Аутентификация ASA к Резервному ASA, Когда Устройство AAA Расположено Через Пример конфигурации L2L

Содержание

Введение

Этот документ описывает, как обойти сценарий, где Администратор не в состоянии аутентифицироваться на Резервном устройстве адаптивной защиты Cisco (ASA) в Паре аварийного переключения вследствие того, что аутентификация, авторизация и учет (AAA) расположена на удаленном местоположении через LAN-LAN (L2L).

Несмотря на то, что нейтрализация к Локальной проверке подлинности может использоваться, Проверка подлинности RADIUS для обоих модулей предпочтена.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Аварийное переключение ASA
- VPN
- !--- преобразования сетевых адресов (NAT)

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

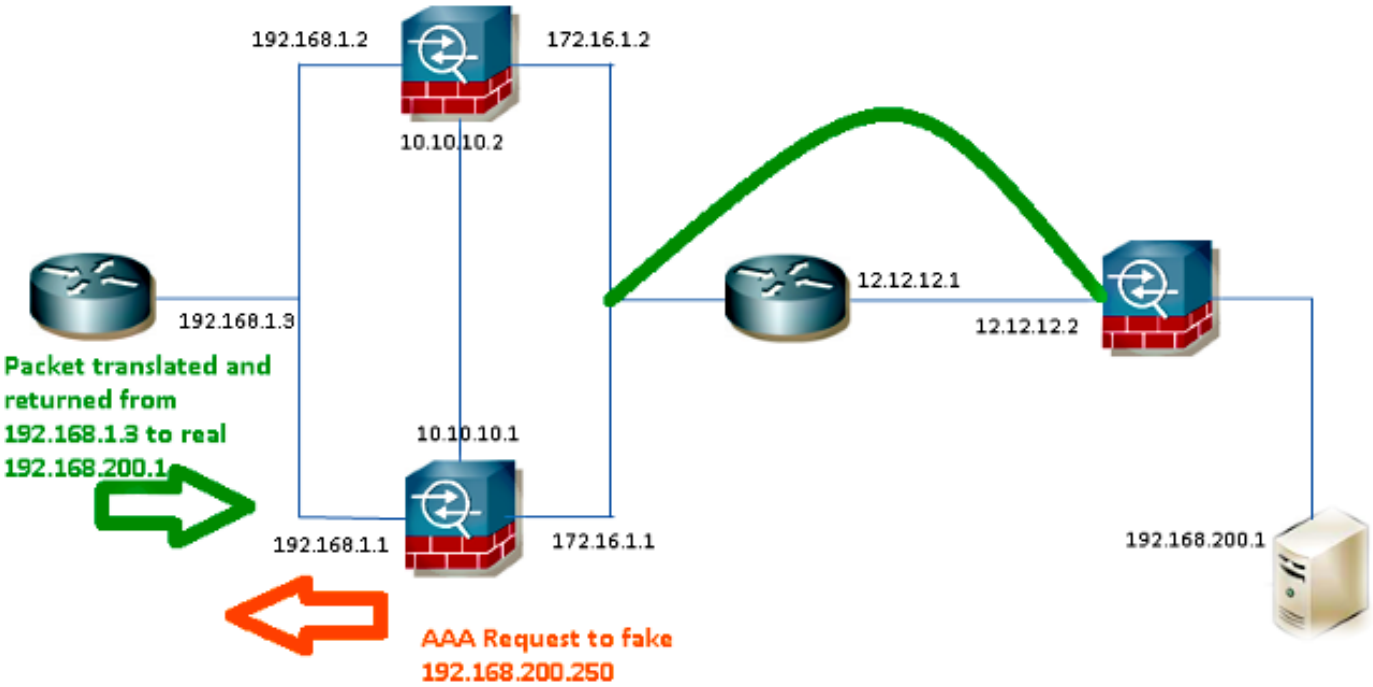
Настройка

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

Сервер RADIUS расположен за пределами Пары аварийного переключения, и это достижимо через туннель L2L к 12.12.12.2. Это - то, что вызывает probem, потому что резервный ASA пытается достигнуть его через свой собственный внешний интерфейс, но нет никакого туннеля, основывался на нем на этом этапе; для него для работы это должно отправить запрос к активному интерфейсу, таким образом, пакет может течь через VPN, но маршруты реплицированы от активного модуля.

Одна опция должна использовать поддельный IP-адрес для сервера RADIUS на ASA и указать его к внутренней части. Поэтому IP - адрес источника и получателя этого пакета может быть преобразован на внутреннем устройстве.



Маршрутизатор 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
```

> **Примечание: 192.168.200.250** IP-адреса использовались в примере, но работает любой неиспользованный IP-адрес.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Маршрутизатор

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

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.