# 수동 방법을 사용하여 보안 서비스 에지와 SD-WAN 간에 프라이빗 앱 상호 연결 구성

## 목차



## 소개

이 문서에서는 SD-WAN 라우터를 통해 Cisco Secure Access를 연결하는 방법에 대한 종합적인 가이드로서 보안 프라이빗 앱 액세스를 중심으로 설명합니다.

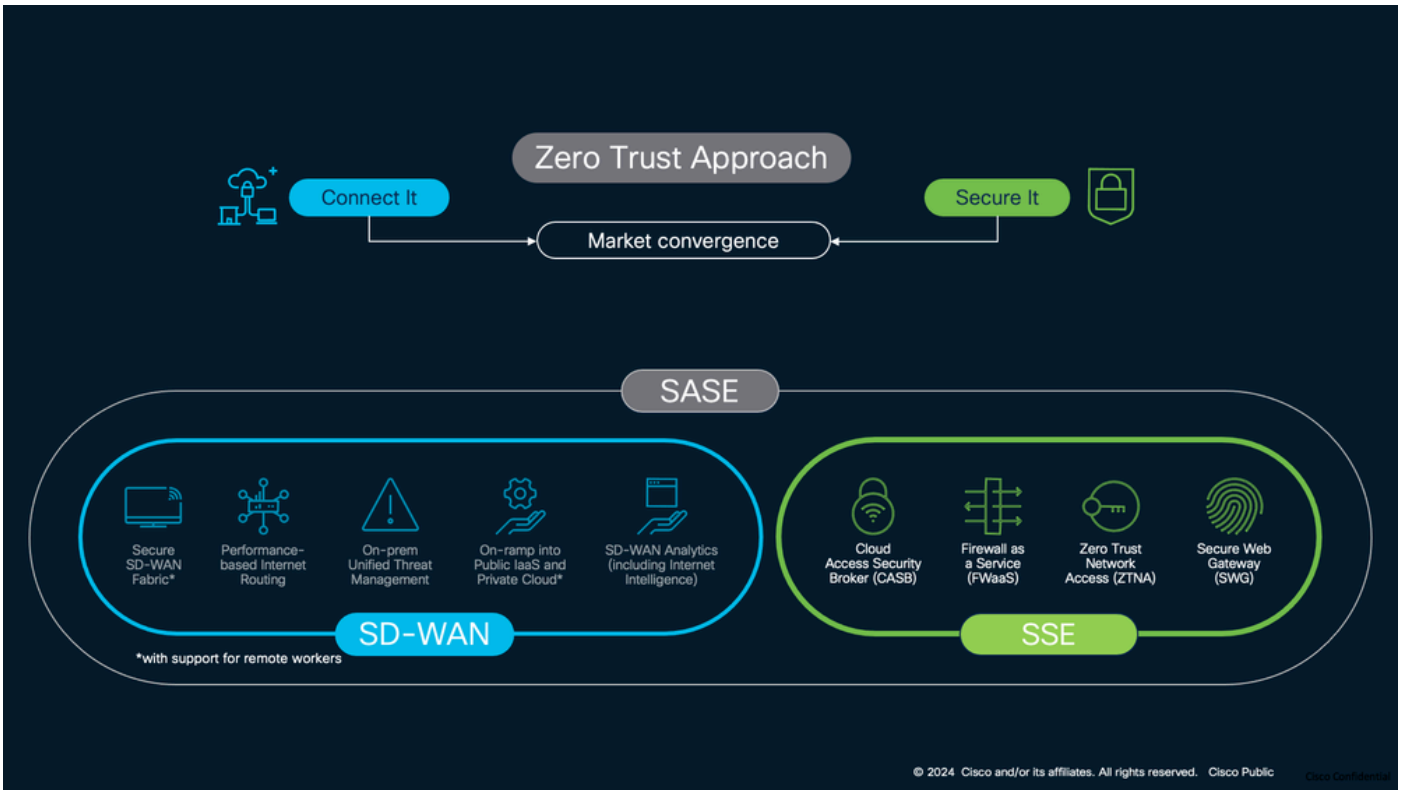
## 가이드 정보

> 참고: 여기에 나열된 컨피그레이션은 SD-WAN의 UX1.0 및 17.9/20.9 버전용으로 개발되었습니다.

이 설명서에서는 다음 주요 단계를 체계적으로 살펴봅니다.

- NTG(Network Tunnel Group) 정의
- IPSec 터널 구성: Cisco SD-WAN 라우터와 Cisco Secure Access NTG 간의 보안 IPSec 터널 설정에 대한 자세한 지침입니다.
- BGP 인접 디바이스: 동적 라우팅과 향상된 네트워크 탄력성을 보장하기 위해 IPSec 터널을 통해 BGP 네이버를 실행하기 위한 단계별 절차.
- 프라이빗 애플리케이션 액세스: 설정된 터널을 통해 프라이빗 애플리케이션에 대한 액세스를 구성하고 보호하는 방법에 대한 지침.

그림 1: Cisco SD-WAN 및 SSE 제로 트러스트 방식




SD-WAN을 사용하는 SSE

이 설명서에서는 NTG 상호 연결을 위한 설계 고려 사항 및 구축 모범 사례에 대해 중점적으로 설명합니다. 이 가이드에서는 SD-WAN 컨트롤러가 클라우드에 구축되고 WAN 에지 라우터가 데이터 센터에 구축되며 하나 이상의 인터넷 회로에 연결됩니다.

### 주요 가정

- Cisco SSE(Secure Access Secure Service Edge): 조직에 대해 Cisco Secure Access SSE가 이미 프로비저닝된 것으로 가정합니다.
- Cisco SD-WAN WAN 에지 라우터: WAN 에지 라우터는 오버레이 네트워크에 통합되어 SD-WAN 인프라 전체에서 사용자 트래픽을 효율적으로 촉진하는 것으로 가정됩니다.
- 이 설명서는 주로 설계 및 구성의 SD-WAN 측면에 초점을 맞추지만, 기존 네트워크 아키텍처 내에서 Cisco Secure Access 솔루션을 통합하는 전체적인 접근 방식을 제공합니다.

## 이 솔루션 정보

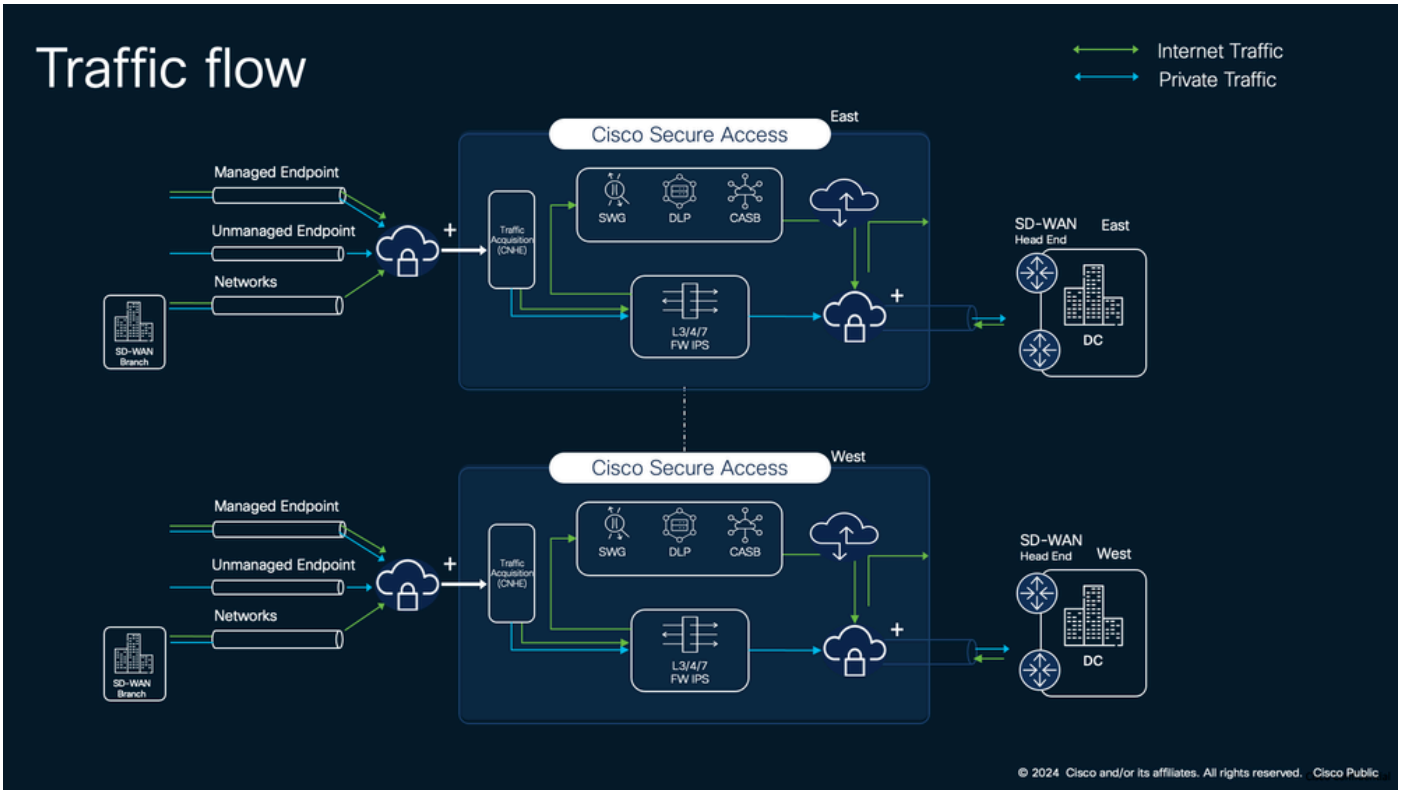
Cisco Secure Access에서 제공하는 프라이빗 앱 터널은 ZTNA(Zero Trust Network Access) 및 VPNaaS(VPN as a Service)를 통해 연결하는 사용자에게 프라이빗 애플리케이션에 대한 보안 연결을 제공합니다. 이러한 터널을 통해 조직은 원격 사용자를 데이터 센터 또는 프라이빗 클라우드에 호스팅된 프라이빗 리소스에 안전하게 연결할 수 있습니다.
이러한 터널 그룹은 IKEv2(Internet Key Exchange 버전 2)를 사용하여 Cisco Secure Access와 SD-WAN 라우터 간에 안전한 양방향 연결을 설정합니다. 동일한 그룹 내의 여러 터널을 통해 고가용성을 지원하고 고정 및 BGP(Dynamic Routing)를 통해 유연한 트래픽 관리를 제공합니다.
IPsec 터널은 다음을 비롯한 다양한 소스의 트래픽을 전달할 수 있습니다.

- 원격 액세스 VPN 사용자

- 브라우저 기반 또는 클라이언트 기반 ZTNA 연결
- Cisco Secure Access에 연결된 다른 네트워크 위치

이러한 접근 방식을 통해 조직은 모든 유형의 프라이빗 애플리케이션 트래픽을 암호화된 통합 채널을 통해 안전하게 라우팅하여 보안 및 운영 효율성을 모두 개선할 수 있습니다.
Cisco SSE(Security Service Edge) 솔루션의 일부인 Cisco Secure Access는 단일 클라우드 매니지드 콘솔, 통합 클라이언트, 중앙 집중식 정책 생성 및 종합 보고를 통해 IT 운영을 간소화합니다. ZTNA, SWG(Secure Web Gateway), CASB(Cloud Access Security Broker), FWaaS(Firewall as a Service), DNS 보안, RBI(Remote Browser Isolation) 등 여러 보안 모듈을 하나의 클라우드 제공 솔루션에 통합합니다. 이 포괄적인 접근 방식은 제로 트러스트 원칙을 적용하고 세분화된 보안 정책을 시행하여 보안 위험을 완화합니다

그림 2: Cisco Secure Access와 프라이빗 앱 간의 트래픽 흐름




SSE 프라이빗 앱 트래픽 흐름

이 가이드에 설명된 솔루션은 데이터 센터의 SD-WAN 라우터와 SSE(Security Service Edge) 측의 NTG(Network Tunnel Group)를 모두 포함하는 포괄적인 이중화 고려 사항을 다룹니다. 이 설명서는 무중단 트래픽 흐름을 유지하고 고가용성을 보장하는 활성/활성 SD-WAN 허브 구축 모델을 중점적으로 다룹니다.

---

# 사전 요구 사항

## 요구 사항

다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco SD-WAN 구성 및 관리
- IKEv2 및 IPSec 프로토콜에 대한 기본 지식
- Cisco Secure Access 포털의 네트워크 터널 그룹 구성
- BGP 및 ECMP에 대한 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 20.9.5a의 Cisco SD-WAN 컨트롤러
- 17.9.5a의 Cisco SD-WAN Wan Edge Router
- Cisco Secure Access 포털

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.

---

## 설계

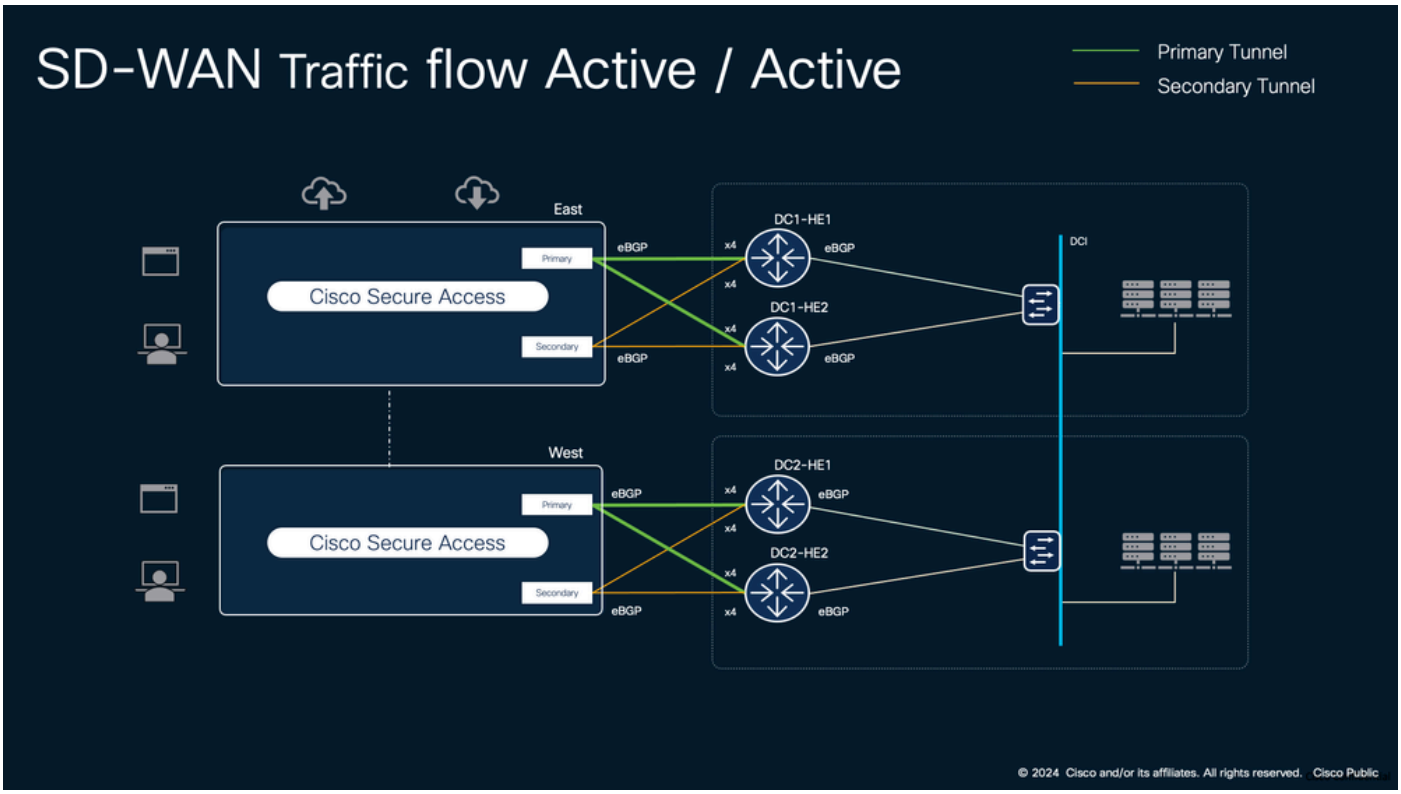
이 가이드에서는 SD-WAN 헤드엔드 라우터에 액티브/액티브 설계 모델을 사용하는 솔루션에 대해 설명합니다. SD-WAN 헤드 엔드 라우터의 컨텍스트에서 활성/활성 설계 모델은 그림 3에 표시된 것처럼 데이터 센터의 두 라우터(둘 다 SSE(Security Service Edge) NTG(Network Tunnel Group)에 연결됨)를 가정합니다. 이 시나리오에서는 데이터 센터의 두 SD-WAN 라우터(DC1-HE1 및 DC1-HE2)가 모두 트래픽 흐름을 능동적으로 처리합니다. 이러한 작업은 동일한 ASPL(AS Path Length)을 내부 DC 네이버에 전송하여 이루어집니다. 따라서 DC 로드 내에서 발생하는 트래픽은 두 헤드엔드 간에 밸런싱됩니다.

각 헤드엔드 라우터는 SSE POP(Points of Presence)에 대한 여러 터널을 설정할 수 있습니다. 터널 수는 요구 사항 및 SD-WAN 디바이스 모델에 따라 달라집니다. 이 설계에서는 다음을 수행합니다.

- 각 라우터에는 기본 SSE 허브에 대한 4개의 터널과 보조 SSE 허브에 대한 4개의 터널이 있습니다.
- 각 SSE 허브가 지원하는 최대 터널 수는 달라질 수 있습니다. 최신 정보는 다음 공식 문서를 참조하십시오. https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

이러한 헤드엔드 라우터는 SSE를 향하는 터널을 통해 BGP 인접 관계를 형성합니다. 헤드엔드는 이러한 네이버십을 통해 프라이빗 애플리케이션 접두사를 SSE 네이버에 광고하여 트래픽을 프라이빗 리소스로 안전하고 효율적으로 라우팅할 수 있도록 합니다.

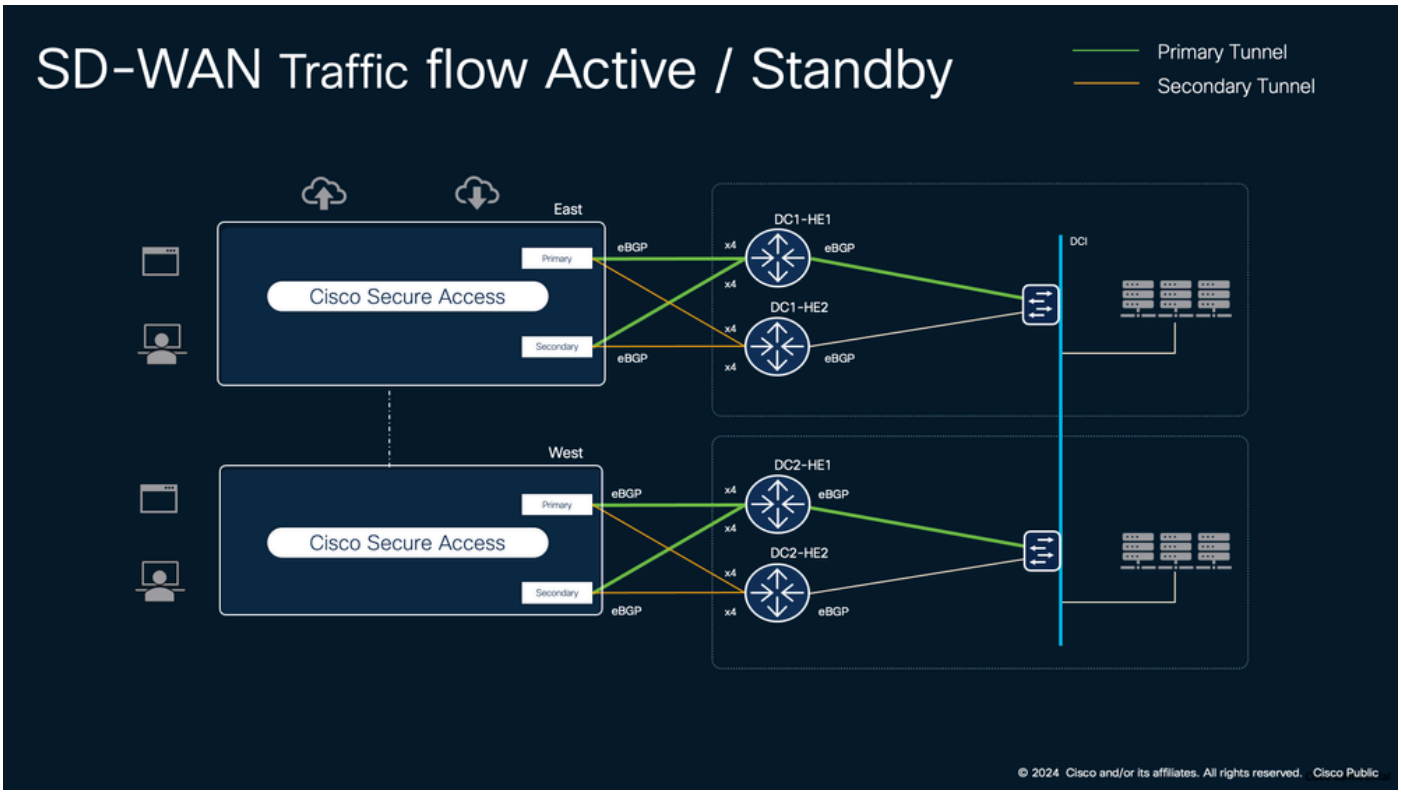
그림 3: SD-WAN to SSE Active/Active 구축 모델




SD-WAN to SSE Active/Active 구축 모델

액티브/스탠바이 설계에서는 하나의 라우터(DC1-HE1)를 항상 액티브 상태로 지정하고 보조 라우터(DC1-HE2)는 스탠바이 상태로 유지합니다. 완전히 장애가 발생하지 않는 한, 트래픽은 지속적으로 액티브 헤드엔드(DC1-HE1)를 통해 흐릅니다. 이 구축 모델의 단점은 다음과 같습니다. sse에 대한 기본 터널이 다운되면 트래픽은 DC1-HE2를 통해서만 보조 SSE 터널로 전환되어 모든 상태 저장 트래픽이 재설정됩니다.
액티브/스탠바이 모델에서 BGP AS-Path Length는 DC 내에서 그리고 SSE를 향해 트래픽을 전달하는 데 사용됩니다. DC1-HE1은 ASPL 2로 SSE BGP 인접 디바이스에 접두사 업데이트를 전송하는 반면 DC1-HE2는 ASPL 3으로 업데이트를 전송합니다. DC1-HE1의 내부 DC 인접 디바이스는 DC1-HE2보다 AS 경로 길이가 짧은 접두사를 광고하여 DC1-HE1에 대한 트래픽 기본 설정을 보장합니다. 고객은 트래픽 기본 설정에 영향을 줄 다른 특성이나 프로토콜을 선택할 수 있습니다.
고객은 특정 요구 사항에 따라 Active/Active 또는 Active/Standby 구축 모델을 선택할 수 있습니다.

그림 4: SD-WAN에서 SSE 액티브/스탠바이 구축 모델




SD-WAN에서 SSE 액티브/스탠바이 구축 모델

---

# 구성

이 섹션에서는 다음 절차에 대해 설명합니다.

1. Cisco Secure Access 포털에서 네트워크 터널 그룹을 프로비저닝하기 위한 사전 요구 사항을 확인합니다.
2. IPsec 수동 방법을 사용하여 Cisco NTG(Secure Access Network Tunnel Group)를 사용하여 SD-WAN 상호 연결을 구성합니다.
3. BGP 인접 디바이스 구성

---

참고: 이 컨피그레이션은 액티브/액티브 구축 모델을 기반으로 합니다

---

## 절차 1. Cisco Secure Access Portal에서 네트워크 터널 그룹 컨피그레이션 확인

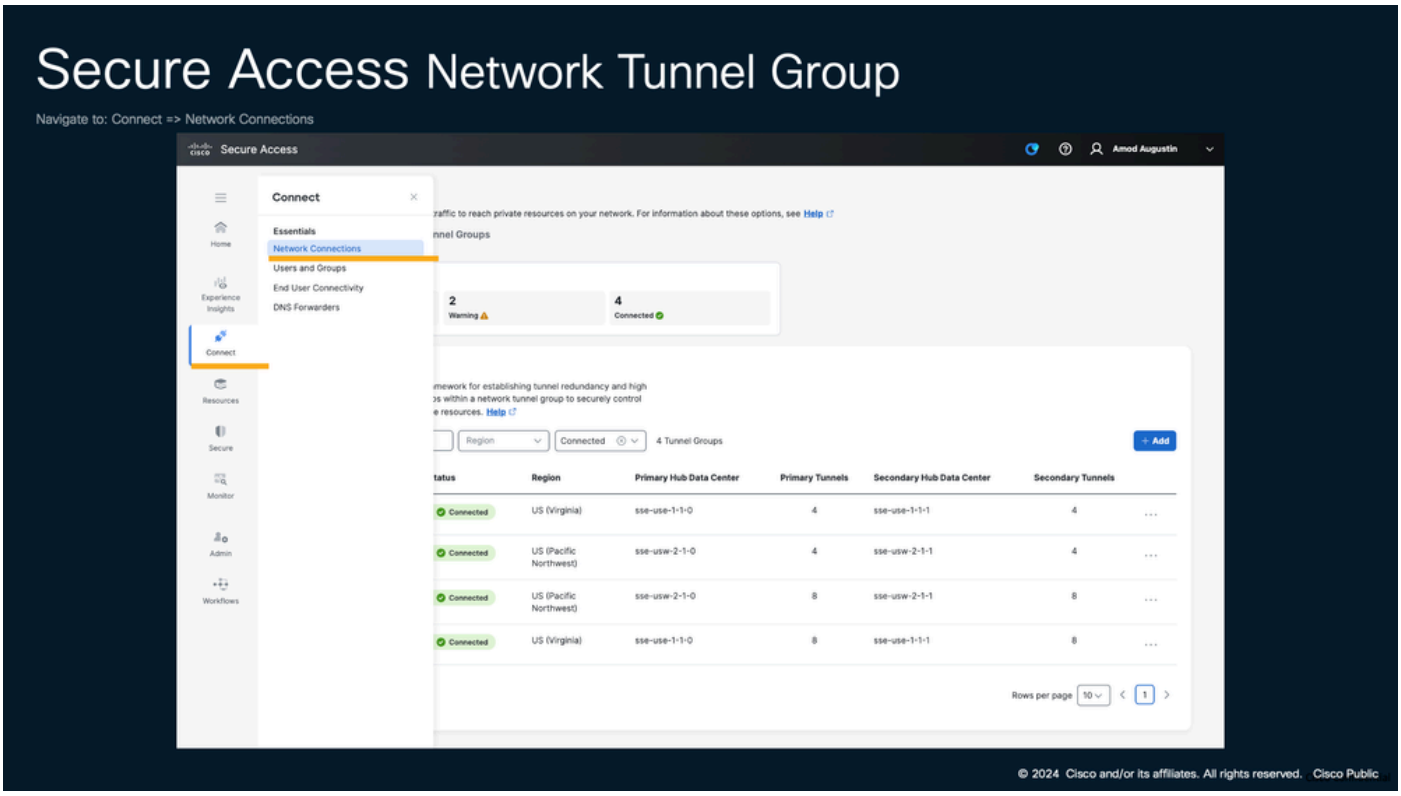
네트워크 터널 그룹을 구성하는 방법은 설명서에서 다루지 않습니다. 이 참조를 검토하십시오.

- 네트워크 터널 그룹 추가: SSE 설명서
- ECMP와 BGP를 사용하여 Cisco Secure Access와 Cisco IOS XE Router 간의 네트워크 터널 구성

Cisco Secure Access(Cisco 보안 액세스)로 이동하여 NTG(Network Tunnel Group)가 프로비저닝되었는지 확인합니다. 현재 설계에서는 서로 다른 두 POP(Point of Presence)에서 NTG를 프로비저닝해야 합니다. 이 가이드에서는 미국(버지니아) POP 및 미국(태평양 북서부) POP의 NTG를 사용합니다.

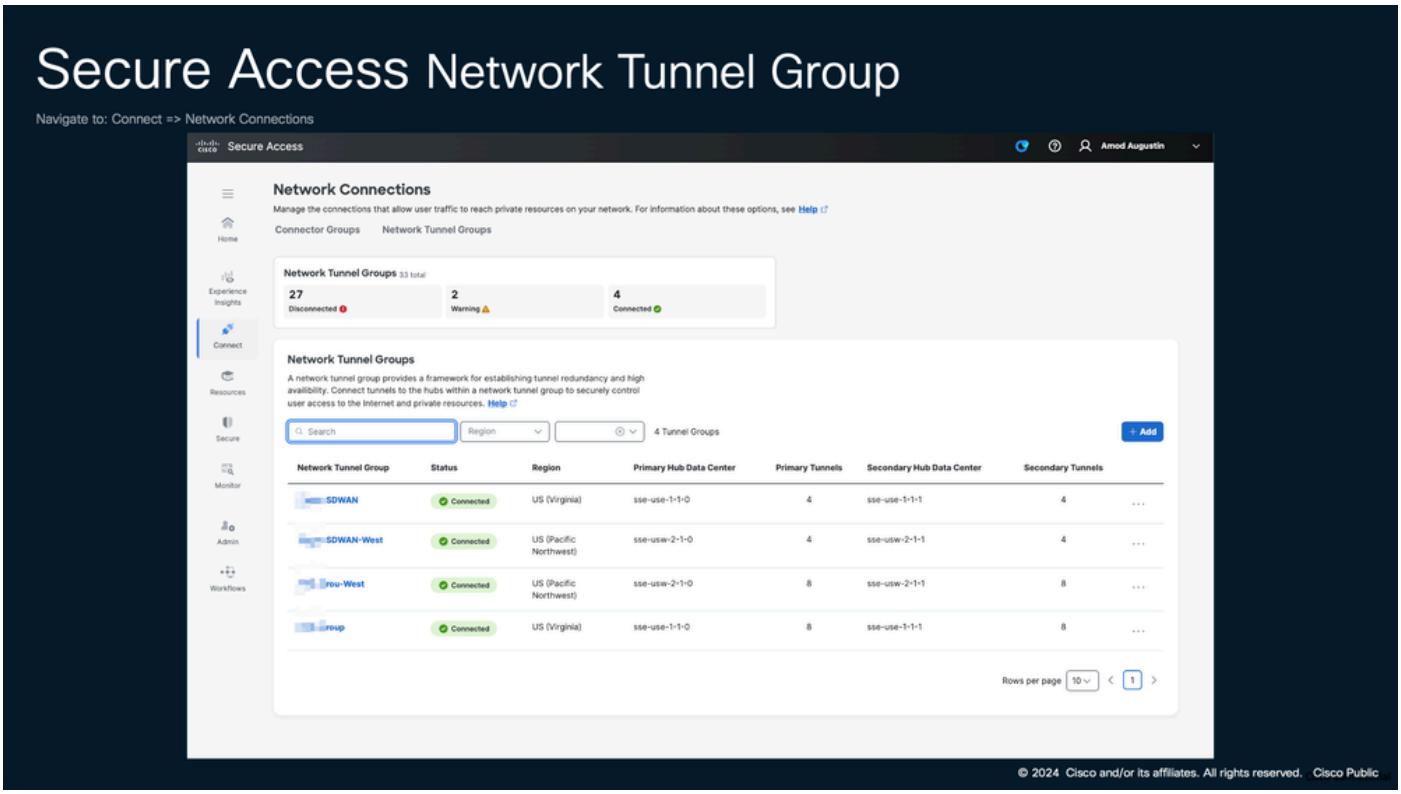
참고: POP의 이름과 위치는 다를 수 있지만, 핵심 개념은 데이터 센터와 지리적으로 가까운 위치에 여러 NTG를 프로비저닝하는 것입니다. 이러한 접근 방식은 네트워크 성능을 최적화하고 이중화를 제공합니다.

그림 5: Cisco Secure Access Network 터널 그룹




Cisco Secure Access Network 터널 그룹

그림 6: Cisco 보안 액세스 네트워크 터널 그룹 목록




보안 액세스 네트워크 터널 그룹 목록

터널 패스프레이즈를 기록했는지 확인합니다(터널 생성 중 한 번만 표시됨).

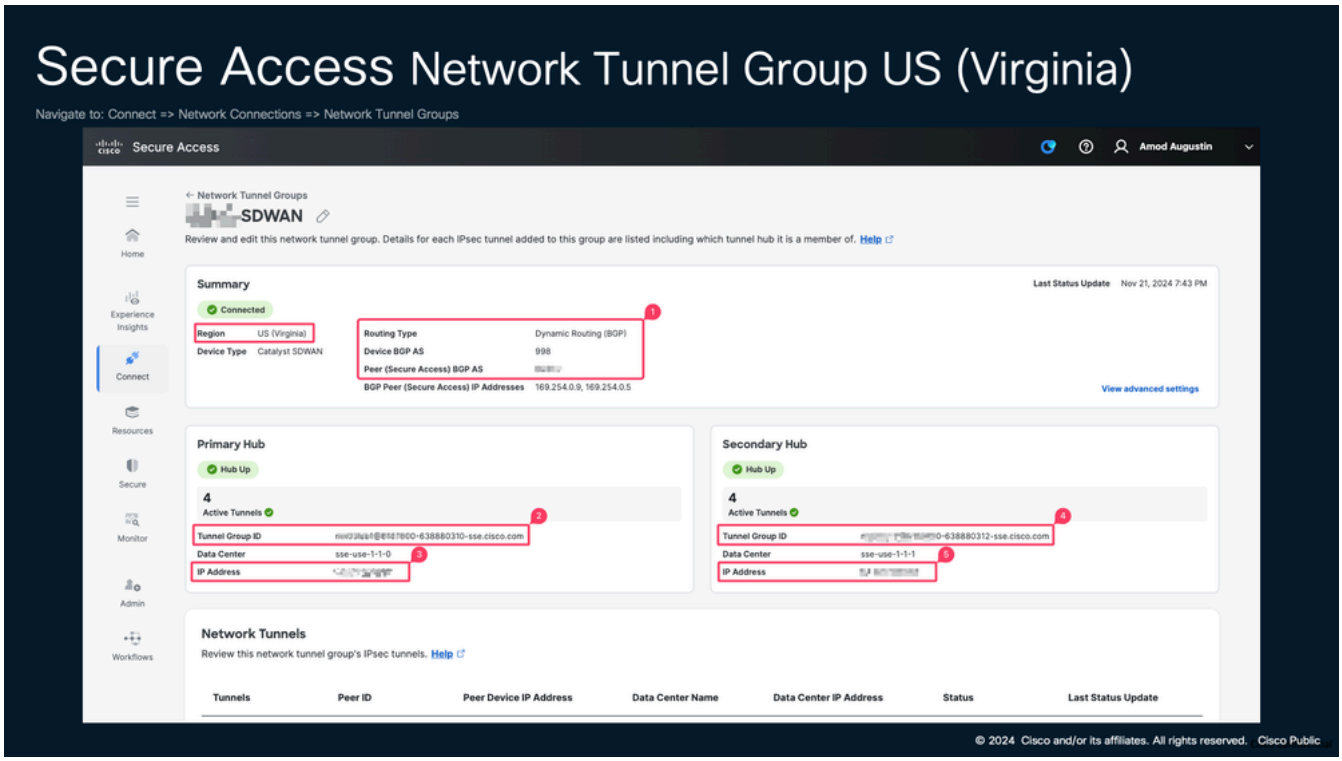
---

참고: 네트워크 터널 그룹 추가의 6단계

---

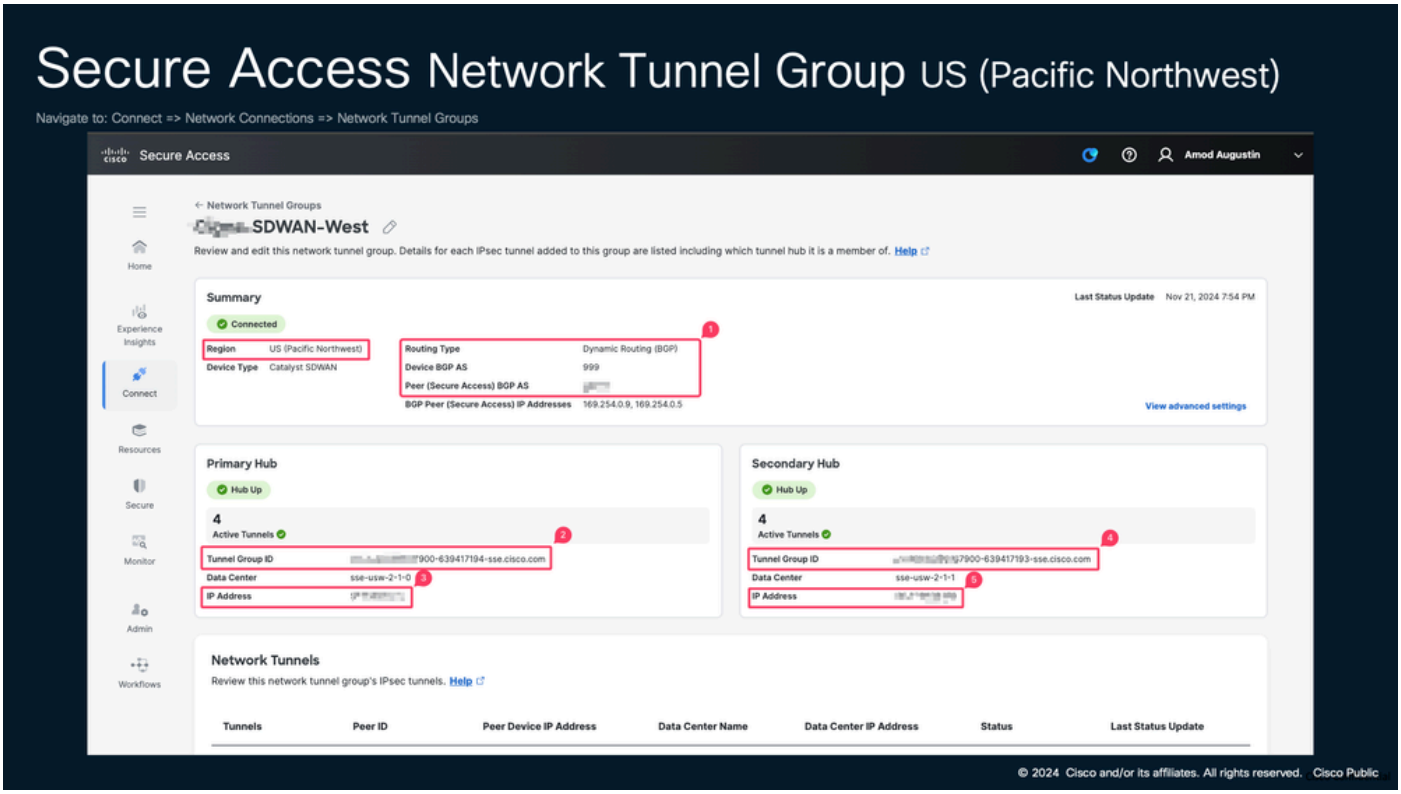
또한 IPSec 컨피그레이션 중에 사용하는 터널 그룹 특성도 기록해 둡니다. 이 스크린샷(그림 6)은 랩 환경에서 프로덕션 시나리오가 설계 또는 사용 권장 사항에 따라 NTG 그룹을 생성하도록 했습니다.

그림 7: Secure Access Network Tunnel Group US(버지니아)




Secure Access Network Tunnel Group US(버지니아)

그림 8: Secure Access Network Tunnel Group US(Pacific Northwest)



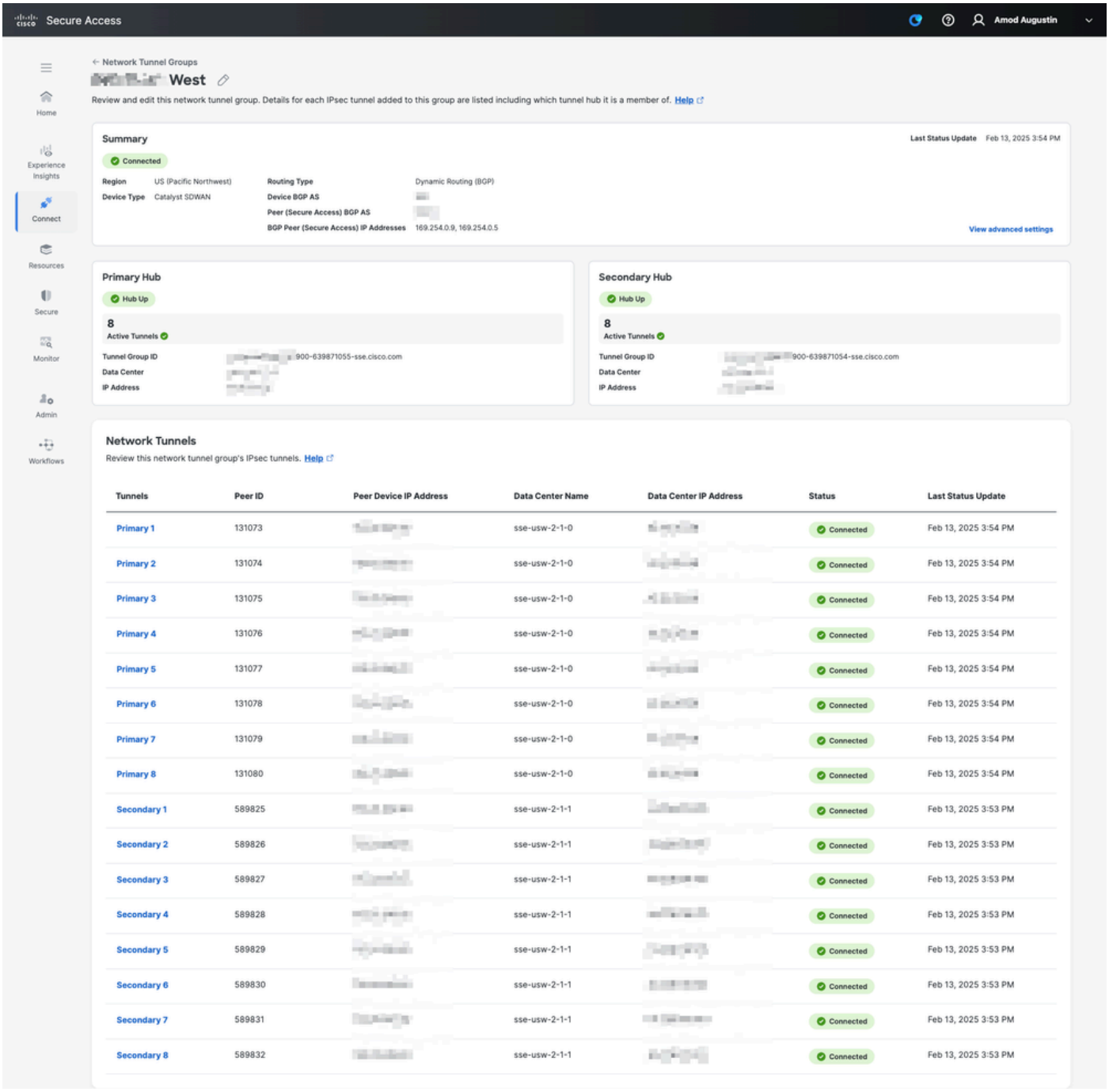

Secure Access Network Tunnel Group US(태평양 북서부)

그림 8에는 기본 및 보조 허브 모두에 있는 터널이 4개만 나와 있습니다. 그러나 컨트롤러 환경에서 최대 8개의 터널이 성공적으로 테스트되었습니다. 최대 터널 지원은 사용하는 하드웨어 디바이스 및 현재 SSE 터널 지원에 따라 달라질 수 있습니다. 최신 정보는 다음 공식 문서를 참조하십시오. https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels 및 해당 하드웨어

장치의 릴리스 정보입니다.

8 터널 설정에 대한 예는 여기에 나와 있습니다.

그림 8a: NTG 터널 최대 8개




SSE NTG 최대 8개 터널

## 절차 2. IPsec 수동 방법을 사용하여 Cisco NTG(Secure Access Network Tunnel Group)를 사용하여 SD-WAN 상호 연결을 구성합니다.

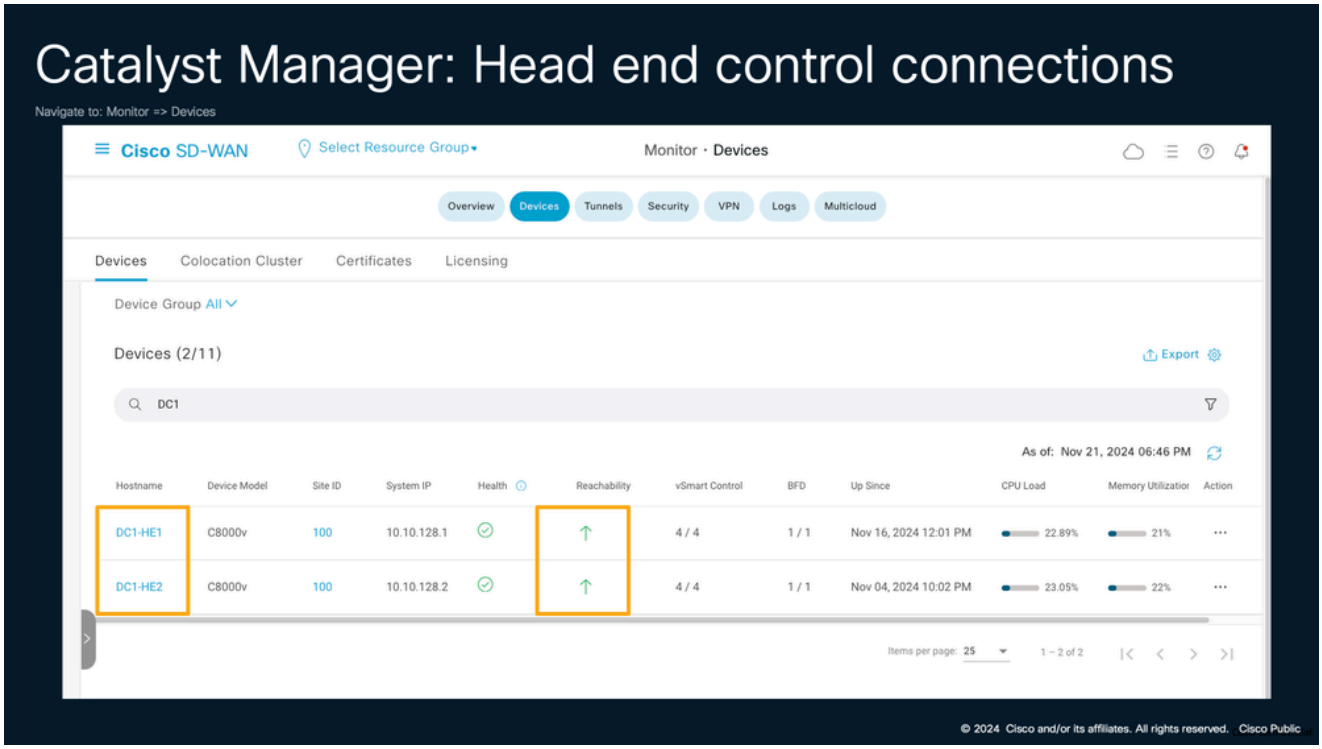
이 절차에서는 Cisco Catalyst SD-WAN Manager 20.9 및 17.9 릴리스를 실행하는 Cisco Catalyst Edge Router에서 기능 템플릿을 사용하여 NTG(Network Tunnel Group)를 연결하는 방법을 보여 줍니다.

참고:이 가이드에서는 허브가 데이터 센터에서 호스팅되는 사설 애플리케이션에 대한 액세스 엔트리 포인트 역할을 하는 허브 앤 스포크(hub-and-spoke) 또는 풀 메시(fully mesh) 토폴로지를 사용하는 기존 SD-WAN 오버레이 구축을 가정합니다. 이 절차는 지사 또는 클라우드 구축에도 적용할 수 있습니다.

계속하기 전에 사전 요구 사항이 충족되었는지 확인합니다.

1. Cisco Catalyst SD-WAN Manager에서 필요한 업데이트를 허용하기 위해 디바이스에서 제어 연결이 활성화됩니다.

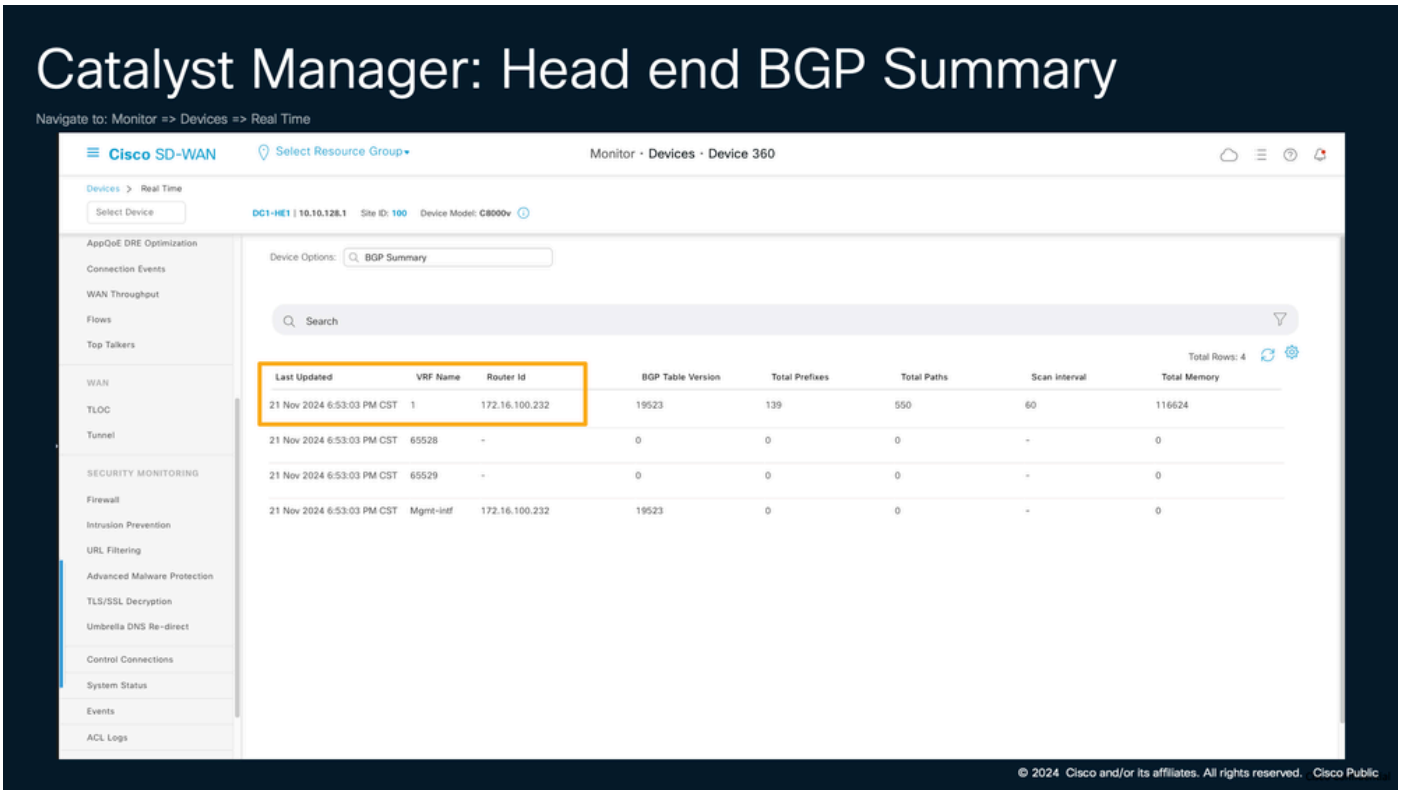
   그림 9: Cisco Catalyst SD-WAN Manager: 헤드 엔드 제어 연결




   Catalyst 관리자: 헤드 엔드 제어 연결

2. 서비스 측 VPN이 구성되고 라우팅 프로토콜을 사용하여 접두사를 알립니다. 이 가이드에서는 서비스 측의 라우팅 프로토콜로 BGP를 사용합니다.

그림 10: Cisco Catalyst SD-WAN Manager: 헤드 엔드 BGP 요약




수동 IPSec 방법을 사용하여 NTG(Network Tunnel Group)를 사용하여 SD-WAN 상호 연결을 구성하는 절차는 다음과 같습니다.

---

✎ 참고: 구축에 필요한 터널 수에 대해 이 단계를 반복합니다.

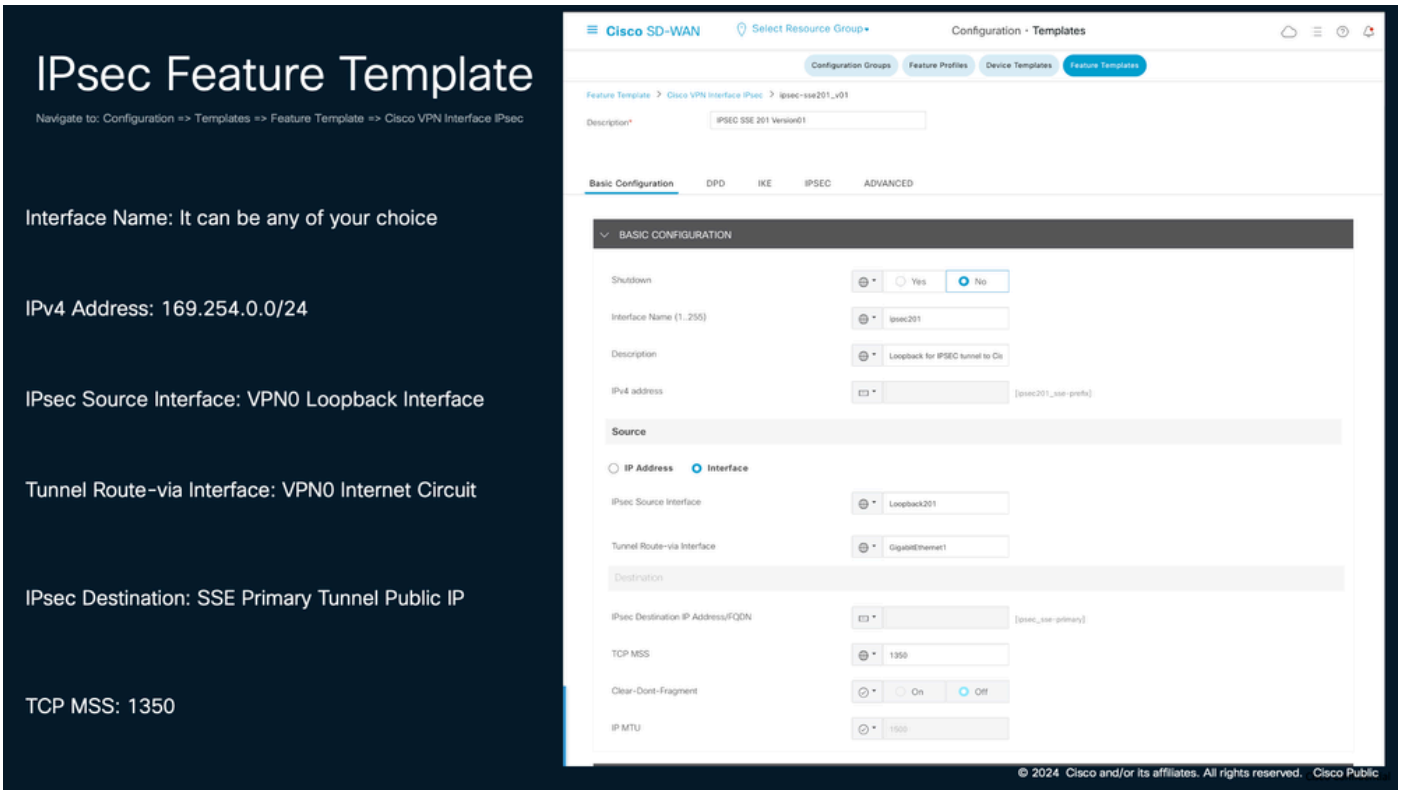
---

터널 제한에 대한 공식 문서를 참조하십시오. https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

다음 단계에서는 DC1-HE1(데이터 센터 1 헤드 엔드 1)을 SSE Virginia 기본 허브에 연결하는 프로세스를 자세히 설명합니다. 이 컨피그레이션은 데이터 센터의 SD-WAN 라우터와 버지니아 POP(Point of Presence)에 있는 Cisco NTG(Secure Access Network Tunnel Group) 간에 보안 터널을 설정합니다

1단계: IPSec 기능 템플릿 만들기
SD-WAN 헤드 엔드 라우터를 NTG에 연결하는 IPSec 터널의 매개변수를 정의하려면 IPSec 기능 템플릿을 생성합니다.

그림 11: IPsec 기능 템플릿: 기본 설정




IPsec 기능 템플릿: 기본 설정

인터페이스 이름: 원하는 대로 선택할 수 있습니다.
IPv4 주소: SSE는 169.254.0.0/24을 수신 대기합니다. 원하는 서브넷으로 서브넷을 나눌 수 있는 요구 사항을 기준으로 합니다. 모범 사례로서 /30과 함께 사용하십시오. 이 가이드에서는 나중에 사용할 수 있도록 첫 번째 블록을 제외합니다.

IPsec 소스 인터페이스: 현재 IPsec 인터페이스에 대해 고유한 VPN0 루프백 인터페이스를 정의합니다. 일관성 및 문제 해결을 위해 동일한 번호 지정을 유지하는 것이 좋습니다.
터널 라우트 경유 인터페이스: SSE에 연결하기 위한 언더레이로 사용할 수 있는 인터페이스를 가리킵니다(인터넷 액세스가 있어야 함).

IPsec 대상:  기본 허브 IP 주소

그림 7: Secure Access Network Tunnel Group US(버지니아) 35.171.214.188을 참조하십시오.

TCP MSS: 1350이어야 합니다(참조: [https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters).](https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters).

예: SSE Virginia 기본 허브를 향하는 DC1-HE1

인터페이스 이름: ipsec201

설명: Cisco에 대한 IPSEC 터널의 루프백

IPv4 주소: 169.254.0.x/30

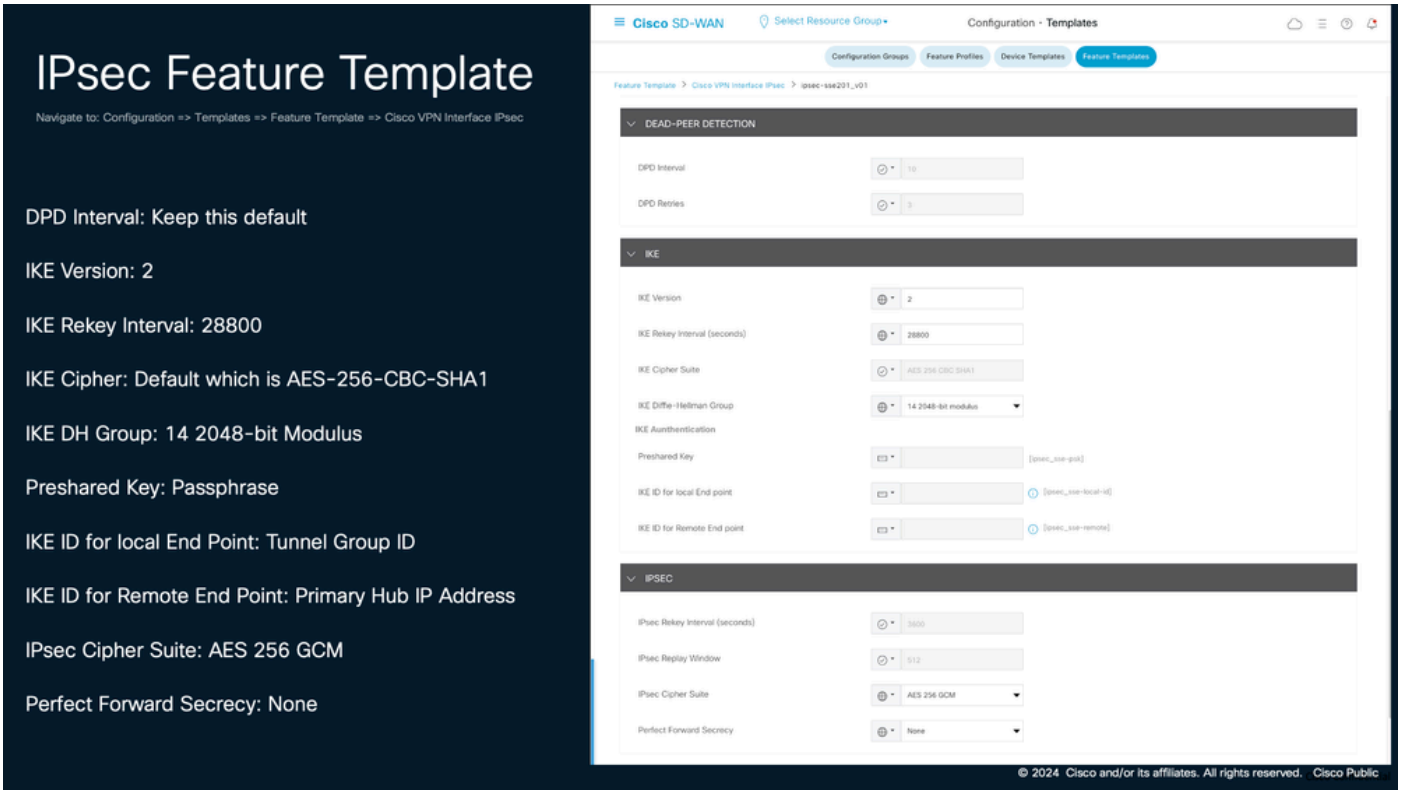
IPsec 소스 인터페이스: 루프백201

Tunnel Route-via Interface: GigabitEthernet1

IPsec 대상 IP 주소/FQDN: 35.xxx.xxx.xxx

TCP MSS: 1350

그림 12: IPsec 기능 템플릿: IKE IPSEC




IPsec 기능 템플릿: IKE IPSEC

DPD 간격: 이 기본값 유지
IKE 버전: 2
IKE 키 재설정 간격: 28800
IKE 암호: 기본값(AES-256-CBC-SHA1)
IKE DH 그룹: 14 2048비트 모듈러스
사전 공유 키: 암호
로컬 엔드포인트의 IKE ID: 터널 그룹 ID

그림 7: Secure Access Network Tunnel Group US(Virginia), mn03lab1+201@8167900-638880310-sse.cisco.com 참조

---

참고: 각 터널에는 이에 대한 고유한 엔드포인트가 있어야 합니다. "+루프백ID" 사용 예: mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com 등입니다.

---

원격 엔드포인트의 IKE ID: 기본 허브 IP 주소
IPsec 암호 그룹: AES 256GCM
PFS(Perfect Forward Secrecy): 없음

참조: https://docs.sse.cisco.com/sse-user-guide/docs/configure-tunnels-with-catalyst-sdwan#define-the-feature-template

예:

IKE 버전: 2
IKE 키 재설정 간격: 28800
IKE 암호: AES-256-CBC-SHA1
IKE DH 그룹: 14 2048비트 모듈러스
사전 공유 키: *****

---

참고: 네트워크 터널 그룹 추가의 6단계

---

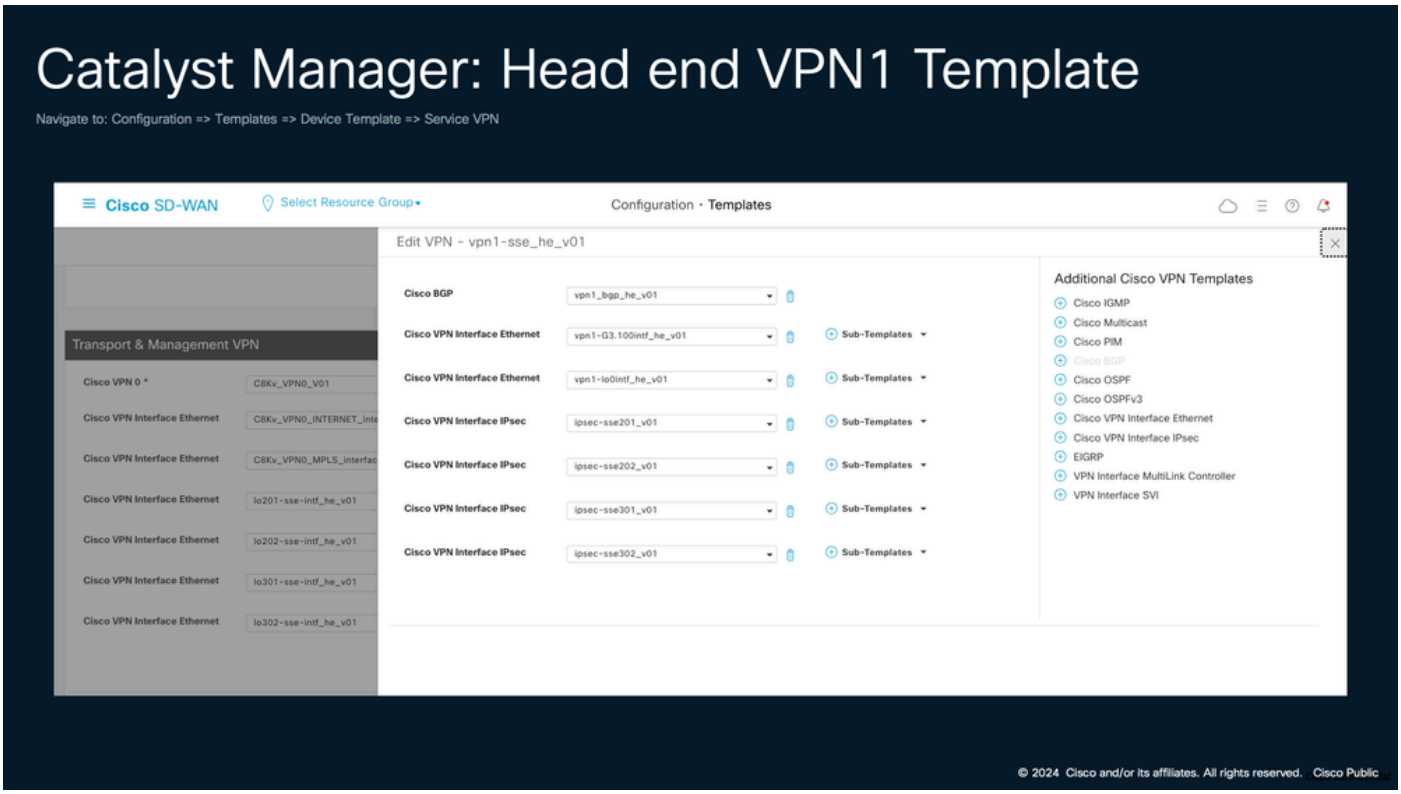
로컬 엔드포인트의 IKE ID: mn03lab1@8167900-638880310-sse.cisco.com
원격 엔드포인트의 IKE ID: 35.171.xxx.xxx
IPsec 암호 그룹: AES 256GCM
PFS(Perfect Forward Secrecy): 없음

기본 및 보조 Secure Access Hub 모두에 필요한 터널을 구성하려면 단계를 반복합니다.2x2 설정의 경우 총 4개의 터널을 생성할 수 있습니다.

- DC1-HE1에서 기본 Secure Access 허브로 이동하는 터널 2개
- DC1-HE1에서 보조 Secure Access 허브로 이동하는 터널 2개

이제 템플릿이 만들어졌으므로 그림 13의 서비스 측 vrf에, 그림 14의 글로벌 vrf에 연결된 루프백에 템플릿을 사용합니다.

그림 13: Catalyst SD-WAN Manager: 헤드 엔드 VPN1 템플릿 2x2




Catalyst 관리자: 헤드 엔드 VPN1 템플릿

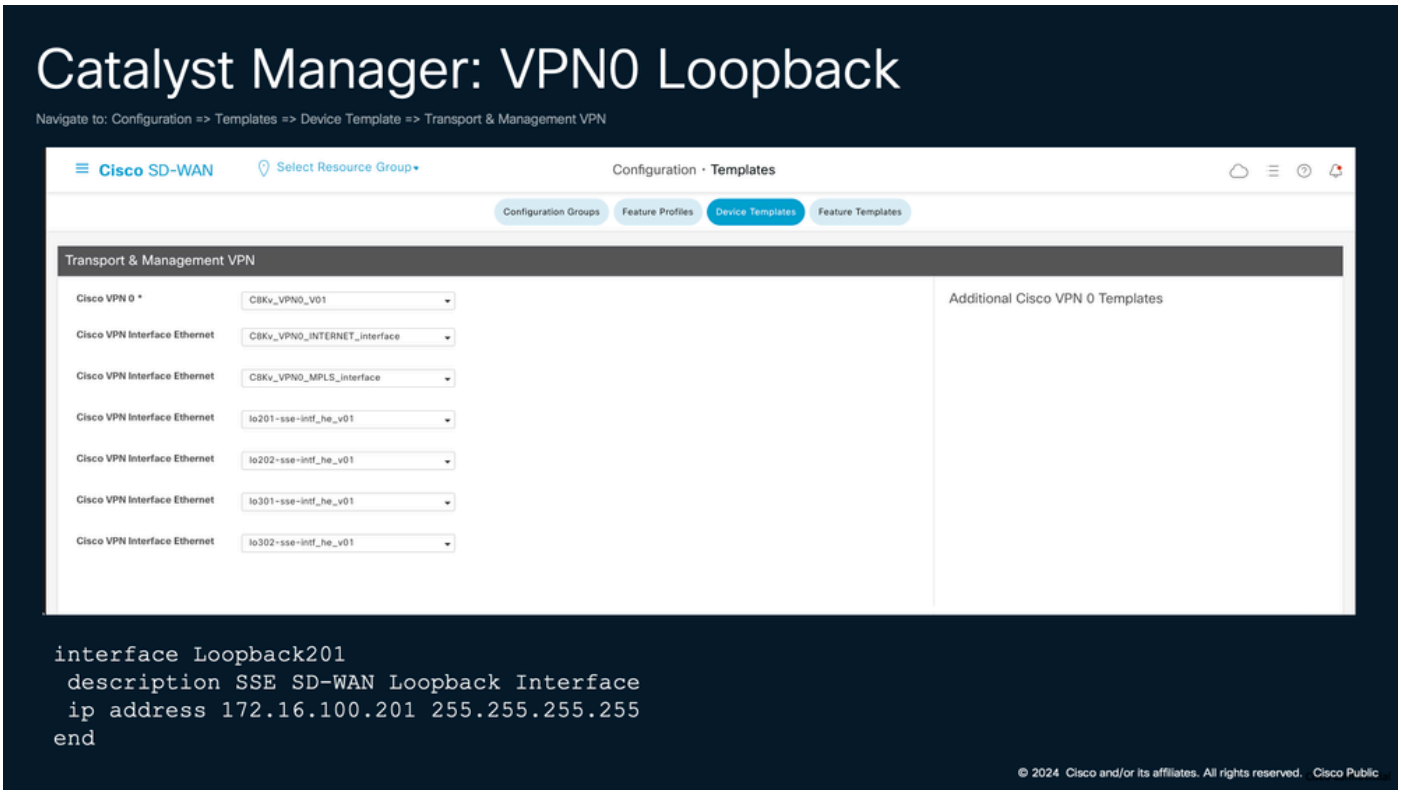
2단계: 전역 VRF에서 루프백 정의

전역 VRF(Virtual Routing and Forwarding) 테이블에서 루프백 인터페이스를 구성합니다. 이 루프백은 1단계에서 생성한 IPSec 터널의 소스 인터페이스 역할을 합니다.

1단계에서 참조되는 모든 루프백은 글로벌 VRF에서 정의되어야 합니다.

IP 주소는 모든 RFC1918 범위에서 정의할 수 있습니다.

그림 14: Catalyst SD-WAN Manager: VPN0 루프백

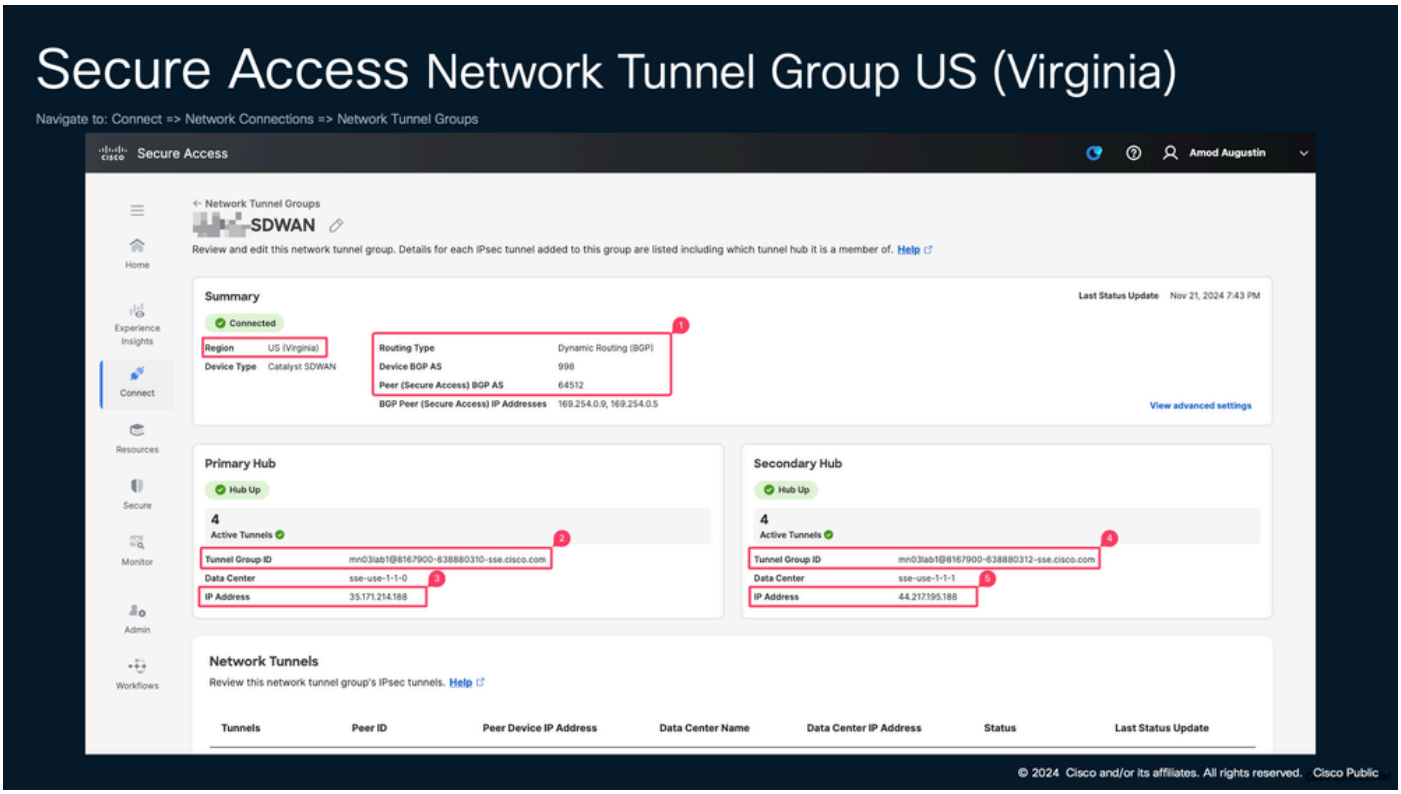



Catalyst 관리자: VPN0 루프백

## 절차 3. BGP 인접 디바이스 구성

Use BGP feature template(BGP 기능 템플릿 사용)은 모든 터널 인터페이스에 대한 BGP 네이버십을 정의합니다. BGP 값을 구성하려면 Cisco 보안 액세스 포털에서 각 네트워크 터널 그룹 BGP 컨피그레이션을 참조하십시오.

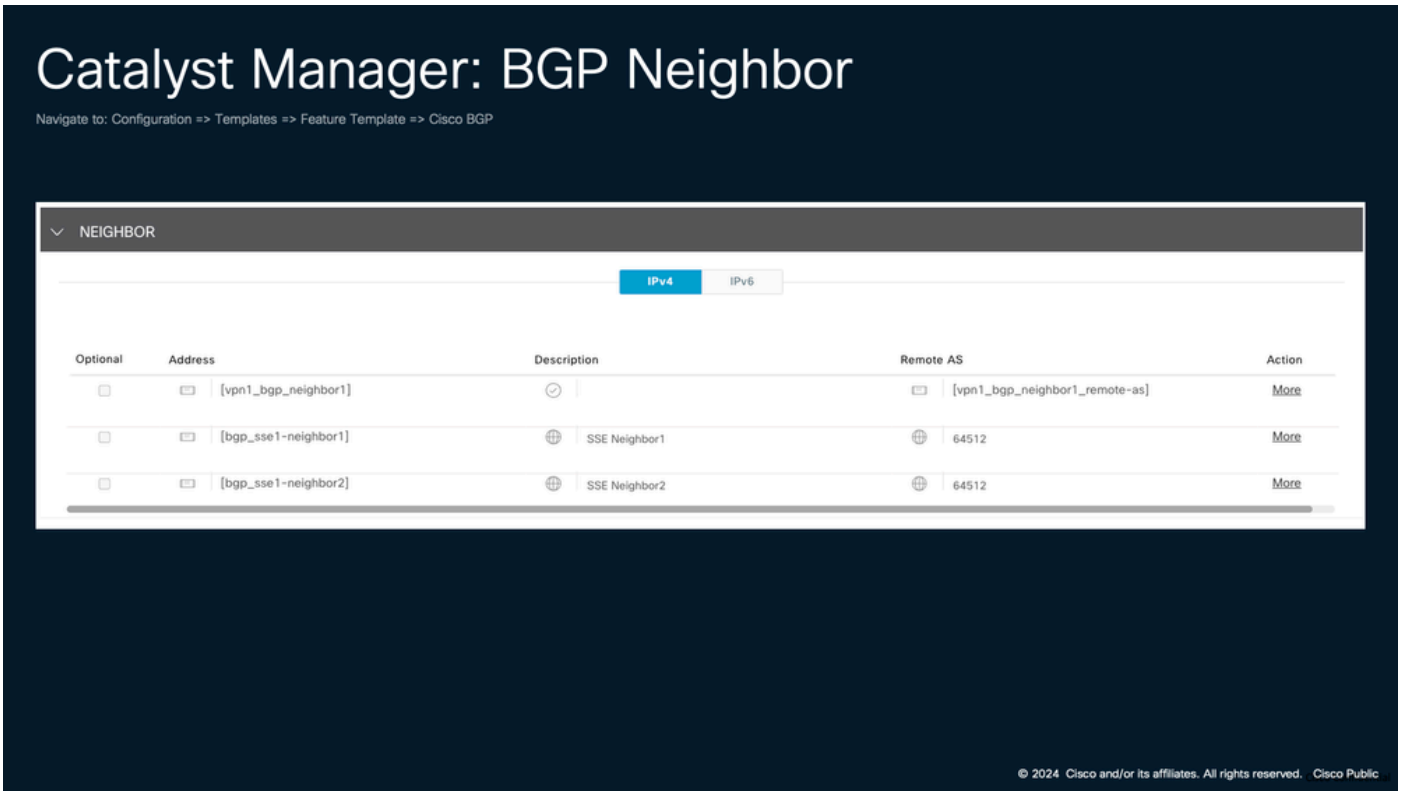
그림 15: Secure Access Network Tunnel Group US(버지니아)




Secure Access Network Tunnel Group US(버지니아)

이 예에서는 그림 15(상자 1)의 정보를 사용하여 기능 템플릿을 사용하여 BGP를 정의합니다.

그림 16: Catalyst SD-WAN Manager BGP 인접 디바이스




Catalyst SD-WAN Manager BGP 인접 디바이스

기능 템플릿을 사용하여 생성된 구성:

```
router bgp 998
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf 1
  network 10.10.128.1 mask 255.255.255.255
  neighbor 169.254.0.5 remote-as 64512
  neighbor 169.254.0.5 description SSE Neighbor1
  neighbor 169.254.0.5 ebgp-multihop 5
  neighbor 169.254.0.5 activate
  neighbor 169.254.0.5 send-community both
  neighbor 169.254.0.5 next-hop-self
  neighbor 169.254.0.9 remote-as 64512
  neighbor 169.254.0.9 description SSE Neighbor2
  neighbor 169.254.0.9 ebgp-multihop 5
  neighbor 169.254.0.9 activate
  neighbor 169.254.0.9 send-community both
  neighbor 169.254.0.9 next-hop-self
  neighbor 169.254.0.105 remote-as 64512
  neighbor 169.254.0.105 description SSE Neighbor3
  neighbor 169.254.0.105 ebgp-multihop 5
  neighbor 169.254.0.105 activate
  neighbor 169.254.0.105 send-community both
  neighbor 169.254.0.105 next-hop-self
  neighbor 169.254.0.109 remote-as 64512
  neighbor 169.254.0.109 description SSE Neighbor4
  neighbor 169.254.0.109 ebgp-multihop 5
  neighbor 169.254.0.109 activate
  neighbor 169.254.0.109 send-community both
  neighbor 169.254.0.109 next-hop-self
  neighbor 172.16.128.2 remote-as 65510
  neighbor 172.16.128.2 activate
  neighbor 172.16.128.2 send-community both
  neighbor 172.16.128.2 route-map sse-routes-in in
  neighbor 172.16.128.2 route-map sse-routes-out out
  maximum-paths eibgp 4
  distance bgp 20 200 20
 exit-address-family
DC1-HE1#
```

# 확인

```
DC1-HE1#show ip route vrf 1 bgp | begin Gateway
Gateway of last resort is not set

35.0.0.0/32 is subnetted, 1 subnets
B 35.95.175.78 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
44.0.0.0/32 is subnetted, 1 subnets
B 44.240.251.165 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
100.0.0.0/8 is variably subnetted, 17 subnets, 2 masks
B 100.81.0.58/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.59/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
```

```
B 100.81.0.60/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.61/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.62/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.63/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.64/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.65/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h

DC1-HE1#show ip bgp vpnv4 all summary
BGP router identifier 172.16.100.232, local AS number 998

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.0.5 4 64512 12787 13939 3891 0 0 4d10h 18
169.254.0.9 4 64512 66124 64564 3891 0 0 3d01h 18
169.254.0.13 4 64512 12786 13933 3891 0 0 4d10h 18
169.254.0.17 4 64512 12786 13927 3891 0 0 4d10h 18
172.16.128.2 4 65510 83956 84247 3891 0 0 7w3d 1

DC1-HE1#show ip interface brief | include Tunnnel
Tunnel1 192.168.128.202 YES TFTP up up
Tunnel4 198.18.128.11 YES TFTP up up
Tunnel100022 172.16.100.22 YES TFTP up up
Tunnel100023 172.16.100.23 YES TFTP up up
Tunnel100201 169.254.0.6 YES other up up
Tunnel100202 169.254.0.10 YES other up up
Tunnel100301 169.254.0.14 YES other up up
Tunnel100302 169.254.0.18 YES other up up
```

# 참조

액티브/액티브 구현에서는 양쪽 SD-WAN 헤드 엔드에 연결된 코어 스위치로부터의 다중 경로가 있습니다.

그림 17: BGP 인접 디바이스에 대한 활성/활성 시나리오

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *m   1.1.1.1/32       172.16.128.5          65535             0 998 ?
 *>                    172.16.128.1          65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5          65535             0 998 ?
 *>                    172.16.128.1          65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5          65535             0 998 ?
 *>                    172.16.128.1          65535             0 998 ?
<snip>
```

활성/활성 BGP 인접 디바이스

액티브/스탠바이 구현에서는 ASPL 앞에 SD-WAN 헤드가 종료되므로 코어 스위치에서 SD-WAN 헤드까지 하나의 액티브 경로가 생깁니다(네이버에 대한 경로 맵을 사용하여 수행).

그림 18: BGP 인접 디바이스에 대한 활성/대기 시나리오

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *    1.1.1.1/32       172.16.128.5             65535             0 998 998?
 *>                    172.16.128.1             65535             0 998 ?
 *    [redacted]32     172.16.128.5             65535             0 998 998?
 *>                    172.16.128.1             65535             0 998 ?
 *    [redacted]/32    172.16.128.5             65535             0 998 998?
 *>                    172.16.128.1             65535             0 998 ?
 <snip>
```

활성/대기 BGP 인접 디바이스

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.