Cisco Secure Access에서 서브넷이 겹치는 Site-to-Site 연결

목차

소개

이 문서에서는 Cisco Secure Access와 중복되는 서브넷 솔루션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Access 관리
- 방화벽/라우터 관리.

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- Cisco 보안 액세스에 대한 관리 액세스.
- IPSec 헤드엔드 디바이스(방화벽 또는 라우터)에 대한 관리 액세스

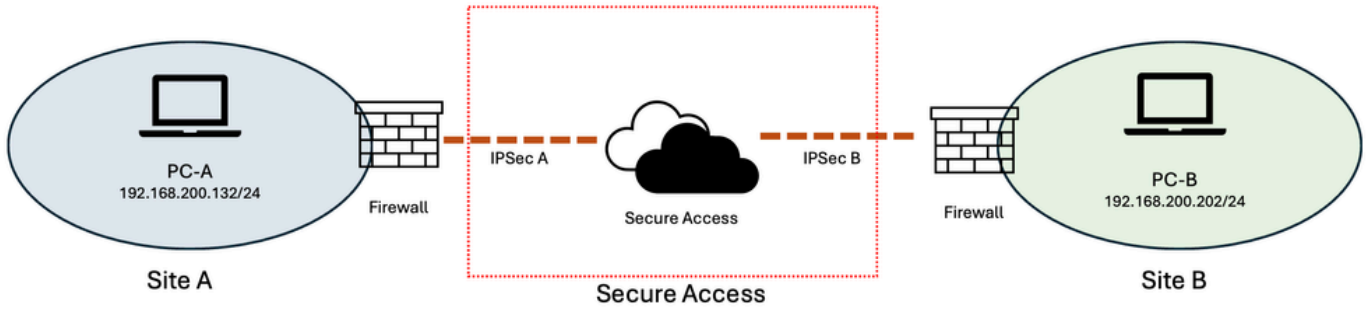
사용되는 구성 요소

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

시작하기 전에

이 예에는 동일한 IP 서브넷 192.168.200.0/24을 사용하는 서로 다른 두 브랜치 사이트가 있으며, 이 사이트에서는 두 개의 개별 IPSec 터널을 통해 Cisco Secure Access에 연결됩니다.



이미지 - 네트워크 다이어그램

목표는 "사이트 A"의 사용자가 "사이트 B"의 리소스에 액세스할 수 있고 그 반대의 경우도 가능합니다.

준비 및 계획

두 사이트 모두 동일한 IP 서브넷(192.168.200.0/24)을 사용하므로 주소 공간이 겹치면 두 사이트 간의 직접 통신이 차단됩니다. 이러한 중복을 해결하기 위해 두 개의 겹치지 않는 가상 서브넷을 할당하여 각 사이트의 리소스를 나타냅니다.

이 예에서는

- 사이트 A: 10.30.30.0/24
- 사이트 B: 10.40.40.0/24

- 두 사이트의 실제 서브넷: 192.168.200.0/24

가상 서브넷은 각 사이트에 고유한 주소 공간을 제공하는 반면, 실제 리소스는 기존 192.168.200.0/24 주소를 계속 사용합니다.

사이트 A의 사용자가 사이트 B에 있는 리소스에 액세스할 때, 사용자는 겹치는 192.168.200.0/24의 주소 공간을 직접 사용하는 대신 사이트 B 가상 서브넷(**10.40.40.0/24**)을 통해 리소스에 액세스합니다.

Cisco Secure Access는 가상 주소를 해당 실제 주소로 변환할 수 있는 D-NAT(One-to-One Destination NAT) 기능을 제공합니다. D-NAT 주소 범위는 원래 서브넷과 크기가 같습니다. 이 예에서는 가상 네트워크와 실제 네트워크 모두 /24 서브넷으로 가상 IP 주소와 실제 IP 주소 간에 일대일 매핑을 제공합니다.

예를 들면 다음과 같습니다.

10.40.40.202 → 192.168.200.202

따라서 10.40.40.202를 대상으로 하는 사이트 A의 요청은 D-NAT에 의해 192.168.200.202로 변환되므로, 두 사이트가 동일한 기본 IP 서브넷을 사용하더라도 사이트 B의 해당 리소스에 요청이 도달할 수 있습니다.

이 접근 방식은 리소스의 기존 IP 주소 지정을 유지하면서 각 사이트에 대해 중복되지 않는 가상 주소 공간을 효과적으로 생성합니다. 또한 가상 주소와 실제 주소 간에 일관적인 일대일 관계를 제공하므로 컨피그레이션의 이해, 관리, 트러블슈팅이 더욱 쉬워집니다.

컨피그레이션 단계

Cisco Secure Access의 현재 설계 및 제한 사항으로 인해 이 시나리오를 달성하려면 IPsec 터널 뒤의 헤드엔드 디바이스와 Cisco Secure Access에서 모두 구성해야 합니다.

헤드엔드 디바이스는 Cisco Secure Access에 대한 IPsec 터널을 설정하는 방화벽 또는 라우터입니다. Cisco Secure Access에서 D-NAT를 구성하는 것 외에, 헤드엔드 방화벽은 반환 트래픽에 대해서도 S-NAT(Source NAT)를 수행해야 합니다.

따라서 이 컨피그레이션은 다음 두 섹션으로 구성됩니다.

1. 각 네트워크 터널에 대해 Cisco Secure Access에서 D-NAT(Destination NAT)를 개별적으로 구성

2. 반환 트래픽이 가상 주소 공간으로 다시 변환되도록 방화벽에서 소스 NAT(S-NAT) 구성

Cisco Secure Access 구성

1단계: Cisco Secure Access 관리 포털에서 Connect(연결) > Network Connections(네트워크 연결)로 이동하고 Network Tunnel Groups(네트워크 터널 그룹) 탭을 선택합니다.

2단계: 겹치는 서브넷을 사용하는 사이트의 IPsec 터널과 연결된 네트워크 터널 그룹을 편집합니다.

이 예에서는 다음을 수행합니다.

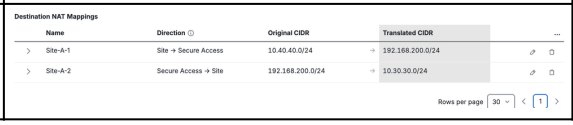
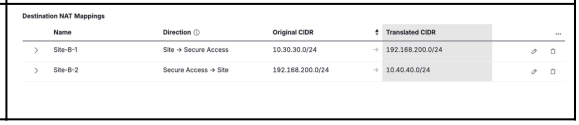
- IPSec-A = 사이트 A의 네트워크 터널 그룹
- IPSec-B = 사이트 B의 네트워크 터널 그룹

3단계: 필요한 네트워크 터널 그룹 옆에 있는 3점 메뉴를 클릭하고 Edit(수정)를 선택합니다.

4단계: 왼쪽 메뉴에서 Routing(라우팅) 탭을 선택하고 아직 활성화되지 않은 경우 NAT(Network Address Translation)를 활성화합니다.

5단계: Destination NAT Mappings 아래에서 Add Mappings를 클릭합니다.

6단계: 다음 표를 사용하여 각 네트워크 터널 그룹에 대한 D-NAT 매핑을 구성합니다.

	사이트 A - IPSec 터널	사이트 B - IPSec 터널
대상 NAT-1	사이트 → 보안 액세스 원래 CIDR: 10.40.40.0/24 변환된 CIDR: 192.168.200.0/24	사이트 → 보안 액세스 원래 CIDR: 10.30.30.0/24 변환된 CIDR: 192.168.200.0/24
대상 NAT-2	보안 액세스 → 사이트 원래 CIDR: 192.168.200.0/24 변환된 CIDR: 10.30.30.0/24	보안 액세스 → 사이트 원래 CIDR: 192.168.200.0/24 번역된 CIDR: 10.40.40.0/24
		

	IPsec 터널 사이트 A - D-NAT 컨피그레이션	IPsec 터널 사이트 B - D-NAT 컨피그레이션

참고: 각 네트워크 터널 그룹에 대한 설정을 구성한 후 Save를 클릭합니다. 확인 창이 나타나면 UPDATE를 입력하여 변경을 확인합니다. 다른 네트워크 터널 그룹에 대해 동일한 절차를 반복합니다

방화벽 구성

현재 네트워크 터널 그룹 뒤에 겹치는 IP 서브넷을 처리하는 데 제한이 있으므로 방화벽 컨피그레이션이 필요합니다.

Cisco Secure Access가 수신 패킷에 대해 D-NAT를 수행하는 경우 변환된 대상 주소를 사용하여 패킷을 대상 리소스에 전달합니다. 그러나 이 중첩 서브넷 시나리오에서 반환 트래픽에 대해 해당 역변환이 자동으로 수행되지 않습니다.

따라서 반환 트래픽은 방화벽에서 수동으로 소스-NAT를 처리해야 합니다.

주요 요구 사항은 대상 서버가 서버의 실제 IP 주소가 아니라 클라이언트가 원래 액세스한 가상 IP 주소를 사용하여 반환 트래픽을 확인하는 것입니다.

예

다음을 가정합니다.

- 사이트 A 클라이언트: 192.168.200.132
- 사이트 B 웹 서버: 192.168.200.202
- 사이트 B 가상 서브넷: 10.40.40.0/24
- 웹 서버의 가상 주소: 10.40.40.202

사이트 A의 클라이언트는 https://10.40.40.202을 사용하여 사이트 B 웹 서버에 액세스합니다.

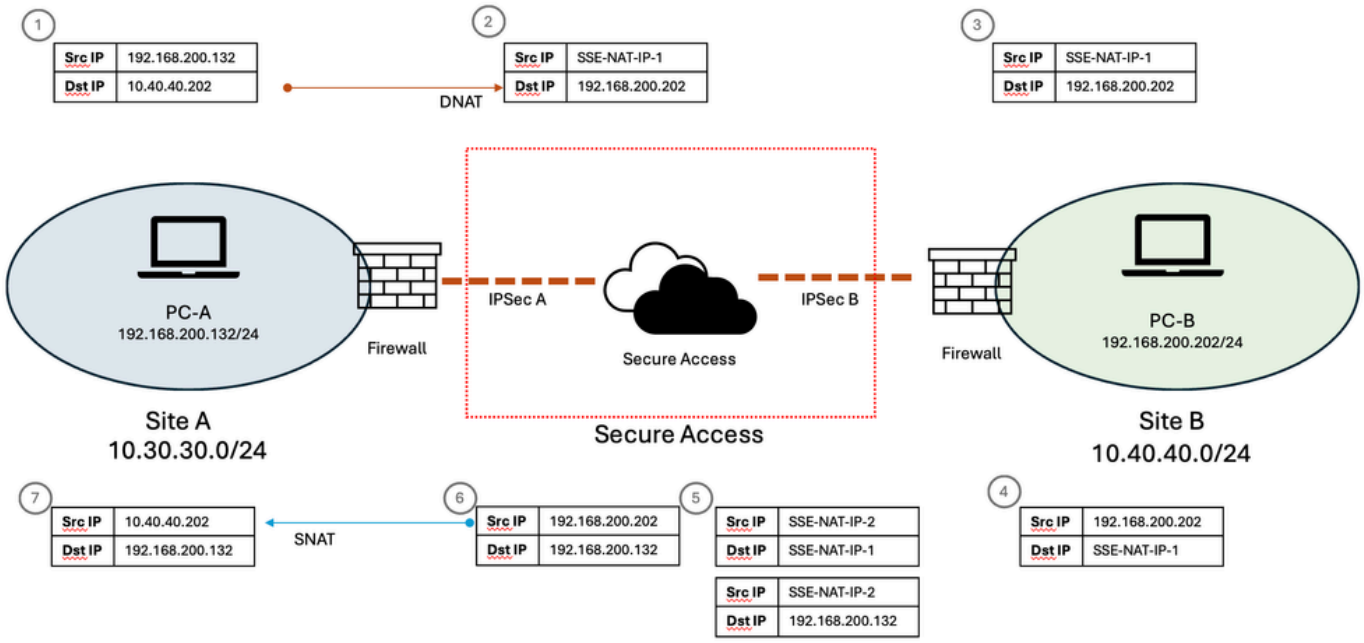
Cisco Secure Access는 D-NAT 10.40.40.202 → 192.168.200.202를 수행합니다.

그런 다음 패킷은 192.168.200.202의 웹 서버에 도달합니다.

반환 트래픽에서 문제가 발생합니다. 방화벽에 추가 NAT가 없으면 웹 서버는 Source(소스): 192.168.200.202

그러나 클라이언트가 Destination에 대한 연결을 시작했습니다. `10.40.40.202`

따라서 클라이언트에 제공되는 소스 주소가 가상 주소 `192.168.200.202 → 10.40.40.202`에 대응하도록 반환 트래픽을 변환해야 합니다



이미지 - 네트워크 흐름

이를 위해 방화벽은 네트워크 터널 그룹을 향해 나가는 트래픽에 대해 소스 NAT를 수행합니다.

이 예에서 필요한 매핑은 `192.168.200.0/24 → 10.40.40.0/24`입니다

이렇게 하면 실제 주소와 해당 가상 주소 간에 역방향 일대일 관계가 생성됩니다.

일대일 스냇

방화벽이 전체 서브넷에 대해 일대일 소스 NAT를 지원하는 경우 단일 NAT 규칙이 전체 `/24` 주소 범위를 나타낼 수 있습니다.

예를 들면 다음과 같습니다.

실제 출처	변환된 소스
192.168.200.0/24	10.40.40.0/24

이렇게 하면 `192.168.200.202 → 10.40.40.202` 및 `192.168.200.203 → 10.40.40.203`과 같은 매핑이 생성됩니다

동일한 일대일 관계가 전체 서브넷에 적용됩니다.

일대일 SNAT가 없는 방화벽

방화벽이 전체 서브넷에 대해 일대일 소스 NAT를 지원하지 않는 경우 필요한 각 매핑을 개별적으로 구성해야 합니다.

예를 들어, 웹 서버의 경우

- 소스 IP: `192.168.200.202`
- 소스 인터페이스: 네트워크 터널 그룹
- 트래픽 방향: 인바운드
- 변환된 소스 IP: `10.40.40.202`

그 결과로 변환되는 값은 `192.168.200.202 → 10.40.40.202`입니다

가상 서브넷을 통한 액세스가 필요한 각 리소스에 동일한 접근 방식을 적용할 수 있습니다.

이렇게 하면 통신의 양방향이 가상 주소 지정 방식을 유지하고 클라이언트가 연결을 설정할 때 사용한 것과 동일한 가상 IP 주소로부터 응답을 받게 됩니다.

관련 정보

Cisco Secure Access NAT 매핑/네트워크 터널 그룹 구성:
https://securitydocs.cisco.com/docs/csa/olh/168842.dita

Cisco Secure Access Network Tunnel Group 구성 및 라우팅 참조:
https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Cisco Secure Access 문제 해결 및 기본 데이터 수집 가이드:
https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

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.