ASA-verificatie aan een Standby-ASA wanneer het AAA-apparaat zich in een L2L-configuratievoorbeeld bevindt

Inhoud

Inleiding

Dit document beschrijft hoe u moet werken bij een scenario waarin de beheerder niet kan authenticeren aan een Standby Cisco adaptieve security applicatie (ASA) in een failover vanwege het feit dat de AAA-server op een externe locatie gelegen is via een LAN-to-LAN (L2L).

Hoewel de back-up naar LOKALE verificatie kan worden gebruikt, verdient RADIUS-verificatie voor beide eenheden de voorkeur.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA-failover
- VPN
- Netwerkadresomzetting (NAT)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

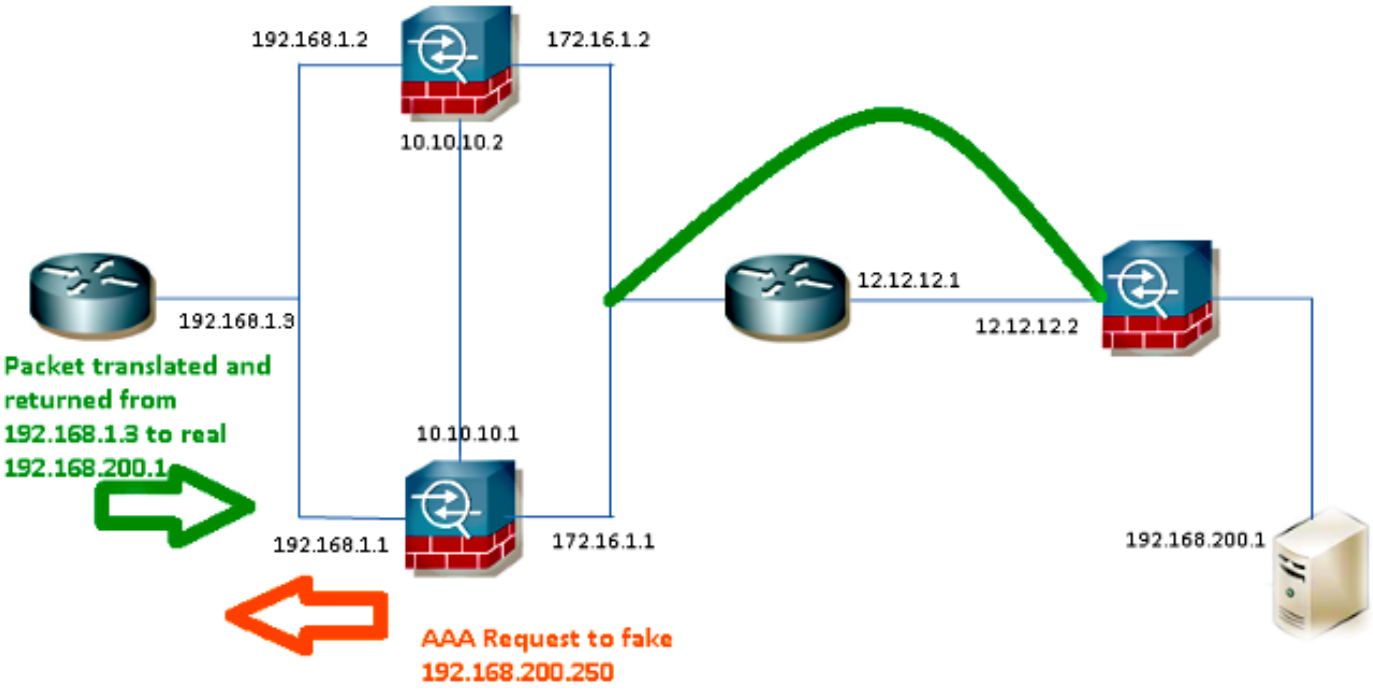
Configureren

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

De RADIUS-server bevindt zich aan de buitenkant van het failover-paar en is bereikbaar via een L2L-tunnel naar 12.12.12.2. Dit is wat het probleem veroorzaakt doordat de stand-by ASA probeert het door zijn eigen buiteninterface te bereiken, maar er is op dit punt geen tunnel op gebouwd; Om te werken, zou het het verzoek naar de actieve interface moeten sturen zodat het pakket over VPN kan stromen maar de routes worden gerepliceerd van de actieve eenheid.

Eén optie is een nep IP-adres voor de RADIUS-server op de ASA's te gebruiken en naar de binnenkant te wijzen. Daarom kan het bron- en doeladres van dit pakket op een intern apparaat worden vertaald.



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's

```
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
```

> **Opmerking:** Het IP-adres **192.168.200.250** is in het voorbeeld gebruikt, maar het ongebruikte IP-adres werkt.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **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 --- ---
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.