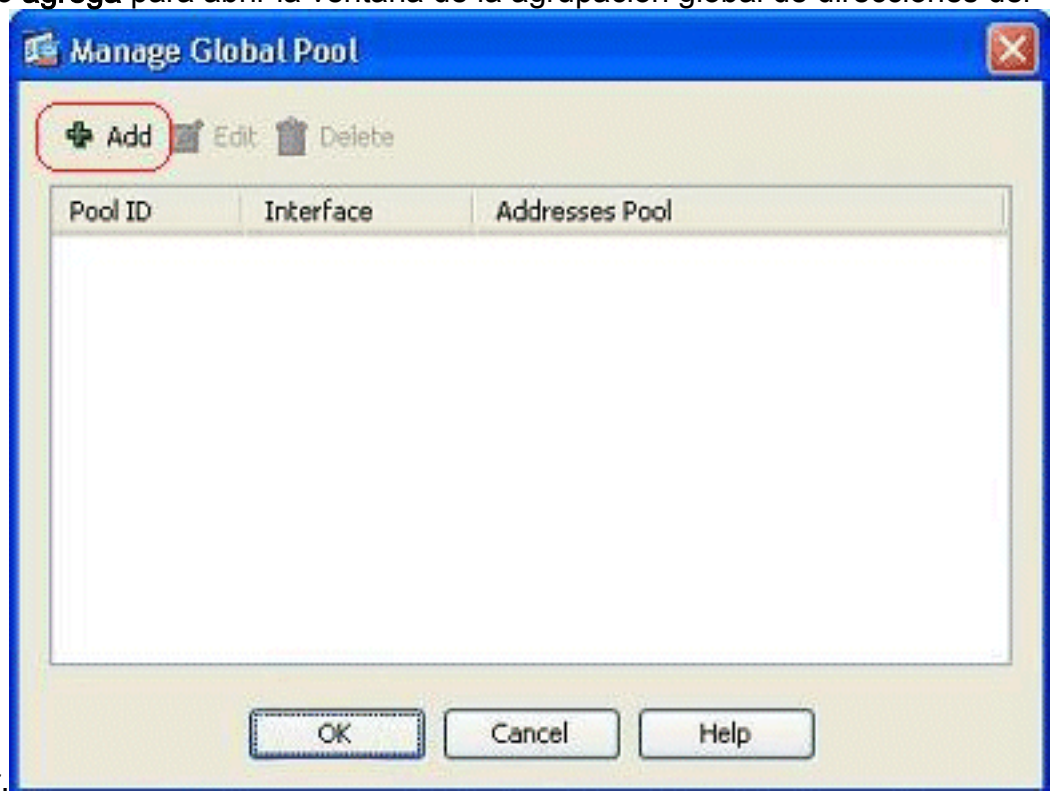
3. En este ejemplo, se ha seleccionado la *red interna* entera. Haga Click en OK para completar la
selección.



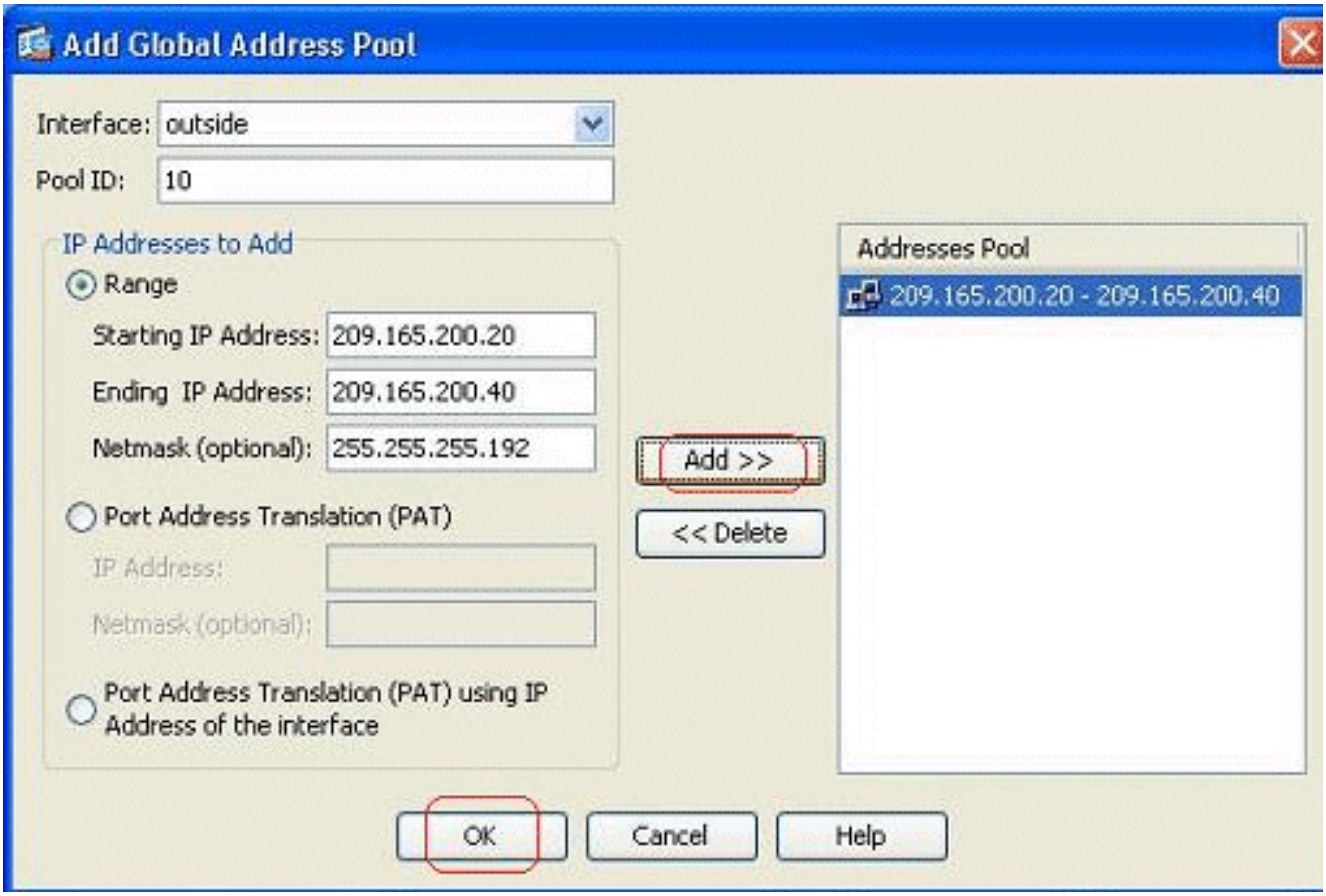
4. El tecleo **maneja** para seleccionar el pool de los IP Addresses a las cuales la red real será asociada.



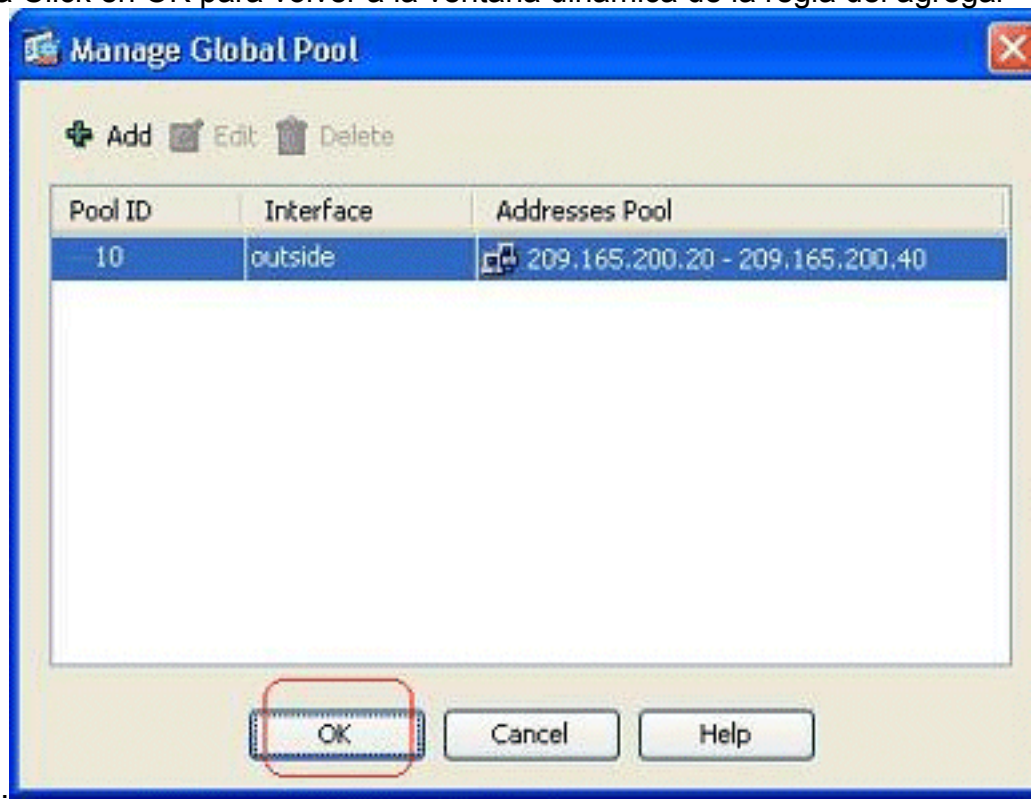
5. El tecleo **agrega** para abrir la ventana de la agrupación global de direcciones del agregar.



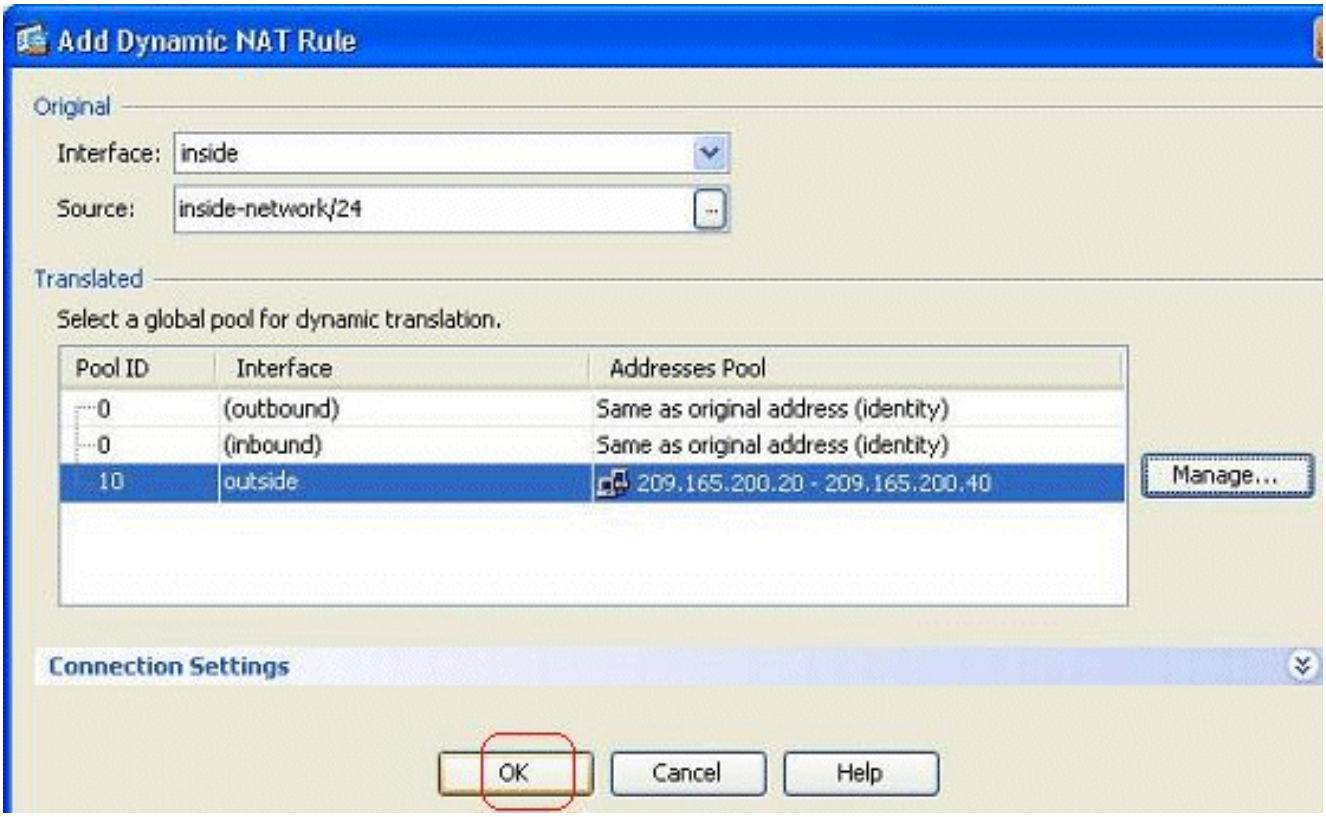
6. Elija la opción del **rango** y especifique los IP Addresses que comienzan y de terminaciones junto con la interfaz de egreso. También, especifique un pool único ID y el tecleo **agregan** para agregar éstos a la agrupación de direcciones. Haga Click en OK para volver a la ventana de la agrupación global del manejo.



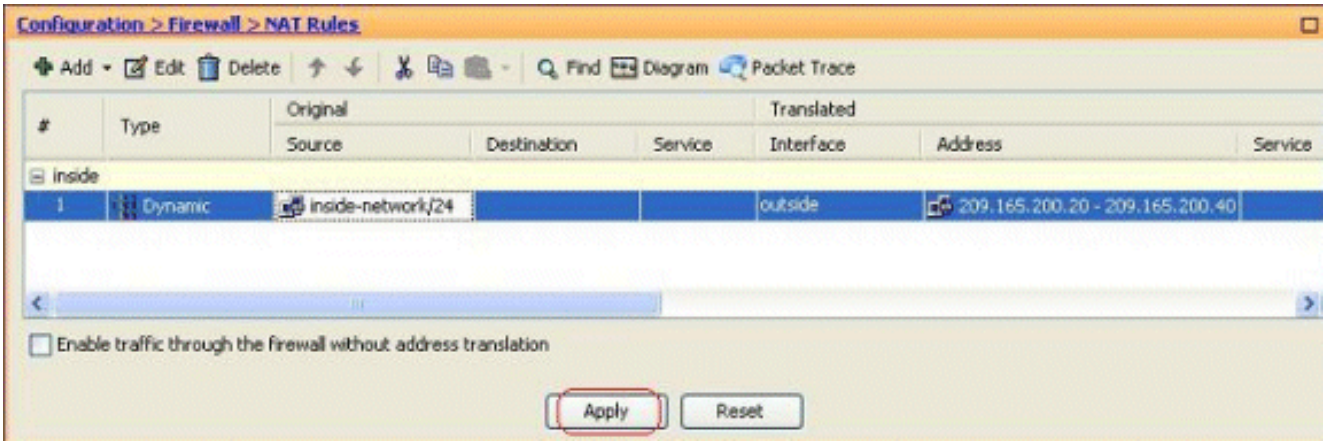
7. Haga Click en OK para volver a la ventana dinámica de la regla del agregar NAT.



8. Haga Click en OK para completar la configuración dinámica de la regla NAT.



9. El tecleo **solicita los** cambios para tomar el efecto.**Nota: El tráfico del permiso con el Firewall sin la** opción de la **traducción de la dirección** se desmarca.



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

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

Según esta configuración, los host en la red de 172.16.11.0 conseguirán traducidos a cualquier dirección IP del agrupamiento NAT, 209.165.200.20-209.165.200.40. Aquí, el agrupamiento NAT ID es muy importante. Usted podría asignar al mismo agrupamiento NAT a otra red interna/del dmz. Si el pool asociado tiene menos direccionamientos que el grupo real, usted podría ejecutarse de los direccionamientos si es la cantidad de tráfico más que esperada. Como consecuencia, usted podría intentar implementar la PALMADITA o usted podría intentar editar a la agrupación de direcciones existente para extenderla.

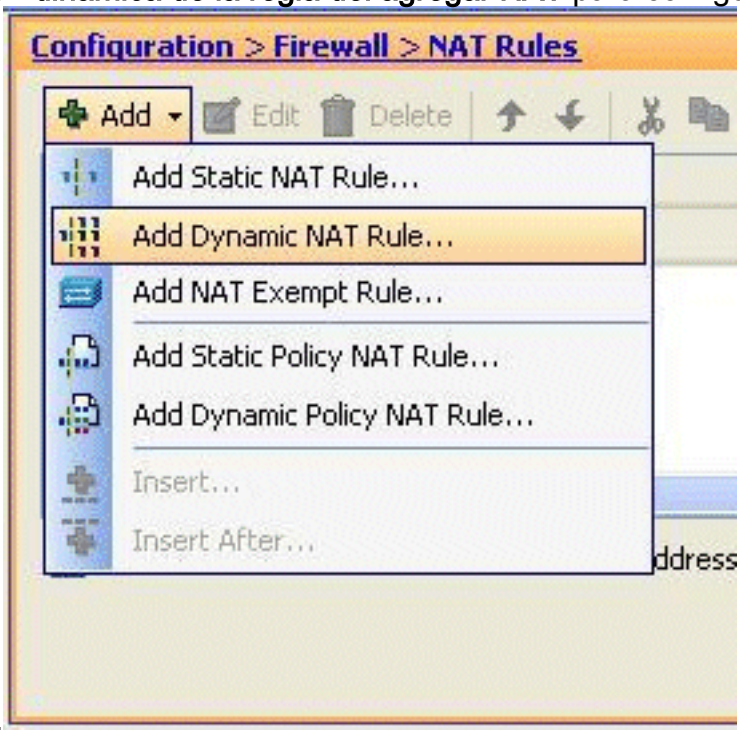
Nota: Mientras que hace cualquier modificación a la regla de la traducción existente, observe que usted necesita utilizar el comando clear xlate para que esas modificaciones tomen el efecto. Si

no, seguirá habiendo la conexión existente anterior allí en la tabla de conexiones hasta ellas descanso. Sea prudente al usar el **comando clear xlate**, porque termina inmediatamente las conexiones existentes.

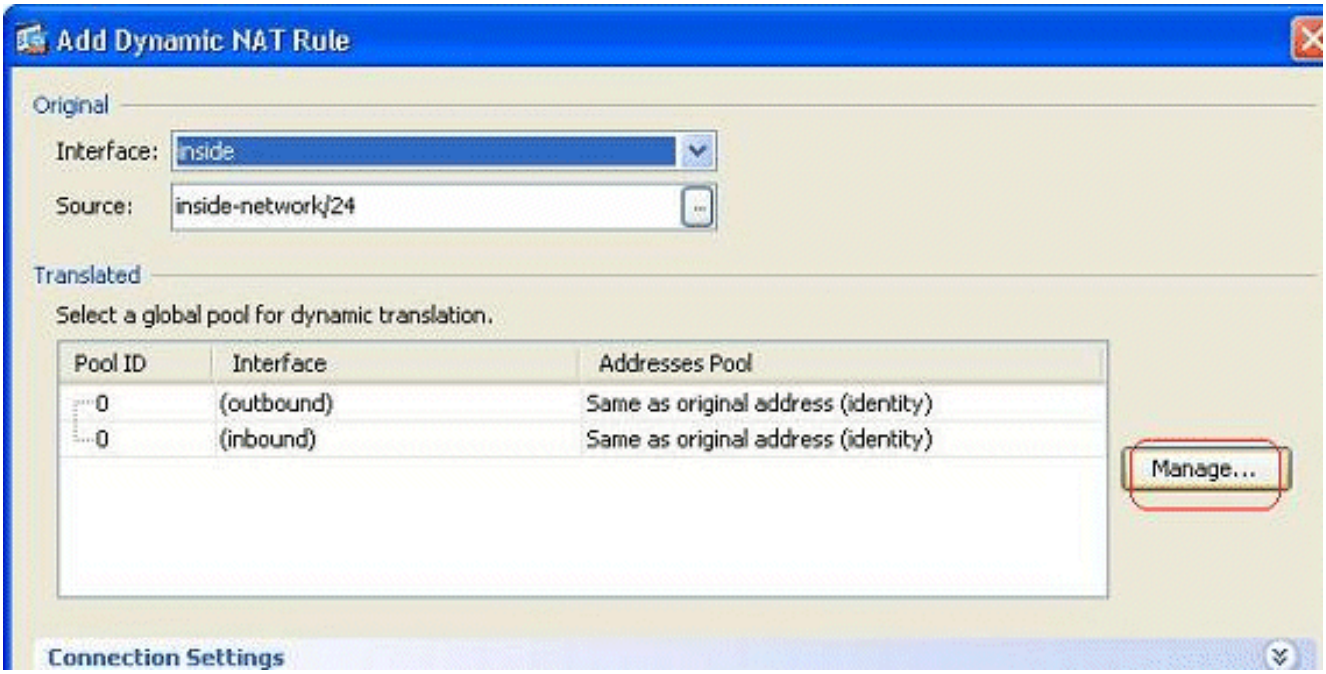
No prohiba a host interiores el acceso a las redes externas con la PALMADITA

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 ASA permite una traducción de puerto por los soportes de la interfaz y de esa traducción hasta 65,535 objetos de traducción activos a la sola dirección global.

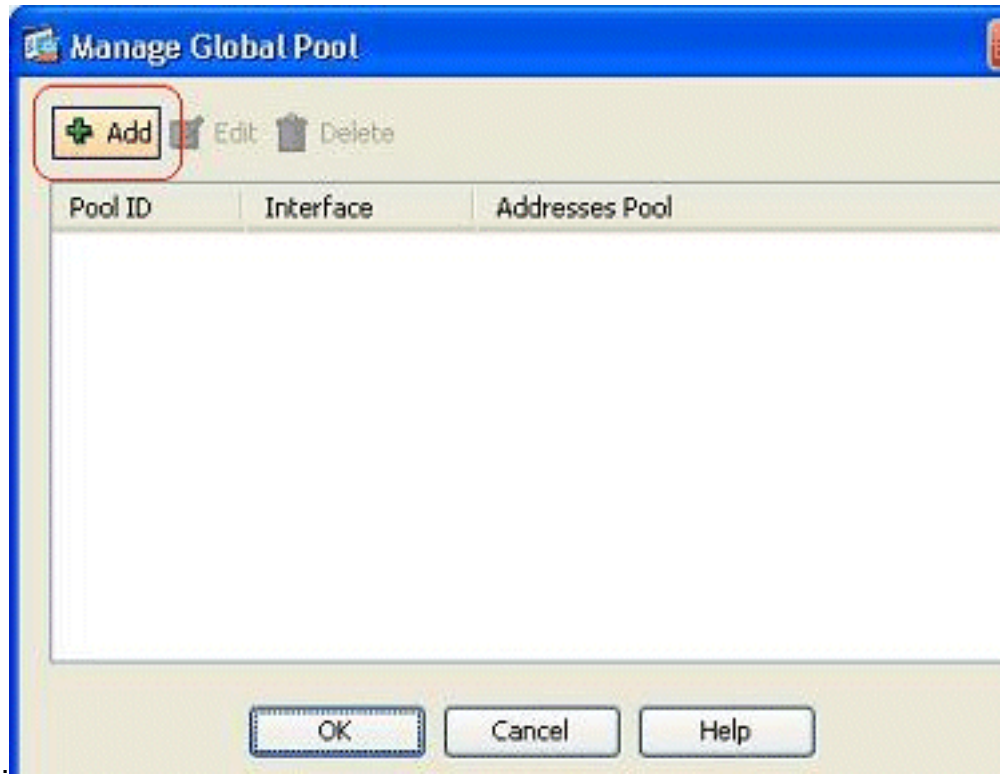
Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con la PALMADITA:

1. Vaya a la **configuración >** al **Firewall >** a las **reglas NAT**, el tecleo **agrega**, y después elige la opción **dinámica de la regla del agregar NAT** para configurar una regla dinámica NAT.


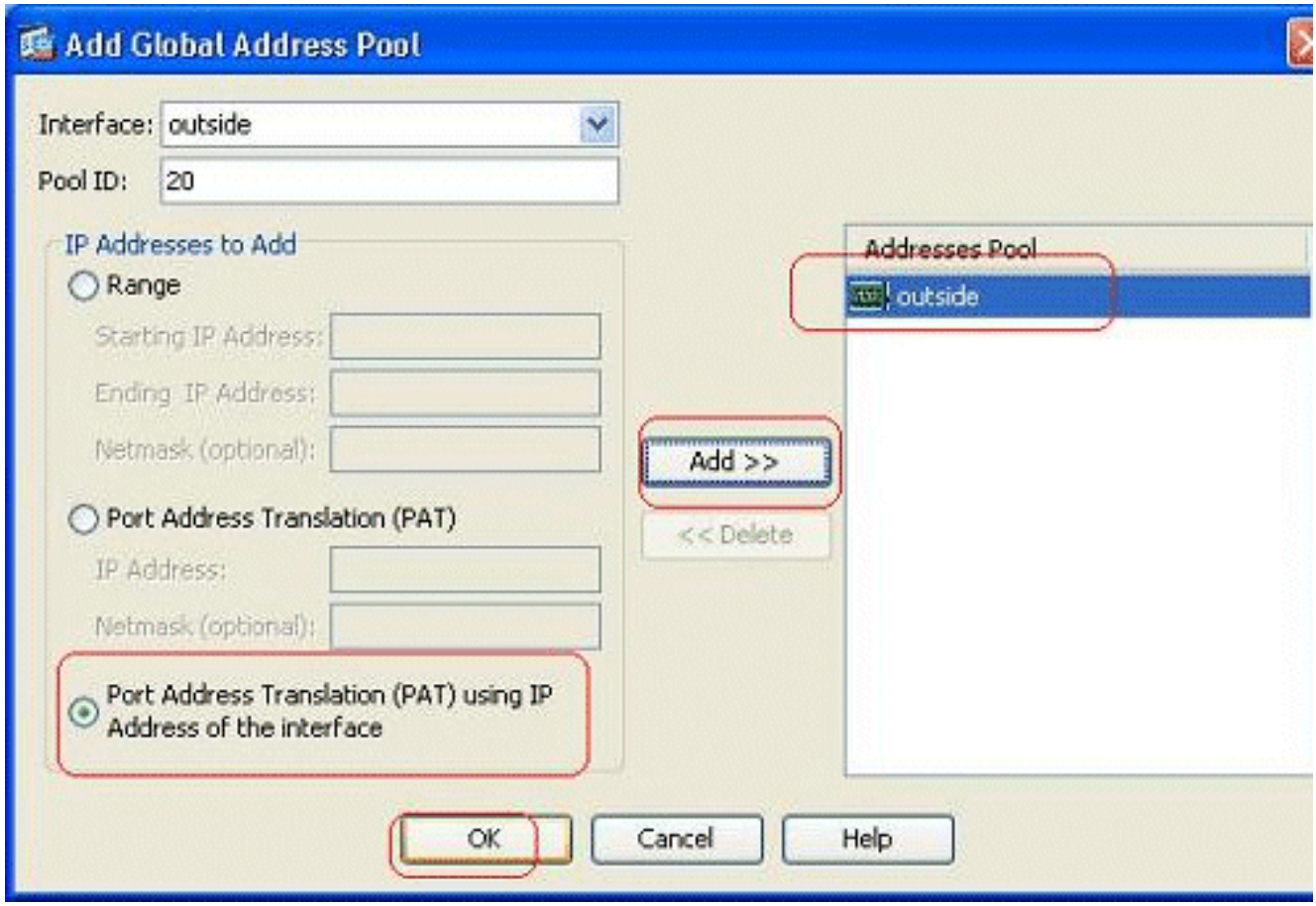
2. Elija el nombre de la interfaz con la cual los host reales están conectados. Elija el IP Address real de los host/de las redes usando el **botón Details Button** en el campo de **fuente**, y elija la **red interna**. El tecleo **maneja** para definir la información de dirección traducida.



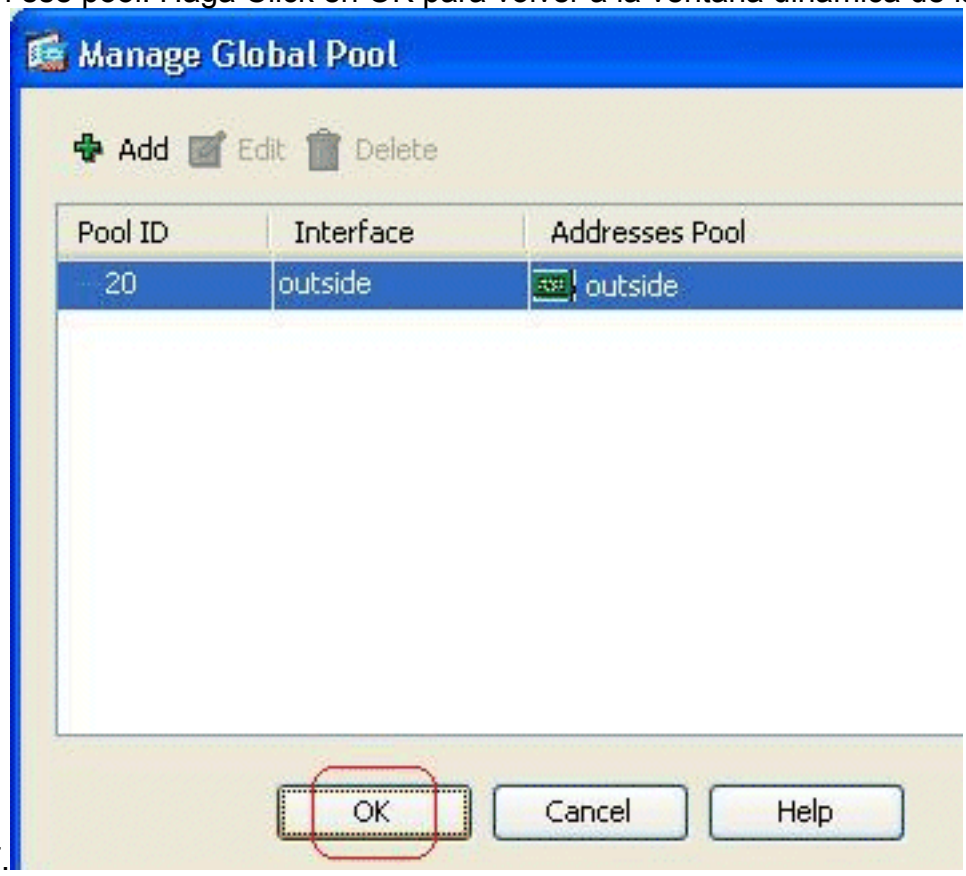
3. Haga clic en Add (Agregar).



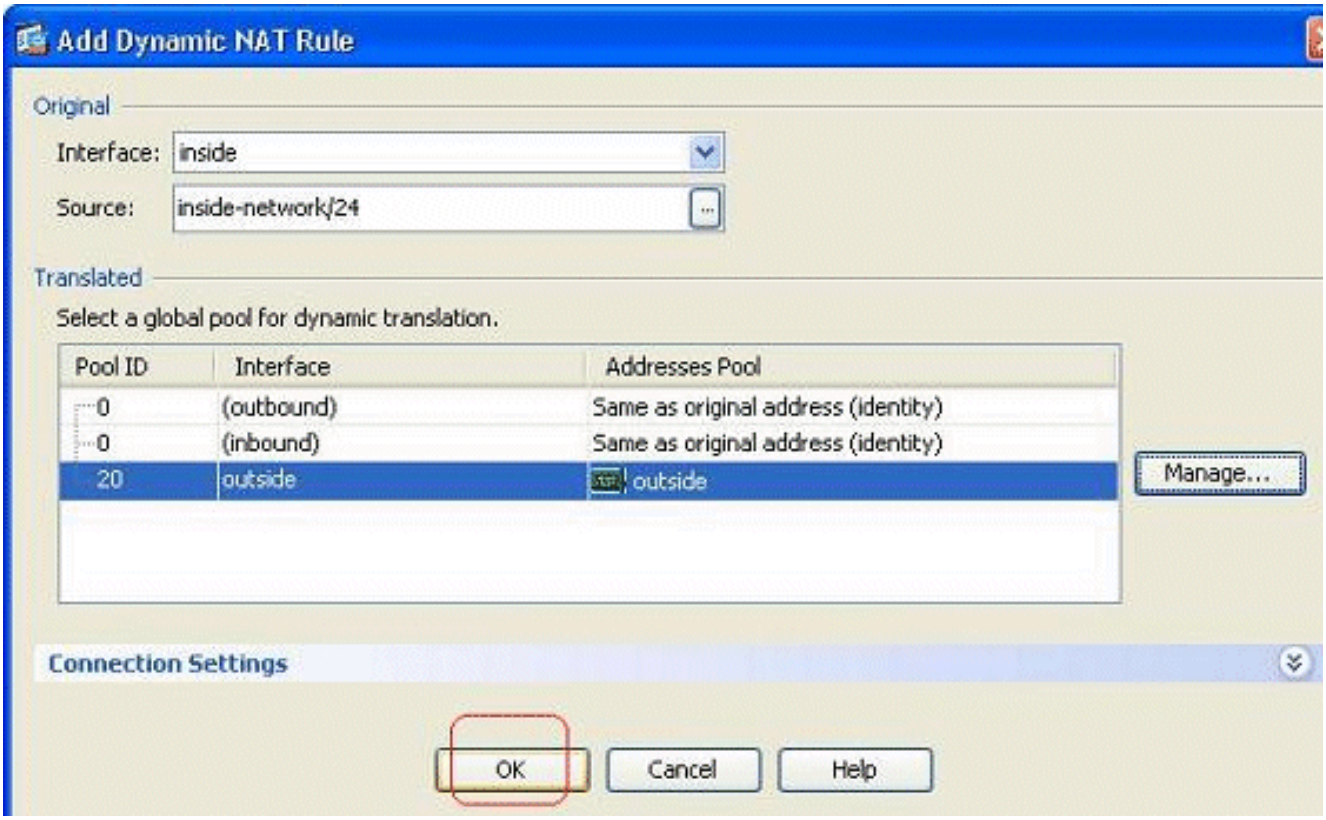
4. Elija el **Port Address Translation (PAT) usando la dirección IP de la Opción de interfaz**, y el tecleo **agrega** para agregarla a la agrupación de direcciones. No olvide asignar un ID único para este conjunto de direcciones
NAT.



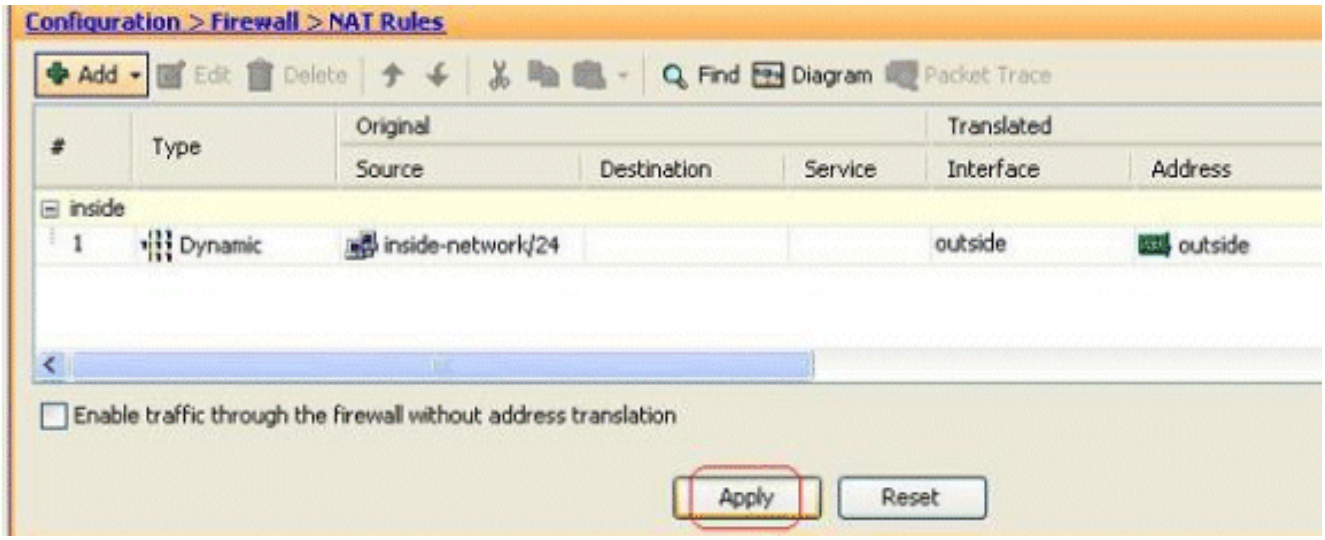
5. Se muestra aquí el pool de la dirección configurada con la interfaz exterior como la única dirección disponible en ese pool. Haga Click en OK para volver a la ventana dinámica de la regla del agregar NAT.



6. Haga clic en OK.



7. La regla dinámica configurada NAT se muestra aquí en cristal la configuración > el Firewall > de las reglas
   NAT.



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

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

Limita el acceso de los Hosts Interiores a las Redes Externas

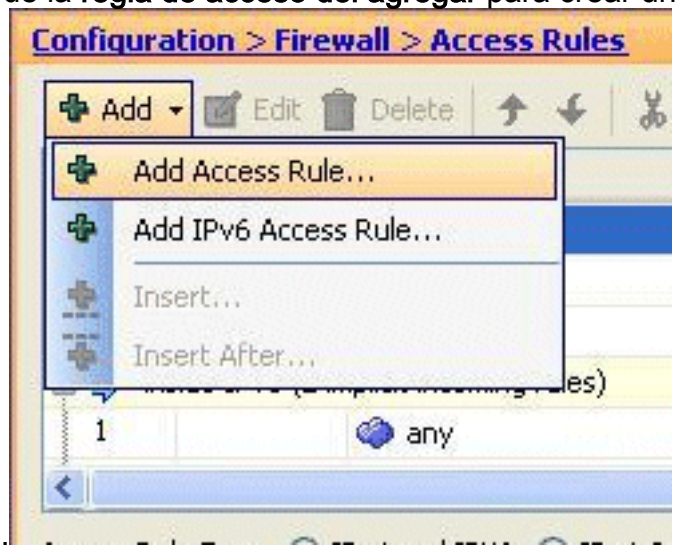
Cuando no se define ningunas reglas de acceso, los usuarios de una interfaz de mayor seguridad pueden acceder cualquier recurso asociado a una interfaz de menor seguridad. Para restringir a los ciertos usuarios de acceder ciertos recursos, utilice las reglas de acceso en el ASDM. Este ejemplo describe cómo permitir que un único usuario acceda los recursos exteriores (con el FTP, el S TP, el POP3, el HTTPS, y el WWW) y restrinja todos los demás de acceder los recursos

exteriores.

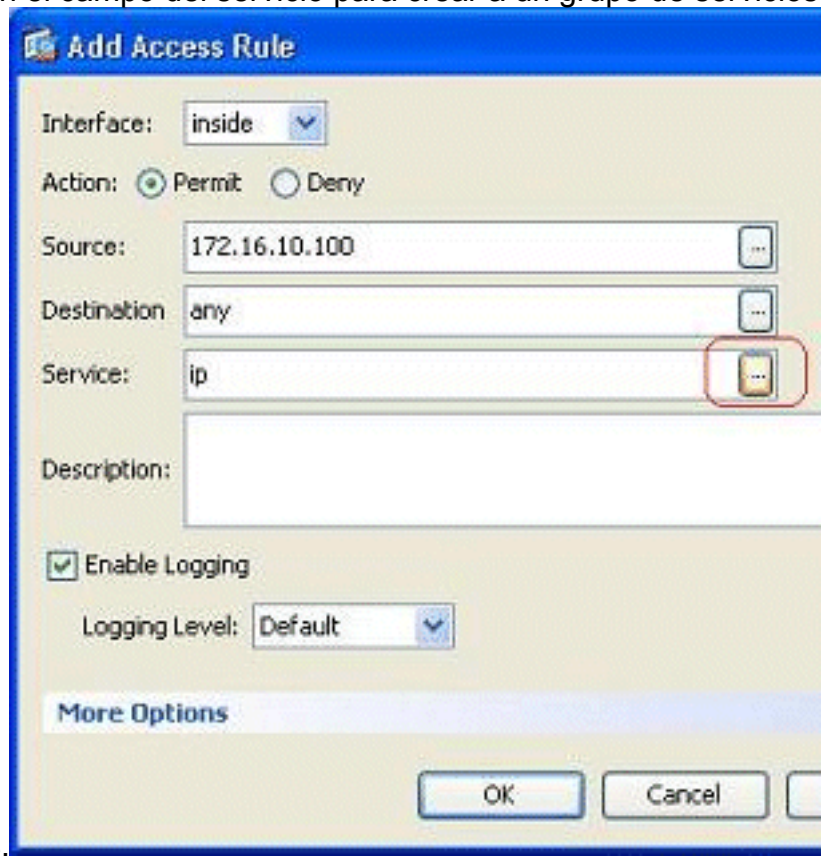
Nota: Habrá un “implícito niega” la regla en el extremo de cada lista de acceso.

Complete estos pasos:

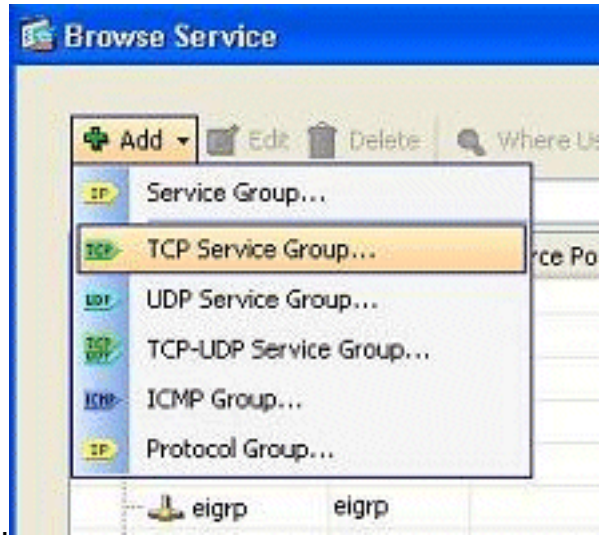
1. Vaya a la **configuración** > al **Firewall** > a las **reglas de acceso**, el tecleo **agrega**, y elige la opción de la **regla de acceso del agregar** para crear una nueva entrada de lista de acceso.



2. Elija la dirección IP de origen que debe ser permitida en el campo de **fuente**. Elija **ningunos** como el destino, **dentro** como de la interfaz, y **permita** como la acción. Pasado, haga clic el **botón Details Button** en el campo del servicio para crear a un grupo de servicios TCP para los puertos requeridos.

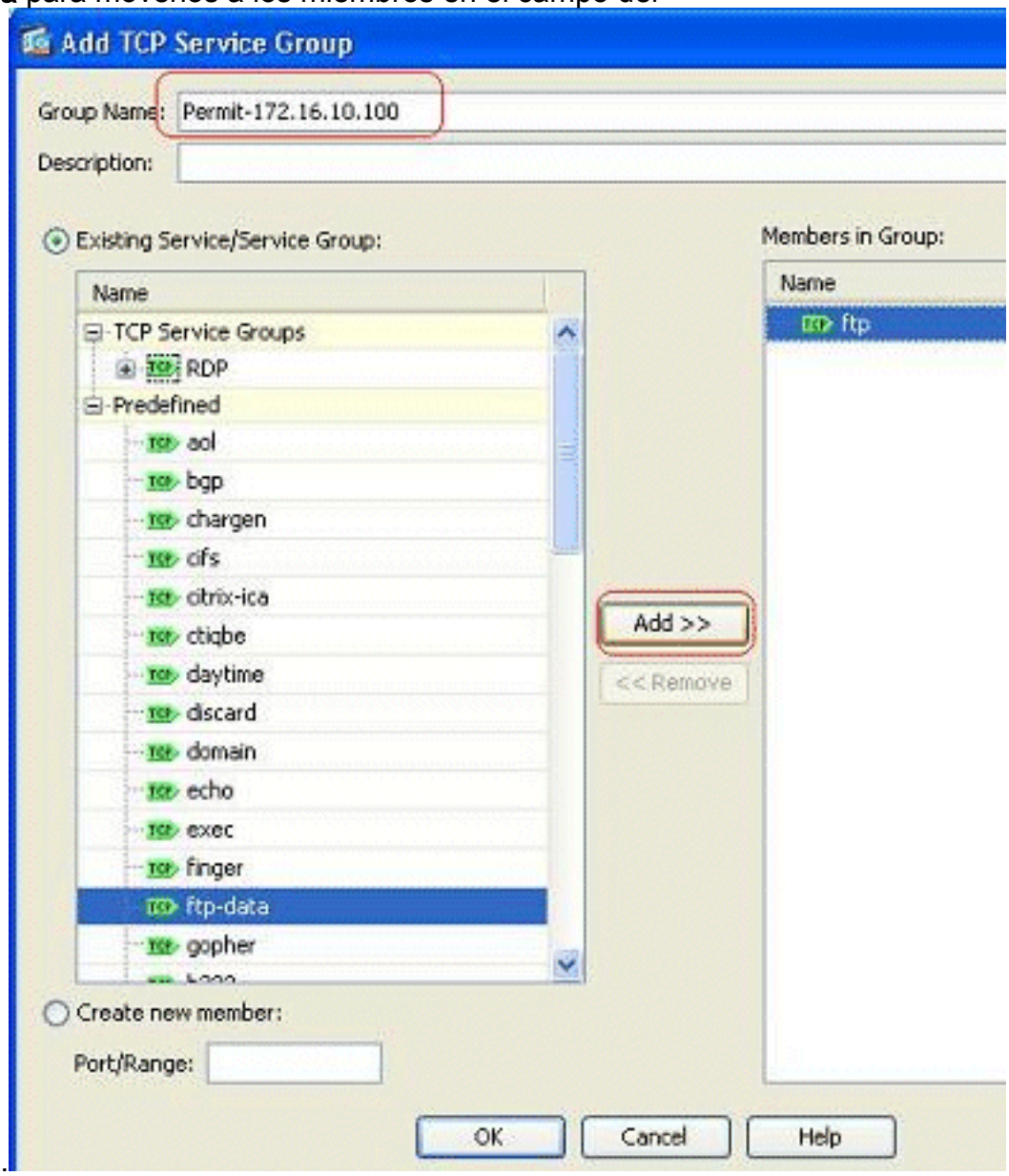


3. El tecleo **agrega**, y después elige la opción del **grupo de servicios**



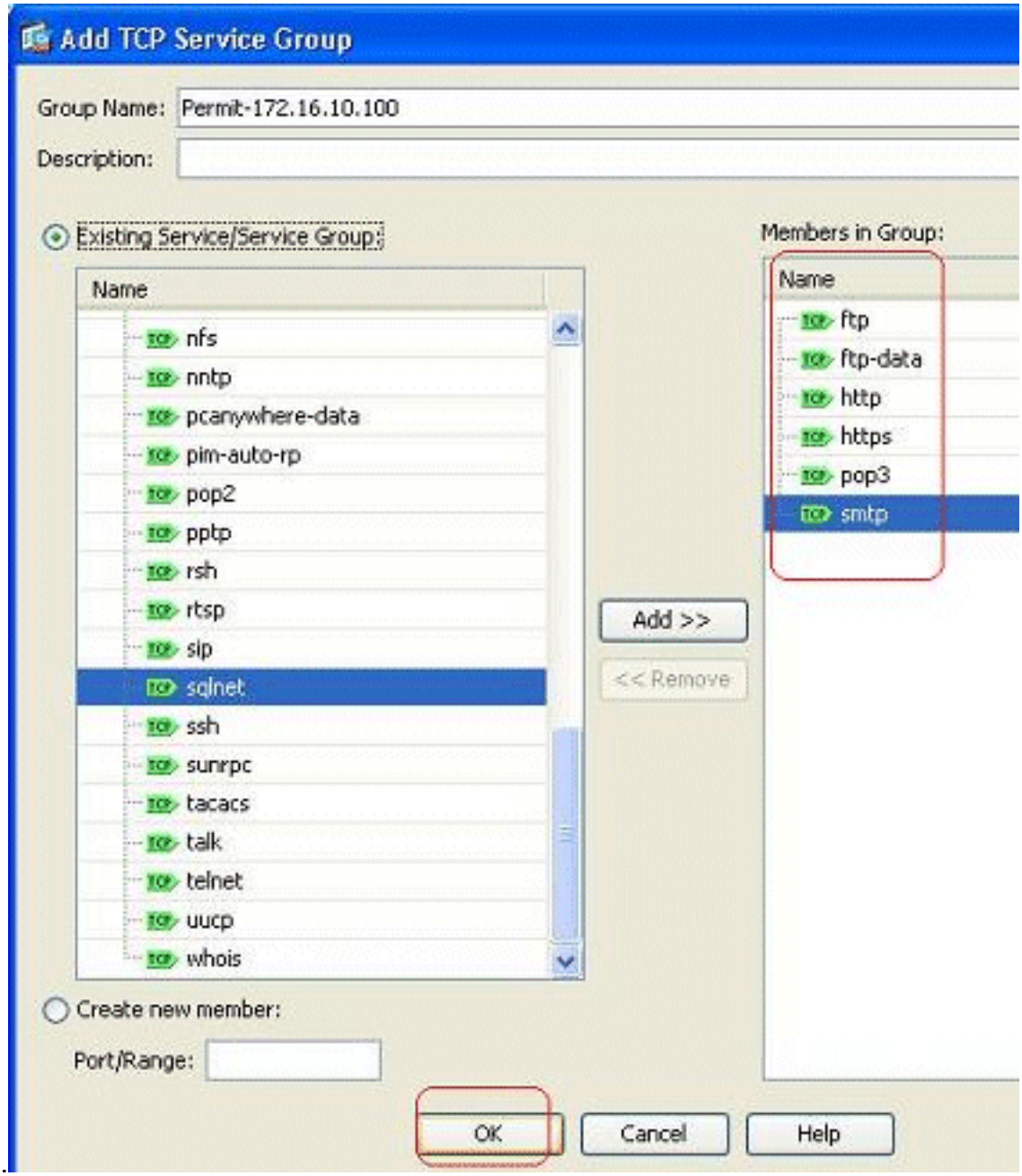
TCP.

4. Ingrese un nombre para este grupo. Elija cada uno de los puertos requeridos, y el tecleo **agrega** para moverlos a los miembros en el campo del



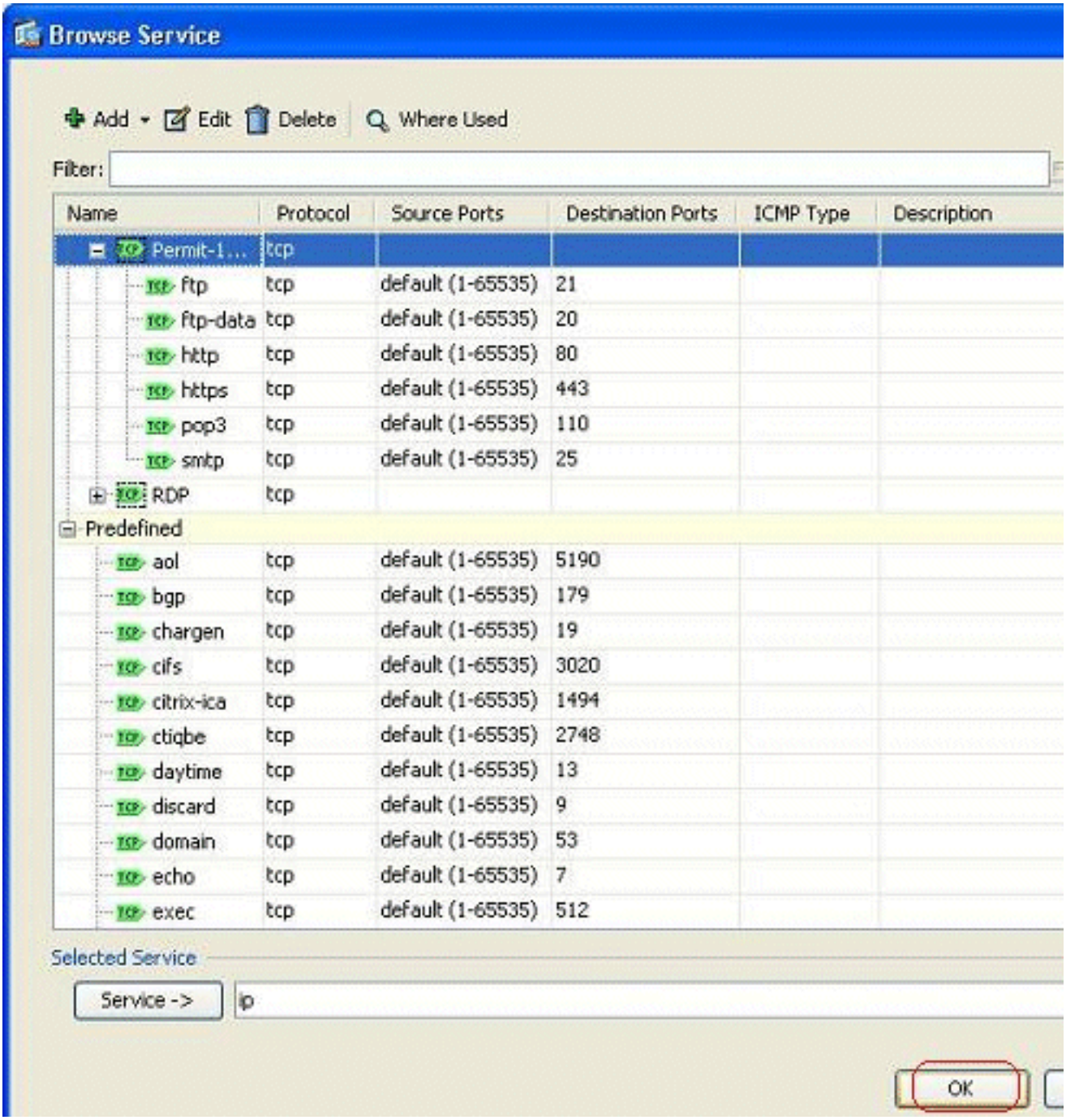
grupo.

5. Usted debe ver todos los puertos seleccionados en el campo derecho. El Haga Click en OK para completar el servicio vira la selección hacia el lado de babor del

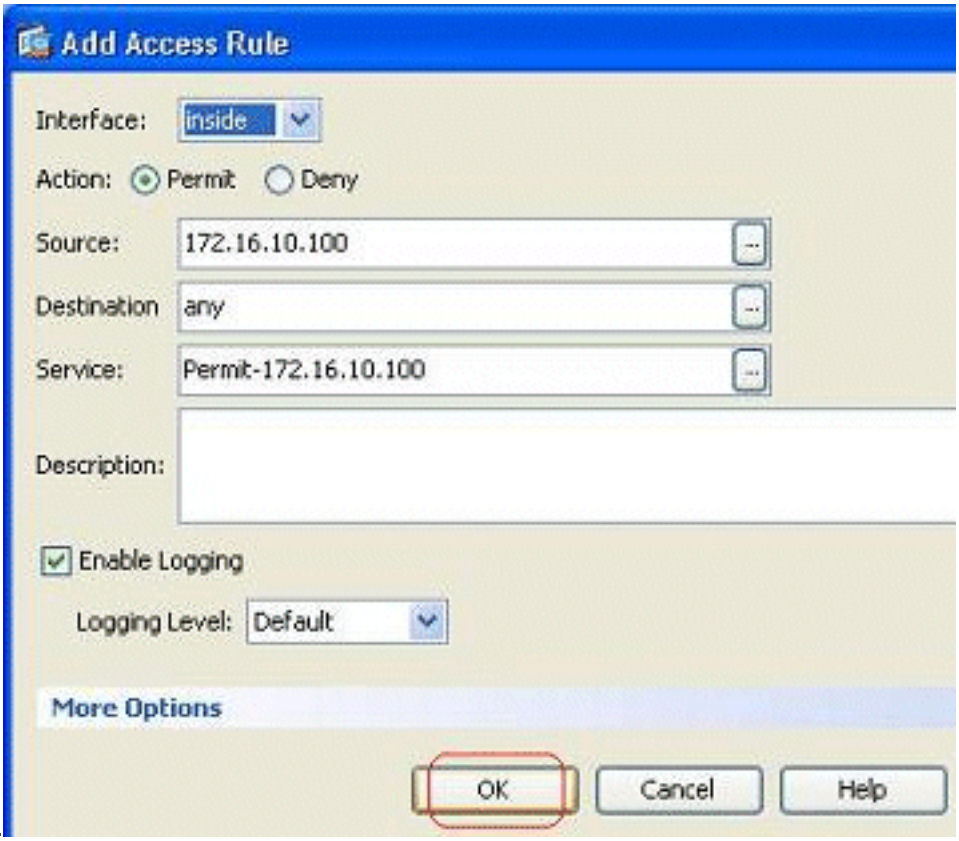


proceso.

6. Usted puede ver al grupo de servicios configurado TCP aquí. Haga clic en OK.

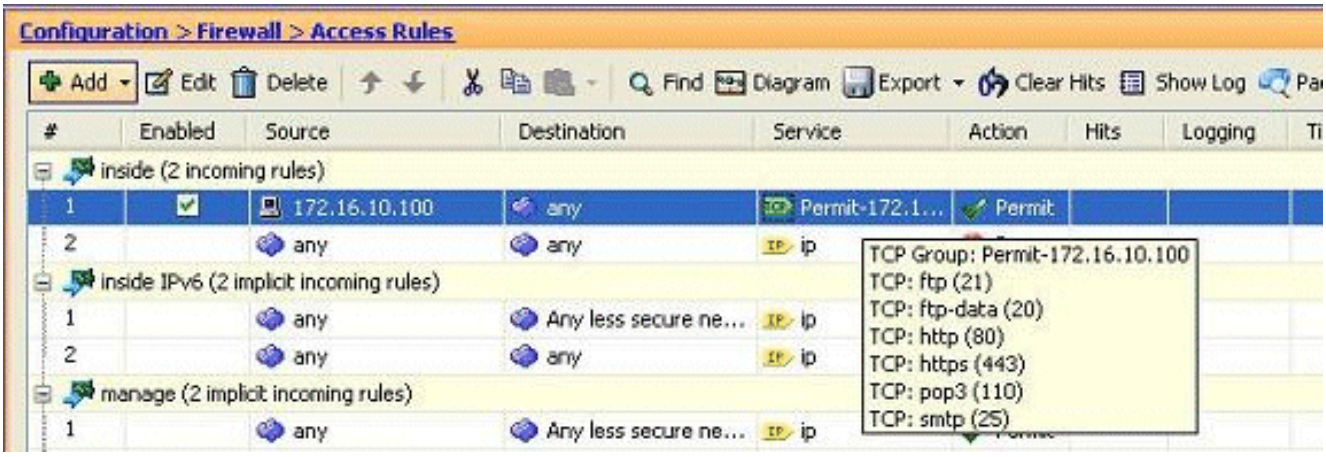


7. Haga Click en OK para completar la

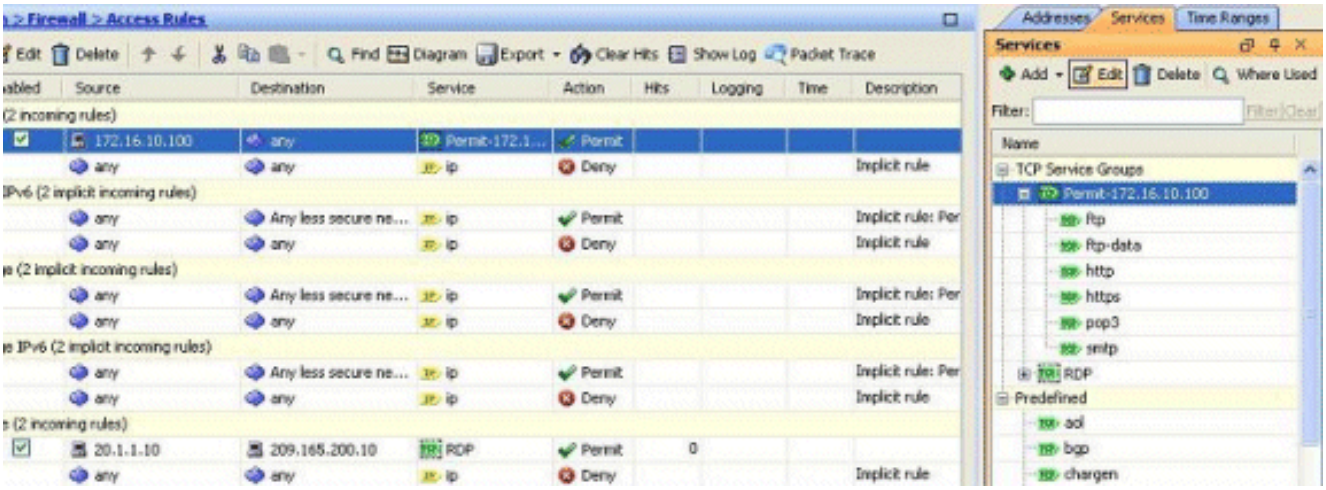


configuración.

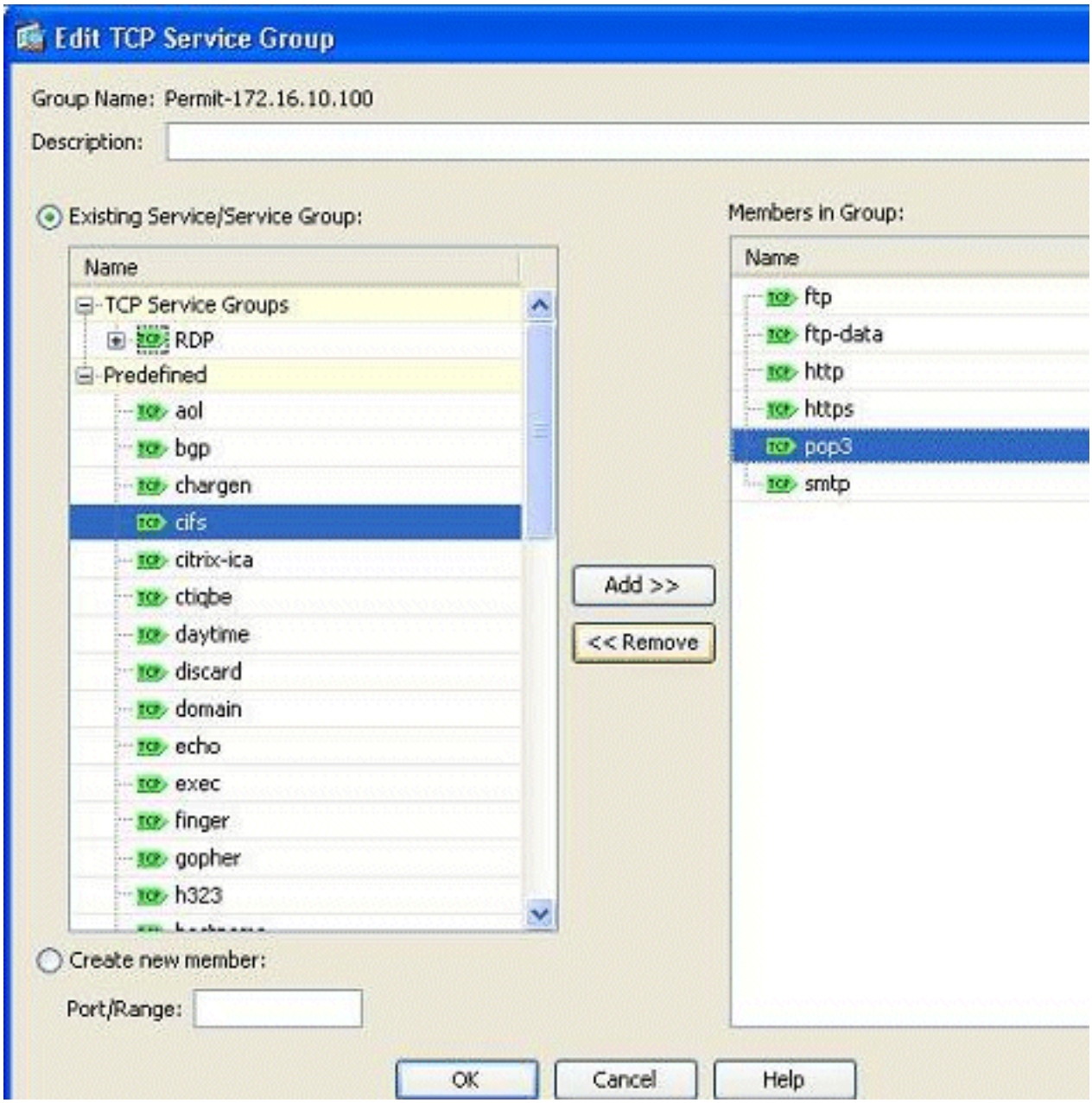
8. La regla del acceso configurado se puede considerar bajo **interfaz interior** en el cristal de la configuración > del Firewall > de las reglas de acceso.



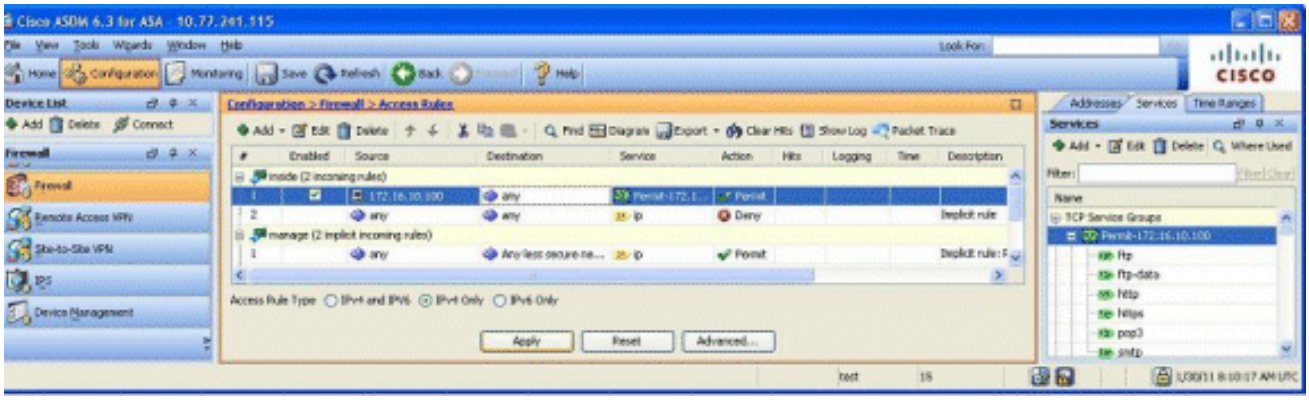
9. Para la facilidad de empleo, usted podría también editar al grupo de servicios TCP directamente en el panel derecho en los **servicios que el** tecleo de cuadro **edita** para modificar este grupo de servicios directamente.



10. Reorienta otra vez a la ventana de grupo de servicios del editar TCP. Realice las modificaciones basadas en sus requisitos, y haga clic la **AUTORIZACIÓN** para salvar los cambios.



11. Se muestra aquí una vista completa del ASDM:



Ésta es la configuración CLI equivalente:

```
object-group service Permit-172.16.10.100 TCP
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
    object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

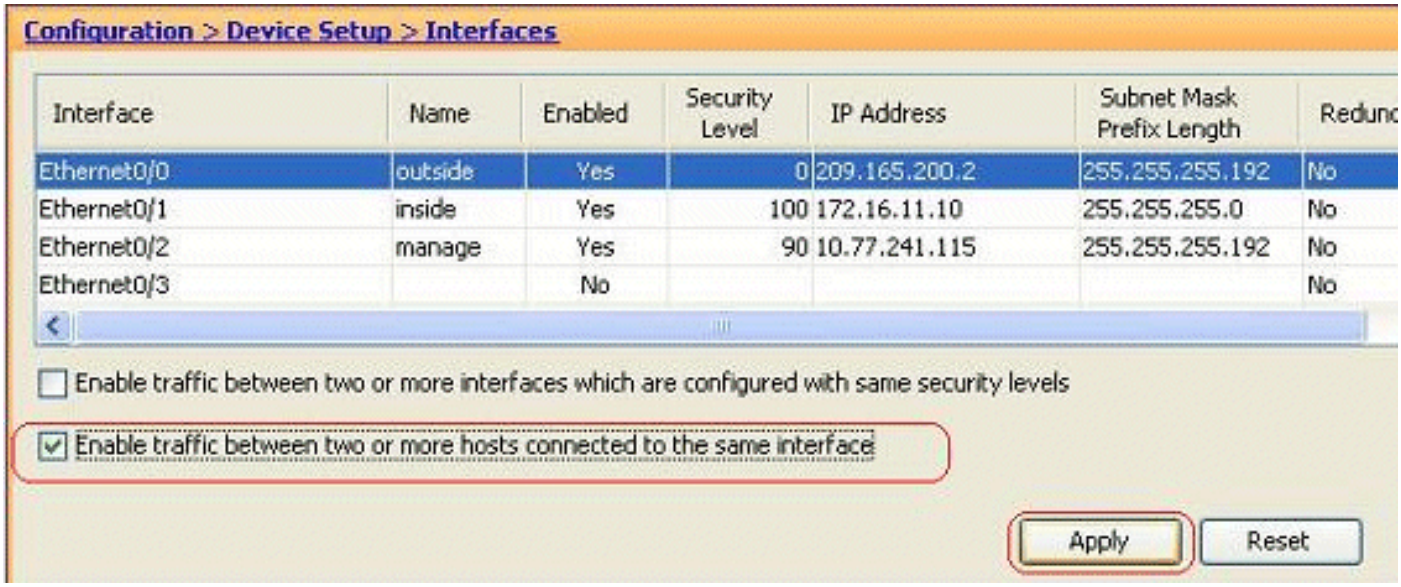
Para toda la información sobre implementar el control de acceso, refiérase agregan o modifican una lista de acceso con el ASDM GUI.

Permita el tráfico entre las interfaces con el mismo nivel de seguridad

Esta sección describe cómo habilitar el tráfico dentro de las interfaces que tienen los mismos niveles de seguridad.

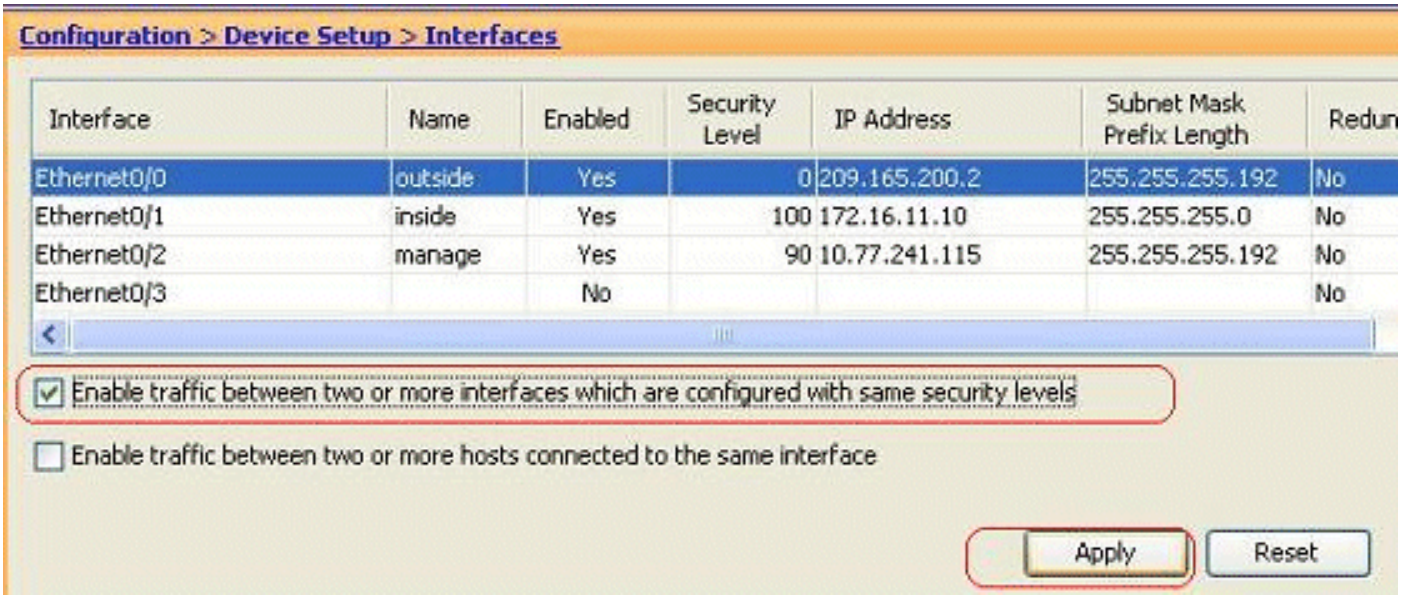
Estas instrucciones describen cómo habilitar la comunicación de la intra-interfaz.

Esto será útil para el tráfico VPN que ingresa una interfaz, pero después se rutea hacia fuera la misma interfaz. El tráfico VPN pudo ser unencrypted en este caso, o puede ser que sea encriptado nuevamente para otra conexión VPN. Va a la **configuración** > la **configuración de dispositivo** > las **interfaces**, y elige el **tráfico del permiso entre dos o más host conectados con la misma Opción de interfaz**.



Estas instrucciones describen cómo habilitar la comunicación de la inter-interfaz.

Esto es útil para permitir la comunicación entre las interfaces con los niveles de seguridad iguales. Va a la **configuración** > la **configuración de dispositivo** > las **interfaces**, y elige el **tráfico del permiso entre dos o más interfaces que se configuran con la misma** opción de los **niveles de seguridad**.



Éste es el CLI equivalente para ambas configuraciones:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

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. Usted requiere para 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 soldado IP del servidor a un IP del público. Este ejemplo describe cómo implementar el NAT estático bidireccional para traducir 172.16.11.5 a 209.165.200.5.

La sección en permitir que el usuario externo acceda a este servidor Web implementando una regla del acceso no se muestra aquí. Un snippet de la descripción CLI se muestra aquí para su comprensión:

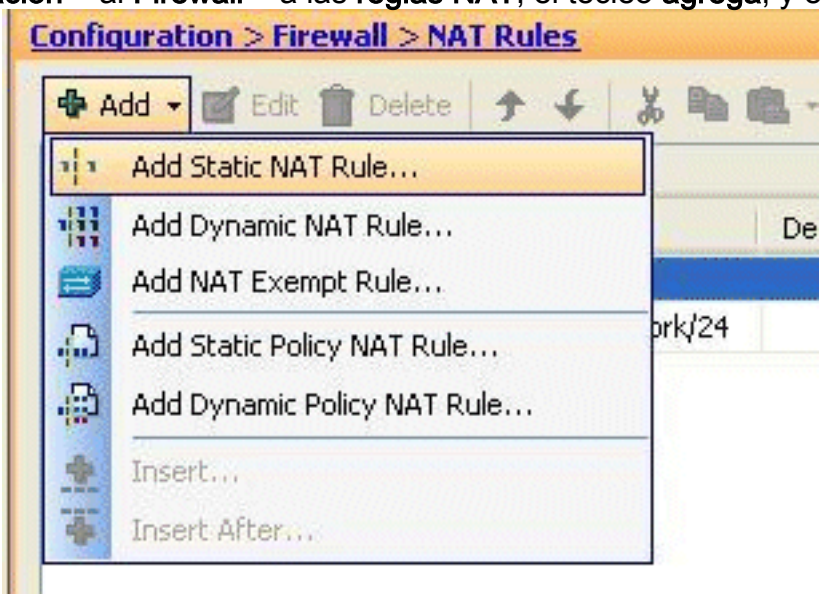
```
access-list 101 permit TCP any host 209.165.200.5
```

Para más información, refiérase agregan o modifican una lista de acceso con el ASDM GUI.

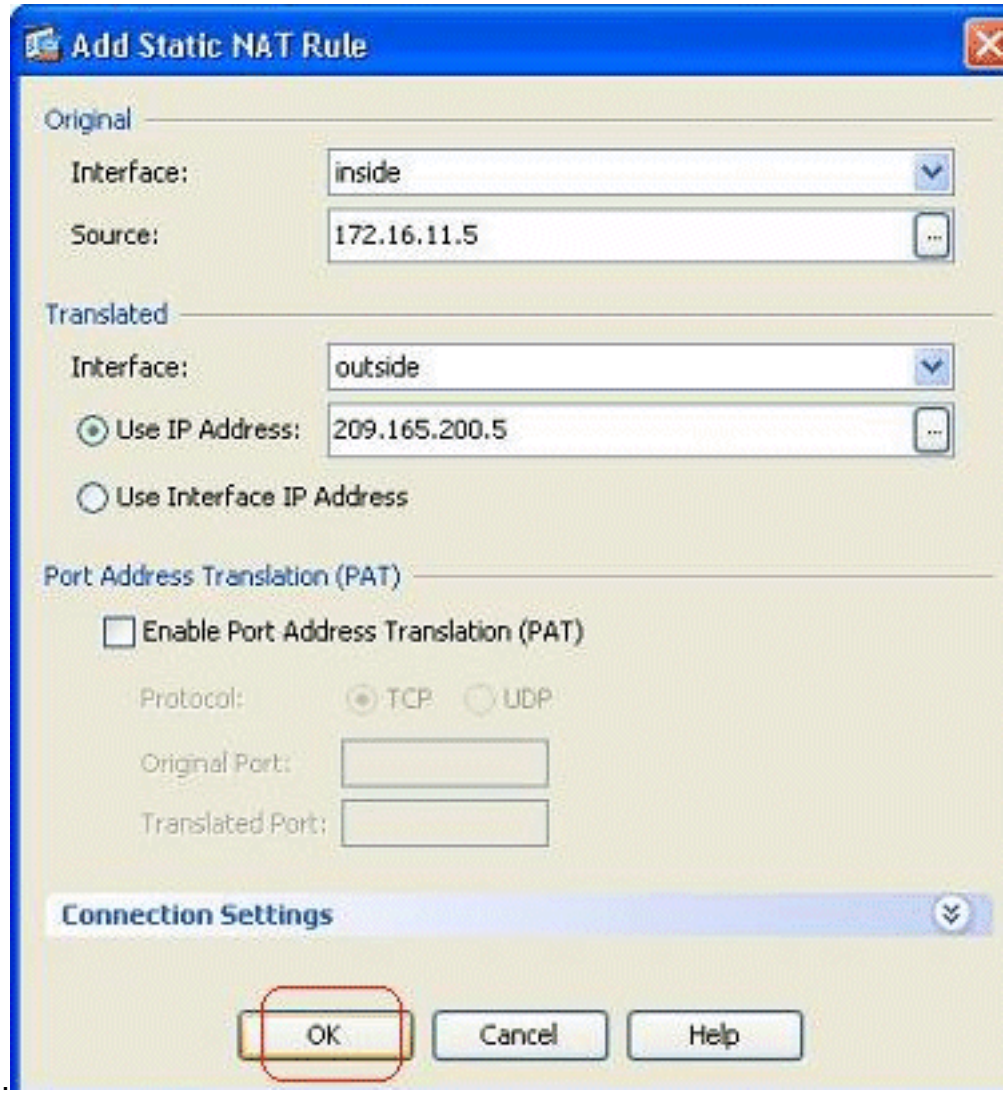
Nota: Especificar la palabra clave "" permite que cualquier usuario del mundo exterior acceda este servidor. También, si no se especifica para ninguna puertos del servicio, el servidor se puede acceder en cualquier puerto del servicio mientras que eso estancia abierta. Tenga cuidado cuando usted implementa, y le aconsejan limitar el permiso al usuario externo individual y también al puerto requerido en el servidor.

Complete estos pasos para configurar el NAT estático:

1. Vaya a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y elige **agrega la regla NAT estática**.

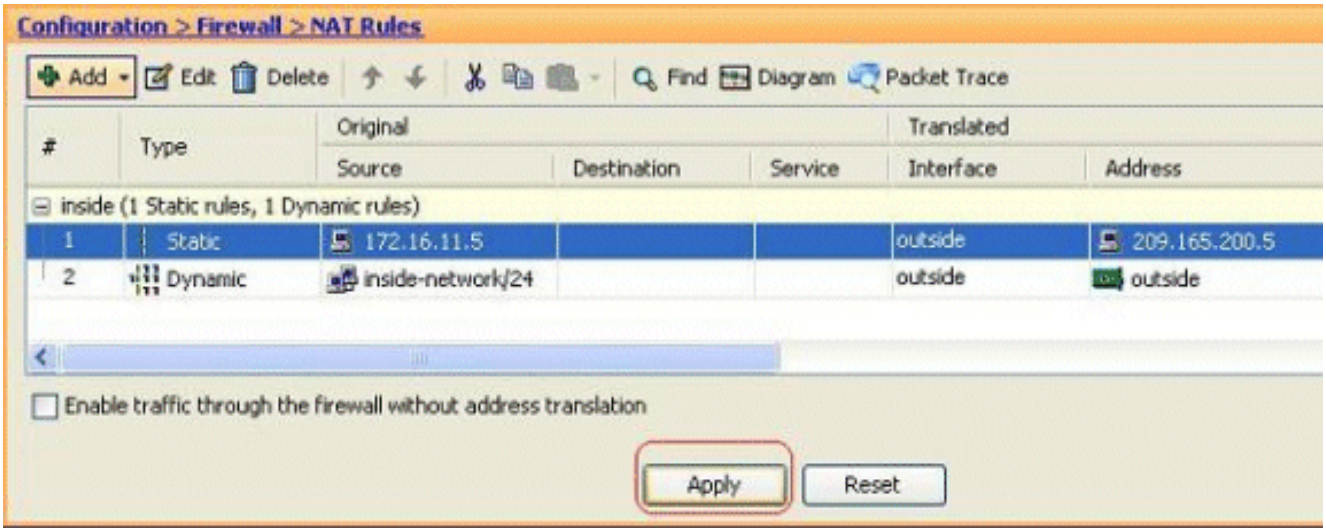


2. Especifique el IP Address original y la dirección IP traducida junto con sus interfaces asociadas, y haga clic la



AUTORIZACIÓN.

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



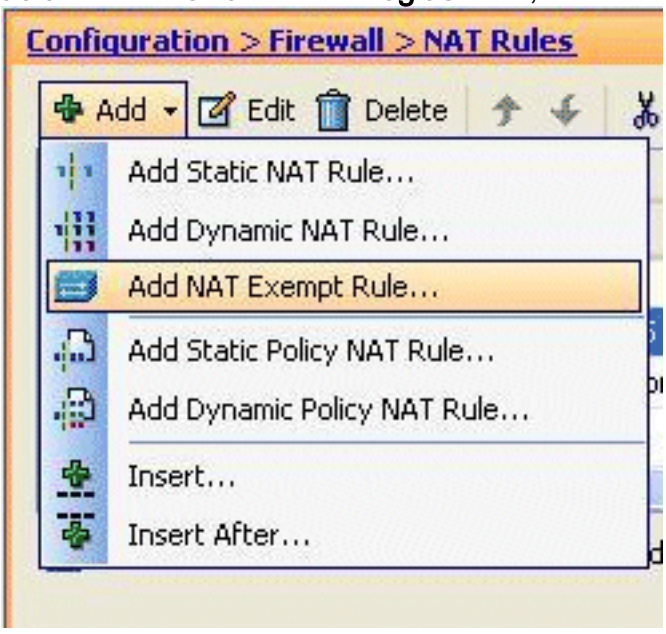
Esto es un ejemplo de la descripción CLI para esta Configuración de ASDM:

```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

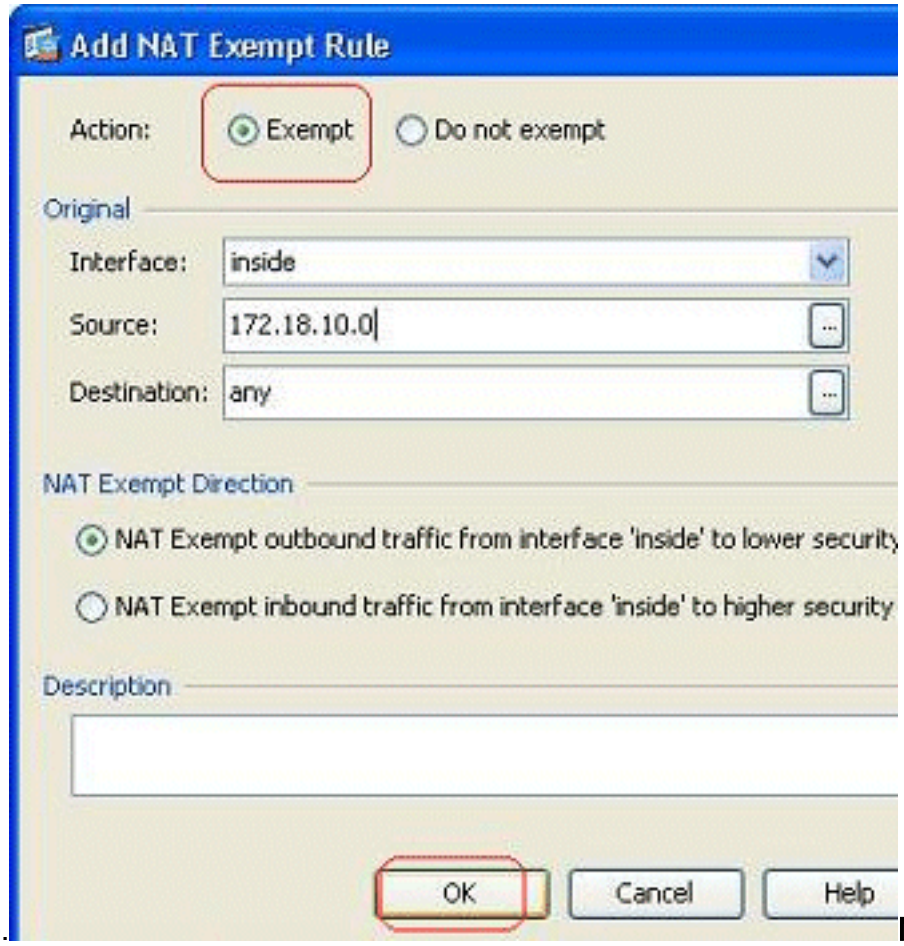
Inhabilite NAT para los Hosts/Redes Específicos

Cuando usted necesita eximir los host o las redes específicos del NAT, agregue una regla exenta NAT para inhabilitar la traducción de la dirección. Esto permite traducido y los host remotos para iniciar las conexiones.

Complete estos pasos:

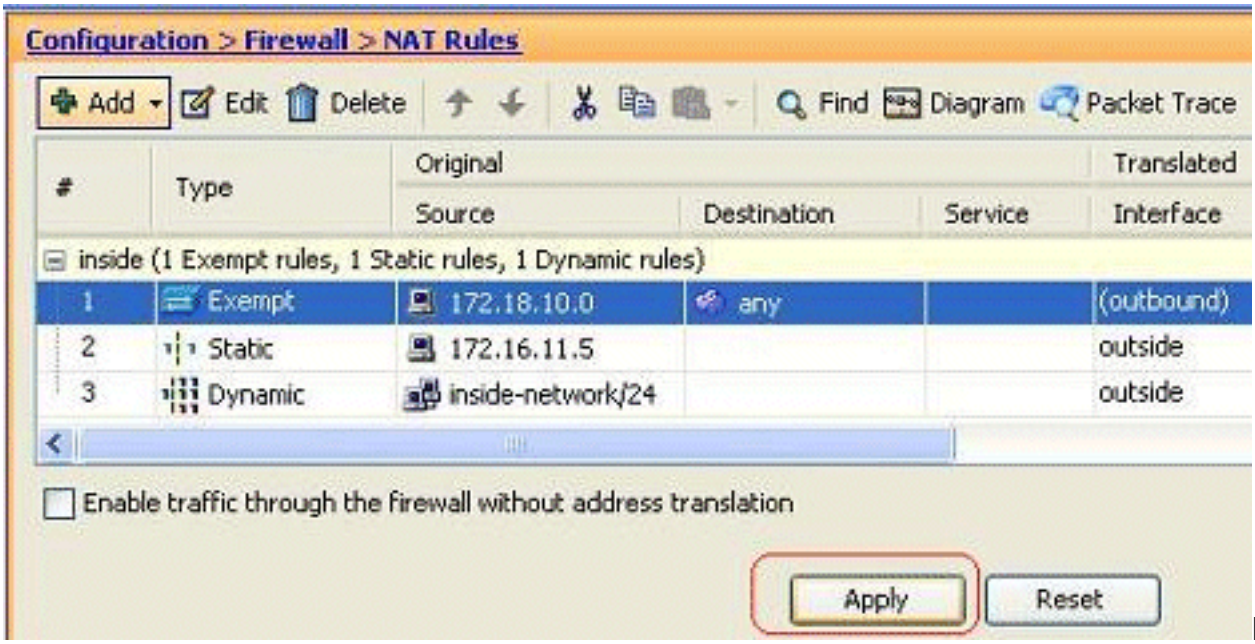
1. Vaya a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y elige **agrega la regla exenta NAT**. 

2. Aquí, la red interna 172.18.10.0 se ha eximido de la traducción de la dirección. Aseegurese que se ha seleccionado la opción **exenta**. La dirección exenta NAT tiene dos opciones:Tráfico saliente a las interfaces de menor seguridadTráfico entrante a las interfaces de mayor seguridadLa opción predeterminada está para el tráfico saliente. Haga Click en OK para completar el



paso. **Nota:** Cuando usted elige **no exima la** opción, ese host determinado no será eximido del NAT y una regla de acceso separada será agregada con “niega” la palabra clave. Esto es útil en evitar los host específicos del NAT tan exenta que la subred completa, excepto estos host, estará NAT eximido.

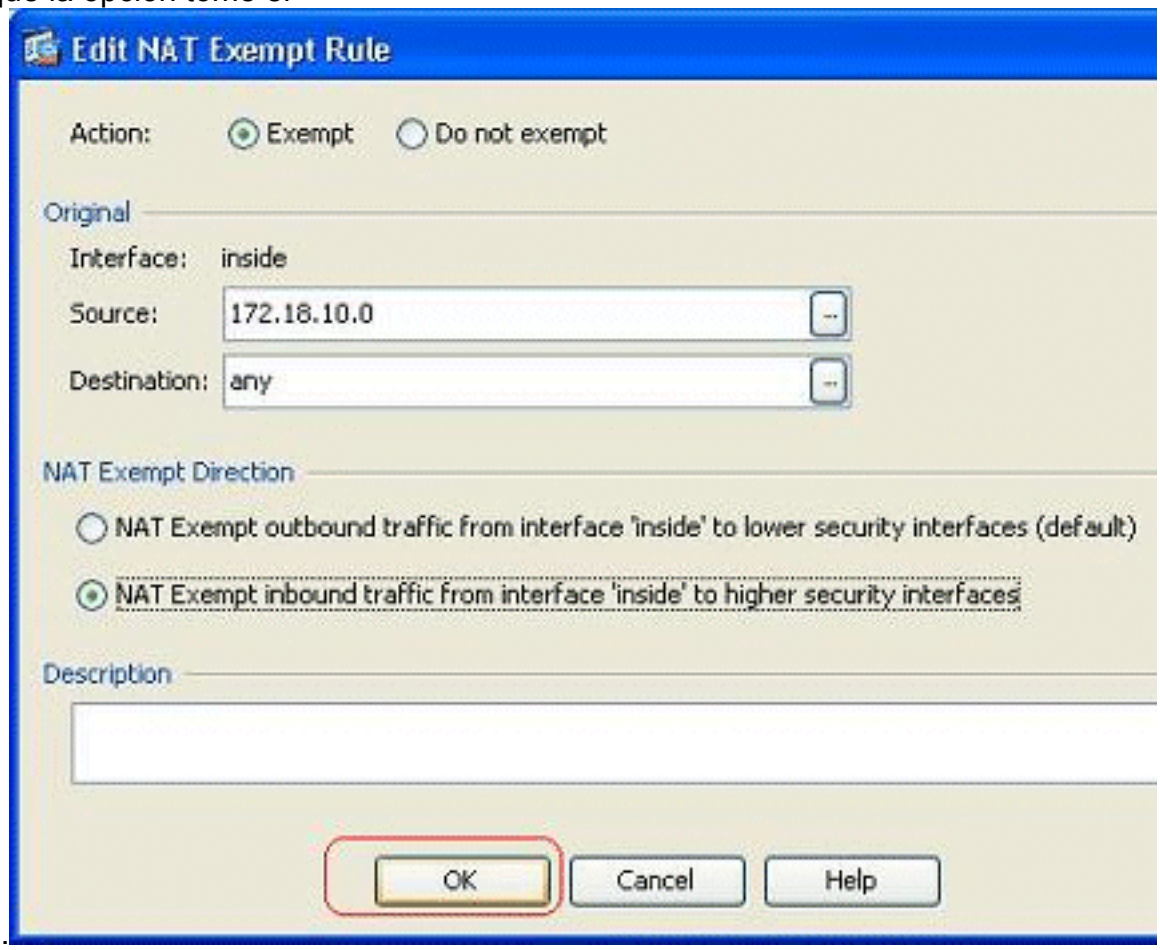
3. Usted puede ver la regla exenta NAT para la dirección saliente aquí. El tecleo **se aplica** para enviar la configuración al
ASA.



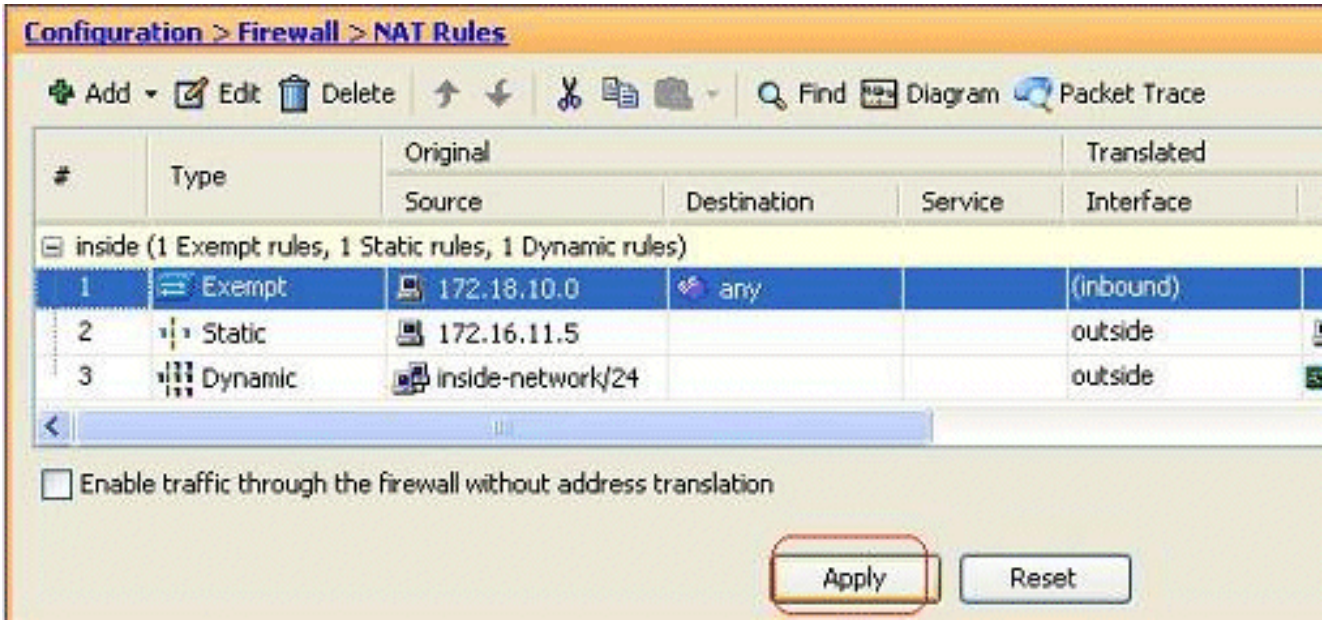
Éste es el CLI equivalente hecho salir para su referencia:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. Aquí usted puede ver cómo editar la regla exenta NAT para su dirección. Haga Click en OK para que la opción tome el efecto.



5. Usted puede ahora ver que la dirección se ha cambiado a *entrante*.



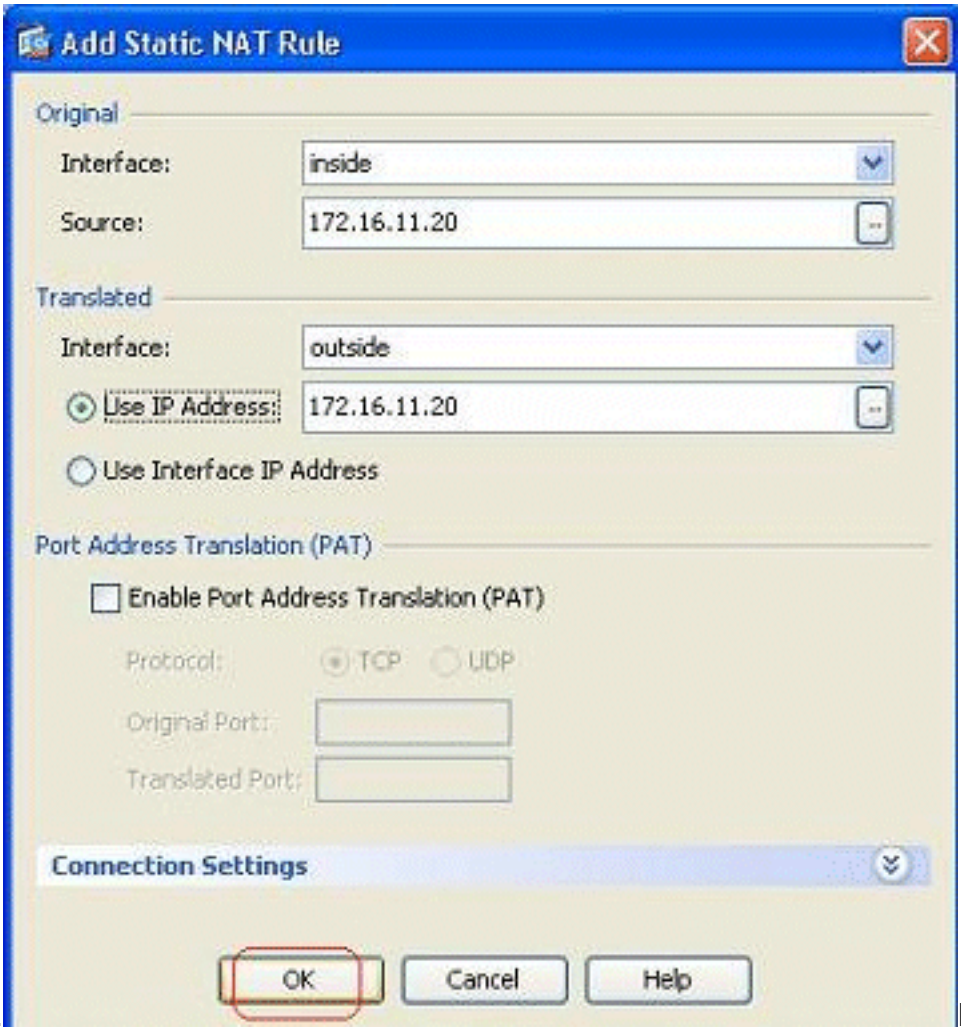
El tecleo **se aplica** para enviar este CLI hecho salir al ASA:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

Nota: De esto, usted puede ver que una nueva palabra clave (afuera) se ha agregado para terminar del **comando nat 0**. Esta característica se llama un **NAT exterior**.

6. Otra manera de inhabilitar el NAT está con la implementación de la identidad NAT. La

identidad NAT traduce un host a la misma dirección IP. Aquí está un ejemplo de NAT estático regular de la identidad, donde el host (172.16.11.20) se traduce a la misma dirección IP cuando se accede del



exterior. Esto es el CLI equivalente hecho salir:

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

Redirección (Reenvío) de Puerto con Estático

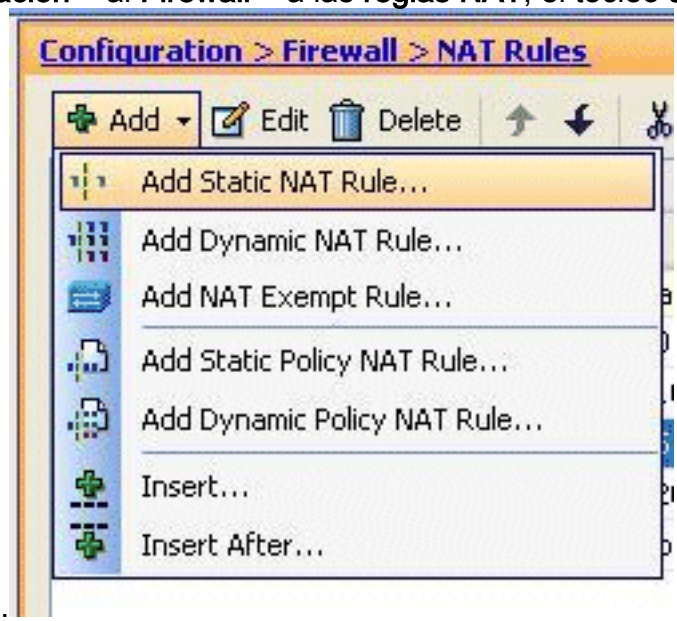
La expedición o la redirección de puerto del puerto es una función útil donde los usuarios externos intentan acceder a un servidor interno en un puerto específico. Para alcanzar esto, traducirán al servidor interno, que tiene un IP Address privado, a un IP Address público que a su vez no se prohiba el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

En este ejemplo, el usuario externo quiere acceder al servidor SMTP, 209.165.200.15 en el puerto 25. Esto se logra en dos pasos:

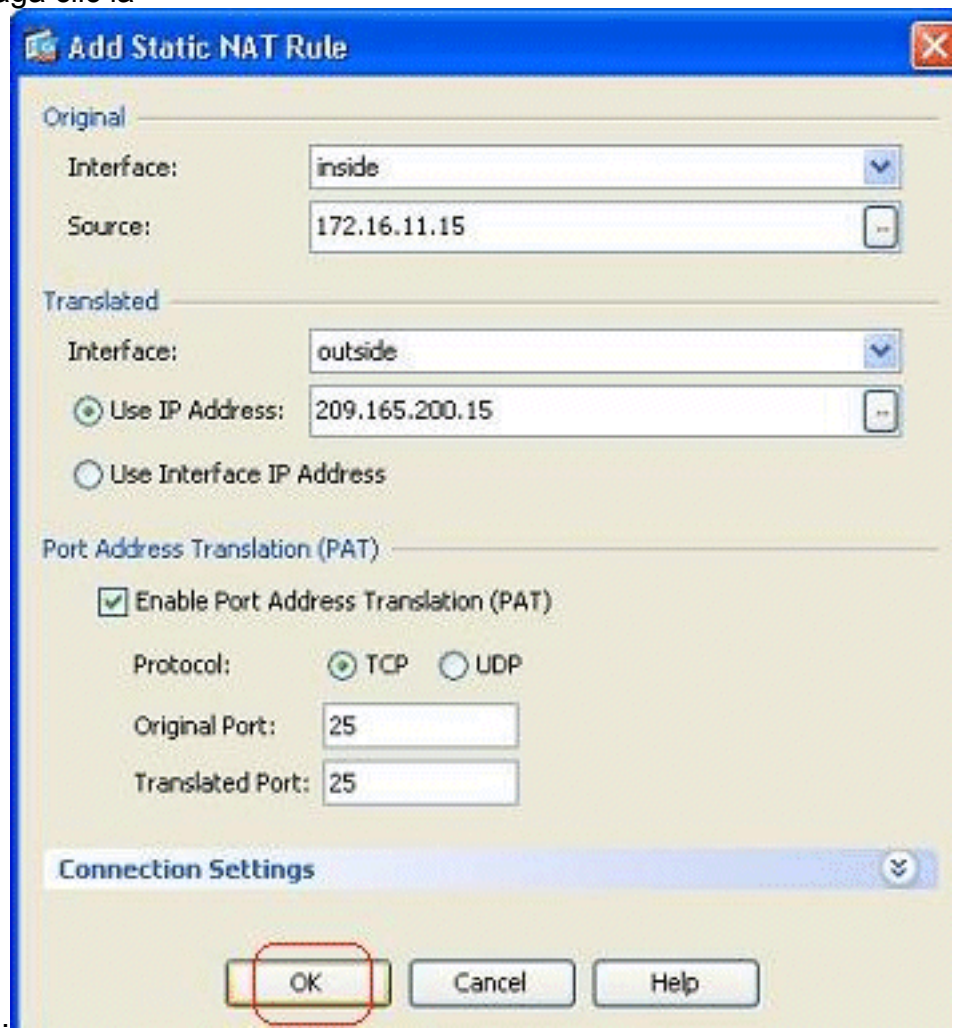
1. Traduzca al servidor de correo interno, 172.16.11.15 en el puerto 25, al IP Address público, 209.165.200.15 en el puerto 25.
2. Permita el acceso al mail server público, 209.165.200.15 en el puerto 25.

Cuando el usuario externo intenta acceder el servidor, 209.165.200.15 en el puerto 25, este tráfico será reorientado al servidor de correo interno, 172.16.11 15 en el puerto 25.

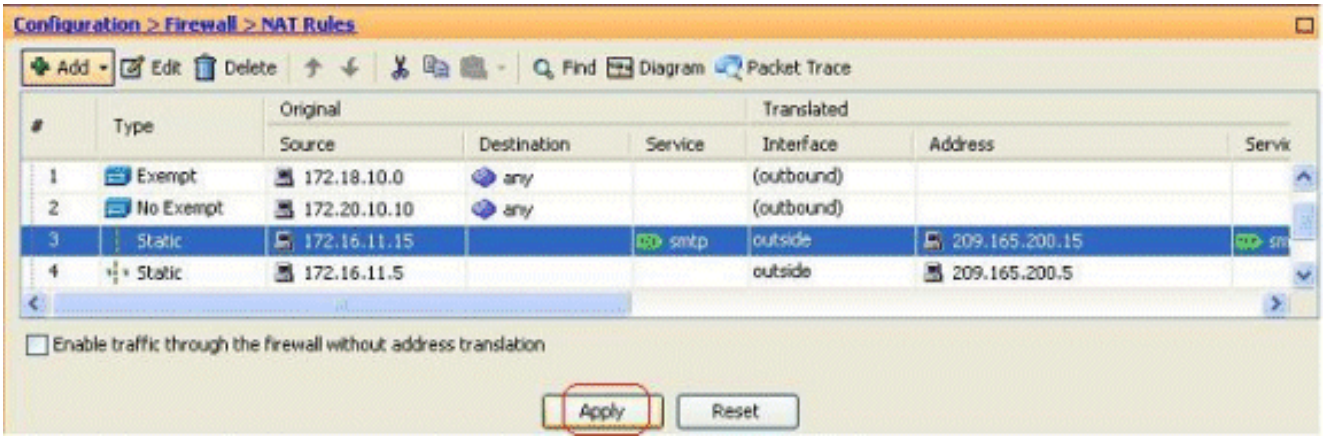
1. Vaya a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y elige **agrega la regla NAT estática**.



2. Especifique la fuente original y la dirección IP traducida junto con sus interfaces asociadas. Elija el **Port Address Translation (PAT) del permiso**, especifique los puertos que se reorientarán, y haga clic la **AUTORIZACIÓN**.



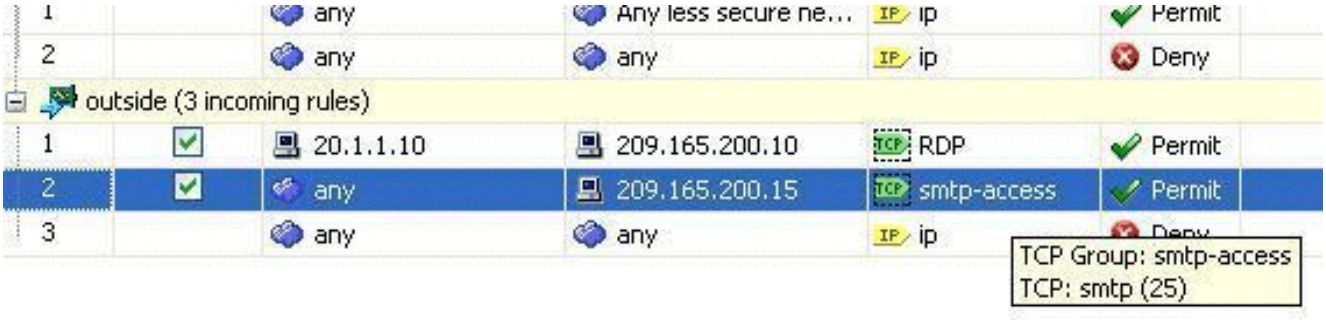
3. La regla configurada del PAT estático se considera aquí:



Esto es el CLI equivalente hecho salir:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255
!
```

4. Ésta es la regla de acceso que permite que el usuario externo acceda el servidor smtp del público en
209.165.200.15:



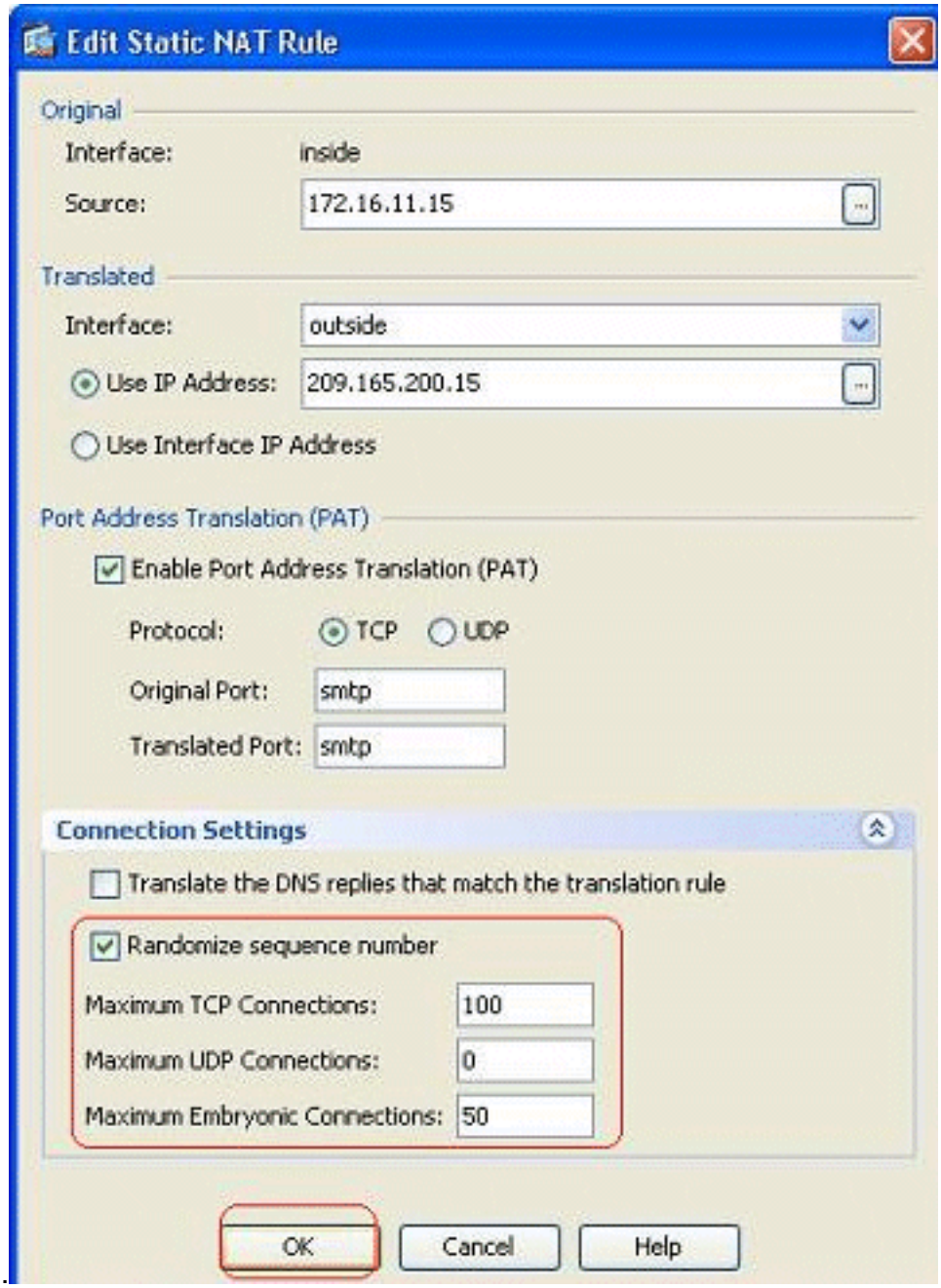
Nota: Aseegurese utilizar los host específicos en vez de usar la **cualquier** palabra clave en la fuente de la regla de acceso.

Limite la Sesión TCP/UDP con Estático

Usted puede especificar el número máximo de conexiones TCP/UDP usando la regla estática. Usted puede también especificar el número máximo de conexiones embrionarias. Una conexión embrionaria es una conexión que es un estado medio abierto. Un número más grande de éstos afectará al funcionamiento del ASA. La limitación de estas conexiones prevendrá ciertos ataques como el DOS y el SYN hasta cierto punto. Para la mitigación completa, usted necesita definir la directiva en el marco del MPF, que está fuera del alcance de este documento. Para más información sobre este tema, refiera a atenuar los ataques a la red.

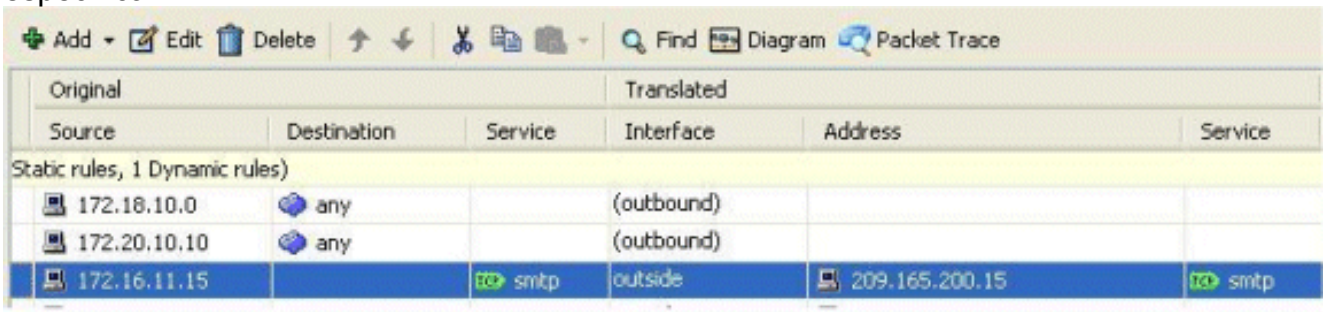
Complete estos pasos:

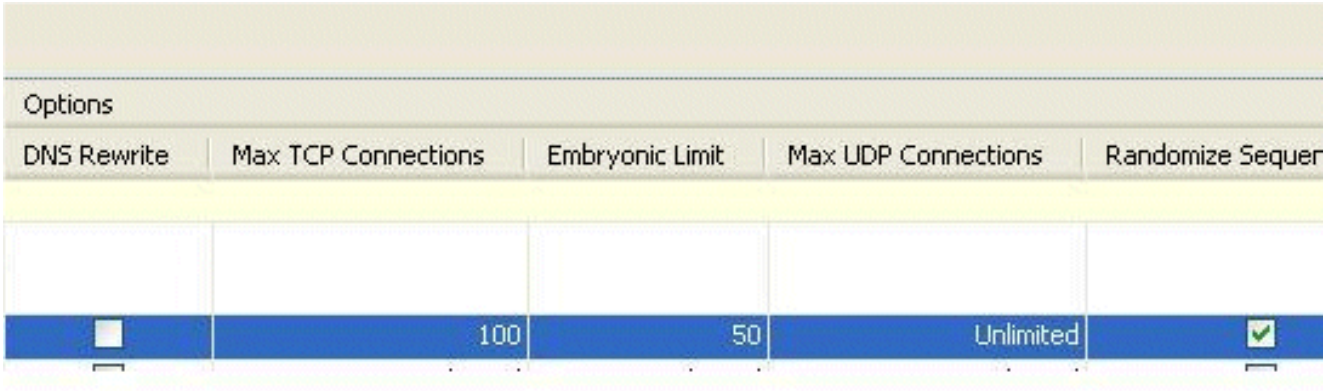
1. Haga clic la lengueta de las **configuraciones de la conexión**, y especifique los valores para las cantidades máximas de conexiones para esta traducción



estática.

2. Estas imágenes muestran los límites de la conexión para esta traducción estática específica:





Esto es el CLI equivalente hecho salir:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255 TCP 100 50
!
```

Lista de Acceso Basada en el Tiempo

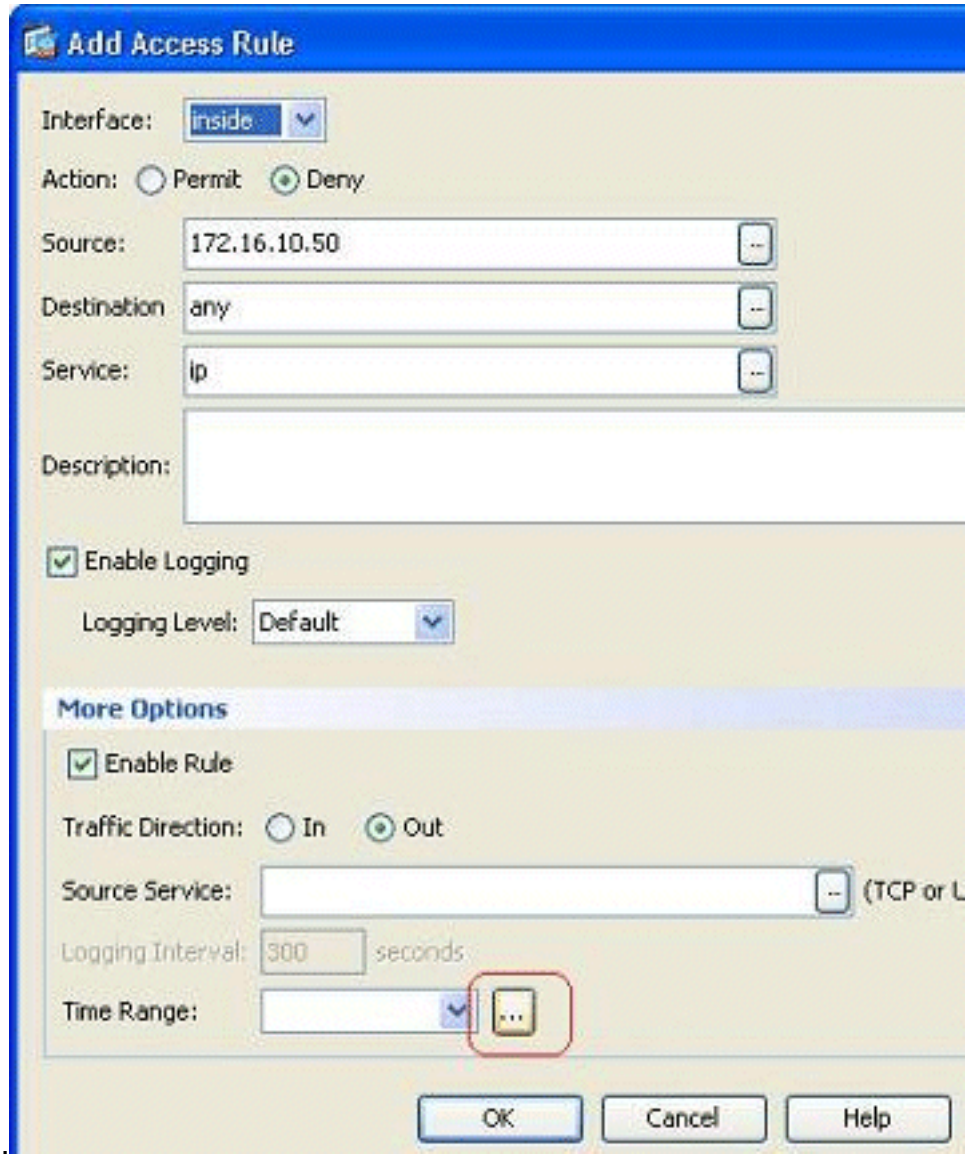
Esta sección se ocupa de implementar las listas de acceso basadas en el tiempo usando el ASDM. Las reglas de acceso pueden ser aplicadas basadas el tiempo. Para implementar esto, usted necesita definir un tiempo-rango que especifique las sincronizaciones por el día/la semana/el mes/año. Entonces, usted necesita atar este tiempo-rango a la regla de acceso requerida. el Tiempo-rango se puede definir de dos maneras:

1. Absoluto - Define un período de tiempo con Starting Time (Tiempo de inicio) y el tiempo de la conclusión.
2. Periódico - También conocido como repetirse. Define un período de tiempo que ocurra en los intervalos especificados.

Nota: Antes de que usted configure el tiempo-rango, aseegurese que el ASA se ha configurado con las configuraciones de la fecha y horas correctas mientras que esta característica utiliza las configuraciones del reloj del sistema para implementar. Tener ASA sincronizado con el servidor NTP rendirá resultados mucho mejores.

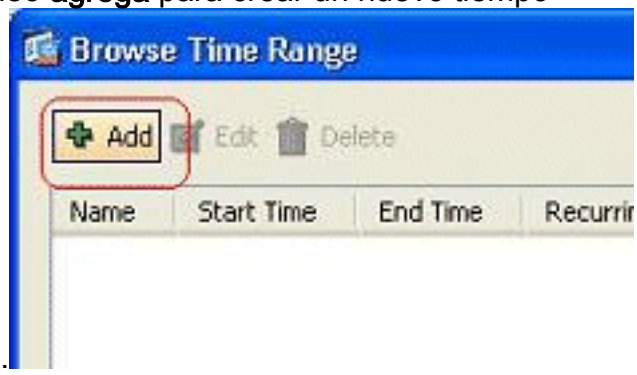
Complete estos pasos para configurar esta característica con el ASDM:

1. Mientras que define la regla de acceso, haga clic el **botón Details Button** en el campo del



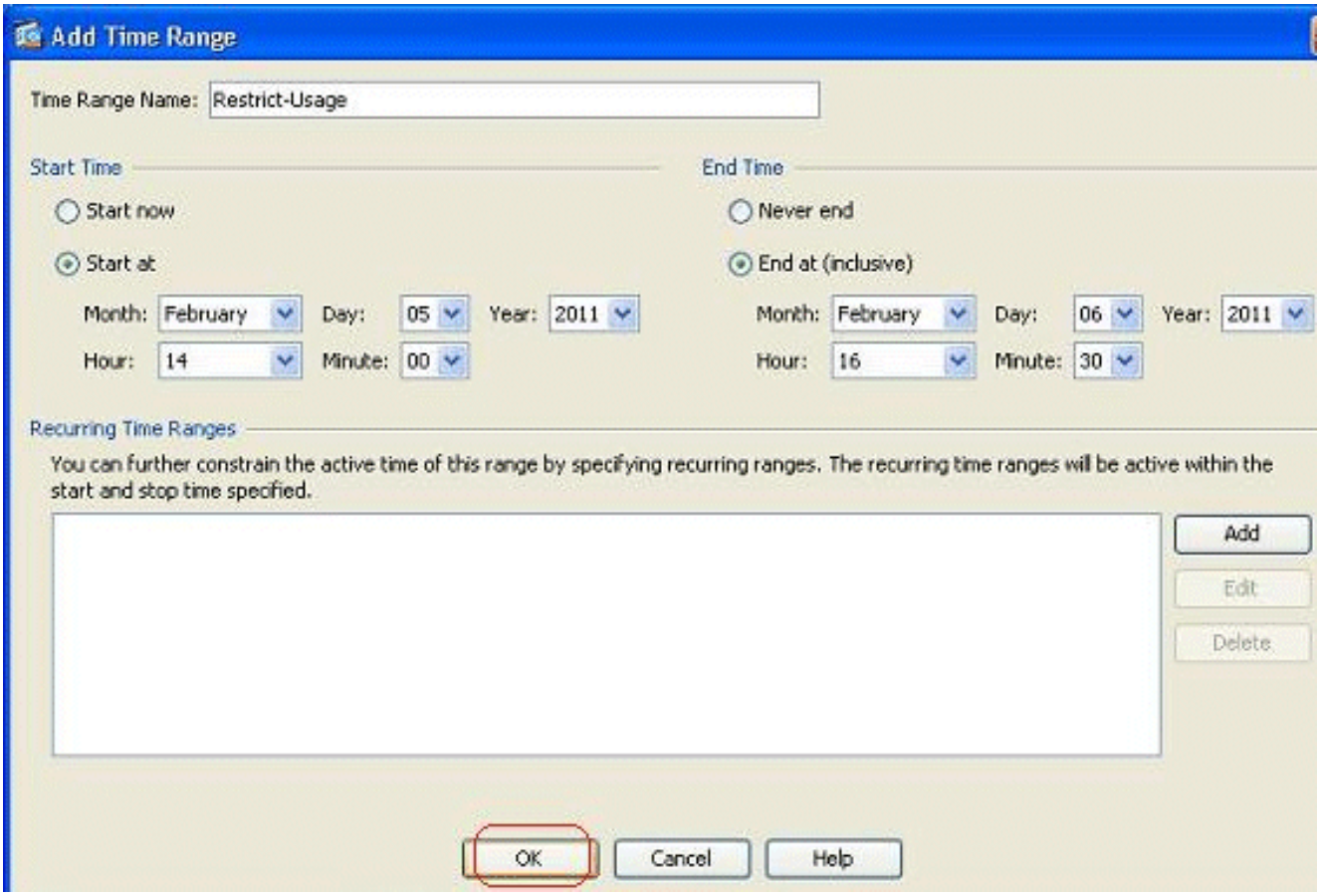
rango de tiempo.

2. El tecleo **agrega** para crear un nuevo tiempo-

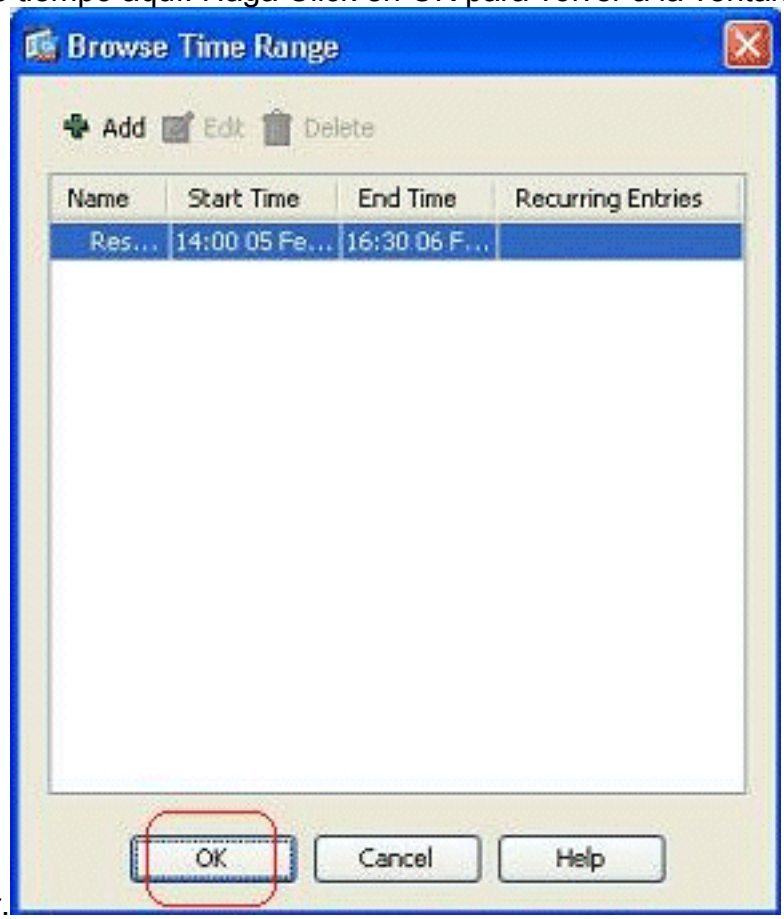


rango.

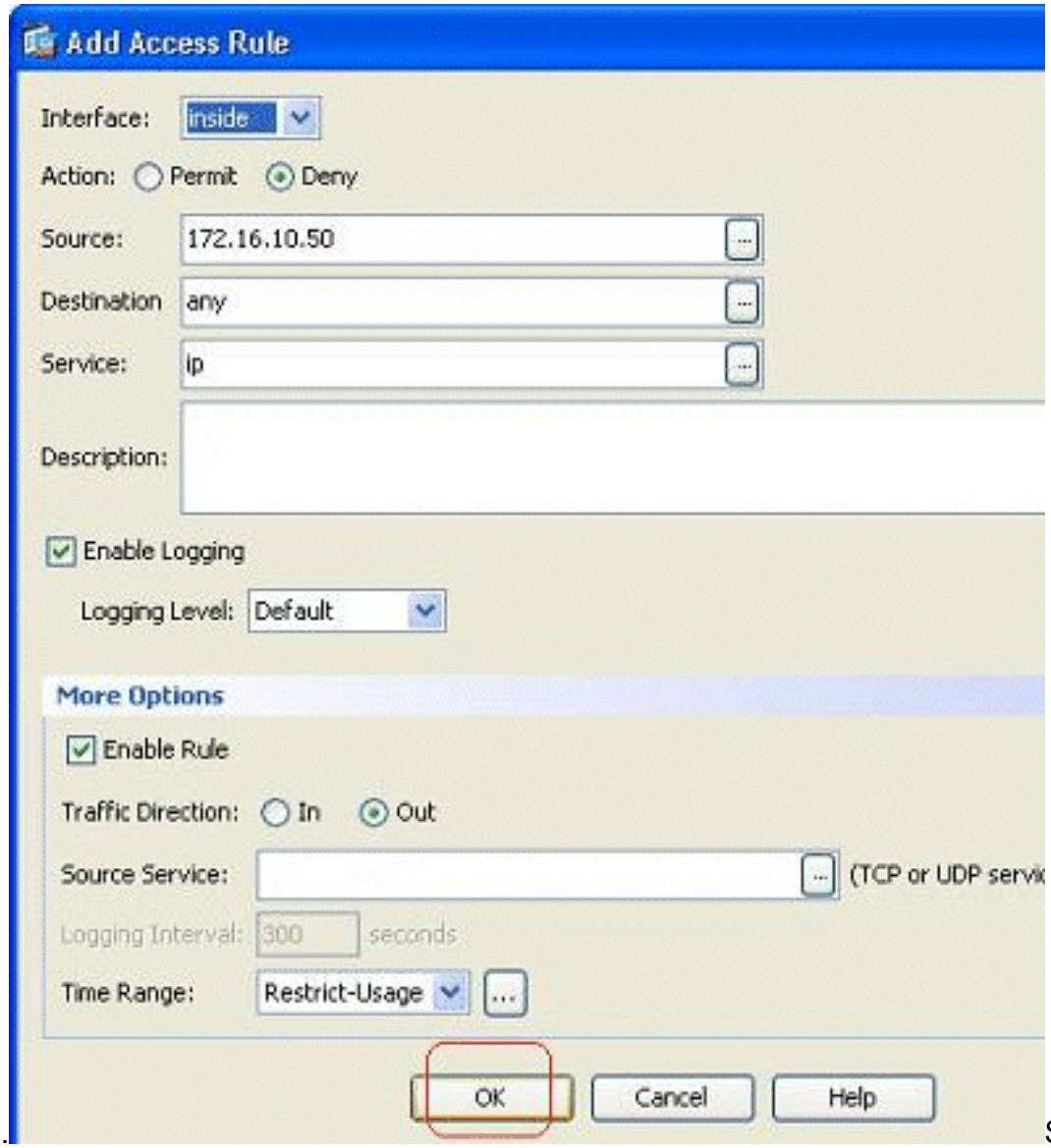
3. Defina el nombre del rango de tiempo, y especifique Starting Time (Tiempo de inicio) y el tiempo de la conclusión. Haga clic en
OK.



4. Usted puede ver el rango de tiempo aquí. Haga Click en OK para volver a la ventana de la regla de acceso del agregar.



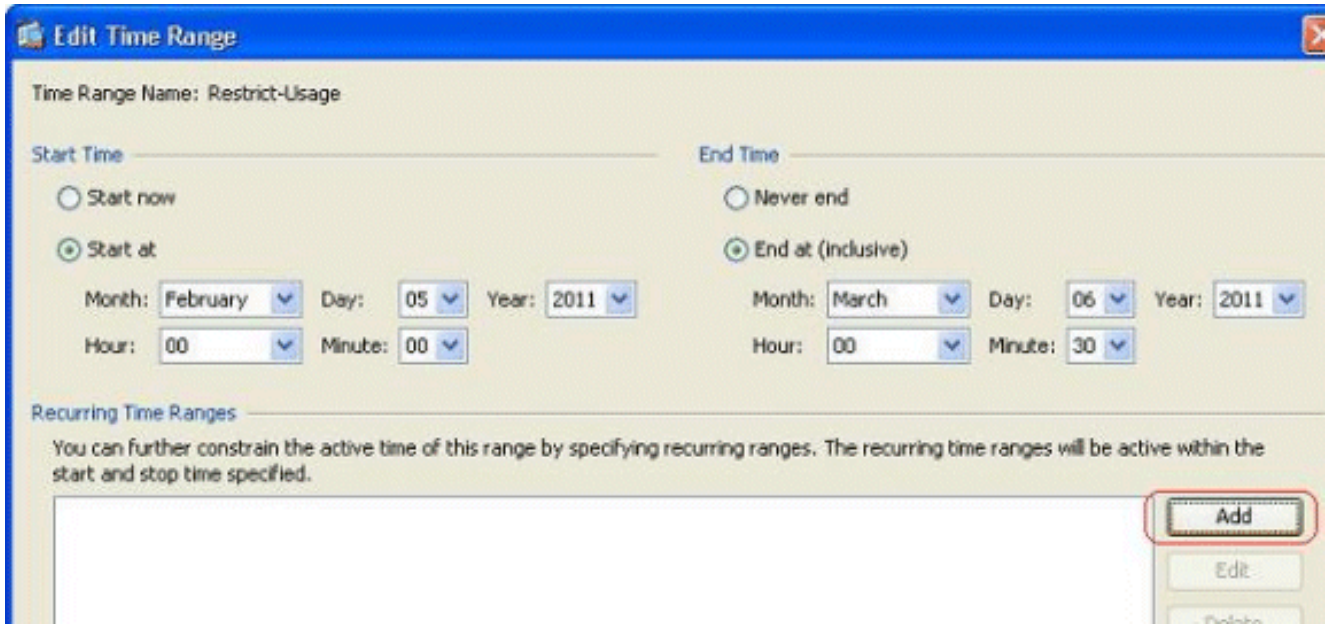
5. Usted puede ahora ver que el rango de tiempo del Restringir-uso ha estado limitado a esta regla de



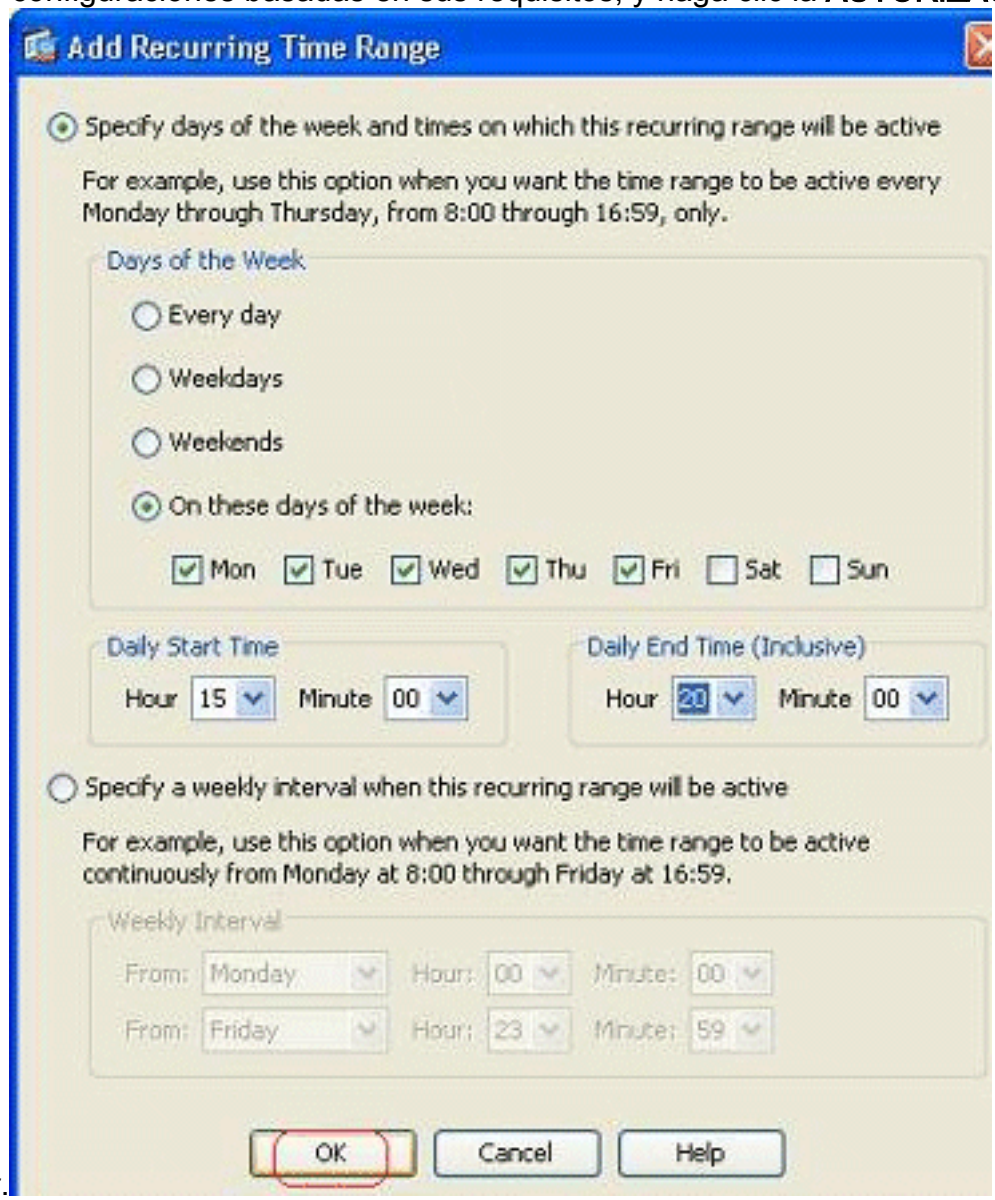
acceso. Según esta configuración de la regla de acceso, han restringido al usuario en 172.16.10.50 de usar cualquier recurso de 05/Feb/2011 2 de la tarde a 06/Feb/2011 4.30 PM. Esto es el CLI equivalente hecho salir:

```
time-range Restrict-Usage
 absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

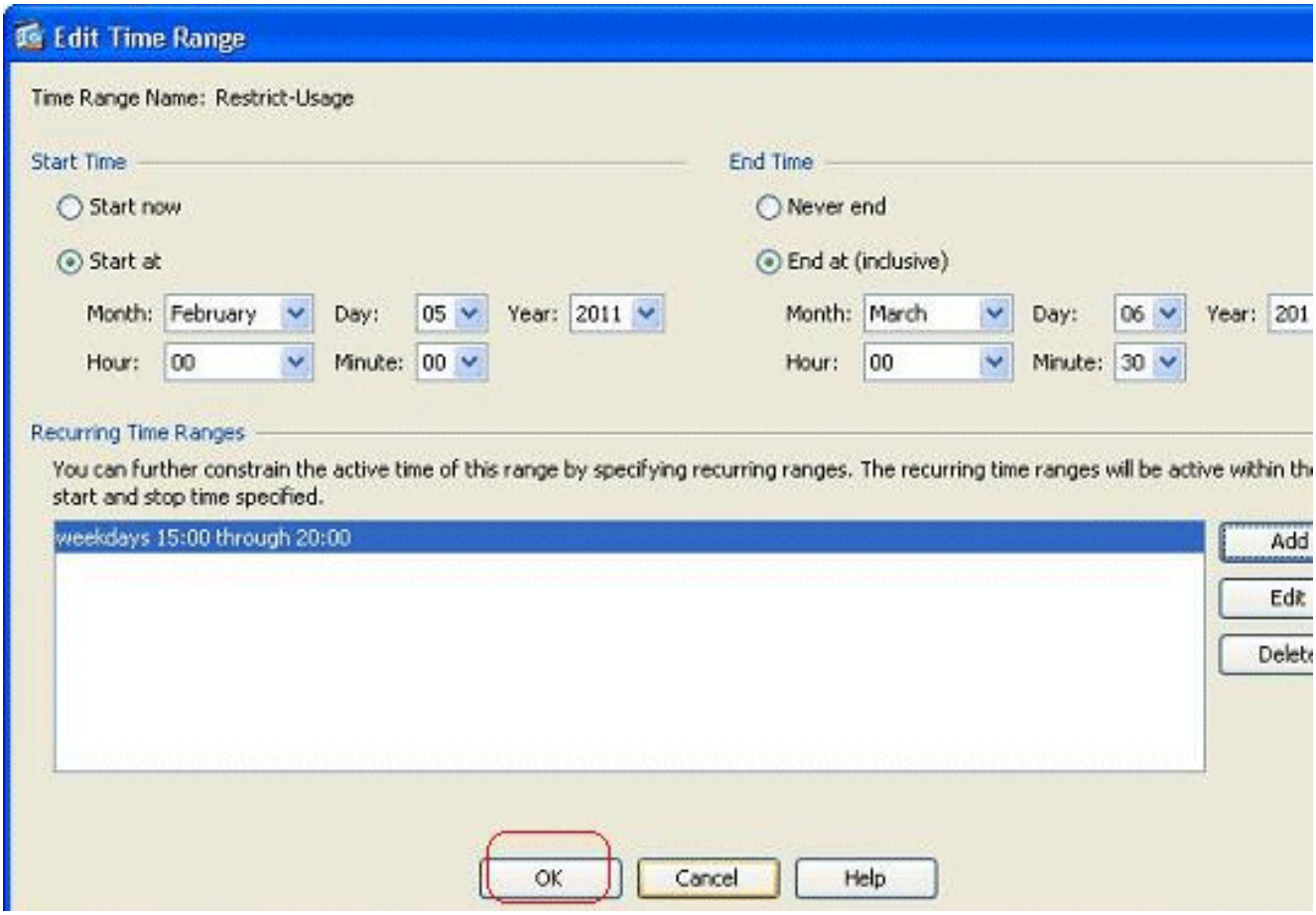
6. Aquí está un ejemplo en cómo especificar un rango de tiempo que se repite. El tecleo **agrega** para definir un rango de tiempo que se repite.



7. Especifique las configuraciones basadas en sus requisitos, y haga clic la **AUTORIZACIÓN** para completar.



8. Haga Click en OK para volver de nuevo a la ventana del rango de tiempo.



Según esta configuración, han negado el usuario en 172.16.10.50 el acceso a cualquier recurso a partir del 3 PM a 8 PM en todos los días laborables excepto sábado y domingo.

```
!
time-range Restrict-Usage
 absolute start 00:00 05 February 2011 end 00:30 06 March 2011
 periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

Nota: Si un **comando time-range** hace los valores absolutos y periódicos especificar, después evalúan solamente después que se alcanza la hora de inicio absoluta, y no son más futuros a los **comandos periodic** evaluados después del tiempo absoluto del final se alcanzan.

Información Relacionada

- Página de documentación de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems