Autenticação ASA para um ASA em standby quando o dispositivo AAA está localizado por meio de um exemplo de configuração L2L

Contents

Introduction

Este documento descreve como trabalhar em um cenário em que o Administrador não é capaz de se autenticar em um Cisco Adaptive Security Appliance (ASA) em standby em um Par de Failover devido ao fato de que o servidor de Autenticação, Autorização e Contabilidade (AAA) está localizado em um local remoto por meio de uma LAN para LAN (L2L).

Embora seja possível usar o fallback para a autenticação LOCAL, a autenticação RADIUS para ambas as unidades é preferida.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Failover do ASA
- VPN
- Tradução de Endereço de Rede (NAT)

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

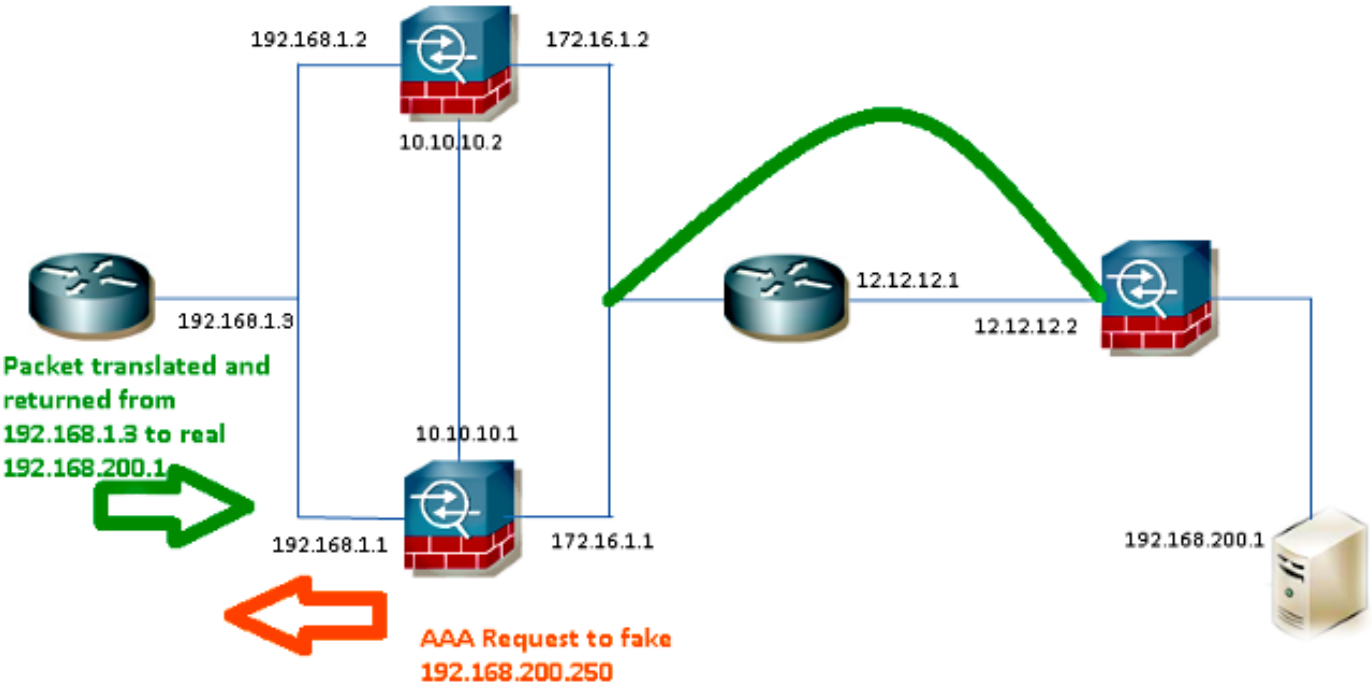
Configurar

> **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 está localizado na parte externa do Par de Failover e pode ser alcançado por meio de um túnel L2L para 12.12.12.2. Isso é o que causa o problema, pois o ASA em standby tenta alcançá-lo através de sua própria interface externa, mas não há túnel embutido nele nesse ponto; para que funcione, ele deve enviar a solicitação à interface ativa para que o pacote possa fluir pela VPN, mas as rotas sejam replicadas da unidade ativa.

Uma opção é usar um endereço IP falso para o servidor RADIUS nos ASAs e apontá-lo para o interior. Portanto, o endereço IP origem e destino desse pacote pode ser convertido em um dispositivo interno.



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
```

ASAs

```
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 qualquer endereço IP não utilizado funciona.

Verificar

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

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

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 --- ---
```

Troubleshoot

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