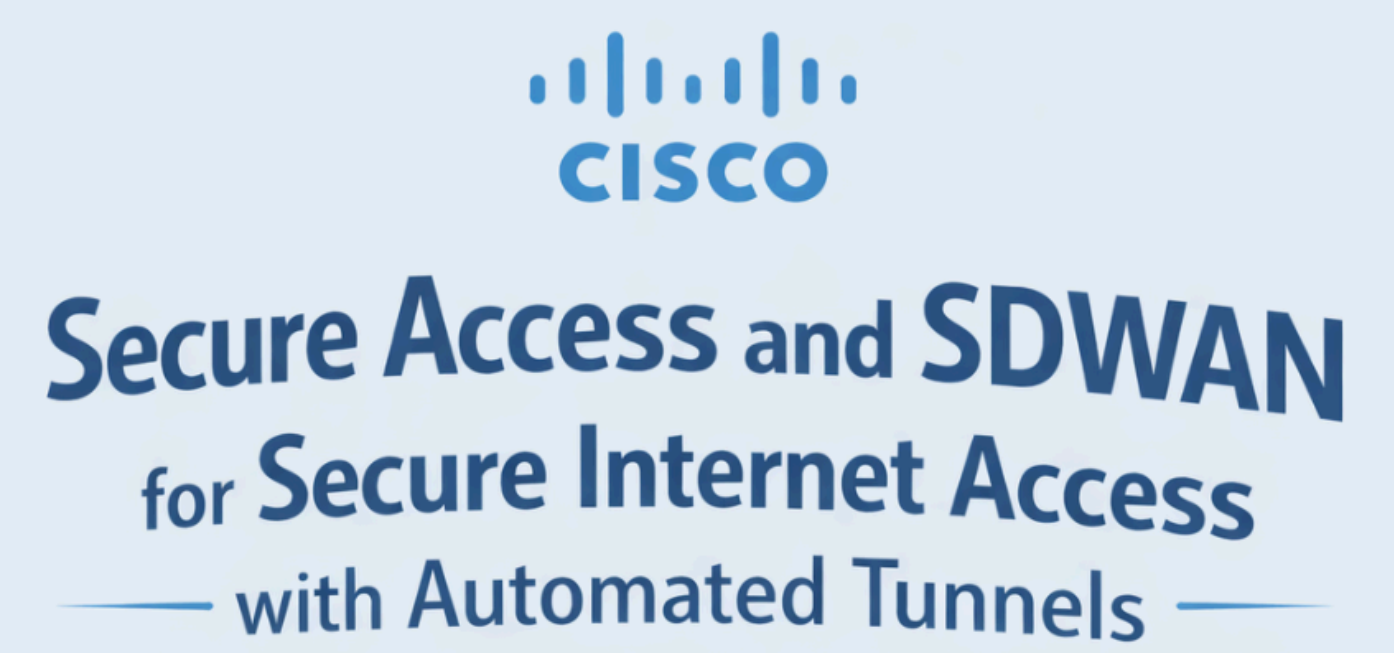
Configuration d'un accès sécurisé avec des tunnels automatisés SD-WAN pour un accès Internet sécurisé

Table des matières

Introduction

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



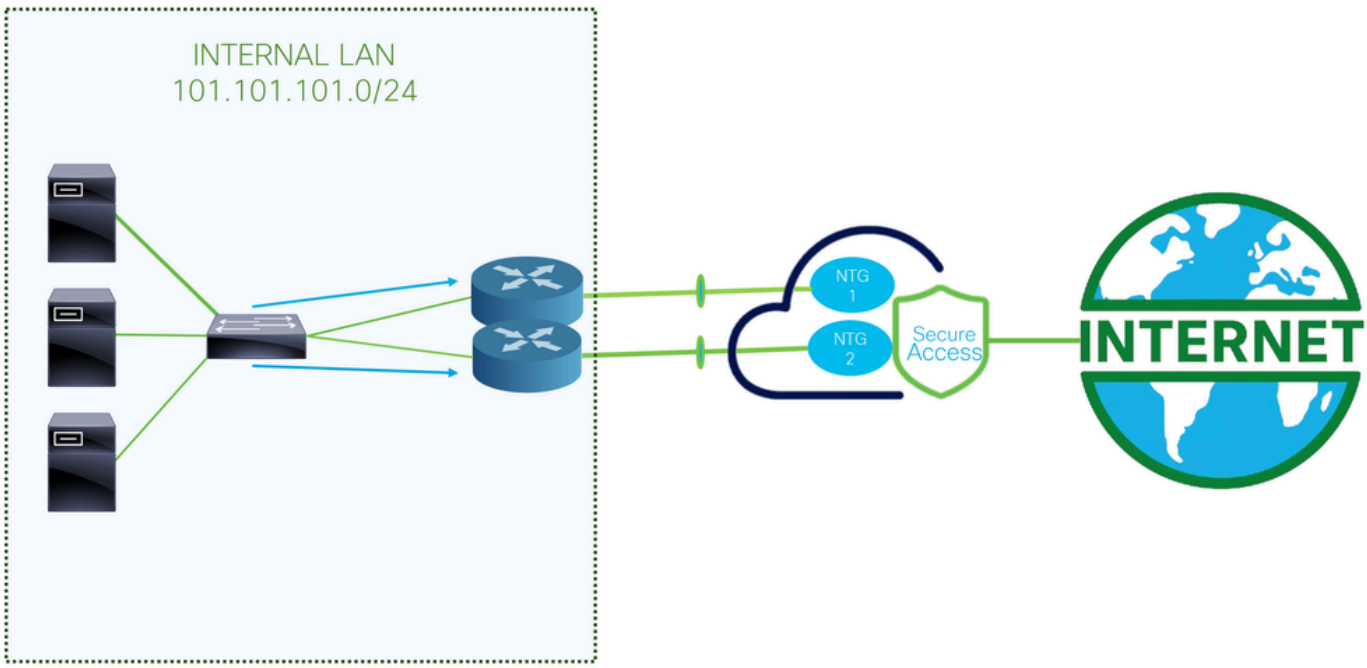
Informations générales

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

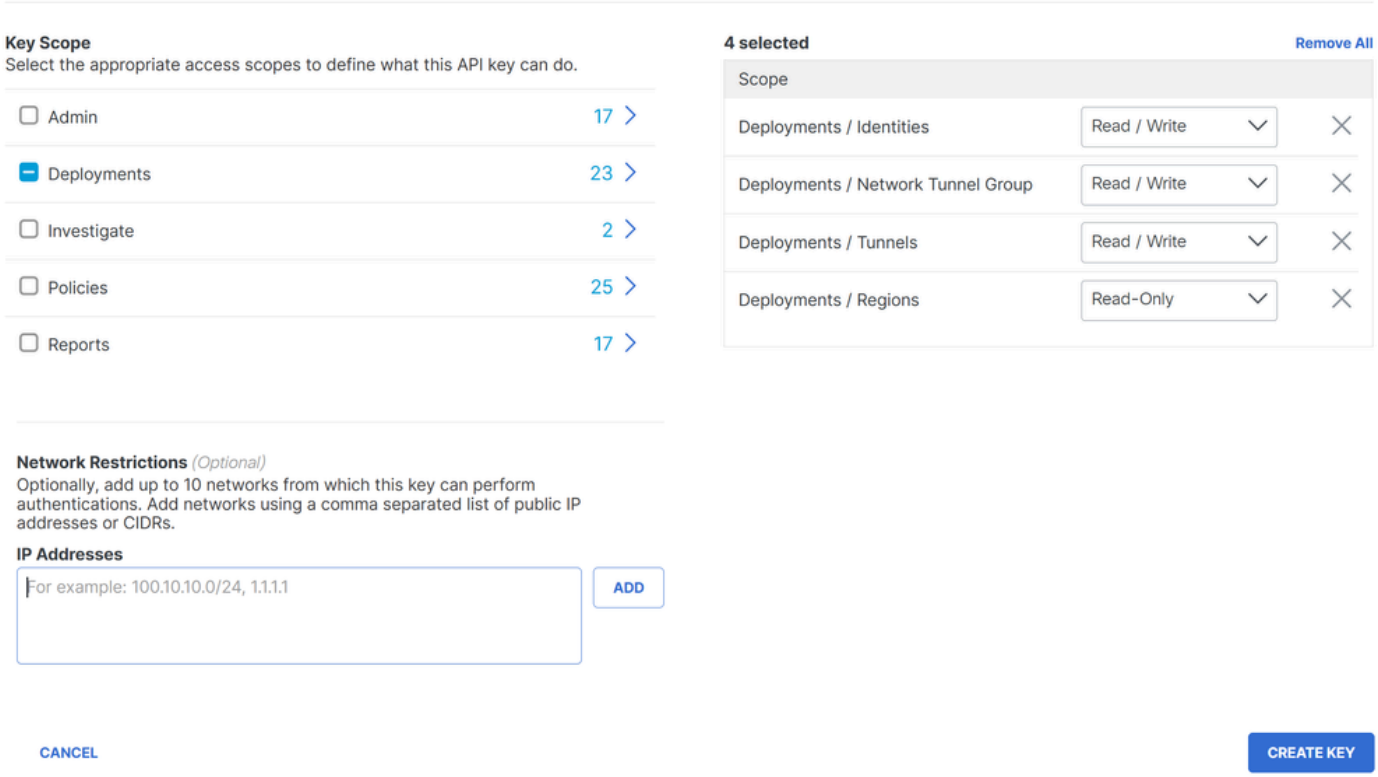
Configuration d'accès sécurisé

Création d'API

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

Accédez à Secure Access Dashboard.

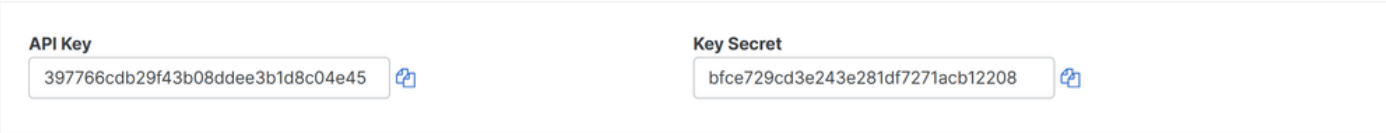
- Cliquez sur Admin > API Keys
- Cliquez sur Add
- Choisissez les options suivantes :
  - Deployments / Network Tunnel Group: Lecture/écriture
  - Deployments / Tunnels: Lecture/écriture
  - Deployments / Regions: Lecture seule
  - Deployments / Identities: Lecture-Écriture
  - Expiry Date: Ne jamais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



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.



⚠ 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.

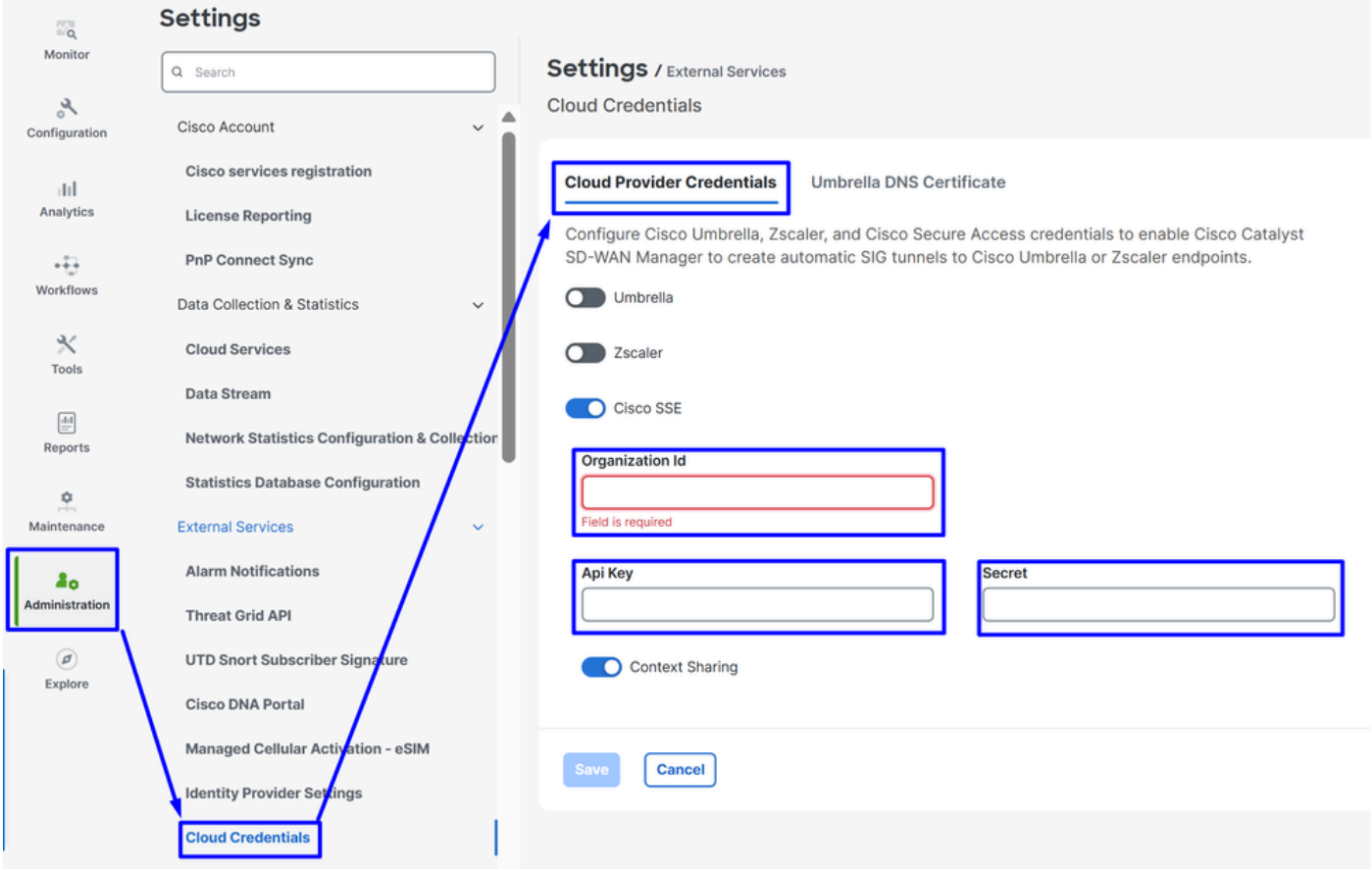
Pour finaliser, cliquez sur ACCEPT AND CLOSE.

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 SSEet remplissez les paramètres d'API et d'organisation



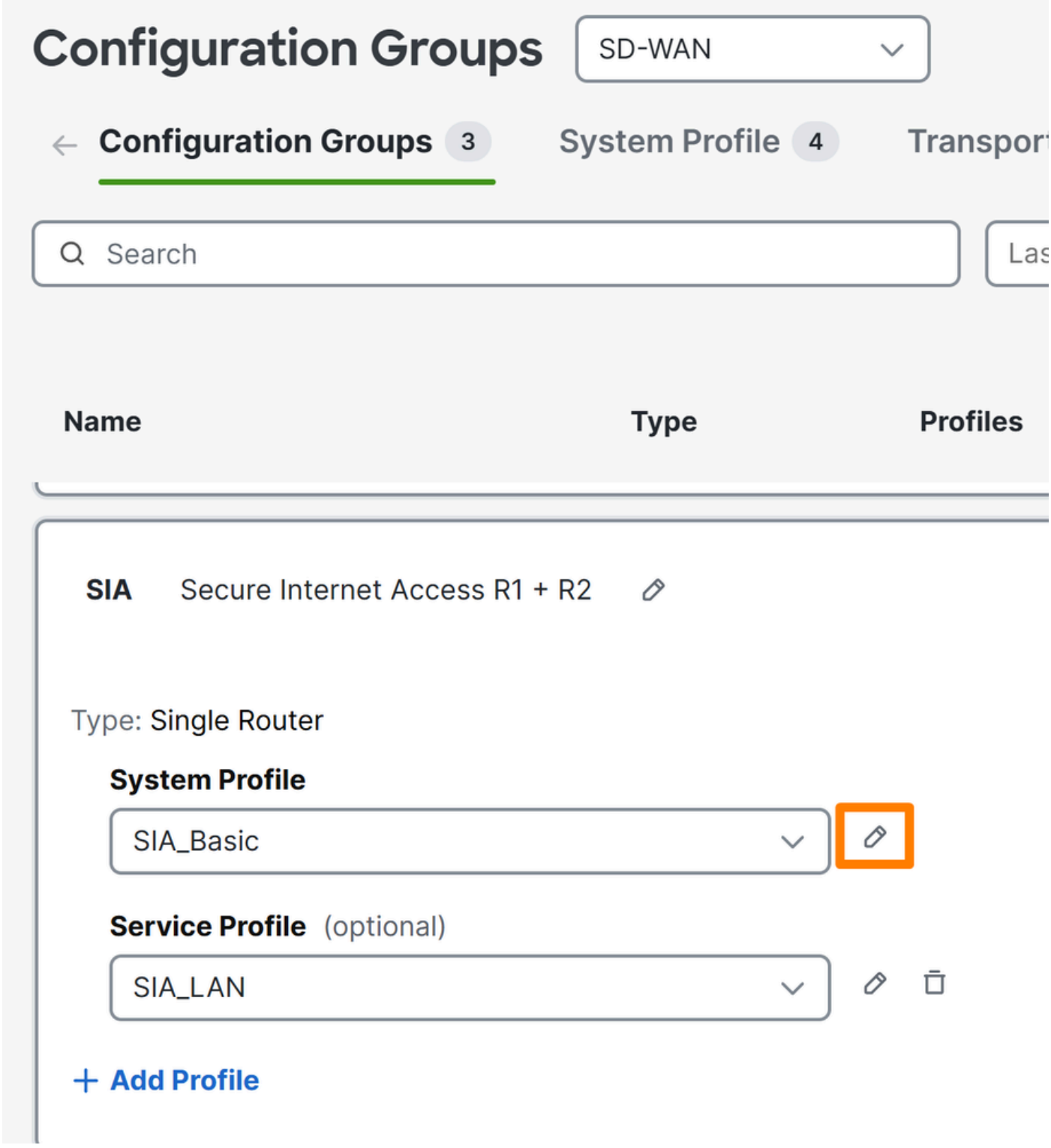
- Organization ID: Vous pouvez l'obtenir à partir de l'URL de votre tableau de bord SSE https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Copiez-le à partir de l'étape Configuration d'accès sécurisé
- Secret: Copiez-le à partir de l'étape Configuration d'accès sécurisé

Ensuite, cliquez sur le bouton qui Save apparaît.

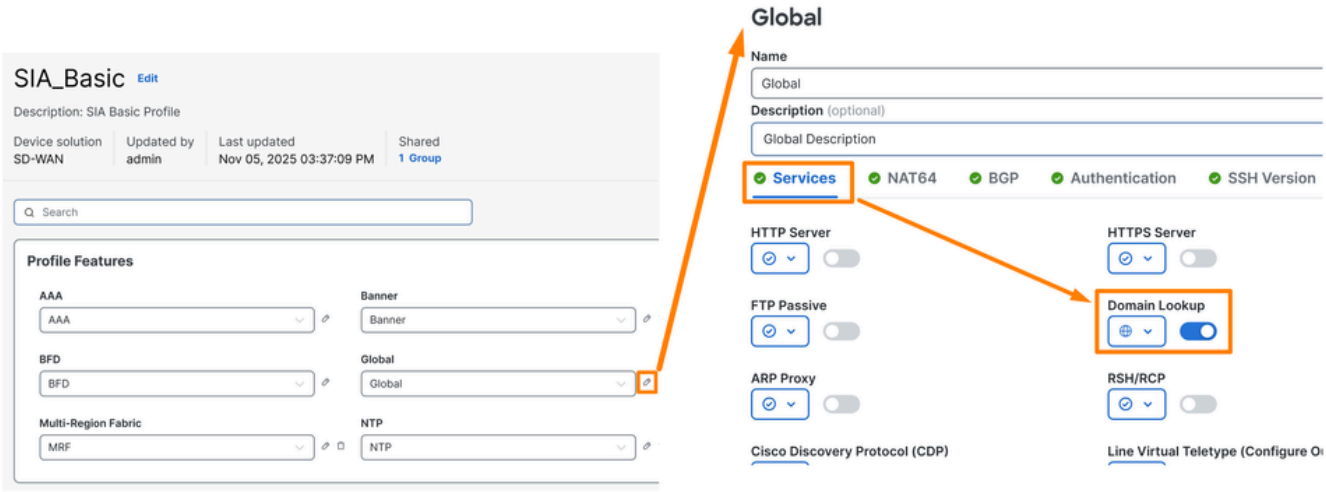
Remarque : Avant de passer aux étapes suivantes, vous devez vous assurer que le gestionnaire SD-WAN et les périphériques SD-WAN Catalyst disposent d'une résolution DNS et d'un accès à Internet.

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



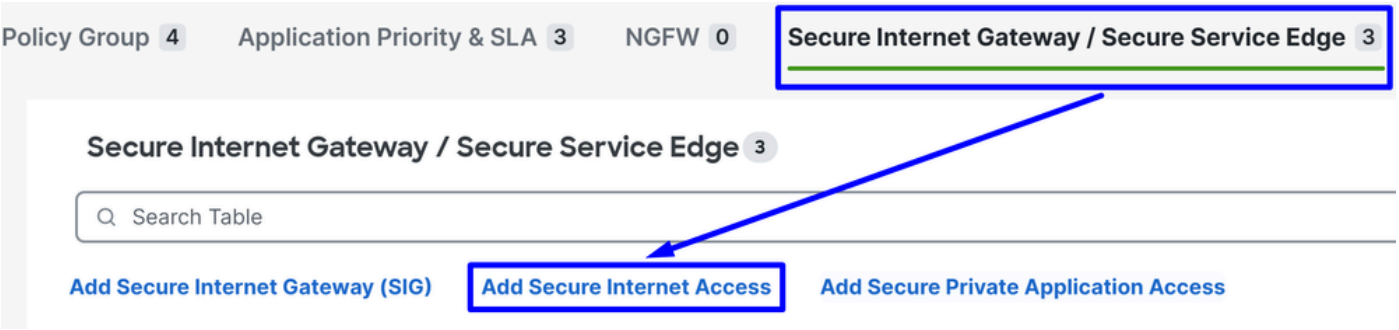
- Modifiez ensuite l'option Global et assurez-vous que l'option Domain Resolution est activée



Configurer le groupe de stratégies

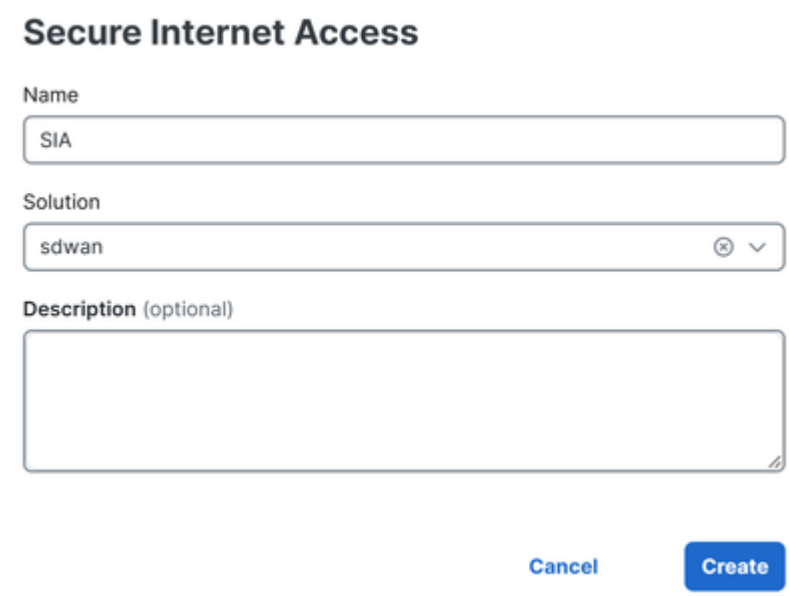
Accédez à Configuration > Policy Groups :

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

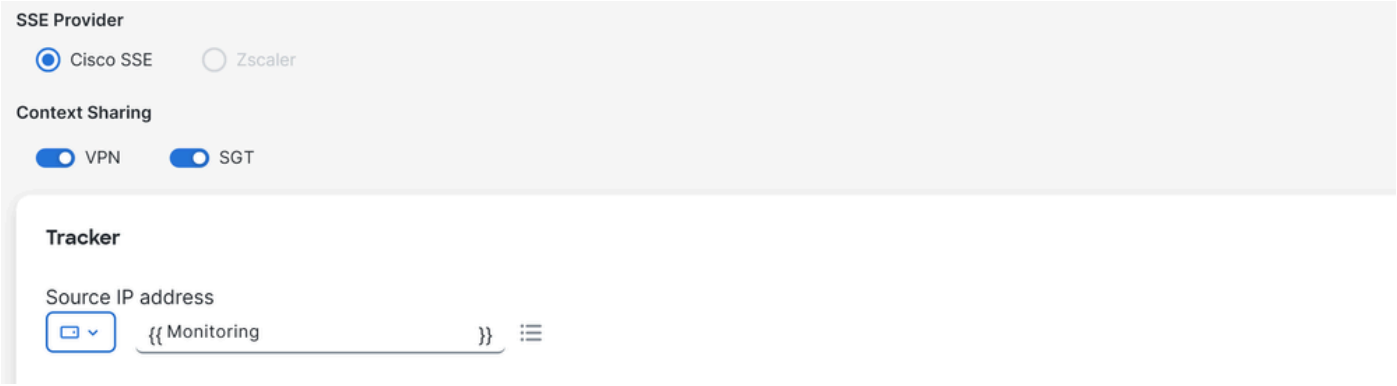


Remarque : Dans les versions inférieures à 20.18, cette option est appelée Add Secure Service Edge (SSE)

- Configurez un nom, une solution et cliquez sur Create

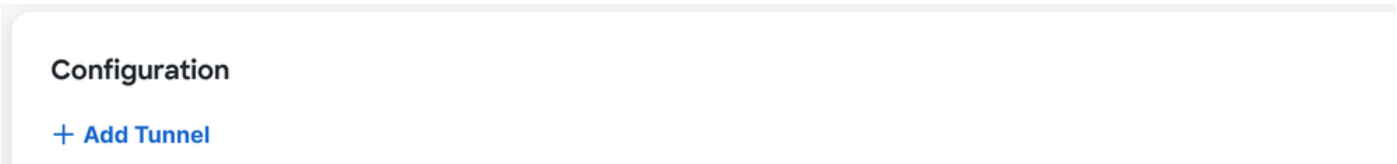


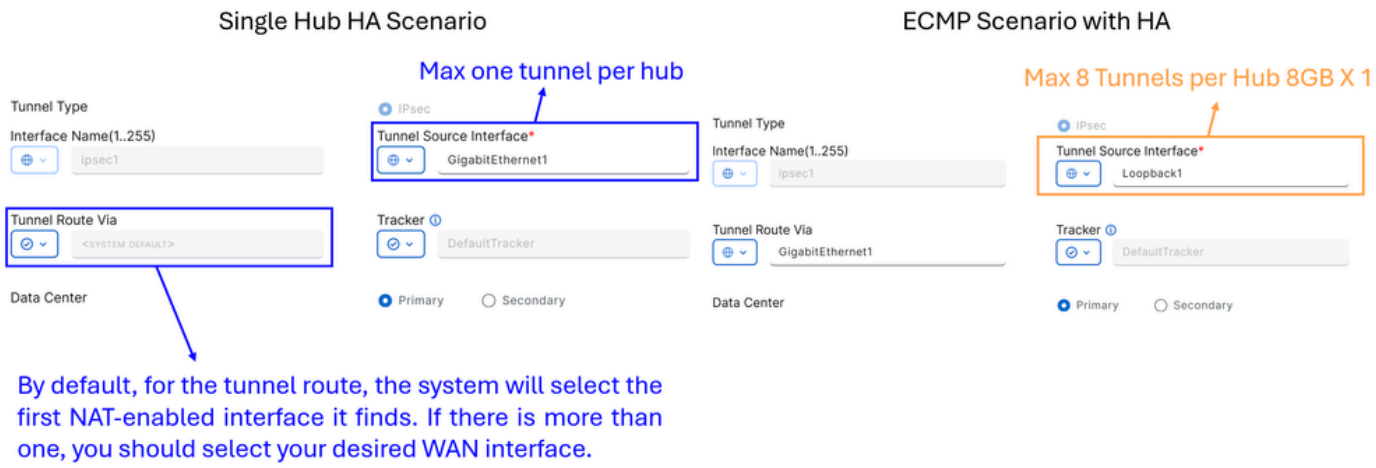
Les configurations suivantes vous permettent de créer les tunnels après avoir déployé la configuration dans vos Catalyst SD-WAN Edge :



- 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 :





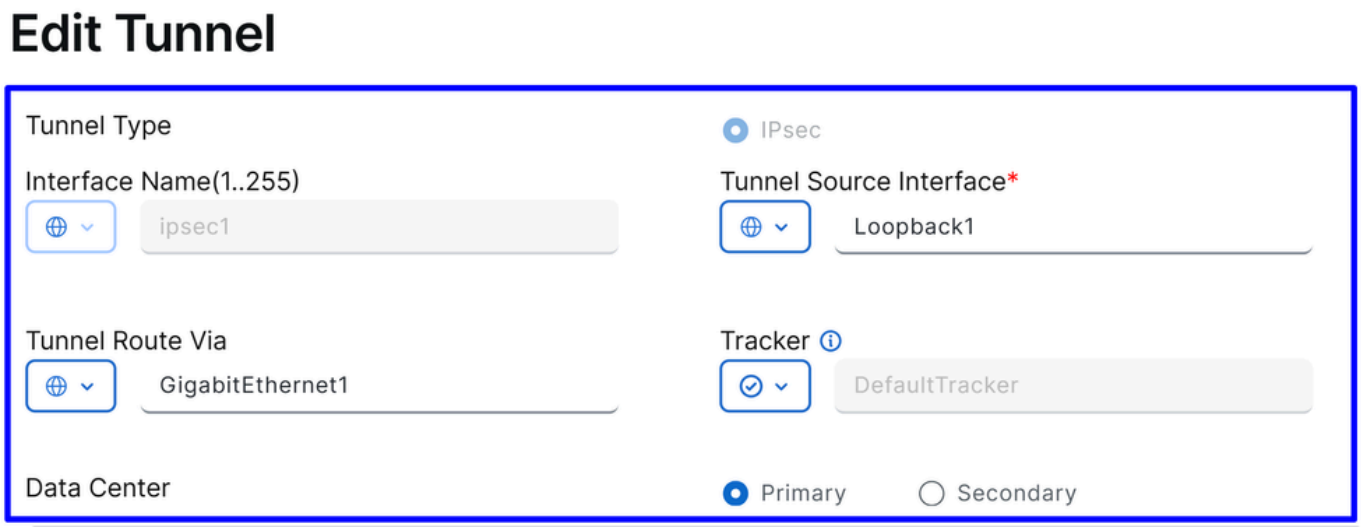
- **Single Hub HA Scenario**: Dans ce scénario, vous pouvez configurer la haute disponibilité en utilisant un NTG comme actif et un autre comme passif, avec un débit maximal de 1 Gbit/s par NTG
- ECMP Scenario with HA: Dans ce scénario, vous pouvez configurer jusqu'à 8 tunnels par concentrateur, prenant 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.

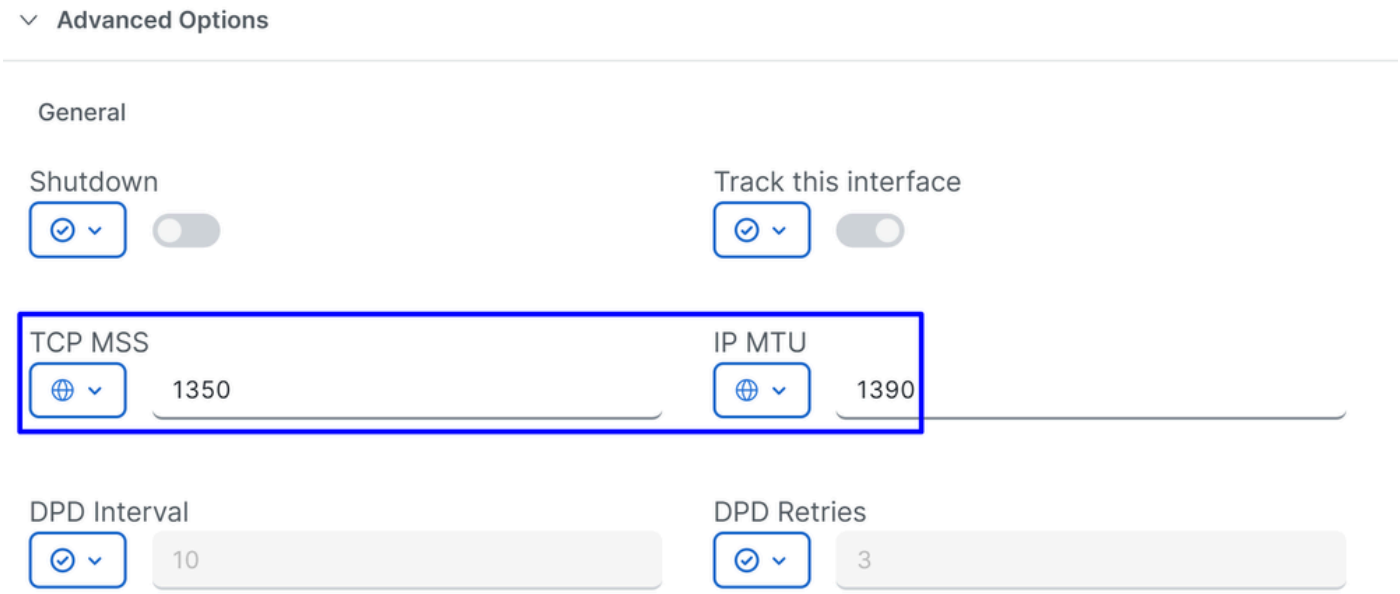
Avertissement : Si vous voulez configurer des interfaces de bouclage pour un scénario ECMP, vous devez d'abord configurer les interfaces de bouclage dans Configuration Groups > Transport & Management Profile, selon la politique que vous utilisez dans votre routeur.

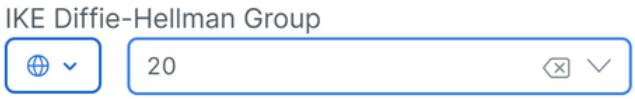
- Cliquez surAdd Tunnel



- 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.

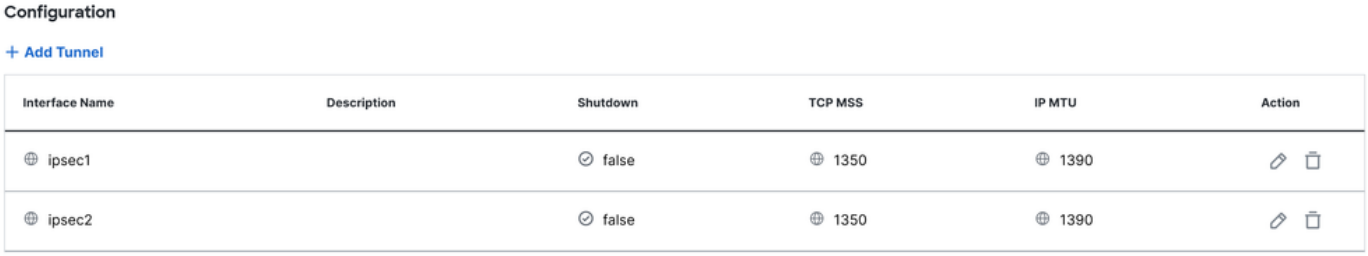




- TCP MSS: 1350
- IP MTU: 1390
- IKE Diffie-Hellman Group: 20

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

SCÉNARIO DE DISPONIBILITÉ HAUTE DISPONIBILITÉ À CONCENTRATEUR UNIQUE



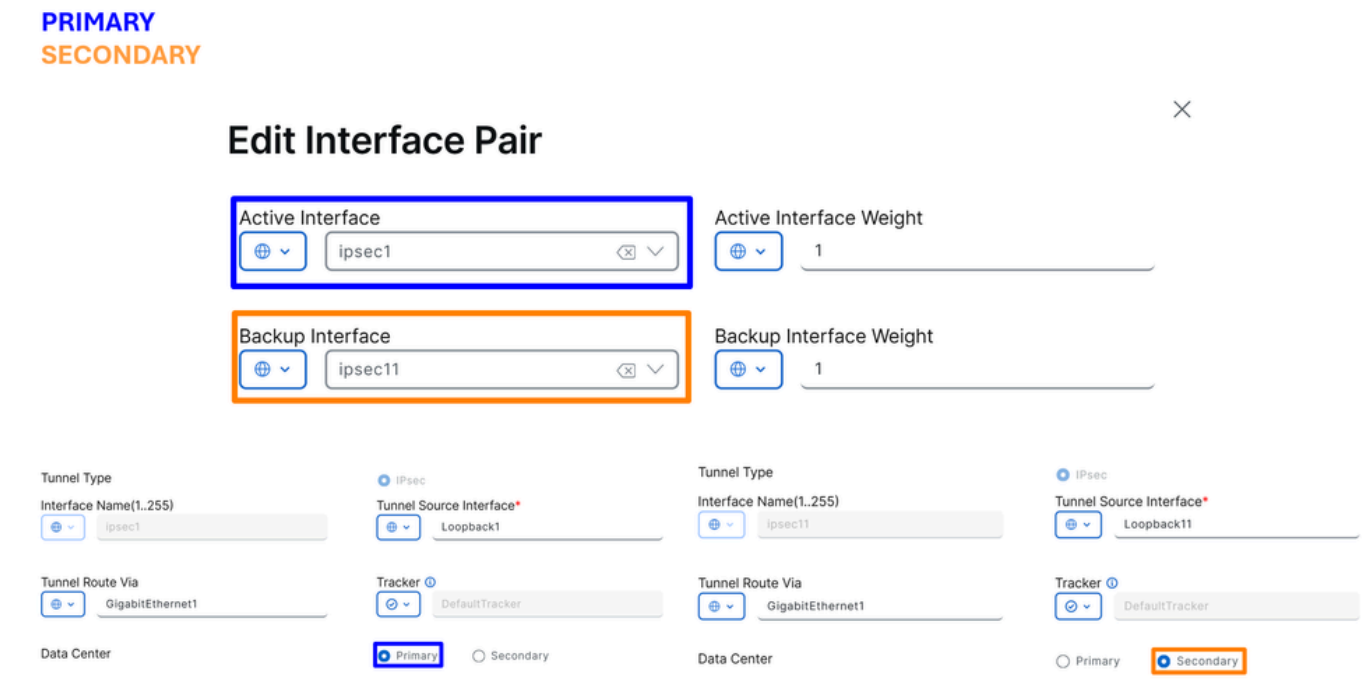
Il s'agit du résultat final lorsque vous utilisez le déploiement de scénario normal.

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.

Cliquez sur Add Interface Pair :

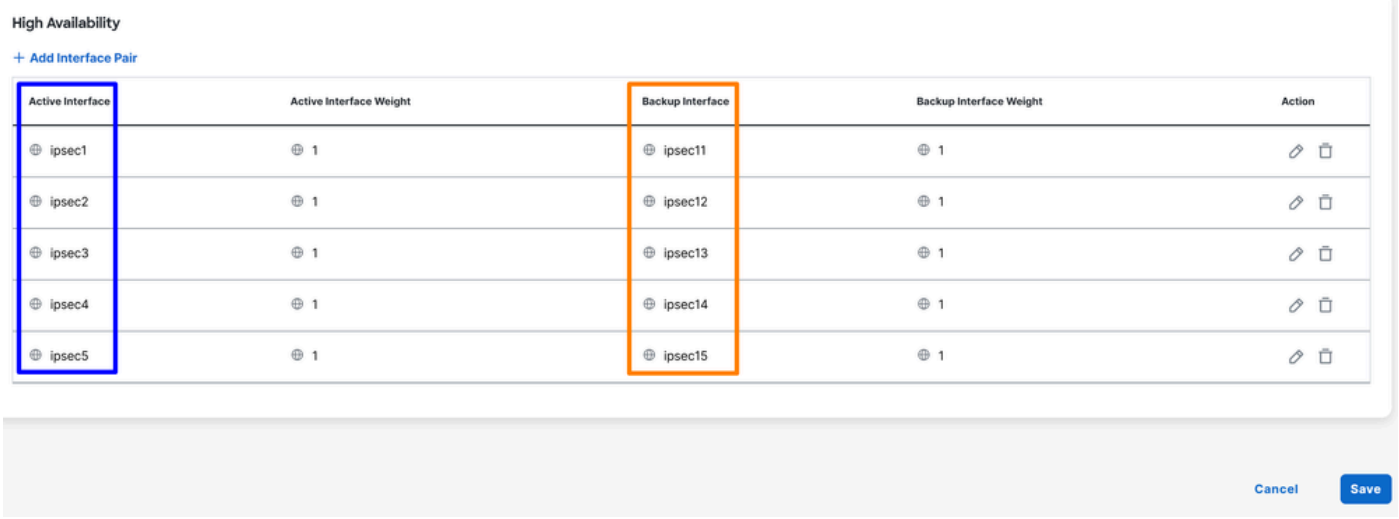


Dans cette étape, vous devez configurer les tunnels principal et secondaire pour chaque paire de tunnels que vous configurez. Cela signifie que chaque tunnel a sa propre sauvegarde. N'oubliez pas que ces tunnels ont été créés en tant que tunnels principal et secondaire à cette fin précise. "Active interface"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



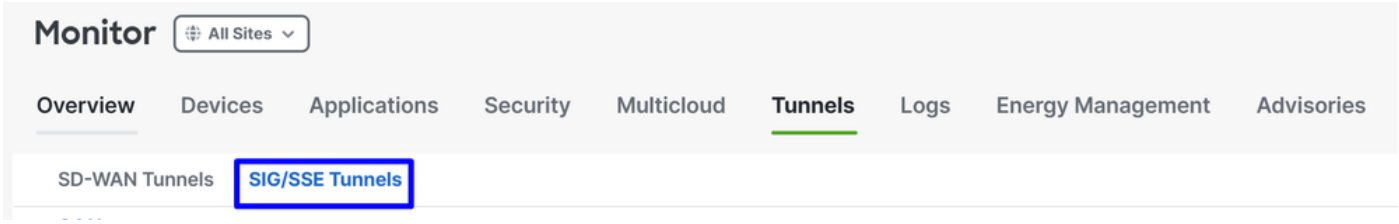
Remarque : Un maximum de 8 paires de tunnels (16 tunnels : 8 principaux et 8 secondaires) peuvent être configurés dans SD-WAN Catalyst vManage. Cisco Secure Access prend en charge jusqu'à 10 paires de tunnels.

- 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 surSIG/SSE Tunnels

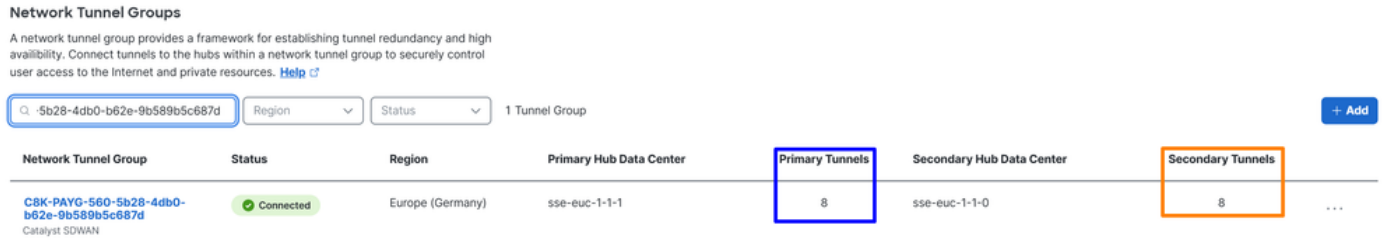


Et vous pouvez voir les tunnels établis vers Cisco Secure Access UP ou non.

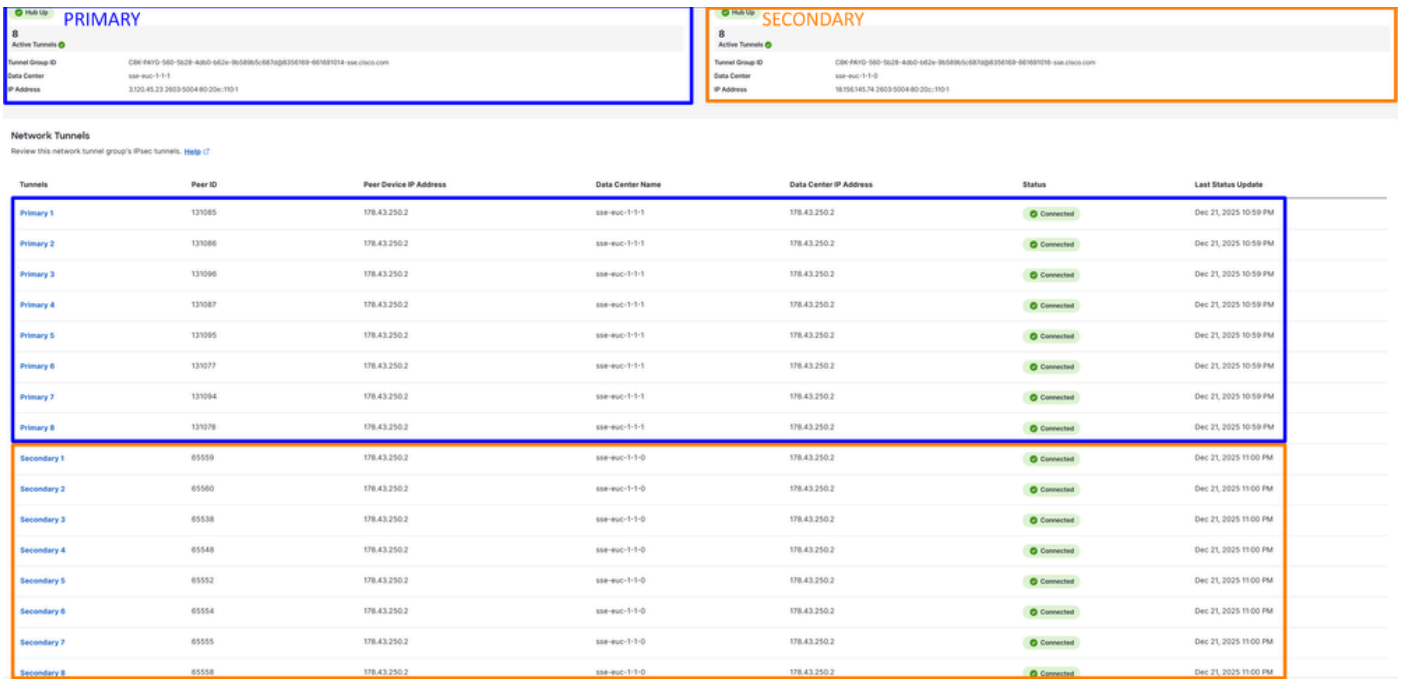
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public 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

Pour vérifier dans Secure Access, procédez comme suit :

- Cliquez sur Connect > Network Connections



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



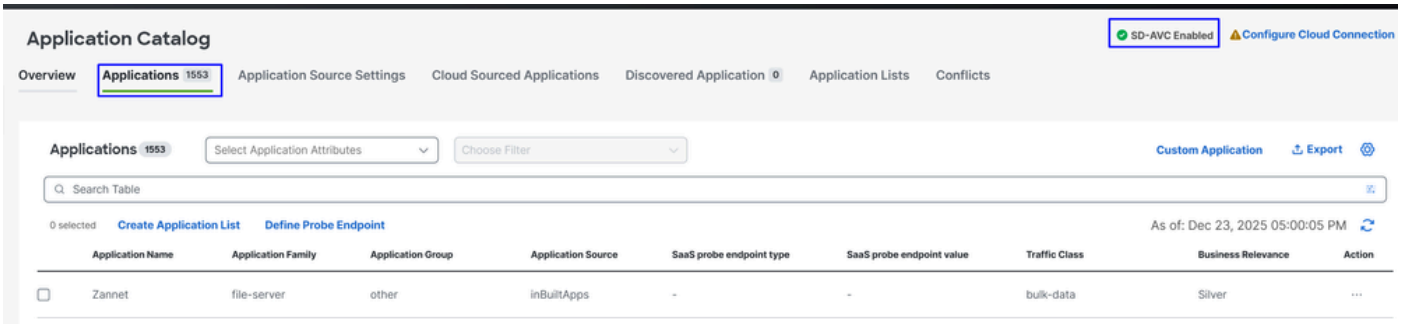
Après cela, vous pouvez passer à l'étape, Create your Custom Bypass FQDN or APP in SD-WAN

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 :

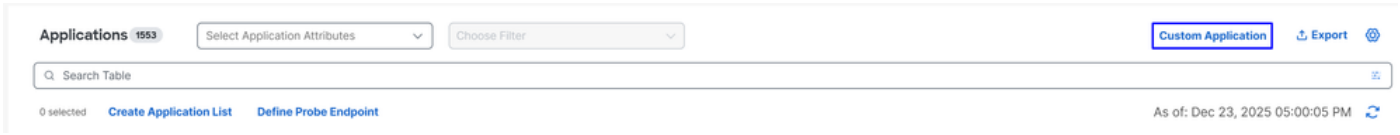
- Cliquez sur Configuration > Application Catalog > Applications



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

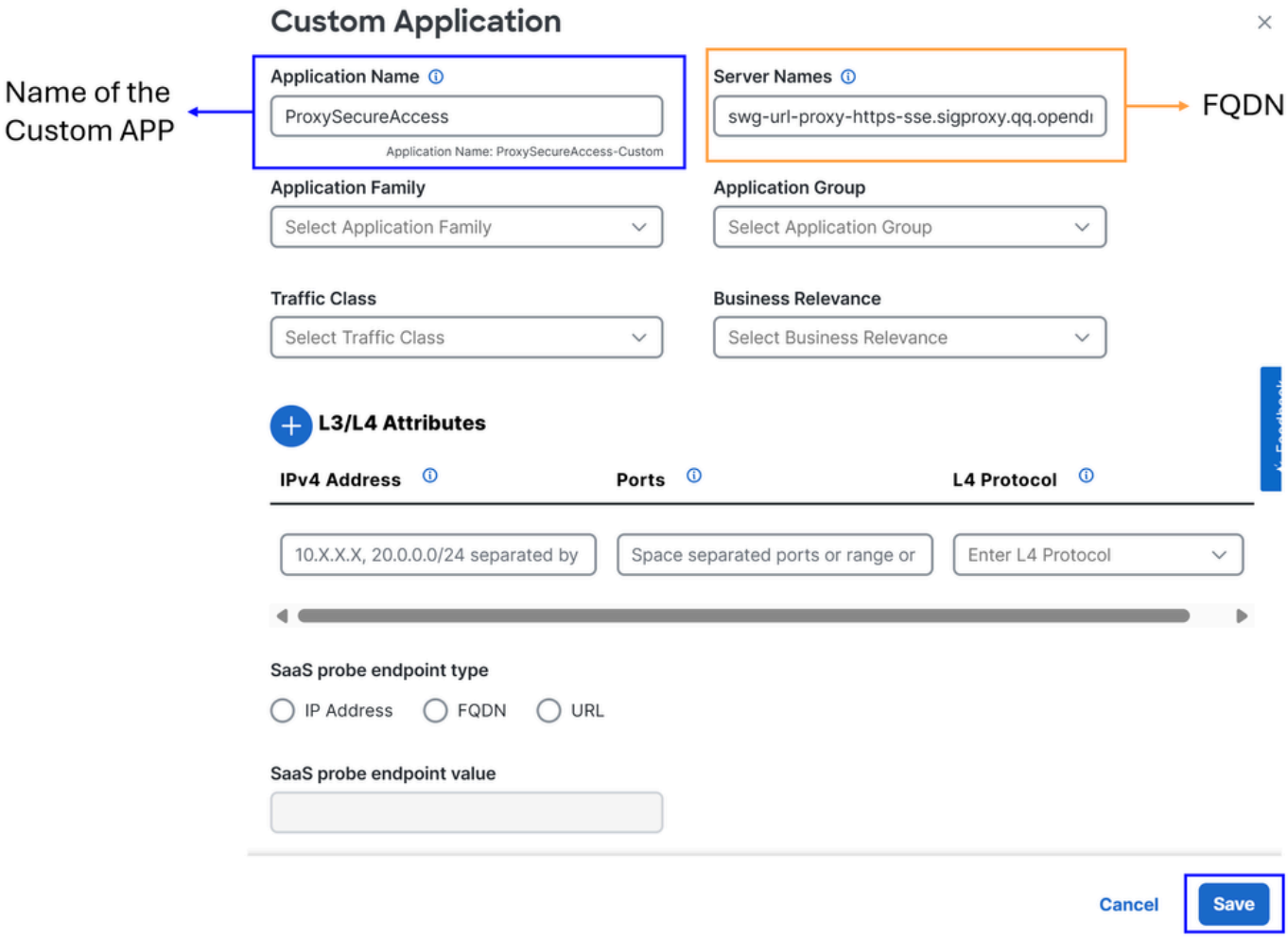
Remarque : Pour avoir accès au catalogue d'applications, vous devez activer SD-AVC.

- Cliquez sur Custom Application



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

ProxySecureAccess

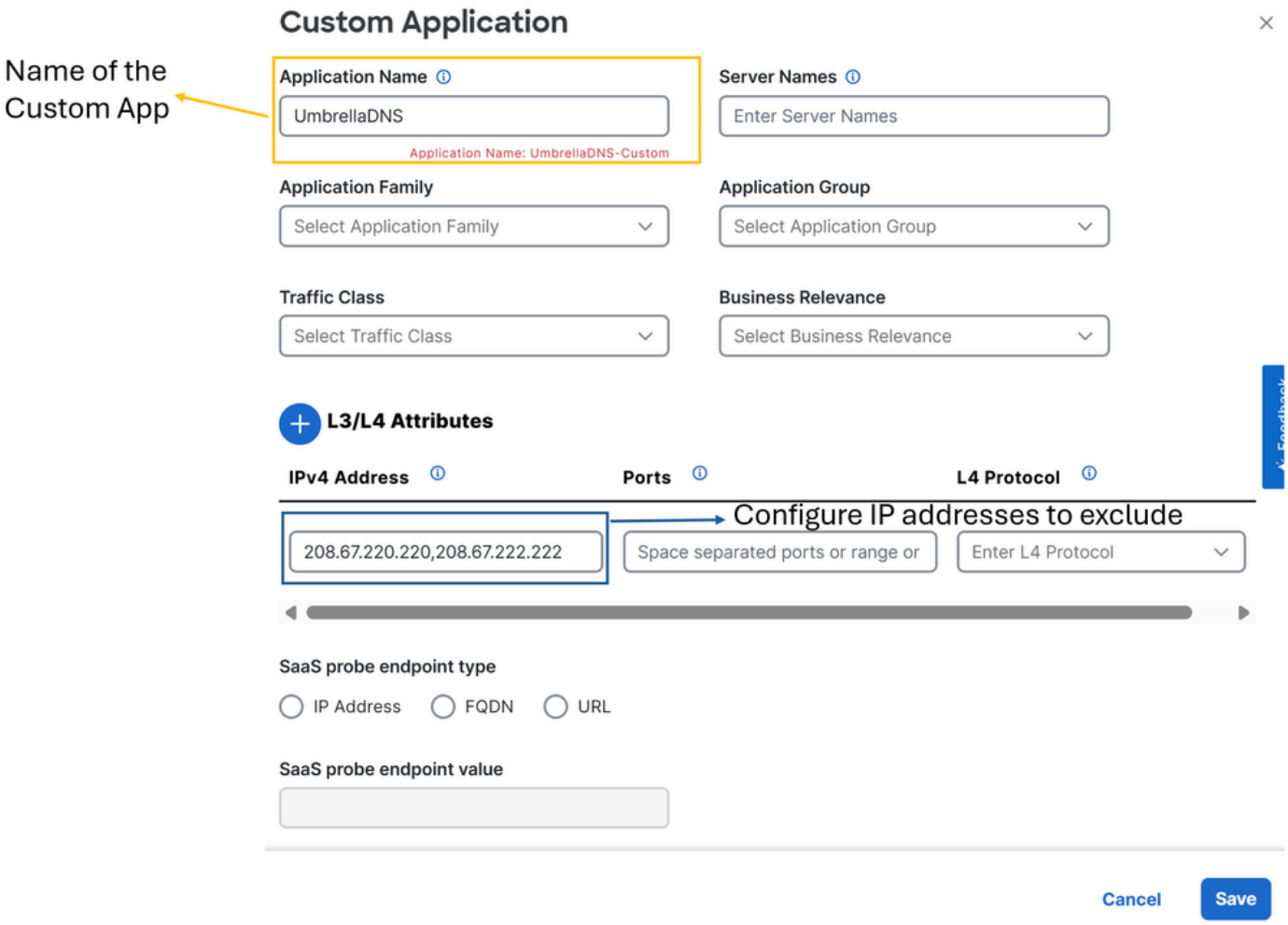


- Server Name: Utilisez le FQDN que vous souhaitez contourner (dans cet exemple, les FQDN de SWG sont configurés)
  - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Cliquez sur Save

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

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

UmbrellaDNS



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 :

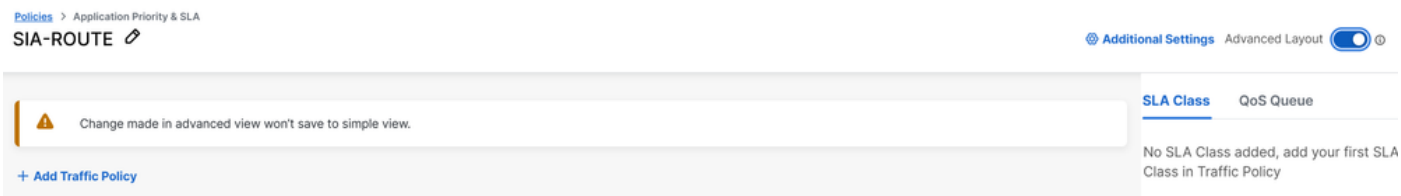
- Configuration > Configuration Groups > Service Profile > Service Route: Cette méthode assure le routage vers l'accès sécurisé, mais manque de flexibilité.
- **Configuration** > Policy Groups > Application Priority & SLA: Cette méthode offre diverses options de routage dans SD-WAN et, plus important 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

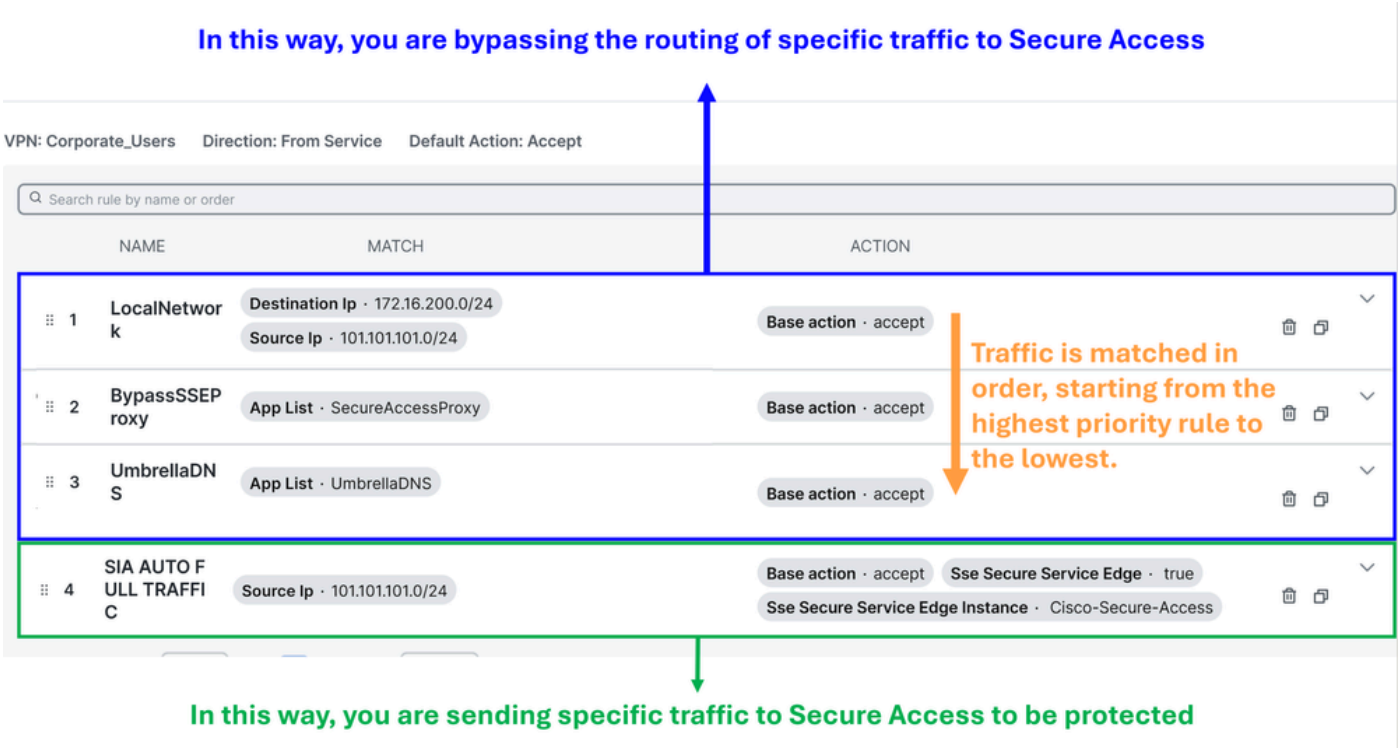
- Configurez un nom de stratégie et cliquez sur Create

- Activer Advanced Layout
- Cliquez sur + Add Traffic Policy



- 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 :



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)

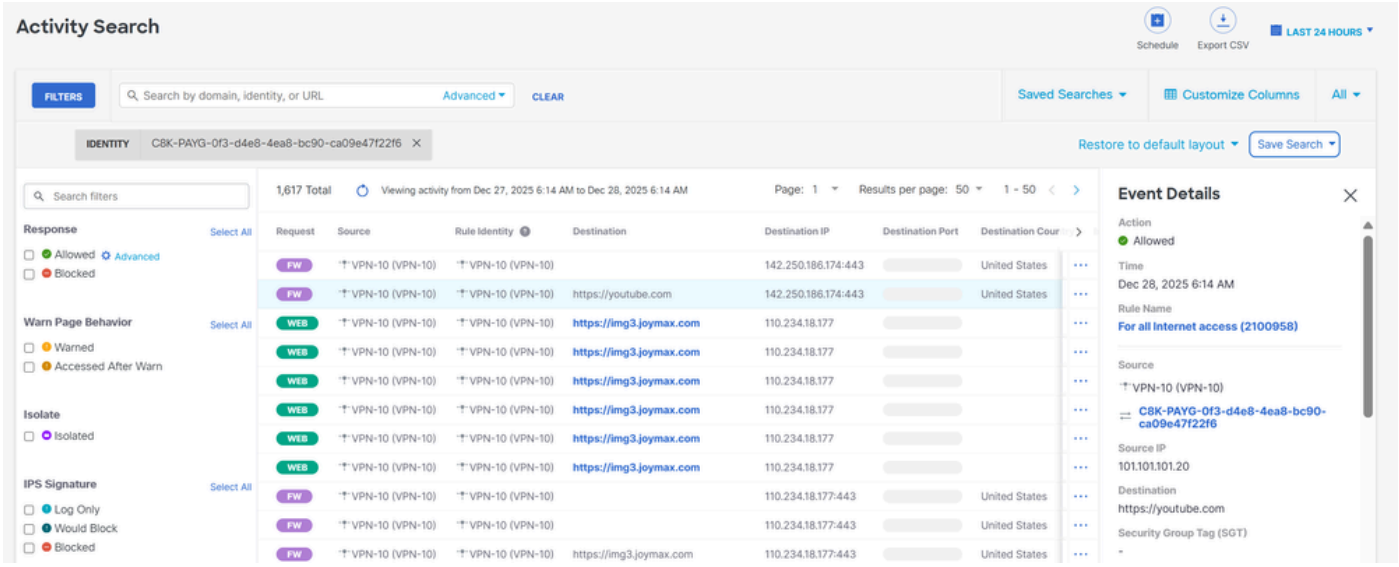
2. **BypassSSEProxy (Optional)**: Cette stratégie empêche les ordinateurs internes sur lesquels le module Cisco Umbrella est activé dans Secure Client et SWG de renvoyer le trafic proxy vers le cloud. Le routage du trafic proxy vers le cloud n'est pas considéré comme une bonne pratique.
3. UmbrellaDNS (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 :

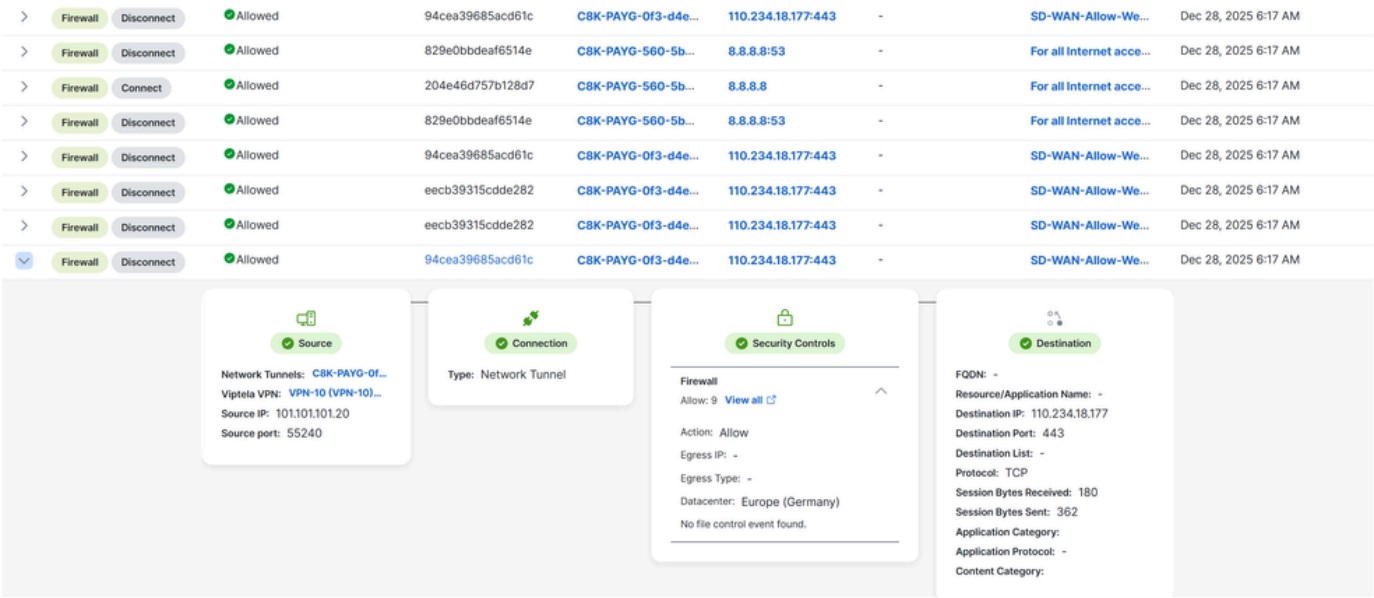
Accès sécurisé - Recherche d'activité

Accédez à Monitor > Activity Search:



Accès sécurisé - Événements

Accédez à Monitor > Events:

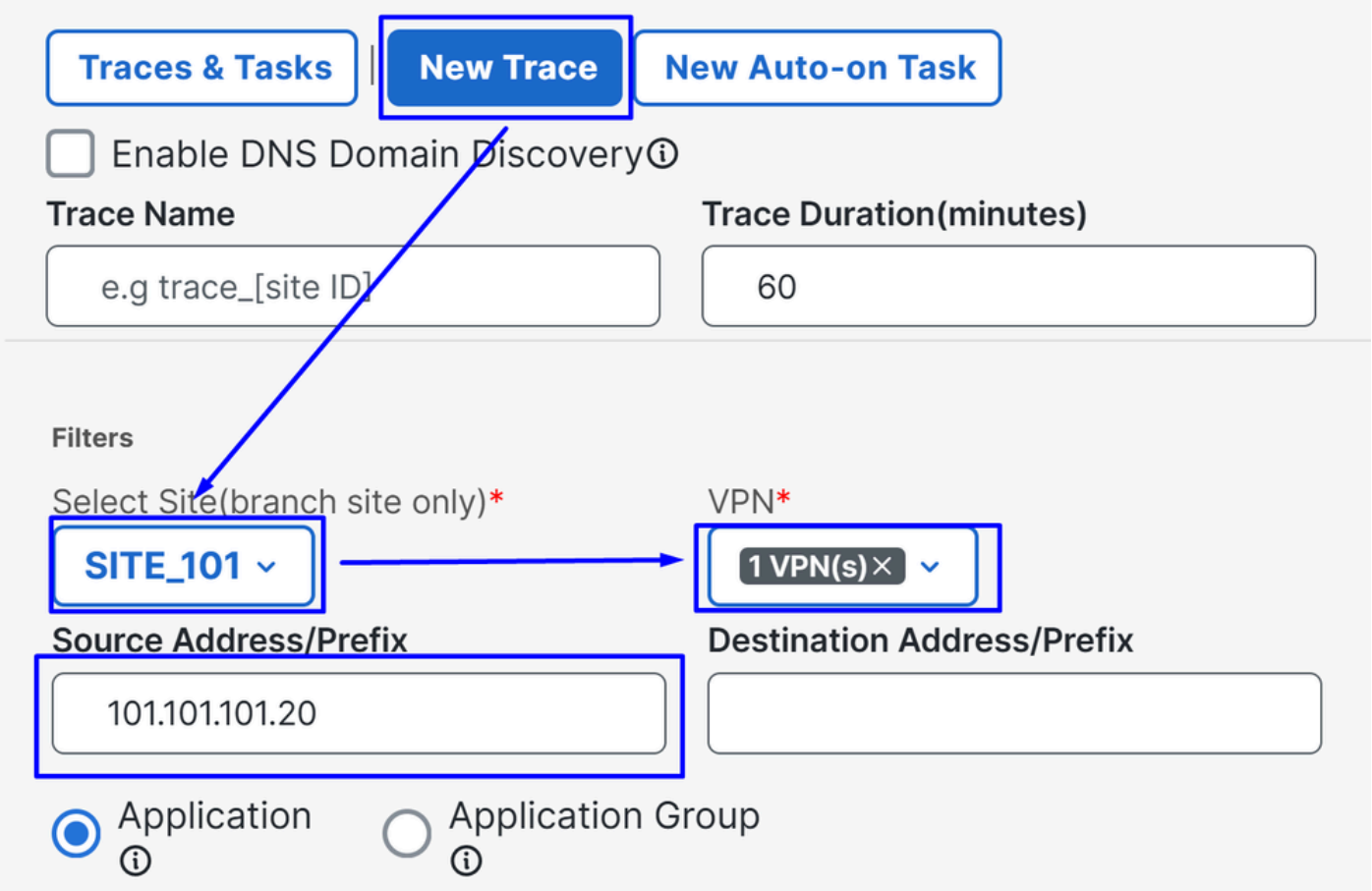


Remarque : Assurez-vous que votre stratégie par défaut avec la journalisation activée est désactivée par défaut.

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

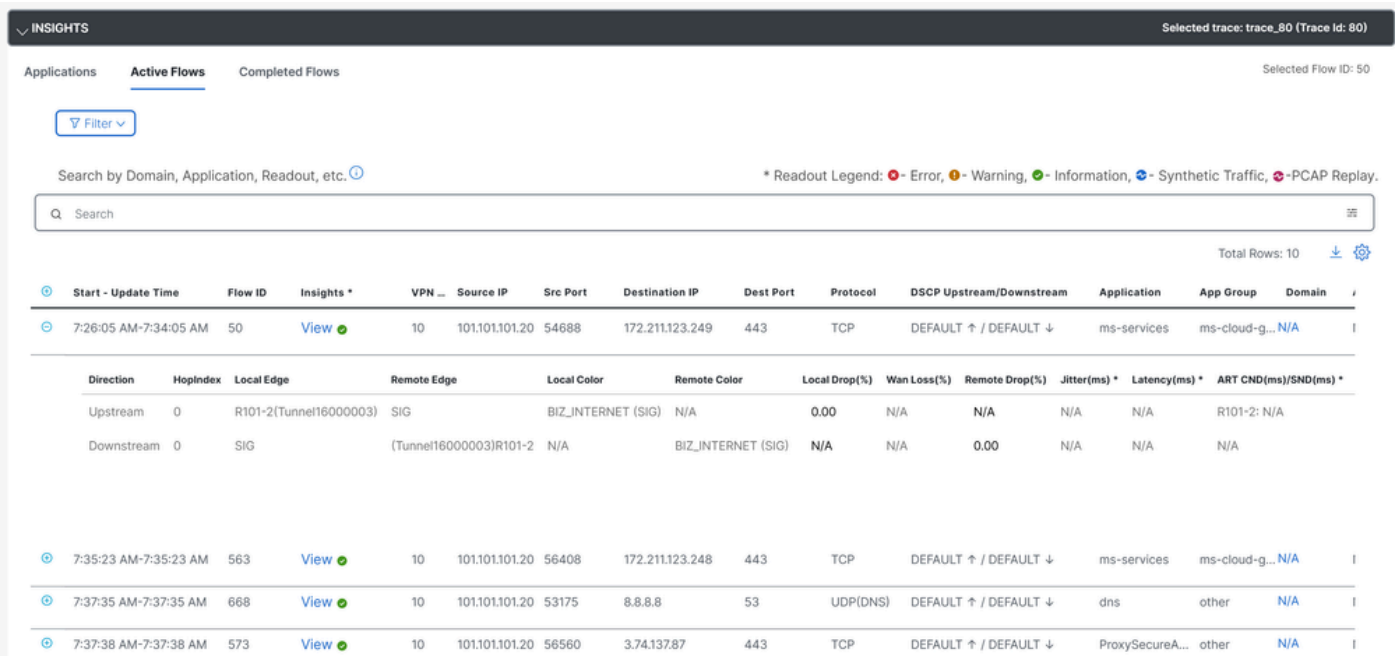
Accédez à Catalyst SD-WAN Manager :

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



- 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 :



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.