IPsec LAN-to-LAN 터널을 통한 ASA 클라이언트리스 SSL VPN 트래픽 컨피그레이션 예

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 클라이언트리스 SSLVPN 포털에 연결하고 IPsec LAN-to-LAN 터널을 통해 연결된 원격 위치에 있는 서버에 액세스하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 클라이언트리스 SSL VPN 컨피그레이션.
- LAN-to-LAN VPN 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 버전 9.2(1)를 실행하는 ASA 5500-X Series를 기반으로 하지만 모든 ASA 버전에 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크를 변경하기 전에 모든

명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

클라이언트리스 SSLVPN 세션의 트래픽이 LAN-to-LAN 터널을 통과하는 경우 두 개의 연결이 있습니다.

- 클라이언트에서 ASA로
- ASA에서 목적지 호스트로 이동합니다.

ASA-to-destination 호스트 연결의 경우 ASA 인터페이스의 IP 주소가 대상 호스트에 "가장 가까운" 상태로 사용됩니다.따라서 LAN-to-LAN 흥미로운 트래픽은 해당 인터페이스 주소에서 원격 네트워크로 향하는 프록시 ID를 포함해야 합니다.

> **참고:** Smart-Tunnel을 책갈피에 사용할 경우, 대상에 가장 가까운 ASA 인터페이스의 IP 주소가 계속 사용됩니다.

구성

이 다이어그램에는 두 ASA 간에 LAN-to-LAN 터널이 있어 192.168.10.x에서 192.168.20.x로 트래픽을 전달할 수 있습니다.

해당 터널에 대해 흥미로운 트래픽을 결정하는 액세스 목록:

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

클라이언트리스 SSLVPN 사용자가 192.168.20.x 네트워크의 호스트와 통신을 시도할 경우 ASA1은 209.165.200.225 주소를 해당 트래픽의 소스로 사용합니다.LAN-to-LAN ACL(Access Control List)에 프록시 ID로 209.168.200.225이 포함되어 있지 않으므로 LAN-to-LAN 터널을 통해 트래픽이 전송되지 않습니다.

LAN-to-LAN 터널을 통해 트래픽을 전송하려면 새로운 ACE(Access Control Entry)를 흥미로운 트래픽 ACL에 추가해야 합니다.

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
```

```
255.255.255.0
```

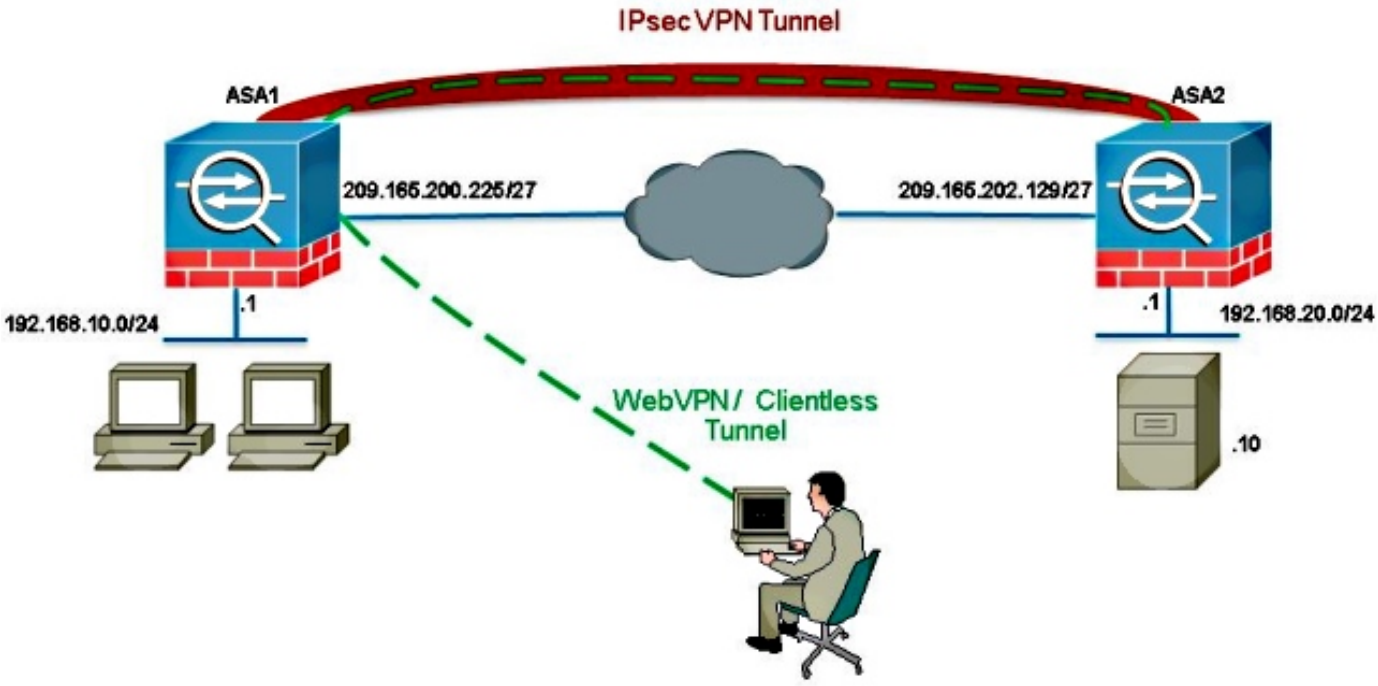
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

이 원칙은 클라이언트리스 SSLVPN 트래픽이 LAN-to-LAN 터널을 통과하지 않아도 동일한 인터페이스를 U-Turn해야 하는 컨피그레이션에 적용됩니다.

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

네트워크 다이어그램



일반적으로 ASA2는 인터넷 액세스를 제공하기 위해 192.168.20.0/24용 PAT(Port Address Translation)를 수행합니다.이 경우 ASA 2의 192.168.20.0/24에서 209.165.200.225으로 이동할 때 PAT 프로세스에서 트래픽을 제외해야 합니다. 그렇지 않으면 LAN-to-LAN 터널을 통과하지 않습니다.예를 들면 다음과 같습니다.

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

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.

- **show crypto ipsec sa**-Verify with this command that a Security Association (SA) between the ASA1 Proxy IP address and the remote network has been created(ASA(SA) 생성).클라이언트리스 SSLVPN 사용자가 해당 서버에 액세스할 때 암호화 및 암호 해독된 카운터가 증가하는지 확인합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

보안 연결이 빌드되지 않은 경우 IPsec 디버깅을 사용하여 실패의 원인을 파악할 수 있습니다.

- **debug crypto ipsec <level>**

  참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.