Configuración de Hairpin con Firepower Management Center

Contenido

Introducción

Este documento describe los pasos necesarios para configurar Hairpin correctamente en Firepower Threat Defense (FTD) con Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de administración Firepower (FMC)
- Firepower Threat Defence (FTD)

Componentes Utilizados

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

- Firepower Management Center Virtual 7.2.4.
- Firepower Threat Defense Virtual 7.2.4.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

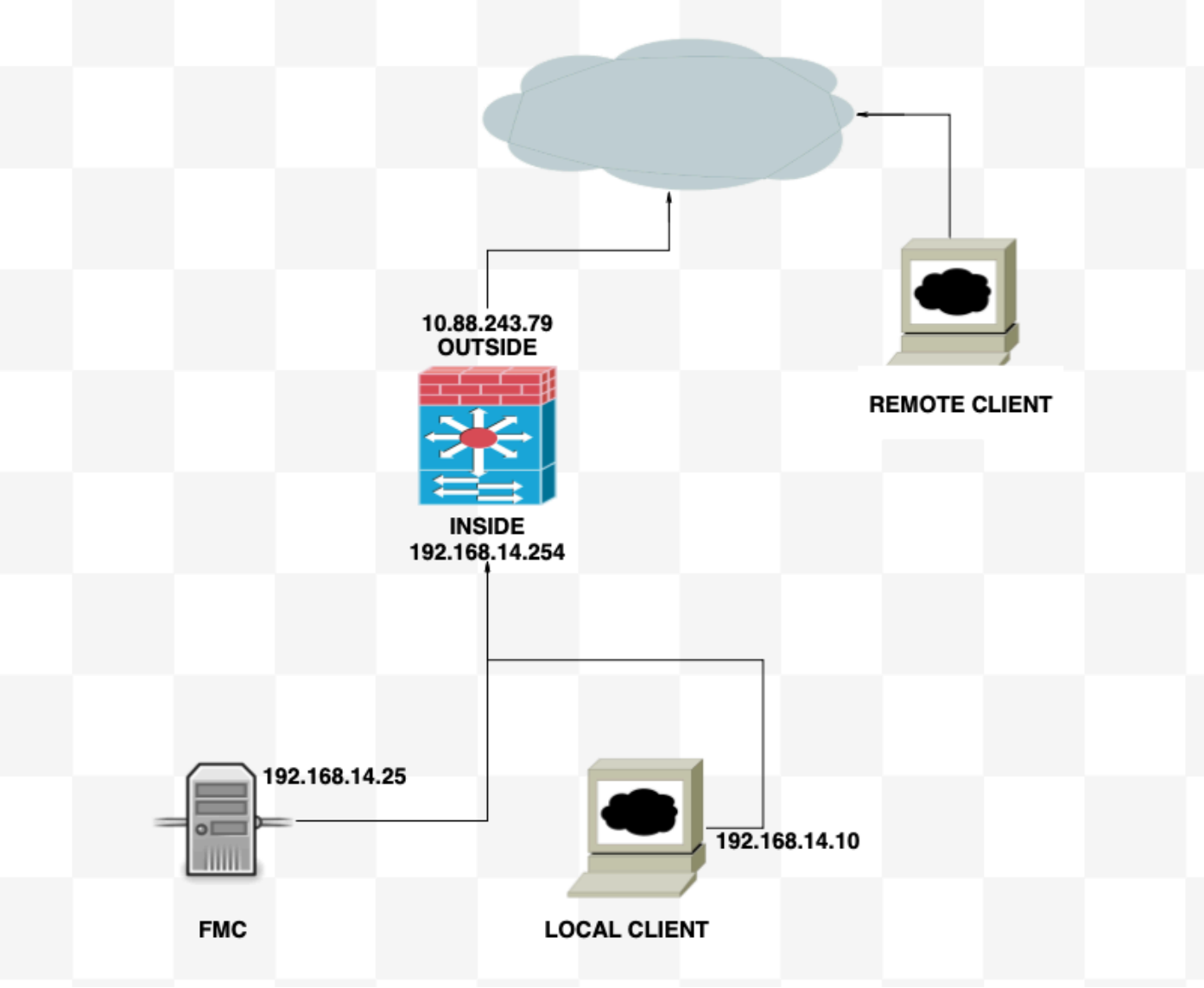
Configurar

El término hairpin se utiliza porque el tráfico del cliente llega al router (o firewall que implementa NAT) y luego se vuelve como una hairpin a la red interna después de la traducción para acceder a la dirección IP privada del servidor.

Esta función es útil para servicios de red, como el alojamiento web dentro de una red local, donde los usuarios de la red local necesitan acceder al servidor interno utilizando la misma URL o dirección IP que los usuarios externos usarían. Garantiza un acceso uniforme a los recursos independientemente de si la solicitud se origina dentro o fuera de la red local.

En este ejemplo, se debe acceder a un FMC a través de la IP de la interfaz externa del FTD

Diagrama

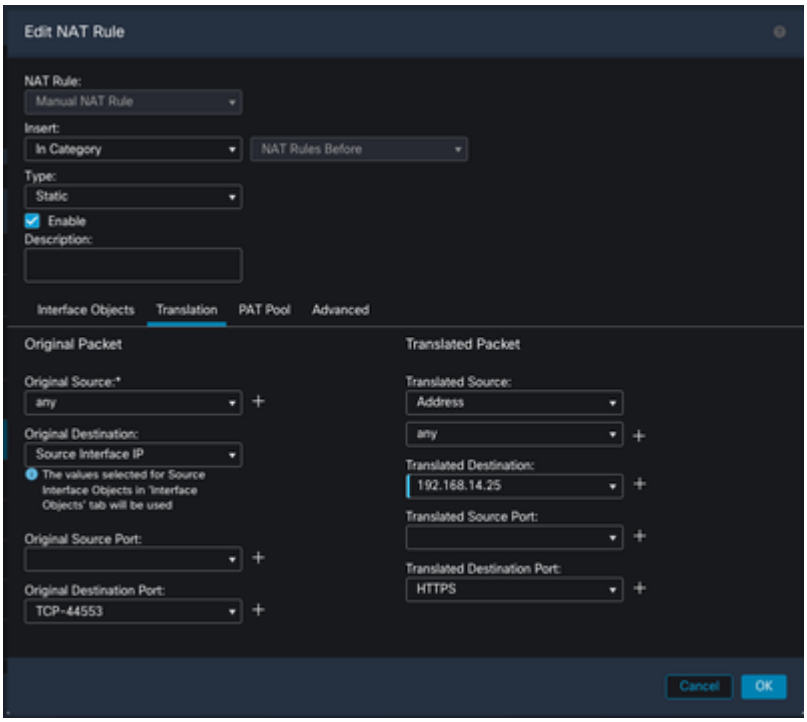


Paso 1. Configuración De Nat Exterior-Interior

Como primer paso, debe configurarse una NAT estática; en este ejemplo, la IP de destino y el puerto de destino se traducen utilizando la IP de la interfaz externa y el puerto de destino es 44553.

En el FMC, vaya a Device > NAT para crear o editar la política existente y, a continuación, haga clic en el cuadro Add Rule.

- Regla NAT: Regla Nat Manual
- Fuente original: cualquiera
- Destino original: IP de interfaz de origen
- Puerto de destino original: 44553
- Destino traducido: 192.168.14.25
- Puerto de destino traducido: 443



Configure la directiva. Navegue hasta Políticas > Control de acceso para crear o editar la política existente, luego haga clic en el cuadro Agregar regla.

Zona de origen: Fuera

Zona de destino: Dentro

Red de origen: cualquiera

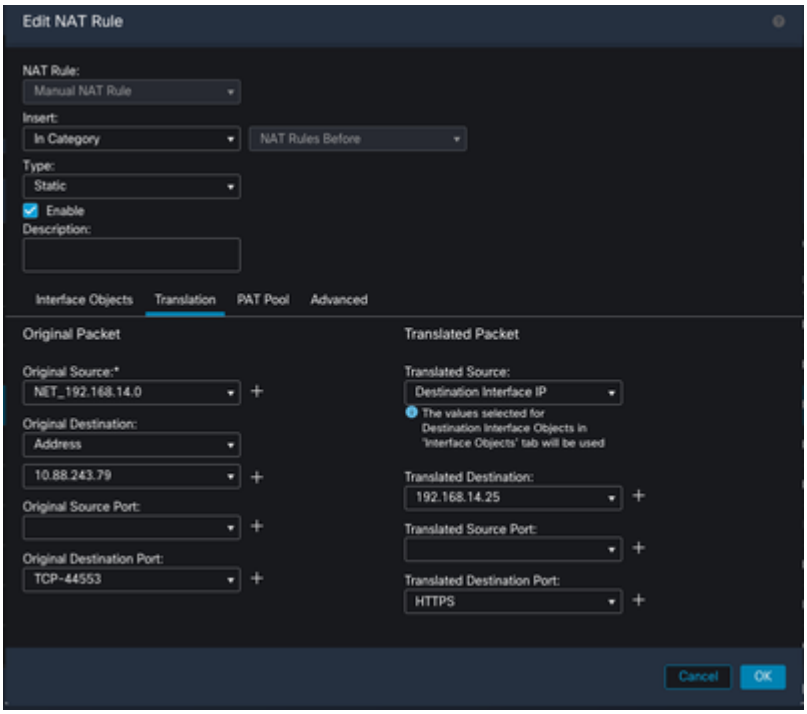
Red de destino: 10.88.243.79

Paso 2. Configure Inside-Inside Nat (Hairpin)

Como segundo paso, debe configurarse una NAT estática de Inside a Inside; en este ejemplo, la IP de destino y el puerto de destino se traducen utilizando un objeto con la IP de la interfaz externa y el puerto de destino es 44553.

En el FMC, vaya a Device > NAT para editar la política existente y, a continuación, haga clic en el cuadro Add Rule.

- Regla NAT: Regla Nat Manual
- Fuente original: 192.168.14.0/24
- Destino original: Address 10.88.243.79
- Puerto de destino original: 44553
- Fuente traducida: IP de interfaz de destino
- Destino traducido: 192.168.14.25
- Puerto de destino traducido: 443



Configure la directiva. Navegue hasta Políticas > Control de acceso para editar la política existente, luego haga clic en el cuadro Agregar regla.

Zona de origen: cualquiera

Zona de destino: cualquiera

Red de origen: 192.168.14.0/24

Red de destino: 10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	*Any*
2	Hairpin	*Any*	*Any*	NET_192.168.14	10.88.243.79

Verificación

Desde el cliente local, haga una telnet con la IP de destino y el puerto de destino:

Si este mensaje de error "telnet cannot connect to remote host: Se agotó el tiempo de espera de la conexión", se produjo un error en algún momento de la configuración.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

Pero si dice Connected, la configuración fue exitosa.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

Troubleshoot

Si tiene problemas con la traducción de direcciones de red (NAT), utilice esta guía paso a paso para solucionar problemas comunes.

Paso 1: Comprobación de la configuración de reglas NAT

- Revisar reglas NAT: Asegúrese de que todas las reglas NAT estén correctamente configuradas en FMC. Compruebe que las direcciones IP de origen y de destino, así como los puertos, son precisos.
- Asignación de interfaz: Confirme que las interfaces de origen y de destino estén asignadas correctamente en la regla NAT. La asignación incorrecta puede hacer que el tráfico no se traduzca o rutee correctamente.
- Prioridad de regla NAT: Verifique que la regla NAT se coloque en la parte superior de

cualquier otra regla que pueda coincidir con el mismo tráfico. Las reglas de FMC se procesan en orden secuencial, por lo que una regla situada en una posición superior tiene prioridad.

Paso 2: Verificación de reglas de control de acceso (ACL)

- Revisar ACL: Verifique las Listas de control de acceso para asegurarse de que sean apropiadas para permitir el tráfico NAT. Las ACL se deben configurar para reconocer las direcciones IP traducidas.
- Orden de reglas: Asegúrese de que la lista de control de acceso está en el orden correcto. Al igual que las reglas NAT, las ACL se procesan de arriba a abajo, y la primera regla que coincide con el tráfico es la que se aplica.
- Permisos de tráfico: Verifique que exista una lista de control de acceso adecuada para permitir el tráfico de la red interna al destino traducido. Si falta una regla o ésta no está configurada correctamente, es posible que se bloquee el tráfico deseado.

Paso 3: Diagnósticos adicionales

- Utilice las herramientas de diagnóstico: Utilice las herramientas de diagnóstico disponibles en FMC para supervisar y depurar el tráfico que pasa a través del dispositivo. Esto incluye la visualización de registros en tiempo real y eventos de conexión.
- Reiniciar conexiones: En algunos casos, las conexiones existentes no pueden reconocer los cambios realizados en las reglas NAT o ACL hasta que se reinician. Considere la posibilidad de borrar las conexiones existentes para forzar la aplicación de nuevas reglas.

Desde LINA:

```
<#root>
firepower#
 clear xlate
```

- Verificar traducción: Utilice comandos como show xlate y show nat en la línea de comandos si está trabajando con dispositivos FTD para verificar que las traducciones NAT se realizan según lo esperado.

Desde LINA:

```
<#root>
firepower#
 show nat
```

<#root>

firepower#

 show xlate

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).