

Configuración del acceso seguro con túneles automatizados SD-WAN para un acceso seguro a Internet

Contenido

[Introducción](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de Secure Access](#)

[Creación de API](#)

[Configuración de SD-WAN](#)

[Integración de API](#)

[Configurar grupo de políticas](#)

[Cree su FQDN o APP de bypass personalizado en SD-WAN \(OPCIONAL\)](#)

[Enrutamiento del tráfico](#)

[Verificación](#)

[Acceso seguro - Búsqueda de actividad](#)

[Acceso seguro - Eventos](#)

[Catalyst SD-WAN Manager: Network-Wide Path Insights](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar Secure Access con túneles automatizados SD-WAN para Secure Internet Access.



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

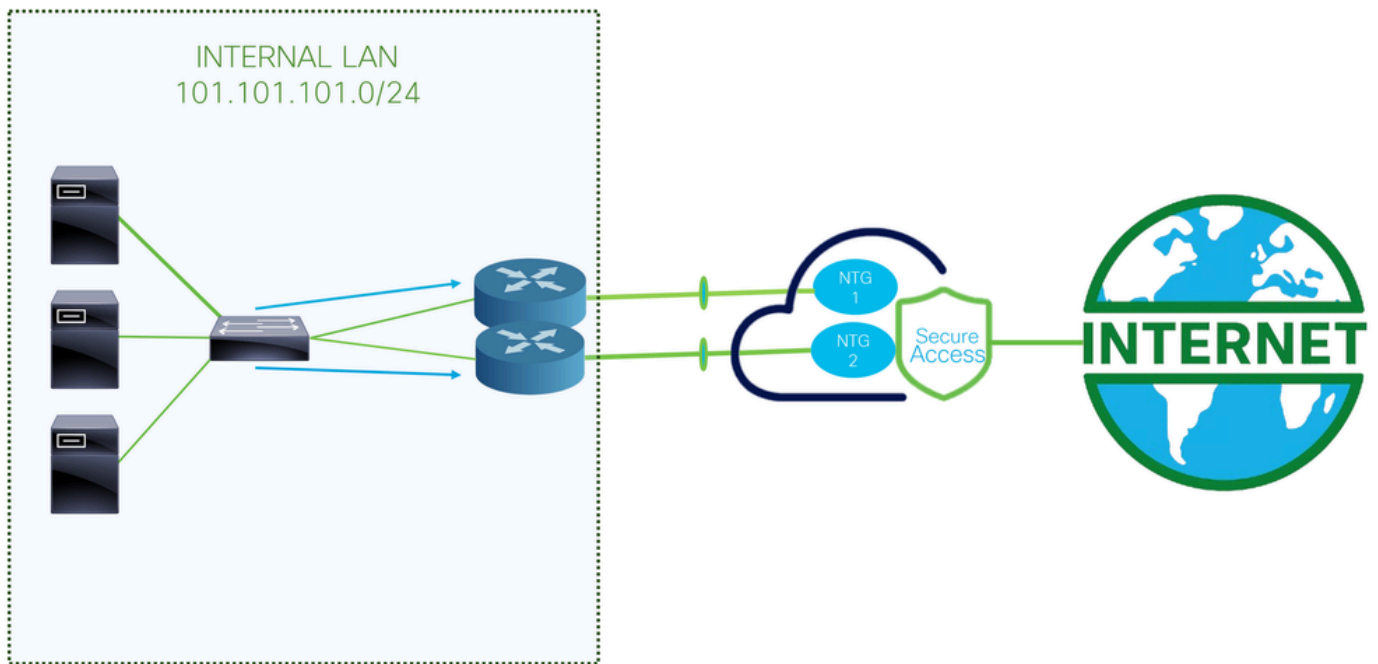
Antecedentes

A medida que las organizaciones adoptan cada vez más aplicaciones basadas en la nube y prestan apoyo a los empleados distribuidos, las arquitecturas de red deben evolucionar para proporcionar un acceso seguro, fiable y escalable a los recursos. Secure Access Service Edge (SASE) es un marco que converge la red y la seguridad en un único servicio proporcionado en la nube, que combina las capacidades de SD-WAN con funciones de seguridad avanzadas como Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), seguridad de capa DNS, Zero Trust Network Access (ZTNA) o VPN integrada para un acceso remoto seguro.

La integración de Cisco Secure Access con SD-WAN a través de túneles automatizados permite a las organizaciones enrutar el tráfico de Internet de forma segura y eficiente. La SD-WAN ofrece una selección inteligente de rutas y una conectividad optimizada entre ubicaciones distribuidas, mientras que Cisco Secure Access garantiza que todo el tráfico se inspecciona y protege de acuerdo con las políticas de seguridad corporativas antes de llegar a Internet.

Al automatizar la configuración de túneles entre los dispositivos SD-WAN y Secure Access, las organizaciones pueden simplificar la implementación, mejorar la escalabilidad y garantizar una aplicación de seguridad uniforme para los usuarios, independientemente de dónde se encuentren. Esta integración es un componente clave de una arquitectura SASE moderna, que permite un acceso seguro a Internet para sucursales, sitios remotos y usuarios móviles.

Diagrama de la red



Esta es la arquitectura utilizada para este ejemplo de configuración. Como puede ver, hay dos routers de borde:

Si decide implementar las políticas en dos dispositivos diferentes, se configura un NTG para cada router y se habilita NAT en el lado de Secure Access. Esto permite que ambos routers envíen tráfico desde la misma fuente a través de los túneles. Normalmente, esto no está permitido; sin embargo, habilitar la opción NAT para estos túneles permite que dos routers de borde envíen tráfico originado en la misma dirección de origen.

Prerequisites

Requirements

- Conocimiento de Secure Access
- Cisco Catalyst SD-WAN Manager versión 20.15.1 y Cisco IOS XE Catalyst SD-WAN versión 17.15.1 o posterior
- Conocimiento intermedio de routing y switching
- Conocimiento de ECMP
- Conocimiento de VPN

Componentes Utilizados

- Arrendatario de acceso seguro
- Catalyst SD-WAN Manager versión 20.18.1 y Cisco IOS XE Catalyst SD-WAN versión 17.18.1
- Administrador Catalyst SD-WAN

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración de Secure Access

Creación de API

Para crear los túneles automatizados con Secure Access, marque los siguientes pasos:

Vaya a [Panel de acceso seguro](#).

- Haga clic en Admin > API Keys
- Haga clic en Add
- Seleccione las siguientes opciones:
 - Deployments / Network Tunnel Group: **Lectura/escritura**
 - Deployments / Tunnels: **Lectura/escritura**
 - Deployments / Regions: **Sólo-Lectura**
 - Deployments / Identities: **Lectura-escritura**
 - Expiry Date: **Nunca caduca**

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

ADD

[CANCEL](#)[CREATE KEY](#)

Nota: Opcionalmente, agregue hasta 10 redes desde las cuales esta clave puede realizar autenticaciones. Agregue redes mediante una lista de direcciones IP públicas o CIDR separadas por comas.

- Haga clic **CREATE KEY** para finalizar la creación de API Key y Key Secret.

API Key 397766cdb29f43b08ddee3b1d8c04e45 	Key Secret bfce729cd3e243e281df7271acb12208 
--	---



Precaución: Copie antes de hacer clic en **ACCEPT AND CLOSE**; de lo contrario, tendrá que crearlos de nuevo y eliminar los que no se copiaron.

A continuación, para finalizar, haga clic en **ACCEPT AND CLOSE**.

Configuración de SD-WAN

Integración de API

Vaya a Catalyst SD-WAN Manager:

- Haga clic en **Administration** > **Settings** > **Cloud Credentials**
- A continuación, haga clic en **Cloud Provider Credentials** , **active** Cisco SSEy rellene los parámetros de organización y API

Settings

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

Explore

Search

Cisco Account

Cisco services registration

License Reporting

PnP Connect Sync

Data Collection & Statistics

Cloud Services

Data Stream

Network Statistics Configuration & Collection

Statistics Database Configuration

External Services

Alarm Notifications

Threat Grid API

UTD Snort Subscriber Signature

Cisco DNA Portal

Managed Cellular Activation - eSIM

Identity Provider Settings

Cloud Credentials

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

Save **Cancel**

- Organization ID: Puede tomarlo de la URL del panel de SSE
<https://dashboard.sse.cisco.com/org/xxxxx>
- Api Key: Cópielo del paso [Configuración de Secure Access](#)
- Secret: cópielo del paso [Configuración de Secure Access](#)

Luego, haga clic en el **Save** botón.



Nota: Antes de continuar con los siguientes pasos, debe asegurarse de que el administrador de SD-WAN y los extremos de Catalyst SD-WAN tengan resolución DNS y acceso a Internet.

Para comprobar si la búsqueda de DNS está activada, vaya a:

- Haga clic en **Configuration > Configuration Groups**.
- Haga clic en el perfil de sus dispositivos periféricos y edite el perfil del sistema

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

SIA_Basic



Service Profile (optional)

SIA_LAN



[+ Add Profile](#)

- A continuación, edite la opción Global y asegúrese de que la opción Domain Resolution esté habilitada

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 \(Configure O\)](#)

Configurar grupo de políticas

Vaya a Configuration > Policy Groups:

- Haga clic en 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](#)



Nota: En versiones anteriores a la 20.18, esta opción se denomina Agregar extremo de servicio seguro (SSE)

- Configure un nombre, una solución y haga clic en Create

Secure Internet Access

Name

SIA

Solution

sdwan

Description (optional)

Cancel

Create

Las siguientes configuraciones le permiten crear los túneles después de implementar la configuración en sus Catalyst SD-WAN Edges:

SSE Provider



Cisco SSE



Zscaler

Context Sharing



VPN



SGT

Tracker

Source IP address



{{ Monitoring }}



- SSE Provider: **SSE**
- Context Sharing: Elija VPN o SGT según sus necesidades
- Tracker
 - **Source IP Address:** Elegir dispositivo específico (esto le permite modificarlo por dispositivo e identificar el caso práctico en la fase de implementación)

En el Configuration paso que configure los túneles:

Configuration

+ Add Tunnel

Single Hub HA Scenario

ECMP Scenario with HA

Max one tunnel per hub

Max 8 Tunnels per Hub 8GB X 1

Single Hub HA Scenario Configuration:

- Tunnel Type: IPsec
- Interface Name(1..255): ipsec1
- Tunnel Source Interface*: GigabitEthernet1
- Tunnel Route Via: <SYSTEM DEFAULT>
- Tracker: DefaultTracker
- Primary: ☒ Secondary: ☐

ECMP Scenario with HA Configuration:

- Tunnel Type: IPsec
- Interface Name(1..255): ipsec1
- Tunnel Source Interface*: Loopback1
- Tunnel Route Via: GigabitEthernet1
- Tracker: DefaultTracker
- Primary: ☒ Secondary: ☐

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:** En esta situación, puede configurar la alta disponibilidad utilizando un NTG como activo y otro como pasivo, con un rendimiento máximo de 1 Gbps por NTG
- **ECMP Scenario with HA:** En este escenario, puede configurar hasta 8 túneles por hub, admitiendo un total de hasta 16 túneles por NTG. Esta configuración permite un mayor rendimiento en los túneles



Nota: Si las interfaces de red tienen un rendimiento superior a 1 Gbps y necesita escalabilidad, debe utilizar interfaces de bucle invertido. De lo contrario, puede utilizar interfaces estándar en el dispositivo. Esto es para habilitar ECMP desde el lado de Secure Access.



Advertencia: Si desea configurar las interfaces de loopback para un escenario ECMP, primero debe configurar las interfaces de loopback en [Configuration Groups > Transport & Management Profile](#), bajo la política que utilice en su router.

- Haga clic en [Add Tunnel](#)

Edit Tunnel

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

- Interface Name: ipsec1, ipsec2, ipsec3, etc.
- Tunnel Source Interface: Elija Interfaces de Loopback o una específica desde la que se establece el túnel
- Tunnel Route Via: Si elige Loopback, debe seleccionar la interfaz física desde la que desea rutear el tráfico. Si no selecciona Loopback, esta opción aparece atenuada y utiliza la primera interfaz habilitada para NAT que el sistema encuentra. Si hay más de una, debe seleccionar la interfaz WAN que desee
- Data Center: Esto significa a qué concentrador de Secure Access se establece la conexión

La siguiente parte de la configuración del túnel se configuran con las prácticas recomendadas proporcionadas por Cisco.

Advanced Options

General

Shutdown

☒ ☐

Track this interface

☒ ☐

TCP MSS

IP MTU

DPD Interval

DPD Retries

IKE Diffie-Hellman Group

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

Después de esto, debe configurar el túnel secundario que apunta al centro de datos secundario.

ESCENARIO DE HA DE UN SOLO HUB









































Configuration

+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
 ipsec1		 false	 1350	 1390	 
 ipsec2		 false	 1350	 1390	 

Este es el resultado final cuando se utiliza la implementación de escenario normal.

ECMP SCENARIO WITH HA

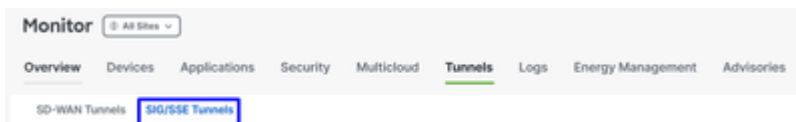
Interface Name	Description	Shutdown	TCP MSS	IP MTU
 ipsec1		 false	 1350	 1390
 ipsec2		 false	 1350	 1390
 ipsec3	PRIMARY HUB	 false	 1350	 1390
 ipsec4		 false	 1350	 1390
 ipsec5		 false	 1350	 1390
 ipsec11		 false	 1350	 1390
 ipsec12		 false	 1350	 1390
 ipsec13	SECONDARY HUB	 false	 1350	 1390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

A continuación, debe configurar la alta disponibilidad en la directiva de Internet segura.

High Availability

+ Add Interface Pair

Haga clic en Agregar par de interfaces:



PRIMARY
SECONDARY

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

En este paso, debe configurar el túnel principal y el secundario para cada par de túneles que esté configurando. Esto significa que cada túnel tiene su propia copia de seguridad. Recuerde, estos túneles fueron creados como Primario y Secundario para este propósito exacto.

"Active interface" se refiere al túnel principal, mientras que "Backup interface" se refiere al túnel secundario:

- Active Interface: **Principal**
- Backup Interface: **Secundario**



Advertencia: Si se omite este paso, los túneles no se activan y no se establece ninguna conexión desde los routers a Secure Access.

Después de configurar High Availability para los túneles, la configuración se muestra como se muestra en la siguiente imagen. En el ejemplo de laboratorio utilizado para esta guía, se muestran cinco túneles en HA. El número de túneles se puede ajustar según sea necesario.

High Availability

+ Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	1	ipsec11	1	 
ipsec2	1	ipsec12	1	 
ipsec3	1	ipsec13	1	 
ipsec4	1	ipsec14	1	 
ipsec5	1	ipsec15	1	 

Cancel

Save



Nota: Un máximo de 8 pares de túneles (16 túneles: 8 principales y 8 secundarias) se pueden configurar en SD-WAN Catalyst vManage. Cisco Secure Access admite hasta 10 pares de túneles.

- Haga clic en **Save**

Después de este punto, si todo está correctamente configurado, los túneles aparecen como UP en el Administrador de SD-WAN y Secure Access.

Para verificar en SD-WAN, verifique los siguientes pasos:

- Haga clic en **Monitor > Tunnels**
- Haga clic en **SIG/SSE Tunnels**

Monitor All Sites ▼

Overview **Devices** **Applications** **Security** **Multicloud** **Tunnels** **Logs** **Energy Management** **Advisories**

SD-WAN Tunnels **SIG/SSE Tunnels**

Además, podrá ver los túneles establecidos para Cisco Secure Access UP o no.

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

Para verificar en Secure Access, marque los siguientes pasos:

- Haga clic en 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](#)

C8K-PAYG-560-5b28-4db0-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 SD-WAN	Connected	Europe (Germany)	SSE-euc-1-1-1	8	SSE-euc-1-1-0	8	...

En una vista detallada, haga clic en el nombre del túnel:

PRIMARY

8 Active Tunnels

Tunnel Group ID: C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d

Data Center: SSE-euc-1-1-1

IP Address: 3.120.45.23

SECONDARY

8 Active Tunnels

Tunnel Group ID: C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d

Data Center: SSE-euc-1-1-0

IP Address: 18.156.145.74

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	137085	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 2	137086	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 3	137096	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 4	137087	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 5	137095	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 6	137077	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 7	137084	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 8	137078	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

Después de esto, puede pasar al paso, Create your Custom Bypass FQDN or APP in SD-WAN

Cree su FQDN o APP de bypass personalizado en SD-WAN (OPCIONAL)

Hay casos prácticos especiales en los que debe crear Application Bypass y FQDN o IP que puede aplicar a sus políticas de routing:

Vaya al portal de SD-WAN Manager:

- Haga clic en Configuration > Application Catalog > Applications

Application Catalog

SD-AVC Enabled

Configure Cloud Connection

Overview

Applications 1553

Application Source Settings

Cloud Sourced Applications

Discovered Application 0

Application Lists

Conflicts

Applications 1553

Select Application Attributes

Choose Filter

Custom Application

Export

Q Search Table

0 selected

Create Application List

Define Probe Endpoint

As 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
<input type="checkbox"/>	Zannet	file-server	other	inBuiltApps	-	-	bulk-data	Silver	...



Consejo: Si se ejecuta una versión inferior a 20.15, se pueden crear aplicaciones personalizadas en Listas de directivas



Nota: Para tener acceso al catálogo de aplicaciones, debe habilitar SD-AVC.

- Haga clic en Custom Application

Applications 1553

Select Application Attributes

Choose Filter

Custom Application

Export

Q Search Table

0 selected

Create Application List

Define Probe Endpoint

As of: Dec 23, 2025 05:00:05 PM

En esta etapa, se configura una exclusión básica mediante el FQDN de SWG de Secure Client - Umbrella Module:

ProxySecureAccess

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

Configure IP addresses to exclude

Space separated ports or range or

Enter L4 Protocol

SaaS probe endpoint type

☐ IP Address ☐ FQDN ☐ URL

SaaS probe endpoint value

Cancel Save

Ahora puede continuar con las configuraciones de las políticas de ruteo.

Enrutamiento del tráfico

En este paso, debe enrutar el tráfico de Internet a través de los túneles para protegerlo mediante Cisco Secure Access. En este caso, se utiliza una política de routing flexible que nos permite omitir cierto tráfico, lo que ayuda a evitar el envío de tráfico no deseado a través de Secure Access o evitar posibles malas prácticas.

En primer lugar, deje que defina los dos métodos de routing que se pueden utilizar:

- **Configuration > Configuration Groups > Service Profile > Service Route:** Este método proporciona routing a Secure Access, pero carece de flexibilidad.
- **Configuration > Policy Groups > Application Priority & SLA:** Este método ofrece varias opciones de routing dentro de la SD-WAN y, lo que es más importante, le permite omitir tráfico específico para que no se envíe a través de Secure Access.

Para obtener flexibilidad y alineación con las prácticas recomendadas, se utiliza esta configuración, Application Priority & SLA:

- Haga clic en **Configuration > Policy Groups > Application Priority & SLA**
- Haga clic en **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 un nombre de directiva y haga clic en [Create](#)

Application Priority & SLA Policy

Policy Name

SIA-ROUTE

Description (optional)

[Cancel](#)

Create

- [Habilitar](#) [Advanced Layout](#)
- Haga clic en [+ Add Traffic Policy](#)

[Policies](#) > [Application Priority & SLA](#)

SIA-ROUTE [✎](#)

[Additional Settings](#) [Advanced Layout](#) [ⓘ](#)

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

[+ Add Traffic Policy](#)

[SLA Class](#) [QoS Queue](#)

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

Add Traffic Policy List

Policy Name

VPN(s)

Direction

Default action

☒ Accept ☐ Drop

Cancel

Add

- Policy Name: Nombre que lo ajusta al propósito de esta lista de políticas de tráfico
- VPN(s): Elija el servicio VPN del usuario desde el que enruta el tráfico
- Direction: Desde el servicio
- Default action: Aceptar

Después de esto, puede iniciar la creación de la política de tráfico:

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

VPN: Corporate_Users Direction: From Service Default Action: Accept

	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	UmbrellaDNS	App List · UmbrellaDNS	Base action · accept	⋮
4	SIA AUTO FULL TRAFFIC	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): Origen 101.101.101.0/24, Destino 172.16.200.0/24. Esta ruta evita que el tráfico dentro de la red se envíe a Cisco Secure Access. Normalmente, los clientes no lo hacen, ya que el routing interno lo gestiona normalmente el router de distribución en implementaciones SD-WAN. Esta configuración garantiza que el tráfico interno entre estas

subredes no se enrute a Secure Access, dependiendo de si su situación lo requiere (opcional, depende de su entorno de red)

2. **BypassSSEProxy (Optional):** Esta política impide que los ordenadores internos con el módulo Cisco Umbrella en Secure Client y SWG habilitados envíen tráfico proxy de vuelta a la nube. El routing del tráfico proxy a la nube de nuevo no se considera una práctica recomendada.
3. **UmbrellaDNS (Best Practice):** Esta directiva impide que las consultas DNS destinadas a Internet se envíen a través del túnel. No se recomienda enviar consultas de DNS a resolvers de Umbrella (208.67.222.222, 208.67.220.220) a través del túnel.
4. **SIA AUTO FULL TRAFFIC:** Esta política dirige todo el tráfico desde el origen 101.101.101.0/24 a Internet a través de los túneles SSE que creó anteriormente, asegurándose de que este tráfico esté protegido en la nube.

Verificación

para verificar si el tráfico ya se está inundando a través de Cisco Secure Access, navegue hasta **Events** **Activity Search** **Network-Wide Path Insights** y filtre por su identidad de túnel:

Acceso seguro - Búsqueda de actividad

Vaya a **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, a table of activity results is shown. The table has columns for Request, Source, Rule Identity, Destination, Destination IP, Destination Port, and Destination Country. The results show activity from Dec 27, 2025 6:14 AM to Dec 28, 2025 6:14 AM. The table lists several events, including those from VPN-10 (VPN-10) to various destinations like youtube.com and img3.joymax.com. On the right side, an 'Event Details' panel is open, showing details for a specific event, including the Action (Allowed), Time (Dec 28, 2025 6:14 AM), Rule Name (For all Internet access (2100958)), Source (VPN-10 (VPN-10)), Source IP (101.101.101.20), Destination (https://youtube.com), and Security Group Tag (SGT).

Acceso seguro - Eventos

Vaya a **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: -



Nota: Asegúrese de que tiene la política predeterminada con el registro activado; de forma predeterminada, esta opción está desactivada.

Catalyst SD-WAN Manager: Network-Wide Path Insights

Vaya a Catalyst SD-WAN Manager:

- Haga clic en **Tools > Network-Wide Path Insights**
- Haga clic en **New Trace**

Traces & Tasks

New Trace

New Auto-on Task

☐ Enable DNS Domain Discovery ⓘ

Trace Name

e.g trace_[site ID]

Trace Duration(minutes)

60

Filters

Select Site(branch site only)*

SITE_101 ▾

VPN*

1 VPN(s) × ▾

Source Address/Prefix

101.101.101.20

Destination Address/Prefix

☒ Application ⓘ
 ☐ Application Group ⓘ

- Site: Elija el sitio desde el que se origina el tráfico
- VPN: Elija el ID de VPN de su subred desde la que egresa el tráfico
- Source: Coloque la IP o déjela en blanco para filtrar todo el tráfico filtrado por el site y VPN elegido

A continuación, en Insights podrá ver el tráfico que fluye a través de los túneles y el tipo de tráfico que va a 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. ⓘ

Search

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

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	I																																										
<table> <tr> <th>Direction</th><th>HopIndex</th><th>Local Edge</th><th>Remote Edge</th><th>Local Color</th><th>Remote Color</th><th>Local Drop(%)</th><th>Wan Loss(%)</th><th>Remote Drop(%)</th><th>Jitter(ms) *</th><th>Latency(ms) *</th><th>ART CND(ms)/SND(ms) *</th><th colspan="2"></th></tr> <tr> <td>Upstream</td><td>0</td><td>R101-2(Tunnel16000003)</td><td>SIG</td><td>BIZ_INTERNET (SIG)</td><td>N/A</td><td>0.00</td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td><td>R101-2: N/A</td><td colspan="2"></td></tr> <tr> <td>Downstream</td><td>0</td><td>SIG</td><td>(Tunnel16000003)R101-2</td><td>N/A</td><td>BIZ_INTERNET (SIG)</td><td>N/A</td><td>N/A</td><td>0.00</td><td>N/A</td><td>N/A</td><td>N/A</td><td colspan="2"></td></tr> </table>														Direction	HopIndex	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		
Direction	HopIndex	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	I																																										
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	I																																										
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	I																																										

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)
- [Centro de ayuda de Cisco Secure Access](#)
- [Guía de diseño de Cisco SASE](#)
- [Guía de Configuración de Seguridad de Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN Release 17.x](#)
- [Solución Cisco SASE: Guía rápida de Cisco Catalyst SD-WAN integrado con Cisco Secure Access](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).