Configuración de horquilla en ASA

Contenido

Introducción

Este documento describe los pasos necesarios para configurar Hairpin correctamente en un Cisco Adaptive Security Appliance (ASA)

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Configuración NAT en ASA
- Configuración de ACL en ASA

Componentes Utilizados

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

- Software Cisco Adaptive Security Appliance Versión 9.18(4)22

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

La Traducción de direcciones de red (NAT) de horquilla, también conocida como bucle invertido NAT o reflexión NAT, es una técnica utilizada en el routing de red por medio de la cual un dispositivo de una red privada puede acceder a otro dispositivo de la misma red privada a través de una dirección IP pública.

Se utiliza cuando un servidor está alojado detrás de un router y desea habilitar dispositivos en la misma red local que el servidor para acceder a él mediante la dirección IP pública (la asignada al router por el proveedor de servicios de Internet) tal y como lo haría un dispositivo externo.

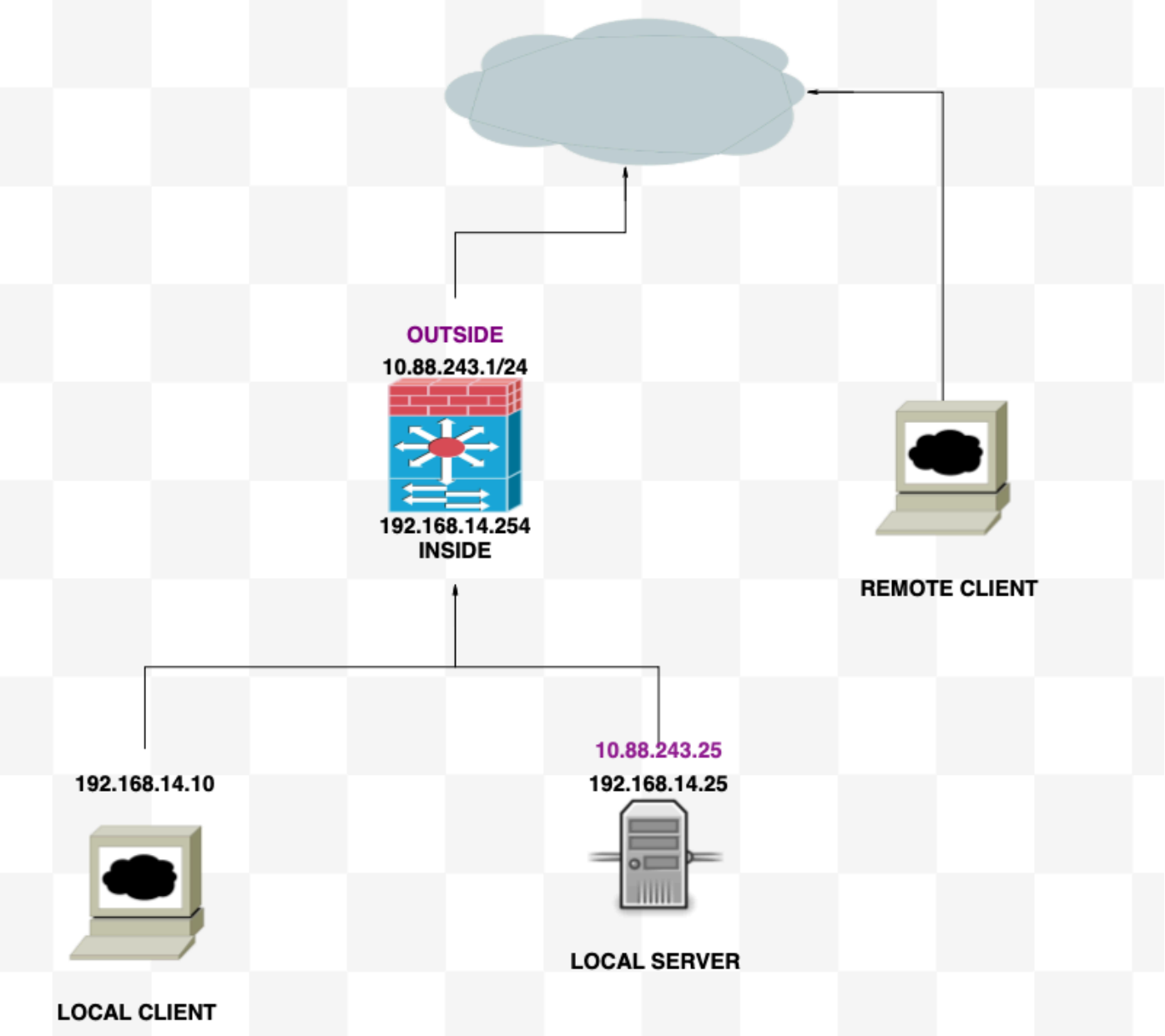
El término "hairpin" se utiliza porque el tráfico del cliente llega al router (o firewall que implementa NAT) y luego se "devuelve" como una horquilla a la red interna después de la traducción para acceder a la dirección IP privada del servidor.

Por ejemplo, tiene un servidor Web en la red local con una dirección IP privada. Desea tener acceso a este servidor mediante su dirección IP pública o un nombre de dominio que se resuelva en la dirección IP pública, incluso cuando se encuentra en la misma red local.

Sin la NAT Hairpin, el router no entendería esta solicitud porque espera que las solicitudes de la dirección IP pública provengan de fuera de la red.

La NAT de horquilla resuelve este problema al permitir que el router reconozca que, aunque la solicitud se realiza a una IP pública, debe enrutarse a un dispositivo de la red local.

Diagrama de la red



Configuraciones

Paso 1. Crear los objetos

- Red interna:192.168.14.10
- Servidor web: 192.168.14.25
- Servidor web público: 10.88.243.25
- Puerto: 80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

Paso 2. Creación de la NAT

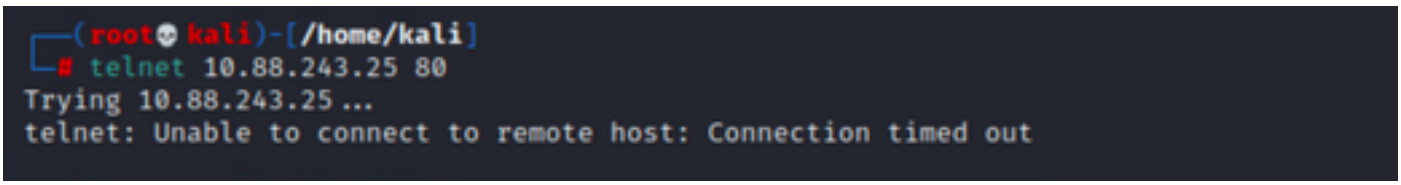
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

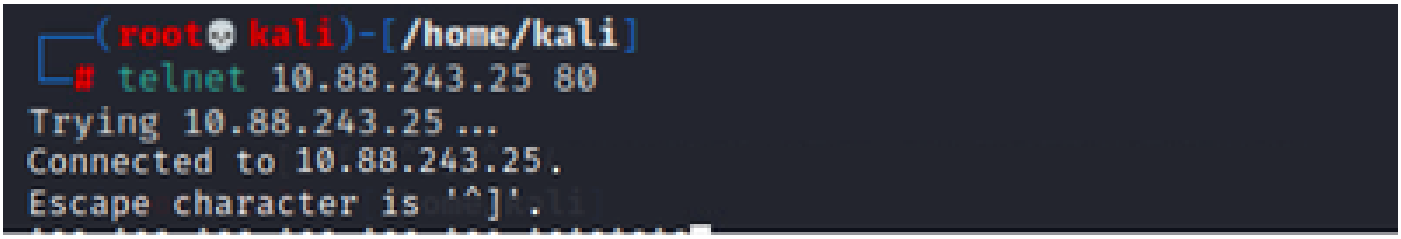
Verificación

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

Si aparece este mensaje "telnet cannot connect to remote host: Connection timed out", algo salió mal en algún momento de la configuración.



Pero si dice "Conectado", ¡funciona!



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 configuradas correctamente. 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 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 tenga una prioridad mayor que cualquier otra regla que posiblemente coincida con el mismo tráfico. Las reglas se procesan en orden secuencial, por lo que una regla situada en una posición superior tiene prioridad.

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

- Revise las 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 las 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 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 reconocen 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.

<#root>

```
ciscoasa(config)#
```

```
 clear xlate
```

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

<#root>

ciscoasa(config)#

show xlate

<#root>

ciscoasa(config)#

show nat

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).