L2L を通して AAA デバイスが配置されている場合のスタンバイ ASA に対する ASA 認証の設定例

内容

概要

このドキュメントでは、認証、認可、およびアカウンティング（AAA）サーバが LAN-to-LAN（L2L）経由のリモート ロケーションにあることが原因で、フェールオーバー ペアのスタンバイ Cisco 適応型セキュリティ アプライアンス（ASA）に管理者が認証できないシナリオを回避する方法について説明します。

ローカル認証にフォールバックする方法も使用できますが、両方のユニットが RADIUS で認証されるほうが望まれます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA フェールオーバー
- VPN
- ネットワーク アドレス変換（NAT）

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

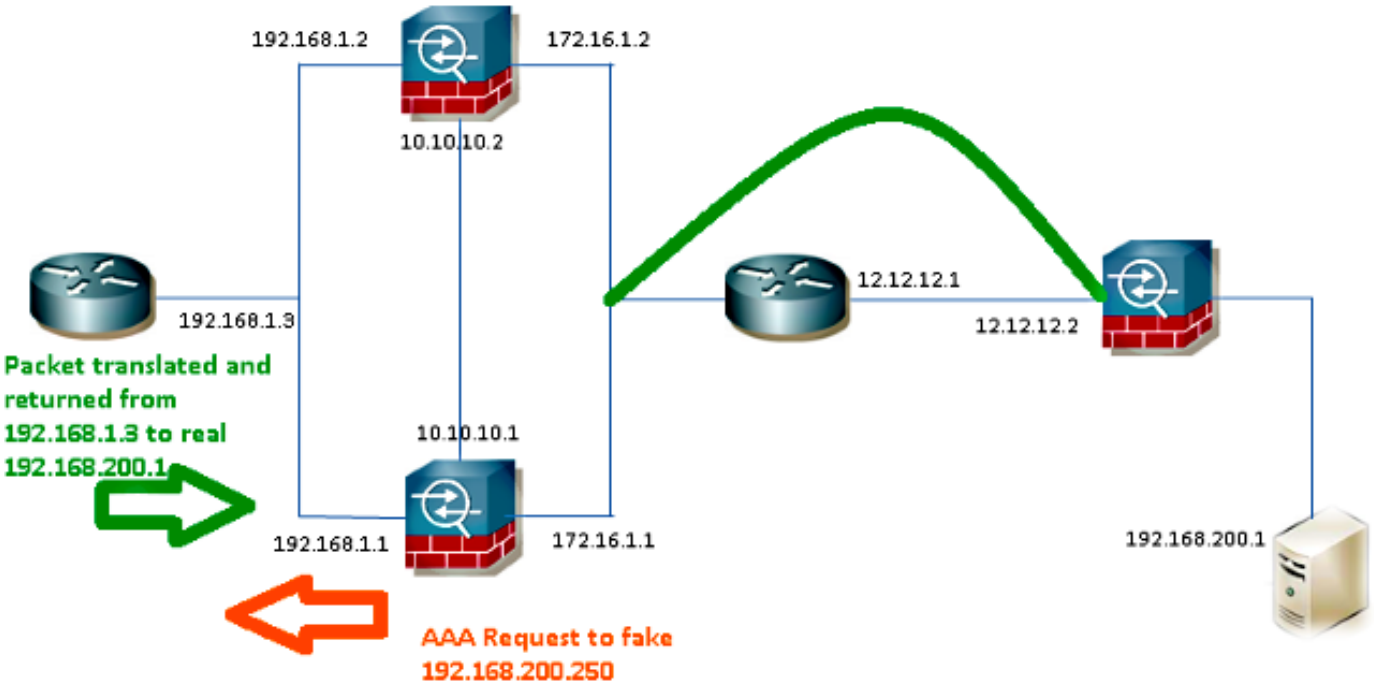
設定

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

RADIUSサーバはフェールオーバーペアの外側にあり、L2Lトンネルを介して12.12.12.2に到達できます。これは、スタンバイASAが自身の外部インターフェイスを介して到達しようとしますが、この時点ではトンネルが構築されていないため、問題の原因になります。これが機能するには、パケットが VPN 上を流れることができるように、スタンバイ ASA がアクティブ インターフェイスに対して要求を送信する必要がありますが、このルートはアクティブ ユニットから複製されます。

選択肢の 1 つは、ASA 上の RADIUS サーバ用に疑似 IP アドレスを使用し、内部を指定することです。したがって、このパケットの送信元と宛先 IP アドレスは、内部デバイスに変換されます。



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
```

注：この例では、192.168.200.250 という IP アドレスが使用されていますが、任意の未使用 IP アドレスで動作します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

ルータ

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

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。