

Configure Secure Access with SD-WAN Automated Tunnels for Secure Internet 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](#)

[Create your Custom Bypass FQDN or APP in SD-WAN \(OPTIONAL\)](#)

[Routing your Traffic](#)

[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 SD-WAN Automated Tunnels for Secure Internet Access.



Secure Access and SDWAN for Secure Internet Access — with Automated Tunnels —

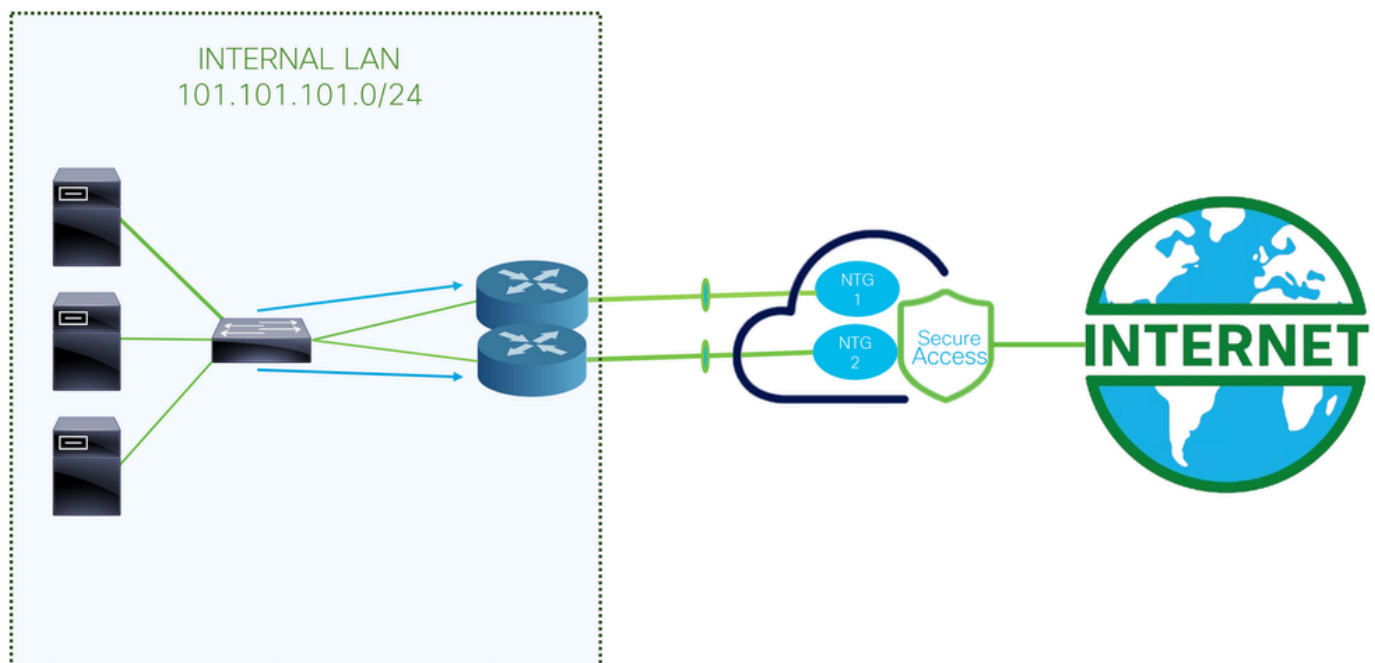
Background Information

As organizations increasingly adopt cloud-based applications and support distributed workforces, network architectures must evolve to provide secure, reliable, and scalable access to resources. Secure Access Service Edge (SASE) is a framework that converges networking and security into a single cloud-delivered service, combining SD-WAN capabilities with advanced security functions such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), DNS-layer security, Zero Trust Network Access (ZTNA) or integrated VPN for secure remote access.

Integrating Cisco Secure Access with SD-WAN through automated tunnels enables organizations to route internet traffic securely and efficiently. SD-WAN provides intelligent path selection and optimized connectivity across distributed locations, while Cisco Secure Access ensures that all traffic is inspected and protected according to corporate security policies before reaching the internet.

By automating tunnel configuration between SD-WAN devices and Secure Access, organizations can simplify deployment, improve scalability, and ensure consistent security enforcement for users-no matter where they are located. This integration is a key component of a modern SASE architecture, enabling secure internet access for branch offices, remote sites, and mobile users.

Network Diagram



This is the architecture used for this configuration example. As you can see, there are two edge routers:

If you choose to deploy the policies to two different devices, an NTG is configured for each router, and NAT is enabled on the Secure Access side. This allows both routers to send traffic from the same source through the tunnels. Normally, this is not permitted; however, enabling the NAT option for these tunnels allows two edge routers to send traffic originating from the same source address.

Prerequisites

Requirements

- Secure Access Knowledge
- Cisco Catalyst SD-WAN Manager Release 20.15.1 and Cisco IOS XE Catalyst SD-WAN Release 17.15.1 or later
- Intermediate knowledge of routing and switching
- ECMP Knowledge
- VPN Knowledge

Components Used

- Secure Access Tenant
- Catalyst SD-WAN Manager Release 20.18.1 and Cisco IOS XE Catalyst SD-WAN Release 17.18.1
- 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.

<input type="checkbox"/> Admin	17 >
<input checked="" type="checkbox"/> Deployments	23 >
<input type="checkbox"/> Investigate	2 >
<input type="checkbox"/> Policies	25 >
<input type="checkbox"/> 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

[ADD](#)

[CANCEL](#)

[CREATE KEY](#)



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

397766cdb29f43b08dde3b1d8c04e45 [Copy](#)

Key Secret

bfce729cd3e243e281df7271acb12208 [Copy](#)



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 SSE and fill the API and Organization Settings

- Organization ID: You can take that from the URL of your 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 4

Transport

Q Search

Las

Name	Type	Profiles
SIA Secure Internet Access R1 + R2 		
Type: Single Router		
System Profile		
<div>SIA_Basic</div>		
Service Profile (optional)		
<div>SIA_LAN</div>		 
+ Add Profile		

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

SIA_Basic [Edit](#)

Description: SIA Basic Profile

Device solution: SD-WAN Updated by: admin Last updated: Nov 05, 2025 03:37:09 PM Shared: 1 Group

Q 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

HTTP Server: ☐ ☐
 FTP Passive: ☐ ☐
 ARP Proxy: ☐ ☐
 Cisco Discovery Protocol (CDP): [Cisco Discovery Protocol \(CDP\)](#)

HTTPS Server: ☐ ☐
 Domain Lookup: ☒ ☒
 RSH/RCP: ☐ ☐
 Line Virtual Teletype (Configure O): [Line Virtual Teletype \(Configure O\)](#)

Configure Policy Group

Navigate to **Configuration > Policy Groups**:

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

Policy Group 4 Application Priority & SLA 3 NGFW 0 **Secure Internet Gateway / Secure Service Edge 3**

Secure Internet Gateway / Secure Service Edge 3

Q Search Table

[Add Secure Internet Gateway \(SIG\)](#)
[Add Secure Internet Access](#)
[Add Secure Private Application Access](#)



Note: In releases lower than 20.18 this option is called Add Secure Service Edge (SSE)

- Configure a name, solution and click on Create

Secure Internet Access

Name

SIA

Solution

sdwan

Description (optional)

Cancel

Create

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

SSE Provider

☒ Cisco SSE ☐ Zscaler

Context Sharing

☒ VPN ☒ SGT

Tracker

Source IP address

{{ Monitoring }}

- SSE Provider: **SSE**
- Context Sharing: Choose VPN or/and SGT depends of your needs
- Tracker
 - **Source IP Address:** Choose Device Specific (This permit you to modify it per device and identify the use case for it in the deployment stage)

Under the Configuration step you set up the tunnels:

Configuration

[+ Add Tunnel](#)

Single Hub HA Scenario

ECMP Scenario with HA

Single Hub HA Scenario

Max one tunnel per hub

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface*: GigabitEthernet1

Tunnel Route Via: <SYSTEM DEFAULT>

Tracker: DefaultTracker

Data Center: Primary

ECMP Scenario with HA

Max 8 Tunnels per Hub 8GB X 1

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface*: Loopback1

Tunnel Route Via: GigabitEthernet1

Tracker: DefaultTracker

Data Center: Primary

By default, for the tunnel route, the system will select the first NAT-enabled interface it finds. If there is more than one, you should select your desired WAN interface.

- **Single Hub HA Scenario:** In this scenario, you can configure high availability using one NTG as active and another as passive, with a maximum throughput of 1Gbps per NTG
- **ECMP Scenario with HA:** In this scenario, you can configure up to 8 tunnels per hub, supporting a total of up to 16 tunnels per NTG. This setup allows for higher throughput across the tunnels



Note: If your network interfaces have a throughput greater than 1Gbps and you require scalability, you must use loopback interfaces. Otherwise, you can use standard interfaces on your device. This is to enable ECMP from Secure Access side.



Warning: If you want to configure loopback interfaces for an ECMP scenario, you must first set up the loopback interfaces in Configuration Groups > Transport & Management Profile, under the policy that you use in your router.

- Click on Add Tunnel

Edit Tunnel

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface*: Loopback1

Tunnel Route Via: GigabitEthernet1

Tracker: DefaultTracker

Data Center: Primary

- Interface Name: ipsec1, ipsec2, ipsec3 and so on
- Tunnel Source

Interface: Choose Loopback Interfaces or specific one from where you establish the tunnel

- **Tunnel Route Via:** If you choose Loopback, you need to select the physical interface from which you want to route the traffic. If you do not select Loopback, this option appeared grayed out, and use the first NAT enabled interface the system founds. If there is more than one, you must select your desired WAN interface
- **Data Center:** This means to which Hub in Secure Access you establish the connection

The next part of the tunnel configuration you configure the tunnels with the best practices provided by Cisco.

▼ Advanced Options

General

Shutdown

☒ ☐

Track this interface

☒ ☐

TCP MSS

☒

1350

IP MTU

☒

1390

DPD Interval

☒

10

DPD Retries

☒

3

IKE Diffie-Hellman Group

☒

20

- TCP MSS: 1350
- IP MTU: 1390
- IKE Diffie-Hellman Group: 20

After that you must configure the Secondary Tunnel pointing to the Secondary Datacenter.

SINGLE HUB HA SCENARIO

Configuration

+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		<input checked="" type="checkbox"/> false	1350	1390	
ipsec2		<input checked="" type="checkbox"/> false	1350	1390	

This is the final result when you use the normal scenario deployment.

ECMP SCENARIO WITH HA

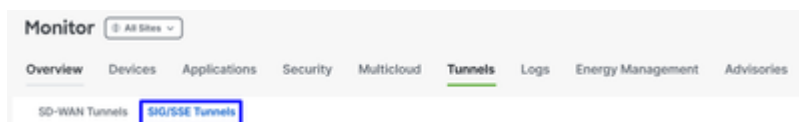
Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1	PRIMARY HUB	☑ false	1350	1390
ipsec2		☑ false	1350	1390
ipsec3		☑ false	1350	1390
ipsec4		☑ false	1350	1390
ipsec5		☑ false	1350	1390
ipsec11	SECONDARY HUB	☑ false	1350	1390
ipsec12		☑ false	1350	1390
ipsec13		☑ false	1350	1390
ipsec14		☑ false	1350	1390
ipsec15		☑ false	1350	1390

Then, you need to configure High Availability in the Secure Internet Policy.

High Availability

[+ Add Interface Pair](#)

Click on Add Interface Pair:



Edit Interface Pair



Active Interface		Active Interface Weight	
<input type="text" value="ipsec1"/>	<input type="text" value="1"/>		
Backup Interface		Backup Interface Weight	
<input type="text" value="ipsec11"/>	<input type="text" value="1"/>		

Tunnel Type	<input checked="" type="radio"/> IPsec	Tunnel Type	<input checked="" type="radio"/> IPsec
Interface Name(1..255)	<input type="text" value="ipsec1"/>	Interface Name(1..255)	<input type="text" value="ipsec11"/>
Tunnel Source Interface*	<input type="text" value="Loopback1"/>	Tunnel Source Interface*	<input type="text" value="Loopback11"/>
Tunnel Route Via	<input type="text" value="GigabitEthernet1"/>	Tunnel Route Via	<input type="text" value="GigabitEthernet1"/>
Tracker	<input type="text" value="DefaultTracker"/>	Tracker	<input type="text" value="DefaultTracker"/>
Data Center	<input checked="" type="radio"/> Primary <input type="radio"/> Secondary	Data Center	<input type="radio"/> Primary <input checked="" type="radio"/> Secondary

In this step, you need to configure the primary and secondary tunnel for each tunnel pair you are setting up. This means that each tunnel have its own backup. Remember, these tunnels were created as Primary and Secondary for this exact purpose.

"Active interface" refers to the Primary tunnel, while "Backup interface" refers to the Secondary tunnel:

- Active Interface: Primary
- Backup Interface: Secondary



Warning: If this step is skipped, the tunnels do not come up, and no connection is established from the routers to Secure Access.

After High Availability is configured for the tunnels, the setup is displayed as shown in the image below. In the lab example used for this guide, five tunnels are shown in HA. The number of tunnels can be adjusted as needed.

High Availability

[+ Add Interface Pair](#)

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
<input checked="" type="radio"/> ipsec1	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> ipsec11	<input checked="" type="radio"/> 1	
<input checked="" type="radio"/> ipsec2	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> ipsec12	<input checked="" type="radio"/> 1	
<input checked="" type="radio"/> ipsec3	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> ipsec13	<input checked="" type="radio"/> 1	
<input checked="" type="radio"/> ipsec4	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> ipsec14	<input checked="" type="radio"/> 1	
<input checked="" type="radio"/> ipsec5	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> ipsec15	<input checked="" type="radio"/> 1	

Cancel

Save



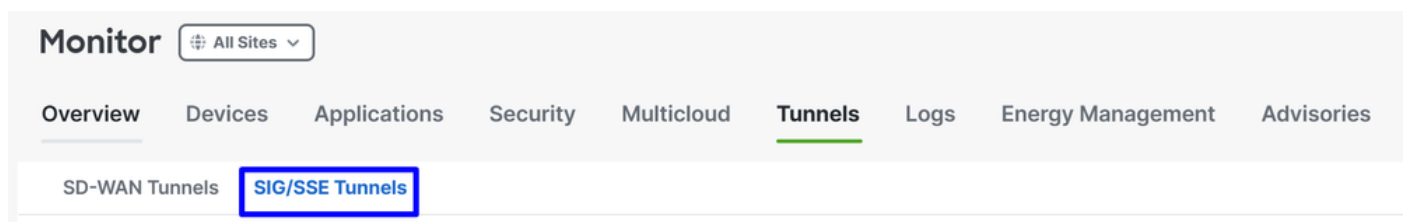
Note: A maximum of 8 tunnel pairs (16 tunnels: 8 primary and 8 secondary) can be configured in SD-WAN Catalyst vManage. Cisco Secure Access supports up to 10 tunnel pairs.

- Click Save

After this point, if everything is correctly configured, the tunnels appear as UP in the SD-WAN Manager and Secure Access.

To verify in SD-WAN, check the next steps:

- Click on Monitor > Tunnels
- Then Click on SIG/SSE Tunnels



And you are able to see the tunnels established to Cisco Secure Access UP or not.

Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000002	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000003	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000004	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000005	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000006	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000007	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000008	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000011	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000012	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000013	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000014	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000015	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000016	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000017	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000018	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

To verify in Secure Access, check the next steps:

- Click on Connect > Network Connections

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Q

5b28-4db0-b62e-9b589b5c687d

Region

Status

1 Tunnel Group

+ Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels	
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d Catalyst SDWAN	Connected	Europe (Germany)	sse-euc-1-1-1	8	sse-euc-1-1-0	8	...

In a detailed view, click the name of the tunnel:

PRIMARY

Active Tunnels

Tunnel Group ID: C98-PRV-500-5028-4800-642e-9658965c687a9d35d169-601691014-see.cisco.com

Data Center: sse-euc-1-1-1

IP Address: 3.120.43.23.2603.5004.80.20c.110.1

SECONDARY

Active Tunnels

Tunnel Group ID: C98-PRV-500-5028-4800-642e-9658965c687a9d35d169-601691014-see.cisco.com

Data Center: sse-euc-1-1-0

IP Address: 18.106.145.74.2603.5004.80.20c.110.1

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	131085	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 2	131086	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 3	131086	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 4	131087	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 5	131095	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 6	131077	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 7	131094	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 8	131078	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Secondary 1	65559	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 2	65560	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 3	65538	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 4	65548	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 5	65552	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 6	65554	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 7	65555	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 8	65558	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM

After this, you can move to the step, Create your Custom Bypass FQDN or APP in SD-WAN

Create your Custom Bypass FQDN or APP in SD-WAN (OPTIONAL)

There are special use cases where you need to create Application Bypass and FQDN or IP that you can apply to your routing policies:

Navigate to SD-WAN Manager portal:

- Click on Configuration > Application Catalog > Applications

Application Catalog

SD-AVC EnabledConfigure Cloud Connection

OverviewApplicationsApplication Source SettingsCloud Sourced ApplicationsDiscovered Application0Application ListsConflicts

Applications 1553Select Application AttributesChoose FilterCustom ApplicationExport

Search Table

0 selectedCreate Application ListDefine Probe EndpointAs of: Dec 23, 2025 05:00:05 PM

Application Name	Application Family	Application Group	Application Source	SaaS probe endpoint type	SaaS probe endpoint value	Traffic Class	Business Relevance	Action
Zannet	file-server	other	inBuiltApps	-	-	bulk-data	Silver	...



Tip: If running a version lower than 20.15, custom applications can be created under Policy Lists



Note: In order to have access to the Application Catalog you must enable SD-AVC.

- Click on Custom Application

Applications 1553 Select Application Attributes Choose Filter Custom Application Export

Search Table

0 selected [Create Application List](#) [Define Probe Endpoint](#) As of: Dec 23, 2025 05:00:05 PM

At this stage, a basic exclusion is configured using the Secure Client – Umbrella Module SWG FQDN:

ProxySecureAccess

Custom Application

Application Name ProxySecureAccess
Application Name: ProxySecureAccess-Custom

Server Names swg-url-proxy-https-sse.sigproxy.qq.opendns.com

Name of the Custom APP

FQDN

Application Family Select Application Family

Application Group Select Application Group

Traffic Class Select Traffic Class

Business Relevance Select Business Relevance

+ L3/L4 Attributes

IPv4 Address	Ports	L4 Protocol
10.X.X.X, 20.0.0.0/24 separated by	Space separated ports or range or	Enter L4 Protocol

SaaS probe endpoint type
☐ IP Address ☐ FQDN ☐ URL

SaaS probe endpoint value

Cancel Save

- Server Name: Use the FQDN that you would like to bypass (In this example FQDN of SWG are configured)
 - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
 - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Click on Save



Note: Change ORGID with your SSE organization number.

Next, a basic exclusion is created; in this case, the Umbrella DNS servers:

UmbrellaDNS

Custom Application ×

Name of the Custom App → **Application Name** ⓘ

UmbrellaDNS
Application Name: UmbrellaDNS-Custom

Server Names ⓘ
Enter Server Names

Application Family
Select Application Family ▼

Application Group
Select Application Group ▼

Traffic Class
Select Traffic Class ▼

Business Relevance
Select Business Relevance ▼

+ L3/L4 Attributes

IPv4 Address ⓘ	Ports ⓘ	L4 Protocol ⓘ
208.67.220.220,208.67.222.222	Space separated ports or range or	Enter L4 Protocol ▼

Configure IP addresses to exclude

SaaS probe endpoint type
☐ IP Address ☐ FQDN ☐ URL

SaaS probe endpoint value

Cancel Save

Now you can proceed with the configurations of the routing policies.

Routing your Traffic

In this step, you need to route internet traffic through the tunnels to protect it via Cisco Secure Access. In this case, you use a flexible routing policy that allows us to bypass certain traffic-helping to prevent sending unwanted traffic through Secure Access or to avoid potential bad practices.

First, let it define the two routing methods that can be used:

- Configuration > Configuration Groups > Service Profile > Service Route: This method provides routing to Secure Access, but lacks flexibility.
- **Configuration** > Policy Groups > Application Priority & SLA: This method offers various routing options within SD-WAN and, most importantly, allows you to bypass specific traffic so it is not sent through Secure Access.

For flexibility and alignment with best practices, this configuration is used, Application Priority & SLA:

- Click on **Configuration** > Policy Groups > Application Priority & SLA
- Then click on Application Priority & SLA Policy

Policy Groups

Policy Group 4

Application Priority & SLA 4

NGFW 0

Secure Internet Gateway / Secure Service Edge 3

DNS Security 0

Application Priority & SLA Policy 4

Q Search Table

Application Priority & SLA Policy

Name

Description

References

Update

- Configure a Policy Name and click Create

Application Priority & SLA Policy

Policy Name

SIA-ROUTE

Description (optional)

Cancel

Create

- Enable Advanced Layout
- Click on + Add Traffic Policy

Policies > Application Priority & SLA
SIA-ROUTE 

 Additional Settings Advanced Layout 

SLA Class QoS Queue

No SLA Class added, add your first SLA Class in Traffic Policy

 Change made in advanced view won't save to simple view.

[+ Add Traffic Policy](#)

Add Traffic Policy List

Policy Name

SSE

VPN(s)

Corporate_Users

Direction

From Service

Default action

☒ Accept ☐ Drop

Cancel

Add

- Policy Name: Name that adjust this to the purpose of this Traffic Policy List
- VPN(s): Choose the Service VPN of user from where you route the traffic
- **Direction:** From Service
- Default action: Accept

After that you are able to start the creation of the Traffic Policy:

In this way, you are bypassing the routing of specific traffic to Secure Access

VPN: Corporate_Users Direction: From Service Default Action: Accept

Search rule by name or order

	NAME	MATCH	ACTION	
1	LocalNetwork	Destination Ip · 172.16.200.0/24 Source Ip · 101.101.101.0/24	Base action · accept	⋮
2	BypassSSEP	App List · SecureAccessProxy	Base action · accept	⋮
3	UmbrellaDN	App List · UmbrellaDNS	Base action · accept	⋮
4	SIA AUTO F	Source Ip · 101.101.101.0/24	Base action · accept Sse Secure Service Edge · true Sse Secure Service Edge Instance · Cisco-Secure-Access	⋮

Traffic is matched in order, starting from the highest priority rule to the lowest.

In this way, you are sending specific traffic to Secure Access to be protected

1. Local Network Policy (Optional): Source 101.101.101.0/24, Destination 172.16.200.0/24. This route prevents intra-network traffic from being sent to Cisco Secure Access. Typically, customers do not do this, as internal routing is usually handled by the distribution router in SD-WAN deployments. This configuration ensures that internal traffic between these subnets is not routed to Secure Access, depending on whether your scenario requires it (Optional, depends of your network enviroment)
2. BypassSSEProxy (Optional): This policy prevents internal computers with the Cisco Umbrella module in

Secure Client and SWG enabled from sending proxy traffic back to the cloud. Routing proxy traffic to the cloud again is not considered best practice.

3. UmbrellaDNS (Best Practice): This policy prevents DNS queries destined for the internet from being sent through the tunnel. Sending DNS queries to Umbrella resolvers (208.67.222.222,208.67.220.220) via the tunnel is not recommended.
4. SIA AUTO FULL TRAFFIC: This policy routes all traffic from the source 101.101.101.0/24 to the internet through the SSE tunnels you previously created, ensuring this traffic is protected in the cloud.

Verify

in order to verify if the traffic is flooding already through Cisco Secure Access, navigate to Events OR Activity Search OR Network-Wide Path Insights and filter by your tunnel identity:

Secure Access - Activity Search

Navigate to Monitor > Activity Search:

The screenshot displays the Cisco Secure Access Activity Search interface. At the top, there's a search bar with filters and a 'CLEAR' button. Below the search bar, the interface is divided into three main sections: filters, activity results, and event details.

Filters: The 'Response' filter is set to 'Allowed'. The 'Warn Page Behavior' filter is set to 'Warned'. The 'Isolate' filter is set to 'Isolated'. The 'IPS Signature' filter is set to 'Log Only'.

Activity Results: The table shows 1,617 total results. The columns are: Request, Source, Rule Identity, Destination, Destination IP, Destination Port, and Destination Country. The results are filtered by the identity 'CSK-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6'.

Event Details: The sidebar shows details for the selected event. The Action is 'Allowed'. The Time is 'Dec 28, 2025 6:14 AM'. The Rule Name is 'For all Internet access (2100958)'. The Source is 'VPN-10 (VPN-10)'. The Source IP is '101.101.101.20'. The Destination is 'https://youtube.com'. The Security Group Tag (SGT) is '1'.

Secure Access - Events

Navigate to Monitor > Events:

>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	829e0bbdea6514e	C8K-PAYG-560-5b...	8.8.8.8:53	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Connect	Allowed	204e46d757b128d7	C8K-PAYG-560-5b...	8.8.8.8	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	829e0bbdea6514e	C8K-PAYG-560-5b...	8.8.8.8:53	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	eecb39315cdde282	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	eecb39315cdde282	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
✓	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM

Source

Network Tunnels: C8K-PAYG-0f3-d4e...

Viptela VPN: VPN-10 (VPN-10)...

Source IP: 101.101.101.20

Source port: 55240

Connection

Type: Network Tunnel

Security Controls

Firewall

Allow: 9 [View all](#)

Action: Allow

Egress IP: -

Egress Type: -

Datacenter: Europe (Germany)

No file control event found.

Destination

FQDN: -

Resource/Application Name: -

Destination IP: 110.234.18.177

Destination Port: 443

Destination List: -

Protocol: TCP

Session Bytes Received: 180

Session Bytes Sent: 362

Application Category: -

Application Protocol: -

Content Category: -

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

Traces & Tasks
New Trace
New Auto-on Task

☐ Enable DNS Domain Discovery ⓘ

Trace Name
Trace Duration(minutes)

e.g trace_[site ID]
60

Filters

Select Site(branch site only)*
VPN*

SITE_101 ▾
1 VPN(s) × ▾

Source Address/Prefix
Destination Address/Prefix

101.101.101.20

☒ Application ⓘ
☐ Application Group ⓘ

- Site: Choose the site from where your traffic is egressing
- VPN: Choose the VPN ID of your subnet from where your traffic is egressing
- Source: Put the IP or let it on blank to filter all the traffic filtered by the Site and VPN chosen

Then in Insights you are able to see the traffic flooding through the tunnels and the type of traffic going to Secure Access:

INSIGHTS Selected trace: trace_80 (Trace ID: 80)

Applications **Active Flows** Completed Flows Selected Flow ID: 50

Filter

Search by Domain, Application, Readout, etc.

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

Search

Total Rows: 10

Start - Update Time	Flow ID	Insights *	VPN	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	
7:26:05 AM-7:34:05 AM	50	View	10	101.101.101.20	54688	172.211.123.249	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g...	N/A	
Direction	Hop Index	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms) *	Latency(ms) *	ART CND(ms)/SND(ms) *		
Upstream	0	R101-2(Tunnel16000003)	SIG	BIZ_INTERNET (SIG)	N/A	0.00	N/A	N/A	N/A	N/A	R101-2: N/A		
Downstream	0	SIG	(Tunnel16000003)R101-2	N/A	BIZ_INTERNET (SIG)	N/A	N/A	0.00	N/A	N/A	N/A		
7:35:23 AM-7:35:23 AM	563	View	10	101.101.101.20	56408	172.211.123.248	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g...	N/A	
7:37:35 AM-7:37:35 AM	668	View	10	101.101.101.20	53175	8.8.8.8	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	N/A	
7:37:38 AM-7:37:38 AM	573	View	10	101.101.101.20	56560	3.74.137.87	443	TCP	DEFAULT ↑ / DEFAULT ↓	ProxySecureA...	other	N/A	

Related Information

- [Cisco Technical Support & Downloads](#)
- [Cisco Secure Access Help Center](#)
- [Cisco SASE Design Guide](#)
- [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](#)