

Configuration d'un accès sécurisé avec les tunnels automatisés SD-WAN de Catalyst pour un accès privé 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](#)

[Configurer le routage](#)

[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 l'accès sécurisé avec les tunnels automatisés SD-WAN de Catalyst pour l'accès privé sécurisé.



Secure Access and Catalyst SDWAN for Secure Private Access — with Automated Tunnels —

Informations générales

À mesure que les entreprises évoluent au-delà des réseaux périmétriques traditionnels, l'accès sécurisé aux ressources privées devient tout aussi important que la sécurisation du trafic Internet. Les applications ne sont plus confinées à un seul data center. Elles sont désormais présentes dans des environnements sur site, des clouds publics et des architectures hybrides. Cette évolution nécessite une approche plus souple et moderne de l'accès privé.

C'est là qu'une architecture basée sur SASE et Cisco Secure Access entrent en jeu. Au lieu de s'appuyer sur des concentrateurs VPN traditionnels et un accès réseau linéaire, Cisco Secure Access fournit une connectivité privée sous la forme d'un service cloud, combinant VPN-as-a-Service (VPNaaS) et Zero Trust Network Access (ZTNA).

Pour l'accès privé au niveau du réseau, Cisco Secure Access s'intègre à SD-WAN à l'aide de tunnels IPsec site à site automatisés. Ces tunnels permettent au trafic privé de circuler en toute sécurité entre Secure Access et les réseaux sur site ou cloud, tout en conservant l'inspection de la sécurité et l'application des politiques centralisées dans le cloud. D'un point de vue opérationnel, cela élimine le besoin de déployer et de maintenir des têtes de réseau VPN traditionnelles et simplifie l'évolutivité à mesure que les environnements se développent.

Dans un modèle VPNaaS, Secure Access agit comme point de terminaison VPN dans le cloud. SD-WAN gère le routage intelligent et la résilience avec un accès sécurisé et garantit que le trafic est protégé et régi par des politiques de sécurité cohérentes avant d'atteindre des ressources privées.

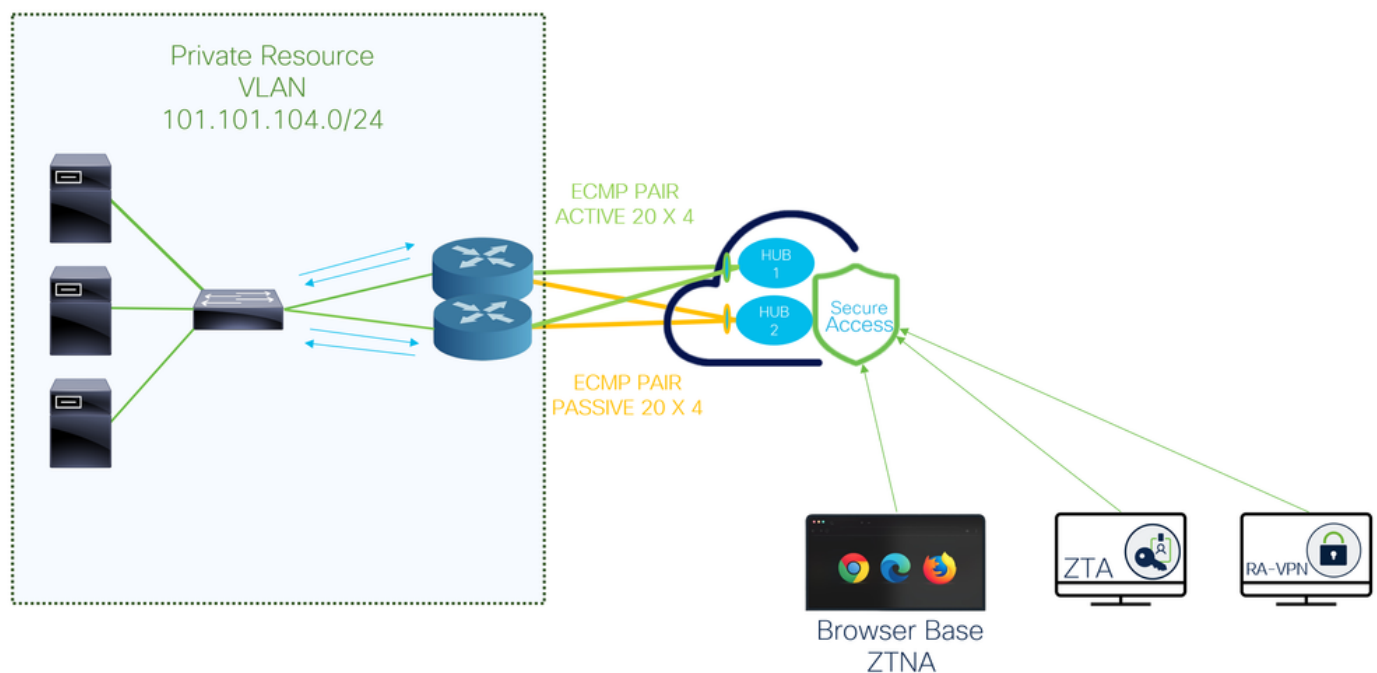
Cisco Secure Access prend également en charge les architectures de tunnel site à site avancées, y compris la liaison multirégionale. Cette fonctionnalité permet aux entreprises d'établir des tunnels vers plusieurs régions d'accès sécurisé simultanément, offrant ainsi une redondance géographique et une disponibilité supérieure. En se connectant à différentes régions, le trafic peut basculer automatiquement en cas de panne régionale, de dégradation de la latence ou d'événements de maintenance.

Par exemple, une entreprise peut établir des tunnels site à site depuis son environnement SD-WAN vers les régions d'accès sécurisé de Londres et d'Allemagne. Les deux tunnels restent actifs, permettant un accès privé résilient entre les régions et assurant la continuité même si une région devient indisponible. Cette conception multirégionale renforce la haute disponibilité, améliore la tolérance aux pannes et s'aligne sur les exigences de résilience de niveau entreprise.

Pour un accès plus granulaire, Cisco Secure Access applique le modèle ZTNA (Zero Trust Network Access). Au lieu d'accorder aux utilisateurs une connectivité réseau étendue, ZTNA autorise l'accès uniquement à des applications spécifiques, en fonction de l'identité, de la position du périphérique et du contexte. Cette approche réduit considérablement la surface d'attaque et s'aligne sur les principes Zero Trust.

L'accès ZTNA est activé via une combinaison de tunnels de site à site et de connecteurs de ressources. Les connecteurs de ressources sont des appareils virtuels légers qui établissent des connexions sortantes uniquement vers l'accès sécurisé, ce qui signifie que les ressources privées n'ont jamais besoin d'être directement exposées à Internet.

Diagramme du réseau



Conditions préalables

Exigences

- Connaissances sur l'accès sécurisé
- Cisco Catalyst SD-WAN Manager version 20.18.2 et Cisco IOS XE Catalyst SD-WAN version 17.18.2 ou ultérieure
- Connaissance intermédiaire du routage et de la commutation
- Connaissances ECMP
- Connaissances VPN

- Comme cette intégration est basée sur une disponibilité contrôlée, vous devez soumettre un dossier TAC pour demander l'activation de la fonctionnalité dans Cisco Secure Access

Composants utilisés

- Locataire d'accès sécurisé
- Catalyst SD-WAN Manager version 20.18.2 et Cisco IOS XE Catalyst SD-WAN version 17.18.2
- Catalyst SD-WAN Manager

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 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.

☐ Admin	17 >
☒ Deployments	23 >
☐ Investigate	2 >
☐ Policies	25 >
☐ Reports	17 >

4 selected

[Remove All](#)

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

Network Restrictions *(Optional)*

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

IP Addresses

For example: 100.10.10.0/24, 1.1.1.1

ADD

CANCEL

CREATE KEY



Remarque : Ajoutez éventuellement jusqu'à 10 réseaux à partir desquels cette clé peut effectuer des authentications. 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

397766cddb29f43b08ddee3b1d8c04e45



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

- **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** 5 **Transport & Management**

Q Search

Name	Type	Profiles
SPA-AUTO		

Type: Single Router

System Profile

SPA-AUTO

Policy Profile (optional)

Default_Policy_Object_Profile

CLI Add-on Profile (optional)

SPA_Auto_Route-maps

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

SPA-AUTO [Edit](#)

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

Q Search

Profile Features

AAA	Banner
BFD	Global
Multi-Region Fabric	NTP

Global

Name: Global

Description (optional): Global Description

Services NAT64 BGP Authentication SSH Version Ether C

HTTP Server ⓘ ⌵ ☐

FTP Passive ⓘ ⌵ ☐

ARP Proxy ⓘ ⌵ ☐

HTTPS Server ⓘ ⌵ ☐

Domain Lookup ⓘ ⌵ ☒

RSH/RCP ⓘ ⌵ ☐

Configurer le groupe de stratégies

Accédez à Configuration > Policy Groups :

- Cliquez sur Secure Internet Gateway / Secure Service Edge > Add Secure Private Access

Policy Groups

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

Secure Internet Gateway / Secure Service Edge 4

Q Search Table

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

Name	Description	Solution
------	-------------	----------

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

Secure Private Application Access

Name

SPA-AUTO

Description (optional)

[Cancel](#) [Create](#)

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

Configuration

Segment (VPN)

  Corporate_User

Cisco Secure Access Region

  Europe (Germany) 

- Configuration
 - Segment (VPN): Sélectionnez le VRF qui héberge la ou les applications auxquelles vous souhaitez accéder via Secure Access
 - Cisco Secure Access Region: Choisissez la région la plus proche du concentrateur SD-WAN ou de la filiale où les applications sont hébergées

Définissez ensuite la configuration du tunnel. Les tunnels créés vers le data center d'accès sécurisé principal sont actifs, tandis que ceux créés vers le data center d'accès sécurisé

secondaire fonctionnent comme des tunnels de sauvegarde.

Sous Tunnel Configuration cliquez sur + Add Tunnel:

Tunnel Configuration

[+ Add Tunnel](#)

Tunnel

BASIC SETTINGS

Interface Name(1..255) ipsec101	Description <system default>
Tunnel Source Interface Auto	Tunnel Route-Via Interface Auto
Data Center ☐ Primary ☐ Secondary	

Advanced Settings

GENERAL

Shutdown

TCP MSS

IP MTU

DPD Interval

- Tunnel

- Interface Name: Spécifiez le nom du tunnel, il est automatiquement mis à jour à chaque ajout d'un nouveau tunnel
- Tunnel Source Interface: Il n'est pas nécessaire de modifier ce paramètre. Lorsque vous laissez la valeur Auto, le système crée automatiquement une interface de bouclage avec un masque /31.
- Tunnel Route-Via Interface: Il n'est pas nécessaire de modifier ce paramètre. Par défaut, elle utilise la première interface WAN physique NATed sur le routeur de périphérie, mais elle peut être modifiée si une interface WAN spécifique est requise

- Data Center: Sélectionnez Primary (Principal) ou Secondary (Secondaire). Si le tunnel principal est déjà configuré, sélectionnez Secondary. Dans des scénarios normaux, un tunnel peut être configuré comme principal et un autre comme secondaire
- Advanced Settings
 - IP MTU: Utiliser 1390
 - TCP MSS: Utiliser 1350



Remarque : Si vous souhaitez créer plusieurs tunnels pour activer ECMP et augmenter la capacité du tunnel, vous pouvez configurer jusqu'à 10 tunnels actifs/10 tunnels de secours par routeur. Cela permet d'obtenir jusqu'à 10×4 Gbit/s par NTG.

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action	
ipsec101	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec102	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec103	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec104	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec105	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec106	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec107	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec108	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec109	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	MAXIMUM OF 10 TUNNELS PER HUB
ipsec110	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	10 x 1 Primary
ipsec111	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	10 x 1 Secondary
ipsec112	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec113	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec114	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec115	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec116	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec117	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec118	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	
ipsec119	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	
ipsec120	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	



Remarque : si vous déployez plusieurs tunnels par routeur, assurez-vous que l'interface de transport peut supporter la bande passante totale de tous les tunnels actifs combinés. Par exemple, si deux tunnels doivent transporter jusqu'à 1 Gbit/s chacun, la liaison de transport doit prendre en charge un débit d'au moins 2 Gbit/s.

Une fois les tunnels configurés, poursuivez avec la configuration BGP.

BGP Routing

BGP ASN ⓘ

 ▼

65000

In Route Policy

 ▼

SPA_Auto-In

Out Route Policy

 ▼

SPA_Auto-Out

- **BGP Routing**

- **BGP ASN:** Spécifiez le numéro de système autonome pour le concentrateur SD-WAN. L'AS 64512 est réservé à l'accès sécurisé et ne peut pas être utilisé. Pour plus d'informations sur BGP, consultez
- **In Route Policy:** Le système crée automatiquement cette stratégie de route entrante avec une instruction `deny all` pour empêcher les problèmes de routage. Il doit être modifié manuellement via un [CLI Add-On Template](#) pour autoriser/refuser les routes appropriées.
- **Out Route Policy:** Le système crée cette stratégie de routage sortant avec une `deny all` instruction pour éviter les problèmes de routage. Elle doit être modifiée manuellement via un [CLI Add-On Template](#) pour autoriser/refuser les routes appropriées.



Avertissement : À partir de novembre 2025, toutes les organisations d'accès sécurisé nouvellement créées utilisent l'ASN public 32644 par défaut pour l'appairage BGP dans les groupes de tunnels réseau. Les organisations existantes établies avant novembre 2025 continuent d'utiliser le ASN privé 64512 qui était précédemment réservé aux homologues BGP d'accès sécurisé. Si le numéro de système autonome privé 64512 est attribué à un périphérique sur votre réseau, il ne peut pas être homologué avec un groupe de tunnel réseau configuré pour l'homologue (accès sécurisé) BGP AS 64512.

La configuration suivante BGP et `route-map` est créée automatiquement pour chaque voisin BGP après que vous ayez `Deploy` défini la nouvelle stratégie dans votre `Policy Group`.

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

```
R104#sh run | s r b
router bgp 65000
bgp log-neighbor-changes
```

```

!
address-family ipv4 vrf 10
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
...
maximum-paths 32
exit-address-family

```

Ensuite, cliquez sur **Save** et poursuivez le déploiement de la stratégie pour activer les tunnels.

- Cliquez sur **Configuration > Policy Groups**
- Choisissez sous votre **Policy > Secure Service Edge > Secure Private Application Access** et cliquez sur le profil récent créé pour SPA.
- Cliquez **Deploy** pour finaliser

The screenshot shows the 'Policy Groups' configuration interface. The 'Secure Private Application Access' dropdown menu is open, displaying 'SPA-Auto' as the selected option. A blue arrow points from the 'Deploy' button in the 'Device Solution' panel to the 'SPA-Auto' option in the dropdown.

Pour vérifier dans Secure Access, procédez comme suit :

- Cliquez sur **Connect > Network Connections**

ÉTABLISSEMENT DE TUNNEL

The screenshot displays the 'eu-central-1' network tunnel group configuration. It includes a summary section with details like Region (Europe (Germany)), Device Type (Catalyst SD-WAN), and Routing Type (Dynamic Routing (BGP)). Below the summary, there are two sections for the Primary Hub and Secondary Hub, each showing details like Tunnel Group ID, Data Center, and IP Address. The Primary Hub section is highlighted with a green border, and the Secondary Hub section is highlighted with an orange border.

Configurer le routage

Accédez à Configurer > Configuration Groups

- Cliquez sur votre Configuration Group et créez/modifiez votre CLI Add-on Profile

The screenshot shows the 'Configuration Groups' page for the 'SD-WAN' group. The 'SPA-AUTO' configuration is selected, showing details for a 'Single Router' type. The configuration includes a 'System Profile' (SPA-AUTO), a 'Policy Profile' (Default_Policy_Object_Profile), and a 'CLI Add-on Profile' (SPA_Auto_Route-maps). The 'Transport & Management Profile' is set to 'SPA-SIA-Auto_WAN' and the 'Service Profile' is 'SPA-SIA-Auto_LAN'. The 'Deployment' section shows 'Associated' (1 device) and 'Provisioning' (1 out of sync) status, with 'Save' and 'Deploy' buttons.

Pour autoriser l'échange de routes BGP, utilisez les **In Route Policy** et **Out Route Policy** précédemment configurés. Vous pouvez trouver un exemple de base pour la configuration de la route CLI Add-On. Ce modèle fournit un point de départ et doit être personnalisé selon les besoins :

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

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

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

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



Avertissement : Une planification minutieuse est requise lors de la définition des réseaux autorisés en entrée et en sortie via les route-maps BGP. L'autorisation de toutes les routes, comme illustré dans l'exemple ci-dessus, peut introduire un comportement de

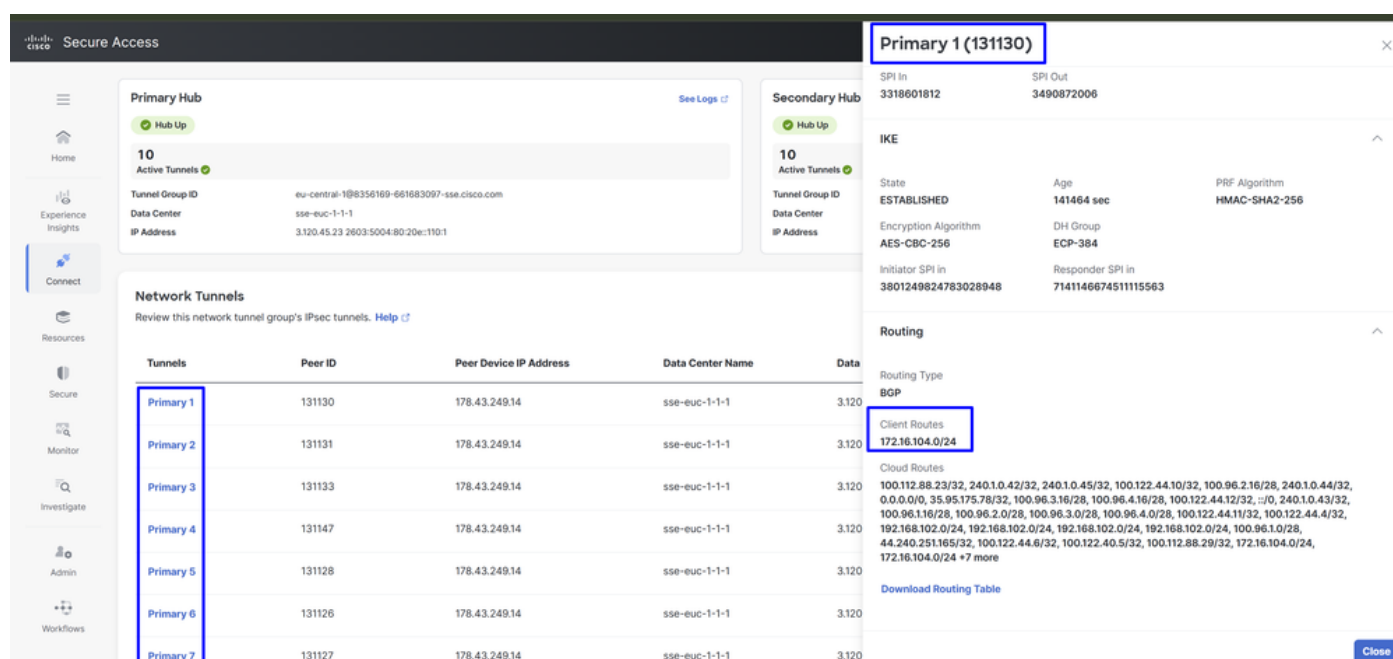
routing non souhaité. Pour un déploiement optimal, spécifiez explicitement uniquement les réseaux nécessaires dans vos feuilles de route afin de garantir des résultats de routing contrôlés et prévisibles

Vous pouvez maintenant passer à Deploy the changes

Pour vérifier si les routes BGP sont reçues dans Secure Access, vérifiez les étapes suivantes :

- Cliquez sur **Connect** > **Network Connections** > **Network Tunnel Groups** et sur select le nom NTG

ÉTABLISSEMENT D'ACHEMINEMENT



The screenshot displays the Cisco Secure Access management console. On the left, a sidebar contains navigation options: Home, Experience Insights, Connect, Resources, Secure, Monitor, Investigate, Admin, and Workflows. The main content area is divided into two sections: 'Primary Hub' and 'Secondary Hub', both showing '10 Active Tunnels'. Below these is a 'Network Tunnels' table with columns for Tunnel Name, Peer ID, Peer Device IP Address, Data Center Name, and Data. The table lists tunnels from Primary 1 to Primary 7. A modal window titled 'Primary 1 (131130)' is open on the right, showing details for the selected tunnel. It includes fields for SPI In (3318601812) and SPI Out (3490872006), and a section for 'Routing' with 'Client Routes' listed as 172.16.104.0/24. Other details include IKE State (ESTABLISHED), Age (141464 sec), PRF Algorithm (HMAC-SHA2-256), Encryption Algorithm (AES-CBC-256), DH Group (ECP-384), Initiator SPI In (3801249824783028948), and Responder SPI In (7141146674511115563).

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data
Primary 1	131130	178.43.249.14	sse-euc-1-1-1	3.120
Primary 2	131131	178.43.249.14	sse-euc-1-1-1	3.120
Primary 3	131133	178.43.249.14	sse-euc-1-1-1	3.120
Primary 4	131147	178.43.249.14	sse-euc-1-1-1	3.120
Primary 5	131128	178.43.249.14	sse-euc-1-1-1	3.120
Primary 6	131126	178.43.249.14	sse-euc-1-1-1	3.120
Primary 7	131127	178.43.249.14	sse-euc-1-1-1	3.120



Remarque : Dans cet exemple, le sous-réseau de l'utilisateur d'entreprise 172.16.104.0/24 est annoncé à Secure Access via BGP. Cela permet un routing correct entre le SD-WAN Catalyst et l'environnement SSE.

La même politique peut être appliquée aux deux extrémités WAN dans les concentrateurs Catalyst SD-WAN, ce qui donne 20 tunnels actifs et 20 tunnels de secours. Le nombre total de tunnels dépend du nombre de tunnels configurés sur chaque périphérie. Tout routeur connecté aux deux concentrateurs d'accès sécurisé (concentrateur 1 et concentrateur 2) forme une paire ECMP à travers tous les tunnels établis.

Par exemple, si Catalyst SD-WAN Edge 1 comporte 10 tunnels et Catalyst SD-WAN Edge 2 10 tunnels, Secure Access forme un ECMP sur les 20 tunnels actifs. Le même comportement s'applique au concentrateur SSE secondaire.

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](#)

eu-central-1

Region

Status

1 Tunnel Group

+ Add

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

Vérifier

afin de vérifier si le trafic passe par Cisco Secure Access, accédez à Eventsou 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

FILTERS

Q Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

IP ADDRESS172.16.104.11

IDENTITYAlejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)

Restore to

Search filters

Response

Allowed

Blocked

Warn Page Behavior

Warned

Accessed After Warn

4 Total

Viewing activity from Feb 17, 2026 11:27 AM to Feb 18, 2026 11:27 AM

Page: 1

Resu

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

Accès sécurisé - Événements

Accédez à Monitor>Events:

Events

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

[Schedule report](#)[Export CSV](#)

Events 1 total

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

Status Select status... Last 24 hours

[Saved searches](#)[Restore](#)

Event Type: ZTA Clientless OR DNS x Reset all

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

Source

AD Users: Alejandro Ruiz Sanchez...

Source IP:

Location:

Browser: Firefox 147.0

Operating system: Mac OS X 10.15

Connection

Type: ZTA

Endpoint Posture:

Status: Compliant

Posture profile: System provided (Brow...)

Security Controls

ZTA Clientless

Action: Allowed

Ingress region: —

Tunnel type: HTTP2

Resource connector group: —

Egress IP: —

Datacenter: —

Firewall (3)

Destination

FQDN: PC-site-104

Resource/Application Name: PC-site-104

Destination IP: 172.16.104.11

Destination Port: 3389

Application Category: Private Resource

Application Protocol: RDP-TCP

Rows per page 30 1-1 of 1 < 1 >



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 SPA Trace Duration(minutes) 60

Filters

Select Site(branch site only)* SITE_104 VPN* 1 VPN(s)

Source Address/Prefix Destination Address/Prefix 172.16.104.0/24

☒ Application ☐ Application Group

Please select one or more applications

Advanced Filters

Monitor Settings

Grouping Fields

Synthetic Traffic

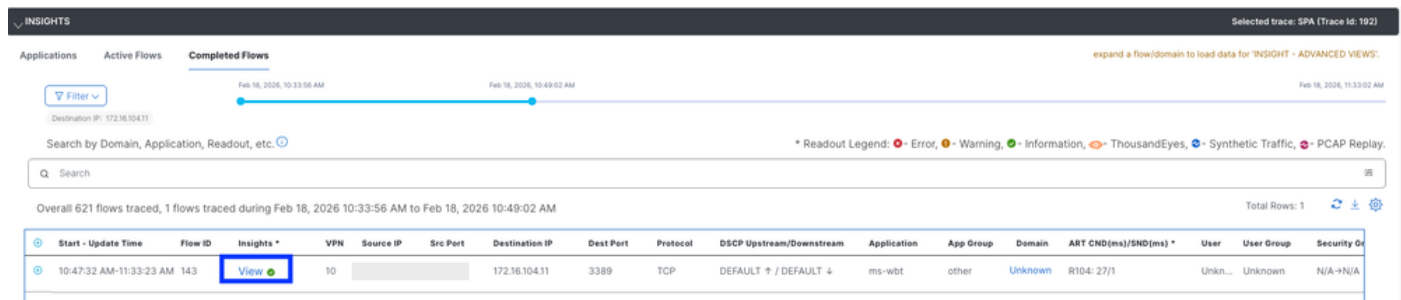
Cancel Start

- Trace Name: (Facultatif) Spécifiez le nom de trace

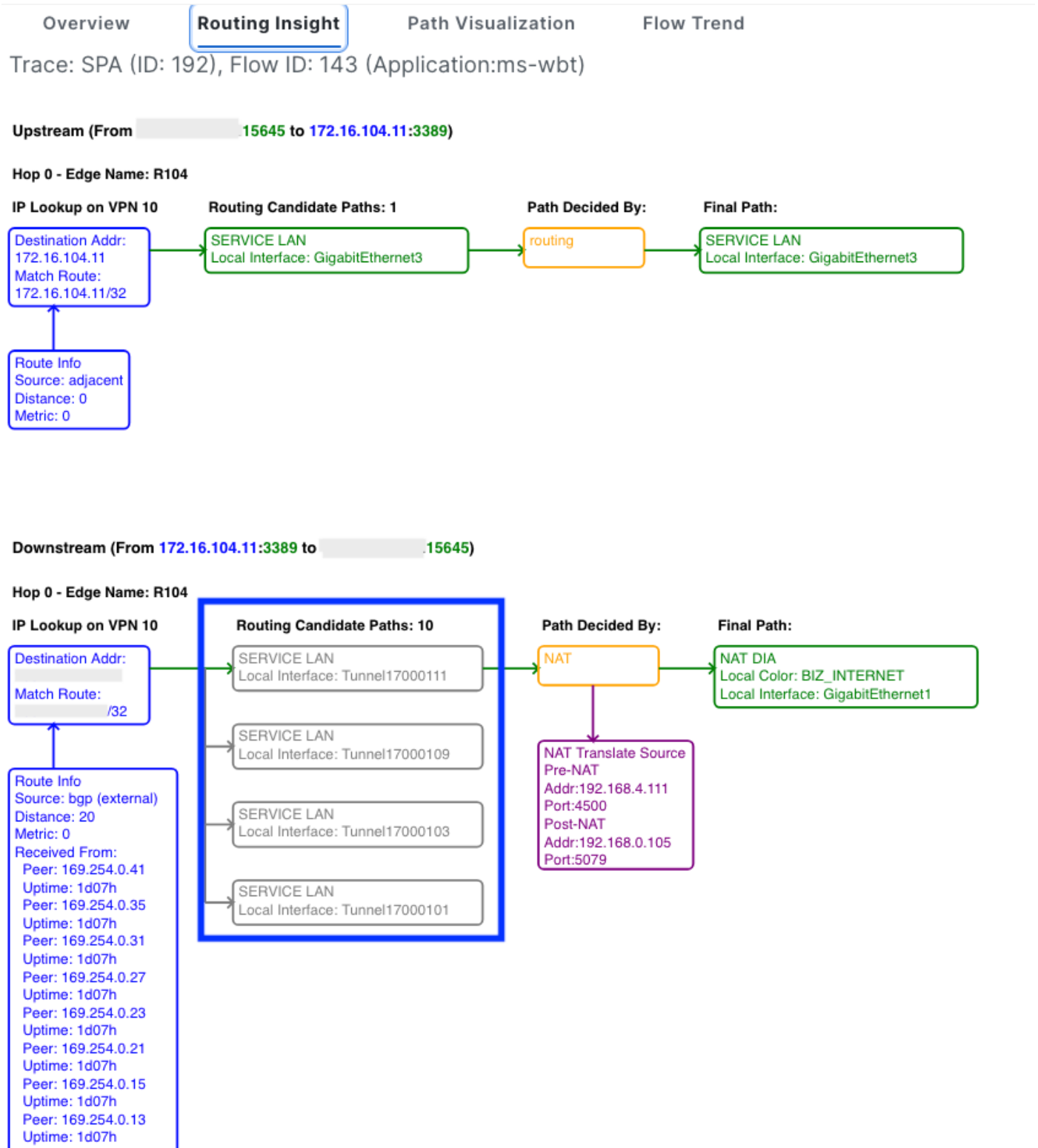
- Site: Choisissez le site où se trouve la ressource privée
- VPN: Sélectionnez l'ID VPN où se trouve la ressource privée
- Source/Destination Address: (Facultatif) Saisissez l'adresse IP ou laissez-la vide pour capturer tout le trafic filtré en fonction de site et VPN choisis

Démarrer le suivi

Localisez le flux de trafic et cliquez sur View dans la colonne Insights



La colonne routing Insights affiche les chemins candidats et les tunnels IPsec vers Secure Access



Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Centre d'aide Cisco Secure Access](#)
- [Guide de conception Cisco SASE](#)
- [Configuration d'un accès sécurisé avec des tunnels automatisés SD-WAN pour un accès Internet sécurisé](#)

- [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.