두 Site-to-Site 터널 간의 트래픽 헤어피닝 구성

목차

소개

이 문서에서는 단일 인터페이스에서 두 VPN 터널 간에 VPN 트래픽을 전달하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

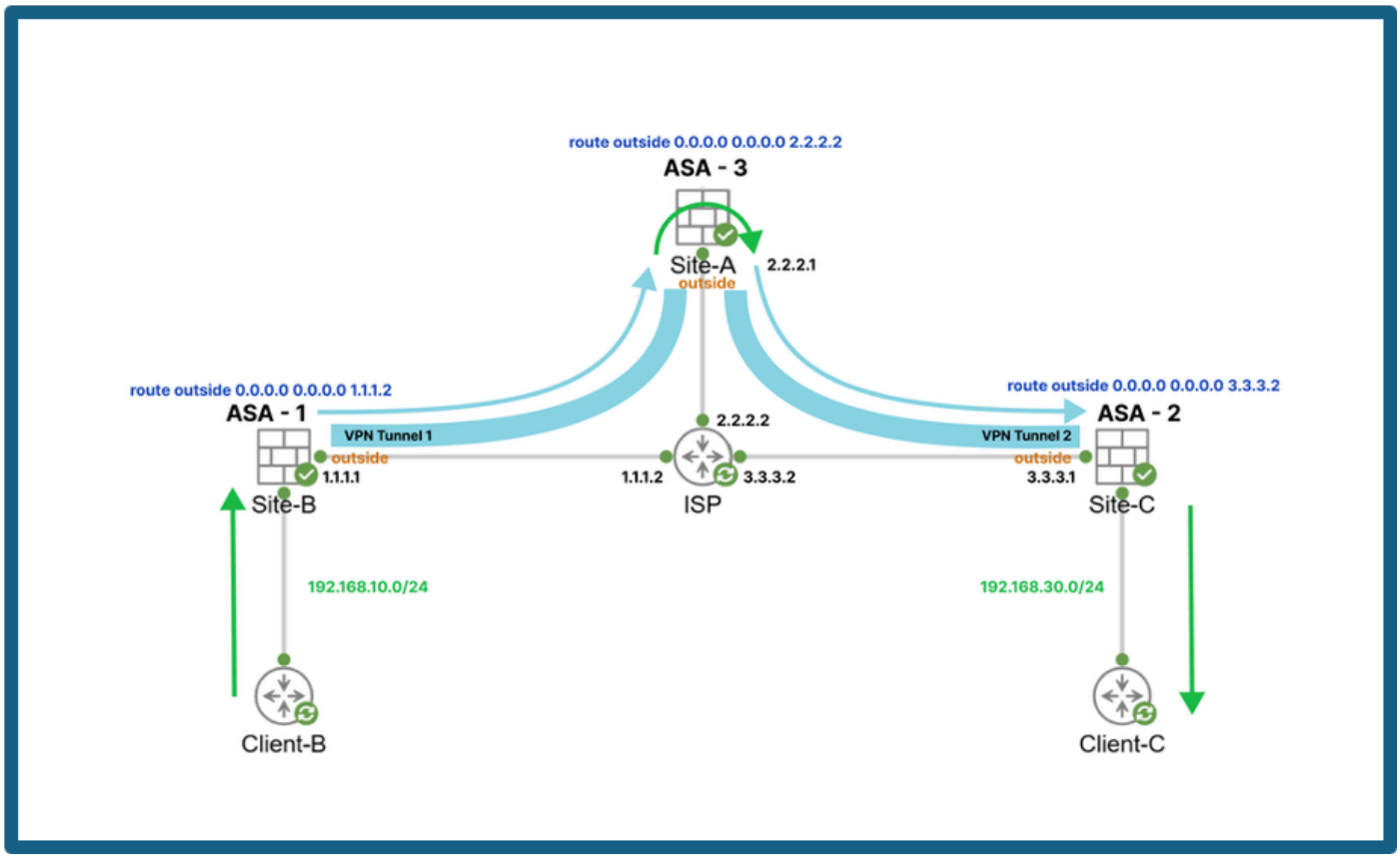
Cisco에서는 다음 항목에 대한 지식을 권장합니다.
· Policy Based Site-to-Site VPN에 대한 기본 이해
· ASA 명령줄 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
· ASA(Adaptive Security Appliance) 버전 9.20
· IKEv1

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

토폴로지



토폴로지

배경 정보

이 컨피그레이션에서는 하나의 사이트 대 사이트 터널에서 동일한 디바이스의 다른 터널로 트래픽을 리디렉션하는 방법을 보여줍니다. 이러한 설정을 설명하기 위해 사이트 A, 사이트 B 및 사이트 C를 나타내는 세 개의 ASA를 사용했습니다.

설정

이 섹션에서는 ASA-1(사이트 B)에서 ASA-2(사이트 C)를 통해 ASA-3(사이트 A)으로 이동하는 트래픽을 허용하는 데 필요한 컨피그레이션에 대해 설명합니다.

2개의 VPN 터널이 구성되어 있습니다.

- VPN 터널 1: Site-B와 Site-A 간의 VPN 터널
- VPN 터널 2: Site-C와 Site-A 간의 VPN 터널

ASA에서 정책 기반 VPN 터널을 생성하는 방법에 대한 자세한 지침은 Cisco 설명서의 ASA Configuration 섹션을 참조하십시오. ASA와 Cisco IOS XE Router 간의 사이트 간 IPSec IKEv1 터널 구성

ASA(사이트 B) 구성

ASA 1의 외부 인터페이스에 있는 VPN Tunnel 1의 암호화 액세스 목록에서 Site-B 네트워크에서 Site-C 네트워크로 가는 트래픽을 허용해야 합니다.
이 시나리오에서는 192.168.10.0/24~192.168.30.0/24입니다.

암호화 액세스 목록:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Nat 예외:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

VPN 터널 1에 대한 암호화 맵:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA(사이트 C) 암호화 컨피그레이션

ASA 2의 외부 인터페이스에 있는 VPN Tunnel 2의 암호화 액세스 목록에서 Site-C 네트워크에서 Site-B 네트워크로의 트래픽을 허용합니다.
이 시나리오에서는 192.168.30.0/24~192.168.10.0/24입니다.

암호화 액세스 목록:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Nat 예외:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

VPN 터널 2에 대한 암호화 맵:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA(사이트 A) 암호화 컨피그레이션

VPN 터널 1의 암호화 액세스 목록에 있는 Site-C 네트워크에서 Site-B 네트워크로 가는 트래픽, Site-A에 있는 ASA 외부 인터페이스의 VPN 터널 2의 암호화 액세스 목록에 있는 Site-C 네트워크에서 Site-C 네트워크로 가는 트래픽(ASA에서 구성한 것과 반대 방향)을 허용합니다.

이 시나리오에서는 VPN 터널 1의 경우 192.168.30.0/24에서 192.168.10.0/24으로, VPN 터널 2의 경우 192.168.10.0/24에서 192.168.30.0/24으로 계산됩니다

암호화 액세스 목록:

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

VPN 터널 1 및 2에 대한 암호화 맵 컨피그레이션:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

이 외에도 동일한 보안 레벨을 가진 동일한 인터페이스인 외부에서 외부로 트래픽을 라우팅해야 하므로 다음 명령을 구성해야 합니다.

```
same-security-traffic permit intra-interface
```

Site-B에서 Site-C로의 트래픽 흐름

192.168.10.0/24에서 192.168.30.0/24까지의 Site-B에서 Site-c로 트래픽이 시작되었다고 가정해 보겠습니다.

Site-B(소스)

1. 192.168.10.0/24 network(Site-B)에서 시작되어 192.168.30.0/24 network(Site-C)으로 향하는 트래픽은 구성된 라우팅 테이블을 기반으로 ASA-1의 외부 인터페이스로 라우팅됩니다.

2. 트래픽이 ASA-1에 도달하면 ASA-1에 구성된 암호화 액세스 목록 110과 일치합니다. 이렇게 하면 VPN 터널 1을 사용하여 트래픽의 암호화가 트리거되어 데이터를 Site-A로 안전하게 전송합니다
.

사이트 A(중간)

1. 사이트 A에 있는 ASA의 외부 인터페이스에 있는 192.168.10.0/24 to 192.168.30.0/24 arrives에서 암호화된 트래픽.
2 . 사이트 A에서 트래픽은 VPN 터널 1에 의해 해독되어 원래 페이로드를 복원합니다.
3 . 해독된 트래픽은 사이트 A의 ASA 외부 인터페이스에서 VPN 터널 2를 사용하여 다시 암호화됩

니다.

사이트-C(대상)

1. Site-C에 있는 ASA-2의 외부 인터페이스인 192.168.10.0/24 to 192.168.30.0/24 reaches에서 암호화된 트래픽.
2 . ASA-2는 VPN Tunnel 2를 사용하여 트래픽을 해독하고 패킷을 Site-C의 LAN측으로 전달하여 192.168.30.0/24 network 내의 원하는 목적지로 전달합니다.

Site-C에서 Site-B로의 역방향 트래픽 흐름

Site-C(192.168.30.0/24) and, Site-B(192.168.10.0/24)에서 시작되는 역방향 트래픽 흐름은 동일한 프로세스를 생성하지만 반대 방향으로 진행합니다.
1. Site-C에서 트래픽은 Site-A로 전송되기 전에 VPN 터널 2에 의해 암호화됩니다.
2. Site-A에서 트래픽은 VPN Tunnel 2에 의해 암호 해독된 다음 Site-B로 전달되기 전에 VPN Tunnel 1을 사용하여 다시 암호화됩니다.
3. Site-B에서 트래픽은 VPN 터널 1에 의해 암호 해독되어 192.168.10.0/24 network에 전달됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.