Ejemplo de Configuración de Autenticación ASA a un ASA en Espera cuando el Dispositivo AAA se Encuentra a Través de un L2L

Contenido

Introducción

Este documento describe cómo trabajar en un escenario en el que el administrador no puede autenticarse en un Cisco Adaptive Security Appliance (ASA) en espera en un par de conmutación por fallas debido al hecho de que el servidor de autenticación, autorización y contabilidad (AAA) se encuentra en una ubicación remota a través de una LAN a LAN (L2L).

Aunque se puede utilizar el repliegue a la autenticación LOCAL, se prefiere la autenticación RADIUS para ambas unidades.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Failover 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.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

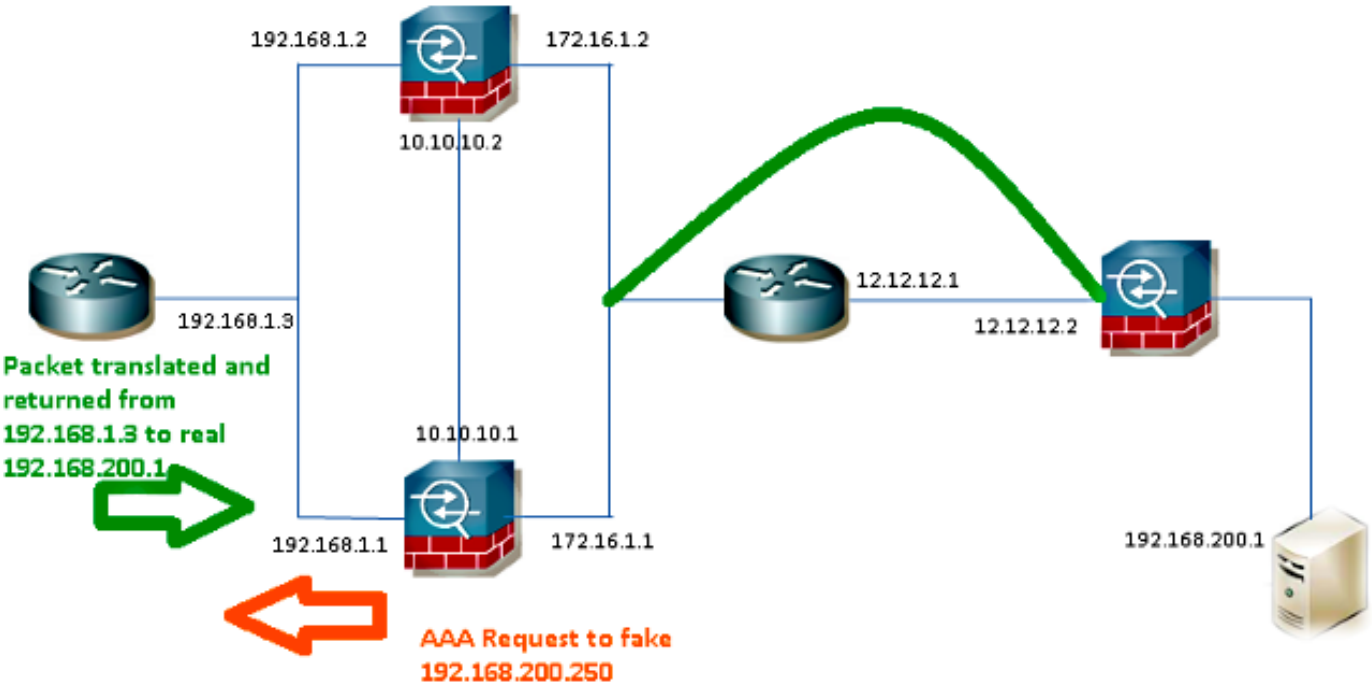
Configurar

> **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 RADIUS se encuentra en el exterior del par de conmutación por fallas y se puede alcanzar a través de un túnel L2L a 12.12.12.2. Esto es lo que causa el problema porque el ASA en espera intenta alcanzarlo a través de su propia interfaz externa pero no hay ningún túnel construido en él en este punto; para que funcione, debe enviar la solicitud a la interfaz activa para que el paquete pueda fluir a través de la VPN pero las rutas se replican desde la unidad activa.

Una opción es utilizar una dirección IP falsa para el servidor RADIUS en los ASA y señalarla al interior. Por lo tanto, la dirección IP de origen y 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:** La dirección IP **192.168.200.250** se utilizó en el ejemplo, pero cualquier dirección IP no utilizada funciona.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de 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 --- ---
```

Troubleshoot

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