

Configuration d'un accès sécurisé avec des tunnels automatisés SD-WAN pour un accès Internet sécurisé

Table des matières

[Introduction](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Configuration d'accès sécurisé](#)

[Création d'API](#)

[Configuration SD-WAN](#)

[Intégration API](#)

[Configurer le groupe de stratégies](#)

[Créez votre FQDN ou APP de contournement personnalisé dans SD-WAN \(FACULTATIF\)](#)

[Acheminement de votre trafic](#)

[Vérifier](#)

[Accès sécurisé - Recherche d'activité](#)

[Accès sécurisé - Événements](#)

[Catalyst SD-WAN Manager - Aperçu du chemin à l'échelle du réseau](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un accès sécurisé avec des tunnels automatisés SD-WAN pour un accès Internet sécurisé.



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

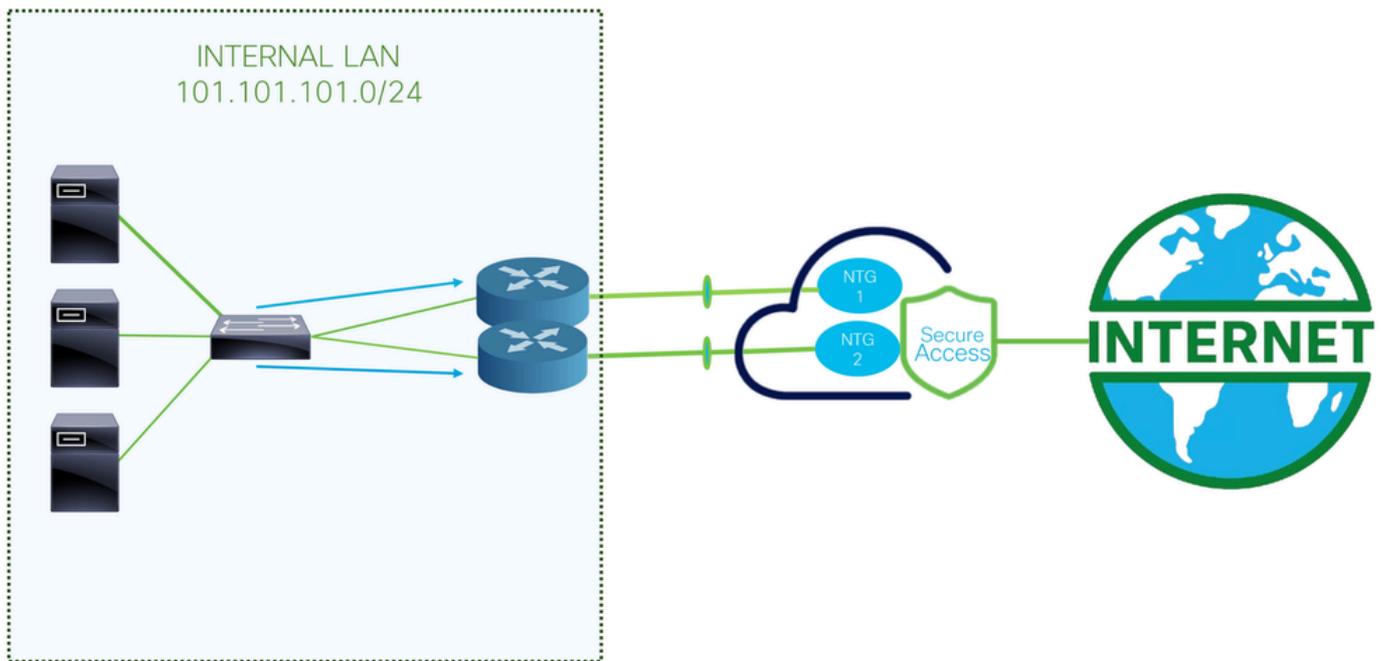
Informations générales

À mesure que les entreprises adoptent de plus en plus les applications cloud et prennent en charge des équipes distribuées, les architectures réseau doivent évoluer pour fournir un accès aux ressources sécurisé, fiable et évolutif. Secure Access Service Edge (SASE) est une structure qui converge la mise en réseau et la sécurité en un service unique fourni dans le cloud, combinant des fonctionnalités SD-WAN avec des fonctions de sécurité avancées telles que Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), la sécurité de la couche DNS, Zero Trust Network Access (ZTNA) ou un VPN intégré pour un accès à distance sécurisé.

L'intégration de Cisco Secure Access avec SD-WAN via des tunnels automatisés permet aux entreprises d'acheminer le trafic Internet de manière sécurisée et efficace. Le SD-WAN offre une sélection intelligente des chemins et une connectivité optimisée sur les sites distribués, tandis que Cisco Secure Access garantit que tout le trafic est inspecté et protégé conformément aux politiques de sécurité de l'entreprise avant d'atteindre Internet.

En automatisant la configuration des tunnels entre les périphériques SD-WAN et l'accès sécurisé, les entreprises peuvent simplifier le déploiement, améliorer l'évolutivité et garantir une application cohérente de la sécurité pour les utilisateurs, où qu'ils se trouvent. Cette intégration est un composant clé d'une architecture SASE moderne, permettant un accès Internet sécurisé pour les filiales, les sites distants et les utilisateurs mobiles.

Diagramme du réseau



Voici l'architecture utilisée pour cet exemple de configuration. Comme vous pouvez le voir, il existe deux routeurs de périphérie :

Si vous choisissez de déployer les stratégies sur deux périphériques différents, un NTG est configuré pour chaque routeur et la fonction NAT est activée du côté de l'accès sécurisé. Cela permet aux deux routeurs d'envoyer du trafic provenant de la même source via les tunnels. Normalement, cela n'est pas autorisé ; Cependant, l'activation de l'option NAT pour ces tunnels permet à deux routeurs de périphérie d'envoyer le trafic provenant de la même adresse source.

Conditions préalables

Exigences

- Connaissances sur l'accès sécurisé
- Cisco Catalyst SD-WAN Manager version 20.15.1 et Cisco IOS XE Catalyst SD-WAN version 17.15.1 ou ultérieure
- Connaissance intermédiaire du routage et de la commutation
- Connaissances ECMP
- Connaissances VPN

Composants utilisés

- Locataire d'accès sécurisé
- Catalyst SD-WAN Manager version 20.18.1 et Cisco IOS XE Catalyst SD-WAN version 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Configuration d'accès sécurisé

Création d'API

Afin de créer les tunnels automatisés avec un accès sécurisé, vérifiez les étapes suivantes :

Accédez à [Secure Access Dashboard](#).

- Cliquez sur Admin > API Keys
- Cliquez sur Add
- Choisissez les options suivantes :
 - Deployments / Network Tunnel Group: **Lecture/écriture**
 - Deployments / Tunnels: **Lecture/écriture**
 - Deployments / Regions: **Lecture seule**
 - Deployments / Identities: **Lecture-Écriture**
 - Expiry Date: **Ne jamais expirer**

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 >

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

4 selected Remove All

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



Remarque : Ajoutez éventuellement jusqu'à 10 réseaux à partir desquels cette clé peut

effectuer des authentifications. Ajoutez des réseaux à l'aide d'une liste d'adresses IP publiques ou de CIDR séparés par des virgules.

- Cliquez sur **CREATE KEY** pour finaliser la création du **API Key** et du **Key Secret**.

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



Mise en garde : Copiez-les avant de cliquer sur **ACCEPT AND CLOSE**; sinon, vous devez les créer à nouveau et supprimer ceux qui n'ont pas été copiés.

Pour finaliser, cliquez sur **ACCEPT AND CLOSE**.

Configuration SD-WAN

Intégration API

Accédez à Catalyst SD-WAN Manager :

- Cliquez sur **Administration** > **Settings** > **Cloud Credentials**
- Ensuite, cliquez sur **Cloud Provider Credentials** et activez **Cisco SSE** et remplissez les paramètres d'API et d'organisation

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

Save Cancel

- Organization ID: Vous pouvez l'obtenir à partir de l'URL de votre tableau de bord SSE <https://dashboard.sse.cisco.com/org/xxxxx>
- Api Key: Copiez-le à partir de l'étape [Configuration d'accès sécurisé](#)
- Secret: Copiez-le à partir de l'étape [Configuration d'accès sécurisé](#)

Ensuite, cliquez sur le bouton qui `Save` apparaît.



Remarque : Avant de passer aux étapes suivantes, vous devez vous assurer que le gestionnaire SD-WAN et les périphériques SD-WAN Catalyst disposent d'une résolution DNS et d'un accès à Internet.

Pour vérifier si la recherche DNS est activée, accédez à :

- Cliquez sur Configuration > Configuration Groups
- Cliquez sur le profil de vos périphériques de périphérie et modifiez le profil système

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](#)

- Modifiez ensuite l'option Global et assurez-vous que l'option Domain Resolution est activée

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: | HTTPS Server:

FTP Passive: | Domain Lookup:

ARP Proxy: | RSH/RCP:

Cisco Discovery Protocol (CDP) | Line Virtual Teletype (Configure O)

Configurer le groupe de stratégies

Accédez à Configuration > Policy Groups :

- Cliquez sur 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



Remarque : Dans les versions inférieures à 20.18, cette option est appelée Add Secure Service Edge (SSE)

- Configurez un nom, une solution et cliquez sur [Create](#)

Secure Internet Access

Name

Solution

Description (optional)

Cancel

Create

Les configurations suivantes vous permettent de créer les tunnels après avoir déployé la configuration dans vos Catalyst SD-WAN Edge :

SSE Provider

Cisco SSE Zscaler

Context Sharing

VPN SGT

Tracker

Source IP address

- SSE Provider: **SE**
- Context Sharing: Choisissez VPN ou/et SGT en fonction de vos besoins
- Tracker
 - **Source IP Address:** Sélectionnez Device Specific (Spécifique au périphérique) (Cela vous permet de le modifier par périphérique et d'identifier l'exemple d'utilisation de ce périphérique lors de la phase de déploiement)

Dans l'étape *Configuration* vous configurez les tunnels :

Configuration

[+ Add Tunnel](#)

Single Hub HA Scenario

ECMP Scenario with HA

The image shows two side-by-side configuration screenshots for IPsec tunnels. The left screenshot, titled 'Single Hub HA Scenario', shows the 'Tunnel Source Interface' set to 'GigabitEthernet1' and 'Tunnel Route Via' set to '<SYSTEM DEFAULT>'. A blue box highlights the 'Tunnel Source Interface' field with the text 'Max one tunnel per hub' above it. The right screenshot, titled 'ECMP Scenario with HA', shows the 'Tunnel Source Interface' set to 'Loopback1' and 'Tunnel Route Via' set to 'GigabitEthernet1'. An orange box highlights the 'Tunnel Source Interface' field with the text 'Max 8 Tunnels per Hub 8GB X 1' above it. Both screenshots show 'Tracker' set to 'DefaultTracker' and 'Data Center' with 'Primary' selected.

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:** Dans ce scénario, vous pouvez configurer la haute disponibilité en utilisant un NTG comme actif et un autre comme passif, avec un débit maximal de 1 Gbit/s par NTG
- **ECMP Scenario with HA:** Dans ce scénario, vous pouvez configurer jusqu'à 8 tunnels par concentrateur, prenant en charge un total de 16 tunnels par NTG. Cette configuration permet un débit plus élevé à travers les tunnels



Remarque : Si vos interfaces réseau ont un débit supérieur à 1 Gbit/s et que vous avez besoin d'une évolutivité, vous devez utiliser des interfaces de bouclage. Sinon, vous pouvez utiliser des interfaces standard sur votre périphérique. Ceci permet d'activer ECMP du côté de l'accès sécurisé.



Avertissement : Si vous voulez configurer des interfaces de bouclage pour un scénario ECMP, vous devez d'abord configurer les interfaces de bouclage dans [Configuration Groups](#) > [Transport & Management Profile](#), selon la politique que vous utilisez dans votre routeur.

- Cliquez sur [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: Choisissez les interfaces de bouclage ou une interface spécifique à partir de laquelle vous établissez le tunnel
- Tunnel Route Via: Si vous choisissez Bouclage, vous devez sélectionner l'interface physique à partir de laquelle vous souhaitez acheminer le trafic. Si vous ne sélectionnez pas Bouclage, cette option est grisée et utilise la première interface NAT activée trouvée par le système. S'il y en a plusieurs, vous devez sélectionner l'interface WAN de votre choix
- Data Center: Cela signifie à quel concentrateur dans Secure Access vous établissez la connexion

La partie suivante de la configuration des tunnels vous permet de configurer les tunnels avec les meilleures pratiques fournies par 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

Ensuite, vous devez configurer le tunnel secondaire pointant vers le centre de données secondaire.

SCÉNARIO DE DISPONIBILITÉ HAUTE DISPONIBILITÉ À CONCENTRATEUR UNIQUE

Configuration

[+ Add Tunnel](#)

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

Il s'agit du résultat final lorsque vous utilisez le déploiement de scénario normal.

ECMP SCENARIO WITH HA

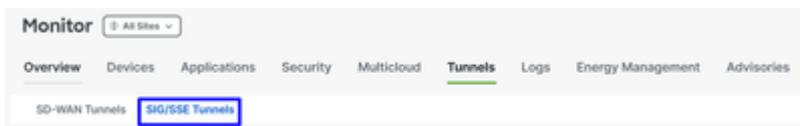
Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1		☑ false	1350	1390
ipsec2		☑ false	1350	1390
ipsec3	PRIMARY HUB	☑ false	1350	1390
ipsec4		☑ false	1350	1390
ipsec5		☑ false	1350	1390
ipsec11		☑ false	1350	1390
ipsec12		☑ false	1350	1390
ipsec13	SECONDARY HUB	☑ false	1350	1390
ipsec14		☑ false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

Ensuite, vous devez configurer la haute disponibilité dans la stratégie Internet sécurisé.

High Availability

[+ Add Interface Pair](#)

Cliquez sur Add Interface Pair :



PRIMARY
SECONDARY

Edit Interface Pair



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

Dans cette étape, vous devez configurer les tunnels principal et secondaire pour chaque paire de tunnels que vous configurez. Cela signifie que chaque tunnel a sa propre sauvegarde. N'oubliez pas que ces tunnels ont été créés en tant que tunnels principal et secondaire à cette fin précise. "Active interface" fait référence au tunnel principal, tandis que "Backup interface" fait référence au tunnel secondaire :

- Active Interface: **Principal**
- Backup Interface: **Secondaire**



Avertissement : Si cette étape est ignorée, les tunnels ne s'activent pas et aucune connexion n'est établie entre les routeurs et Secure Access.

Une fois la haute disponibilité configurée pour les tunnels, la configuration s'affiche comme illustré dans l'image ci-dessous. Dans l'exemple de TP utilisé pour ce guide, cinq tunnels sont illustrés dans HA. Le nombre de tunnels peut être ajusté selon les besoins.

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



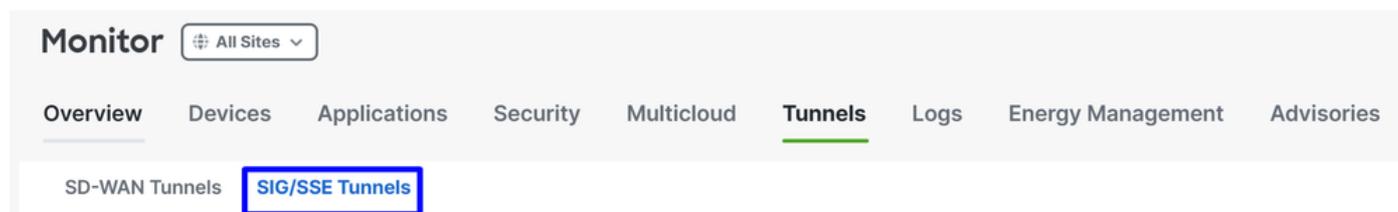
Remarque : Un maximum de 8 paires de tunnels (16 tunnels : 8 principaux et 8 secondaires) peuvent être configurés dans SD-WAN Catalyst vManage. Cisco Secure Access prend en charge jusqu'à 10 paires de tunnels.

- Cliquer *Save*

Après ce point, si tout est correctement configuré, les tunnels apparaissent comme étant UP dans le gestionnaire SD-WAN et l'accès sécurisé.

Pour vérifier dans SD-WAN, procédez comme suit :

- Cliquez sur *Monitor* > *Tunnels*
- Cliquez ensuite sur *SIG/SSE Tunnels*



Et vous pouvez voir les tunnels établis vers Cisco Secure Access UP ou non.

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_301								
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000002	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000003	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000004	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000005	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000006	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000007	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000008	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000011	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000012	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000013	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000014	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000015	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000016	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000017	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000018	R101-1	SITE_301	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

Pour vérifier dans Secure Access, procédez comme suit :

- Cliquez sur 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](#)

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

Dans une vue détaillée, cliquez sur le nom du tunnel :

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

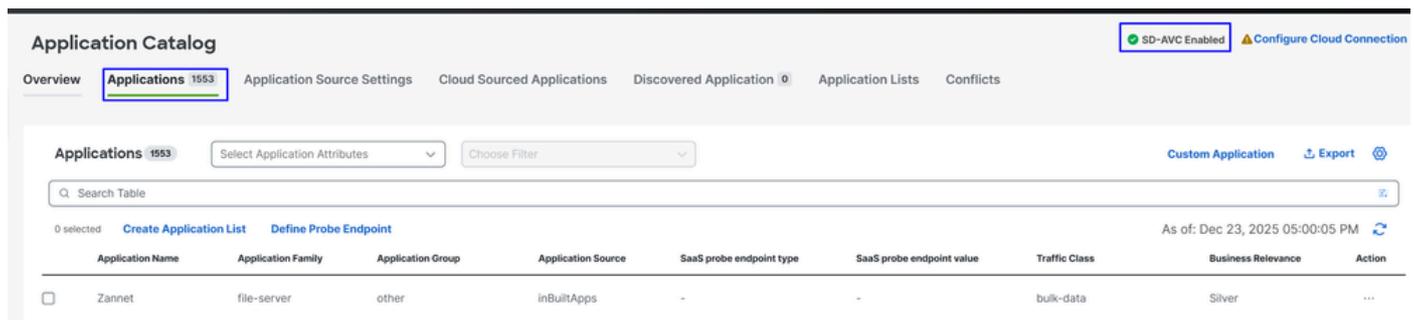
Après cela, vous pouvez passer à l'étape, Create your Custom Bypass FQDN or APP in SD-WAN

Créez votre FQDN ou APP de contournement personnalisé dans SD-WAN (FACULTATIF)

Il existe des cas d'utilisation spéciaux où vous devez créer un contournement d'application et un FQDN ou IP que vous pouvez appliquer à vos politiques de routage :

Accédez au portail SD-WAN Manager :

- Cliquez sur Configuration > Application Catalog > Applications



The screenshot shows the 'Application Catalog' page. At the top right, there are status indicators: 'SD-AVC Enabled' (green) and 'Configure Cloud Connection' (yellow). The main navigation bar includes 'Overview', 'Applications 1553' (highlighted), 'Application Source Settings', 'Cloud Sourced Applications', 'Discovered Application 0', 'Application Lists', and 'Conflicts'. Below the navigation, there are filters for 'Select Application Attributes' and 'Choose Filter'. A search bar is present. The table below has columns: Application Name, Application Family, Application Group, Application Source, SaaS probe endpoint type, SaaS probe endpoint value, Traffic Class, Business Relevance, and Action. One application is listed: 'Zannet' with family 'file-server' and group 'other'. The 'Custom Application' button is highlighted in blue.



Conseil : Si vous exécutez une version antérieure à 20.15, vous pouvez créer des applications personnalisées sous Listes de stratégies



Remarque : Pour avoir accès au catalogue d'applications, vous devez activer SD-AVC.

- Cliquez sur Custom Application



This screenshot is a close-up of the top right area of the Application Catalog page. The 'Custom Application' button is highlighted with a blue box. Other elements visible include the 'Export' button and the refresh icon.

À ce stade, une exclusion de base est configurée à l'aide du nom de domaine complet Secure Client - Umbrella Module SWG :

ProxySecureAccess

Custom Application ✕

Name of the Custom APP

Application Name ⓘ

Application Name: ProxySecureAccess-Custom

Server Names ⓘ

Application Family

Application Group

Traffic Class

Business Relevance

+ **L3/L4 Attributes**

IPv4 Address	Ports	L4 Protocol
<input type="text" value="10.X.X.X, 20.0.0.0/24 separated by"/>	<input type="text" value="Space separated ports or range or"/>	<input type="text" value="Enter L4 Protocol"/>

SaaS probe endpoint type

IP Address
 FQDN
 URL

SaaS probe endpoint value

FQDN

Cancel Save

- Server Name: Utilisez le FQDN que vous souhaitez contourner (dans cet exemple, les FQDN de SWG sont configurés)
 - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
 - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Cliquez sur Save



Remarque : Modifiez ORGID avec votre numéro d'organisation SSE.

Ensuite, une exclusion de base est créée ; dans ce cas, les serveurs DNS Umbrella :

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

Vous pouvez maintenant procéder aux configurations des stratégies de routage.

Acheminement de votre trafic

Dans cette étape, vous devez acheminer le trafic Internet à travers les tunnels pour le protéger via Cisco Secure Access. Dans ce cas, vous utilisez une politique de routage flexible qui nous permet de contourner certains trafics, ce qui contribue à empêcher l'envoi de trafic indésirable via Secure Access ou à éviter les mauvaises pratiques potentielles.

Commençons par définir les deux méthodes de routage qui peuvent être utilisées :

- **Configuration > Configuration Groups > Service Profile > Service Route:** Cette méthode assure le routage vers l'accès sécurisé, mais manque de flexibilité.
- **Configuration > Policy Groups > Application Priority & SLA:** Cette méthode offre diverses options de routage dans SD-WAN et, plus important encore, vous permet de contourner le trafic spécifique afin qu'il ne soit pas envoyé via Secure Access.

Pour plus de flexibilité et l'alignement sur les meilleures pratiques, cette configuration est utilisée, Application Priority & SLA:

- Cliquez sur **Configuration > Policy Groups > Application Priority & SLA**
- Cliquez ensuite sur **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

- Configurez un nom de stratégie et cliquez sur **Create**

Application Priority & SLA Policy

Policy Name

SIA-ROUTE

Description (optional)

Cancel

Create

- **Activer** Advanced Layout
- Cliquez sur **+ 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: Nom qui ajuste ceci à l'objectif de cette liste de stratégie de trafic
- VPN(s): Sélectionnez le VPN de service de l'utilisateur à partir duquel vous acheminez le trafic
- Direction: Du service
- Default action: Accept (accepter)

Après cela, vous pouvez commencer la création de la politique de trafic :

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 ULL TRAFFI C	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. Cette route empêche le trafic intra-réseau d'être envoyé à Cisco Secure Access. En général, les clients ne le font pas, car le routage interne est généralement géré par le routeur de distribution dans les déploiements SD-WAN. Cette configuration garantit que le trafic interne entre ces

sous-réseaux n'est pas acheminé vers l'accès sécurisé, selon que votre scénario l'exige ou non (facultatif, selon votre environnement réseau)

2. **BypassSSEProxy (Optional)**: Cette stratégie empêche les ordinateurs internes sur lesquels le module Cisco Umbrella est activé dans Secure Client et SWG de renvoyer le trafic proxy vers le cloud. Le routage du trafic proxy vers le cloud n'est pas considéré comme une bonne pratique.
3. **UmbrellaDNS (Best Practice)**: Cette stratégie empêche les requêtes DNS destinées à Internet d'être envoyées via le tunnel. L'envoi de requêtes DNS aux résolveurs Umbrella (208.67.222.222,208.67.220.220) via le tunnel n'est pas recommandé.
4. **SIA AUTO FULL TRAFFIC**: Cette stratégie achemine tout le trafic de la source 101.101.101.0/24 vers Internet par le biais des tunnels SSE que vous avez précédemment créés, en s'assurant que ce trafic est protégé dans le cloud.

Vérifier

afin de vérifier si le trafic inonde déjà via Cisco Secure Access, naviguez vers [Events](#) ou [Activity Search](#) ou [Network-Wide Path Insights](#) et filtrez par votre identité de tunnel :

Accès sécurisé - Recherche d'activité

Accédez à [Monitor](#) > [Activity Search](#):

Activity Search

1,617 Total Viewing activity from Dec 27, 2025 6:14 AM to Dec 28, 2025 6:14 AM Page: 1 Results per page: 50 1 - 50

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)		142.250.186.174:443		United States
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://youtube.com	142.250.186.174:443		United States
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)		110.234.18.177:443		United States
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)		110.234.18.177:443		United States
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177:443		United States

Event Details

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
Security Group Tag (SGT): -

Accès sécurisé - Événements

Accédez à [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	829e0bbdeaf6514e	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	829e0bbdeaf6514e	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-Of...

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: -



Remarque : Assurez-vous que votre stratégie par défaut avec la journalisation activée est désactivée par défaut.

Catalyst SD-WAN Manager - Aperçu du chemin à l'échelle du réseau

Accédez à Catalyst SD-WAN Manager :

- Cliquez sur **Tools** > **Network-Wide Path Insights**
- Cliquez sur **New Trace**

Traces & Tasks
New Trace
New Auto-on Task

Enable DNS Domain Discovery ⓘ

Trace Name

Trace Duration(minutes)

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: Choisissez le site à partir duquel votre trafic est en train de sortir
- VPN: Choisissez l'ID VPN de votre sous-réseau d'où part votre trafic
- Source: Placez l'adresse IP ou laissez-la vide pour filtrer tout le trafic filtré par le site et VPN le choix

Ensuite, dans Insights, vous pouvez voir le trafic qui inonde les tunnels et le type de trafic allant vers 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																																				
			<table border="1" style="width: 100%; border-collapse: collapse; font-size: 0.8em;"> <thead> <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> </tr> </thead> <tbody> <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> </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> </tr> </tbody> </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																																				
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																																				

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Centre d'aide Cisco Secure Access](#)
- [Guide de conception Cisco SASE](#)
- [Guide de configuration de la sécurité Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN version 17.x](#)
- [Solution Cisco SASE : Cisco Catalyst SD-WAN intégré à Cisco Secure Access en quelques mots](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.