ASA 8.X y posterior: Agregue o modifique una lista de acceso con el ejemplo de la Configuración del GUI del ASDM

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Configurar
Diagrama de la red
Agregue una nueva lista de acceso
Cree una lista de acceso estándar
Cree una regla de acceso global
Edite una lista de acceso existente
Borre una lista de acceso
Exporte la regla de acceso
Exporte la información de la lista de acceso
Verificación
Troubleshooting
Información Relacionada

Introducción

Este documento explica cómo utilizar al Cisco Adaptive Security Device Manager (ASDM) para trabajar con las listas de control de acceso. Esto incluye la creación de una nueva lista de acceso, cómo editar una lista de acceso existente y otras funciones con las Listas de acceso.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

hardware.

- Dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.2.X
- Cisco Adaptive Security Device Manager (ASDM) con la versión 6.3.X

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.

Antecedentes

Las Listas de acceso se utilizan sobre todo para controlar el tráfico atraviesan el Firewall. Usted puede permitir o negar los tipos de tráfico específicos con las Listas de acceso. Cada lista de acceso contiene varias entradas de lista de acceso (ACE) ese control el flujo de tráfico de una fuente específica a un destino específico. Normalmente, esta lista de acceso está limitada a una interfaz para notificar la dirección del flujo en el cual debe mirar. Las Listas de acceso se categorizan principalmente en dos tipos amplios.

1. Listas de acceso de entrada
2. Listas de acceso de salida

Las listas de acceso de entrada se aplican al tráfico que ingresa esa interfaz, y las listas de acceso de salida se aplican al tráfico que sale la interfaz. La notación entrante/saliente refiere a la dirección del tráfico en términos de esa interfaz pero no al movimiento del tráfico en medio más arriba y de las interfaces de menor seguridad.

Para el TCP y las conexiones UDP, usted no necesita una lista de acceso permitir el volver del tráfico porque el dispositivo de seguridad permite todo el tráfico de vuelta para las conexiones bidireccionales establecidas. Para los protocolos sin conexión tales como ICMP, el dispositivo de seguridad establece las sesiones unidireccionales, así que usted necesita las Listas de acceso aplicar las Listas de acceso a la fuente y a las interfaces de destino para permitir el ICMP en las ambas direcciones, o usted necesidad de habilitar el motor de la inspección icmp. El motor de inspección del ICMP trata las sesiones del ICMP como conexiones bidireccionales.

De la versión 6.3.X del ASDM, hay dos tipos de Listas de acceso que usted pueda configurar.

1. Reglas de acceso de la interfaz
2. Reglas de acceso globales

Nota: La regla de acceso refiere a una entrada de la lista del acceso individual (ACE).

Las reglas de acceso de la interfaz están limitadas a cualquier interfaz a la hora de su creación. Sin atarlas a una interfaz, usted no puede crearlas. Esto diferencia del ejemplo de la línea de comando. Con el CLI, usted primero crea la lista de acceso con el **comando access list**, y en seguida ata esta lista de acceso a una interfaz con el **comando access-group**. El ASDM 6.3 y posterior, la lista de acceso se crea y está limitado a una interfaz como sola tarea. Esto se aplica al tráfico que atraviesa esa interfaz específica solamente.

Las reglas de acceso globales no están limitadas a ninguna interfaz. Pueden ser configuradas a través de la lengueta del ACL Manager en el ASDM y se aplican al Tráfico de ingreso global. Se implementan cuando hay un emparejamiento basado en la fuente, el destino, y el Tipo de protocolo. Estas reglas no se replican en cada interfaz, así que salvan el espacio de memoria.

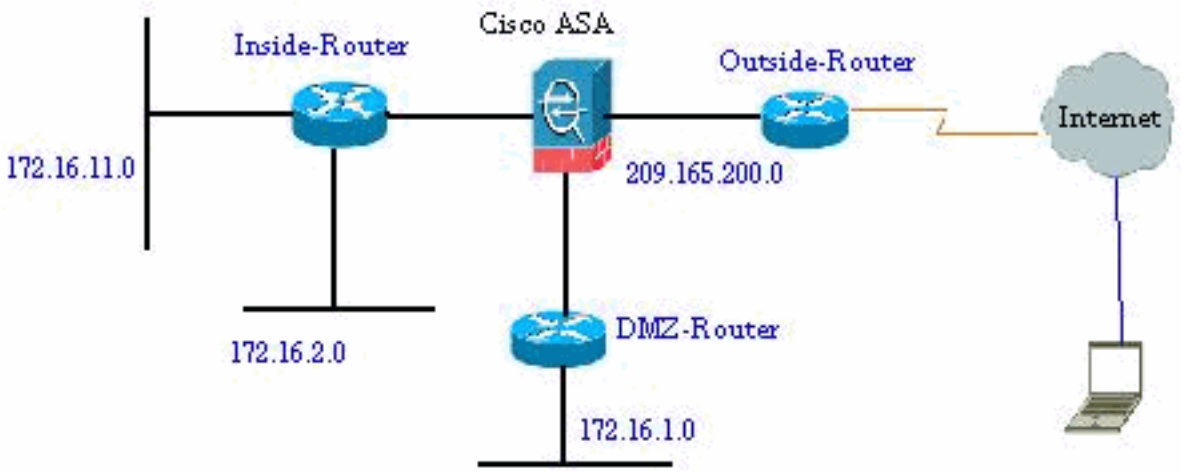
Cuando ambas estas reglas deben ser implementadas, las reglas del acceso de la interfaz toman normalmente la precedencia sobre las reglas globales del acceso.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

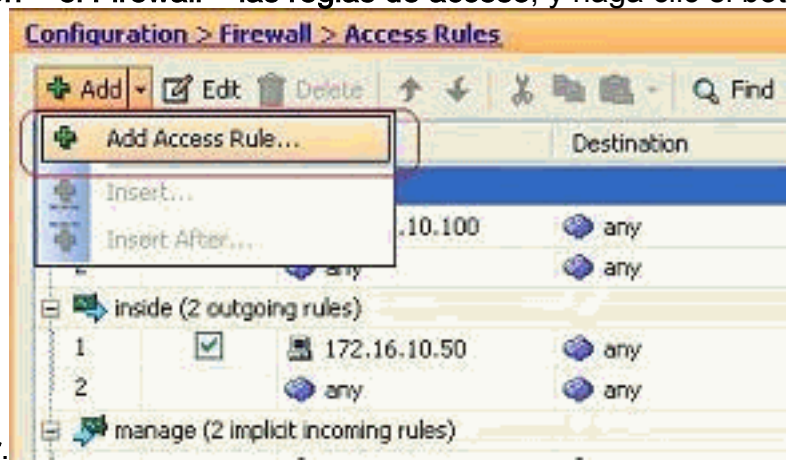
En este documento, se utiliza esta configuración de red:



Agregue una nueva lista de acceso

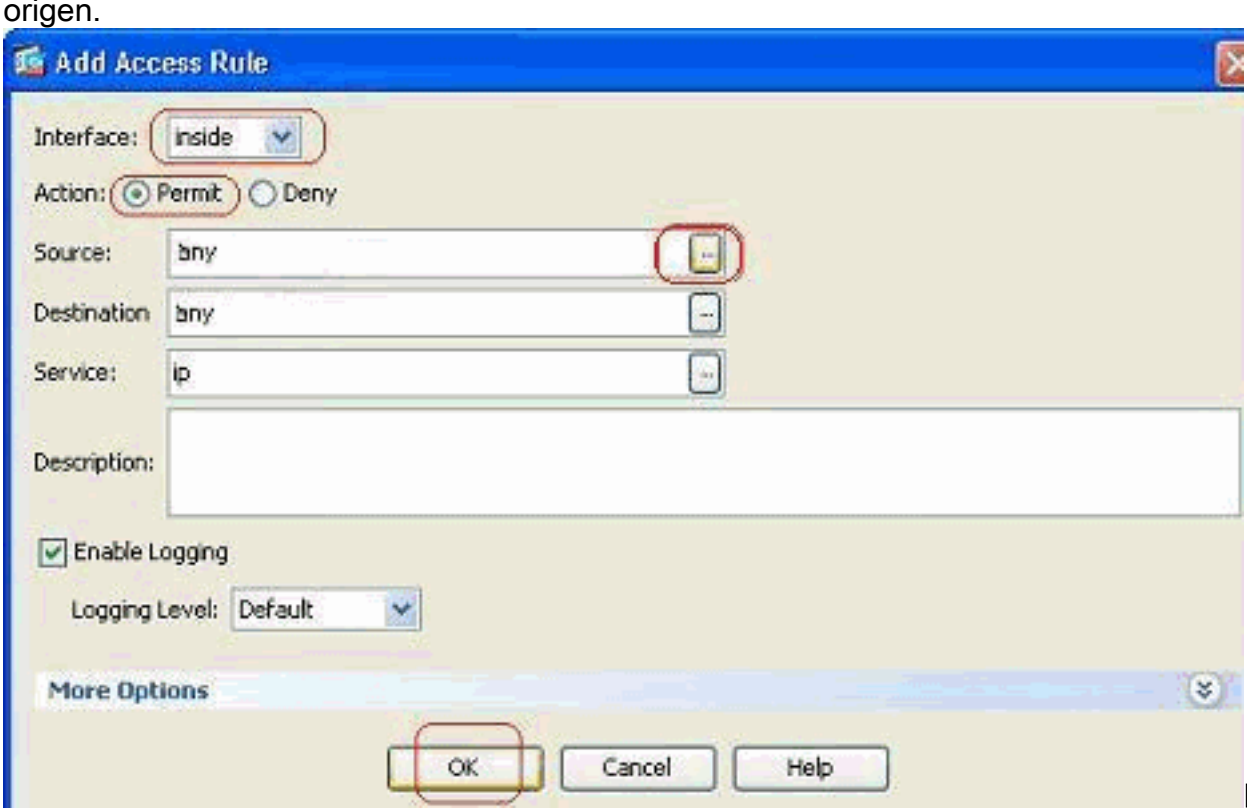
Complete estos pasos para crear una nueva lista de acceso con el ASDM:

1. Elija la **configuración > el Firewall > las reglas de acceso**, y haga clic el botón de la **regla de acceso del agregar**.



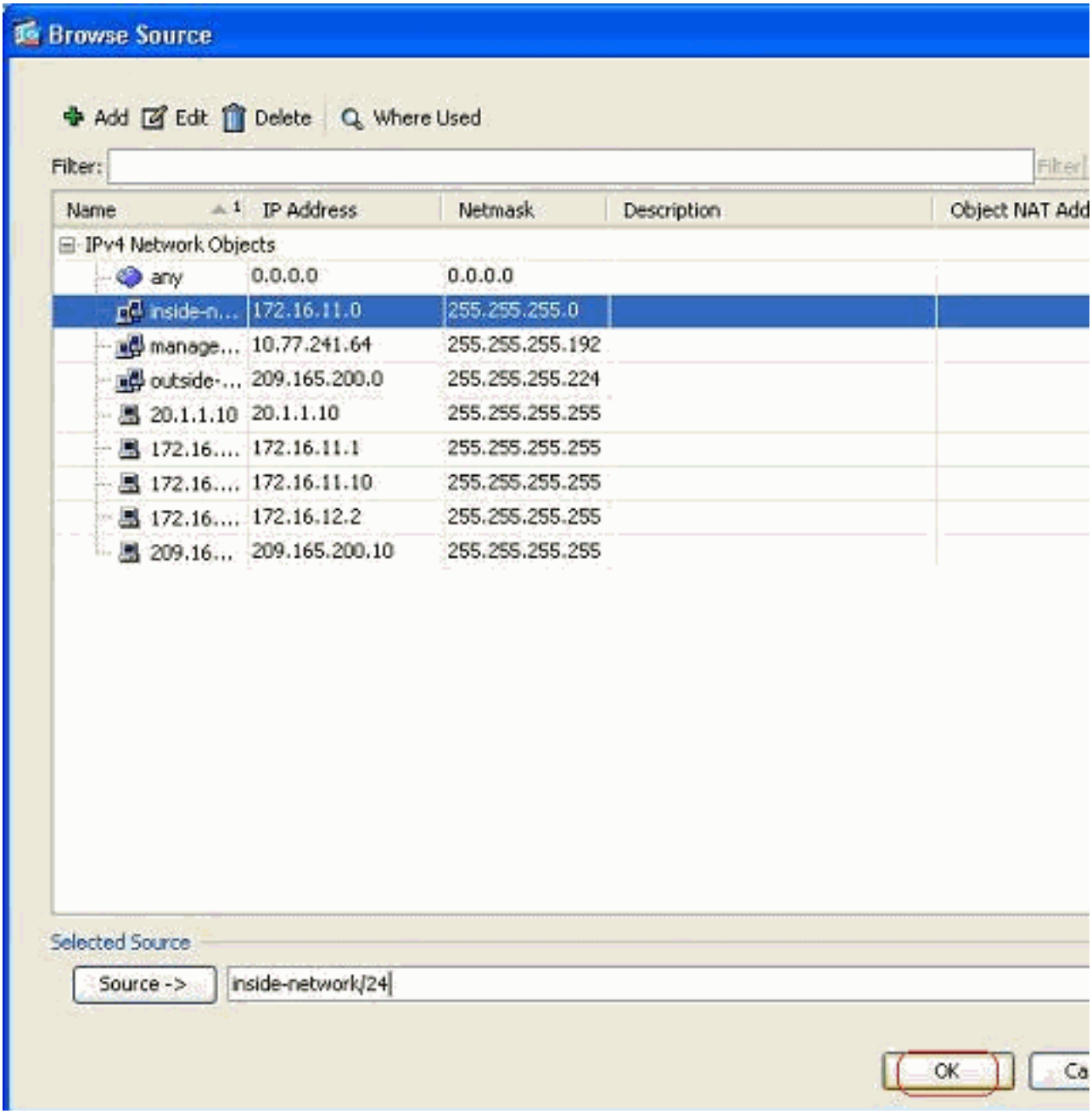
2. Elija la interfaz a la cual esta lista de acceso tiene que limitar, junto con la acción que se realizará en del tráfico el permiso es decir,/niegue. Entonces haga clic el Detailsbutton para

seleccionar la red de origen.

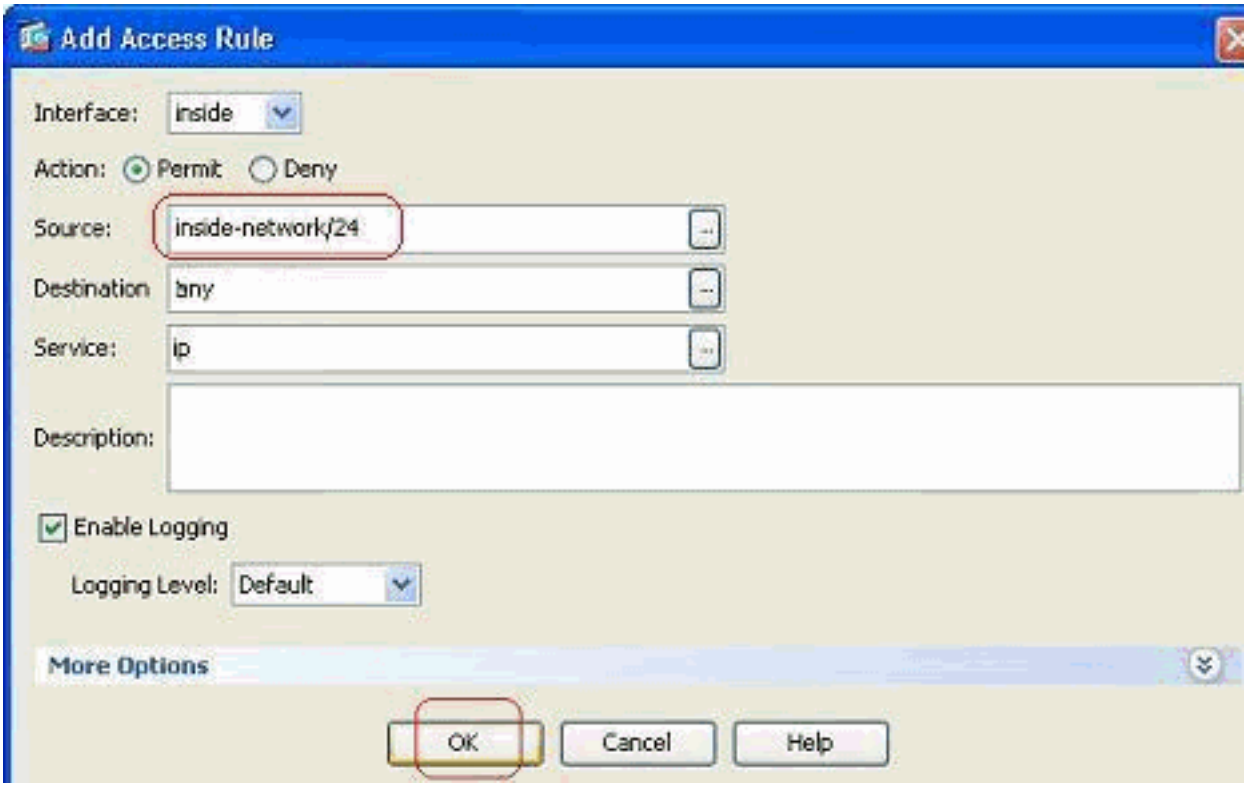


Nota: Aquí está una explicación abreviada de los diversos campos que se muestran en esta ventana:**Interfaz** — Determina la interfaz a la cual esta lista de acceso está limitada.**Acción** — Determina el tipo de la acción de la nueva regla. Dos opciones están disponibles. **Permita** permite todo el tráfico coincidente y **niega a** bloques todo el tráfico coincidente.**Fuente** — Este campo especifica la fuente del tráfico. Éste puede ser cualquier cosa entre una sola dirección IP, una red, una dirección IP de la interfaz del Firewall o un grupo de objeto de red. Éstos se pueden seleccionar con el **botón Details Button**.**Destino** — Este campo especifica la fuente del tráfico. Éste puede ser cualquier cosa entre una sola dirección IP, una red, una dirección IP de la interfaz del Firewall o un grupo de objeto de red. Éstos se pueden seleccionar con el **botón Details Button**.**Servicio** — Este campo determina el protocolo o el servicio del tráfico al cual esta lista de acceso es aplicada. Usted puede también definir a un grupo de servicios que contenga un conjunto de diversos protocolos.

3. Después de que usted haga clic el **botón Details Button**, se visualiza una nueva ventana que contiene los objetos de red existente. Seleccione la **red interna**, y haga clic la **AUTORIZACIÓN**.



4. Le vuelven a la ventana de la **regla de acceso del agregar**. Teclee **ningunos** en el Campo Destination. y **AUTORIZACIÓN del** tecleo para completar la configuración de la regla de acceso.

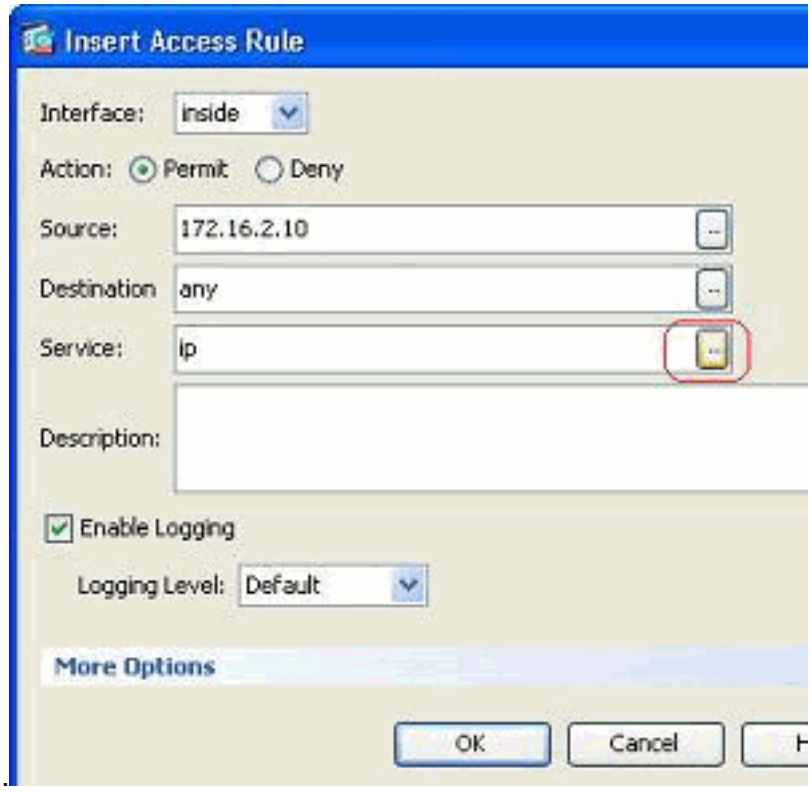


Agregue una regla de acceso antes existente:

Complete estos pasos para agregar una regla de acceso momentos antes de una regla de acceso ya existente:

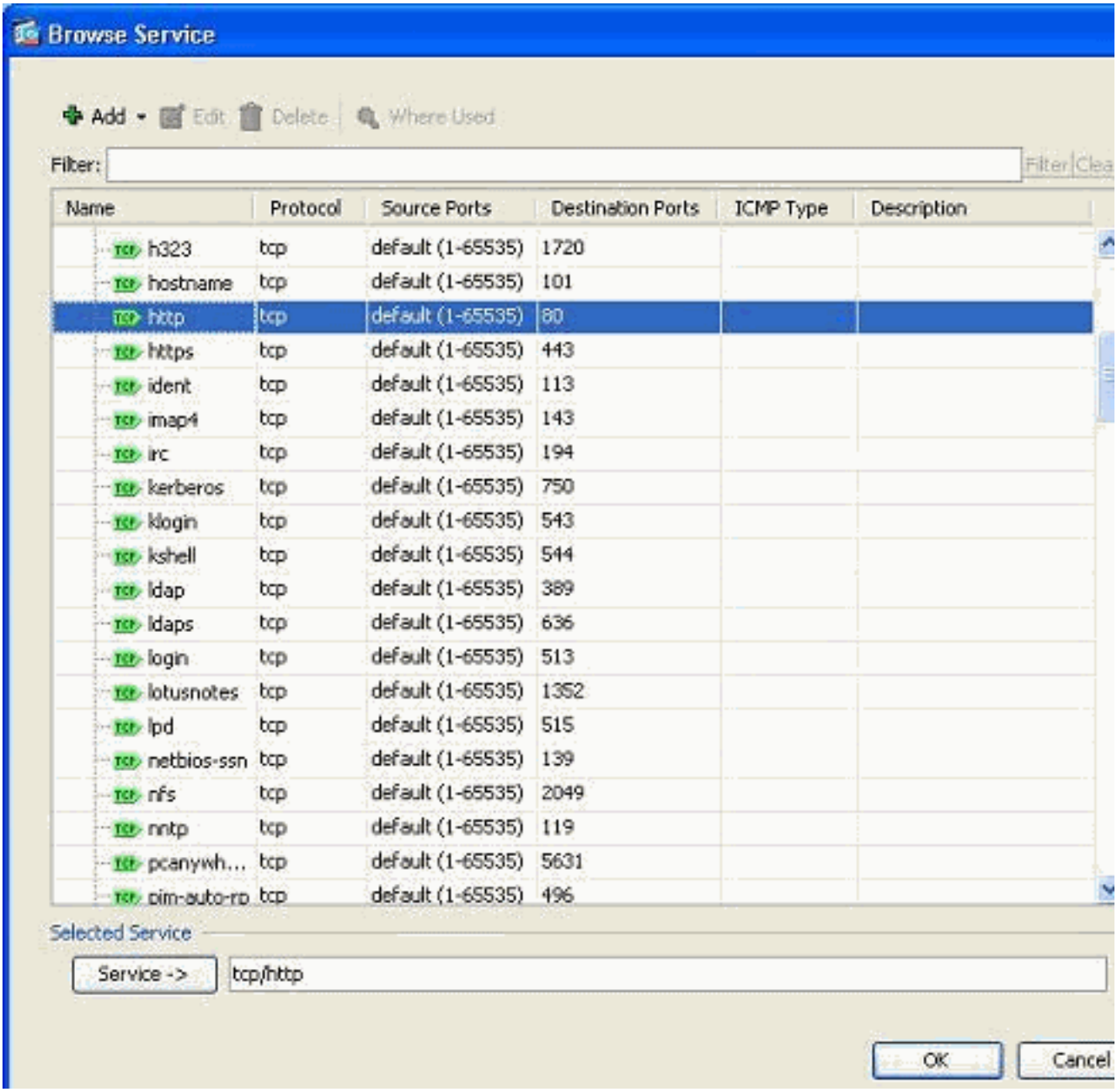
1. Seleccione la entrada de lista de acceso existente, y haga clic el **separador de millares del** menú desplegable del **agregar**

2. Elija la fuente y el destino, y haga clic el **botón Details Button del** campo del servicio para



elegir el protocolo.

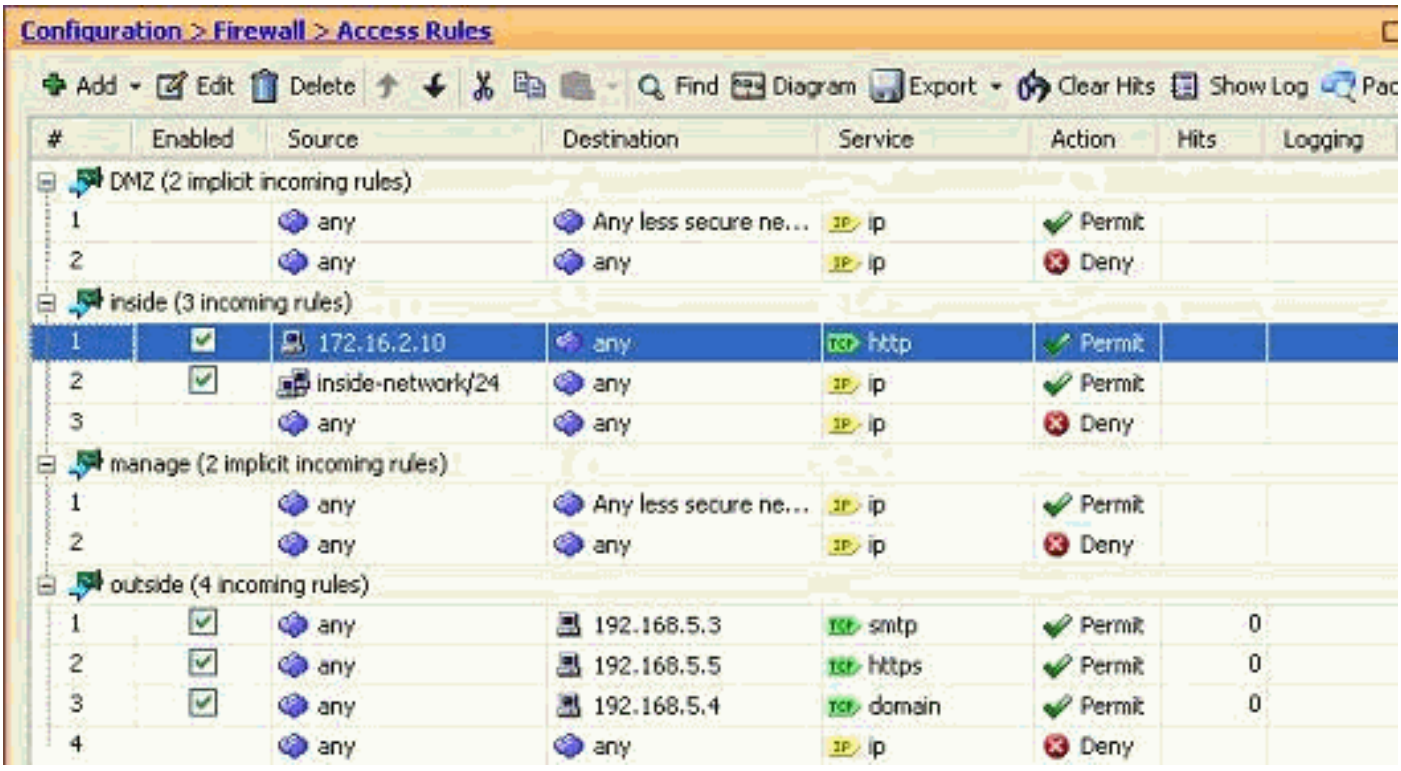
3. Elija el HTTP el protocolo, y haga clic la AUTORIZACIÓN.



4. Le vuelven a la ventana de la regla de acceso del separador de millares. El campo del servicio se llena del **tcp/del HTTP** como el protocolo seleccionado. Haga Click en OK para completar la configuración de la nueva entrada de lista de

acceso.

Usted puede ahora observar la nueva regla de acceso mostrada momentos antes ya de la entrada existente para la red interna.

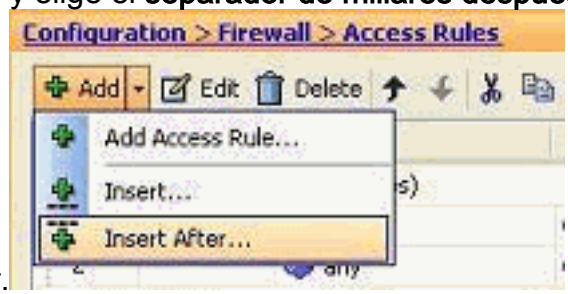


Nota: La orden de las reglas de acceso es muy importante. Mientras que procesa cada paquete para filtrar, el ASA examina si el paquete corresponde con el criterio de regla un de los del acceso en un orden consecutivo y si sucede un emparejamiento, implementa la acción de esa regla del acceso. Cuando se corresponde con una regla de acceso, no procede a otras reglas de acceso y las verifica otra vez.

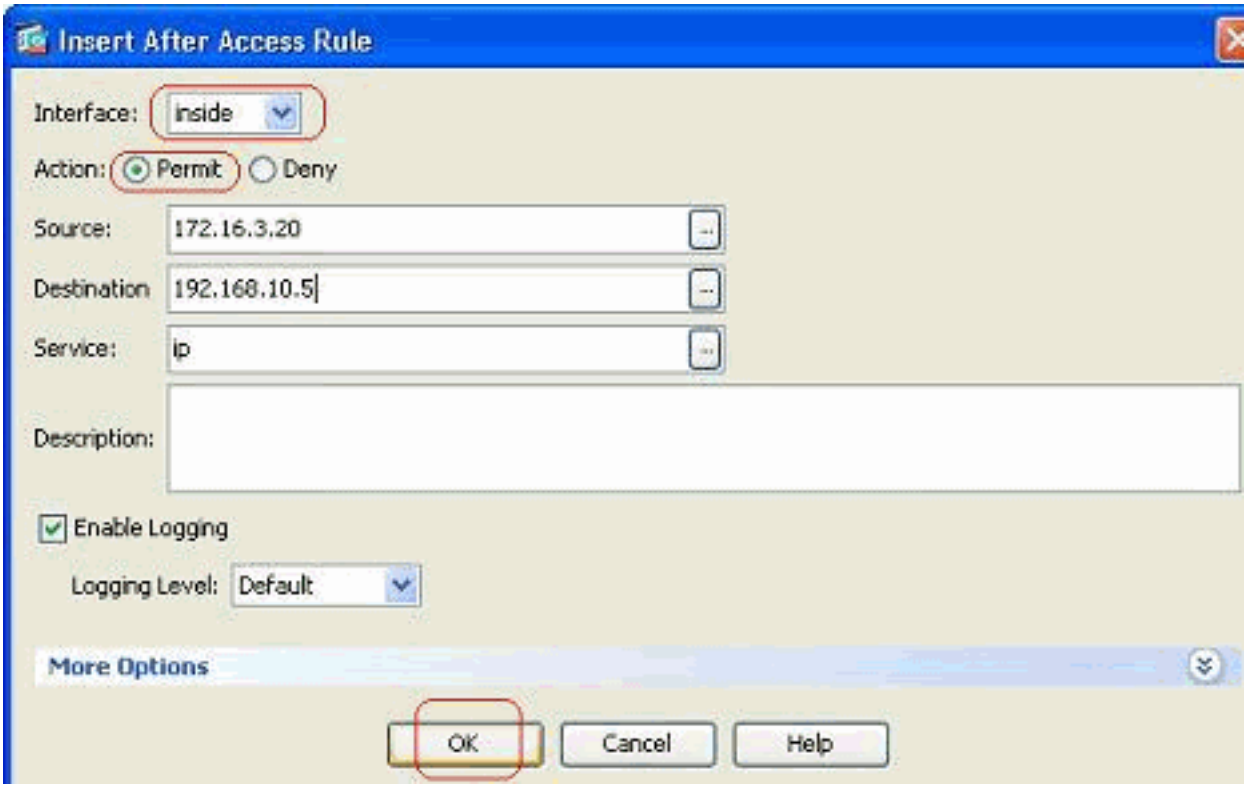
Agregue una regla de acceso después existente:

Complete estos pasos para crear una regla de acceso enseguida después de una regla de acceso ya existente.

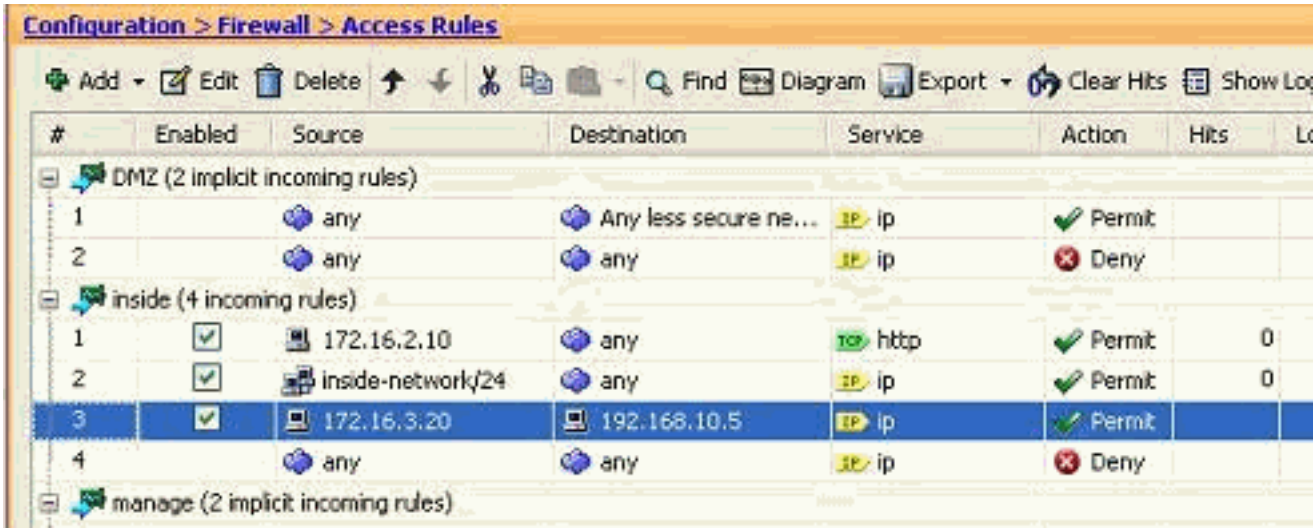
1. Seleccione la regla de acceso después de lo cual usted necesita tener una nueva regla de acceso, y elige el **separador de millares después del** menú desplegable del agregar.



2. Especifique los campos de la interfaz, de la acción, de la fuente, del destino y del servicio, y la **AUTORIZACIÓN del** tecleo para completar la configuración esta regla de acceso.

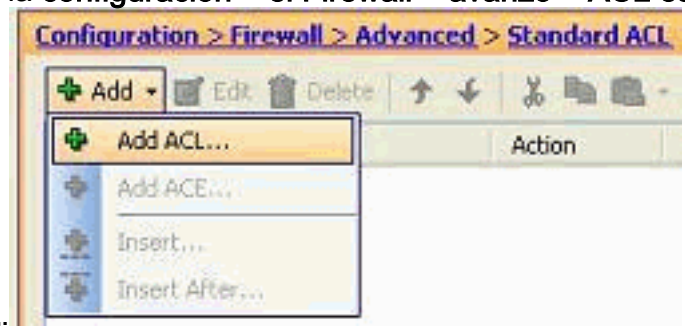


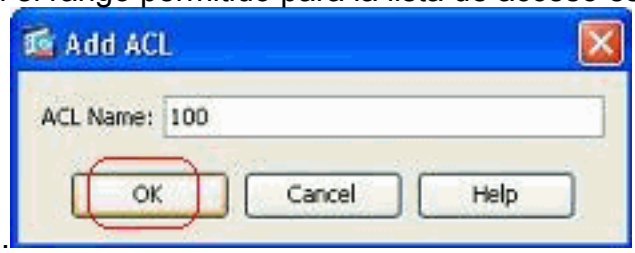
Usted puede ver que la regla del acceso configurado se sienta nuevamente enseguida después que ya configurada.

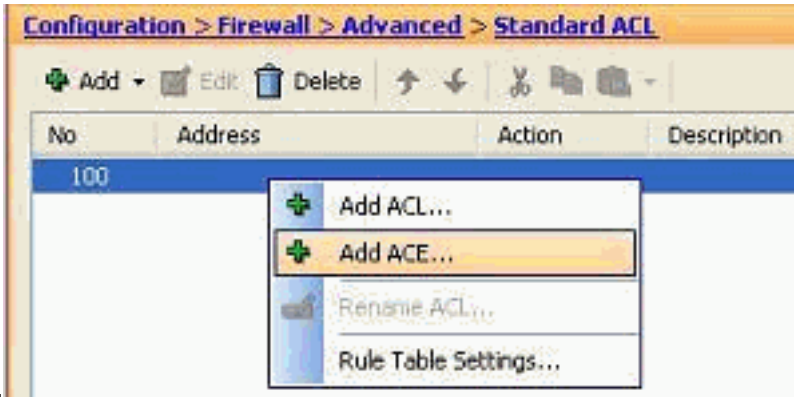


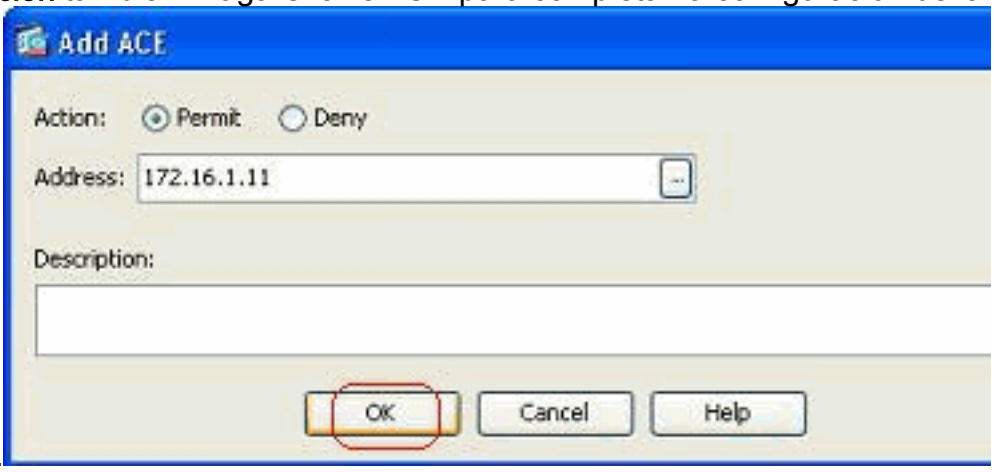
Cree una lista de acceso estándar

Complete estos pasos para crear una lista de acceso estándar con el ASDM GUI.

1. Elija la **configuración > el Firewall > avanzó > ACL estándar > Add**, y el tecleo **agrega el ACL**.


2. Dé un número en el rango permitido para la lista de acceso estándar, y haga clic la **AUTORIZACIÓN**.


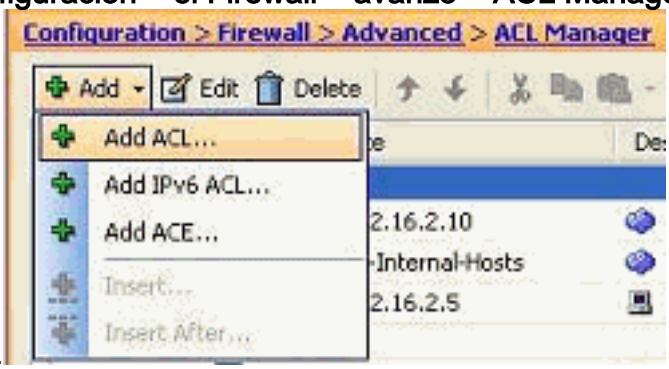
3. Haga clic con el botón derecho del ratón la lista de acceso, y elija **agregan ACE** para agregar una regla de acceso a esta lista de acceso.


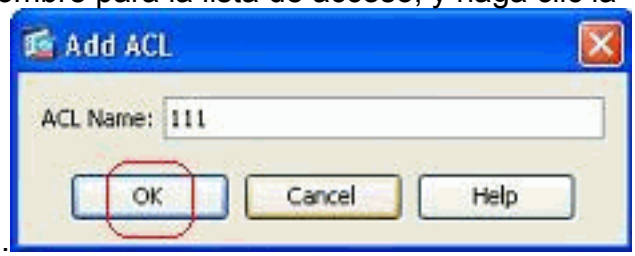
4. Seleccione la **acción**, y especifique a la **dirección de origen**. Si procede, especifique la **descripción** también. Haga Click en OK para completar la configuración de la regla de acceso.


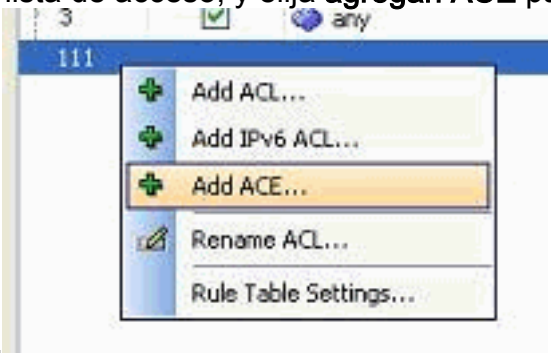
Cree una regla de acceso global

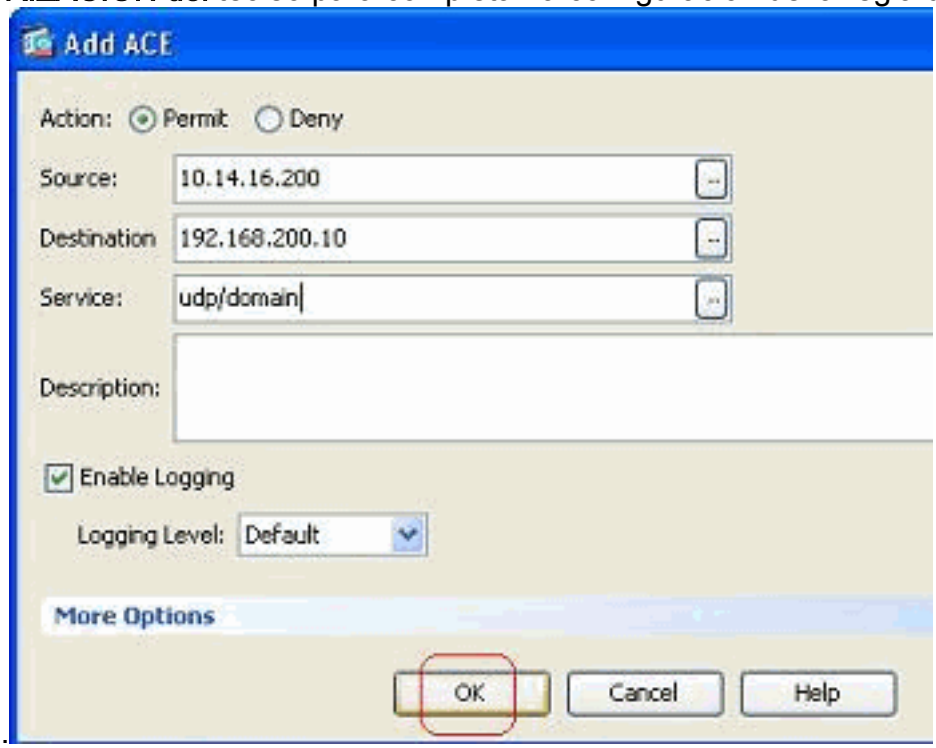
Complete estos pasos para crear una lista de acceso ampliada que contenga las reglas de

acceso globales.

1. Elija la **configuración > el Firewall > avanzó > ACL Manager > Add**, y el tecleo **agrega el** botón **ACL**.


2. Especifique un nombre para la lista de acceso, y haga clic la **AUTORIZACIÓN**.


3. Haga clic con el botón derecho del ratón la lista de acceso, y elija **agregan ACE** para agregar una regla de acceso a esta lista de acceso.


4. Complete los campos de la acción, de la fuente, del destino, y del servicio, y la **AUTORIZACIÓN del** tecleo para completar la configuración de la regla de acceso global.


Usted puede ahora ver la regla de acceso global, como se muestra.

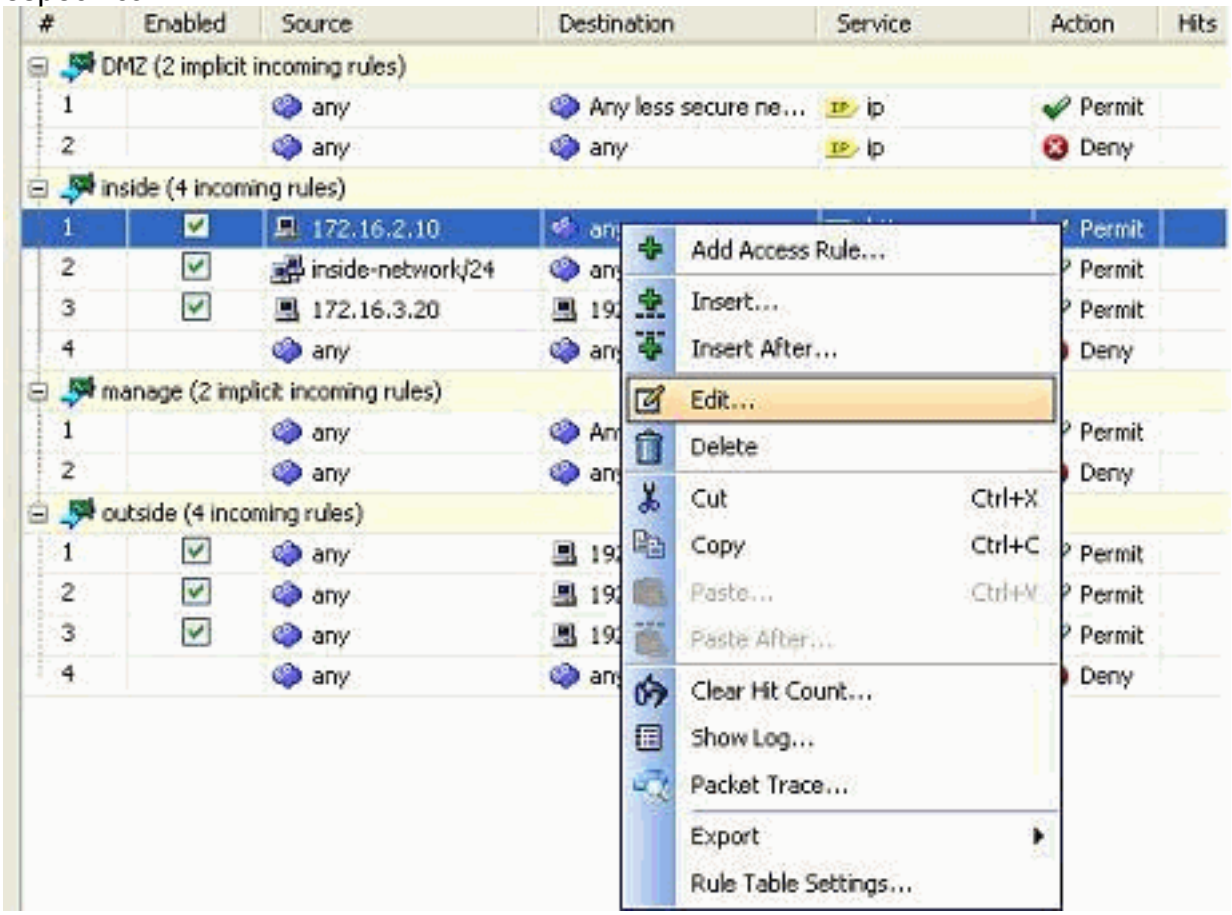
Edite una lista de acceso existente

Esta sección discute cómo editar un acceso existente.

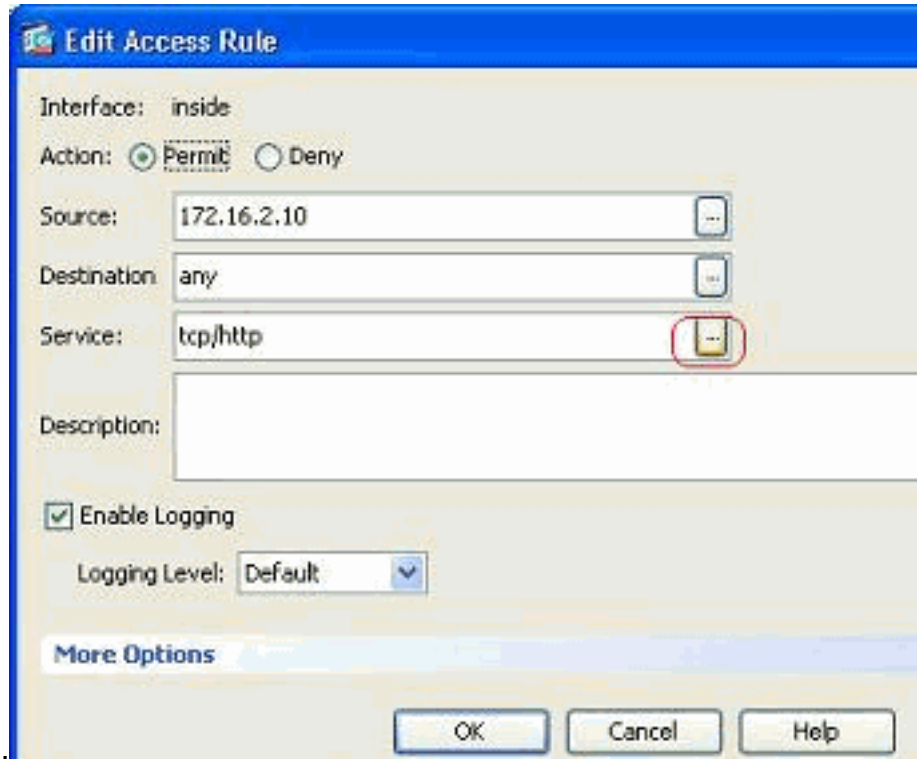
Edite el campo del protocolo para crear a un grupo de servicios:

Complete estos pasos para crear a un nuevo grupo de servicios.

1. Haga clic con el botón derecho del ratón la regla de acceso que necesita ser modificada, y elija **editan** para modificar esa regla de acceso específica.

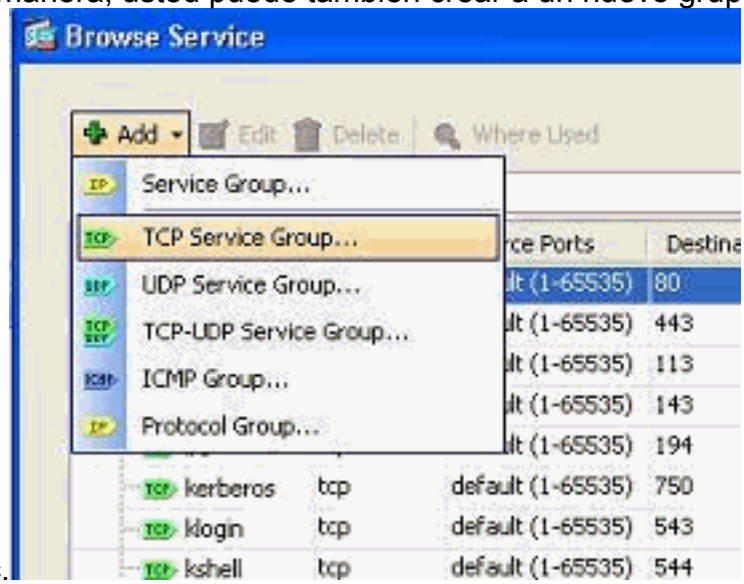


2. Haga clic el **botón Details Button** para modificar el protocolo asociado a esta regla de

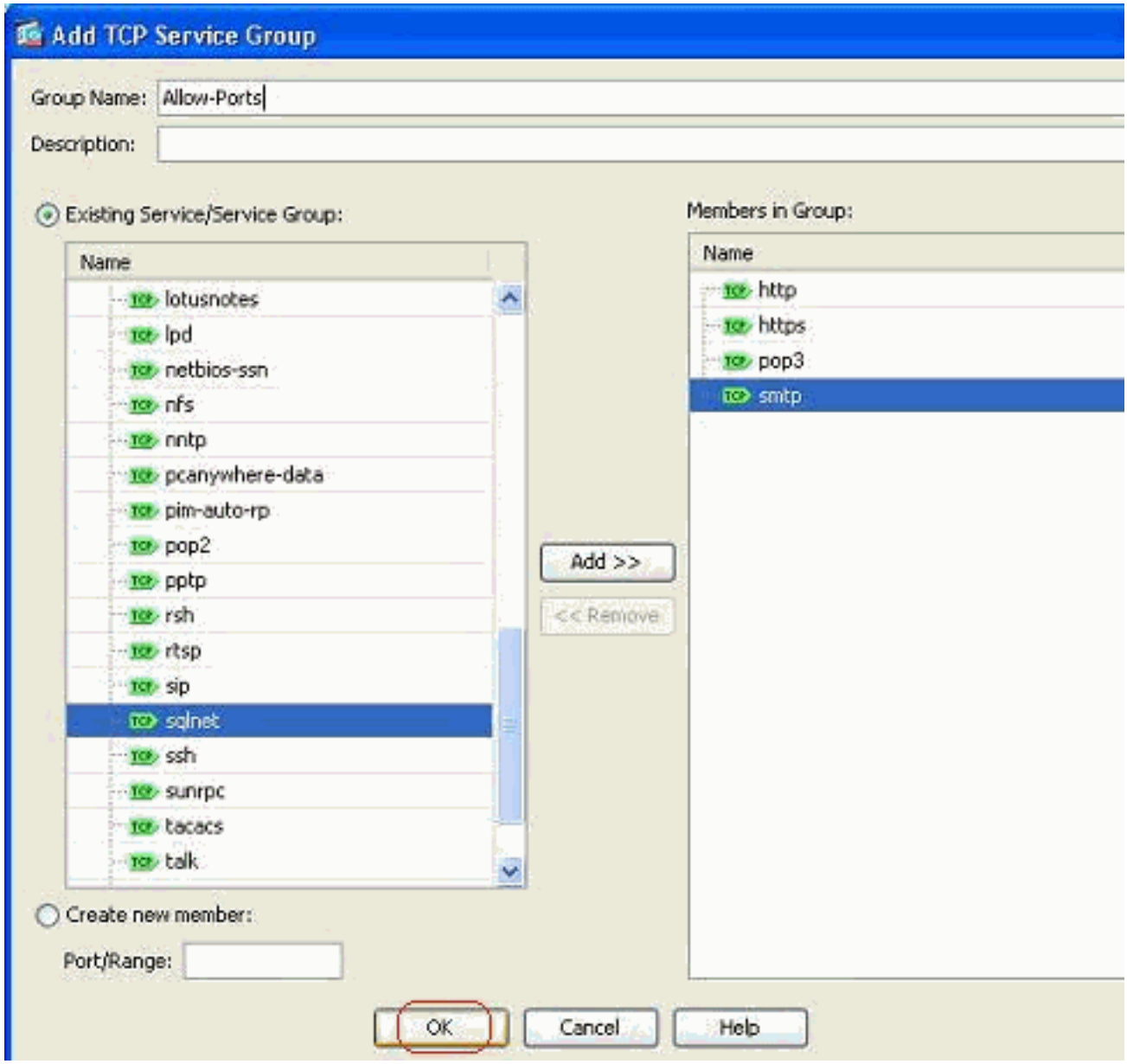


acceso.

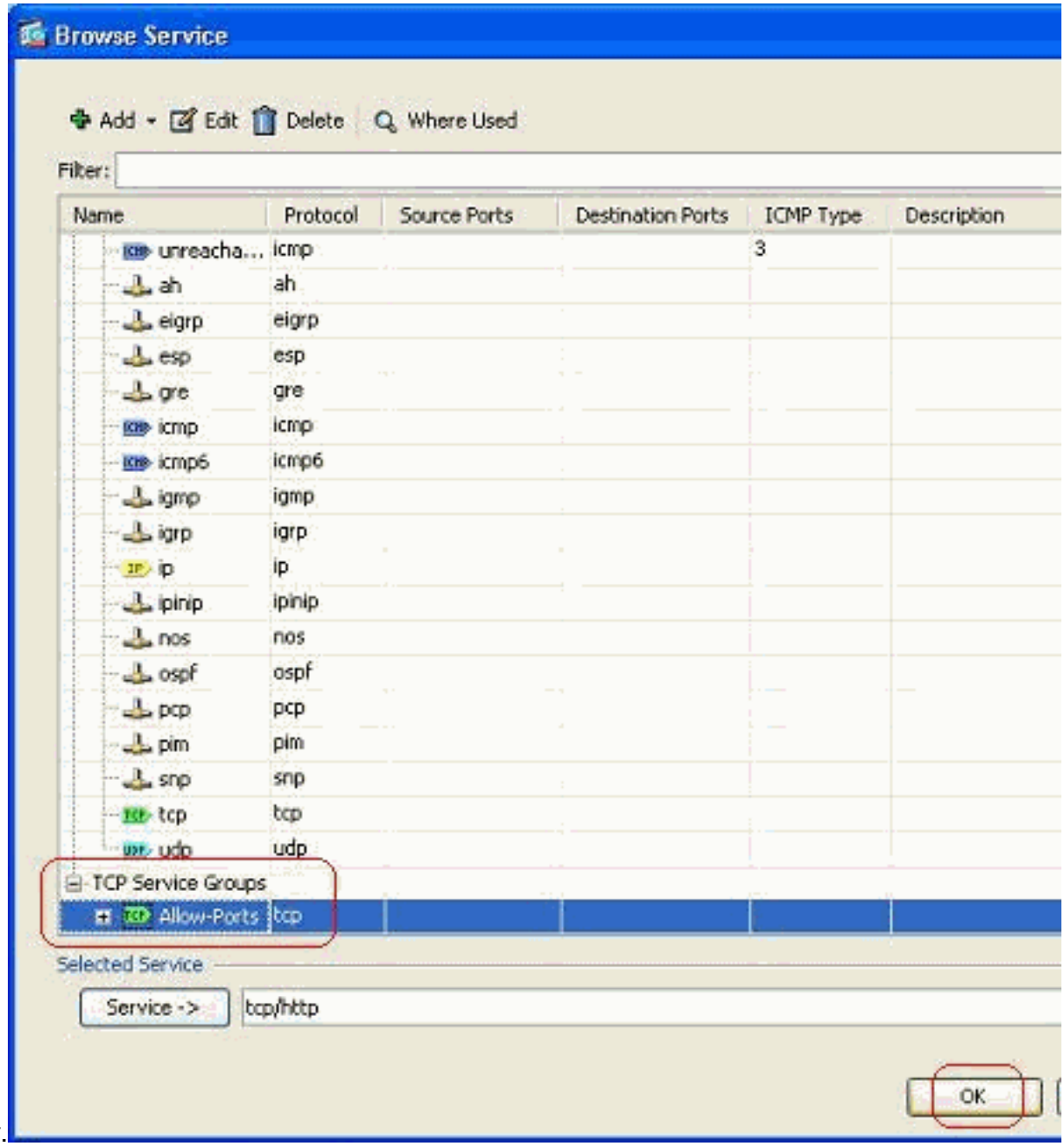
3. Usted puede seleccionar cualquier protocolo con excepción del HTTP si procede. Si hay solamente un solo protocolo que se seleccionará, después no hay necesidad de crear al grupo de servicios. Es útil crear a un grupo de servicios cuando hay un requisito de identificar los protocolos no adyacentes numerosos que se corresponderán con por esta regla de acceso.Elija **agregan > grupo de servicios TCP** para crear a un nuevo grupo de servicios TCP.**Nota:** De la misma manera, usted puede también crear a un nuevo grupo de servicios UDP o grupo ICMP y etc.



4. Especifique un nombre para este grupo de servicios, seleccione el protocolo en el menú del lado izquierdo, y el tecleo **agrega** para moverlos a los miembros en el menú del grupo en el lado derecho. Los protocolos numerosos se pueden agregar como miembros de un grupo de servicios basado en el requisito. Los protocolos se agregan uno por uno. Después de todo agregan a los miembros, **AUTORIZACIÓN del**
tecleo.

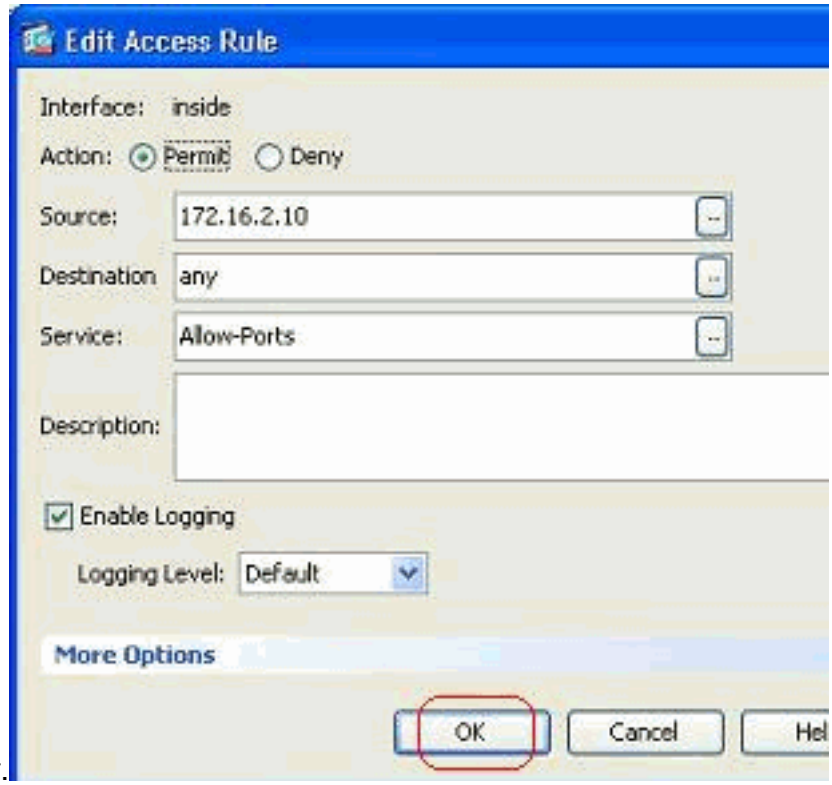


5. El grupo de servicios creado recientemente puede ser visto bajo **grupos de servicios de la** lengueta **TCP**. Botón del Haga Click en OK a volver a la ventana de la regla de acceso del



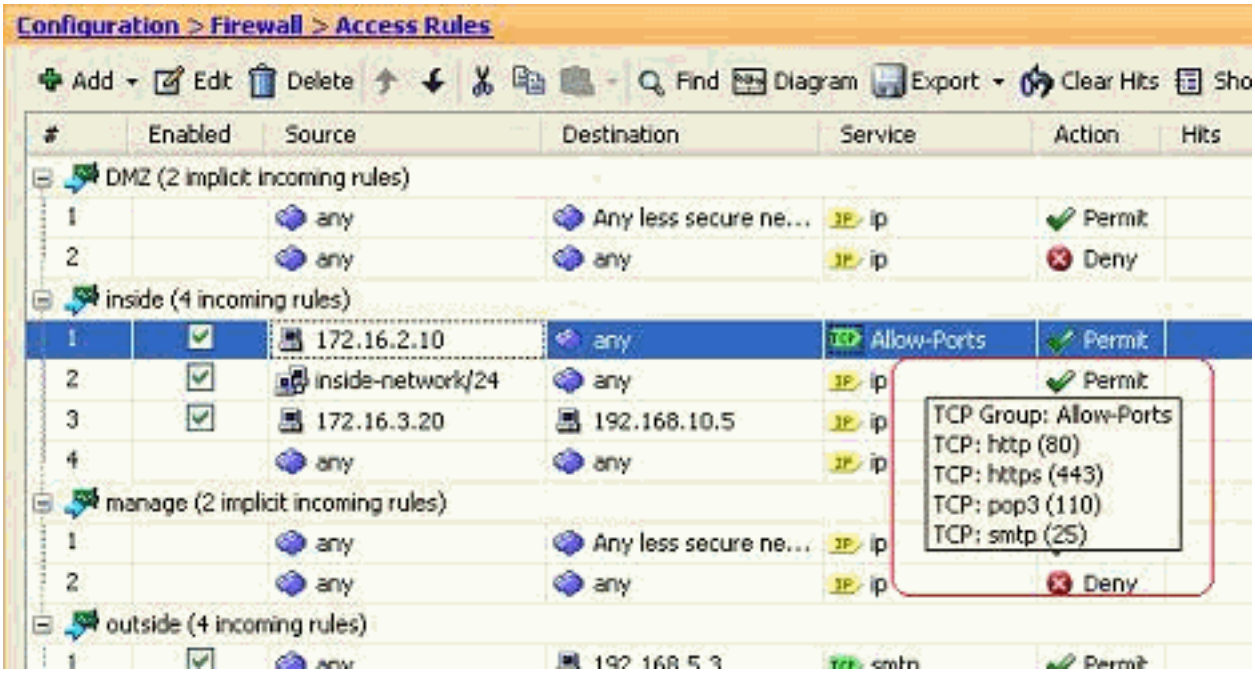
editar.

6. Usted puede ver que el campo del servicio está poblado con el grupo de servicios creado recientemente. Haga Click en OK para completar el



editar.

7. Asoma su ratón sobre ese grupo de servicios específico para ver todos los protocolos asociados.

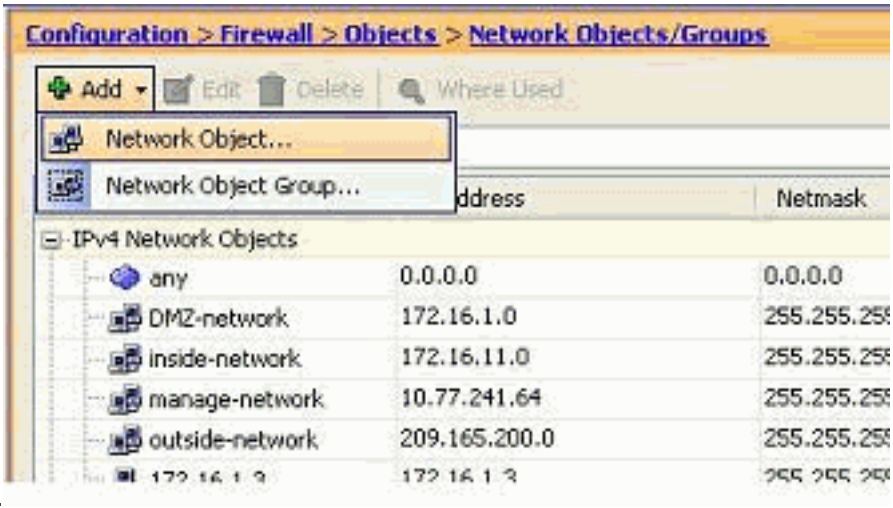


Edite la fuente/los Campos Destination para crear un grupo de objeto de red:

Utilizan a los grupos de objetos para simplificar la creación y el mantenimiento de las Listas de acceso. Cuando usted agrupa como los objetos junto, usted puede utilizar al grupo de objetos en un solo ACE en vez de tener que ingresar un ACE para cada objeto por separado. Antes de que usted cree al grupo de objetos, usted necesita crear los objetos. En la terminología del ASDM, el objeto se llama objeto de red y llaman el grupo de objetos grupo de objeto de red.

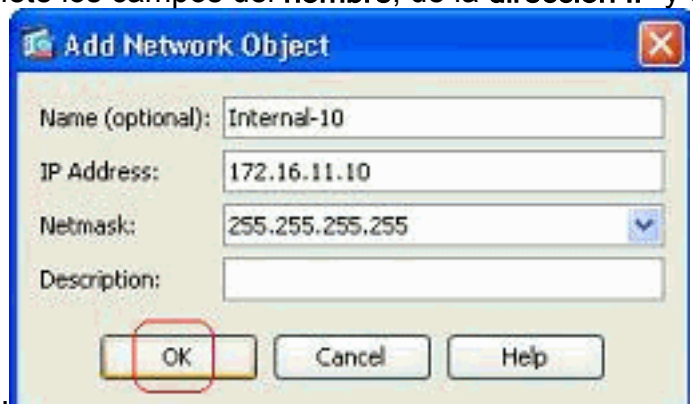
Complete estos pasos:

1. Elija la **configuración > el Firewall > los objetos > los objetos de red/a los grupos > Add**, y haga clic el **objeto de red** para crear un nuevo objeto de

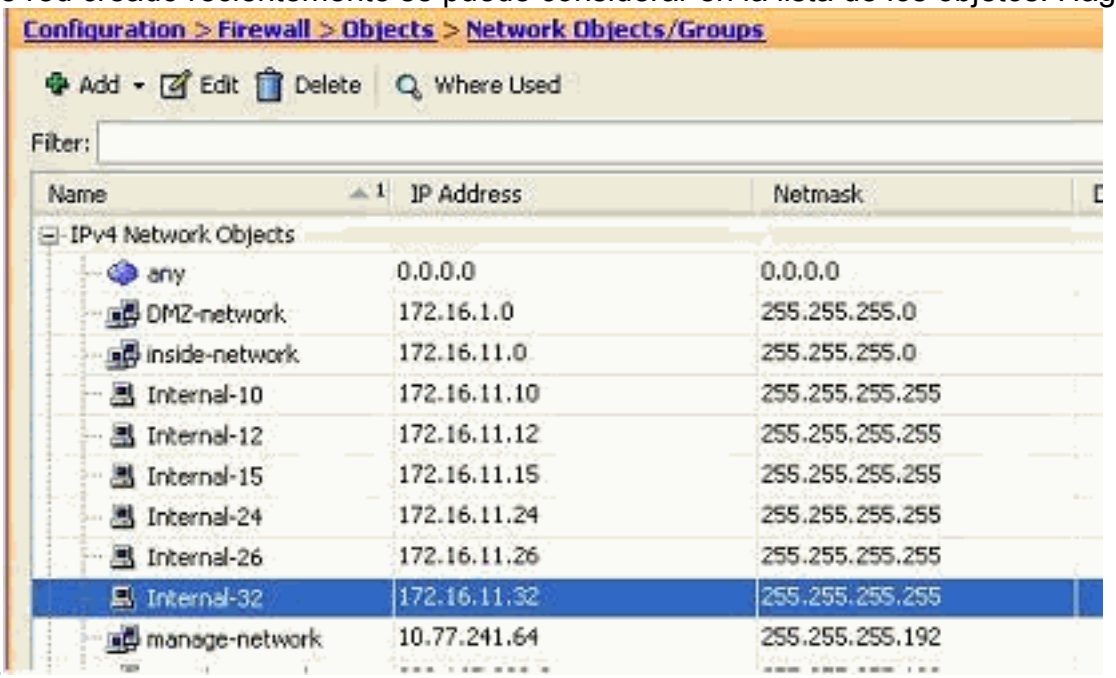


red.

2. Complete los campos del **nombre**, de la **dirección IP** y del **netmask**, y la **AUTORIZACIÓN del** tecleo.



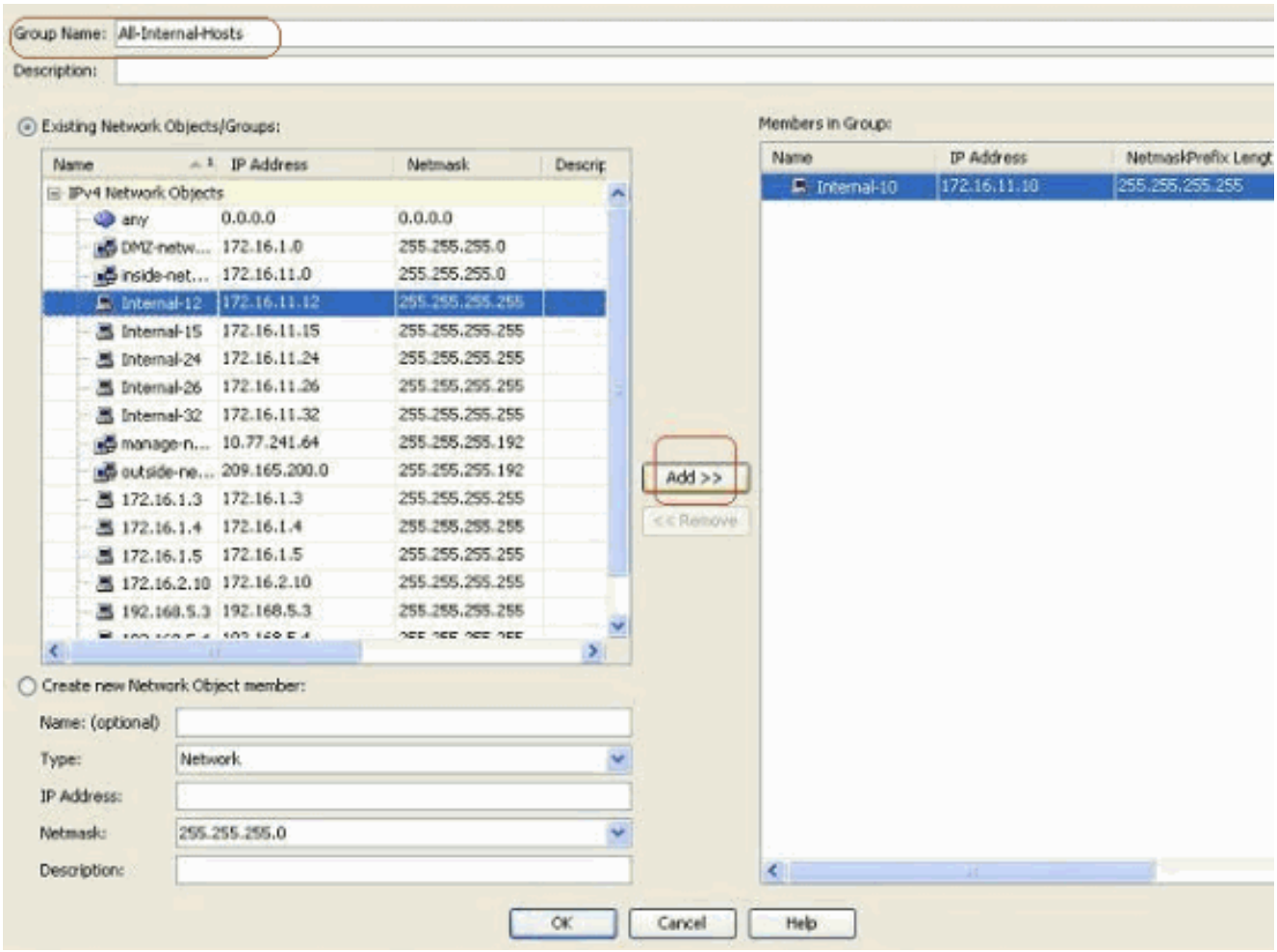
3. El objeto de red creado recientemente se puede considerar en la lista de los objetos. Haga clic en OK.



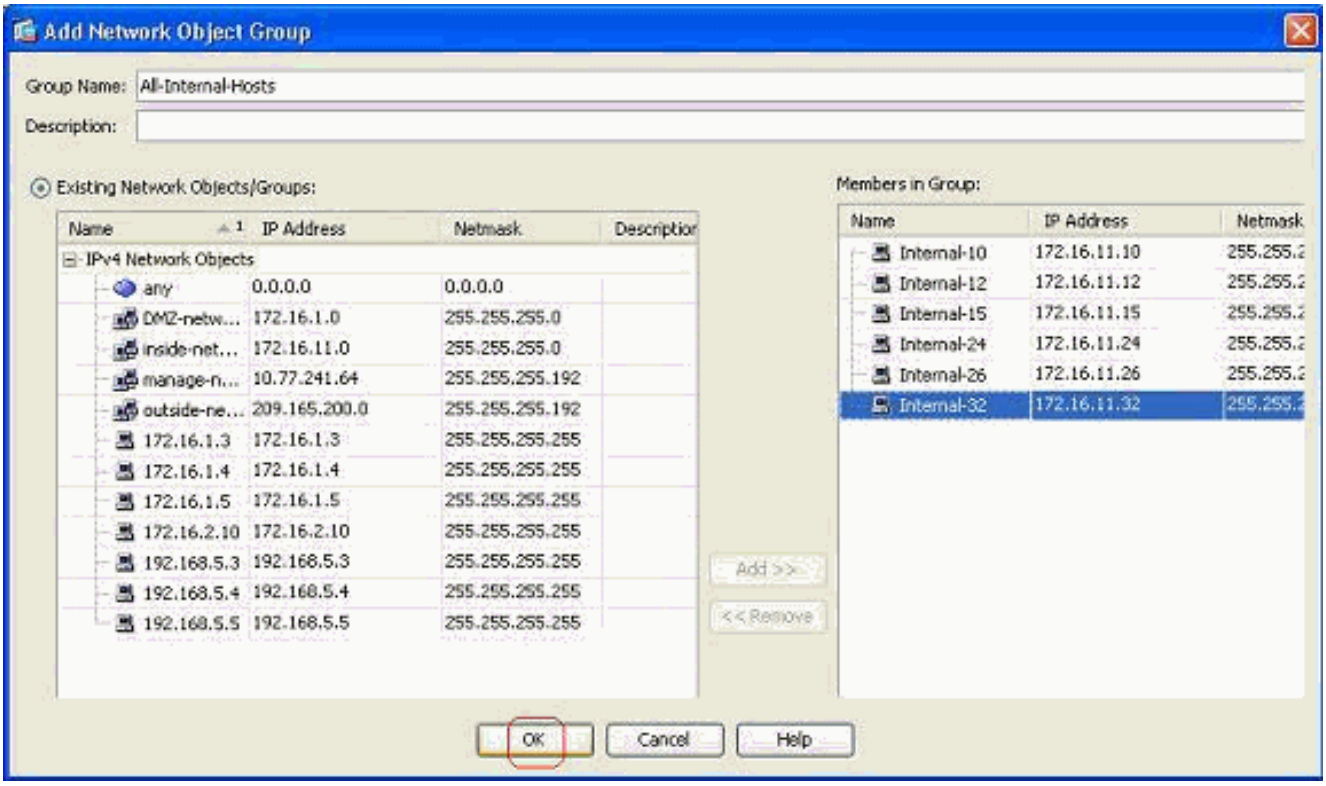
4. Elija la **configuración > el Firewall > los objetos > los objetos de red/a los grupos > Add**, y haga clic el **grupo de objeto de red** para crear un nuevo grupo de objeto de

red.

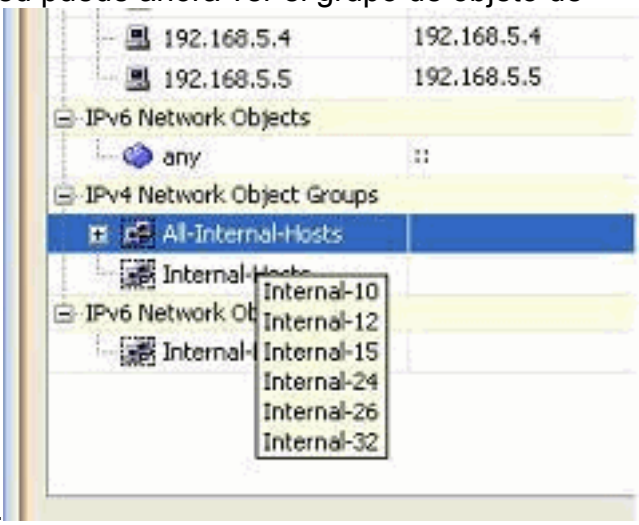
5. La lista disponible de todos los objetos de red se puede encontrar en el panel izquierdo de la ventana. Seleccione los objetos de red individual, y haga clic el **botón Add** para hacerles a los miembros del grupo de objeto de red creado recientemente. El nombre del grupo se debe especificar en el campo afectado un aparato para
él.



6. Haga Click en OK después de que usted agregue a todos los miembros adentro para agrupar.

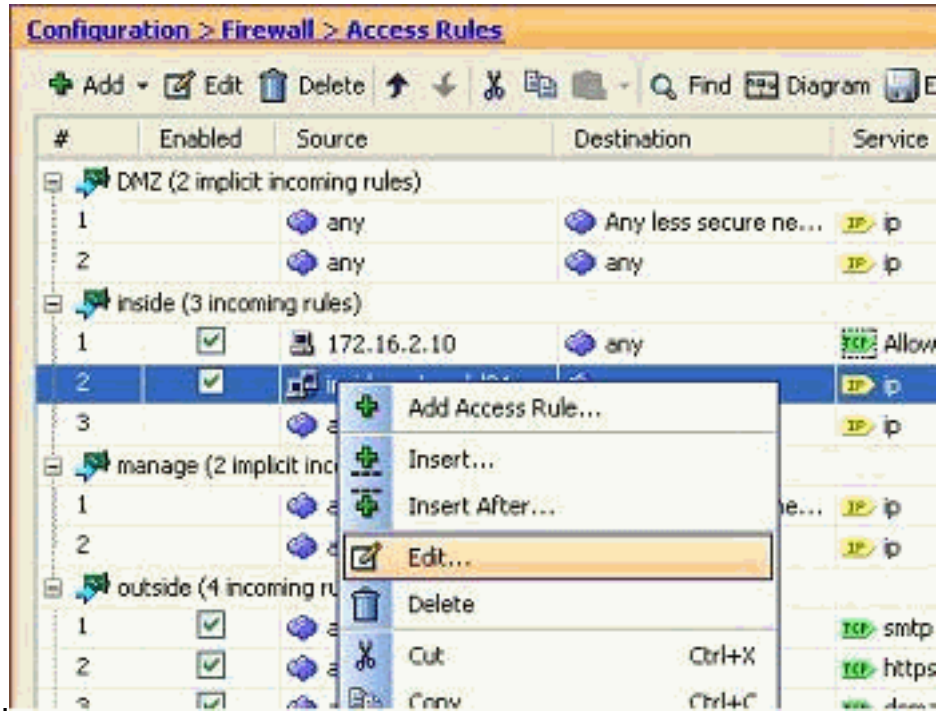


Usted puede ahora ver el grupo de objeto de red.

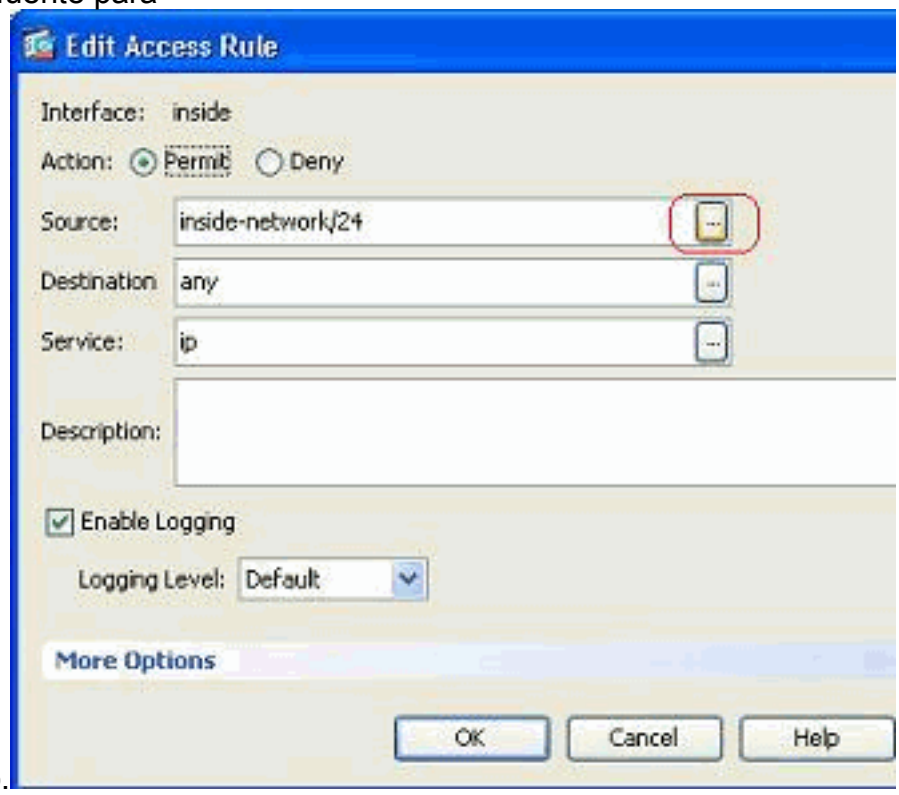


7. Para modificar cualquier fuente/Campo Destination de una lista de acceso existente con un objeto del grupo de red, hacer clic con el botón derecho del ratón la regla de acceso

específica, y elegir **edite**.



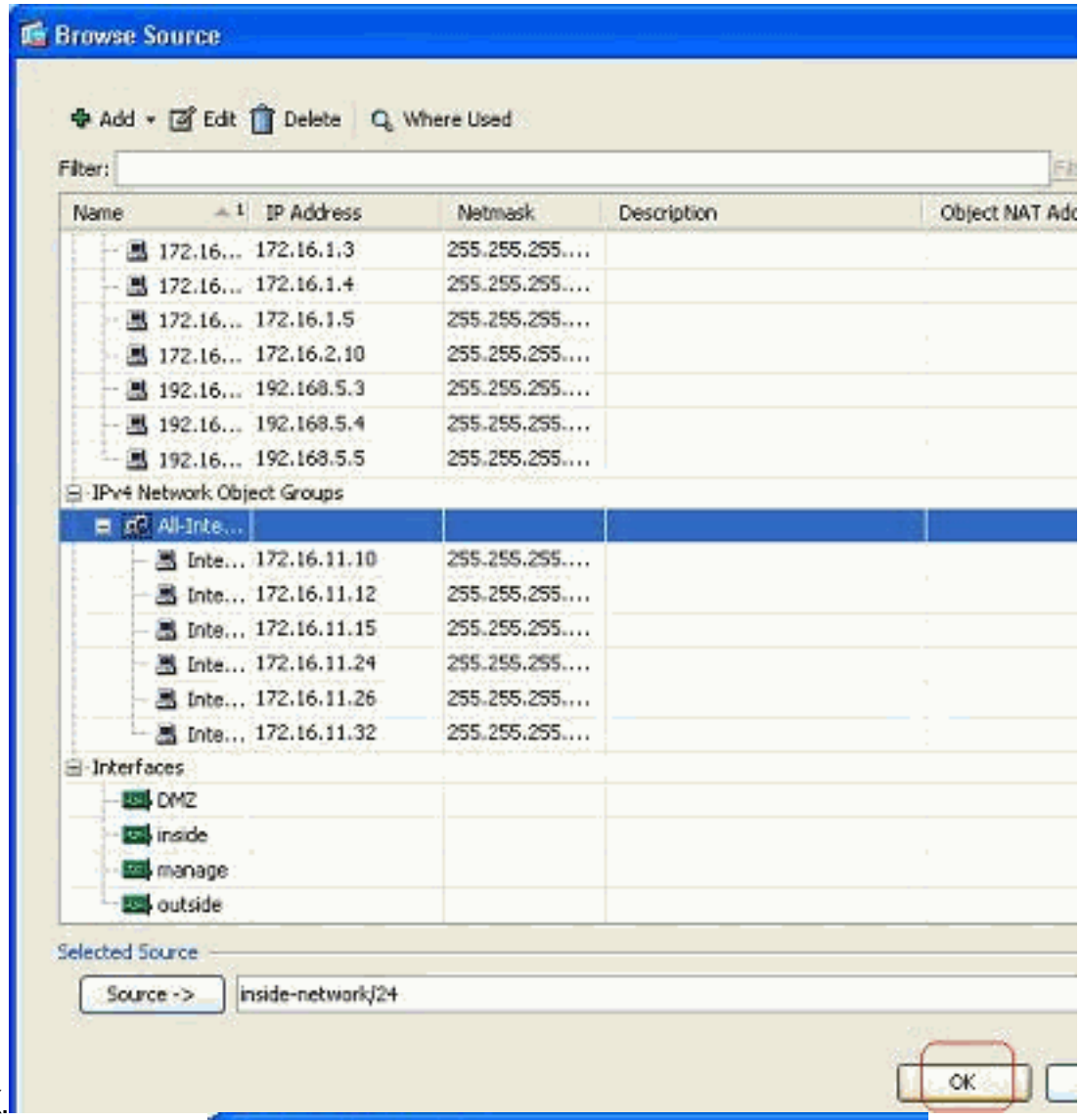
8. La ventana de la regla de acceso del editar aparece. Haga clic en el **botón Details Button del** campo de fuente para



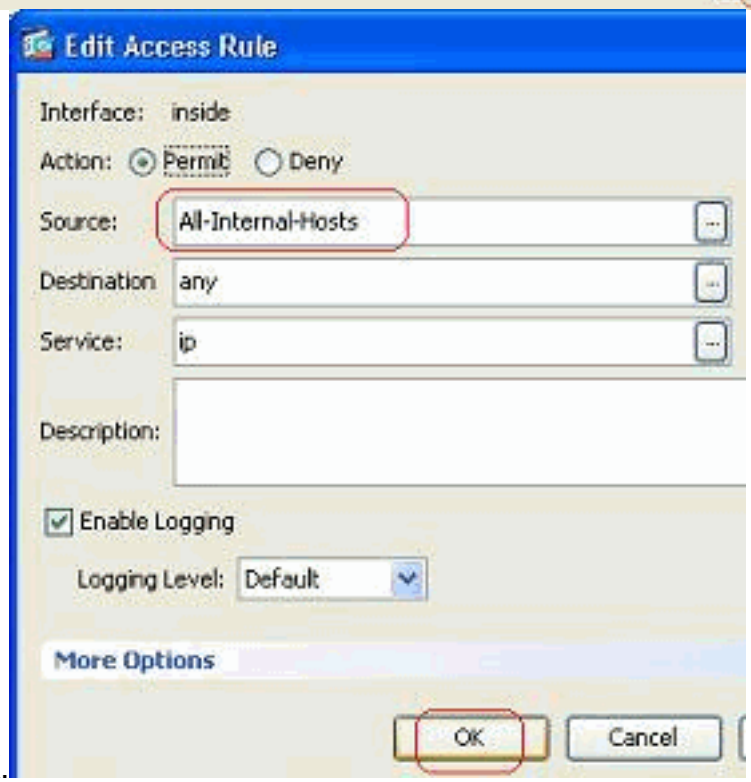
modificarlo.

9. Seleccione el grupo de objeto de red de los Todo-Interno-**host**, y haga clic el **botón**

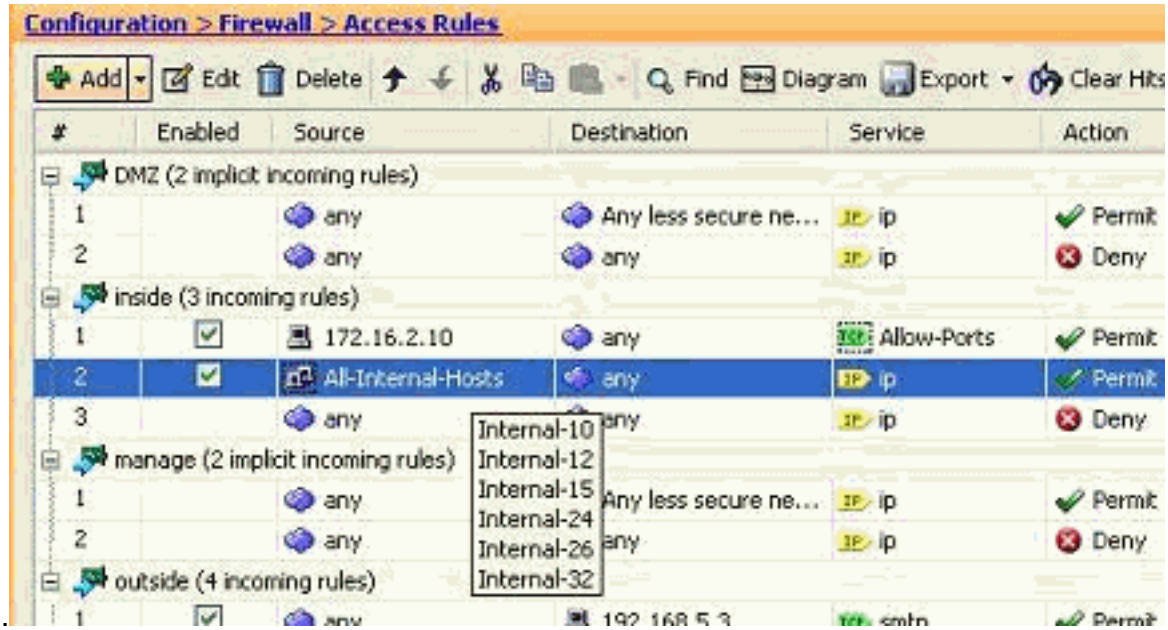
OK.



10. Haga clic en OK.



11. Asoma su ratón sobre el campo de fuente de la regla de acceso para ver a los miembros

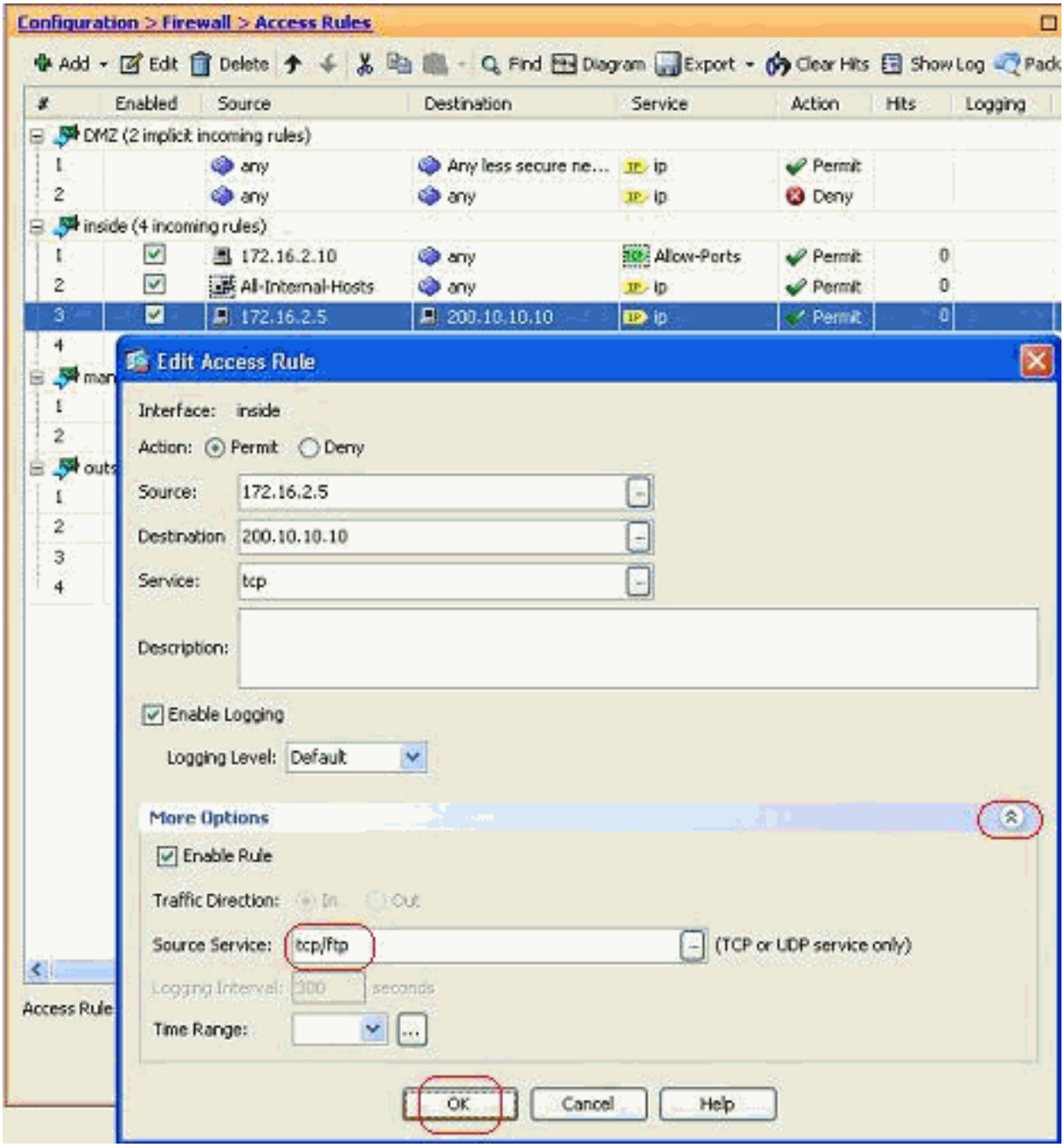


del grupo.

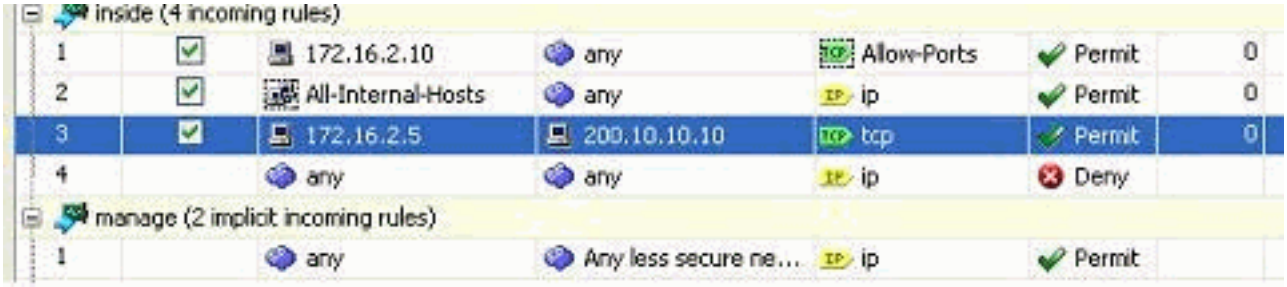
Edite el puerto de origen:

Complete estos pasos para modificar el puerto de origen de una regla de acceso.

1. Para modificar el puerto de origen de una regla de acceso existente, hacerla clic con el botón derecho del ratón, y elegir **edite**.La ventana de la regla de acceso del editar aparece.



2. Haga clic el **más** botón del descenso-abajo de las **opciones** para modificar el campo del servicio de la fuente, y haga clic la **AUTORIZACIÓN**.Usted puede ver la regla de acceso modificada, como se
muestra.

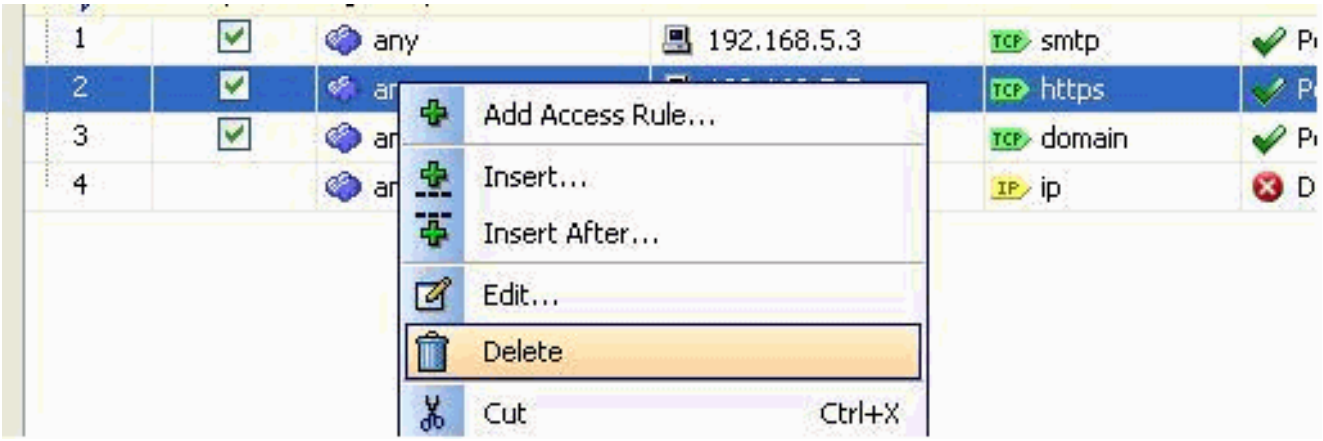


Borre una lista de acceso

Complete estos pasos para borrar una lista de acceso:

1. Antes de que usted borre una lista de acceso existente, usted necesita borrar las entradas

de lista de acceso (las reglas de acceso). No es posible borrar la lista de acceso a menos que usted primero borre todas las reglas de acceso.Haga clic con el botón derecho del ratón la regla de acceso para ser borrado, y elija la **cancelación**.



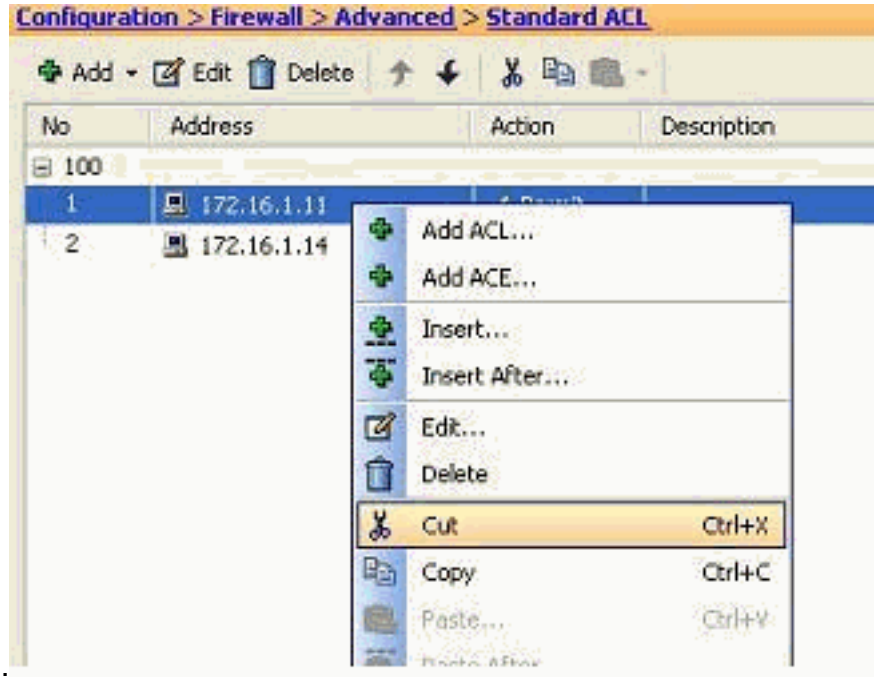
2. Complete la misma operación de eliminación en todas las reglas de acceso existentes, y entonces seleccione la lista de acceso y elija la **cancelación** para borrarla.

Exporte la regla de acceso

Las reglas de acceso del ASDM atan la lista de acceso con la interfaz respectiva mientras que el ACL Manager sigue todas las listas de acceso ampliadas. Las reglas de acceso que se crean con el ACL Manager no atan a ninguna interfaz. Estas Listas de acceso se utilizan generalmente con el fin de NAT-exento, del VPN-filtro y de similar otras funciones donde no hay asociación con la interfaz. El ACL Manager contiene todas las entradas que usted tiene en la sección de la **configuración > del Firewall > de las reglas de acceso**. Además, el **ACL Manager** también contiene las reglas de acceso globales que no se asocian a ninguna interfaz. Se ordena el ASDM de una manera tal que usted pueda exportar una regla de acceso de cualquier lista de acceso a otro fácilmente.

Por ejemplo, si usted necesita una regla de acceso que sea ya una parte de a la regla de acceso global para ser asociado a una interfaz, usted no necesita configurar eso otra vez. En lugar, usted puede realizar una operación del **corte y de la goma** para alcanzar esto.

1. Haga clic con el botón derecho del ratón la regla de acceso especificada, y elija el



corte.

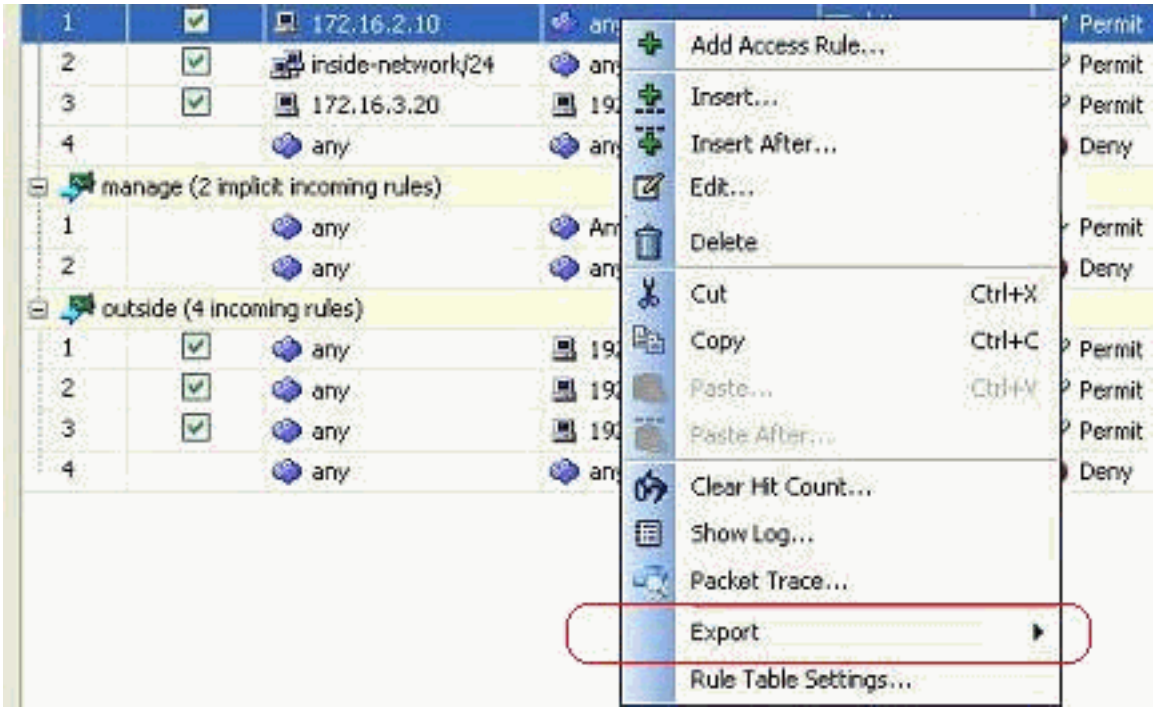
2. Seleccione la lista de acceso requerida en la cual usted necesita insertar esta regla de acceso. Usted puede utilizar la **goma** en la barra de herramienta para insertar la regla de acceso.

Exporte la información de la lista de acceso

Usted puede exportar la información de la lista de acceso a otro archivo. Dos formatos se soportan para exportar esta información.

1. Formato del Comma Separated Value (CSV)
2. Formato HTML

Haga clic con el botón derecho del ratón las reglas de acceso unas de los, y elija la **exportación** para enviar la información de la lista de acceso a un archivo.



Aquí está la información de la lista de acceso mostrada en el formato HTML.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

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

Información Relacionada

- Ejemplos y notas técnicas de la Configuración de ASDM
- Ejemplos de configuración y lista de notas técnicas ASA
- Soporte Técnico y Documentación - Cisco Systems