ASA-Authentifizierung für eine Standby-ASA, wenn sich das AAA-Gerät in einem L2L-Konfigurationsbeispiel befindet

Inhalt

Einführung

Dieses Dokument beschreibt die Vorgehensweise bei einem Szenario, in dem der Administrator keine Authentifizierung für eine Cisco Adaptive Security Appliance (ASA) im Standby-Failover-Paar durchführen kann, da sich der AAA-Server (Authentication, Authorization, and Accounting) an einem Remote-Standort über ein LAN-zu-LAN (L2L) befindet.

Obwohl ein Fallback auf die LOKALE Authentifizierung verwendet werden kann, ist die RADIUS-Authentifizierung für beide Einheiten vorzuziehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ASA-Failover
- VPN
- Network Address Translation (NAT)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

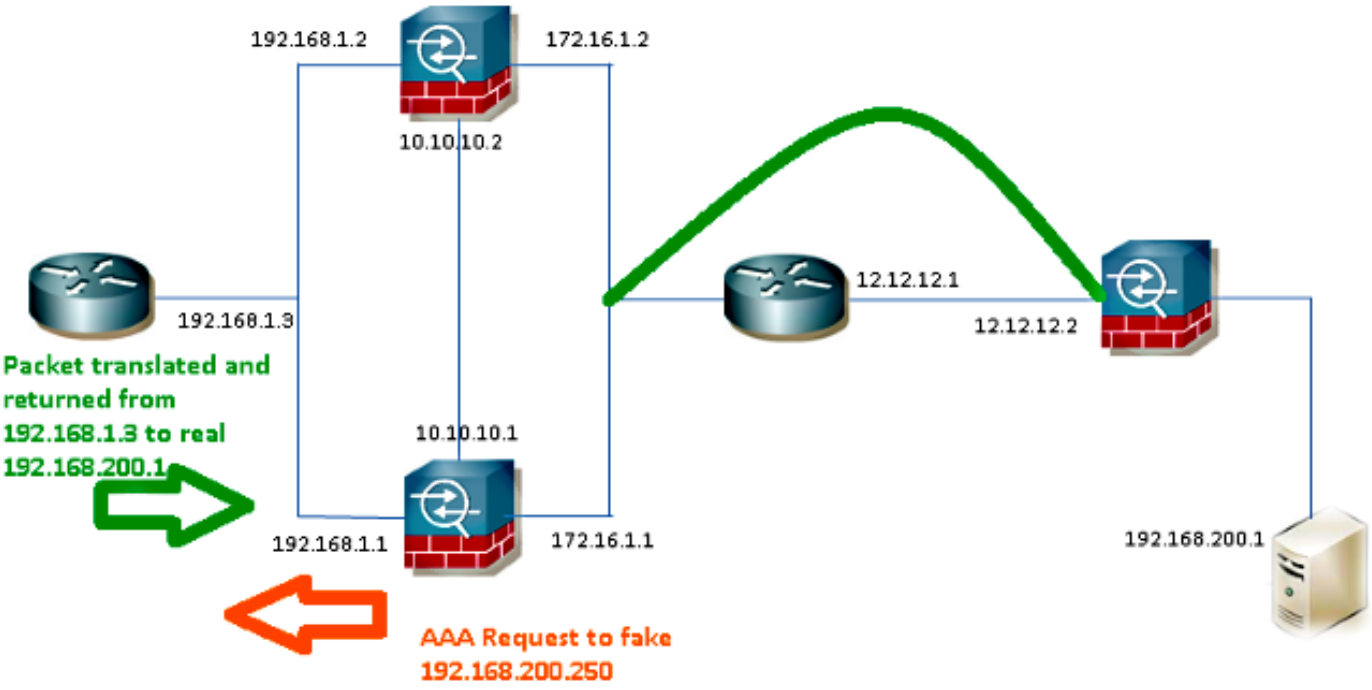
Konfigurieren

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Der RADIUS-Server befindet sich außerhalb des Failover-Paars und ist über einen L2L-Tunnel zu 12.12.12.2 erreichbar. Dies verursacht das Problem, da die Standby-ASA versucht, es über eine eigene Außenschnittstelle zu erreichen, es ist jedoch derzeit kein Tunnel darauf aufgebaut. Damit sie funktioniert, sollte sie die Anforderung an die aktive Schnittstelle senden, damit das Paket über das VPN übertragen werden kann, die Routen jedoch von der aktiven Einheit repliziert werden.

Eine Option besteht darin, eine gefälschte IP-Adresse für den RADIUS-Server auf den ASAs zu verwenden und auf die interne Adresse zu verweisen. Daher können die Quell- und Ziel-IP-Adresse dieses Pakets auf einem internen Gerät übersetzt werden.



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
```

ASAs

```
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
```

> **Hinweis**: Im Beispiel wurde die IP-Adresse **192.168.200.250** verwendet, aber alle nicht verwendeten IP-Adressen funktionieren.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

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 --- ---
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.