# Configure Secure Access with Catalyst SD-WAN Automated Tunnels for Secure Private Access

## Contents

**Introduction**

**Background Information**

**Network Diagram**

**Prerequisites**

- Requirements
- Components Used

**Configure**

- Secure Access Configuration
  - API Creation
- SD-WAN Configuration
  - API Integration
  - Configure Policy Group
  - Configure Routing

**Verify**

- Secure Access - Activity Search
- Secure Access - Events
- Catalyst SD-WAN Manager -Network-Wide Path Insights

**Related Information**

## Introduction

This document describes how to configure Secure Access with Catalyst SD-WAN Automated Tunnels for Secure Private Access.

# Background Information

As organizations move beyond traditional perimeter based networks, securely accessing private resources becomes just as important as securing internet traffic. Applications are no longer confined to a single data center, they now live across on-premises environments, public clouds, and hybrid architectures. This shift requires a more flexible and modern approach to private access.

This is where a SASE based architecture and Cisco Secure Access come into play. Instead of relying on legacy VPN concentrators and flat network access, Cisco Secure Access provides private connectivity as a cloud delivered service, combining VPN-as-a-Service (VPNaaS) and Zero Trust Network Access (ZTNA).

For network-level private access, Cisco Secure Access integrates with SD-WAN using automated site-to-site IPsec tunnels. These tunnels allow private traffic to flow securely between Secure Access and on-premises or cloud networks, while keeping security inspection and policy enforcement centralized in the cloud. From an operational perspective, this removes the need to deploy and maintain traditional VPN headends and simplifies scaling as environments grow.

In a VPNaaS model, Secure Access acts as the VPN termination point in the cloud. SD-WAN handles intelligent routing and resiliency with Secure Access and ensures that traffic is protected and governed by consistent security policies before reaching private resources.

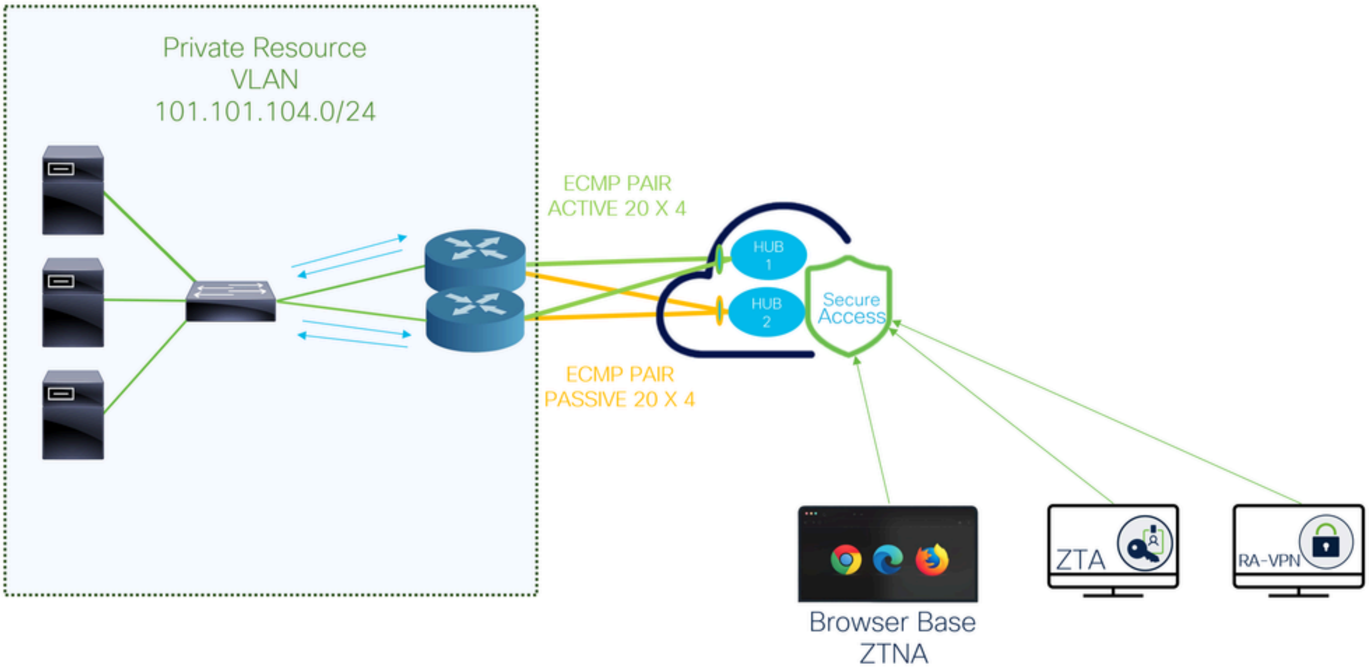
Cisco Secure Access also supports advanced site-to-site tunnel architectures, including multi-regional backhaul. This capability allows organizations to establish tunnels to multiple Secure Access regions simultaneously, providing geographic redundancy and higher availability. By connecting to different regions, traffic can fail over automatically in case of regional outages, latency degradation, or maintenance events.

For example, an organization can establish site-to-site tunnels from its SD-WAN environment to Secure Access regions in London and Germany. Both tunnels remain active, enabling resilient private access across regions and ensuring continuity even if one region becomes unavailable. This multi-regional design strengthens high availability, improves fault tolerance, and aligns with enterprise-grade resilience requirements.

For more granular access, Cisco Secure Access enforce Zero Trust Network Access (ZTNA) model. Instead of granting users broad network connectivity, ZTNA allows access only to specific applications, based on identity, device posture, and context. This approach significantly reduces the attack surface and aligns with Zero Trust principles.

ZTNA access is enabled through a combination of site-to-site tunnels and Resource Connectors. Resource Connectors are lightweight virtual appliances that establish outbound-only connections to Secure Access, meaning private resources never need to be exposed directly to the internet.

# Network Diagram



# Prerequisites

## Requirements

- Secure Access Knowledge
- Cisco Catalyst SD-WAN Manager Release 20.18.2 and Cisco IOS XE Catalyst SD-WAN Release 17.18.2 or later
- Intermediate knowledge of routing and switching
- ECMP Knowledge
- VPN Knowledge
- Since this integration is on controlled availability, you need to submit a TAC case to ask to enable the feature in Cisco Secure Access

## Components Used

- Secure Access Tenant
- Catalyst SD-WAN Manager Release 20.18.2 and Cisco IOS XE Catalyst SD-WAN Release 17.18.2
- Catalyst SD-WAN Manager

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.

# Configure

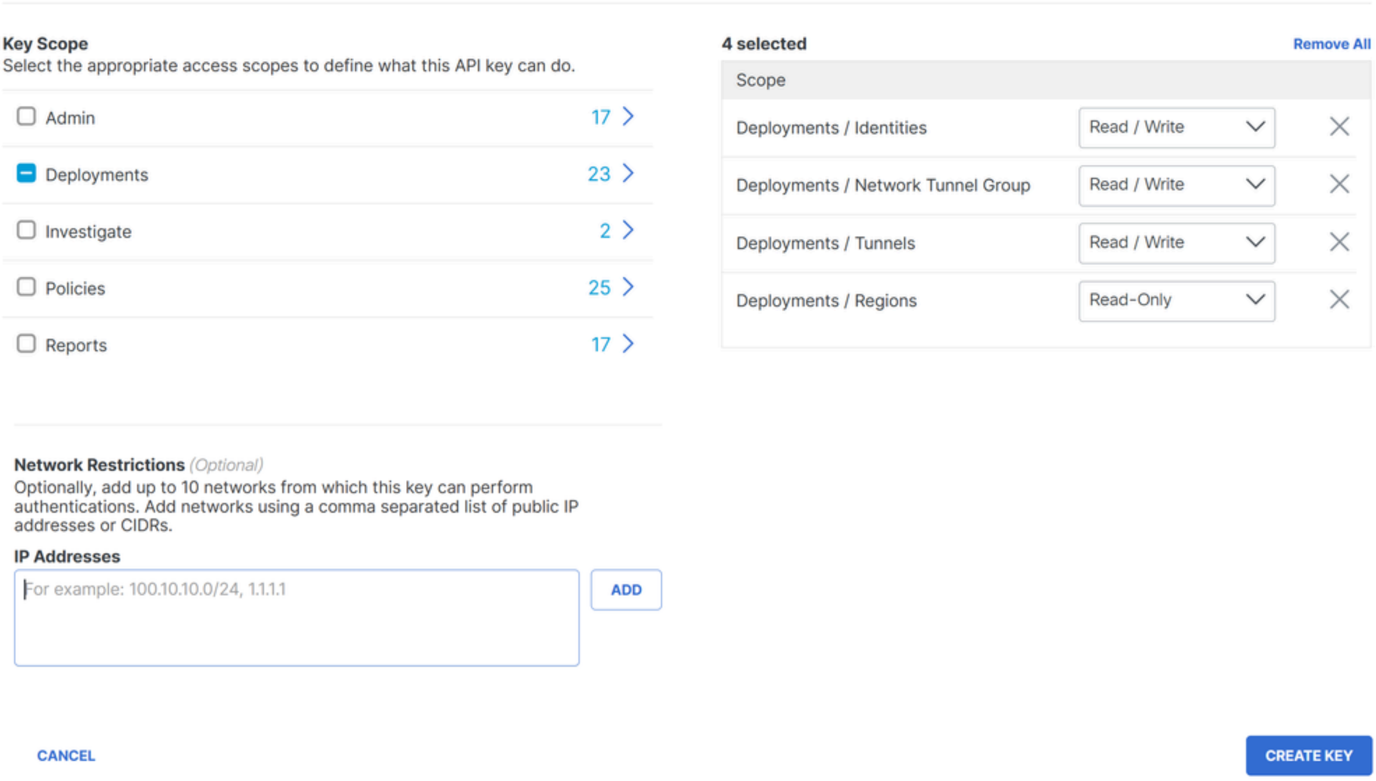
## Secure Access Configuration

### API Creation

In order to create the automated tunnels with Secure Access check the next steps:

Navigate to Secure Access Dashboard.

- Click on Admin > API Keys
- Click on Add
- Choose the next options:
  - Deployments / Network Tunnel Group: Read/Writte
  - Deployments / Tunnels: Read/Writte
  - Deployments / Regions: Read-Only
  - Deployments / Identities: Read-Writte
  - Expiry Date: Never Expire



**Key Scope**
Select the appropriate access scopes to define what this API key can do.

| | |
|---|---|
| □ Admin | 17 > |
| ☑ Deployments | 23 > |
| □ Investigate | 2 > |
| □ Policies | 25 > |
| □ Reports | 17 > |

**4 selected** Remove All

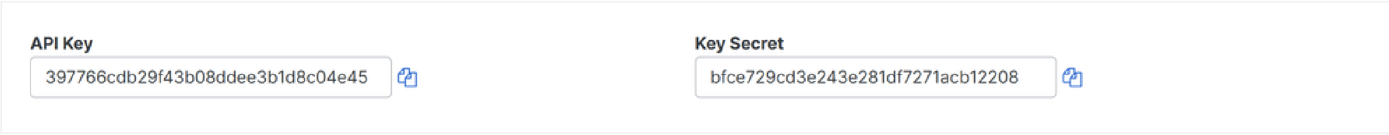
| Scope | | |
|---|---|---|
| Deployments / Identities | Read / Write | ✕ |
| Deployments / Network Tunnel Group | Read / Write | ✕ |
| Deployments / Tunnels | Read / Write | ✕ |
| Deployments / Regions | Read-Only | ✕ |

**Network Restrictions** *(Optional)*
Optionally, add up to 10 networks from which this key can perform authentications. Add networks using a comma separated list of public IP addresses or CIDRs.

**IP Addresses**
For example: 100.10.10.0/24, 1.1.1.1

**Note**: Optionally, add up to 10 networks from which this key can perform authentications. Add networks using a comma separated list of public IP addresses or CIDRs.

- Click CREATE KEY to finalize the creation of the API Key and Key Secret.



**API Key**
397766cdb29f43b08ddee3b1d8c04e45

**Key Secret**
bfce729cd3e243e281df7271acb12208

**Caution**: Copy them before you click ACCEPT AND CLOSE; otherwise, you need to create them again and delete the ones that were not copied.

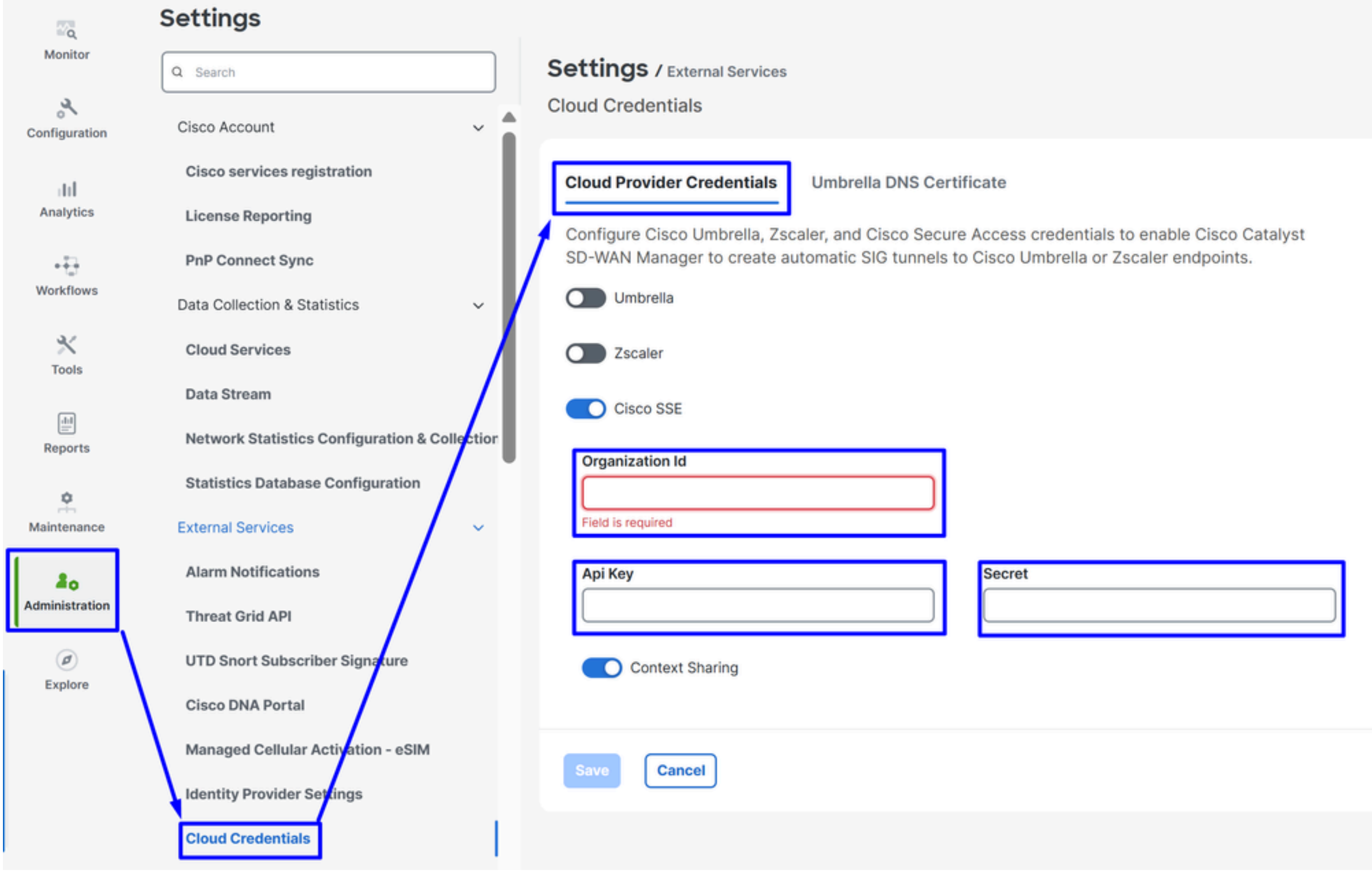
Then to finalize click ACCEPT AND CLOSE.

# SD-WAN Configuration

## API Integration

Navigate to Catalyst SD-WAN Manager:

- Click on **Administration** >Settings > Cloud Credentials
- Then click on Cloud Provider Credentials and enable Cisco SSEand fill the API and Organtiazation Settings



Settings / External Services

Cloud Credentials

Cloud Provider Credentials | Umbrella DNS Certificate

Configure Cisco Umbrella, Zscaler, and Cisco Secure Access credentials to enable Cisco Catalyst SD-WAN Manager to create automatic SIG tunnels to Cisco Umbrella or Zscaler endpoints.

○ Umbrella

○ Zscaler

● Cisco SSE

Organization Id

Field is required

Api Key

Secret

● Context Sharing

- **Organization ID**: You can take that from the URL of you SSE Dashboard https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Copy it from the step Secure Access Configuration
- Secret: Copy it from the step Secure Access Configuration

Then after that click on the Save button.

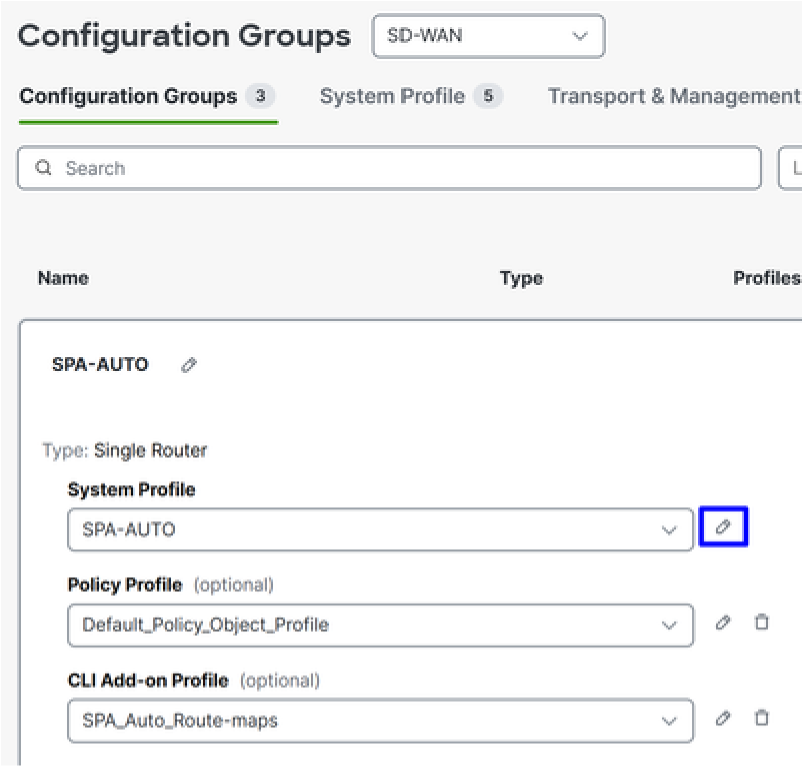
---

**Note**: Before you proceed with the next steps, you need to be sure that the SD-WAN Manager and the Catalyst SD-WAN Edges have DNS resolution and internet access.

---

To check if the DNS-Lookup is enabled please navigate to:

- Click on ***Configuration*** > ***Configuration Groups***
- Click on the profile of your Edge Devices and edit the ***System Profile***



Configuration Groups SD-WAN

Configuration Groups 3 | System Profile 5 | Transport & Management

Search

Name | Type | Profiles

SPA-AUTO

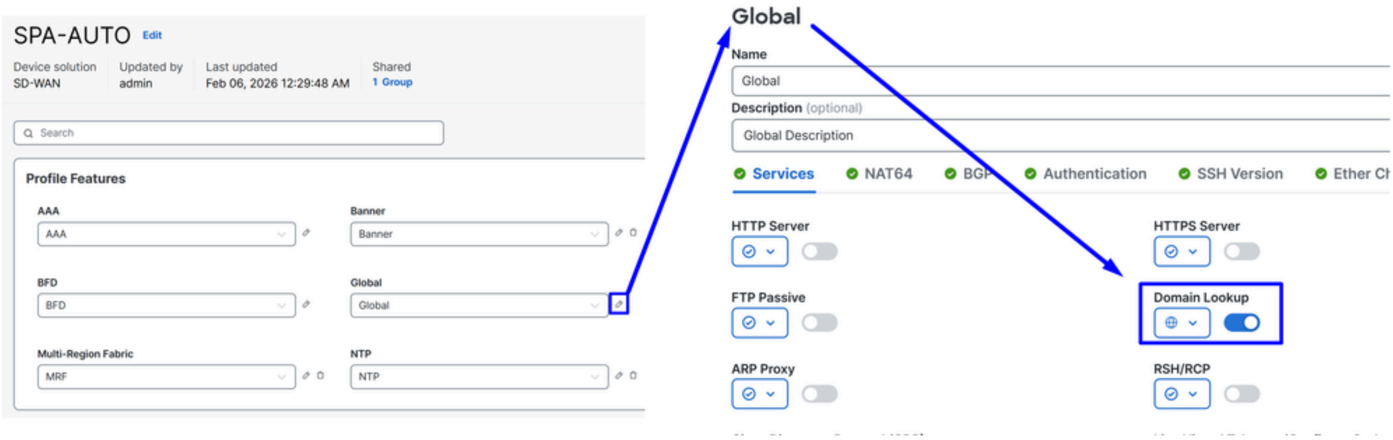
Type: Single Router

System Profile: SPA-AUTO

Policy Profile (optional): Default_Policy_Object_Profile

CLI Add-on Profile (optional): SPA_Auto_Route-maps

- Then Edit the ***Global*** option and be sure the option ***Domain Resolution*** is enabled



SPA-AUTO Edit

Device solution: SD-WAN | Updated by: admin | Last updated: Feb 06, 2026 12:29:48 AM | Shared: 1 Group

Search

Profile Features

AAA: AAA | Banner: Banner

BFD: BFD | Global: Global

Multi-Region Fabric: MRF | NTP: NTP

Global

Name: Global

Description (optional): Global Description

Services | NAT64 | BGP | Authentication | SSH Version | Ether Ch

HTTP Server | HTTPS Server

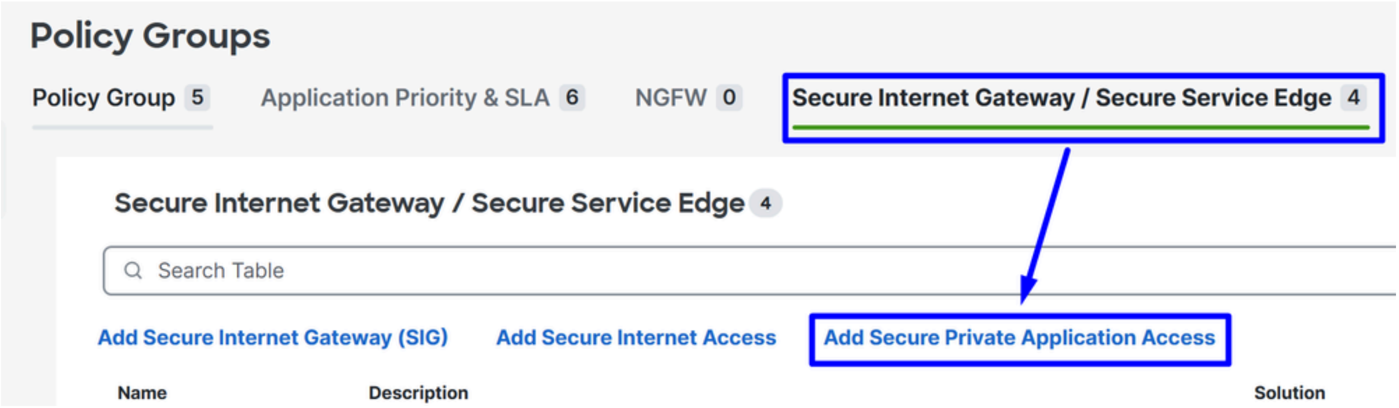
FTP Passive | Domain Lookup

ARP Proxy | RSH/RCP

### Configure Policy Group

Navigate to***Configuration*** > ***Policy Groups***:

- Click on Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



Policy Groups

Policy Group 5 | Application Priority & SLA 6 | NGFW 0 | Secure Internet Gateway / Secure Service Edge 4

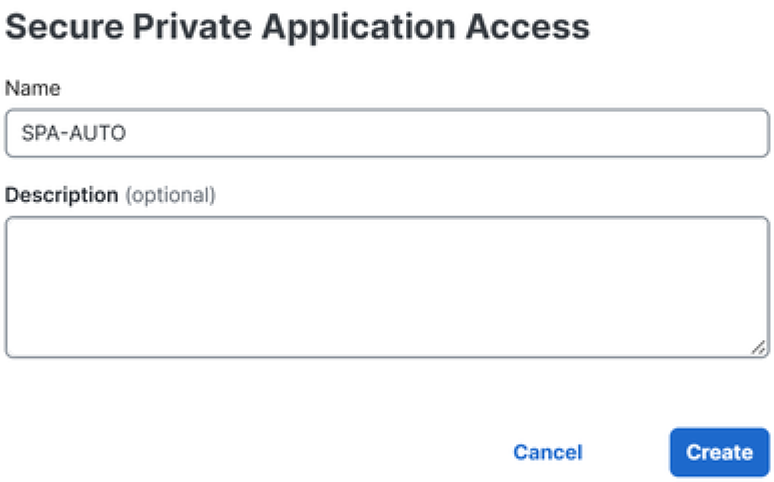
Secure Internet Gateway / Secure Service Edge 4

Search Table

Add Secure Internet Gateway (SIG) | Add Secure Internet Access | Add Secure Private Application Access

Name | Description | Solution

- Configure a name and click on Create

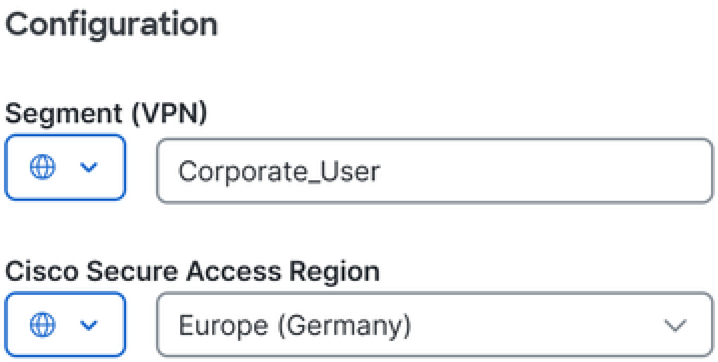


Secure Private Application Access

Name: SPA-AUTO

Description (optional)

The next configurations allows you to create the tunnels after you deploy the configuration in your Catalyst SD-WAN Edges:



Configuration

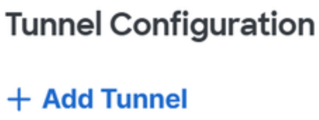
Segment (VPN): Corporate_User

Cisco Secure Access Region: Europe (Germany)

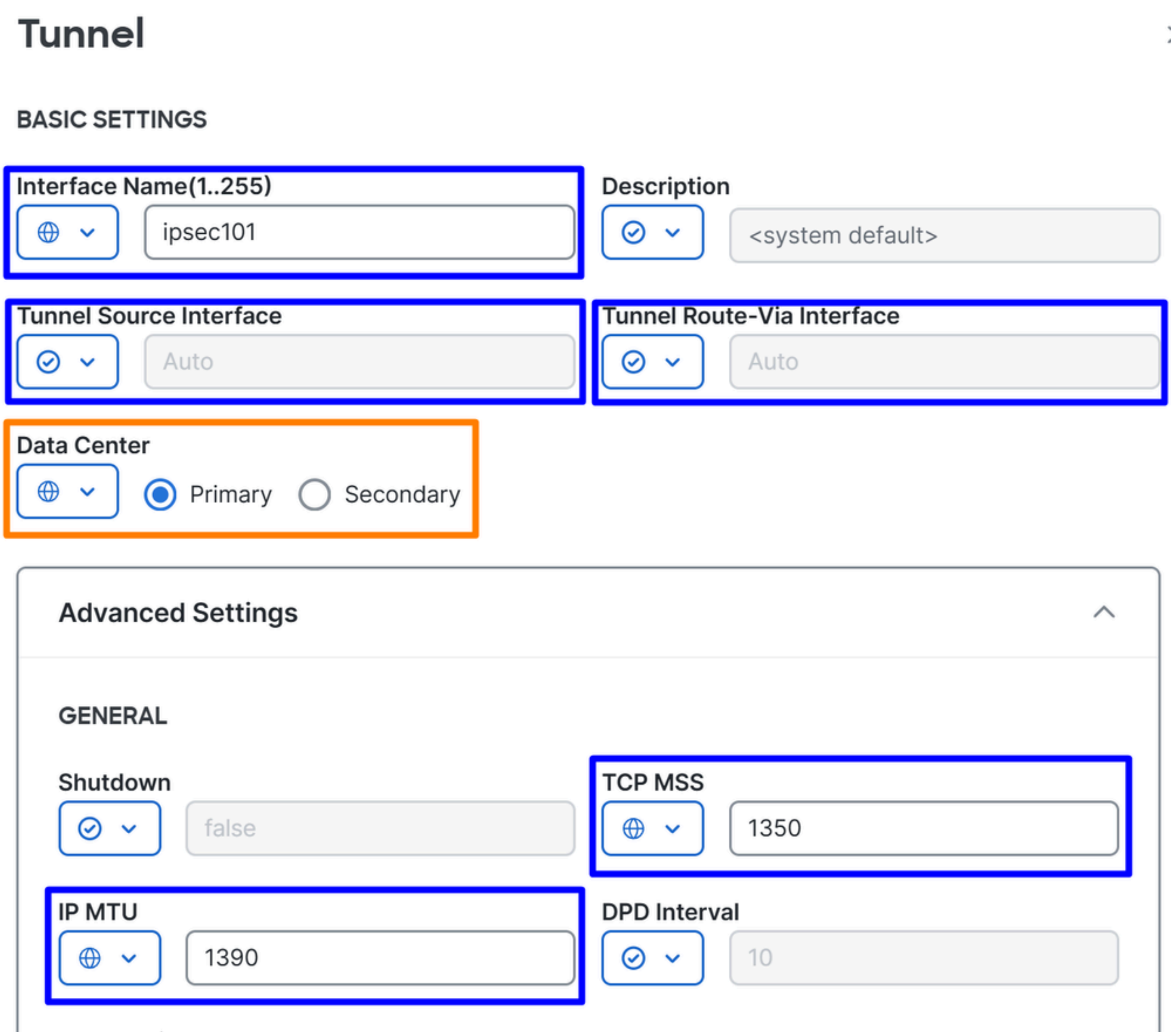
- Configuration
  - Segment (VPN): Choose the VRF that hosts the application(s) to be accessed through Secure Access
  - Cisco Secure Access Region: Choose the region closest to the SD-WAN hub or branch where the applications are hosted

Next, define the tunnel configuration. Tunnels created to the Primary Secure Access Data Center are active, while tunnels created to the Secondary Secure Access Data Center operate as backup.

Under Tunnel Configuration click + Add Tunnel:



Tunnel Configuration



Tunnel

BASIC SETTINGS

Interface Name(1..255): ipsec101

Description: <system default>

Tunnel Source Interface: Auto

Tunnel Route-Via Interface: Auto

Data Center: ● Primary ○ Secondary

Advanced Settings

GENERAL

Shutdown: false

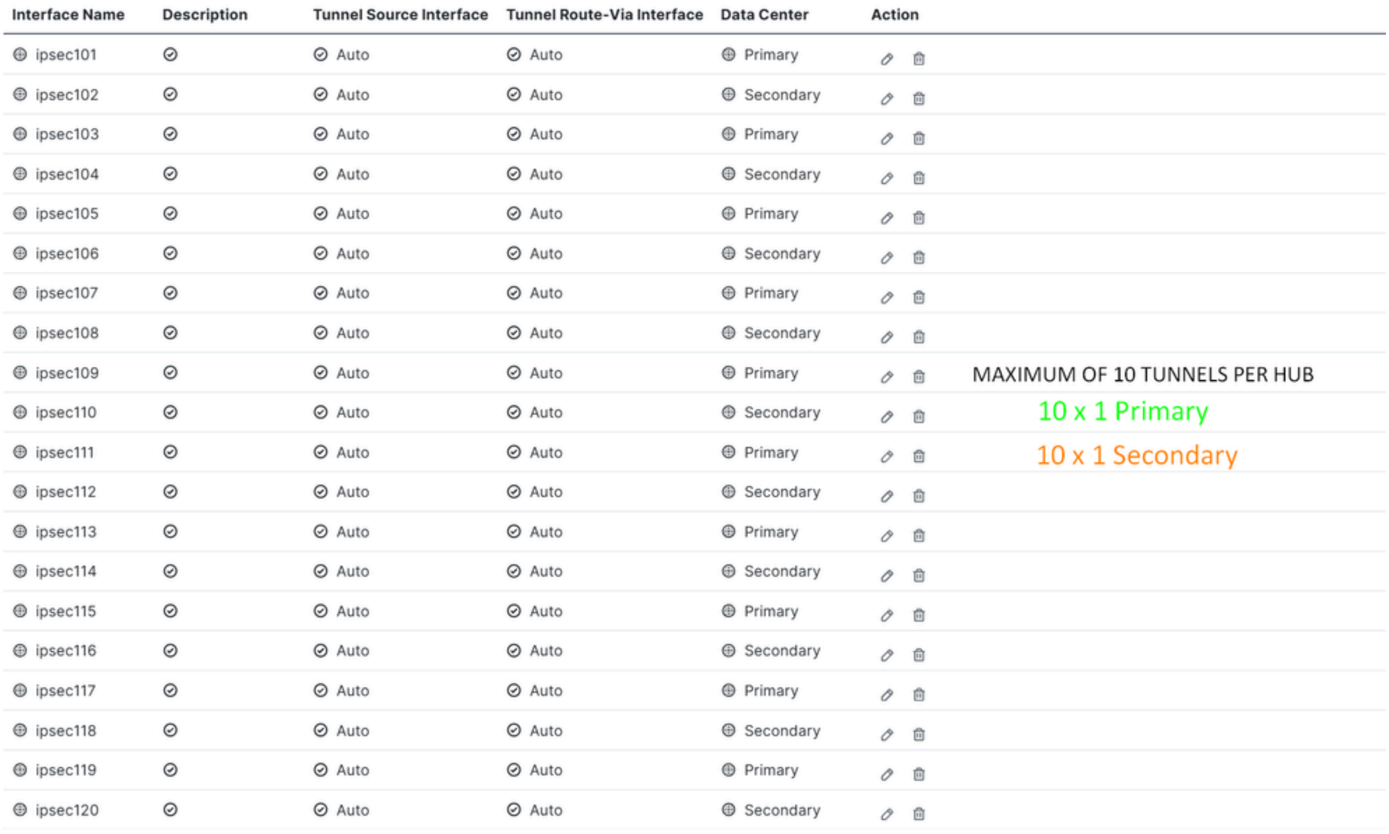
TCP MSS: 1350

IP MTU: 1390

DPD Interval: 10

- Tunnel
  - Interface Name: Specify tunnel name, it is automatically updated each time a new tunnel is added
  - Tunnel Source Interface: You do not need to change this setting. When left as Auto, the system automatically creates a loopback interface with a /31 mask.
  - Tunnel Route-Via Interface: You do not need to change this setting. By default, it uses the first NATed physical WAN interface on the edge router, but it can be changed if a specific WAN interface is required
  - Data Center: Select Primary or Secondary accordingly. If the primary tunnel is already configured, select Secondary. In normal scenarios, one tunnel can be configured as Primary and another as Secondary
  - Advanced Settings
    - IP MTU: Use 1390
    - TCP MSS: Use 1350

**Note**: If you want to create multiple tunnels to enable ECMP and increase tunnel capacity, you can configure up to 10 active/10 backup tunnels per router. This provides up to 10 × 4 Gbps per NTG.



| Interface Name | Description | Tunnel Source Interface | Tunnel Route-Via Interface | Data Center | Action |
|---|---|---|---|---|---|
| ipsec101 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec102 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec103 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec104 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec105 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec106 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec107 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec108 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec109 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec110 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec111 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec112 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec113 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec114 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec115 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec116 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec117 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec118 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |
| ipsec119 | ✓ | Auto | Auto | Primary | ✎ 🗑 |
| ipsec120 | ✓ | Auto | Auto | Secondary | ✎ 🗑 |

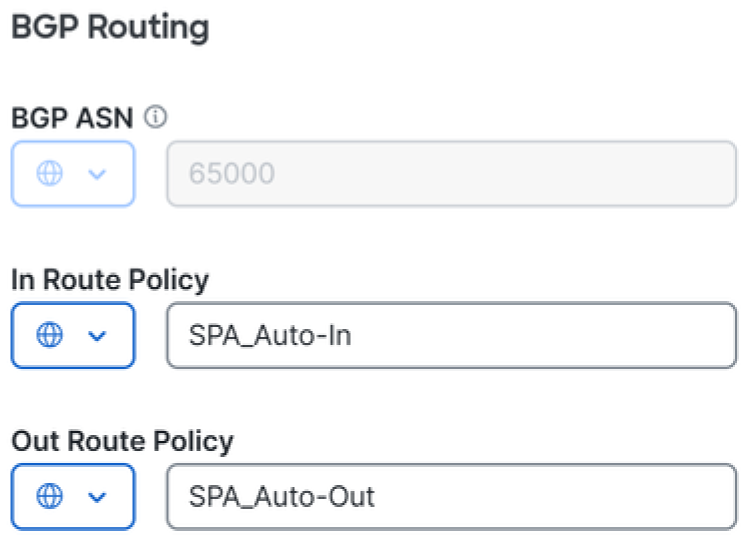
MAXIMUM OF 10 TUNNELS PER HUB

10 x 1 Primary

10 x 1 Secondary

**Note**:If deploying multiple tunnels per router, ensure that the transport interface can sustain the aggregate bandwidth of all active tunnels combined. For example, if two tunnels are expected to carry up to 1 Gbps each, the transport link must support at least 2 Gbps of throughput.

Once the tunnels are configured, proceed with the BGP configuration.



BGP Routing

BGP ASN ⓘ: 65000

In Route Policy: SPA_Auto-In

Out Route Policy: SPA_Auto-Out

- **BGP Routing**
  - BGP ASN**:** Specify AS number for the SD-WAN hub. The AS 64512 is reserved for Secure Access and can not be used. For more information about BGP, see
  - In Route Policy**:** The system automatically creates this inbound route policy with a deny all statement

    to prevent routing issues. It must be manually modified through a CLI Add-On Template to allow/deny the appropriate routes.
    - Out Route Policy: The system create this outbound route policy with a deny all statement to avoid routing problems. It must be manually edited through a CLI Add-On Template to allow/deny the appropriate routes.

---

**Warning**: Starting November 2025, all newly created Secure Access organizations use the public ASN 32644 by default for BGP peering in network tunnel groups. Existing organizations established prior to November 2025 continue to use the private ASN 64512 that was previously reserved for Secure Access BGP peers. If the private AS number 64512 is assigned to a device on your network, it not be able to peer with a network tunnel group configured for Peer (Secure Access) BGP AS 64512.

---

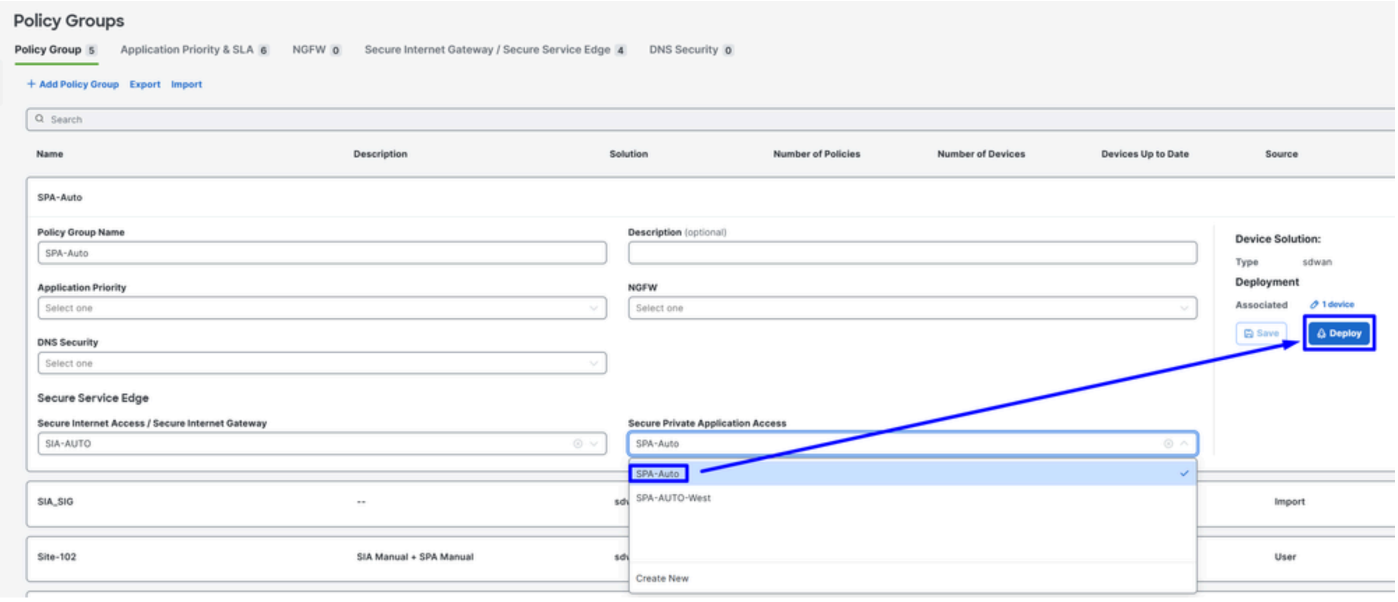
The next BGP and route-map configuration is automatically created for every BGP neighbor after you Deploy the new policy in your Policy Group.

```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

R104#sh run | s r b
router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
 ...
 maximum-paths 32
exit-address-family
```

After this, click Save and proceed with the policy deployment to bring the tunnels up.

- Click on Configuration > Policy Groups
- Choose under your Policy > Secure Service Edge > Secure Private Application Access and click on the recent profile created for SPA.
- Click Deploy to finalize



Policy Groups

Policy Group 5 | Application Priority & SLA 6 | NGFW 0 | Secure Internet Gateway / Secure Service Edge 4 | DNS Security 0

| Name | Description | Solution | Number of Policies | Number of Devices | Devices Up to Date | Source |
|---|---|---|---|---|---|---|
| SPA-Auto | | | | | | |
| SIA_SIG | -- | sd | | | | Import |
| Site-102 | SIA Manual + SPA Manual | sd | | | | User |

Policy Group Name: SPA-Auto

Application Priority: Select one

NGFW: Select one

DNS Security: Select one

Secure Service Edge

Secure Internet Access / Secure Internet Gateway: SIA-AUTO

Secure Private Application Access: SPA-Auto (SPA-Auto, SPA-AUTO-West, Create New)

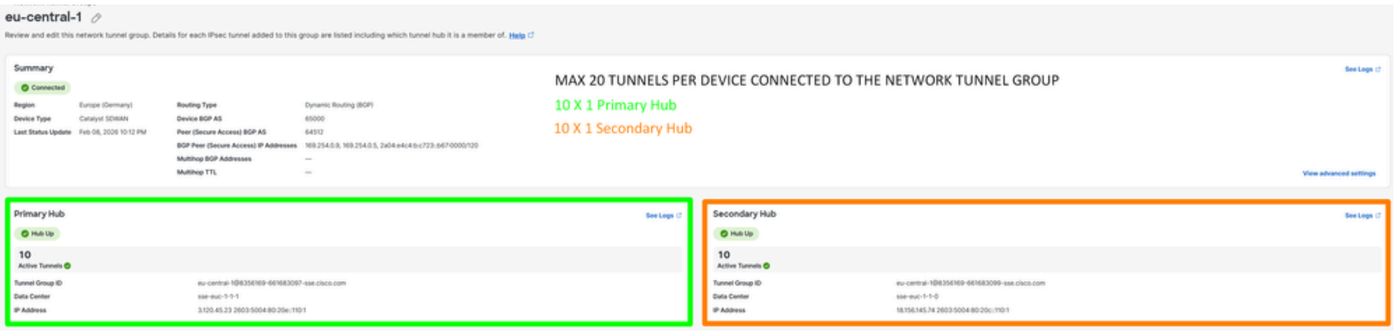
Device Solution: Type sdwan

Deployment: Associated 1 device

To verify inSecure Access, perform the next steps:

- Click on Connect> Network Connections

## TUNNEL ESTABLISHMENT



eu-central-1

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 | Europe (Germany) | Routing Type | Dynamic Routing (BGP) |
| Device Type | Catalyst SDWAN | Device BGP AS | 65000 |
| Last Status Update | Feb 08, 2026 10:12 PM | Peer (Secure Access) BGP AS | 64512 |
| | | BGP Peer (Secure Access) IP Addresses | 169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120 |
| | | Multihop BGP Addresses | — |
| | | Multihop TTL | — |

MAX 20 TUNNELS PER DEVICE CONNECTED TO THE NETWORK TUNNEL GROUP

10 X 1 Primary Hub

10 X 1 Secondary Hub

Primary Hub: Hub Up, 10 Active Tunnels

| | |
|---|---|
| Tunnel Group ID | eu-central-1@8356169-661683097-sse.cisco.com |
| Data Center | sse-euc-1-1-1 |
| IP Address | 3.120.45.23 2603:5004:80:20e::110:1 |

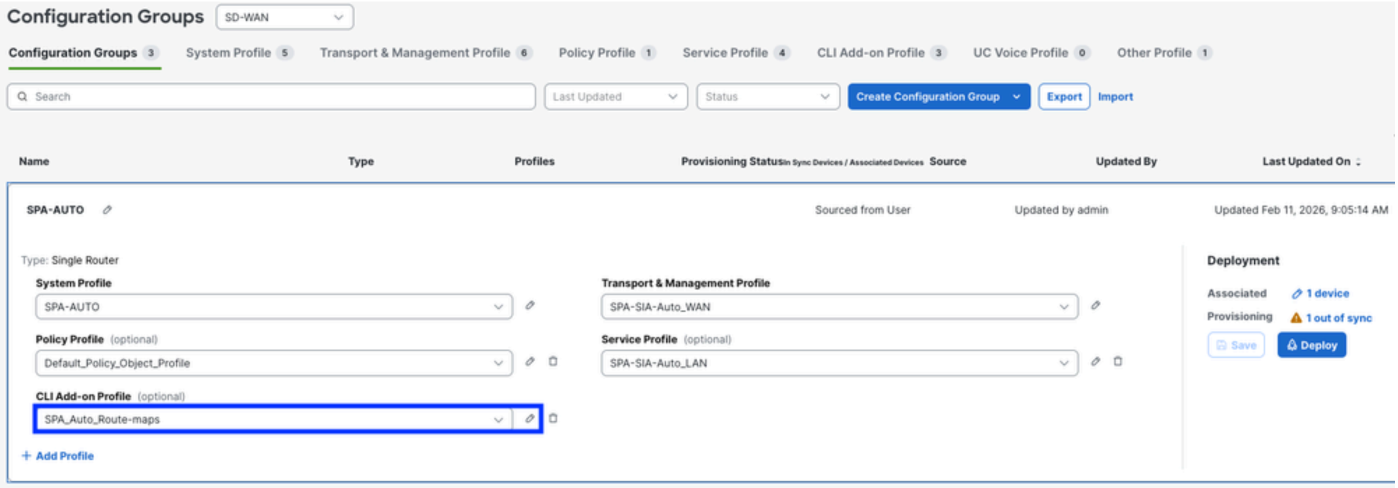
Secondary Hub: Hub Up, 10 Active Tunnels

| | |
|---|---|
| Tunnel Group ID | eu-central-1@8356169-661683099-sse.cisco.com |
| Data Center | sse-euc-1-1-0 |
| IP Address | 18.156.145.74 2603:5004:80:20c::110:1 |

## Configure Routing

Navigate to Configure > Configuration Groups

- Click on your Configuration Group and Create/Edit your CLI Add-on Profile



Configuration Groups SD-WAN

Configuration Groups 3 | System Profile 5 | Transport & Management Profile 6 | Policy Profile 1 | Service Profile 4 | CLI Add-on Profile 3 | UC Voice Profile 0 | Other Profile 1

| Name | Type | Profiles | Provisioning Status In Sync Devices / Associated Devices | Source | Updated By | Last Updated On |
|---|---|---|---|---|---|---|
| SPA-AUTO | | | | Sourced from User | Updated by admin | Updated Feb 11, 2026, 9:05:14 AM |

Type: Single Router

System Profile: SPA-AUTO

Transport & Management Profile: SPA-SIA-Auto_WAN

Policy Profile (optional): Default_Policy_Object_Profile

Service Profile (optional): SPA-SIA-Auto_LAN

CLI Add-on Profile (optional): SPA_Auto_Route-maps

Deployment: Associated 1 device; Provisioning 1 out of sync

To allow BGP routes exchange, use the previously configured In Route Policy and **Out Route Policy**. You can find a basic example for the CLI Add-On route configuration. This template provides a starting point and must be customized as needed:

```
ip bgp-community new-format
ip prefix-list ALL-ROUTES seq 5 permit 0.0.0.0/0 le 32

route-map SPA_Auto-In permit 10
match ip address prefix-list ALL-ROUTES
route-map SPA_Auto-In deny 65534
description Default Deny Configured from Secure Private Application Access feature

route-map SPA_Auto-Out permit 10
match ip address prefix-list ALL-ROUTES
description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
description Default Deny Configured from Secure Private Application Access feature

router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
network 172.16.104.0 mask 255.255.255.0
```

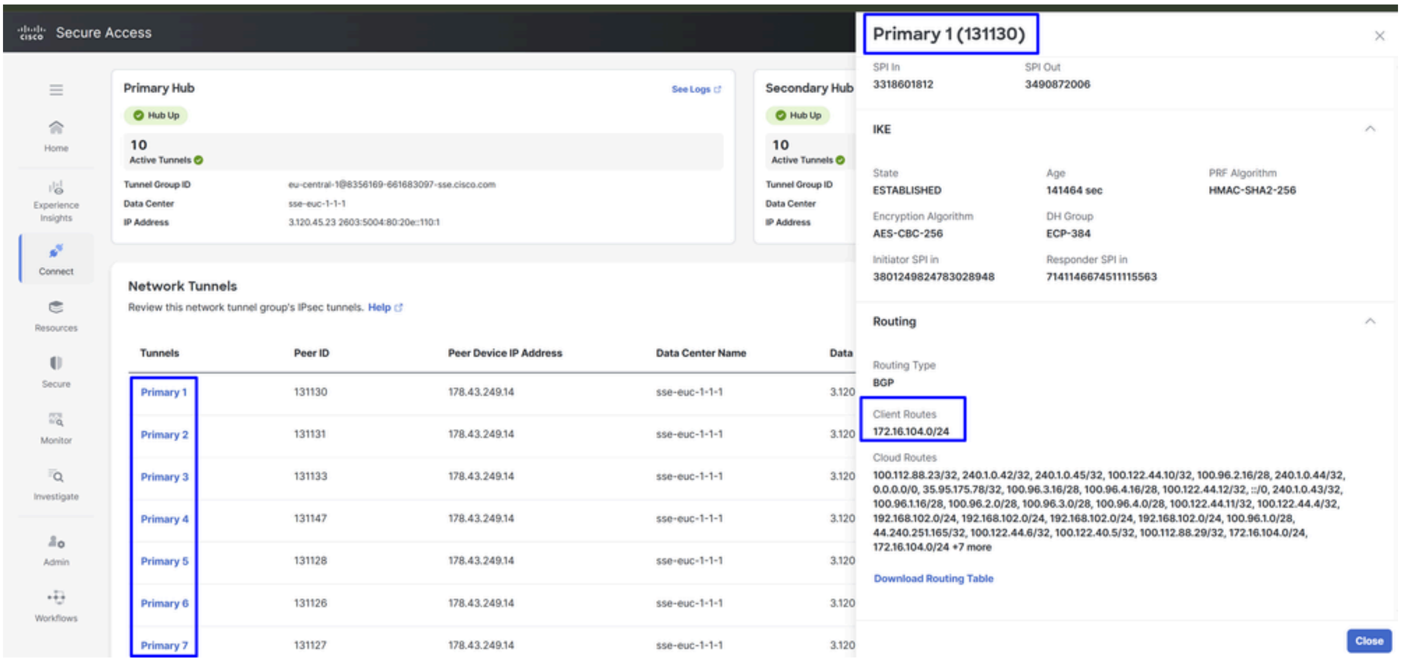
⚠ **Warning**: Careful planning is required when defining the networks permitted in and out through BGP route-maps. Permitting all routes, as shown in the example above, can introduce unintended routing behavior. For optimal deployment, explicitly specify only the necessary networks in your route-maps to ensure controlled and predictable routing outcomes

Now you can proceed to Deploy the changes

To verify if BGP routes are received inSecure Access, check the next steps:

- Click on Connect> Network Connections > Network Tunnel Groups and select the NTG name

**ROUTING ESTABLISHMENT**



Primary Hub

10 Active Tunnels

| | |
|---|---|
| Tunnel Group ID | eu-central-1@8356169-661683097-sse.cisco.com |
| Data Center | sse-euc-1-1-1 |
| IP Address | 3.120.45.23 2603:5004:80:20e::110:1 |

Secondary Hub

10 Active Tunnels

Tunnel Group ID
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 |
|---|---|---|---|---|
| Primary 1 | 131130 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |
| Primary 2 | 131131 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |
| Primary 3 | 131133 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |
| Primary 4 | 131147 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |
| Primary 5 | 131128 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |
| Primary 6 | 131126 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |
| Primary 7 | 131127 | 178.43.249.14 | sse-euc-1-1-1 | 3.120 |

Primary 1 (131130)

| SPI In | SPI Out |
|---|---|
| 3318601812 | 3490872006 |

IKE

| | | |
|---|---|---|
| State<br>ESTABLISHED | Age<br>141464 sec | PRF Algorithm<br>HMAC-SHA2-256 |
| Encryption Algorithm<br>AES-CBC-256 | DH Group<br>ECP-384 | |
| Initiator SPI in<br>3801249824783028948 | Responder SPI in<br>7141146674511115563 | |

Routing

Routing Type: BGP

Client Routes: 172.16.104.0/24

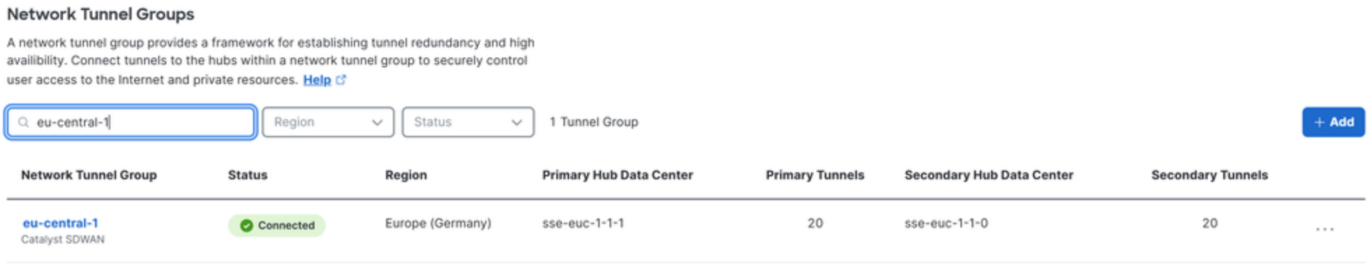
Cloud Routes: 100.112.88.23/32, 240.1.0.42/32, 240.1.0.45/32, 100.122.44.10/32, 100.96.2.16/28, 240.1.0.44/32, 0.0.0.0/0, 35.95.175.78/32, 100.96.3.16/28, 100.96.4.16/28, 100.122.44.12/32, ::/0, 240.1.0.43/32, 100.96.1.16/28, 100.96.2.0/28, 100.96.3.0/28, 100.96.4.0/28, 100.122.44.11/32, 100.122.44.4/32, 192.168.102.0/24, 192.168.102.0/24, 192.168.102.0/24, 192.168.102.0/24, 100.96.1.0/28, 44.240.251.165/32, 100.122.44.6/32, 100.122.40.5/32, 100.112.88.29/32, 172.16.104.0/24, 172.16.104.0/24 +7 more

Download Routing Table

**Note**: In this example, the corporate user subnet 172.16.104.0/24 is advertised to Secure Access through BGP. This allows proper routing between Catalyst SD-WAN and the SSE environment.

The same policy can be applied to both WAN edges in the Catalyst SD-WAN hubs, resulting in 20 active tunnels and 20 standby tunnels. The total number of tunnels depends on how many are configured on each edge. Any router connected to both Secure Access hubs (Hub 1 and Hub 2) forms an ECMP pair across all established tunnels.

For example, if Catalyst SD-WAN Edge 1 has 10 tunnels and Catalyst SD-WAN Edge 2 has 10 tunnels, Secure Access forms ECMP across the 20 active tunnels. The same behavior applies to the secondary SSE hub.



Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availibility. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. Help

1 Tunnel Group

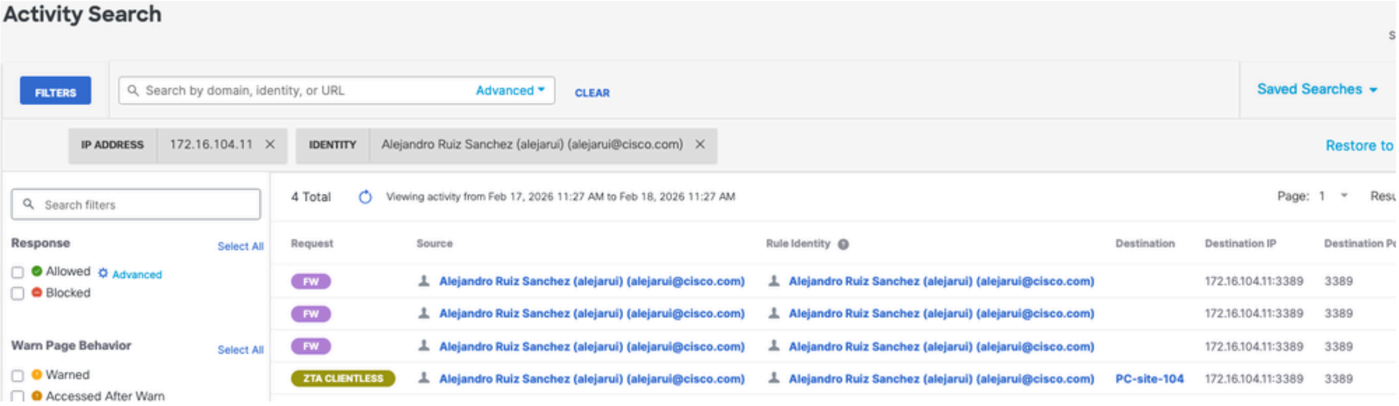
| Network Tunnel Group | Status | Region | Primary Hub Data Center | Primary Tunnels | Secondary Hub Data Center | Secondary Tunnels |
|---|---|---|---|---|---|---|
| eu-central-1<br>Catalyst SDWAN | Connected | Europe (Germany) | sse-euc-1-1-1 | 20 | sse-euc-1-1-0 | 20 |

# Verify

in order to verify if the traffic is going through Cisco Secure Access, navigate to Eventsor Activity Search or Network-Wide Path Insightsand filter by your tunnel identity:

## Secure Access - Activity Search

Navigate to Monitor>Activity Search :



## Activity Search

IP ADDRESS 172.16.104.11 ×   IDENTITY Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) ×

**Response** Select All

□ Allowed  Advanced
□ Blocked

**Warn Page Behavior** Select All

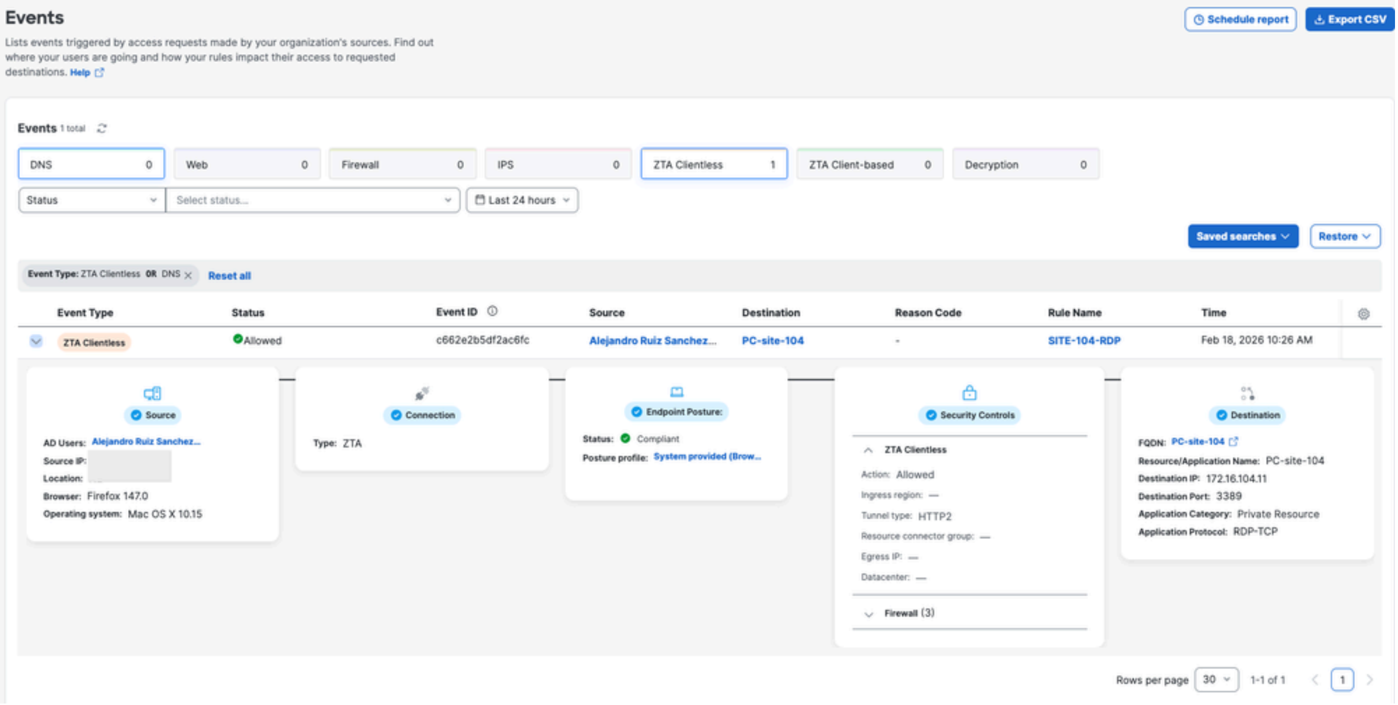
□ Warned
□ Accessed After Warn

4 Total   Viewing activity from Feb 17, 2026 11:27 AM to Feb 18, 2026 11:27 AM   Page: 1   Resu

| Request | Source | Rule Identity | Destination | Destination IP | Destination Po |
|---|---|---|---|---|---|
| FW | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | | 172.16.104.11:3389 | 3389 |
| FW | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | | 172.16.104.11:3389 | 3389 |
| FW | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | | 172.16.104.11:3389 | 3389 |
| ZTA CLIENTLESS | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com) | PC-site-104 | 172.16.104.11:3389 | 3389 |

# Secure Access - Events

Navigate to Monitor>Events:



## Events

Lists events triggered by access requests made by your organization's sources. Find out where your users are going and how your rules impact their access to requested destinations. Help

Events 1 total

| DNS | Web | Firewall | IPS | ZTA Clientless | ZTA Client-based | Decryption |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 | 0 |

Status: Select status...   Last 24 hours

Event Type: ZTA Clientless OR DNS ×   Reset all

| Event Type | Status | Event ID | Source | Destination | Reason Code | Rule Name | Time |
|---|---|---|---|---|---|---|---|
| ZTA Clientless | Allowed | c662e2b5df2ac6fc | Alejandro Ruiz Sanchez... | PC-site-104 | - | SITE-104-RDP | Feb 18, 2026 10:26 AM |

**Source**

AD Users: Alejandro Ruiz Sanchez...
Source IP: [redacted]
Location:
Browser: Firefox 147.0
Operating system: Mac OS X 10.15

**Connection**

Type: ZTA

**Endpoint Posture:**

Status: Compliant
Posture profile: System provided (Brow...

**Security Controls**

ZTA Clientless
Action: Allowed
Ingress region: —
Tunnel type: HTTP2
Resource connector group: —
Egress IP: —
Datacenter: —

Firewall (3)

**Destination**

FQDN: PC-site-104
Resource/Application Name: PC-site-104
Destination IP: 172.16.104.11
Destination Port: 3389
Application Category: Private Resource
Application Protocol: RDP-TCP

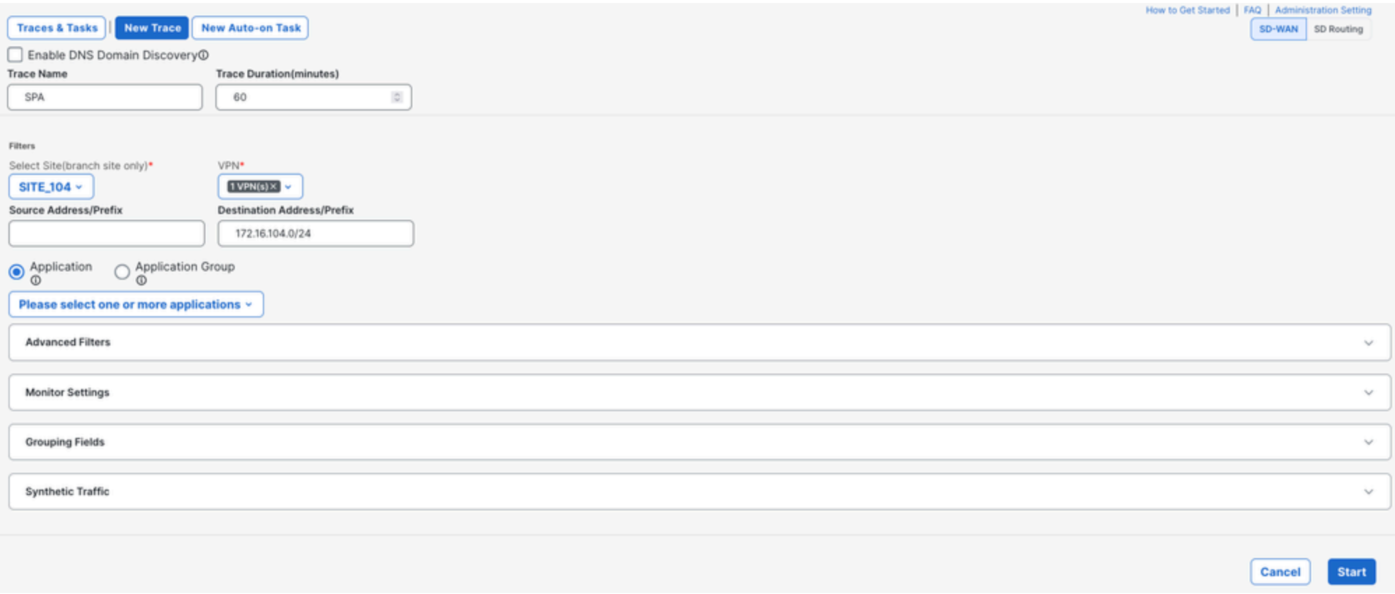
Rows per page 30   1-1 of 1   1

**Note**: Be sure you have your default policy with logging enabled, by default is disabled.

# Catalyst SD-WAN Manager - Network-Wide Path Insights

Navigate to Catalyst SD-WAN Manager:

- Click on Tools> Network-Wide Path Insights
- Click on New Trace



□ Enable DNS Domain Discovery ⓘ

Trace Name: SPA

Trace Duration(minutes): 60

Filters

Select Site(branch site only)*: SITE_104

VPN*: 1 VPN(s)

Source Address/Prefix:

Destination Address/Prefix: 172.16.104.0/24

● Application ⓘ ○ Application Group ⓘ

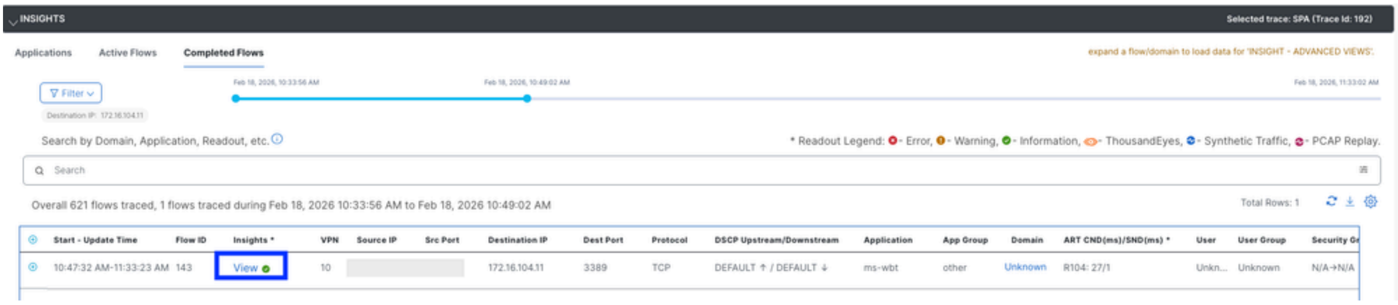
- Trace Name: (Optional) Specify Trace name

- Site: Choose the site where the private resource is located

- VPN: Choose the VPN ID where the private resource is located
- Source/Destination Address: (Optional) Enter the IP or leave it on blanck to capture all the traffic filtered based on **Site**and VPNchoosen

**Start** the trace

Locate the traffic flow and click *View* on the **Insights** column



INSIGHTS
Applications
Active Flows
Completed Flows
Filter
Feb 18, 2026, 10:33:56 AM
Feb 18, 2026, 10:49:02 AM
Feb 18, 2026, 11:33:02 AM
Search

Selected trace: SPA (Trace Id: 192)

expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Destination IP: 172.16.104.11

Search by Domain, Application, Readout, etc. ⓘ

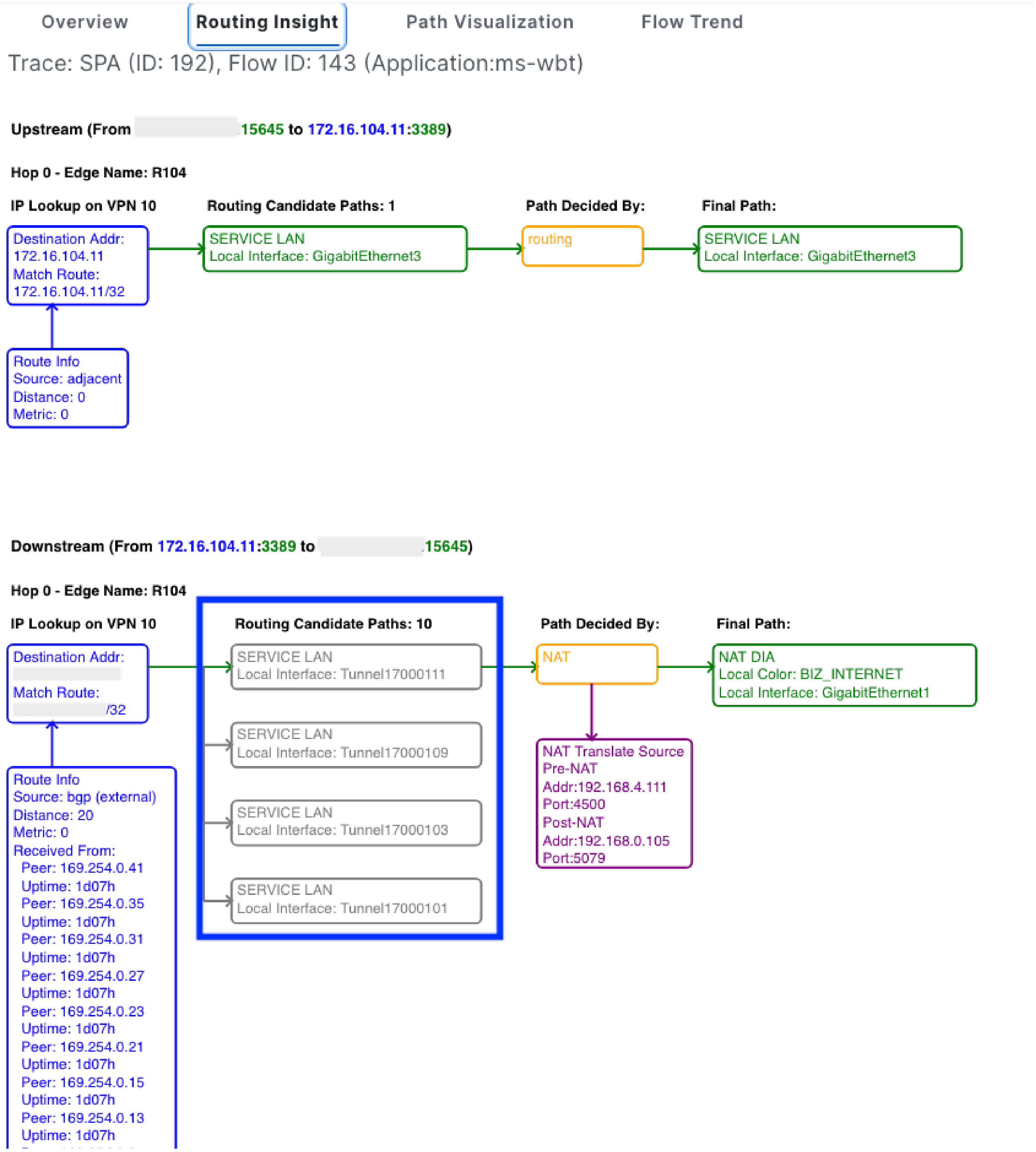
* Readout Legend: ● - Error, ● - Warning, ● - Information, ● - ThousandEyes, ● - Synthetic Traffic, ● - PCAP Replay.

Overall 621 flows traced, 1 flows traced during Feb 18, 2026 10:33:56 AM to Feb 18, 2026 10:49:02 AM

Total Rows: 1

| Start - Update Time | Flow ID | Insights * | VPN | Source IP | Src Port | Destination IP | Dest Port | Protocol | DSCP Upstream/Downstream | Application | App Group | Domain | ART CND(ms)/SND(ms) * | User | User Group | Security G |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10:47:32 AM-11:33:23 AM | 143 | View ● | 10 | [redacted] |  | 172.16.104.11 | 3389 | TCP | DEFAULT ↑ / DEFAULT ↓ | ms-wbt | other | Unknown | R104: 27/1 | Unkn... | Unknown | N/A→N/A |

The *routing Insights* column display the candidate paths and display the IPSec tunnels to Secure Access



Trace: SPA (ID: 192), Flow ID: 143 (Application:ms-wbt)

**Upstream (From [redacted]:15645 to 172.16.104.11:3389)**

**Hop 0 - Edge Name: R104**

**IP Lookup on VPN 10**

Destination Addr:
172.16.104.11
Match Route:
172.16.104.11/32

Route Info
Source: adjacent
Distance: 0
Metric: 0

**Routing Candidate Paths: 1**

SERVICE LAN
Local Interface: GigabitEthernet3

**Path Decided By:**

routing

**Final Path:**

SERVICE LAN
Local Interface: GigabitEthernet3

**Downstream (From 172.16.104.11:3389 to [redacted]:15645)**

**Hop 0 - Edge Name: R104**

**IP Lookup on VPN 10**

Destination Addr:
[redacted]
Match Route:
[redacted]/32

Route Info
Source: bgp (external)
Distance: 20
Metric: 0
Received From:
Peer: 169.254.0.41
Uptime: 1d07h
Peer: 169.254.0.35
Uptime: 1d07h
Peer: 169.254.0.31
Uptime: 1d07h
Peer: 169.254.0.27
Uptime: 1d07h
Peer: 169.254.0.23
Uptime: 1d07h
Peer: 169.254.0.21
Uptime: 1d07h
Peer: 169.254.0.15
Uptime: 1d07h
Peer: 169.254.0.13
Uptime: 1d07h

**Routing Candidate Paths: 10**

SERVICE LAN
Local Interface: Tunnel17000111

SERVICE LAN
Local Interface: Tunnel17000109

SERVICE LAN
Local Interface: Tunnel17000103

SERVICE LAN
Local Interface: Tunnel17000101

**Path Decided By:**

NAT

NAT Translate Source
Pre-NAT
Addr:192.168.4.111
Port:4500
Post-NAT
Addr:192.168.0.105
Port:5079

**Final Path:**

NAT DIA
Local Color: BIZ_INTERNET
Local Interface: GigabitEthernet1

# Related Information

- Cisco Technical Support & Downloads
- Cisco Secure Access Help Center
- Cisco SASE Design Guide
- Configure Secure Access with SD-WAN Automated Tunnels for Secure Internet Access
- Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

- Cisco SASE Solution: Cisco Catalyst SD-WAN integrated with Cisco Secure Access At-a-Glance