ASA 8.4(4): Configuración NAT de identidad no permitida

Contenido

Introducción

Los dispositivos de seguridad adaptable (ASA) que ejecutan 8.4(4) o superior pueden rechazar ciertas configuraciones de NAT y mostrar un mensaje de error similar a este:

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

Este problema también puede aparecer cuando actualiza su ASA a 8.4(4) o superior desde una versión anterior. Es posible que observe que algunos comandos NAT ya no están presentes en la configuración en ejecución del ASA. En estos casos, debe observar los mensajes de la consola impresos para ver si hay mensajes presentes en el formato anterior.

Otro efecto que puede notar es que el tráfico de ciertas subredes detrás del ASA pueden dejar de pasar a través de los túneles VPN (Red privada virtual) que terminan en el ASA. Este documento describe cómo resolver estos problemas.

Antes de comenzar

Requirements

Estas condiciones deben cumplirse para encontrar este problema:

- ASA que ejecuta la versión 8.4(4) o superior, o que se actualiza a la versión 8.4(4) o superior a partir de una versión anterior.
- ASA configurado con una dirección IP en espera en al menos una de sus interfaces.
- Una NAT se configura con la interfaz anterior como la interfaz asignada.

Componentes Utilizados

La información de este documento se basa en esta versión de hardware y software:

- ASA que ejecutan 8.4(4) o superior

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Problema

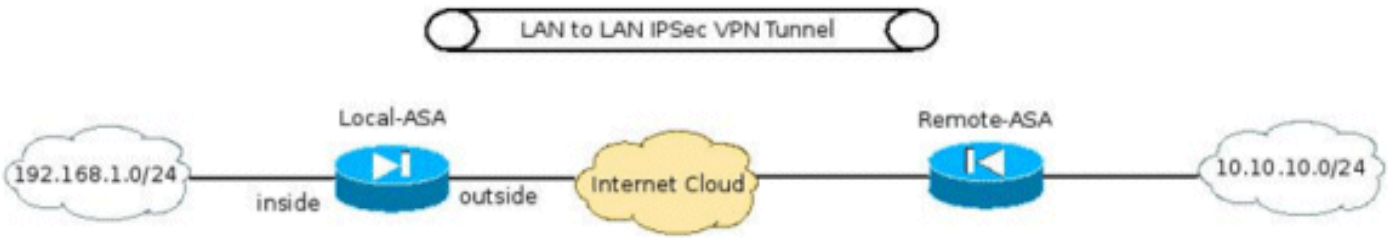
Como sugiere el mensaje de error, si el rango de direcciones mapeadas en una sentencia NAT estática incluye la dirección IP "standby" asignada a la interfaz asignada, se rechaza el comando NAT. Este comportamiento siempre ha existido para la redirección de puertos estáticos, pero se ha introducido para las sentencias NAT estáticas uno a uno, así como con la versión 8.4(4) como solución para el ID de bug de Cisco CSCtw82147 (sólo clientes registrados) .

Este error se ha producido porque antes de 8.4(4) el ASA permitía a los usuarios configurar la dirección asignada en una configuración NAT estática para que sea la misma que la dirección IP standby asignada a la interfaz asignada. Por ejemplo, observe este fragmento de configuración de un ASA:

```
ciscoasa(config)# show run int e0/0
!
interface Ethernet0/0
 nameif vm
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config)# show run nat
!
object network obj-10.76.76.160
 nat (tftp,vm) static 192.168.1.2
```

Aunque se acepte el comando, esta configuración NAT nunca funcionará por diseño. Como resultado, a partir de 8.4(4), el ASA no permite que se configure una regla de NAT en primer lugar.

Esto ha dado lugar a otro problema imprevisto. Por ejemplo, considere la situación en la que el usuario tiene un túnel VPN que termina en el ASA y desea permitir que la subred "interna" pueda comunicarse con la subred VPN remota.



Entre otros comandos necesarios para configurar el túnel VPN, una de las configuraciones más importantes es asegurarse de que el tráfico entre las subredes VPN no se convierta en NAT. Esto se implementa con 8.3 y superiores usando un comando Manual/Dos veces NAT de este formato:

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

Cuando este ASA se actualiza a 8.4(4) o superior, este comando NAT no estará presente en la configuración en ejecución del ASA y este error se imprimirá en la consola del ASA:

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

Como resultado, el tráfico entre las subredes 192.168.1.0/24 y 10.10.10.0/24 ya no fluirá a través del túnel VPN.

Solución

Hay dos soluciones alternativas posibles para esta condición:

- Haga que el comando NAT sea lo más específico posible antes de actualizar a 8.4(4) para que la interfaz asignada no sea "ninguna". Por ejemplo, el comando NAT anterior se puede cambiar a la interfaz a través de la cual se puede alcanzar la subred VPN remota (denominada "externa" en el escenario anterior):
  ```
  nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination
     static obj-10.10.10.0 obj-10.10.10.0
  ```
- Si la solución alternativa anterior no es posible, complete estos pasos:Cuando ASA esté ejecutando 8.4(4) o superior, elimine la dirección IP en espera asignada a la interfaz.Aplique el comando NAT.Vuelva a aplicar la dirección IP en espera en la interfaz.Por ejemplo:
  ```
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
  ciscoasa(config-if)# exit
  ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0
     obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  ```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems