ASA 7.x/PIX 6.x y Versiones Posteriores: Ejemplo de Configuración para Abrir o Bloquear los Puertos

Contenido

Introducción

Este documento proporciona un ejemplo de configuración sobre cómo abrir o bloquear los puertos para diversos tipos de tráfico, tales como http o ftp, en el dispositivo Security Appliance.

Nota: Los términos "abriendo el puerto" y "autorizando el puerto" significan lo mismo. Del mismo modo, "bloqueando el puerto" y "restringiendo el puerto" también significan lo mismo.

Prerequisites

Requirements

Este documento supone que PIX/ASA está configurado y funciona correctamente.

Componentes Utilizados

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que ejecuta la versión 8.2(1)

- Versión 6.3(5) de Cisco Adaptive Security Device Manager (ASDM)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también se puede utilizar con el Cisco 500 Series PIX Firewall Appliance con la versión de software 6.x o posteriores.

Convenciones

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

Configurar

Cada interfaz debe tener un nivel de seguridad de 0 (más bajo) a 100 (más alto). Por ejemplo, debe asignar la red más segura, como la red host interna, al nivel 100. Mientras que la red externa conectada a Internet puede ser el nivel 0, otras redes, como las DMZ, pueden ubicarse entre sí. Puede asignar múltiples interfaces al mismo nivel de seguridad.

De forma predeterminada, todos los puertos se bloquean en la interfaz externa (nivel de seguridad 0) y todos los puertos se abren en la interfaz interna (nivel de seguridad 100) del dispositivo de seguridad. De este modo, todo el tráfico saliente puede pasar a través del dispositivo de seguridad sin necesidad de una configuración, pero el acceso del tráfico entrante debe autorizarse mediante la configuración de la lista de acceso y los comandos estáticos en el dispositivo de seguridad.

Nota: En general, todos los puertos se bloquean desde la Zona de Seguridad Más Baja a la Zona de Seguridad Más Alta y todos los puertos se abren desde la Zona de Seguridad Más Alta a la Zona de Seguridad Más Baja; siempre que esté habilitada la inspección de estado tanto para el tráfico entrante como saliente.

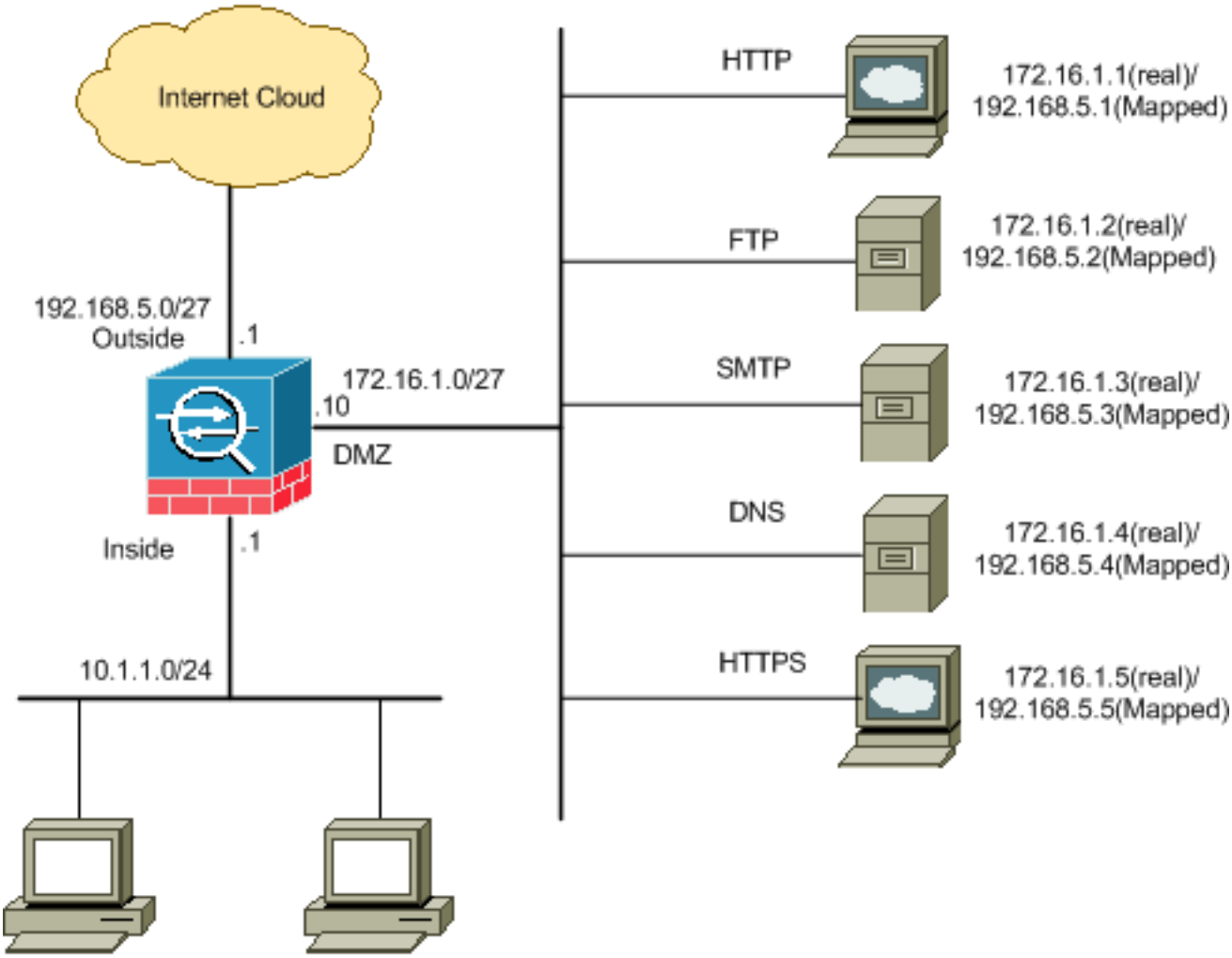
Esta sección comprende las siguientes subsecciones:

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración de Bloqueo de los Puertos

El dispositivo de seguridad permite cualquier tráfico saliente, excepto que esté explícitamente bloqueado por una lista de acceso extendido.

Una lista de acceso está conformada por una o más Access Control Entries (ACE). Según el tipo de lista de acceso, usted puede especificar las direcciones de origen y destino, el protocolo, los puertos (para TCP o UDP), el tipo ICMP (para ICMP) o EtherType.

Nota: Para los protocolos sin conexión, como ICMP, el dispositivo de seguridad establece sesiones unidireccionales, de modo que usted necesita listas de acceso para autorizar el ICMP en ambas direcciones (mediante la aplicación de listas de acceso a las interfaces de origen y destino) o bien debe habilitar el motor de inspección del ICMP. El motor de inspección del ICMP trata las sesiones del ICMP como conexiones bidireccionales.

Siga estos pasos para bloquear los puertos, que generalmente se aplican al tráfico que se origina desde la zona interna (zona de seguridad más alta) a la DMZ (zona de seguridad más baja) o desde la DMZ a la zona externa.

1. Cree una Access Control List (ACL) de forma que bloquee el tráfico del puerto especificado.

```
access-list
```

2. Luego vincule la lista de acceso con el comando **access-group** para activarla.

```
access-group
```

Examples:

1. **Bloqueo del tráfico del puerto HTTP:** Para bloquear el acceso de la red interna 10.1.1.0 al http (servidor Web) con IP 172.16.1.1 ubicada en la red DMZ, cree una ACL como se indica a continuación:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

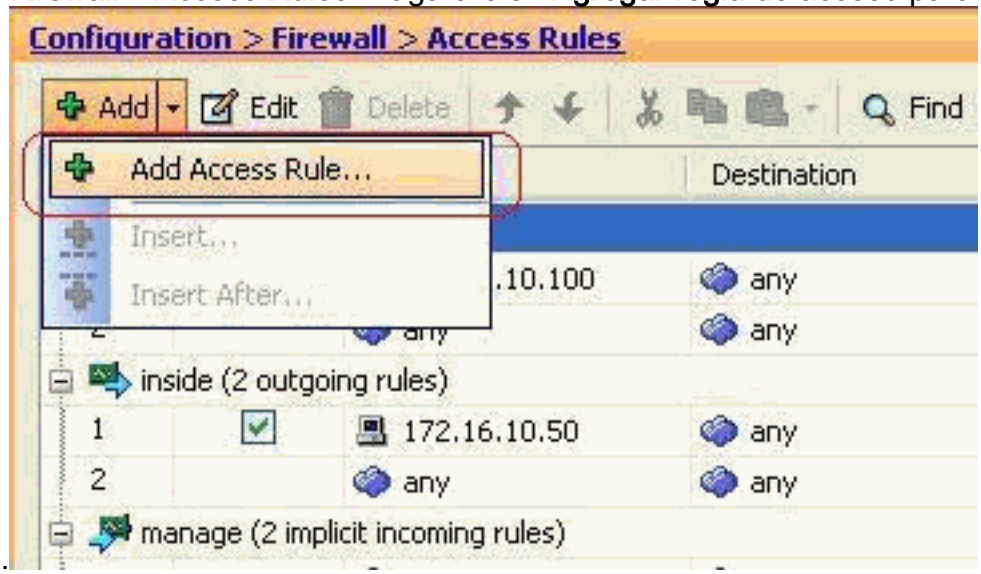
   Nota: Utilice **no** seguido de los comandos de la lista de acceso para eliminar el bloqueo del puerto.
2. **Bloqueo del tráfico del puerto FTP:** Para bloquear el acceso de la red interna 10.1.1.0 al FTP (servidor de archivos) con IP 172.16.1.2 ubicada en la red DMZ, cree una ACL como se indica a continuación:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

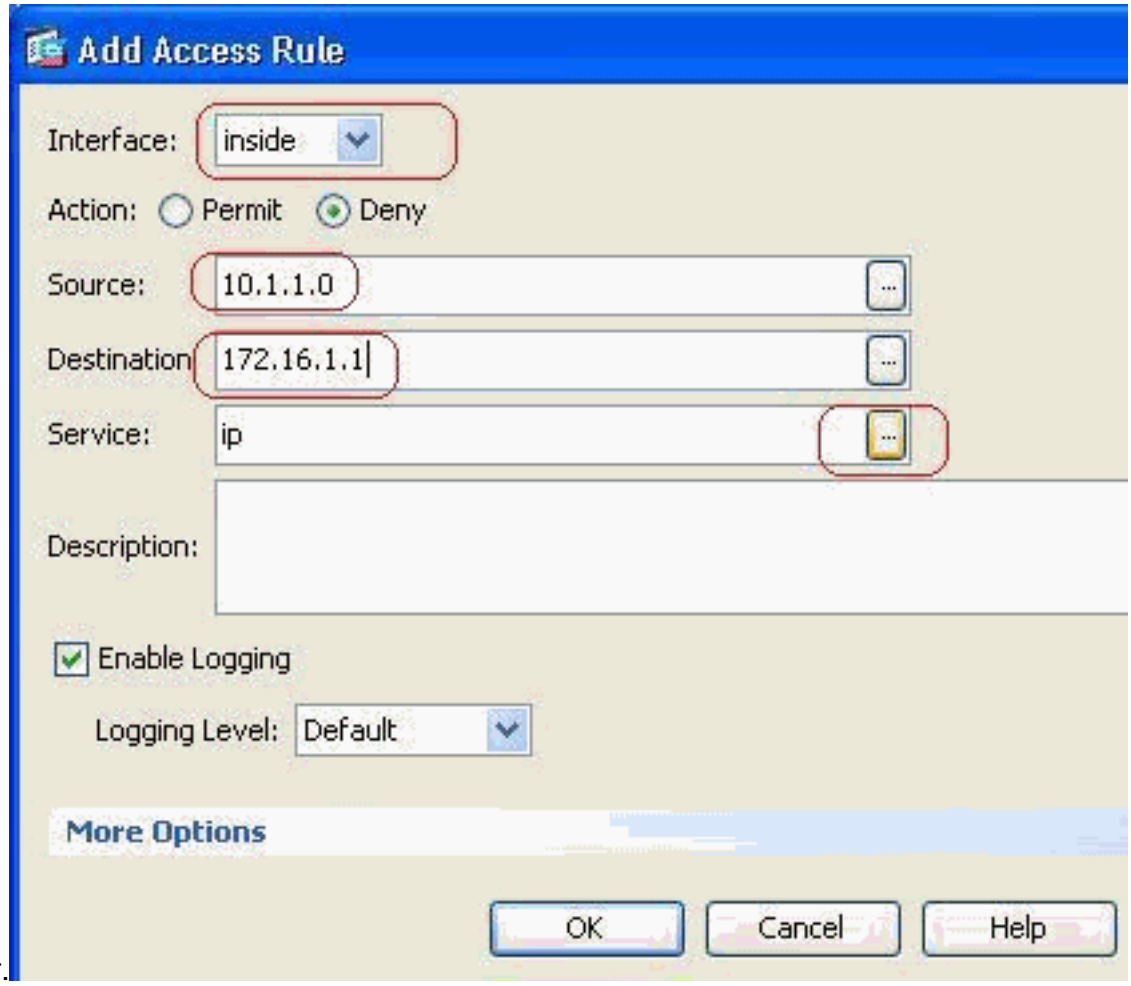
Nota: Consulte Puertos IANA para obtener más información sobre las asignaciones de puerto.

La configuración paso a paso para realizar esto a través del ASDM se muestra en esta sección.

1. Vaya a **Configuration > Firewall > Access Rules**. Haga clic en **Agregar regla de acceso** para crear la lista de acceso.

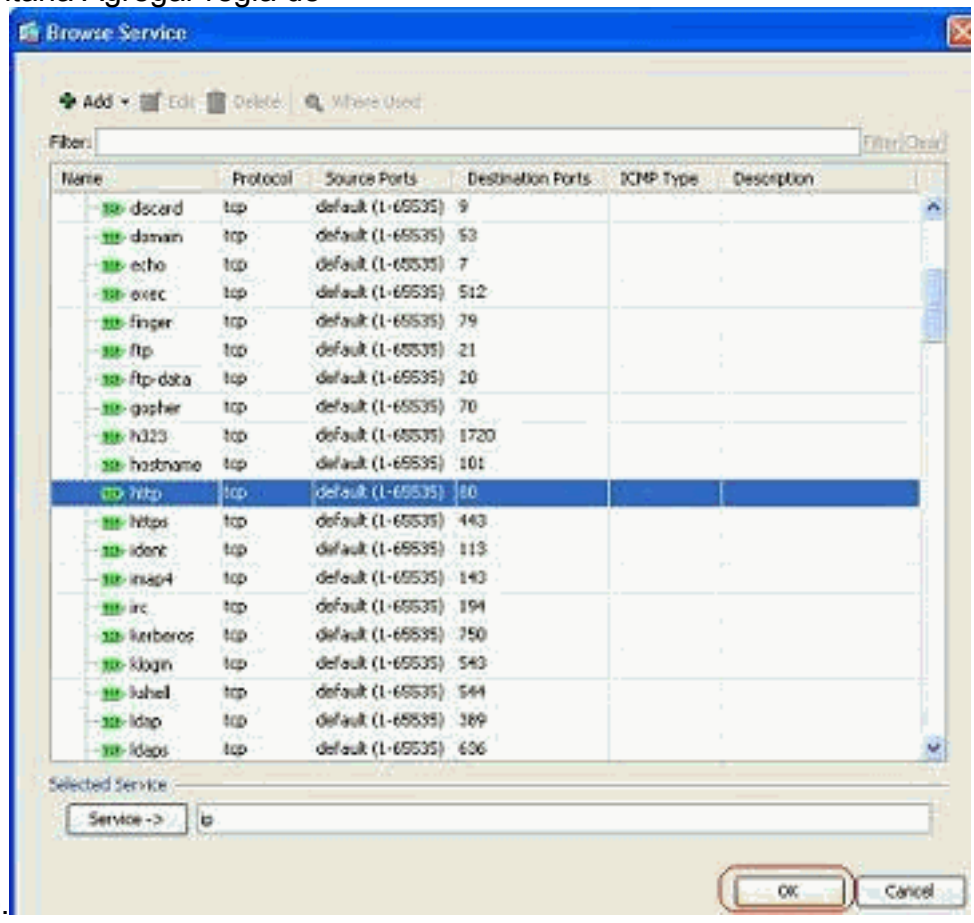


2. Defina el origen y el destino y la acción de la regla de acceso junto con la interfaz a la que se asociará esta regla de acceso. Seleccione los detalles para elegir el puerto específico que desea



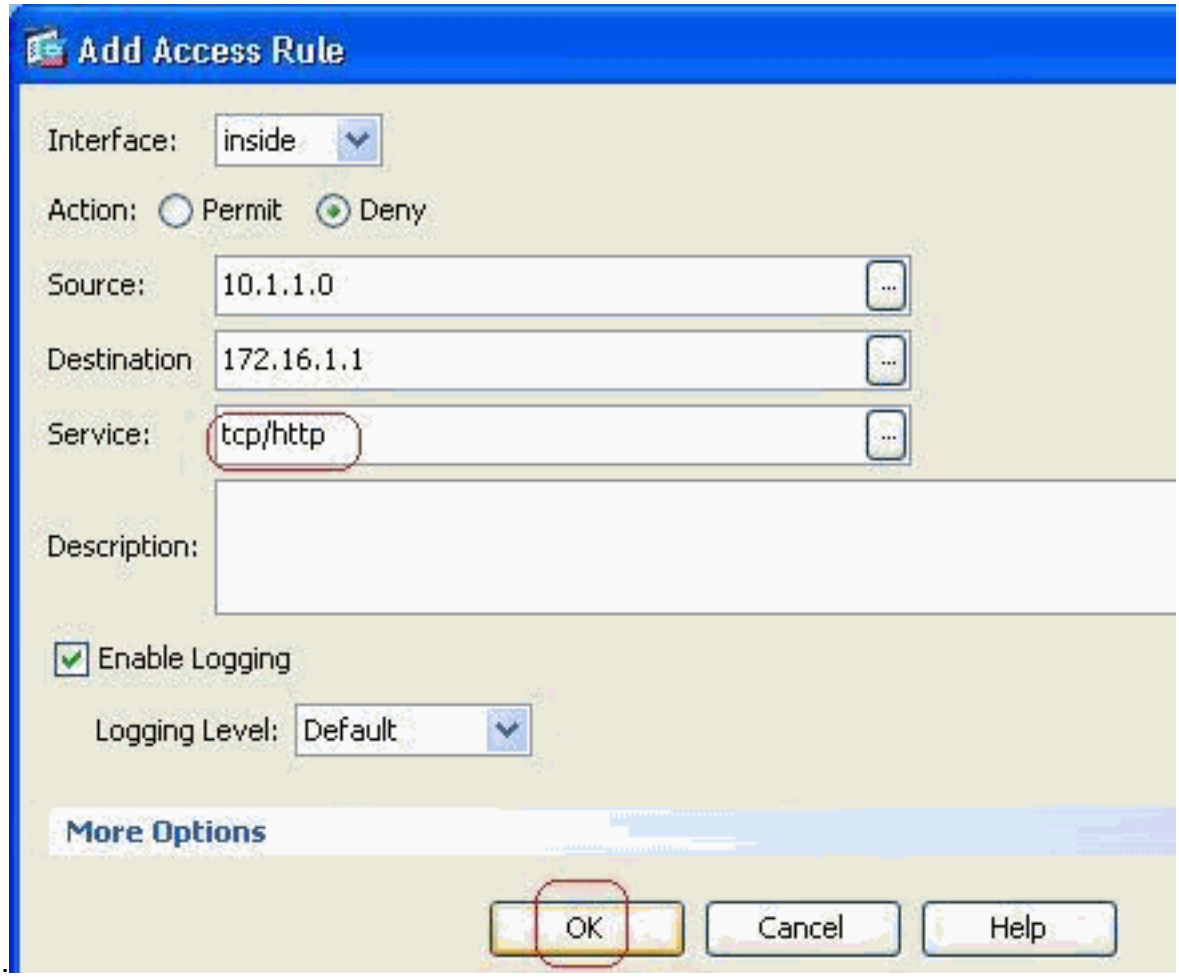
bloquear.

3. Elija **http** de la lista de puertos disponibles y, a continuación, haga clic en **Aceptar** para volver a la ventana Agregar regla de



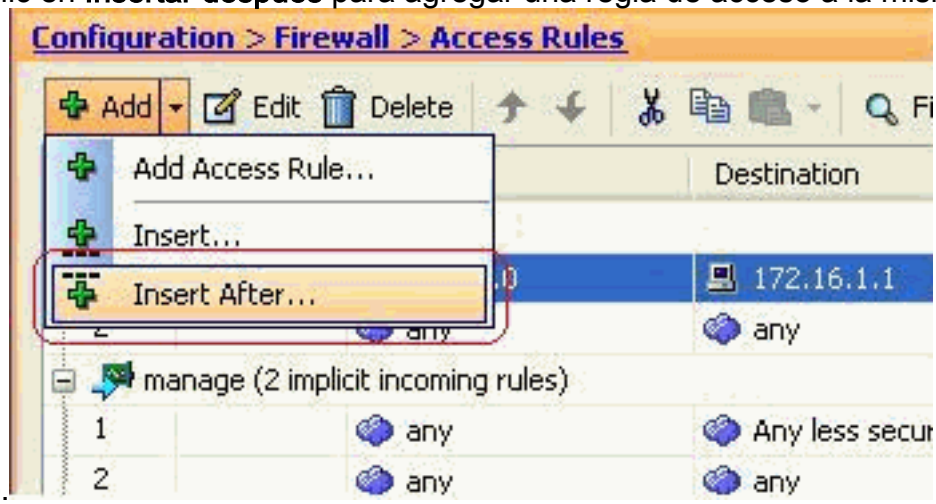
acceso.

4. Haga clic en **Aceptar** para completar la configuración de la regla de



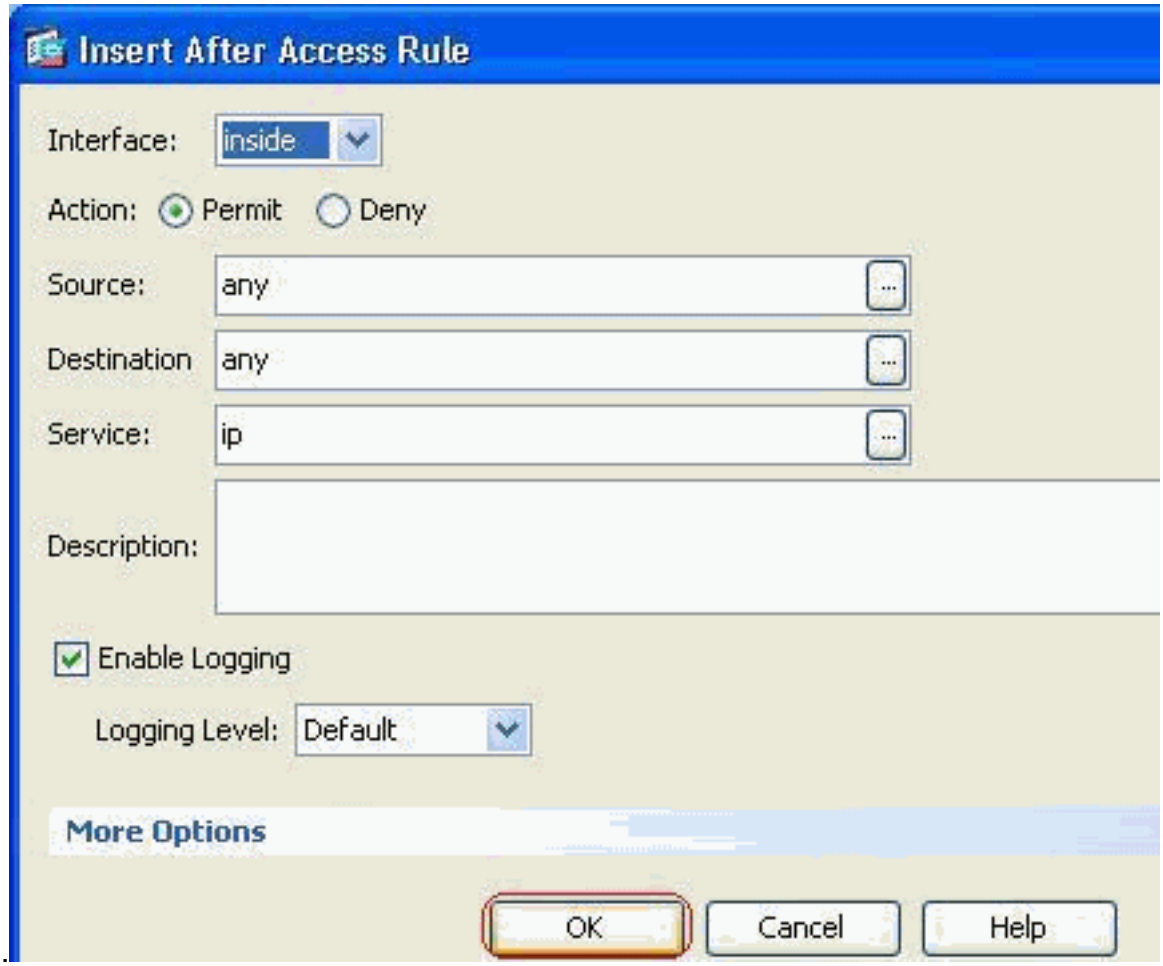
acceso.

5. Haga clic en **Insertar después** para agregar una regla de acceso a la misma lista de



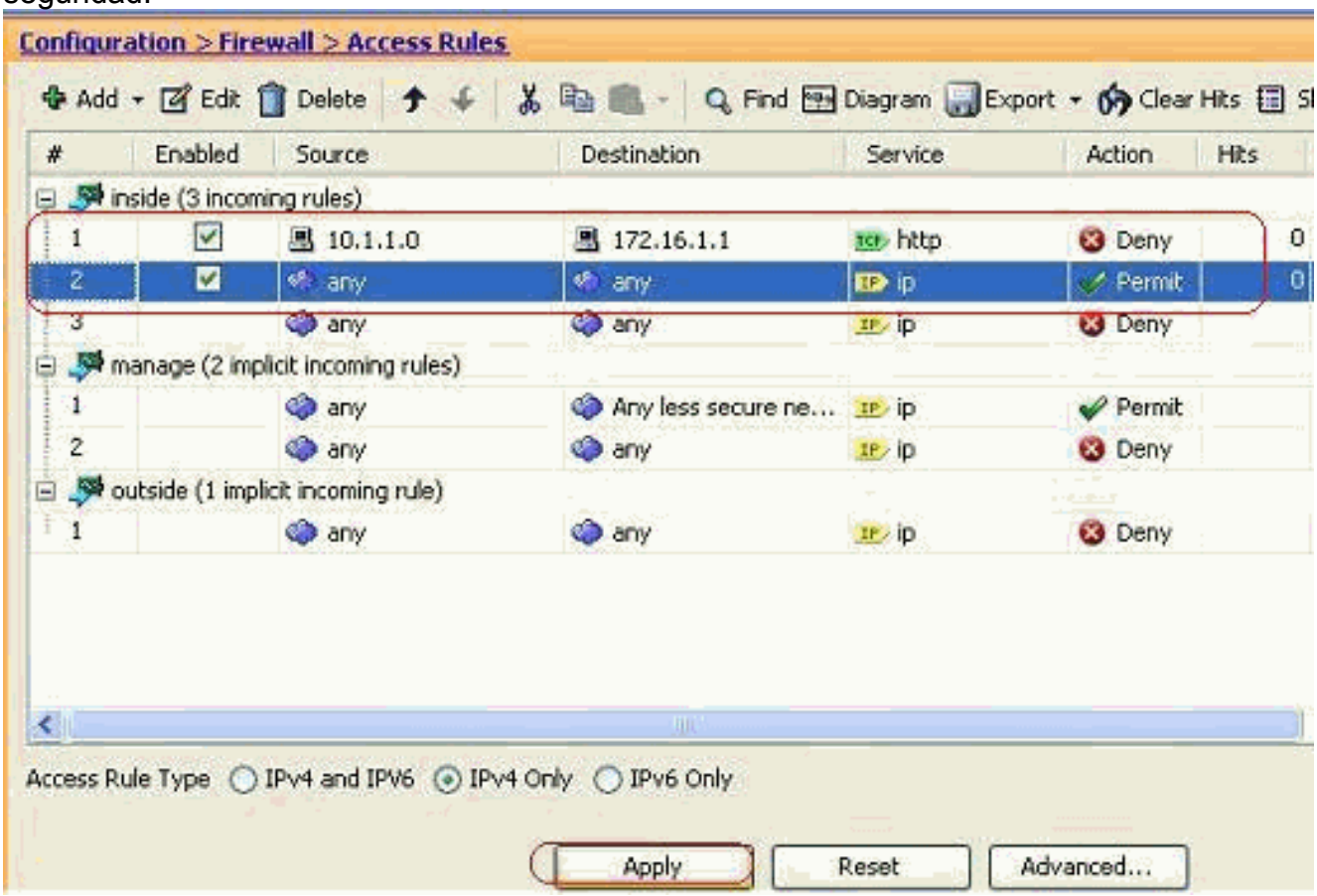
acceso.

6. Permita que el tráfico pase de "cualquiera" a "cualquiera" para evitar la "negación implícita". A continuación, haga clic en **Aceptar** para completar la adición de esta regla de



acceso.

7. La lista de acceso configurada se puede ver en la ficha Access Rules (Reglas de acceso). Haga clic en **Aplicar** para enviar esta configuración al dispositivo de seguridad.



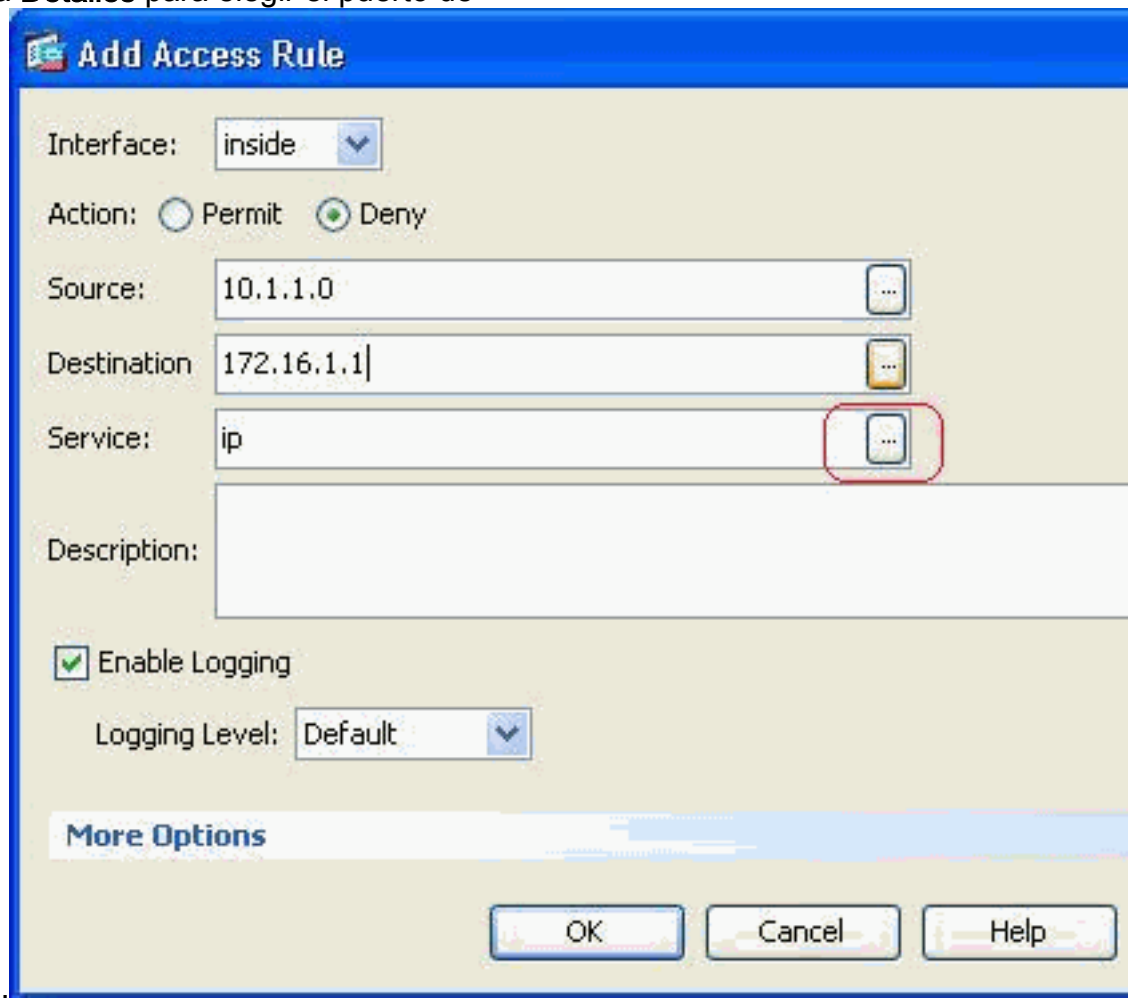
La configuración enviada desde el ASDM da como resultado este conjunto de comandos en

la interfaz de línea de comandos (CLI) del ASA.

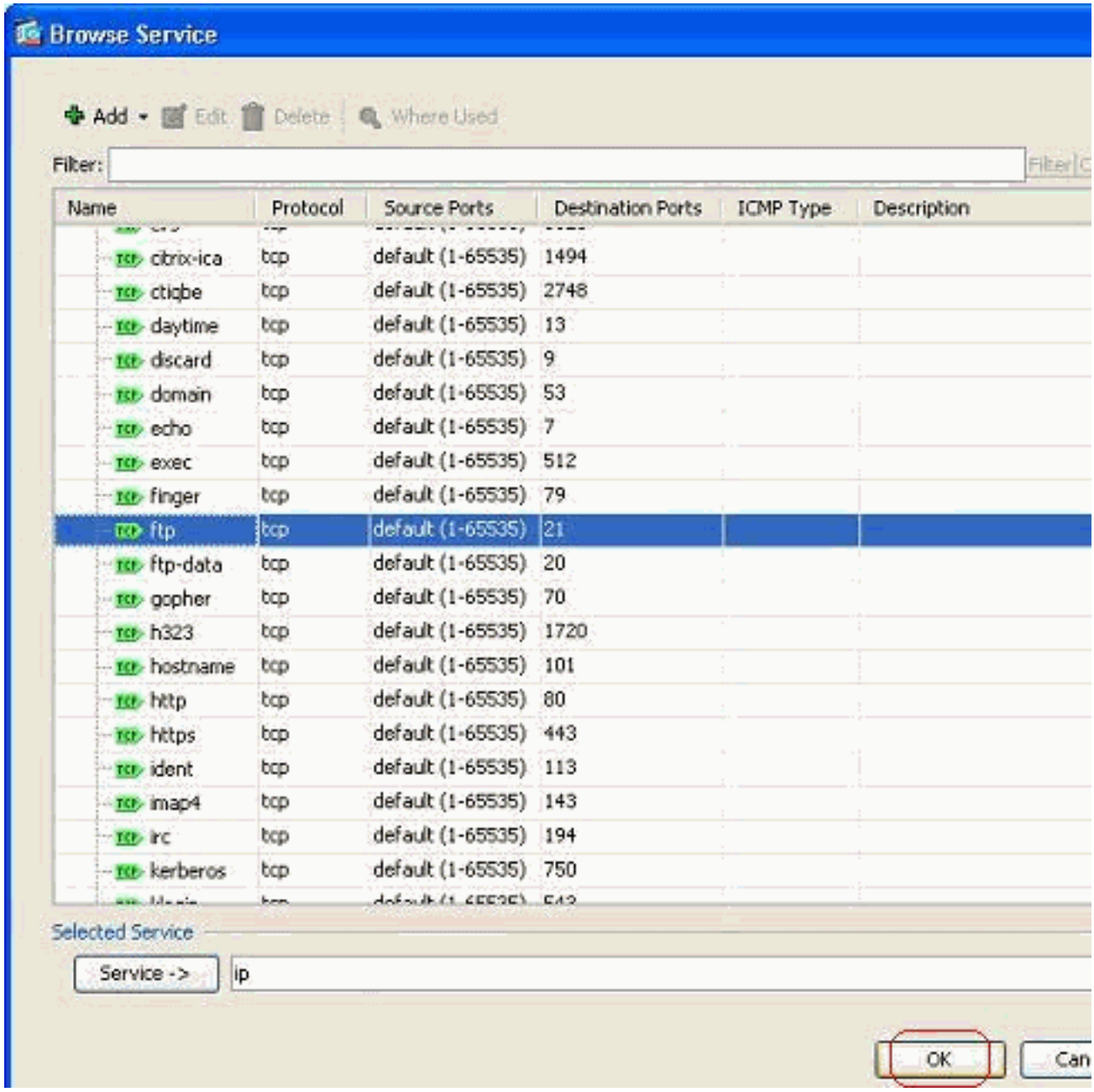
```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

A través de estos pasos, el ejemplo 1 se ha realizado a través de ASDM para bloquear el acceso de la red 10.1.1.0 al servidor web, 172.16.1.1. El ejemplo 2 también se puede lograr de la misma manera para bloquear el acceso de toda la red 10.1.1.0 al servidor FTP, 172.16.1.2. La única diferencia será en el punto de elegir el puerto.**Nota:** Se supone que esta configuración de regla de acceso, por ejemplo, 2, es una configuración nueva.

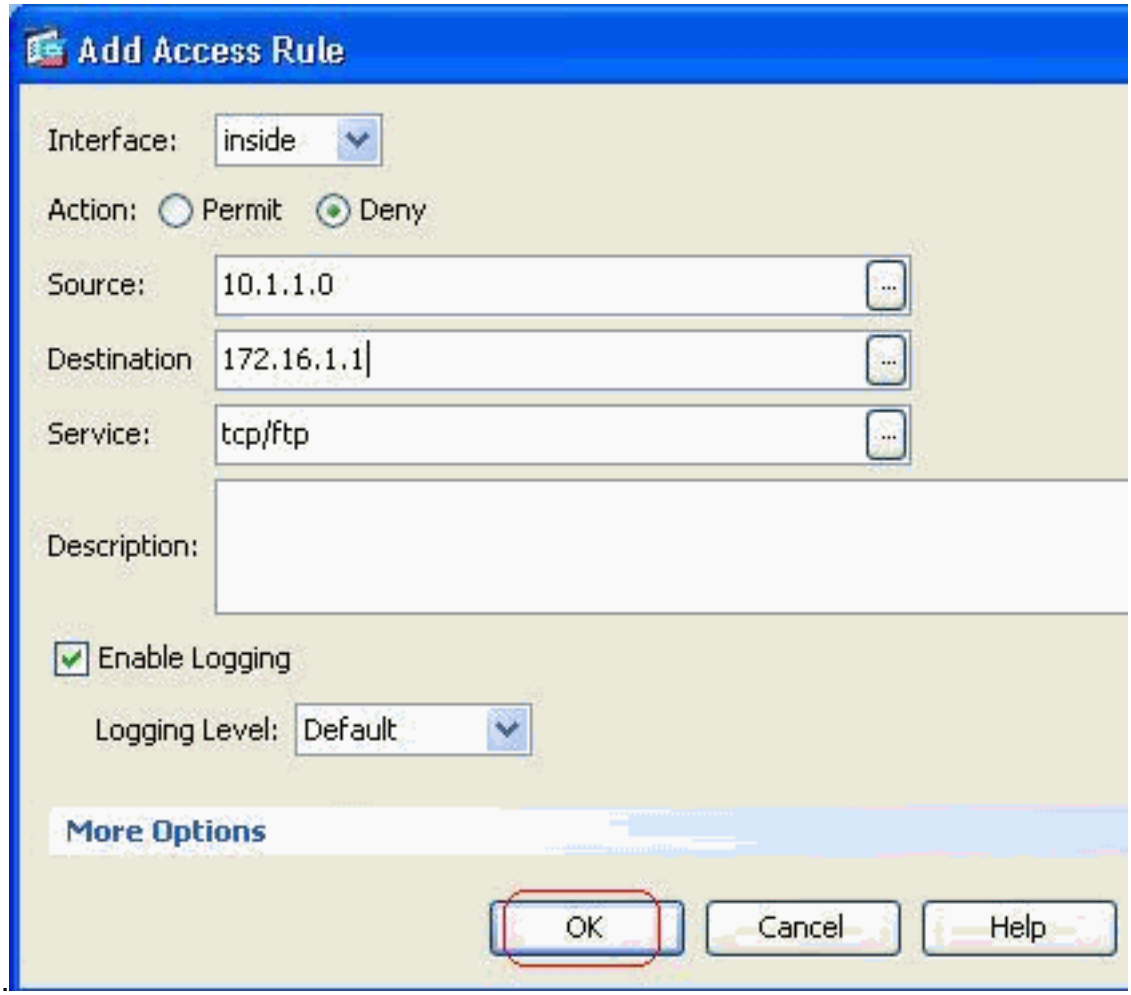
8. Defina la regla de acceso para bloquear el tráfico FTP y, a continuación, haga clic en la pestaña **Detalles** para elegir el puerto de destino.



9. Elija el puerto **ftp** y haga clic en **Aceptar** para volver a la ventana Agregar regla de acceso.

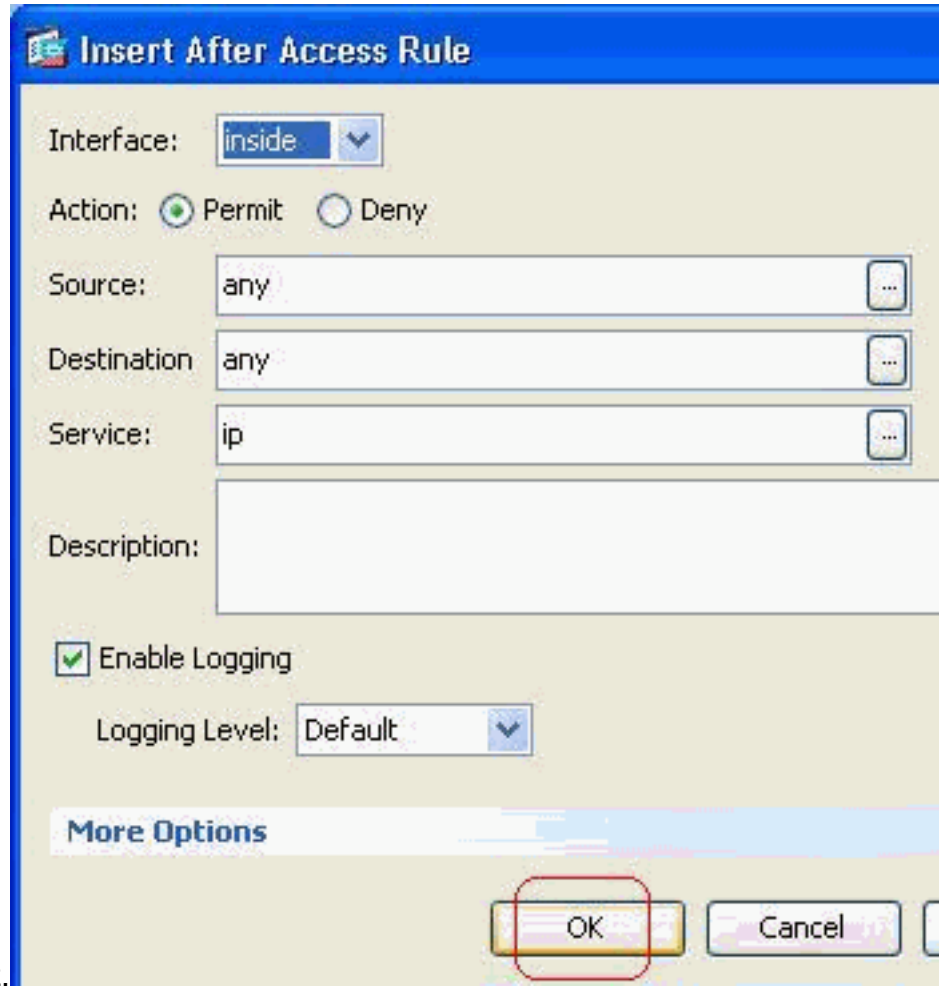


10. Haga clic en **Aceptar** para completar la configuración de la regla de



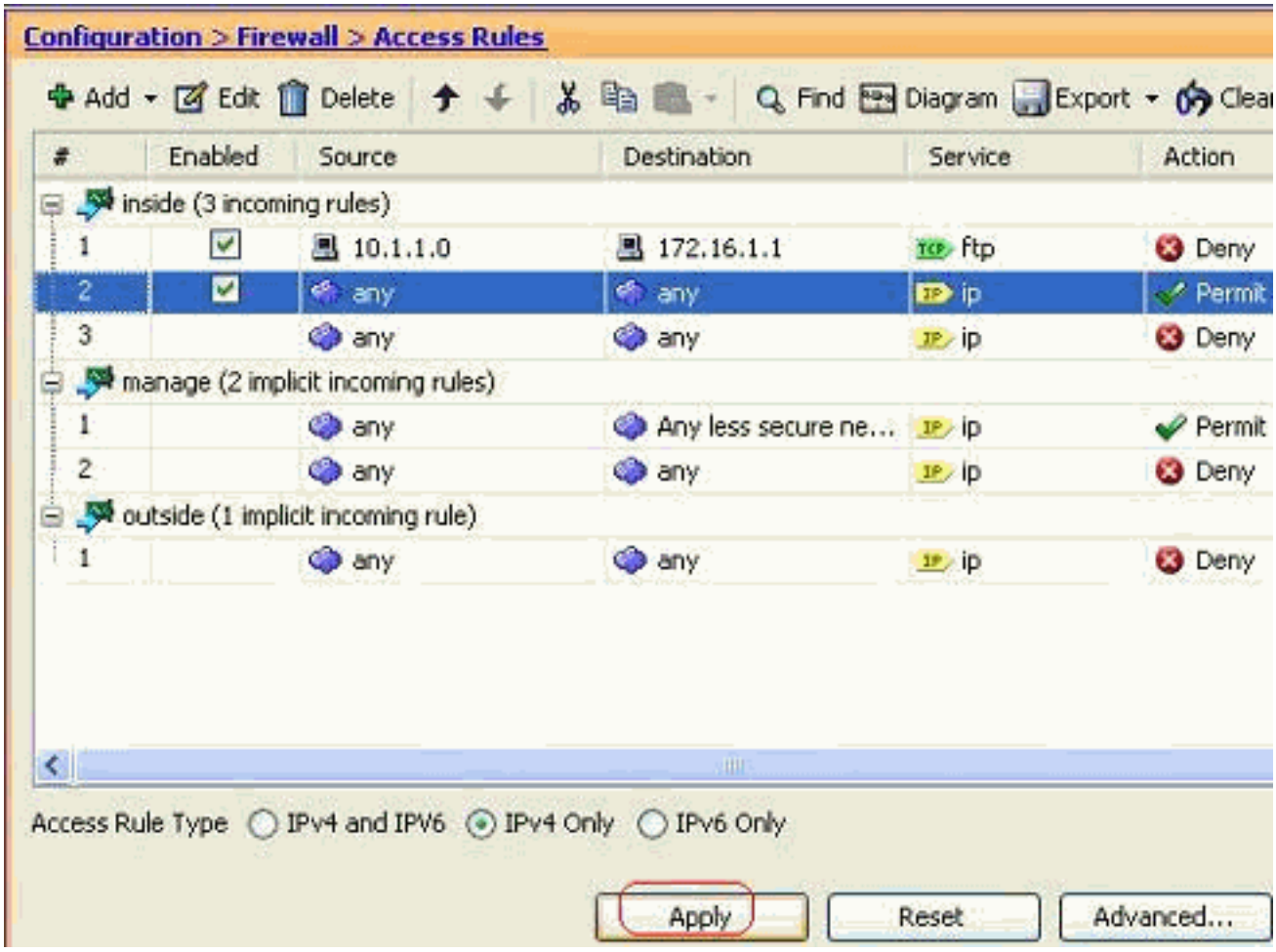
acceso.

11. Agregue otra regla de acceso para permitir cualquier otro tráfico. De lo contrario, la regla Denegar implícita bloqueará todo el tráfico en esta



interfaz.

12. La configuración completa de la lista de acceso es similar a esta en la pestaña Access Rules (Reglas de
acceso).



13. Haga clic en **Aplicar** para enviar la configuración al ASA. La configuración CLI equivalente tiene el siguiente aspecto:

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

Configuración de Apertura de los Puertos

El dispositivo de seguridad no permite ningún tráfico entrante, excepto que esté explícitamente autorizado por una lista de acceso extendido.

Si desea permitir el acceso de un host externo a un host interno, puede aplicar una lista de acceso entrante en la interfaz externa. Debe especificar la dirección traducida del host interno en la lista de acceso porque esta dirección es la que puede utilizarse en la red externa. Siga estos pasos para abrir los puertos desde la zona de seguridad más baja a la zona de seguridad más alta. Por ejemplo, permita el tráfico desde la interfaz externa (zona de seguridad más baja) a la interna (zona de seguridad más alta) o desde la DMZ a la interfaz interna.

1. La NAT estática crea una traducción fija de una dirección real a una dirección asignada. Esta dirección asignada es una dirección que los hosts en Internet pueden utilizar para acceder al servidor de la aplicación de la DMZ sin necesidad de conocer la dirección real del servidor.

   ```
   static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
      access-list access_list_name | interface}
   ```

   Consulte la sección NAT Estática de Referencia de comandos para PIX/ASA para obtener más información.

2. Cree una ACL para permitir el tráfico del puerto específico.

```
access-list
```

3. Vincule la lista de acceso con el comando **access-group** para activarla.

```
access-group
```

Examples:

1. **Apertura del tráfico del puerto SMTP:** Abra el puerto tcp 25 para permitir que los hosts externos (Internet) accedan al servidor de correo ubicado en la red DMZ.El comando **Static** asigna la dirección externa 192.168.5.3 a la dirección DMZ real 172.16.1.3.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. **Apertura del tráfico del puerto HTTPS:** Abra el puerto tcp 443 para permitir que los hosts externos (Internet) accedan al servidor Web (seguro) ubicado en la red DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **Autorización del tráfico de DNS:** Abra el puerto udp 53 para permitir a los hosts externos (Internet) acceder al servidor DNS (seguro) ubicado en la red DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

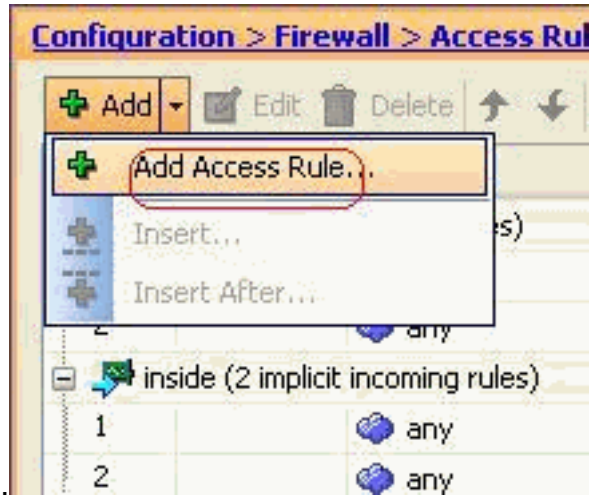
Nota: Consulte Puertos IANA para obtener más información sobre las asignaciones de puerto.

Configuración mediante ASDM

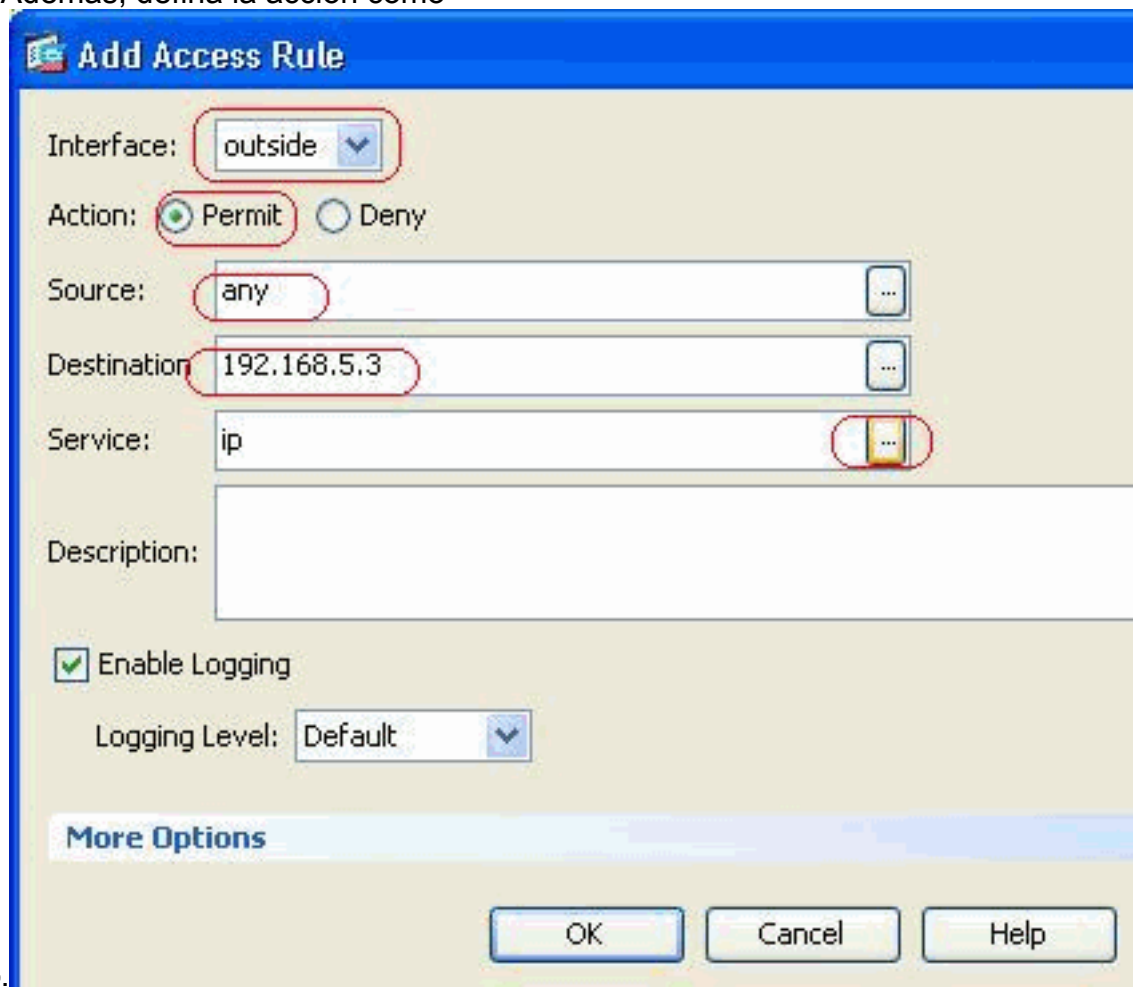
En esta sección se muestra un enfoque paso a paso para llevar a cabo las tareas antes mencionadas mediante ASDM.

1. Cree la regla de acceso para permitir el tráfico smtp al servidor

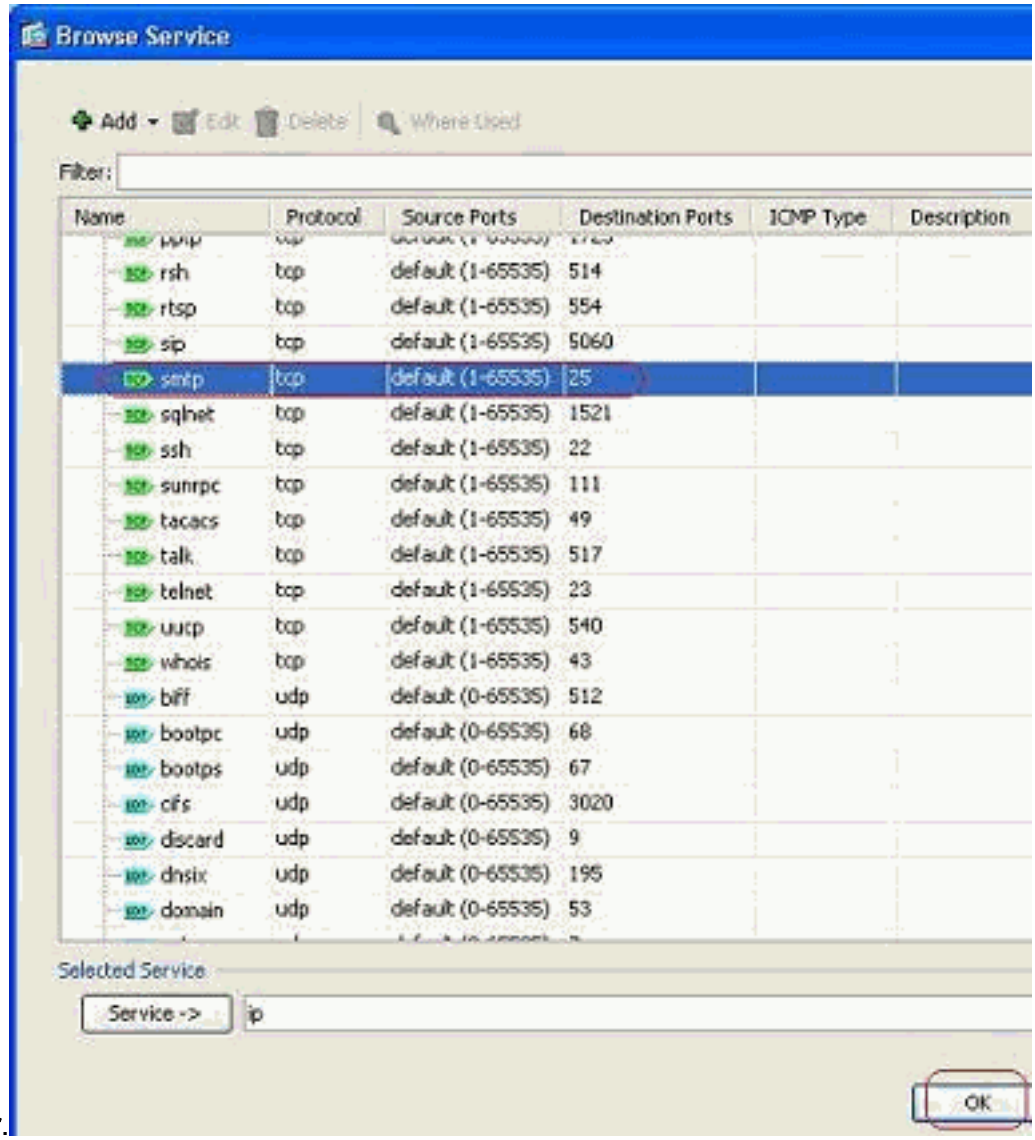
192.168.5.3.



2. Defina el origen y el destino de la regla de acceso y la interfaz con la que esta regla se vincula. Además, defina la acción como **Permiso**.

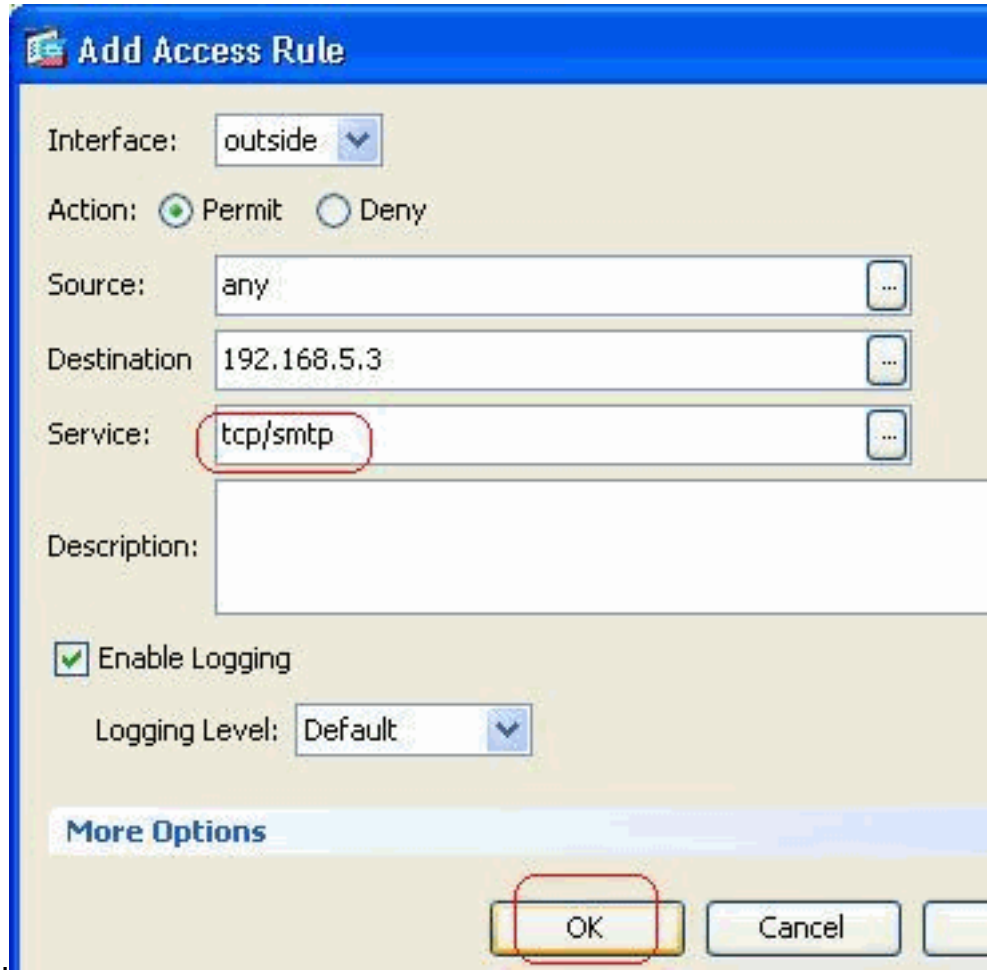


3. Elija **SMTP** como puerto y luego haga clic en



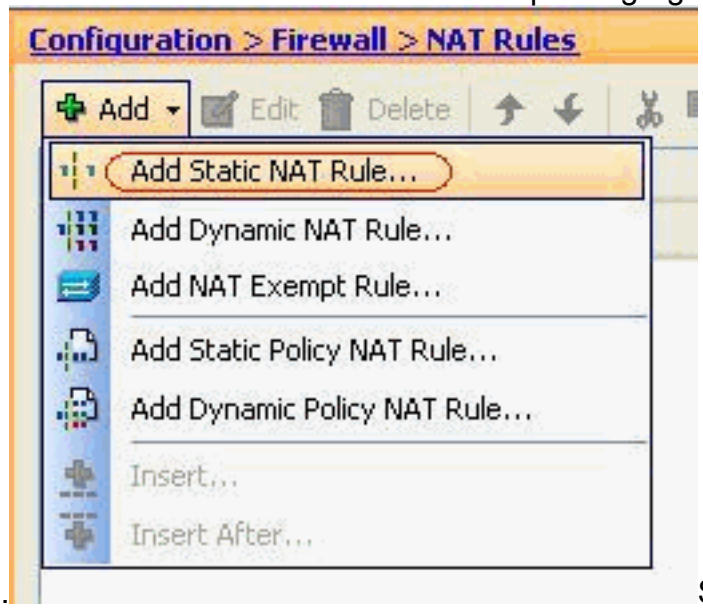
Aceptar.

4. Haga clic en **Aceptar** para completar la configuración de la regla de

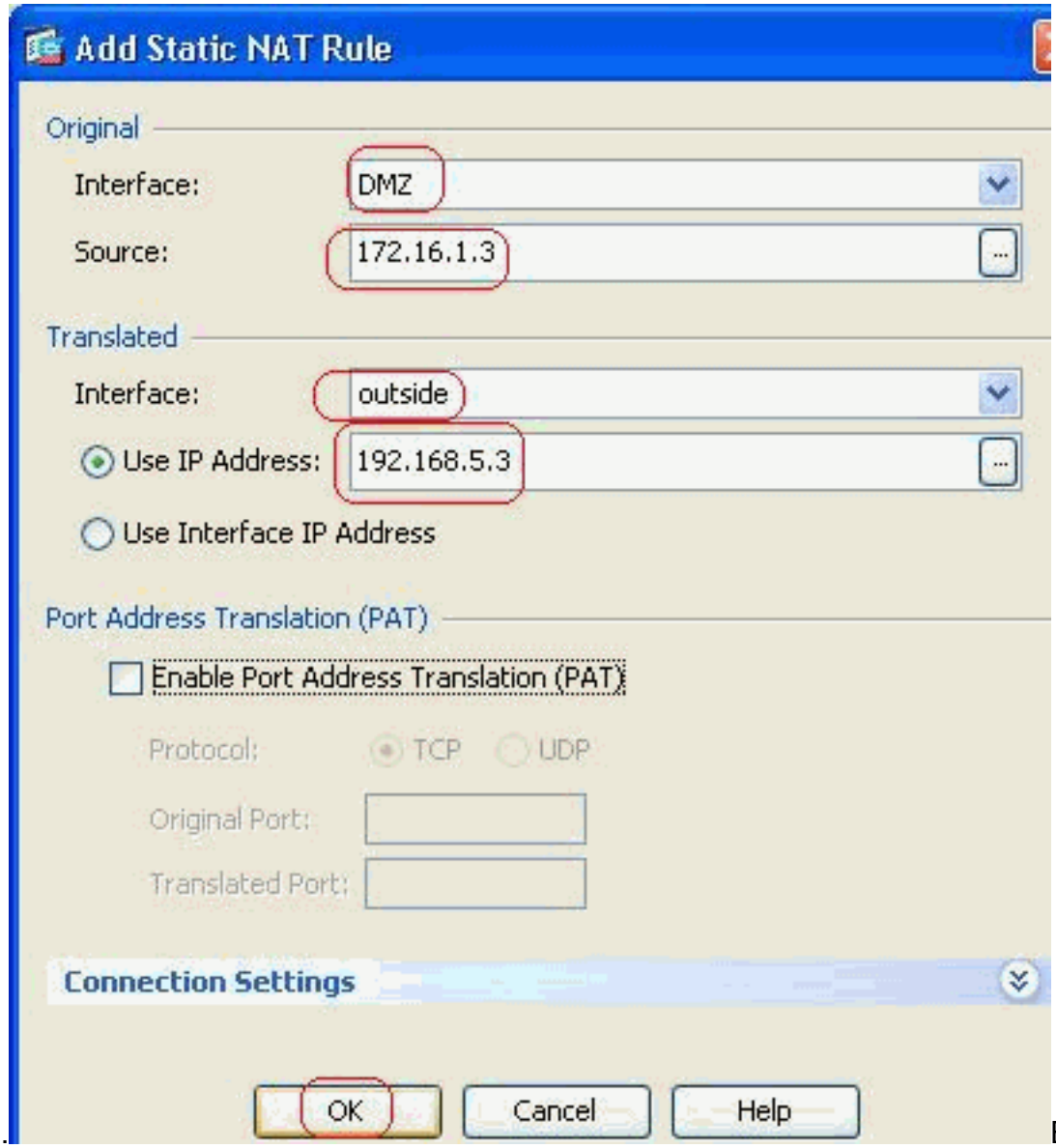


acceso.

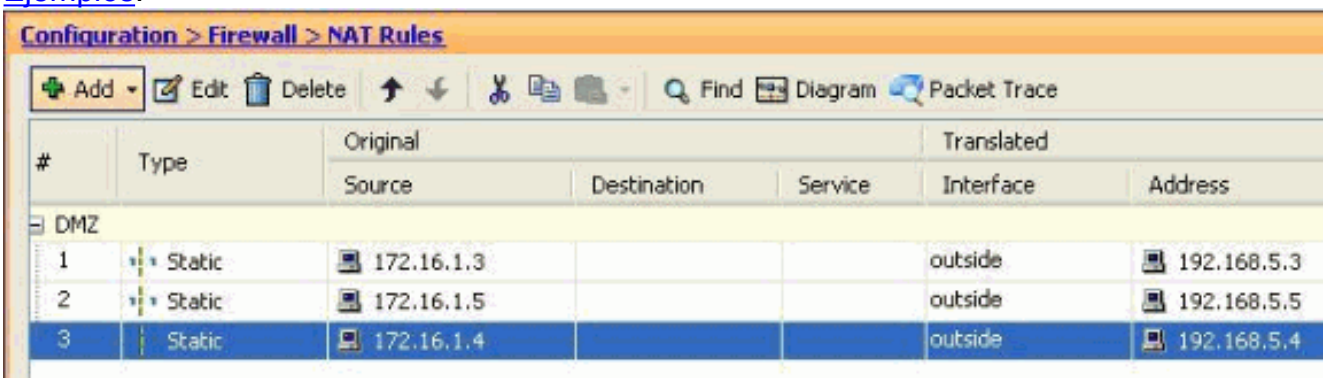
5. Configure la NAT estática para traducir 172.16.1.3 a 192.168.5.3Vaya a **Configuration > Firewall > NAT Rules > Add Static NAT Rule** para agregar una entrada NAT



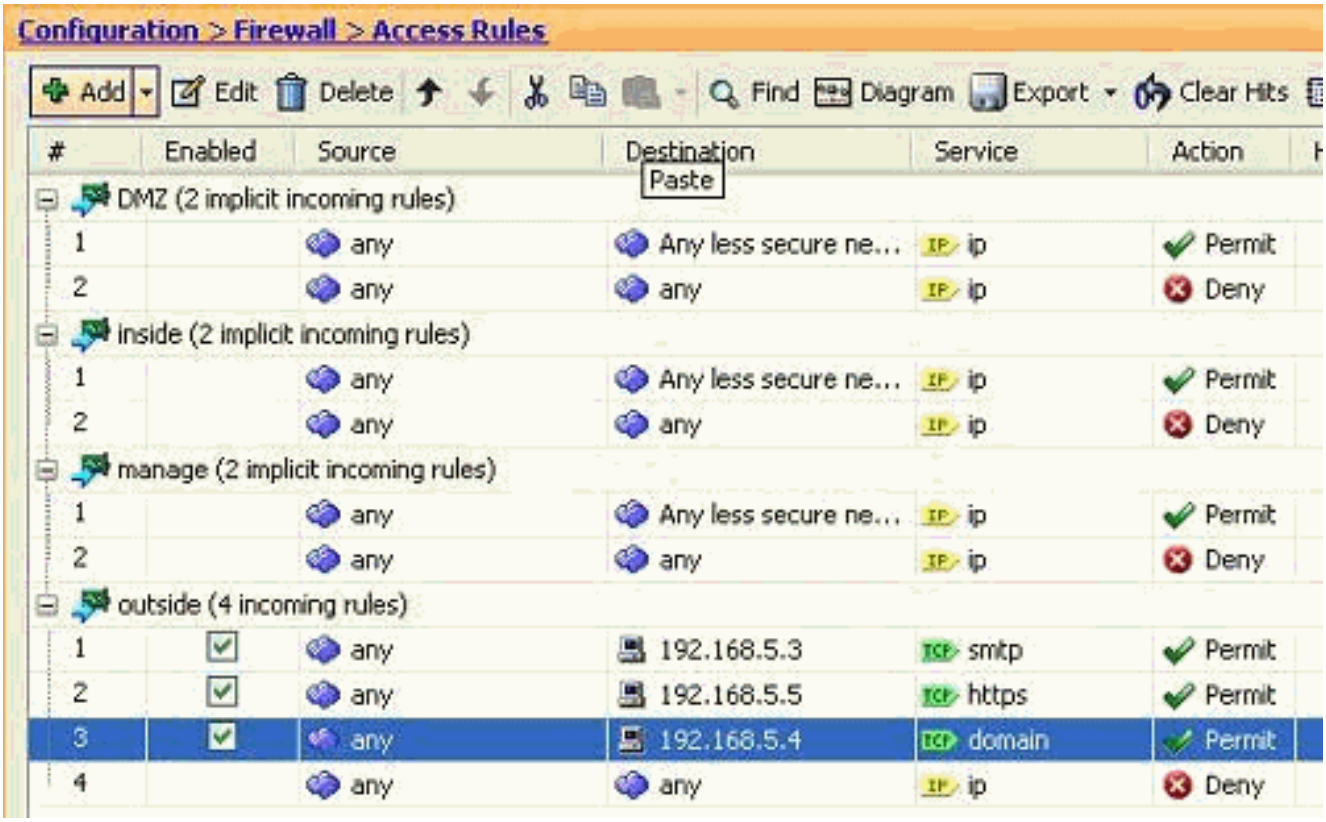
estática. Seleccione el origen original y la dirección IP traducida junto con sus interfaces asociadas y luego haga clic en **Aceptar** para finalizar la configuración de la regla NAT



estática. Esta imagen representa las tres reglas estáticas que se enumeran en la sección Ejemplos:



Esta imagen representa las tres reglas de acceso que se enumeran en la sección Ejemplos:



Verificación

Puede verificar con determinados comandos **show**, como se indica a continuación:

- **show xlate**: muestra la información de la traducción actual
- **show access-list**: muestra los contadores de aciertos para las políticas de acceso
- **show logging**: muestra los registros en el buffer

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

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

Información Relacionada

- PIX/ASA 7.x: Activar/desactivar la comunicación entre interfaces
- PIX 7.0 y Adaptive Security Appliance Port Redirection (Reenvío) con Comandos nat, global, static, conduit y access-list
- Uso de los Comandos NAT, global, static, conduit y access-list y Redirección de Puerto (Reenvío) en PIX
- PIX/ASA 7.x: Ejemplo de Configuración de Habilitar Servicios FTP/TFTP
- PIX/ASA 7.x: Ejemplo de Configuración de Habilitar Servicios VoIP (SIP, MGCP, H323, SCCP)
- PIX/ASA 7.x: Ejemplo de Acceso al Servidor de Correo en la Configuración de DMZ
- Soporte Técnico y Documentación - Cisco Systems