L2L 터널 컨피그레이션을 통한 ASA VPN 클라이언트 연결 예

목차

소개

이 문서에서는 L2L(Lan-to-Lan) 피어 주소에서 원격 VPN 클라이언트 연결을 허용하도록 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA
- 원격 액세스 VPN
- LAN-to-LAN VPN

사용되는 구성 요소

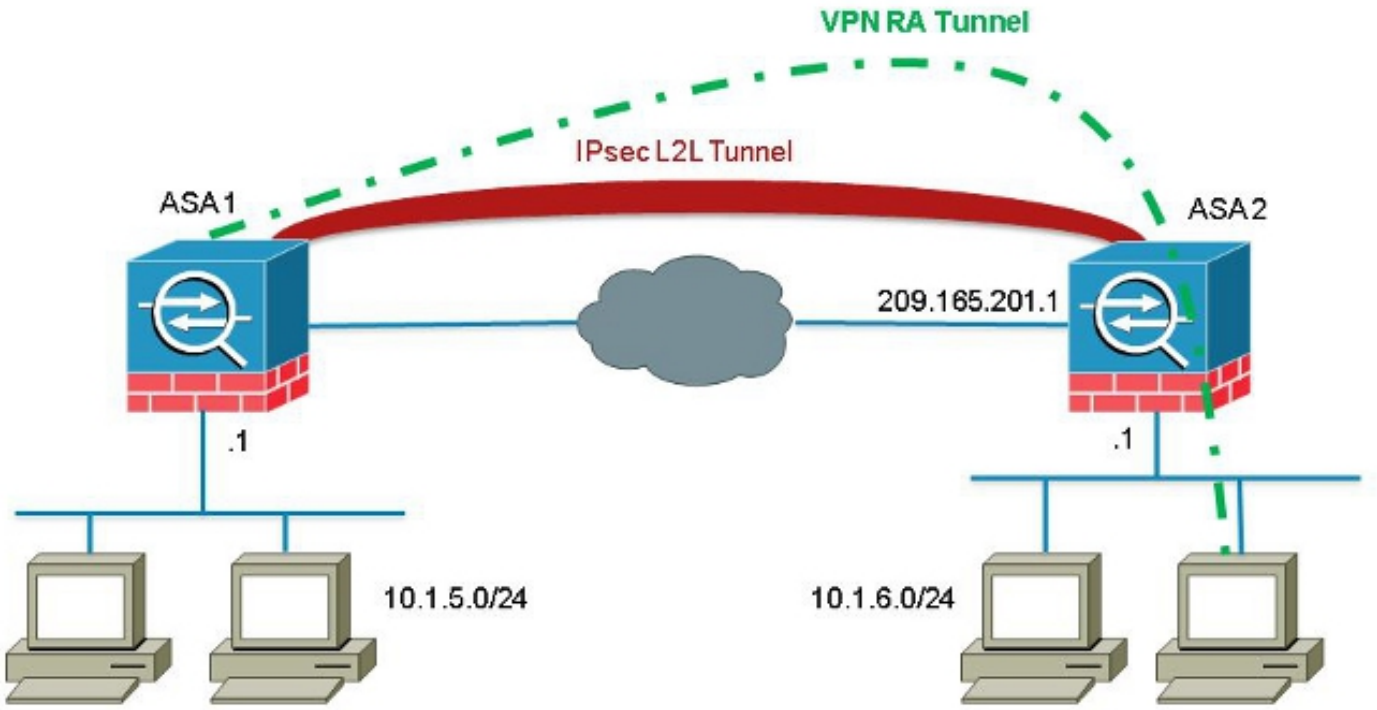
이 문서의 정보는 소프트웨어 버전 8.4(7)를 실행하는 Cisco 5520 Series ASA를 기반으로 합니다.

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.

배경 정보

VPN 클라이언트가 L2L 터널을 통해 연결을 설정하려고 시도하는 시나리오는 일반적으로 없지만 관리자는 특정 원격 사용자에게 특정 권한 또는 액세스 제한을 할당하고 이러한 리소스에 대한 액세스가 필요할 때 소프트웨어 클라이언트를 사용하도록 지시할 수 있습니다.

> **참고:**이 시나리오는 과거에 사용되었지만 헤드엔드 ASA를 버전 8.4(6) 이상으로 업그레이드한 후에는 VPN 클라이언트가 더 이상 연결을 설정할 수 없습니다.



Cisco 버그 ID CSCuc75090에서 동작 변경을 도입했습니다.이전에는 PIX(Private Internet Exchange)를 사용하여 IPSec(Internet Protocol Security) 프록시가 암호화 맵 ACL(Access Control List)과 일치하지 않을 때 항목을 계속 목록의 아래로 검사했습니다.여기에는 지정된 피어가 없는 동적 암호화 맵과 일치하는 항목이 포함됩니다.

이는 취약성으로 간주되었습니다. 원격 관리자는 정적 L2L을 구성할 때 헤드엔드 관리자가 의도하지 않은 리소스에 액세스할 수 있기 때문입니다.

피어와 일치하는 맵 엔트리를 이미 확인한 경우 피어 없이 암호화 맵 엔트리와 일치하는 것을 방지하기 위해 체크 인을 추가한 수정 사항이 생성되었습니다.그러나 이는 이 문서에서 설명하는 시나리오에 영향을 주었습니다.특히 L2L 피어 주소에서 연결을 시도하는 원격 VPN 클라이언트는 헤드엔드에 연결할 수 없습니다.

구성

L2L 피어 주소에서 원격 VPN 클라이언트 연결을 허용하도록 ASA를 구성하려면 이 섹션을 사용합니다.

새 동적 항목 추가

L2L 피어 주소에서 원격 VPN 연결을 허용하려면 동일한 피어 IP 주소를 포함하는 새 동적 항목을 추가해야 합니다.

> **참고:**또한 인터넷의 모든 클라이언트도 연결할 수 있도록 피어 없이 다른 동적 항목을 남겨두어야 합니다.

다음은 이전 동적 암호화 맵 작업 컨피그레이션의 예입니다.

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

다음은 새 동적 엔트리가 구성된 동적 암호화 맵 컨피그레이션입니다.

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

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