ASA 8.4(4): Cierta configuración del NAT de la identidad rechazada

Contenido

Introducción

El funcionamiento de los dispositivos de seguridad (ASA) 8.4(4) o más alto adaptante puede rechazar ciertas configuraciones del NAT y visualizar un mensaje de error similar a esto:

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

Este problema puede también aparecer cuando usted actualiza su ASA a 8.4(4) o más alto de una versión anterior. Usted puede notar que algunos comandos nat están no más presentes en los ejecutar-config del ASA. En estos casos, usted debe mirar los mensajes de la consola impresos para ver si hay mensajes presentes en el formato antedicho.

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

Requisitos

Estas condiciones necesitan ser cumplidas para encontrar este problema:

- Versión 8.4(4) o posterior corriente ASA, o actualizado a la versión 8.4(4) o posterior de una versión anterior.
- ASA configurado con un IP Address en Standby en por lo menos una de sus interfaces.
- Un NAT se configura con la interfaz antedicha como la interfaz asociada.

Componentes Utilizados

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

- Funcionamiento ASA 8.4(4) o más alto

Convenciones

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

Problema

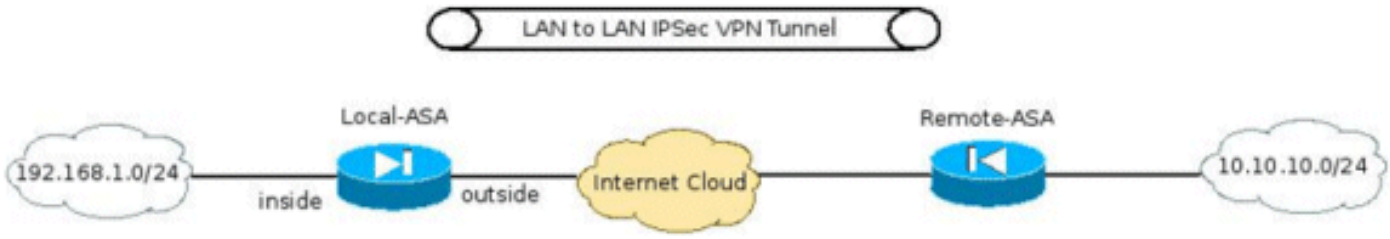
Mientras que el mensaje de error sugiere, si el intervalo de direcciones asociado en una declaración NAT estática incluye la dirección IP “espera” asignada a la interfaz asociada, rechazan al comando nat. Este comportamiento ha existido siempre para el cambio de dirección del puerto estático, pero se ha introducido para las sentencias NAT unas por estáticas también con la versión 8.4(4) como arreglo para el Id. de bug Cisco CSCtw82147 (clientes registrados solamente).

Este bug fue clasifiado porque antes 8.4(4) del ASA permitió que los usuarios configuraran el direccionamiento asociado en una configuración NAT estática para ser lo mismo que el IP Address en Standby asignó a la interfaz asociada. Por ejemplo, mire este snippet de la 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 valida el comando, esta configuración del NAT nunca trabajará por el diseño. Como consecuencia, empezando por 8.4(4), el ASA no permite que tal regla NAT sea configurada en el primer lugar.

Esto ha dado lugar a otro problema imprevisto. Por ejemplo, considere el escenario donde el usuario tiene un túnel VPN que termina en el ASA y quiere permitir que la subred del “interior” pueda hablar con la subred VPN remota.



Entre otros comandos required para configurar el túnel VPN, una de las configuraciones más importantes es asegurarse de que el tráfico entre las subredes VPN no consigue el NATed. Esto se implementa con 8.3 y sobre usar un manual/dos veces un comando 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 más alto, este comando nat no estará presente en los ejecutar-config ASA y este error será impreso en la consola ASA:

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

Como consecuencia, el tráfico entre las subredes 192.168.1.0/24 y 10.10.10.0/24 atravesará no más el túnel VPN.

Solución

Hay dos soluciones alternativas posibles para esta condición:

- Haga el comando nat tan específico como sea posible antes de actualizar a 8.4(4) así que la interfaz asociada no es “ninguna”. Por ejemplo, el comando nat antedicho puede ser cambiado a la interfaz a través de la cual la subred VPN remota es accesible (nombrado “exterior” en el escenario antedicho):`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 antedicha no es posible, complete estos pasos:Cuando el ASA está ejecutando 8.4(4) o más alto, quite el IP Address en Standby asignado a la interfaz.Aplique el comando nat.Reaplique el IP Address en Standby 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