

对待机ASA的ASA验证，当AAA设备通过L2L配置示例查找

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

本文描述如何在管理员不能验证到暂挂思科可适应安全工具的方案附近工作(ASA)在故障切换对由于这样的事实验证、授权和统计(AAA)服务器在一远程位置查找通过LAN对LAN (L2L)。

虽然可以使用对本地认证的fallback，两个单元的RADIUS验证被偏好。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- ASA故障切换
- 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服务器在故障切换对的外部查找，并且通过L2L通道是可及的对12.12.12.2。这是什么导致problem，因为待机ASA设法通过其自己的外部接口到达它，但是没有对此这时构建的通道;为了使它工作，应该发送请求到激活接口，因此数据包能在VPN间流，但是路由从活动装置复制。

一个选项是使用一个假IP地址在ASA的RADIUS服务器和指向它里面。所以，此数据包源和目的地IP地址在内部设备可以翻译。

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
```

注意：192.168.200.250 IP地址用于示例，但是所有未使用IP地址工作。

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。请使用Output Interpreter Tool为了查看show命令输出分析。

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。