

# Autenticação ASA a um ASA à espera quando o dispositivo AAA for ficado situado com um exemplo de configuração L2L

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Verificar](#)

[Router](#)

[Troubleshooting](#)

## Introdução

Este documento descreve como trabalhar em torno de uma encenação onde o administrador não possa autenticar a Cisco uma ferramenta de segurança adaptável à espera (ASA) em um par de failover devido ao fato de que o server do Authentication, Authorization, and Accounting (AAA) está ficado situado em uma posição remota com um LAN para LAN (L2L).

Embora a reserva à autenticação local possa ser usada, a autenticação RADIUS para ambas as unidades é preferida.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

### [Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

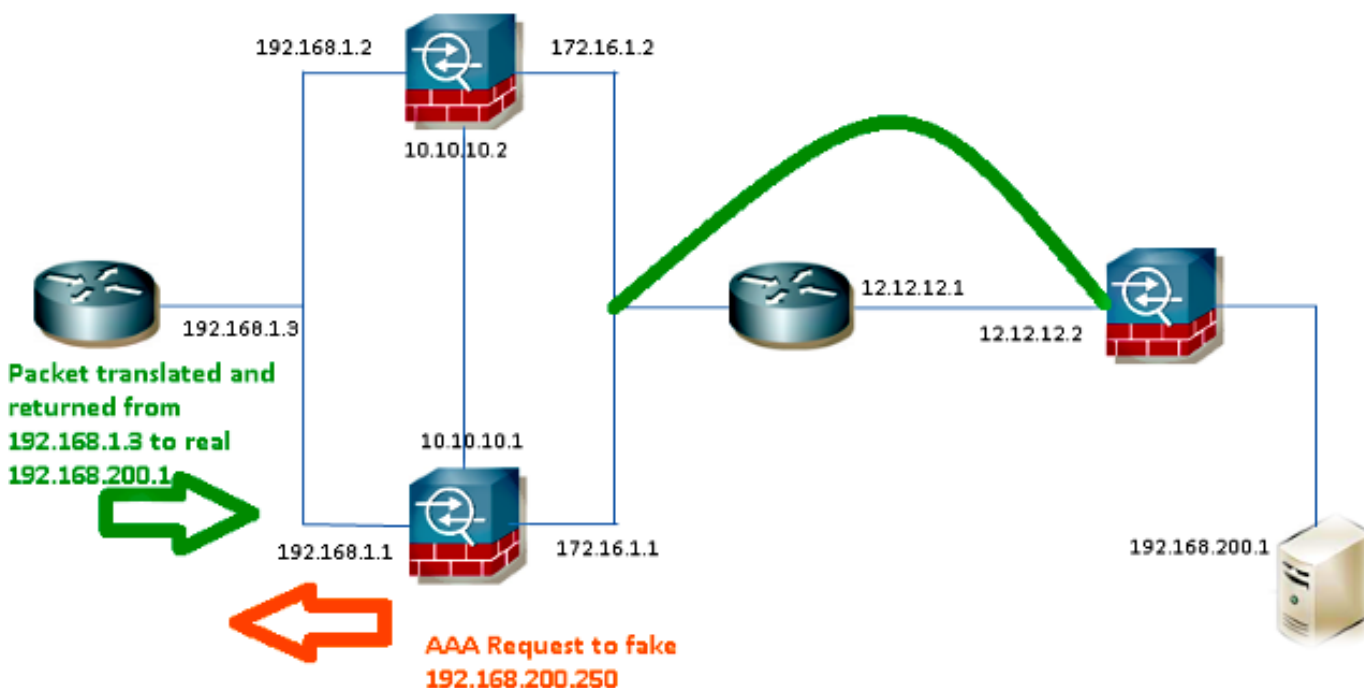
## Configurar

**Note:** Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

O servidor Radius é ficado situado na parte externa do par de failover e é alcançável através de um túnel L2L a 12.12.12.2. Este é o que causa o probem porque as tentativas à espera ASA para o alcançar através de sua própria interface externa mas lá não são nenhum túnel construído nele neste momento; para que trabalhe, deve enviar o pedido à interface ativa assim que o pacote pode fluir através do VPN mas as rotas replicated da unidade ativa.

Uma opção é usar um endereço IP de Um ou Mais Servidores Cisco ICM NT falsificado para o servidor Radius nos ASA e apontá-lo ao interior. Conseqüentemente, o endereço IP de origem e de destino deste pacote pode ser traduzido em um dispositivo interno.



### Roteador1

```
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
```

**Note:** O endereço IP **192.168.200.250** foi usado no exemplo, mas em todos os trabalhos não utilizados do endereço IP de Um ou Mais Servidores Cisco ICM NT.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

[A ferramenta Output Interpreter \(clientes registrados somente\)](#) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

## 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 --- ---
```

## Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.