Autenticación ASA a un ASA espera cuando el dispositivo AAA está situado con un ejemplo de configuración L2L

Contenido

Introducción

Este documento describe cómo trabajar alrededor de un escenario donde no está capaz el administrador de autenticar a Cisco un dispositivo de seguridad adaptante espera (ASA) en un par de fallas debido al hecho de que el servidor del Authentication, Authorization, and Accounting (AAA) está situado en un lugar remoto con un LAN a LAN (L2L).

Aunque el retraso a la autenticación local pueda ser utilizado, la autenticación de RADIUS para ambas unidades se prefiere.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conmutación por falla ASA
- VPN
- [traducción de Dirección de Red (NAT)](#)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

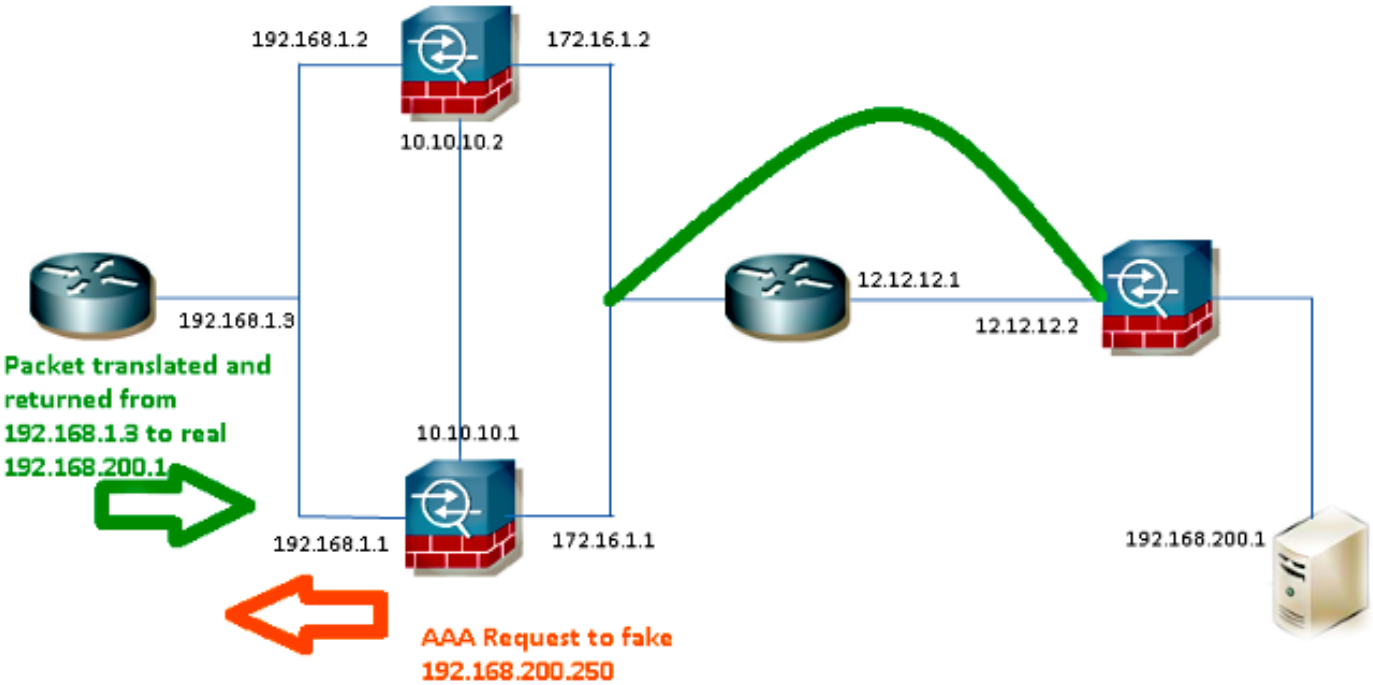
Configurar

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

El servidor de RADIUS está situado en el exterior del par de fallas y es accesible a través de un túnel L2L a 12.12.12.2. Esto es qué causa el probem porque los intentos espera ASA para alcanzarlo a través de su propia interfaz exterior pero allí no son ningún túnel empleado él en este momento; para que trabaje, debe enviar la petición a la interfaz activa así que el paquete puede fluir a través del VPN pero las rutas se replican de la unidad activa.

Una opción es utilizar una dirección IP falsa para el servidor de RADIUS en los ASA y señalarla ante el interior. Por lo tanto, el IP Address de origen y de destino de este paquete se puede traducir en un dispositivo interno.



Router1

```
interface FastEthernet0/0
ip address 192.168.1.3 255.255.255.0
no ip redirects
no ip unreachables
ip nat enable
duplex auto
speed auto
```

```
ip access-list extended NAT
permit ip 192.168.1.0 0.0.0.255 host 192.168.200.250

ip nat source list NAT interface FastEthernet0/0 overload
ip nat source static 192.168.200.1 192.168.200.250

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA

```
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 192.168.200.250
timeout 3
key *****
authentication-port 1812
accounting-port 1813

aaa authentication serial console LOCAL
aaa authentication ssh console RADIUS LOCAL
aaa authentication telnet console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
aaa authentication enable console RADIUS LOCAL

route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
route inside 192.168.200.250 255.255.255.255 192.168.1.3 1
```

> Nota: Utilizaron a la **dirección IP 192.168.200.250** en el ejemplo, pero cualquier trabajo inusitado de la dirección IP.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Router

```
Router#   show ip nat nvi tra
Pro Source global Source local Destin local Destin global
udp 192.168.1.3:1025 192.168.1.1:1025 192.168.200.250:1812 192.168.200.1:1812
--- 192.168.200.1 192.168.2.1 --- ---
--- 192.168.200.250 192.168.200.1 --- ---
```

Troubleshooting

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