

通过L2L配置示例定位AAA设备时对备用ASA的ASA身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[验证](#)

[路由器](#)

[故障排除](#)

简介

本文档介绍如何解决以下情况：由于身份验证、授权和记帐(AAA)服务器通过LAN到LAN(L2L)位于远程位置，因此管理员无法向故障转移对中的备用思科自适应安全设备(ASA)进行身份验证。

虽然可以使用回退到LOCAL身份验证，但两台设备的RADIUS身份验证是首选。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA故障转移
- VPN
- 网络地址转换 (NAT)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

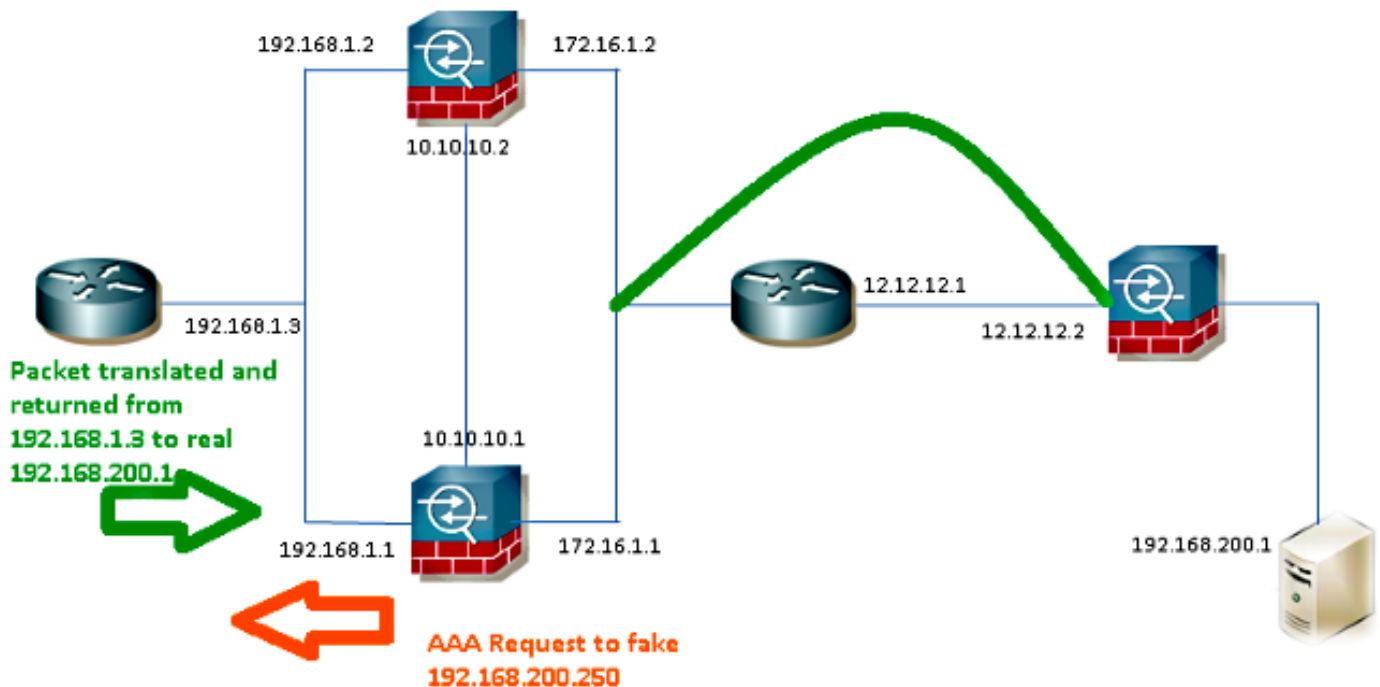
配置

注意：使用[命令查找工具（仅限注册用户）](#)可获取有关本部分所使用命令的详细信息。

网络图

RADIUS服务器位于故障切换对的外部，可通过到12.12.12.2的L2L隧道访问该服务器。这是导致问题的原因，因为备用ASA尝试通过其自己的外部接口访问该服务器，但此时没有在其上构建隧道；为使其工作，它应将请求发送到活动接口，以便数据包可以通过VPN传输，但路由会从活动单元复制。

一个选项是为ASA上的RADIUS服务器使用虚假IP地址并将其指向内部。因此，可以在内部设备上转换此数据包的源IP地址和目的IP地址。



路由器1

```
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
```

注意：本例中使用了192.168.200.250 IP地址，但所有未使用的IP地址都有效。

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序工具（仅限注册用户）支持某些 show 命令。](#) 使用输出解释器工具来查看 show 命令输出的分析。

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 --- ---
```

故障排除

目前没有针对此配置的故障排除信息。