

Configure Private App Interconnect Between Security Service Edge and SD-WAN USING Manual Method

Contents

[Introduction](#)

[About this Guide](#)

[Key Assumptions](#)

[About this solution](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Design](#)

[Configure](#)

[Procedure 1. Verify Network Tunnel Group Configuration on Cisco Secure Access Portal](#)

[Procedure 2. Configure SD-WAN interconnect with Cisco Secure Access Network Tunnel Group \(NTG\) using the IPsec Manual Method.](#)

[Procedure 3. Configure BGP neighborship](#)

[Verification](#)

[Reference](#)

Introduction

This document describes a comprehensive guide for connecting Cisco Secure Access with SD-WAN routers, focusing on secure private app access.

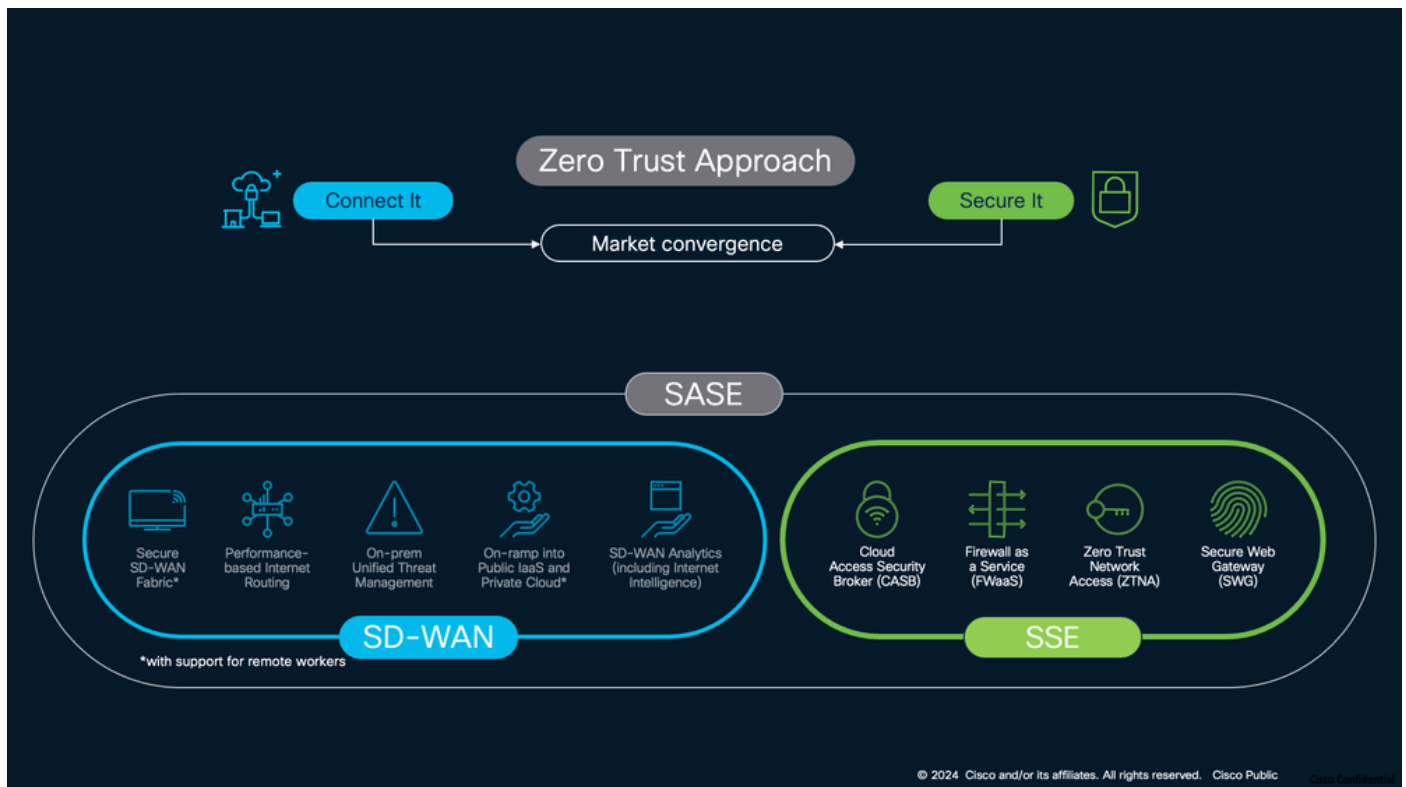
About this Guide

 **Note:** The configurations listed here are developed for UX1.0 and 17.9/20.9 versions of SD-WAN.

This guide presents a structured walkthrough of these key steps:

- Defining Network Tunnel Groups (NTGs)
- IPSec Tunnel Configuration: Detailed instructions on setting up secure IPSec tunnels between Cisco SD-WAN routers and Cisco Secure Access NTGs.
- BGP Neighborship: Step-by-step procedures for running BGP neighborships over the IPSec tunnels to ensure dynamic routing and improved network resilience.
- Private Application Access: Guidance on configuring and securing access to private applications through the established tunnels.

Figure 1: Cisco SD-WAN and SSE Zero Trust Approach



SSE with SD-WAN

This guide focuses on design consideration and deployment best practices for NTG interconnect. In this guide, SD-WAN controllers are deployed in the cloud and WAN Edge routers are deployed at the data center and are connected to atleast one internet circuit.

Key Assumptions

- Cisco Secure Access Secure Service Edge (SSE): It is assumed that Cisco Secure Access SSE is already provisioned for your organization.
- Cisco SD-WAN WAN Edge Router: The WAN Edge router is assumed to be integrated into the overlay network, efficiently facilitating user traffic across the SD-WAN infrastructure.
- While this guide primarily focuses on the SD-WAN aspects of design and configuration, it provides a holistic approach to integrating Cisco Secure Access solutions within your existing network architecture.

About this solution

Private app tunnels, offered by Cisco Secure Access, provide secure connectivity to private applications for users connecting through Zero Trust Network Access (ZTNA) and VPN as a Service (VPNaaS). These tunnels enable organizations to securely link remote users to private resources hosted in data centers or private clouds.

Using IKEv2 (Internet Key Exchange version 2), these tunnel groups establish secure, bidirectional connections between Cisco Secure Access and SD-WAN routers. They support high availability through multiple tunnels within the same group and offer flexible traffic management via both static and dynamic routing (BGP).

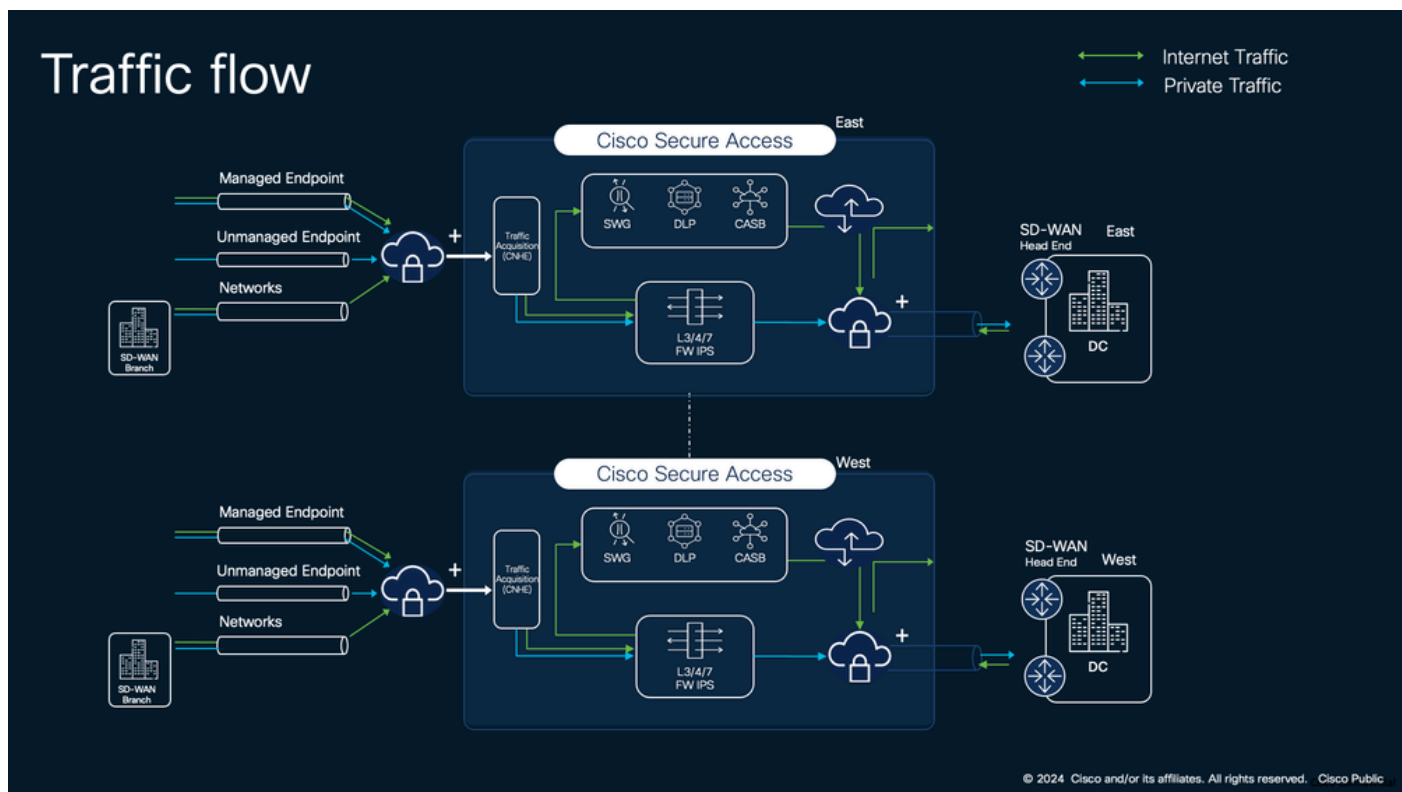
The IPsec tunnels can carry traffic from various sources, including:

- Remote access VPN users
- Browser-based or client-based ZTNA connections
- Other network locations connected to Cisco Secure Access

This approach allows organizations to securely route all types of private application traffic through a unified, encrypted channel, enhancing both security and operational efficiency.

Cisco Secure Access, as part of Cisco Security Service Edge (SSE) solution, simplifies IT operations through a single, cloud-managed console, unified client, centralized policy creation, and aggregated reporting. It incorporates multiple security modules in one cloud-delivered solution, including ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), DNS security, Remote Browser Isolation (RBI) and much more. This comprehensive approach mitigates security risks by applying zero trust principles and enforcing granular security policies

Figure 2: Traffic Flow between Cisco Secure Access and Private App



SSE Private App Traffic Flow

The solution described in this guide addresses comprehensive redundancy considerations, encompassing both the SD-WAN router in the data center and the Network Tunnel Group (NTG) on the Security Service Edge (SSE) side. This guide focuses on an **Active/Active** SD-WAN hub deployment model, which helps maintain uninterrupted traffic flow and ensures high availability.

Prerequisites

Requirements

It is recommended that you have knowledge of these topics:

- Cisco SD-WAN configuration and management
- Basic knowledge of IKEv2 and IPSec protocols
- Configuration of Network Tunnel Group in Cisco Secure Access portal
- Knowledge of BGP and ECMP

Components Used

The information in this document is based on these software and hardware versions:

- Cisco SD-WAN controllers on 20.9.5a
- Cisco SD-WAN Wan Edge Routers on 17.9.5a
- Cisco Secure Access Portal

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Design

This guide describes the solution using an Active/Active design model for SD-WAN head-end routers. An Active/Active design model in the context of SD-WAN head-end routers assumes two routers in a data center, both connected to the Security Service Edge (SSE) Network Tunnel Group (NTG), as illustrated in Figure 3. In this scenario, Both SD-WAN routers in the data center (DC1-HE1 and DC1-HE2) actively handle traffic flow. They achieve this by sending the same AS Path Length (ASPL) to the internal DC neighbor. As a result, traffic from within the DC load balances between the two head-ends.

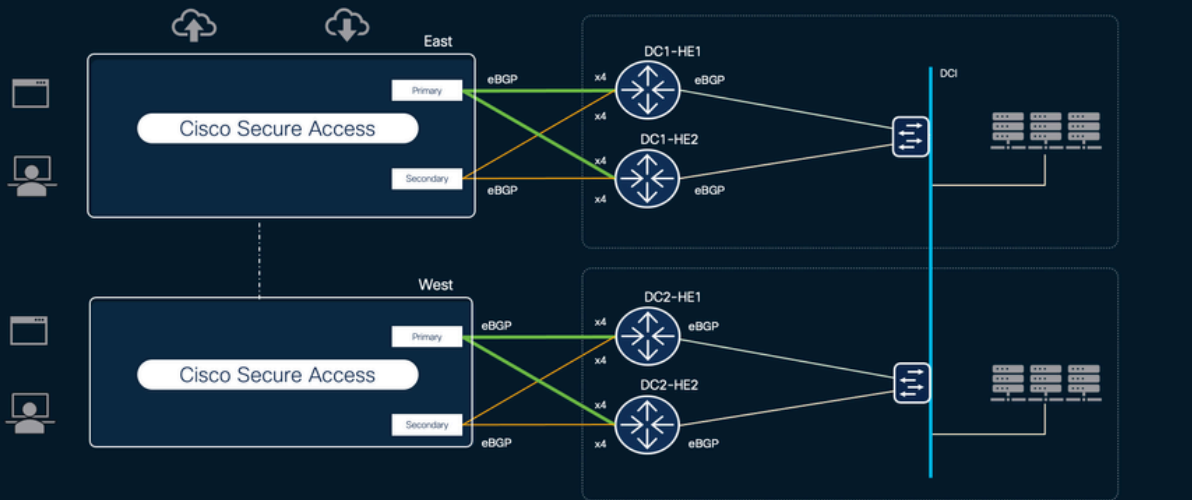
Each head-end router can establish multiple tunnels to SSE Points of Presence (POPs). The number of tunnels varies based on your requirements and SD-WAN device model. In this design:

- Each router has 4 tunnels to the primary SSE Hub and 4 tunnels to the secondary SSE Hub.
- The maximum number of tunnels supported by each SSE Hub can vary. For the most up-to-date information, please refer to the official documentation: <https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels>

These head-end routers form BGP neighborships over the tunnels towards the SSE. Through these neighborships, the head-ends advertise private application prefixes to their SSE neighbors, enabling secure and efficient routing of traffic to private resources.

Figure 3: SD-WAN to SSE Active/Active Deployment Model

SD-WAN Traffic flow Active / Active



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN to SSE Active/Active Deployment Model

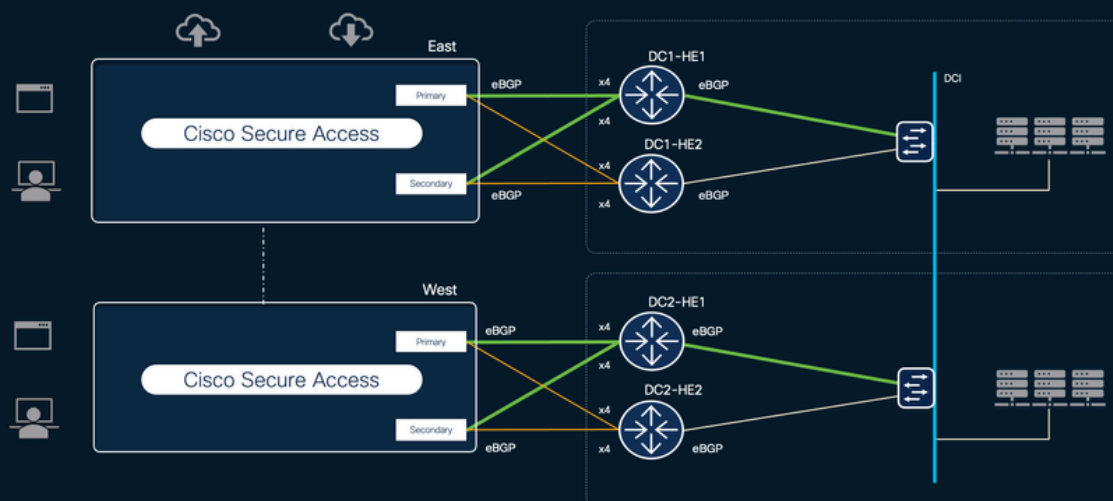
An Active/Standby design designates one router (DC1-HE1) as always active, while the secondary router (DC1-HE2) remains on standby. Traffic consistently flows through the active head-end (DC1-HE1) unless it completely fails. This deployment model has a drawback: if the primary tunnel to SSE goes down, traffic switches to the secondary SSE tunnels which is only via DC1-HE2, causing any stateful traffic to reset. In the Active/Standby model, BGP AS-Path Length is used to steer traffic both within the DC and towards the SSE. DC1-HE1 sends prefix updates to the SSE BGP neighbor with an ASPL of 2, while DC1-HE2 sends updates with an ASPL of 3. The internal DC neighbor of DC1-HE1 advertises prefixes with a shorter AS path length than DC1-HE2, ensuring traffic preference for DC1-HE1. (Customers can choose other attributes or protocols to influence traffic preference.)

Customers can select either an Active/Active or Active/Standby deployment model based on their specific requirements.

Figure 4: SD-WAN to SSE Active/Standby Deployment Model

SD-WAN Traffic flow Active / Standby

— Primary Tunnel
— Secondary Tunnel



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN to SSE Active/Standby Deployment Model

Configure

This section describes the procedure:

1. Verify prerequisites for provisioning a Network Tunnel Group in the Cisco Secure Access portal.
2. Configure SD-WAN interconnect with Cisco Secure Access Network Tunnel Group (NTG) using the **IPsec Manual Method**.
3. Configure BGP neighborship



Note: This configuration is based on an Active/Active deployment model

Procedure 1. Verify Network Tunnel Group Configuration on Cisco Secure Access Portal

How to configure Network Tunnel Group is not be covered in the guide. Please review this reference.

- [Add a Network Tunnel Group: SSE Documentation](#)
- [Configure Network Tunnel between Cisco Secure Access and Cisco IOS XE Router Using ECMP with BGP](#)

Navigate to Cisco Secure Access and ensure that the Network Tunnel Groups (NTGs) are provisioned. For the current design, we need to provision NTGs in two different Points of Presence (POPs). In this guide, we use NTGs in the US (Virginia) POP and US (Pacific Northwest) POP.



Note: The names and locations of POPs can vary, but the key concept is to have multiple NTGs provisioned in locations that are geographically close to your data center. This approach helps


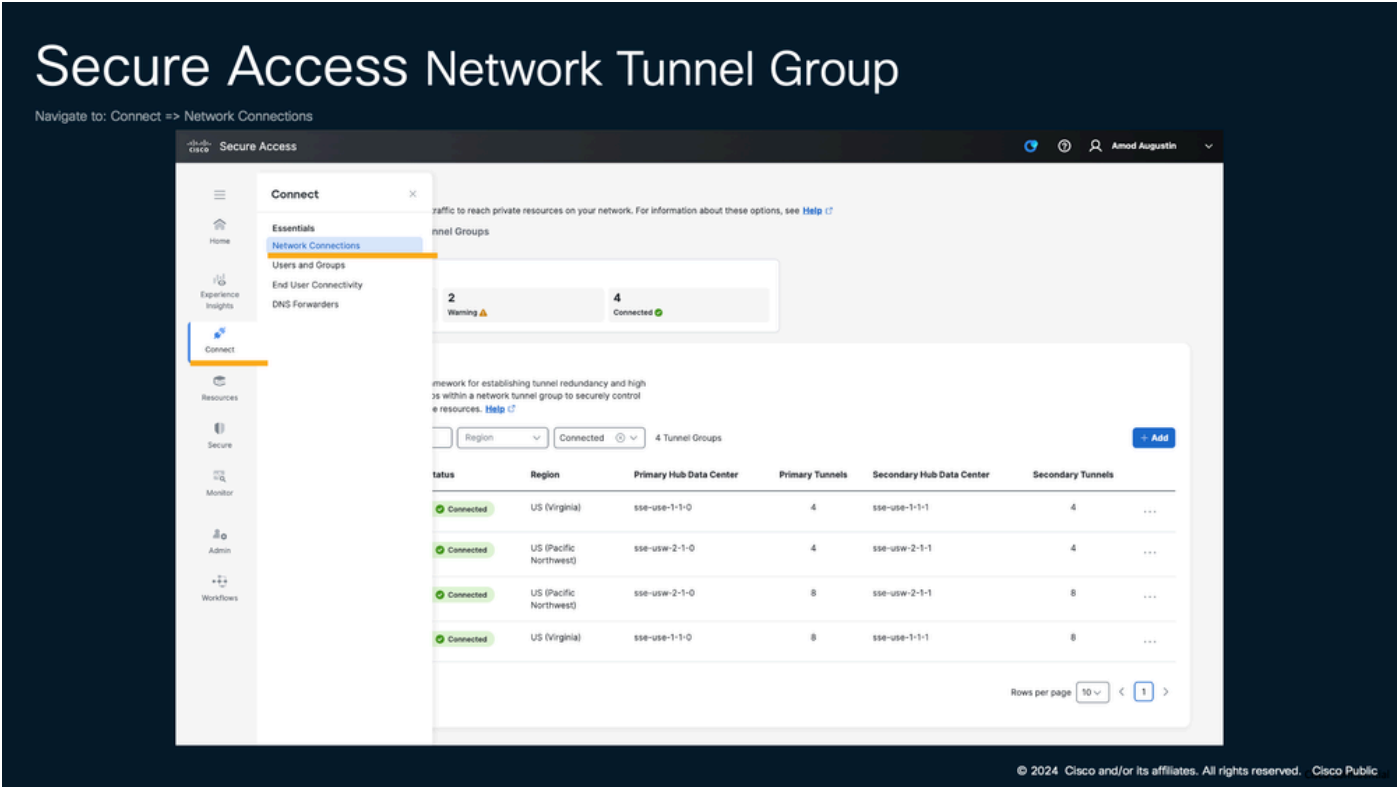
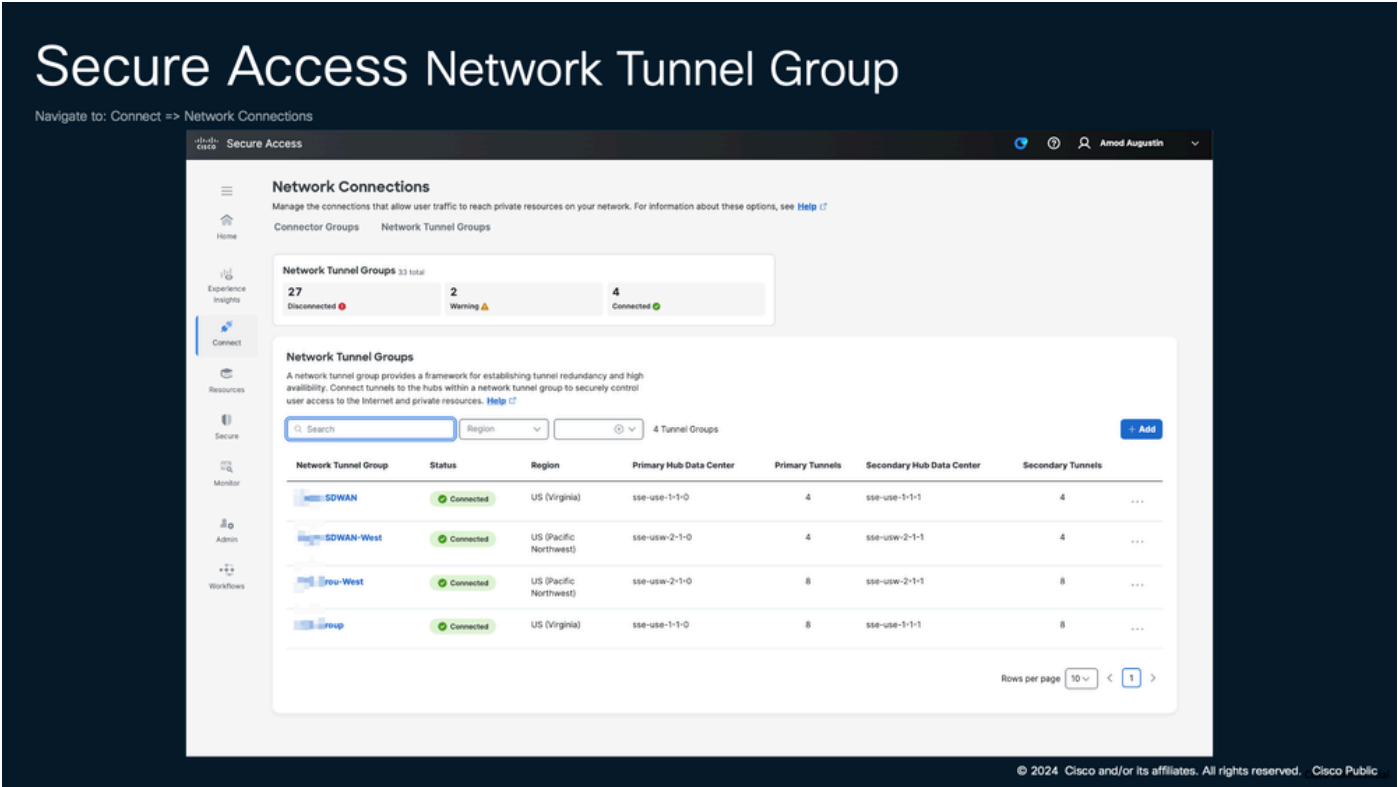
 optimize network performance and provides redundancy.

Figure 5: Cisco Secure Access Network Tunnel Group



Cisco Secure Access Network Tunnel Group

Figure 6: Cisco Secure Access Network Tunnel Group List



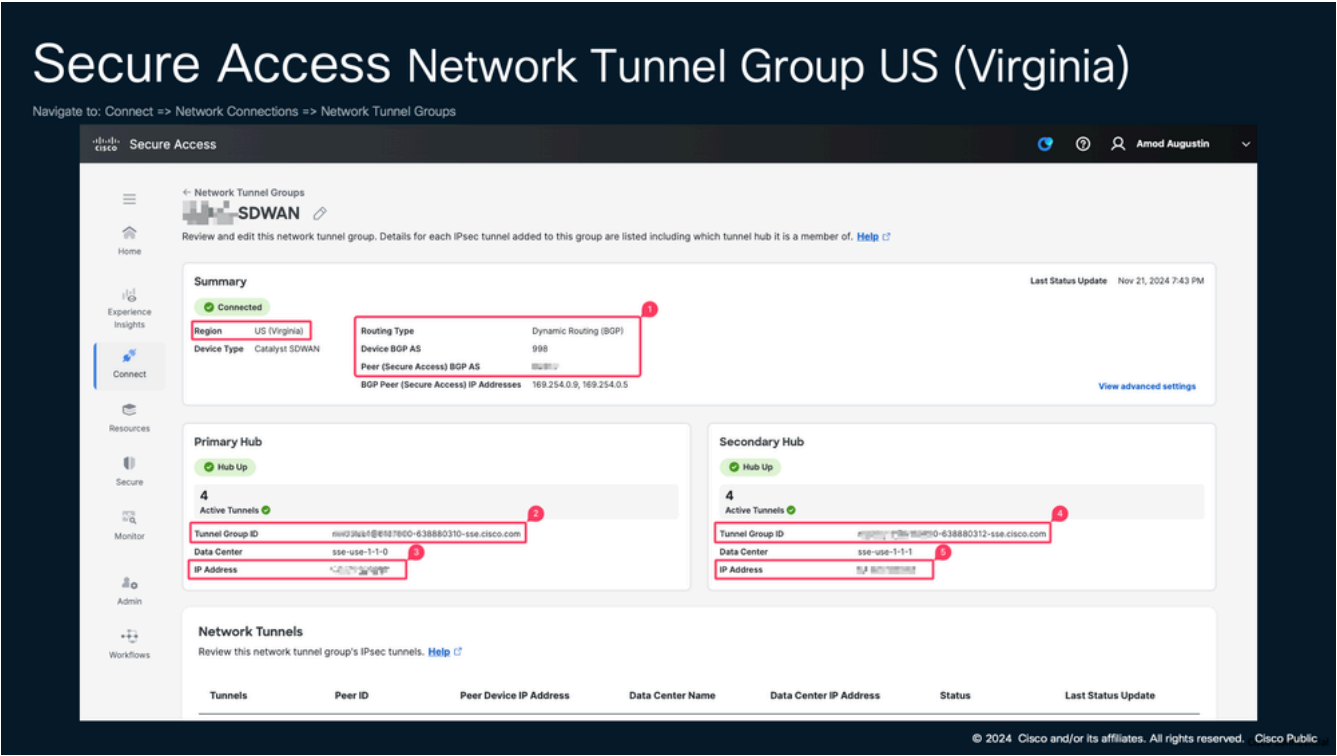
Secure Access Network Tunnel Group list

Make sure you have noted tunnel passphrase (which is shown only one time during tunnel creation).

 **Note:** Step 6 in [Add a Network Tunnel Group](#)

Also make a note of Tunnel Group attributes which we use during our IPSec configuration. The screenshot (Figure 6) is taken from a lab enviornment for a production scenario create NTG groups as per the design or usage recommendation.

Figure 7: Secure Access Network Tunnel Group US (Virginia)



Secure Access Network Tunnel Group US (Virginia)

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

Secure Access Network Tunnel Group US (Pacific Northwest)

Navigate to: Connect => Network Connections => Network Tunnel Groups

The screenshot shows the configuration page for a Network Tunnel Group named 'SDWAN-West'. The page is divided into several sections:

- Summary:** Displays the group's status as 'Connected'. It lists the Region as 'US (Pacific Northwest)', Device Type as 'Catalyst SDWAN', Routing Type as 'Dynamic Routing (BGP)', Device BGP AS as '999', and Peer (Secure Access) BGP AS as '999'. BGP Peer (Secure Access) IP Addresses are '169.254.0.9, 169.254.0.5'. A red box highlights the Region, Device Type, Routing Type, Device BGP AS, and Peer (Secure Access) BGP AS fields, with a red circle '1' next to it.
- Primary Hub:** Shows the hub is 'Hub Up' and has '4 Active Tunnels'. A red box highlights the Tunnel Group ID, Data Center, and IP Address fields, with a red circle '2' next to it.
- Secondary Hub:** Shows the hub is 'Hub Up' and has '4 Active Tunnels'. A red box highlights the Tunnel Group ID, Data Center, and IP Address fields, with a red circle '3' next to it.
- Network Tunnels:** A table listing the tunnels for this group. The table has columns: Tunnels, Peer ID, Peer Device IP Address, Data Center Name, Data Center IP Address, Status, and Last Status Update.

Red boxes and circles are used to highlight specific fields and counts in the configuration page.

Secure Access Network Tunnel Group US (Pacific Northwest)

The figure 8 shows only 4 tunnels on both primary and secondary hubs. However, a maximum of 8 tunnels has been successfully tested in a controller environment. The maximum tunnel support can vary depending on the hardware device you use and the current SSE tunnel support. For the most up-to-date information, please refer to the official documentation: <https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels> and the release note of the respective hardware device.

An example for an 8-tunnel setup is provided here.

Figure 8a: NTG Tunnels up to 8 tunnels

Secure Access

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

Network Tunnel Groups

West

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of.
[Help](#)

Summary

Connected

Region
US (Pacific Northwest)

Device Type
Catalyst SDWAN

Routing Type
Dynamic Routing (BGP)

Device BGP AS

Peer (Secure Access) BGP AS

BGP Peer (Secure Access) IP Addresses
169.254.0.0, 169.254.0.5

Last Status Update
Feb 13, 2025 3:54 PM

[View advanced settings](#)

Primary Hub

Hub Up

8
Active Tunnels

Tunnel Group ID
900-639871055-sse.cisco.com

Data Center

IP Address

Secondary Hub

Hub Up

8
Active Tunnels

Tunnel Group ID
900-639871054-sse.cisco.com

Data Center

IP Address

Network Tunnels

Review this network tunnel group's IPsec tunnels.
[Help](#)

| Tunnels | Peer ID | Peer Device IP Address | Data Center Name | Data Center IP Address | Status | Last Status Update |
|-------------|---------|------------------------|------------------|------------------------|-----------|----------------------|
| Primary 1 | 131073 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 2 | 131074 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 3 | 131075 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 4 | 131076 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 5 | 131077 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 6 | 131078 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 7 | 131079 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Primary 8 | 131080 | | sse-usw-2-1-0 | | Connected | Feb 13, 2025 3:54 PM |
| Secondary 1 | 589825 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 2 | 589826 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 3 | 589827 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 4 | 589828 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 5 | 589829 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 6 | 589830 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 7 | 589831 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |
| Secondary 8 | 589832 | | sse-usw-2-1-1 | | Connected | Feb 13, 2025 3:53 PM |

Procedure 2. Configure SD-WAN interconnect with Cisco Secure Access Network Tunnel Group (NTG) using the IPsec Manual Method.

This procedure demonstrates how to connect a Network Tunnel Group (NTG) using feature templates on Cisco Catalyst SD-WAN Manager 20.9 and Cisco Catalyst Edge Router running 17.9 release.



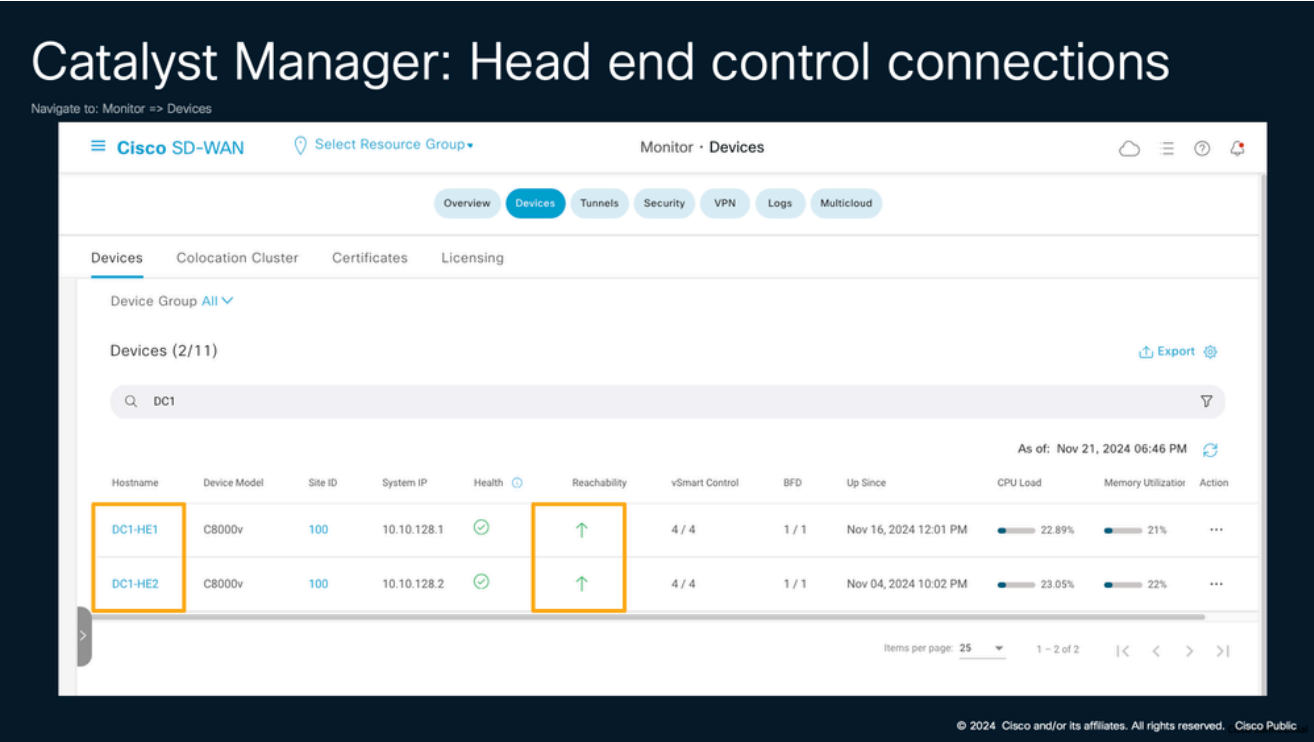
Note: This guide assumes an existing SD-WAN overlay deployment with either a hub-and-spoke or fully meshed topology, where hubs serve as access entry points for private applications hosted in the data center. This procedure can also be applied to branch or cloud deployments.

Before proceeding, ensure the prerequisites are met:

1. Control connections are up on the device to allow necessary updates from Cisco Catalyst SD-WAN

Manager.

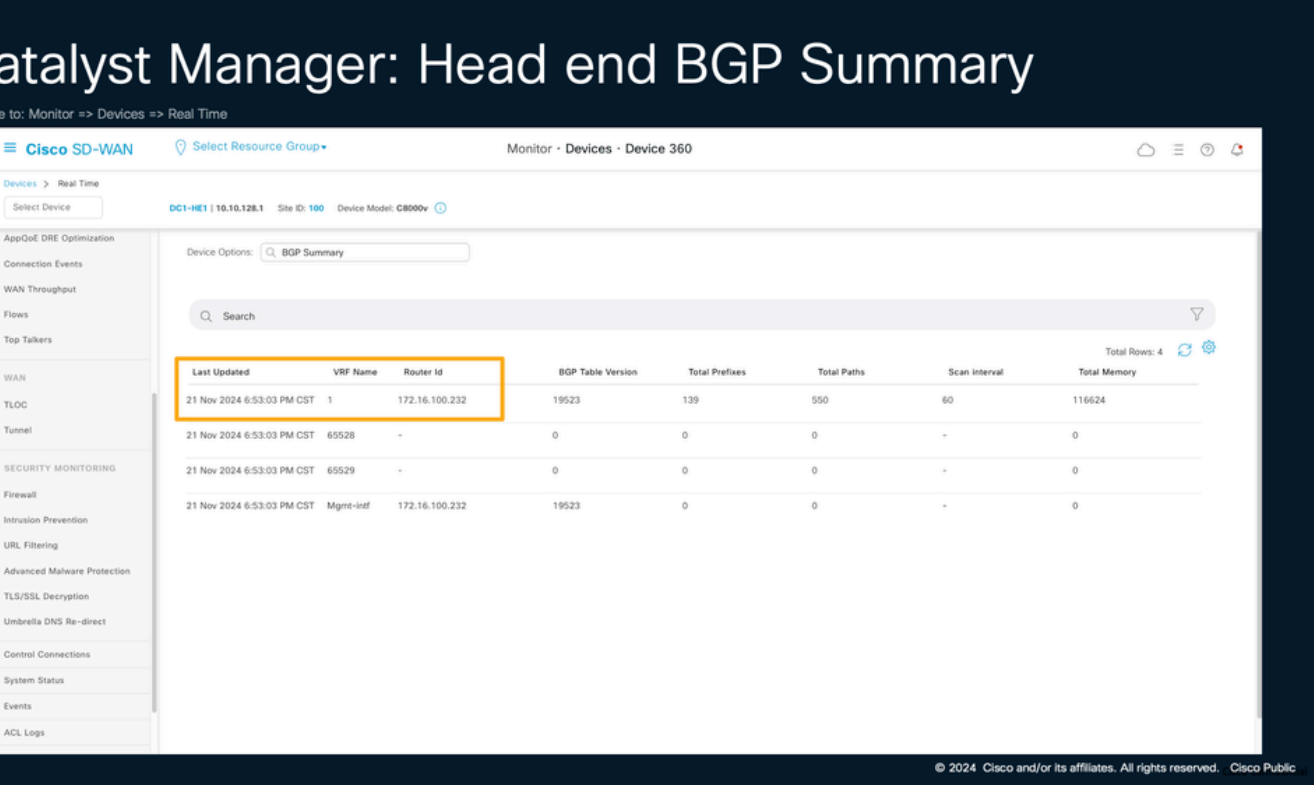
Figure 9: Cisco Catalyst SD-WAN Manager: Head end control connections



Catalyst Manager: Head end control connections

2. Service-side VPNs are configured and use a routing protocol to advertise prefixes. This guide uses BGP as the routing protocol on the service side.

Figure 10: Cisco Catalyst SD-WAN Manager: Head end BGP Summary



To configure SD-WAN interconnect with Network Tunnel Group (NTG) using Manual IPsec Method, complete these steps:

 **Note:** Repeat this step for the required number of Tunnels for the deployment.

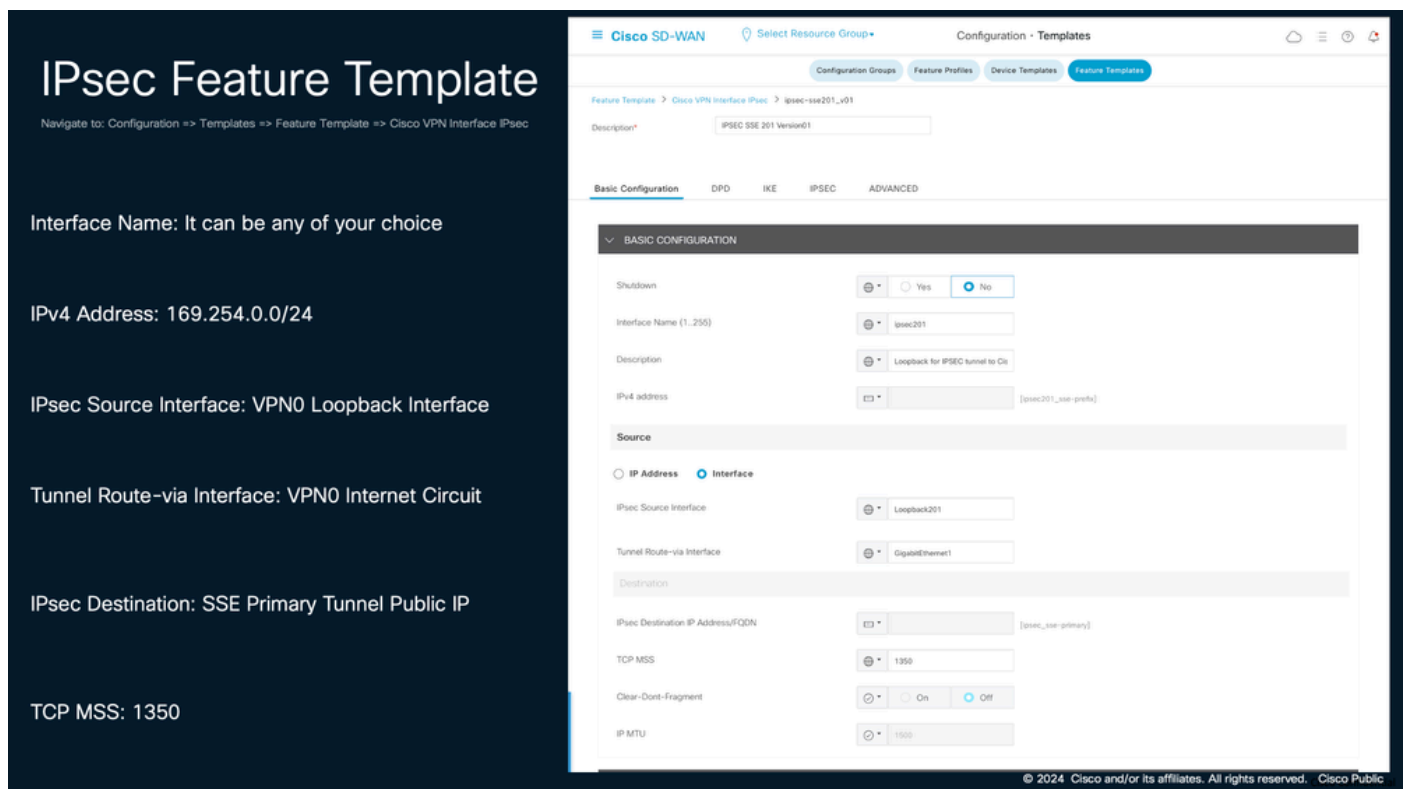
Please refer to the official documentation for Tunnel Limitation: <https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels>

These steps detail the process for connecting DC1-HE1 (Data Center 1 Head-End 1) to the SSE Virginia Primary Hub. This configuration establishes a secure tunnel between the SD-WAN router in the data center and the Cisco Secure Access Network Tunnel Group (NTG) located in the Virginia Point of Presence (POP)

Step 1: Create IPsec Feature Template

Create an IPsec Feature Template to define the parameters for the IPsec tunnel that connects SD-WAN head end router to the NTG.

Figure 11: IPsec Feature Template: Basic Configuration



The screenshot displays the Cisco SD-WAN Configuration - Templates page. The left sidebar shows the navigation path: Configuration > Templates > Feature Template > Cisco VPN Interface IPsec. The main panel is titled "IPsec Feature Template" and shows the "Basic Configuration" tab selected. The configuration fields are as follows:

- Shutdown:** Yes (selected), No (unselected)
- Interface Name (1..255):** ipsec201
- Description:** Loopback for IPsec tunnel to DC
- IPv4 address:** [ipsec201_sse-prefix]
- Source:**
 - IP Address:** (unselected)
 - Interface:** (selected)
 - IPsec Source Interface:** Loopback201
 - Tunnel Route-via Interface:** GigabitEthernet1
- Destination:**
 - IPsec Destination IP Address/FQDN:** [ipsec_sse-primary]
- TCP MSS:** 1350
- Clear-Over-Fragment:** On (selected), Off (unselected)
- IP MTU:** 1500

IPsec Feature Template: Basic Configuration

Interface Name: It can be any of your choice

IPv4 Address: SSE listens to 169.254.0.0/24 based on the requirement you can divide the subnet to your choice, as a best practice please use with /30. In this guide we leave out the first block for future use.

IPsec Source Interface: Define a VPN0 Loopback Interface that is unique for the current IPsec interface. For consistency and troubleshooting purpose its recommended to keep the same numbering.

Tunnel Route-via Interface: Point the interface which can be used as underlay to reach SSE (must have internet access)

IPsec Destination: Primary Hub IP Address

Refer Figure 7: Secure Access Network Tunnel Group US (Virginia) this is 35.171.214.188

TCP MSS: This should be 1350 (Reference: <https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters>)

Example: DC1-HE1 towards SSE Virginia Primary Hub

Interface Name: ipsec201

Description: Loopback for IPSEC tunnel to Cisco

IPv4 address: 169.254.0.x/30

IPsec Source Interface: Loopback201

Tunnel Route-via Interface: GigabitEthernet1

IPsec Destination IP Address/FQDN: 35.xxx.xxx.xxx

TCP MSS: 1350

Figure 12: IPsec Feature Template: IKE IPSEC

The screenshot displays the Cisco SD-WAN Configuration - Templates page. The left sidebar shows the navigation path: Configuration > Templates > Feature Template > Cisco VPN Interface IPsec. The main content area is titled 'IPsec Feature Template' and lists the following configuration details:

- DPD Interval: Keep this default
- IKE Version: 2
- IKE Rekey Interval: 28800
- IKE Cipher: Default which is AES-256-CBC-SHA1
- IKE DH Group: 14 2048-bit Modulus
- Preshared Key: Passphrase
- IKE ID for local End Point: Tunnel Group ID
- IKE ID for Remote End Point: Primary Hub IP Address
- IPsec Cipher Suite: AES 256 GCM
- Perfect Forward Secrecy: None

The right sidebar shows the configuration details for the IPsec Feature Template, categorized into three sections:

- DEAD-PEER DETECTION**
 - DPD Interval: 10
 - DPD Retries: 3
- IKE**
 - IKE Version: 2
 - IKE Rekey Interval (seconds): 28800
 - IKE Cipher Suite: AES-256-CBC-SHA1
 - IKE Diffie-Hellman Group: 14 2048-bit modulus
 - IKE Authentication: Preshared Key
 - IKE ID for local End point: [ipsec_sse-local-id]
 - IKE ID for Remote End point: [ipsec_sse-remote]
- IPSEC**
 - IPsec Rekey Interval (seconds): 28800
 - IPsec Replay Window: 512
 - IPsec Cipher Suite: AES 256 GCM
 - Perfect Forward Secrecy: None

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec Feature Template: IKE IPSEC

DPD Interval: Keep this default

IKE Version: 2

IKE Rekey Interval: 28800

IKE Cipher: Default which is AES-256-CBC-SHA1

IKE DH Group: 14 2048-bit Modulus

Preshared Key: Passphrase

IKE ID for local End Point: Tunnel Group ID

Refer Figure 7: Secure Access Network Tunnel Group US (Virginia) this is mn03lab1+201@8167900-638880310-sse.cisco.com



Note: Each tunnel must have unique Endpoint for this; use "+loopbackID" Example:
mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com and so on.

IKE ID for Remote End Point: Primary Hub IP Address

IPsec Cipher Suite: AES 256 GCM

Perfect Forward Secrecy: None

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

Example:

IKE Version: 2

IKE Rekey Interval: 28800

IKE Cipher: AES-256-CBC-SHA1

IKE DH Group: 14 2048-bit Modulus

Preshared Key: *****



Note: Step 6 in [Add a Network Tunnel Group](#)

IKE ID for local End Point: mn03lab1@8167900-638880310-sse.cisco.com

IKE ID for Remote End Point: 35.171.xxx.xxx

IPsec Cipher Suite: AES 256 GCM

Perfect Forward Secrecy: None

Repeat the steps to configure the required tunnels for both the primary and secondary Secure Access hubs. For a 2x2 setup, you would create four tunnels in total:

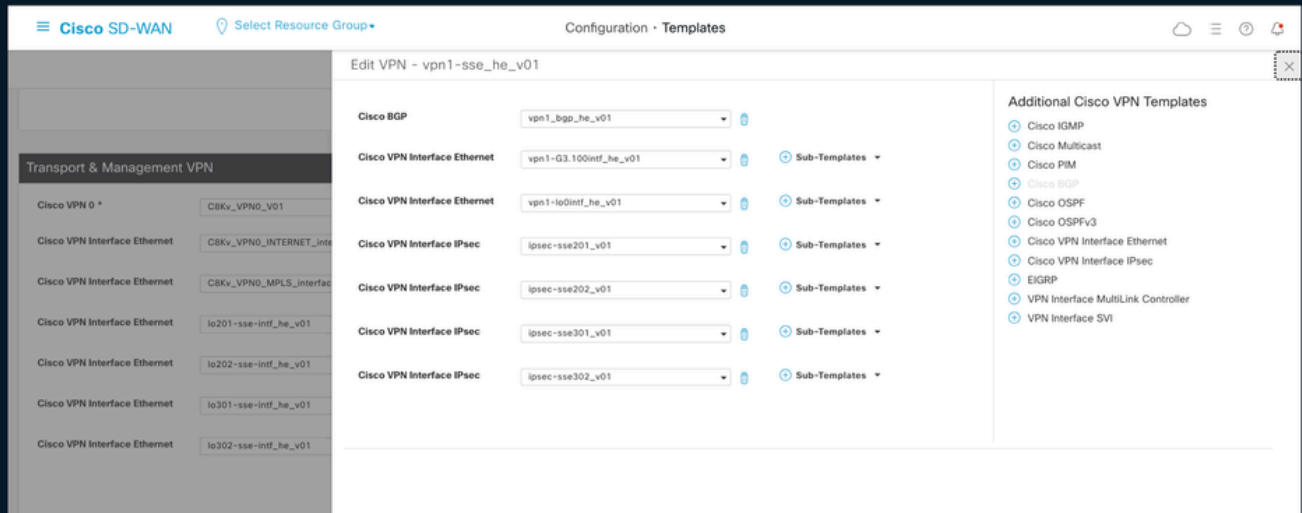
- Two tunnels from DC1-HE1 to the primary Secure Access hub
- Two tunnels from DC1-HE1 to the secondary Secure Access hub

Now that the templates are created, we would use them on the service side vrf show in figure 13 and the loopback defined attached on the global vrf shown in figure 14.

Figure 13: Catalyst SD-WAN Manager: Head end VPN1 Template 2x2

Catalyst Manager: Head end VPN1 Template

Navigate to: Configuration => Templates => Device Template => Service VPN



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst Manager: Head end VPN1 Template

Step 2: Define the Loopback in Global VRF

Configure a loopback interface in the global VRF (Virtual Routing and Forwarding) table. This loopback serves as the source interface for the IPsec tunnel created in Step 1.

All the loopback referenced in Step 1 must be defined in Global VRF.

IP Address can be defined in any RFC1918 range.

Figure 14: Catalyst SD-WAN Manager: VPN0 Loopback

Catalyst Manager: VPN0 Loopback

Navigate to: Configuration => Templates => Device Template => Transport & Management VPN

Cisco SD-WAN Select Resource Group Configuration - Templates

Configuration Groups Feature Profiles **Device Templates** Feature Templates

Transport & Management VPN

Cisco VPN 0 * CBKv_VPN0_V01

Cisco VPN Interface Ethernet CBKv_VPN0_INTERNET_interface

Cisco VPN Interface Ethernet CBKv_VPN0_MPLS_interface

Cisco VPN Interface Ethernet lo201-sse-intf_he_v01

Cisco VPN Interface Ethernet lo202-sse-intf_he_v01

Cisco VPN Interface Ethernet lo301-sse-intf_he_v01

Cisco VPN Interface Ethernet lo302-sse-intf_he_v01

Additional Cisco VPN 0 Templates

```
interface Loopback201
description SSE SD-WAN Loopback Interface
ip address 172.16.100.201 255.255.255.255
end
```

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst Manager: VPN0 Loopback

Procedure 3. Configure BGP neighborship

Use BGP feature template define BGP neighborship for all the tunnel interfaces. Refer respective Network Tunnel Groups BGP configuration in Cisco secure access portal to configure BGP values.

Figure 15: Secure Access Network Tunnel Group US (Virginia)

Secure Access Network Tunnel Group US (Virginia)

Navigate to: Connect => Network Connections => Network Tunnel Groups

Secure Access

Network Tunnel Groups

SDWAN

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

Last Status Update Nov 21, 2024 7:43 PM

Summary

Connected

Region US (Virginia)

Device Type Catalyst SDWAN

Routing Type Dynamic Routing (BGP)

Device BGP AS 998

Peer (Secure Access) BGP AS 64512

BGP Peer (Secure Access) IP Addresses 169.254.0.5, 169.254.0.5

[View advanced settings](#)

Primary Hub

Hub Up

4 Active Tunnels

Tunnel Group ID mn03lab1@8167900-638880310-sse.cisco.com

Data Center sse-use-1-1-0

IP Address 35.171.214.188

Secondary Hub

Hub Up

4 Active Tunnels

Tunnel Group ID mn03lab1@8167900-638880312-sse.cisco.com

Data Center sse-use-1-1-1

IP Address 44.217195.188

Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#)

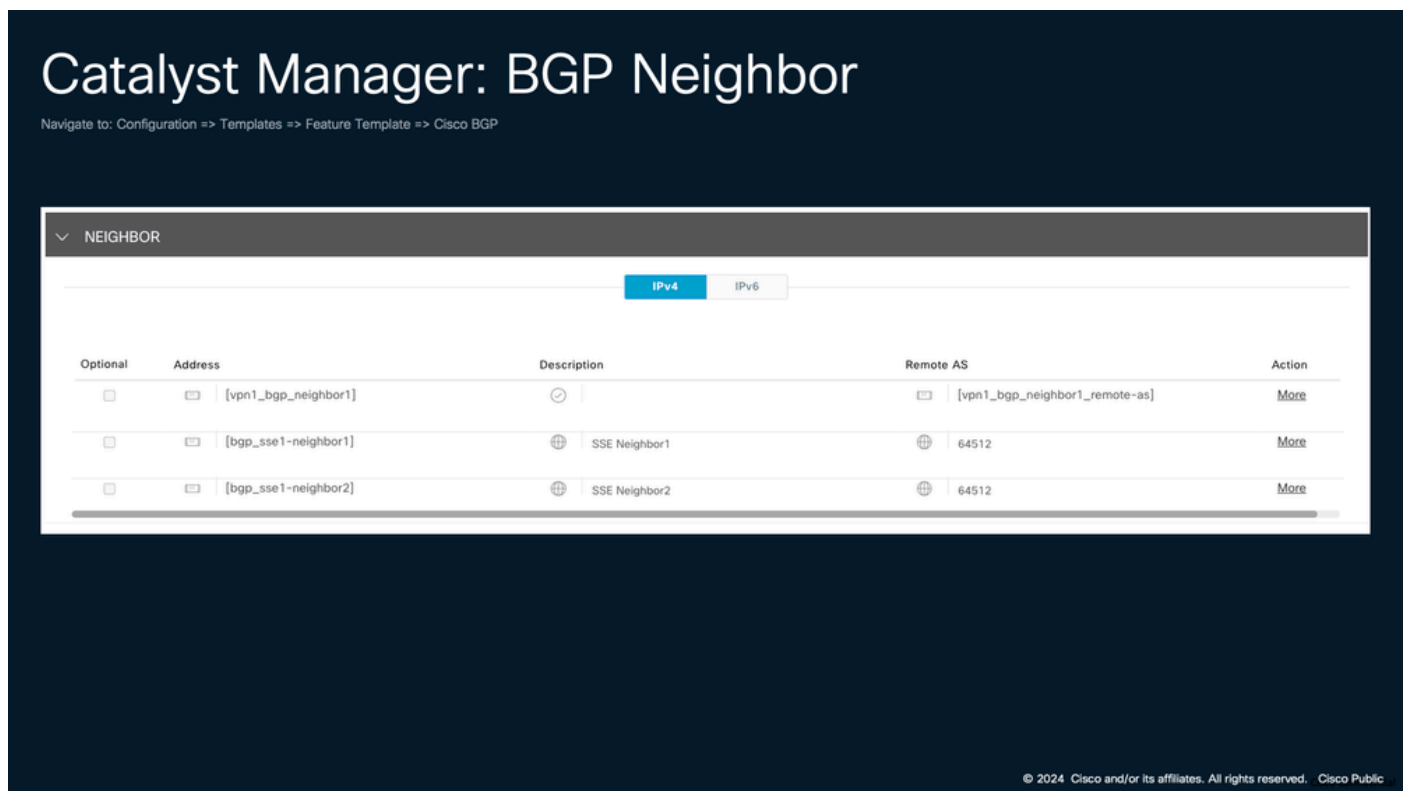
| Tunnels | Peer ID | Peer Device IP Address | Data Center Name | Data Center IP Address | Status | Last Status Update |
|---------|---------|------------------------|------------------|------------------------|--------|--------------------|
|---------|---------|------------------------|------------------|------------------------|--------|--------------------|

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Access Network Tunnel Group US (Virginia)

In this example, we use the information from Figure 15 (box 1) to define BGP using a feature template..

Figure 16: Catalyst SD-WAN Manager BGP Neighbor



Catalyst SD-WAN Manager BGP Neighbor

Configuration generated using the feature template:

```
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#
```

Verification

```
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 Tunnel
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
```

Reference

An Active/Active implementation would have a multipath from the core switch which is connected to both SD-WAN head ends.

Figure 17: Active/Active Scenario for BGP Neighbor

```
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  3.1.1.1/32      172.16.128.5        65535             0 998 ?
  *>             172.16.128.1        65535             0 998 ?
  *m  3.2.1.1/32      172.16.128.5        65535             0 998 ?
  *>             172.16.128.1        65535             0 998 ?
<snip>
```

Active/Active BGP Neighbor

An Active/Standby implementation would have a one active path from the core switch to SD-WAN head ends due to ASPL prepending (which is done using a route map to the neighbor).

Figure 18: Active/Standby Scenario for BGP Neighbor

```
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 ?
  *  3.1.1.1/32      172.16.128.5        65535             0 998 998?
  *>             172.16.128.1        65535             0 998 ?
  *  3.2.1.1/32      172.16.128.5        65535             0 998 998?
  *>             172.16.128.1        65535             0 998 ?
<snip>
```

Active/Standby BGP Neighbor