AAA 디바이스가 L2L 컨피그레이션 예를 통해 있는 경우 스탠바이 ASA에 대한 ASA 인증

목차

소개

이 문서에서는 AAA(Authentication, Authorization, and Accounting) 서버가 LAN-to-LAN(L2L)을 통해 원격 위치에 있기 때문에 관리자가 장애 조치 쌍의 대기 Cisco ASA(Adaptive Security Appliance)를 인증할 수 없는 시나리오를 처리하는 방법에 대해 설명합니다.

LOCAL 인증으로 폴백(fallback to LOCAL) 할 수 있지만 두 유닛에 대해 RADIUS 인증을 사용하는 것이 좋습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA 장애 조치
- VPN
- NAT(Network Address Translation)

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

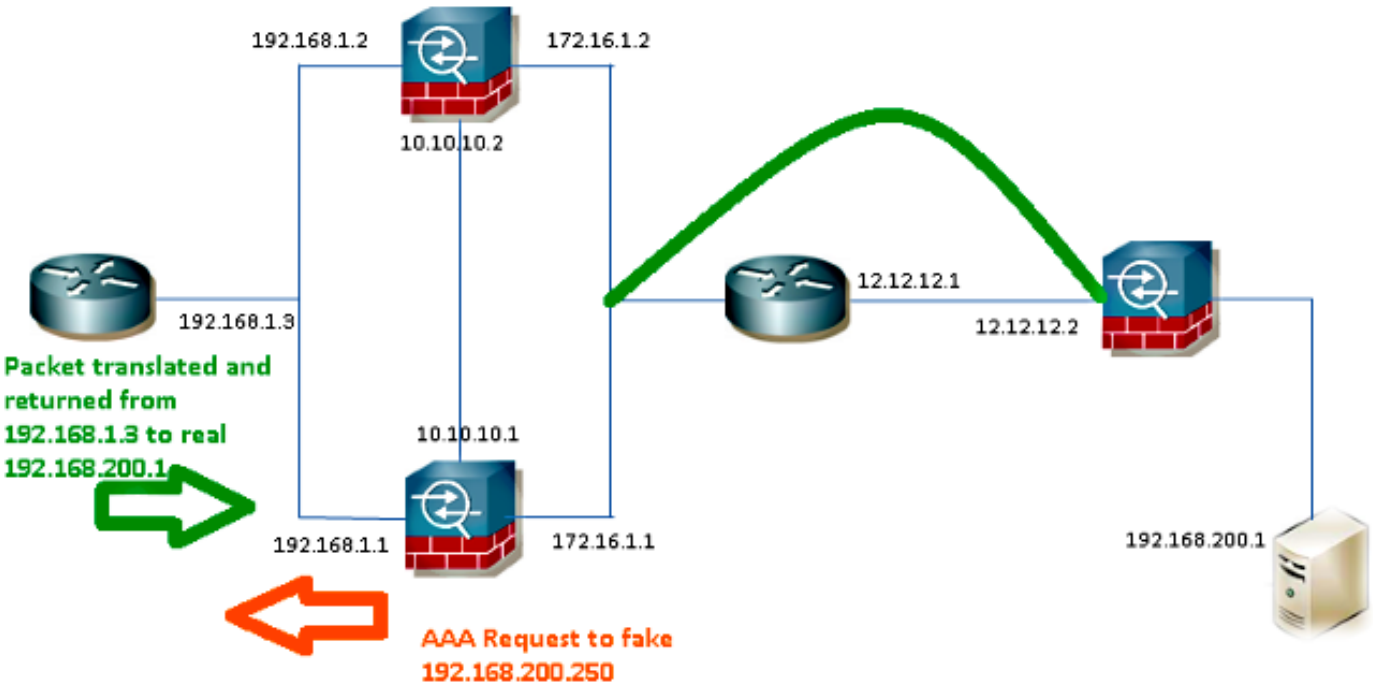
구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

RADIUS 서버는 장애 조치 쌍의 외부에 있으며 L2L 터널을 통해 12.12.12.2으로 연결할 수 있습니다. 대기 ASA가 자체 외부 인터페이스를 통해 연결을 시도하지만 이 시점에서 기본 터널이 없기 때문에 문제가 발생합니다.이를 위해서는 활성 인터페이스로 요청을 전송해야 패킷이 VPN을 통해 이동할 수 있지만 활성 유닛에서 경로가 복제됩니다.

한 가지 옵션은 ASA의 RADIUS 서버에 대해 위조 IP 주소를 사용하고 내부 주소를 가리키는 것입니다.따라서 이 패킷의 소스 및 목적지 IP 주소는 내부 디바이스에서 변환할 수 있습니다.



라우터 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
```

> **참고:192.168.200.250** IP 주소가 이 예에서 사용되었지만 사용되지 않은 IP 주소는 모두 작동합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

라우터

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

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.