

# 通過L2L配置示例定位AAA裝置時對備用ASA的ASA身份驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[驗證](#)

[路由器](#)

[疑難排解](#)

## 簡介

本文說明如何解決以下情況：由於身份驗證、授權和記帳(AAA)伺服器通過LAN到LAN(L2L)位於遠端位置，因此管理員無法在故障轉移對中的備用思科自適應安全裝置(ASA)進行身份驗證。

雖然可以使用回退到本地身份驗證，但兩台裝置的RADIUS身份驗證是首選方法。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ASA故障轉移
- VPN
- 網路位址轉譯(NAT)

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

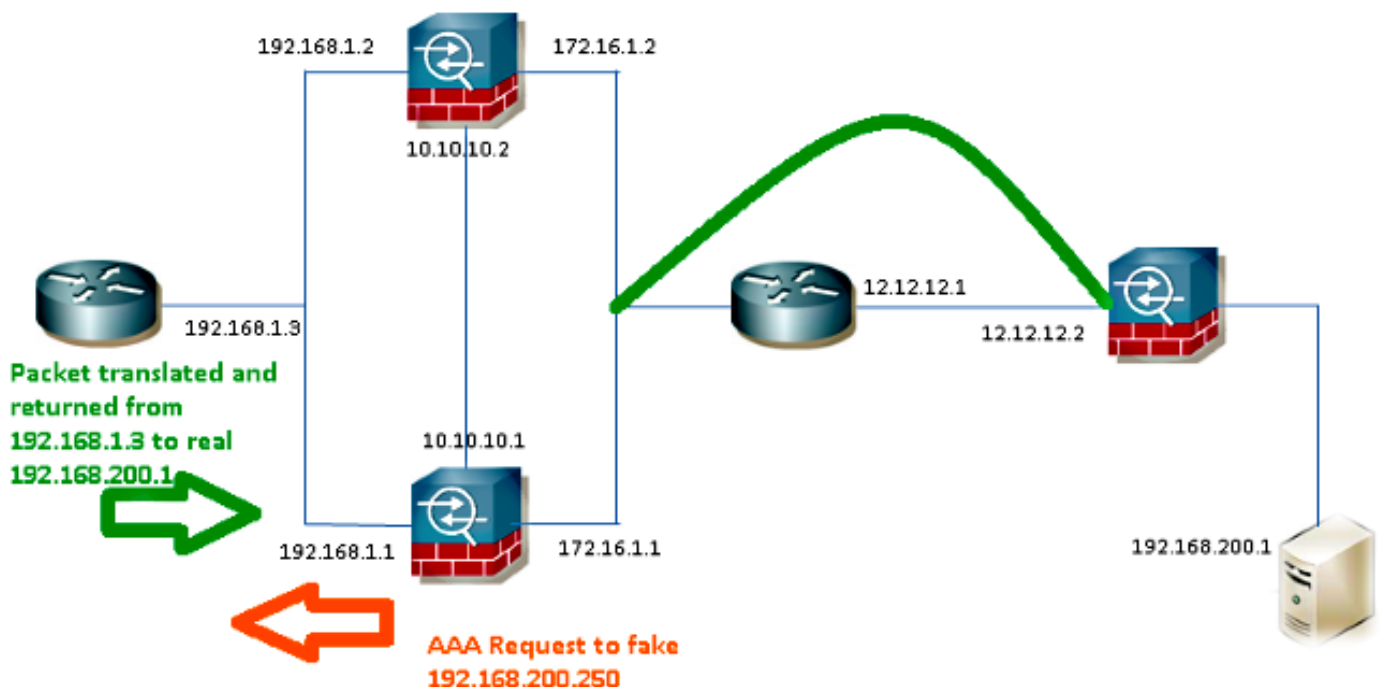
# 設定

附註：使用[命令查詢工具](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

## 網路圖表

RADIUS伺服器位於容錯移轉配對的外部，且可以透過前往12.12.12.2的L2L通道連線。這就是導致問題的原因，因為待命ASA嘗試透過其自己的外部介面連線到該伺服器，但此時沒有在其上建立通道；為了使它正常工作，它應該將請求傳送到活動介面，以便資料包可以通過VPN傳輸，但是路由是從活動單元複製的。

一個選項是為ASA上的RADIUS伺服器使用虛假IP地址並將其指向內部。因此，此資料包的源IP地址和目的IP地址可以在內部裝置上轉換。



### Router1

```
interface FastEthernet0/0
ip address 192.168.1.3 255.255.255.0
no ip redirects
no ip unreachable
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
```

**附註：**本示例中使用了**192.168.200.250** IP地址，但是所有未使用的IP地址都正常工作。

## 驗證

使用本節內容，確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

## 路由器

```
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 --- ---
```

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。