Configurer un accès sécurisé avec le pare-feu Sophos XG

Table des matières

Introduction

Ce document décrit comment configurer l'accès sécurisé avec le pare-feu Sophos XG.

Conditions préalables

- Configurer le provisionnement utilisateur
- Configuration de l'authentification ZTNA SSO
- Configuration de l'accès sécurisé VPN à distance

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu Sophos XG
- Accès sécurisé

- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- ZTNA sans client

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Pare-feu Sophos XG
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA

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.

Informations générales

Accès sécurisé - Sophos

Cisco a conçu Secure Access pour garantir la protection et l'accès aux applications privées, sur site et dans le cloud. Il protège également la connexion du réseau à Internet. Pour ce faire, plusieurs méthodes et couches de sécurité sont mises en oeuvre, toutes visant à préserver les informations lorsqu'elles y accèdent via le cloud.

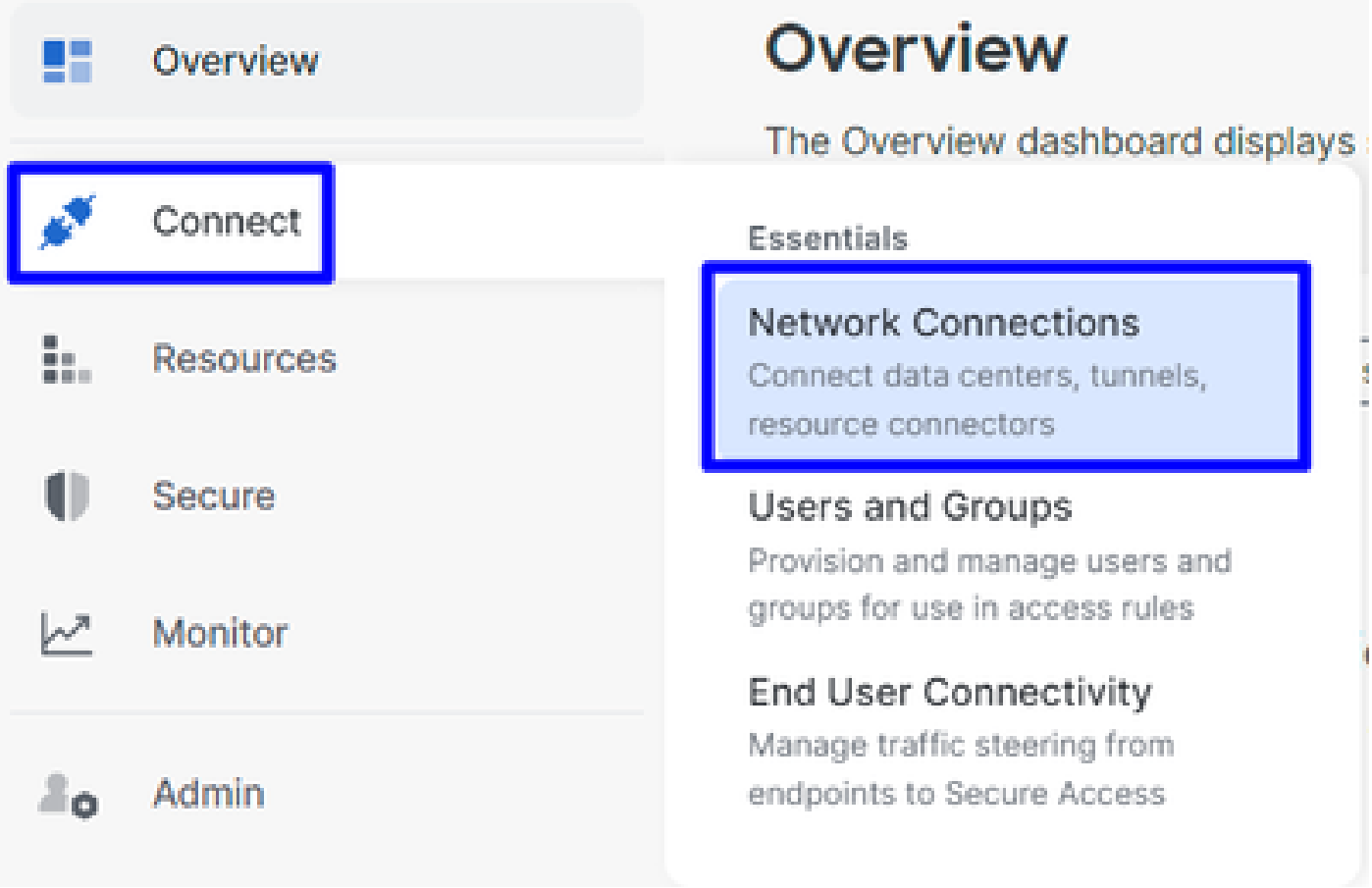
Configurer

Configuration du tunnel sur l'accès sécurisé

Accédez au panneau d'administration de Secure Access.

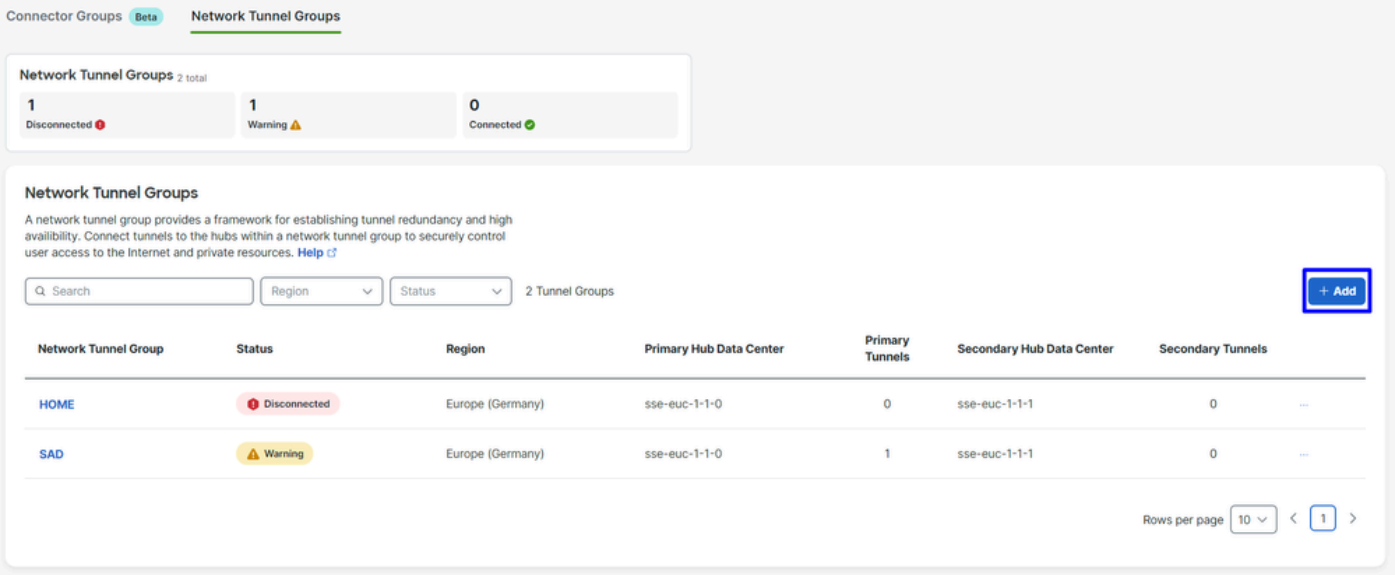
Accès sécurisé - Page principale

- Cliquez sur Connect > Network Connections.



Accès sécurisé - Connexions réseau

- Sous Network Tunnel Groups cliquez sur + Add.



Accès sécurisé - Groupes de tunnels réseau

- Configurez Tunnel Group Name, Region et Device Type.
- Cliquez sur **Next**.

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

SophosFirewall

Region

Europe (Germany)

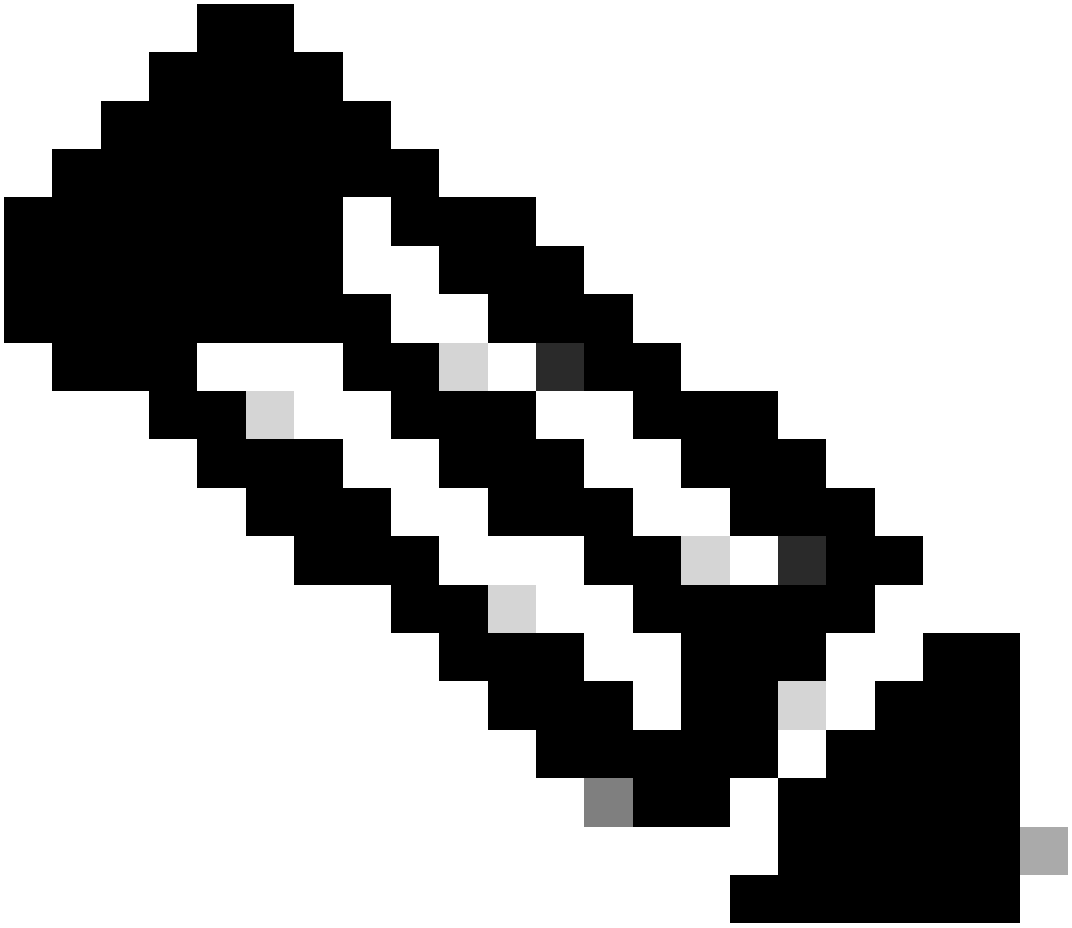
Device Type

Other

Cancel

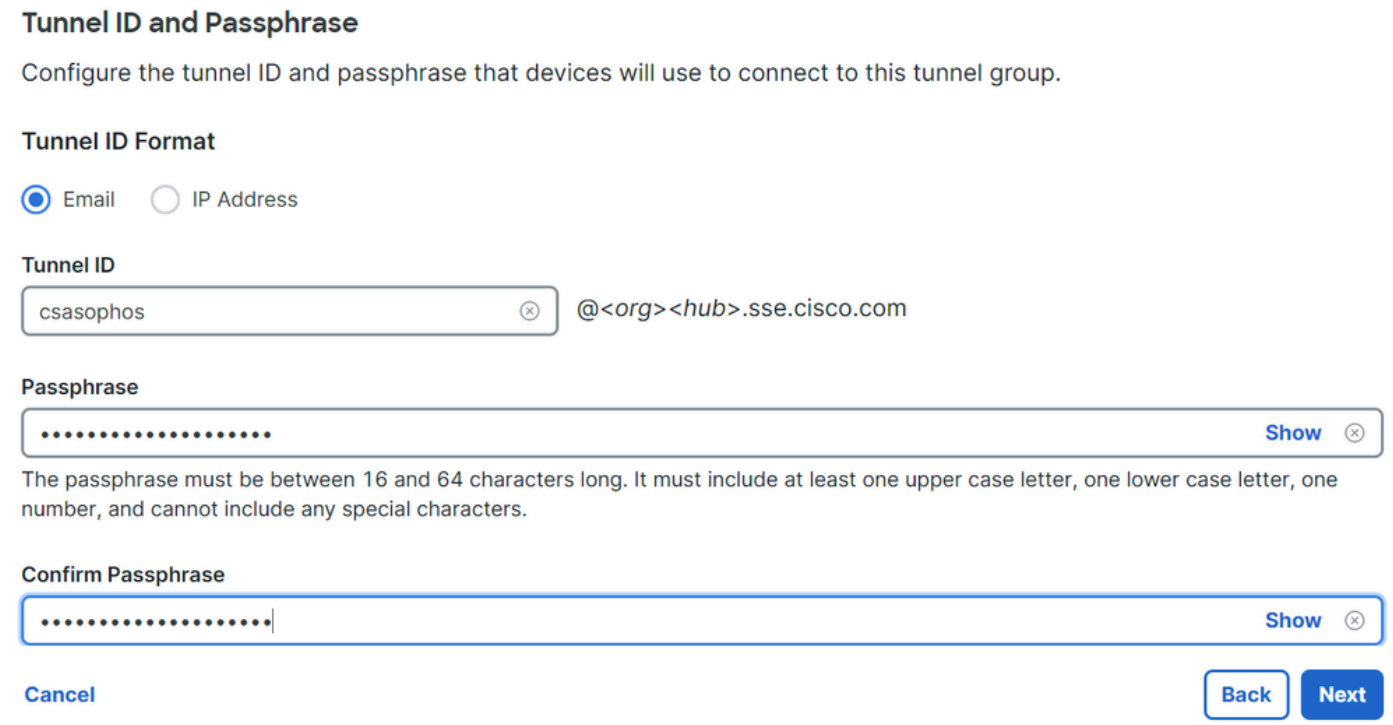
Next

Accès sécurisé - Groupes de tunnels - Paramètres généraux



Remarque : choisissez la région la plus proche de l'emplacement de votre pare-feu.

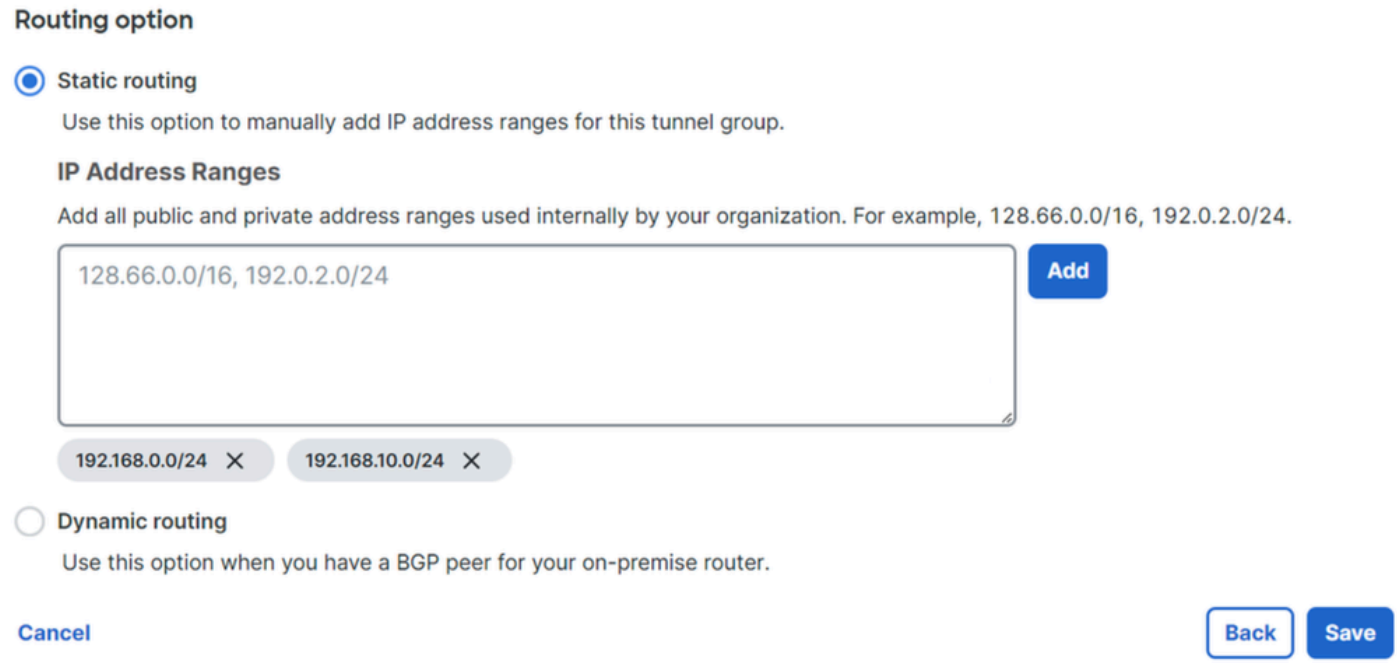
- Configurez les Tunnel ID Format et Passphrase.
- Cliquez sur Next.



Accès sécurisé - Groupes de tunnels - ID de tunnel et phrase de passe

- Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez faire passer le trafic via l'accès sécurisé.

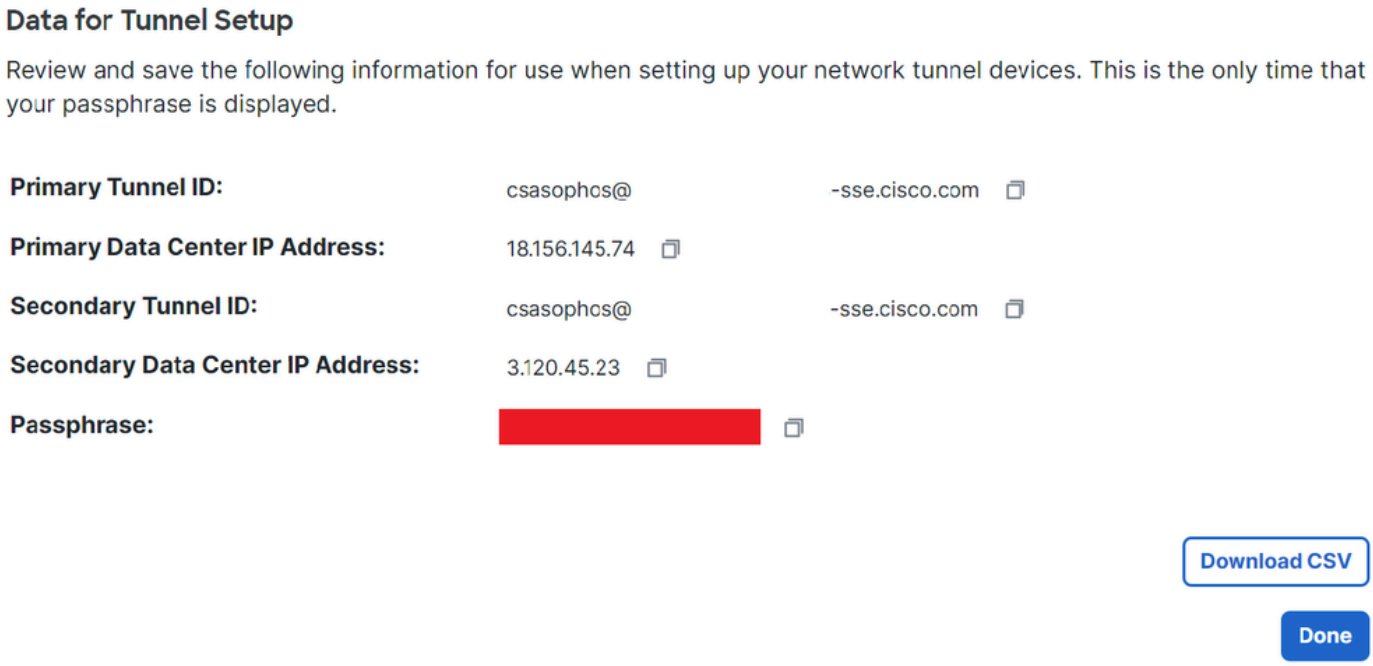
- Cliquez sur **Save**.



Accès sécurisé - Groupes de tunnels - Options de routage

Après avoir cliqué sur **Save** les informations sur le tunnel s'affiche, veuillez enregistrer ces informations pour l'étape suivante, **Configure the tunnel on Sophos**.

Données du tunnel



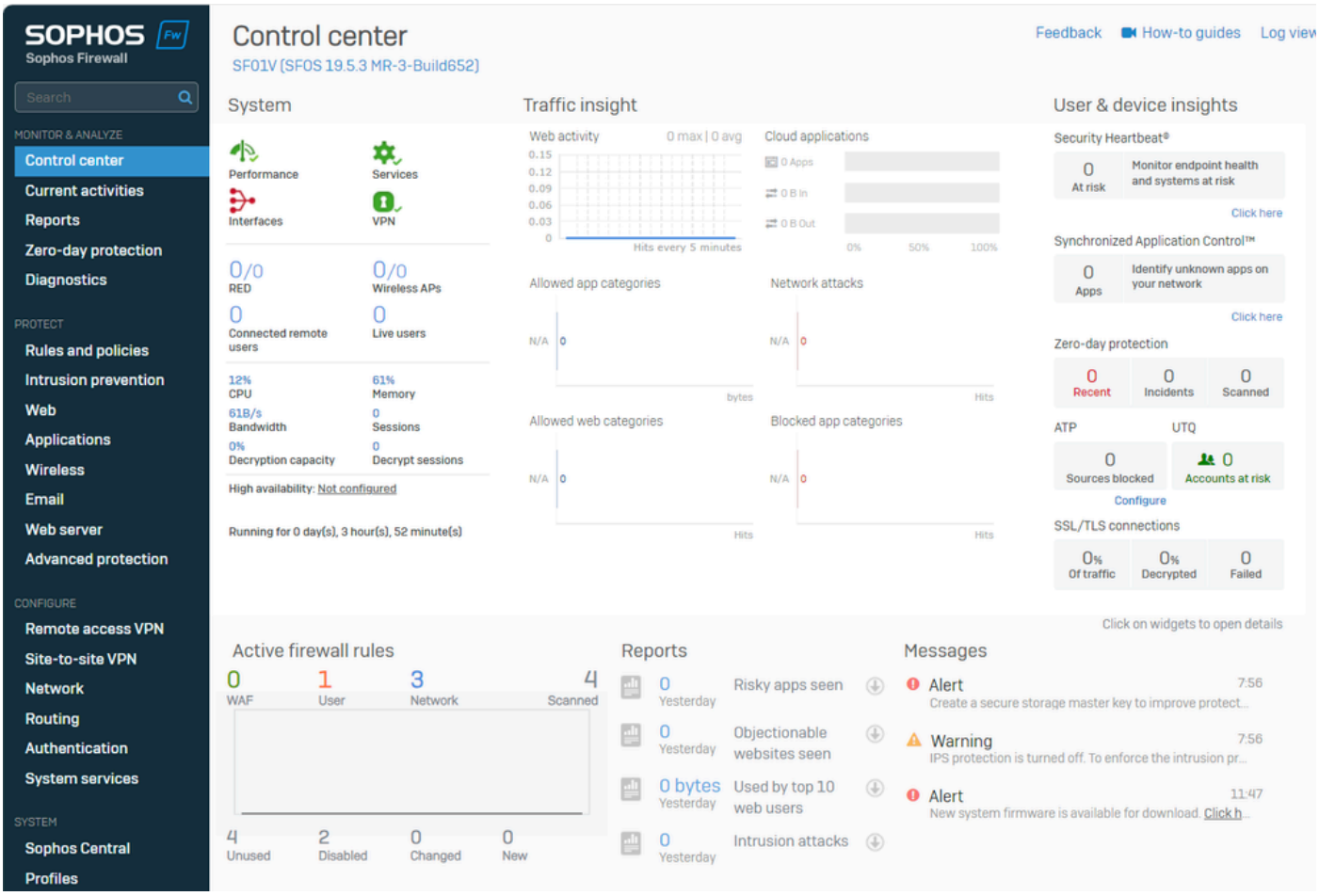
Accès sécurisé - Groupes de tunnels - Reprise de la configuration

Configuration du tunnel sur Sophos

Configurer le profil IPsec

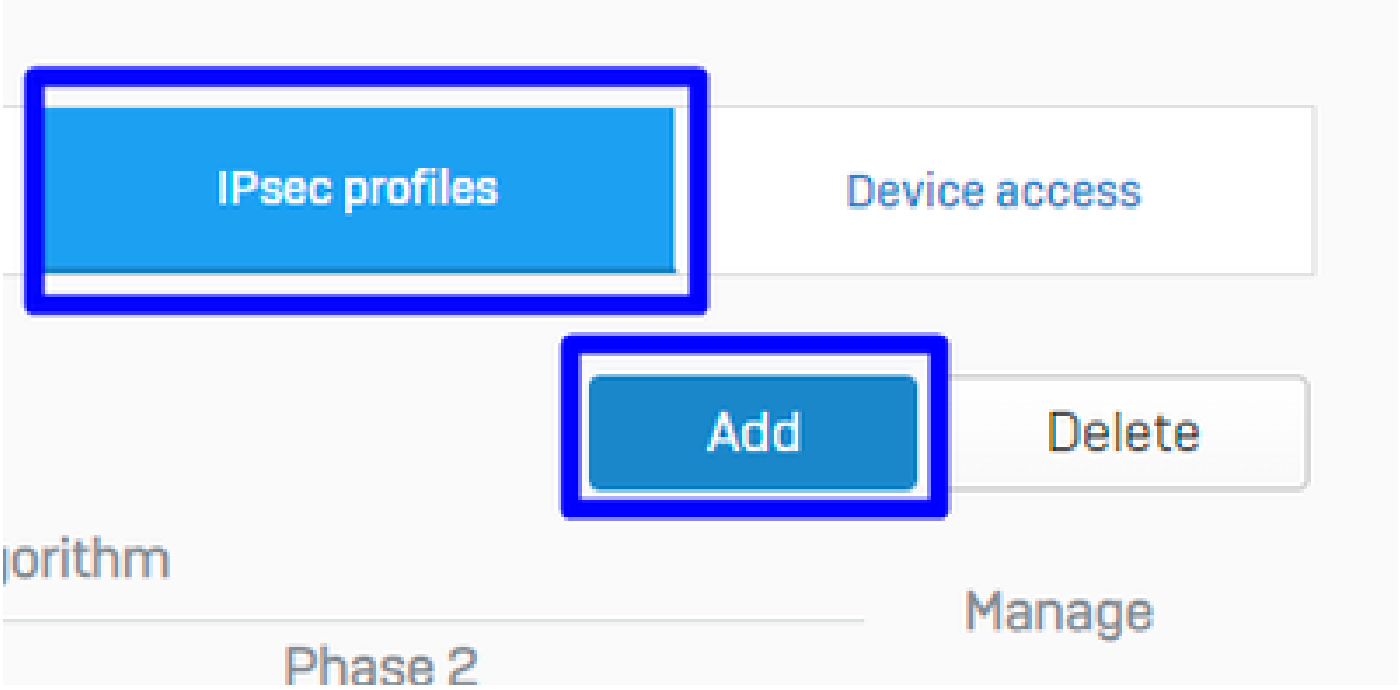
Afin de configurer le profil IPsec, naviguez jusqu'à votre pare-feu Sophos XG.

Vous obtenez quelque chose de semblable à ceci :



Sophos - Panneau d'administration

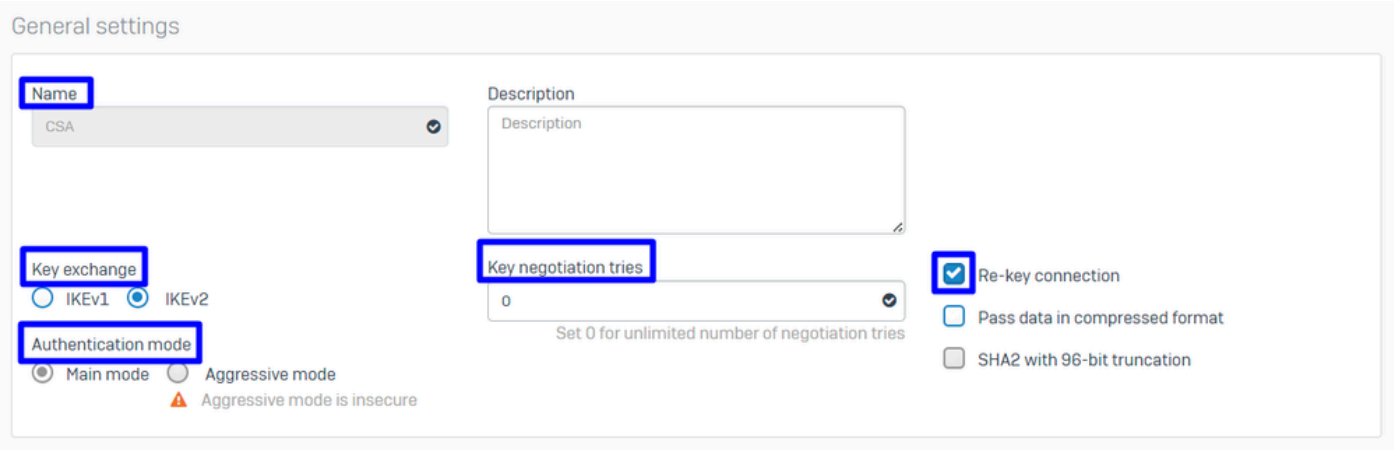
- Naviguez jusqu'à Profiles
- Cliquez sur **IPsec Profiles** et ensuite cliquez surAdd



Sophos - Profils IPsec

Sous **General Settings** configure :

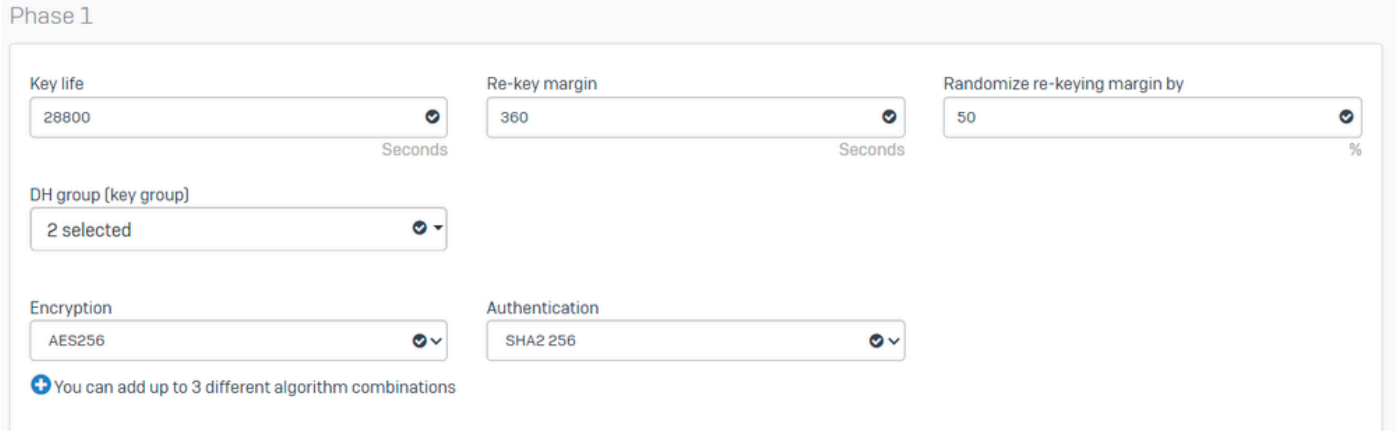
- **Name**: nom de référence à la politique d'accès sécurisé Cisco
- **Key Exchange**: IKEv2
- **Authentication Mode**:Mode principal
- **Key Negotiation Tries**:0
- **Re-Key connection**: cochez l'option



Sophos - Profils IPsec - Paramètres généraux

Sous **Phase 1** configure :

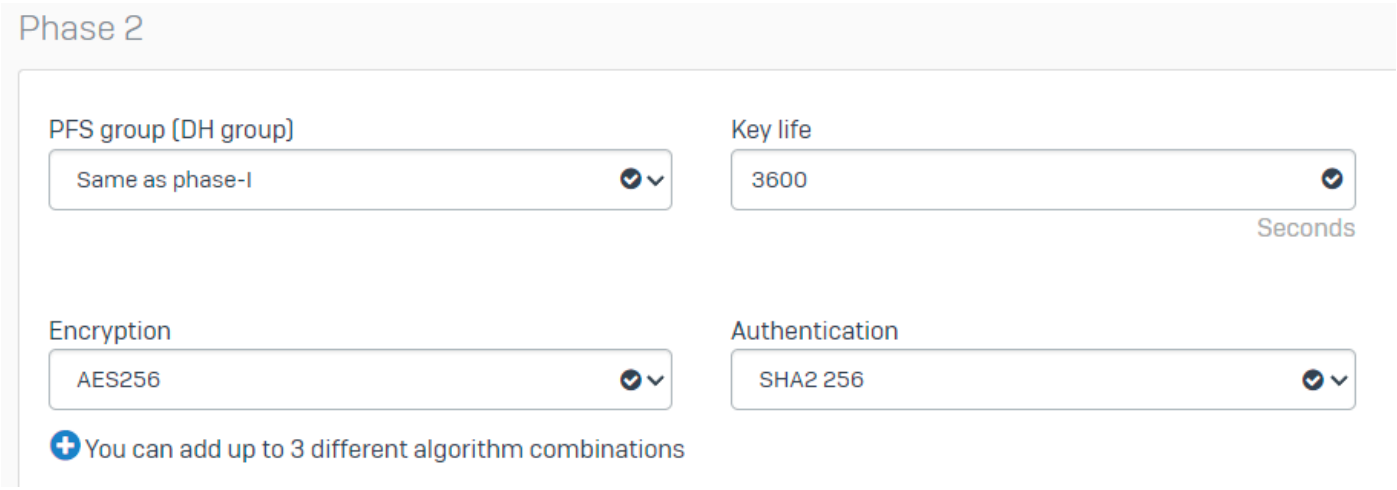
- **Key Life**:28800
- **DH group(key group)**: sélectionnez 19 et 20
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin:360 (Default)
- **Randomize re-keying margin by**:50 (Default)



Sophos - Profils IPsec - Phase 1

Sous **Phase 2** configure :

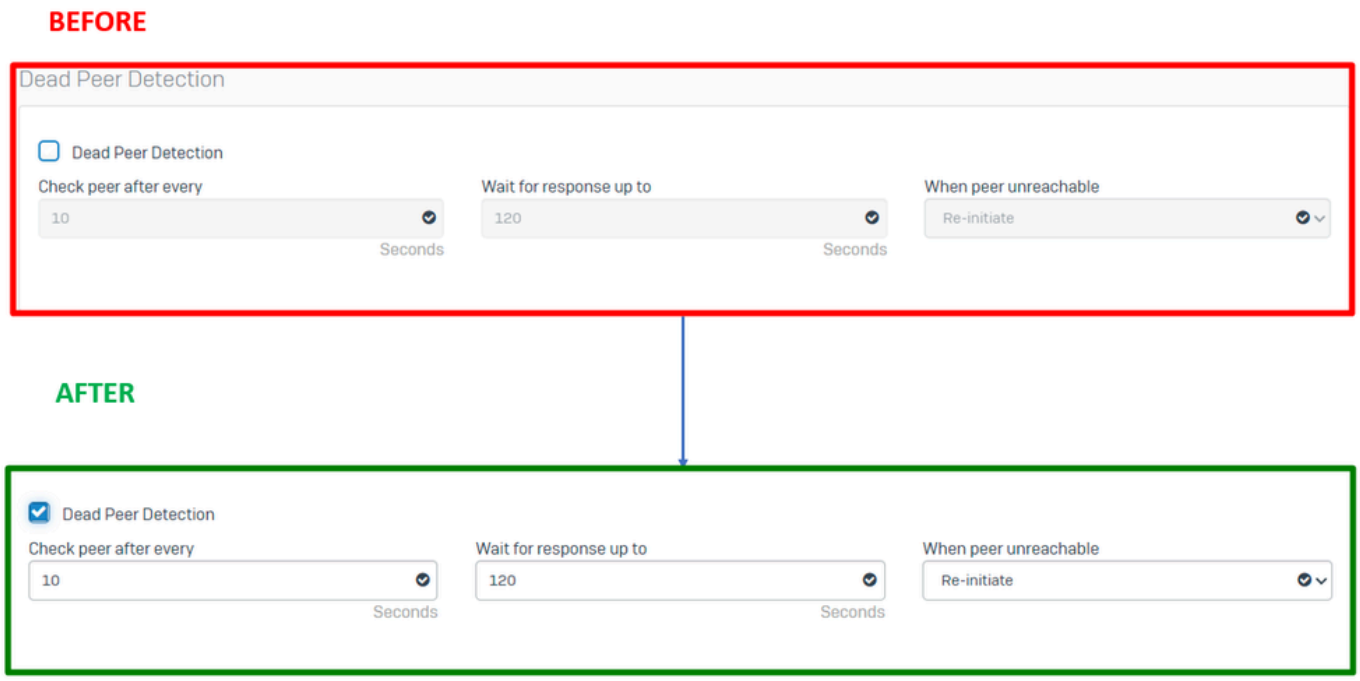
- PFS group (DH group): identique à la phase I
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256



Sophos - Profils IPsec - Phase 2

Sous **Dead Peer Detection** configure :

- **Dead Peer Detection**: cochez l'option
- **Check peer after every**:10
- **Wait for response up to**:120 (Default)
- **When peer unreachable**: relance (par défaut)

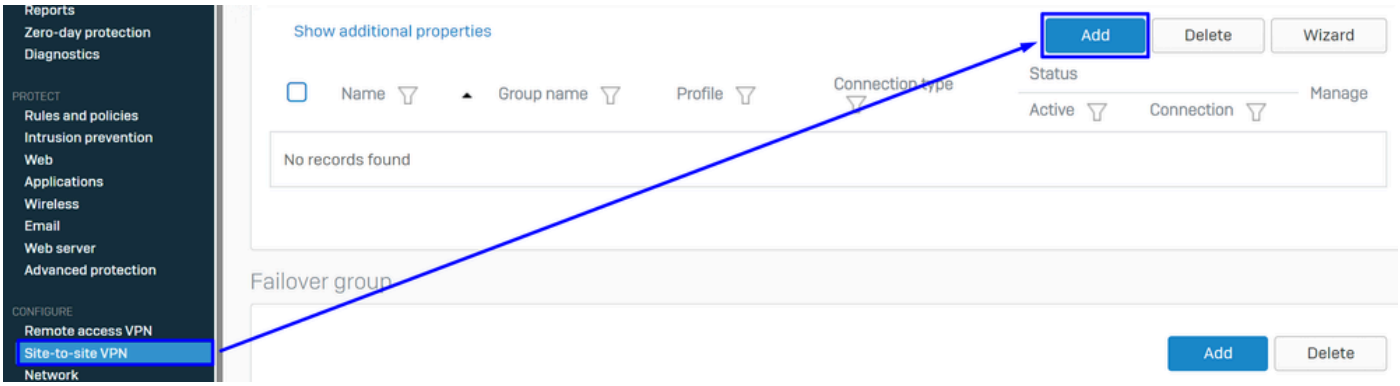


Sophos - Profils IPsec - Détection des homologues morts

Après cela, cliquez sur **Save** and proceed with the next step, Configure Site-to-site VPN.

Configuration d'un VPN site à site

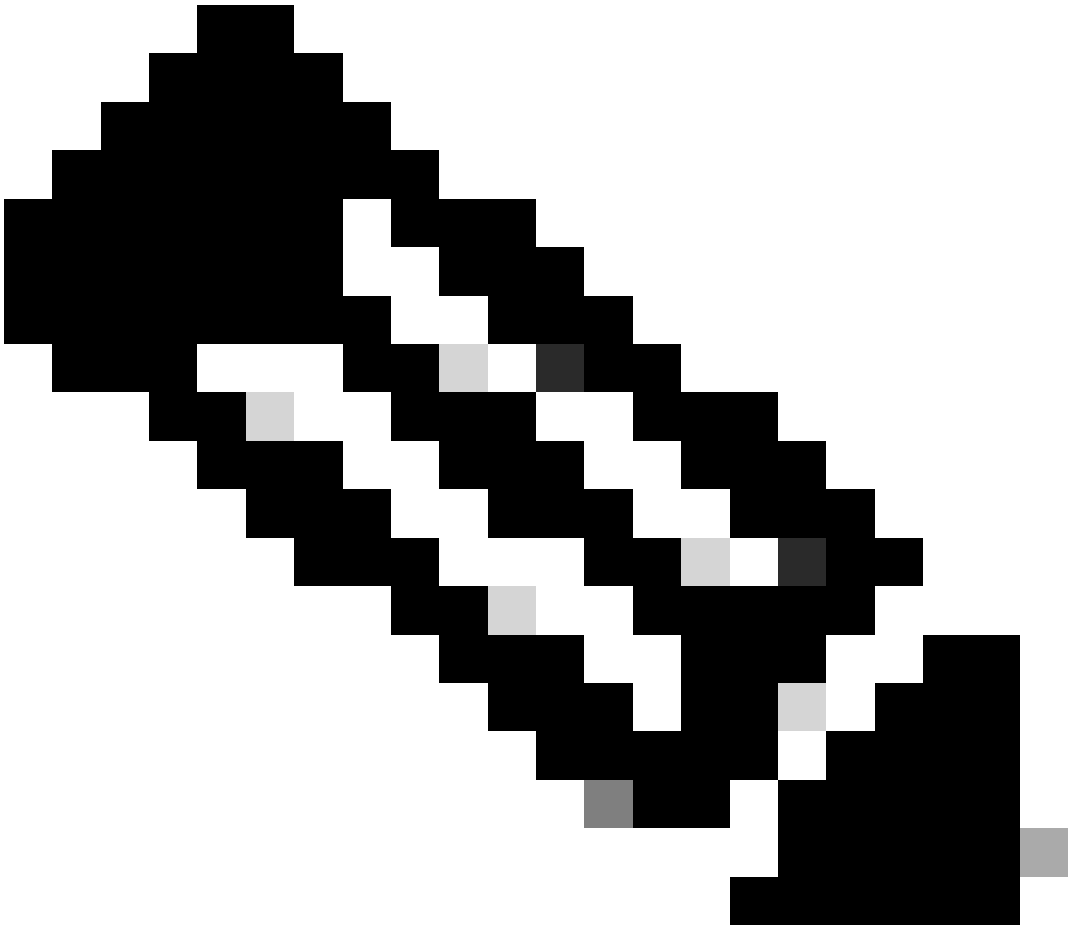
Pour lancer la configuration du VPN, cliquez sur on **Site-to-site VPN** et cliquez sur on **Add**.



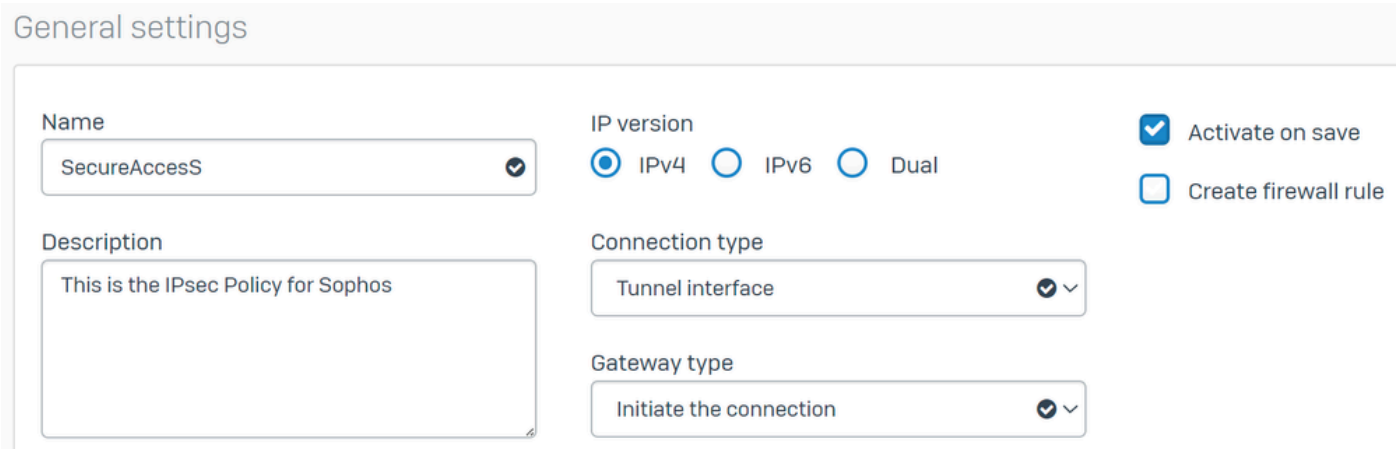
Sophos - VPN de site à site

Sous **General Settings** configure :

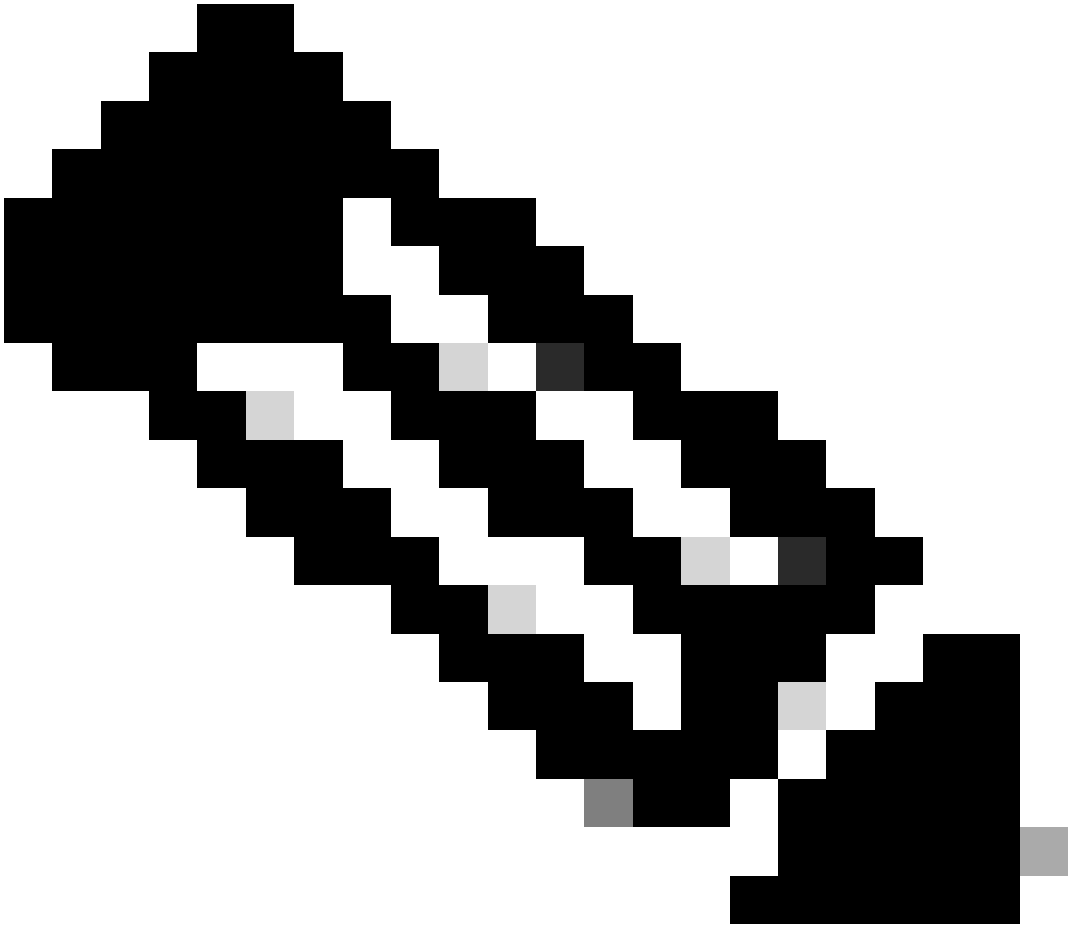
- **Name**: nom de référence à la stratégie IPsec d'accès sécurisé Cisco
- IP version:IPv4
- Connection type: interface de tunnel
- Gateway type: initier la connexion
- Active on save: cochez l'option



Remarque : l'option **Active on save** active automatiquement le VPN une fois que vous avez fini par configurer le VPN site à site.



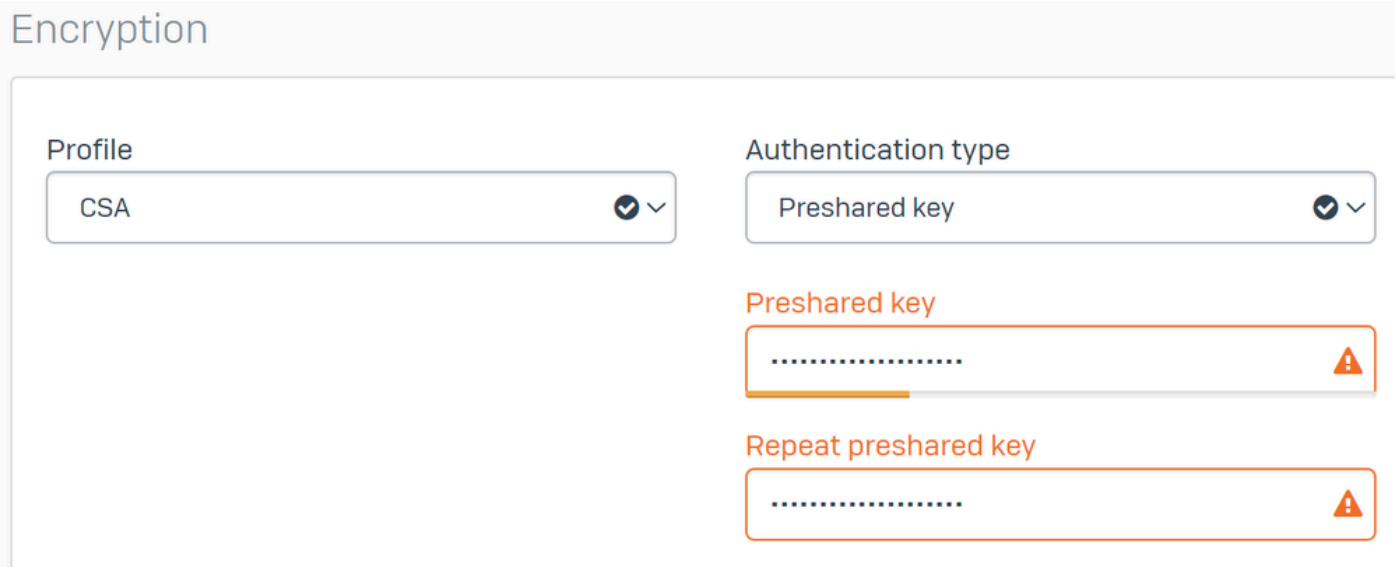
Sophos - VPN site à site - Paramètres généraux



Remarque : l'option Interface de tunnel crée une interface de tunnel virtuelle pour le pare-feu Sophos XG Firewall portant le nom XFRM.

Sous **Encryption** configure :

- **Profile**: le profil que vous créez sur l'étape, **Configure IPsec Profile**
- **Authentication type**: clé pré-partagée
- **Preshared key**: la clé que vous configurez à l'étape, Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**

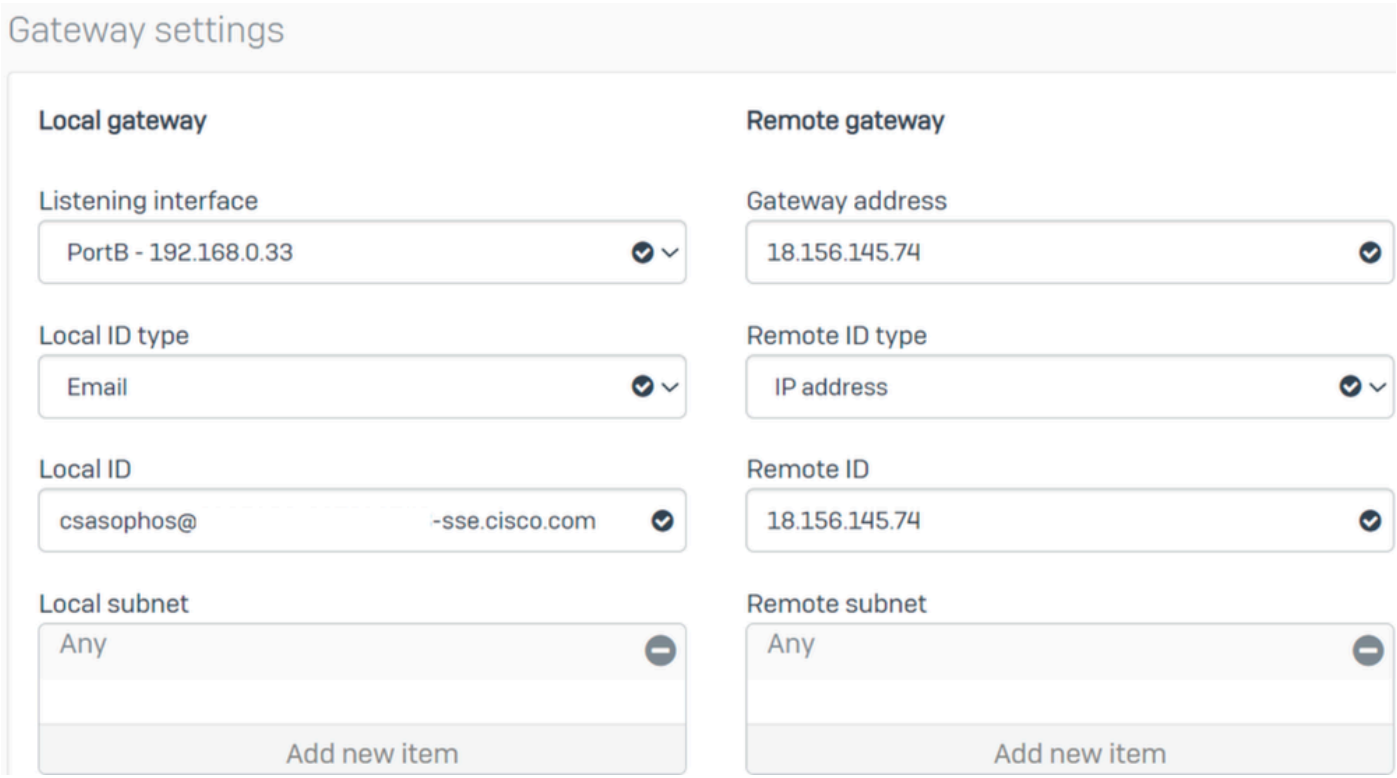


Sophos - VPN de site à site - Cryptage

Sous **Gateway Settings** configure Local Gateway et optionsRemote Gateway, utilisez ce tableau comme référence.

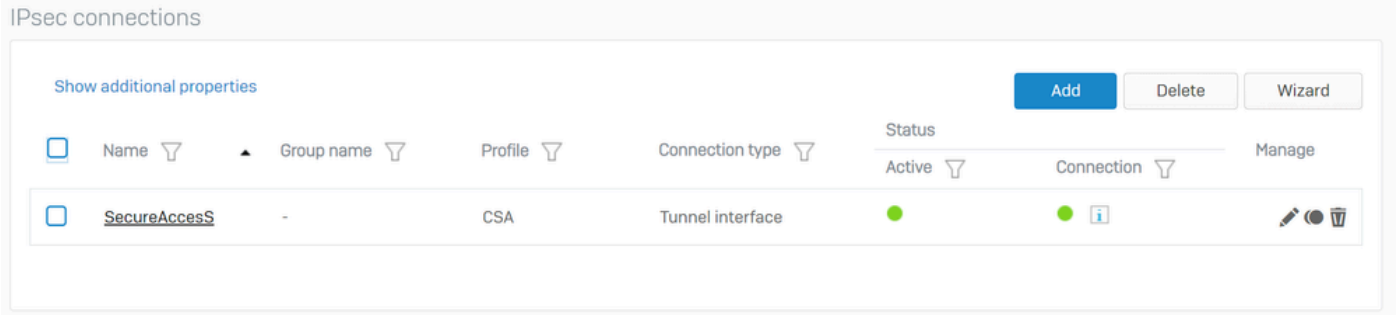
Passerelle locale	Passerelle distante
Interface d'écoute Votre Interface Wan-Internet	Adresse de passerelle L'adresse IP publique générée lors de l'étape, **Tunnel Data**
Type d'ID local Courriel	Type d'ID distant

	Adresse IP
ID local L'e-mail généré à l'étape, Tunnel Data	ID distant L'adresse IP publique générée lors de l'étape, Tunnel Data
Sous-réseau local tous les modèles	Sous-réseau distant tous les modèles

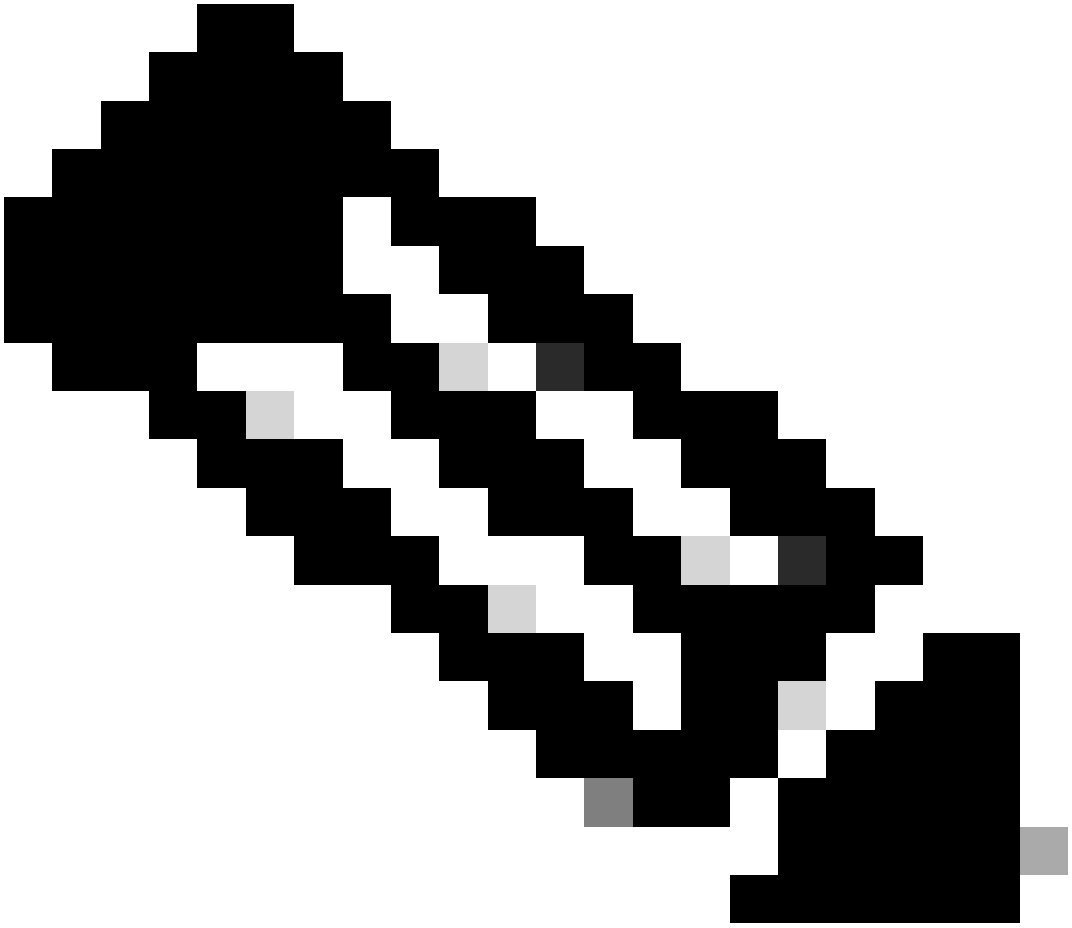


Sophos - VPN site à site - Paramètres de passerelle

Après cela, cliquez sur **Save**, et vous pouvez voir que le tunnel a été créé.

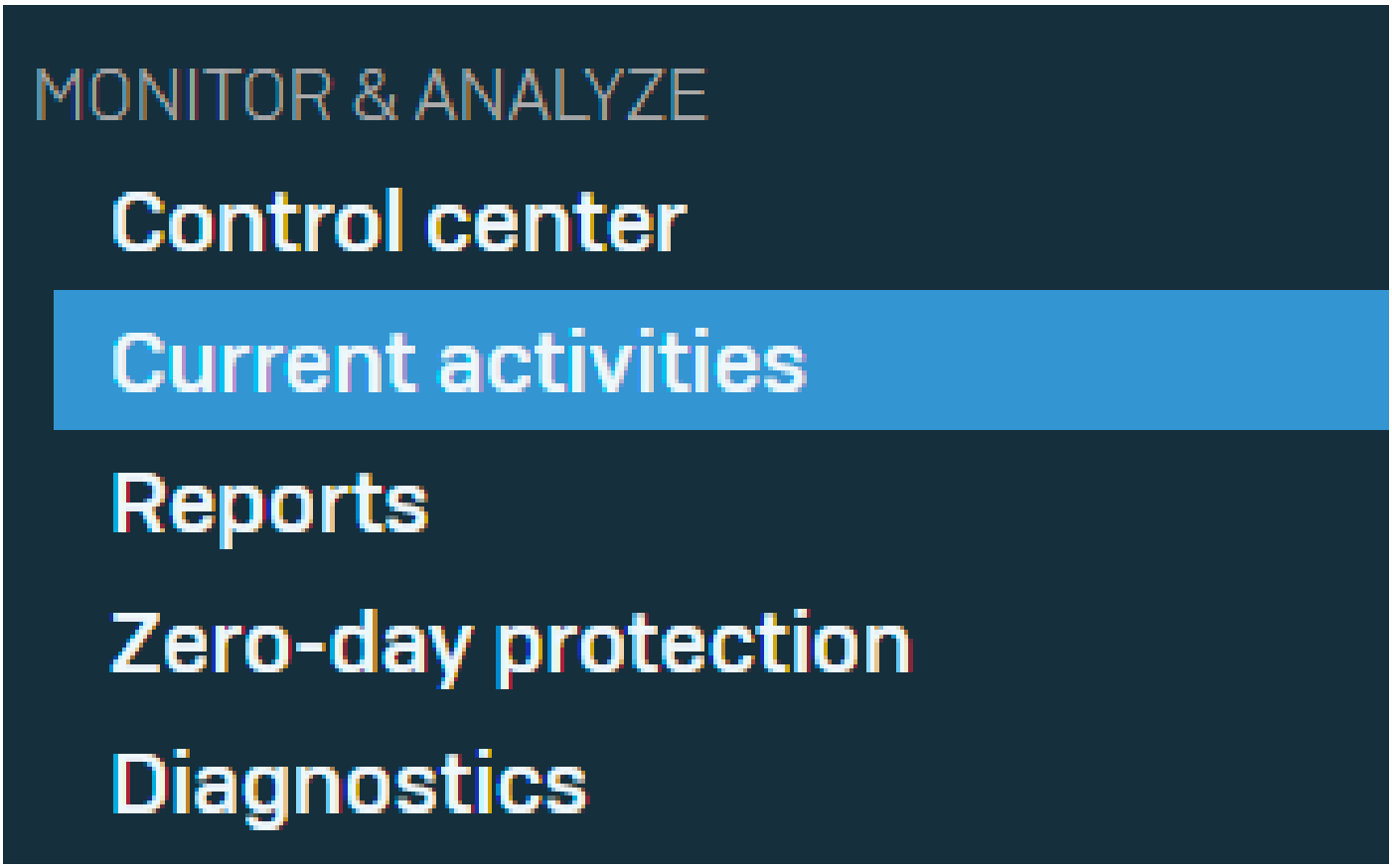


Sophos - VPN site à site - Connexions IPsec

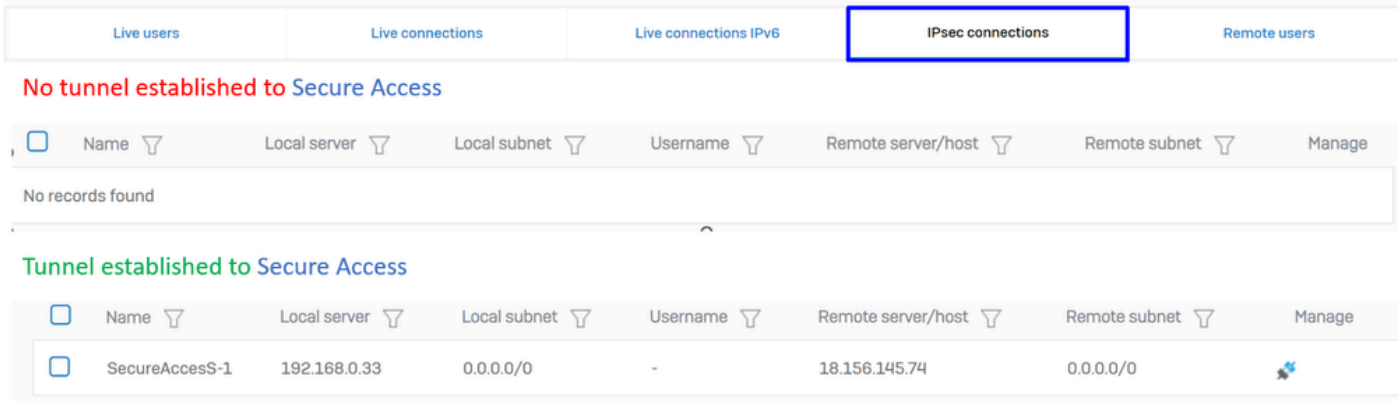


Remarque : Pour vérifier si le tunnel est correctement activé sur la dernière image, vous pouvez vérifier l'**Connection** état, s'il est vert, le tunnel est connecté s'il n'est pas vert et le tunnel n'est pas connecté.

Pour vérifier si un tunnel est établi, accédez à **Current Activities > IPsec Connections**.



Sophos - Surveillance et analyse - IPsec



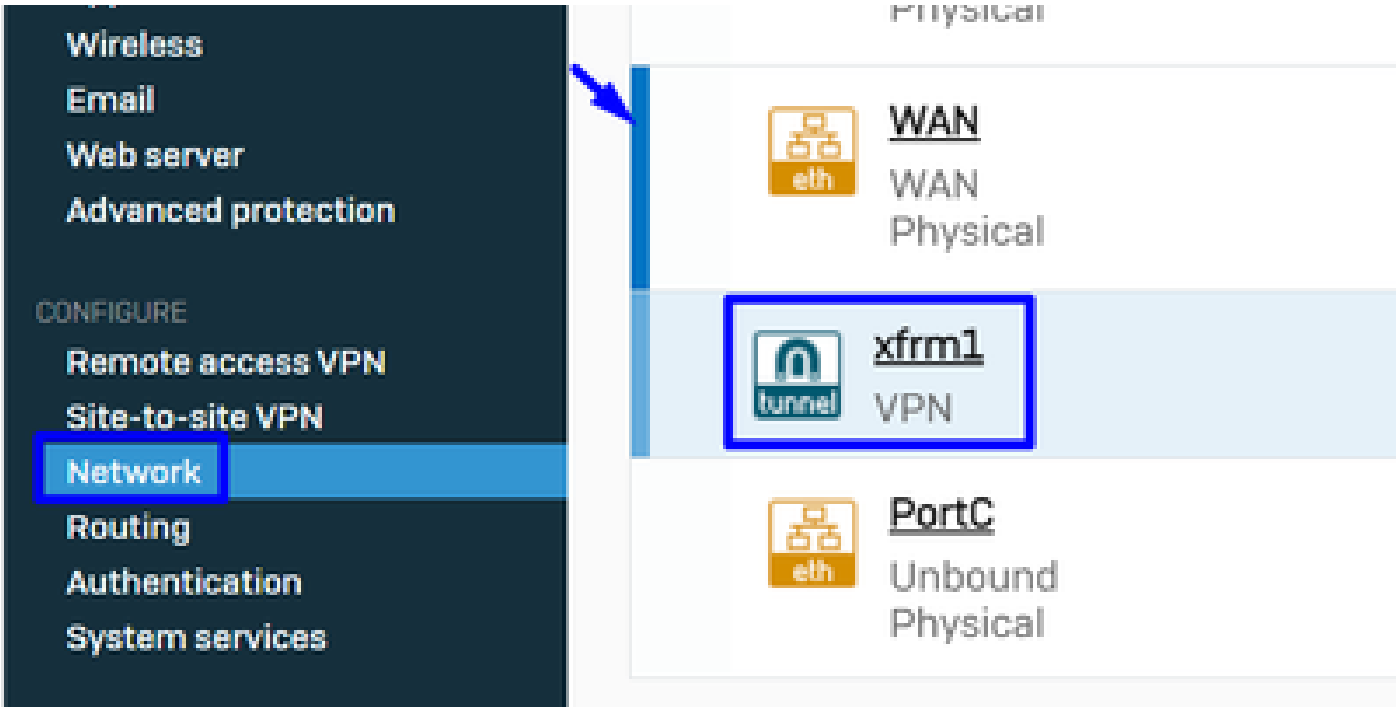
Sophos - Surveillance et analyse - IPsec avant et après

Après cela, nous pouvons continuer avec l'étape, **Configure Tunnel Interface Gateway**.

Configurer l'interface du tunnel

Accédez à **Network** et vérifiez votre WAN interface configurée sur le VPN pour modifier l'interface de tunnel virtuel avec le nom xfrm.

- Cliquez sur **xfrm** l'interface.



Sophos - Réseau - Interface de tunnel

- Configurez l'interface avec une adresse IP non routable dans votre réseau. Par exemple, vous pouvez utiliser 169.254.x.x/30, qui est une adresse IP dans un espace non routable. Dans notre exemple, nous utilisons 169.254.0.1/30

Sophos - Réseau - Interface de tunnel - Configuration

Configuration des passerelles

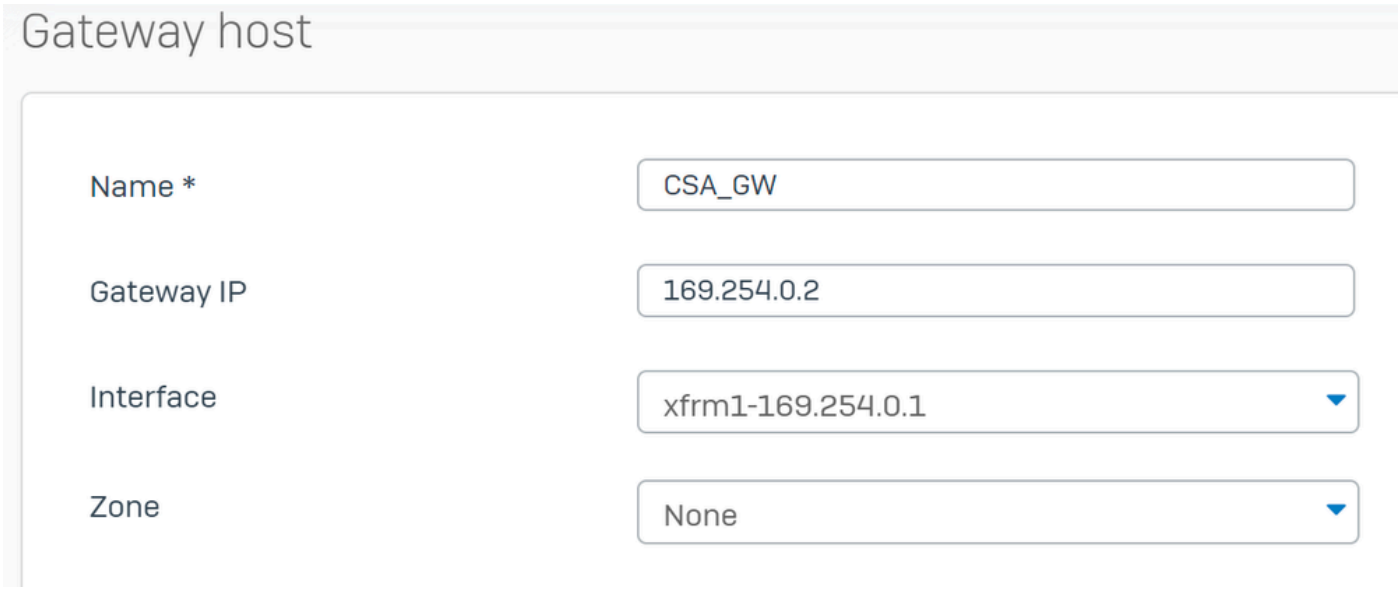
Afin de configurer la passerelle pour l'interface virtuelle (xfrm)

- Naviguez jusqu'à Routing > Gateways
- Cliquer Add

Sophos - Routage - Passerelles

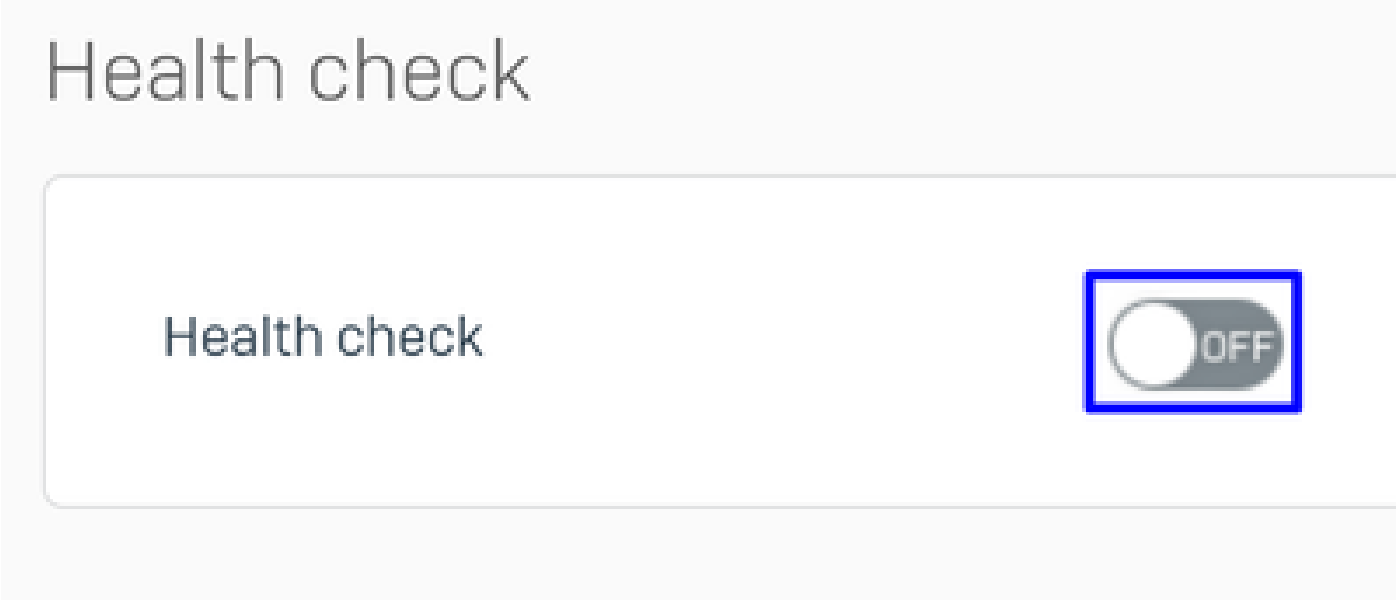
Sous **Gateway host** configure :

- **Name**: nom faisant référence à l'interface virtuelle créée pour le VPN
- **Gateway IP**: dans notre cas 169.254.0.2, il s'agit de l'adresse IP sous le réseau 169.254.0.1/30 que nous avons déjà attribuée à l'étape, Configure Tunnel Interface
- Interface: interface virtuelle VPN
- **Zone**: Aucun (par défaut)



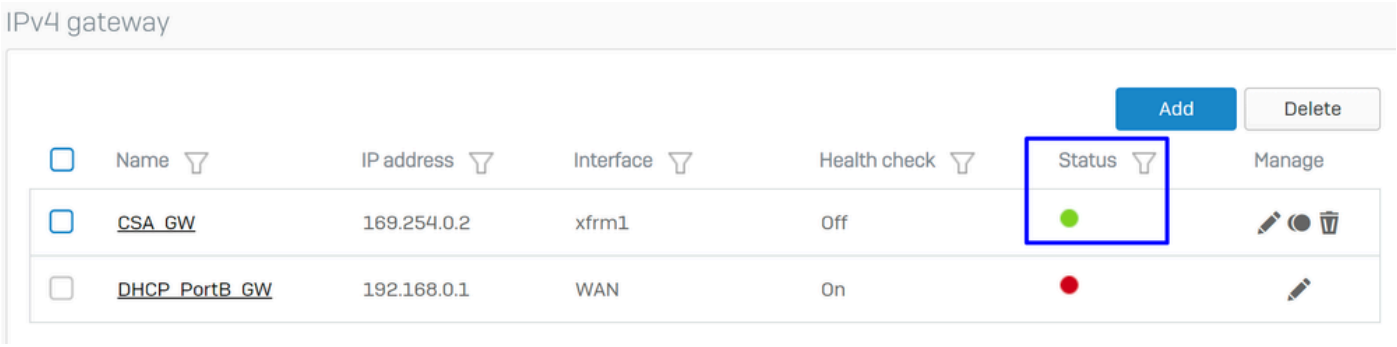
Sophos - Routage - Passerelles - Hôte de passerelle

- Sous **Health check** désactiver la vérification
- Cliquer **Save**



Sophos - Routage - Passerelles - Contrôle d'intégrité

Vous pouvez observer l'état de la passerelle après avoir enregistré la configuration :



Sophos - Routage - Passerelles - État

Configuration de la route SD-WAN

Pour finaliser le processus de configuration, vous devez créer la route qui vous permet de transférer le trafic vers Secure Access.

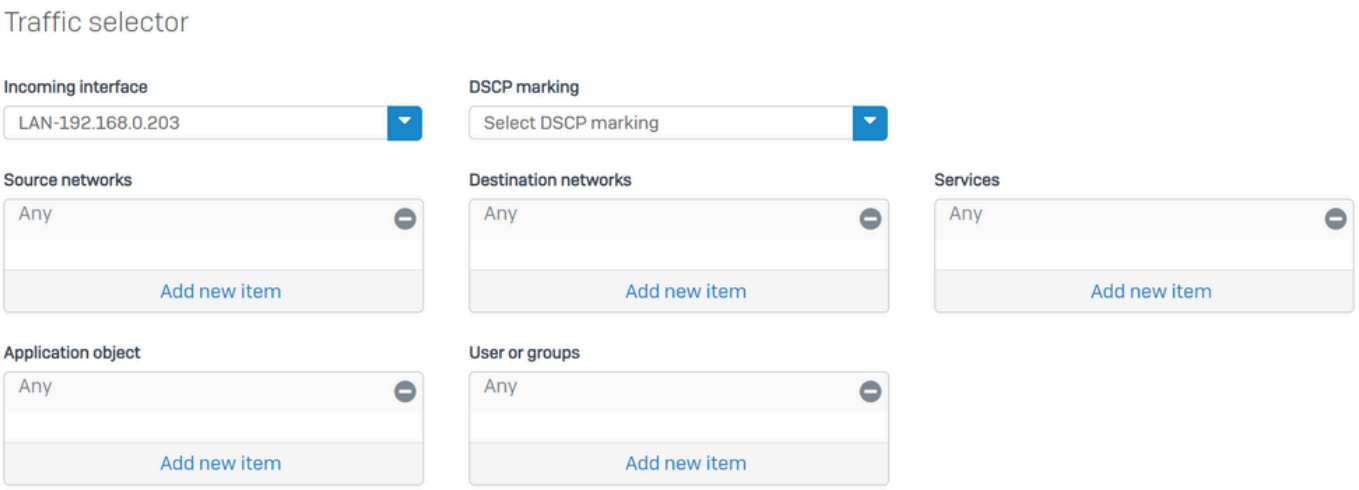
Naviguez jusqu'à **Routing > SD-WAN routes.**

- Cliquez sur **Add**

Sophos - Routes SD-Wan

Sous **Traffic Selector** configure :

- Incoming interface: sélectionnez l'interface à partir de laquelle vous souhaitez envoyer le trafic ou les utilisateurs qui accèdent à partir de RA-VPN, ZTNA ou Clientless-ZTNA
- DSCP marking: rien pour cet exemple
- **Source networks**: sélectionnez l'adresse que vous souhaitez router via le tunnel
- **Destination networks**: Tout ou vous pouvez spécifier une destination
- **Services**: Tout ou vous pouvez spécifier les services
- **Application object**: une application si l'objet est configuré
- User or groups: si vous souhaitez ajouter un groupe spécifique d'utilisateurs pour acheminer le trafic vers l'accès sécurisé

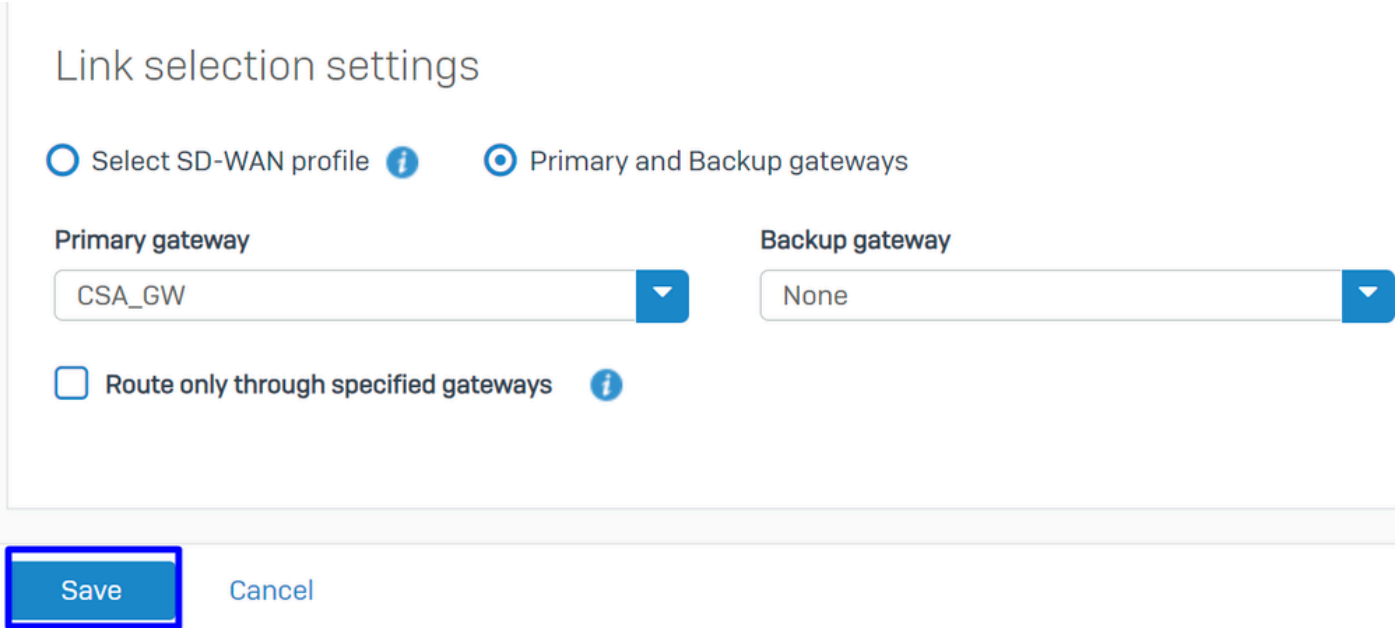


Sophos - Routes SD-Wan - Sélecteur de trafic

Sous **Link selection settings** configure the gateway :

- Primary and Backup gateways: cochez l'option

- **Primary gateway**: sélectionnez la passerelle configurée à l'étape, Configure the Gateways
- Cliquez sur **Save**



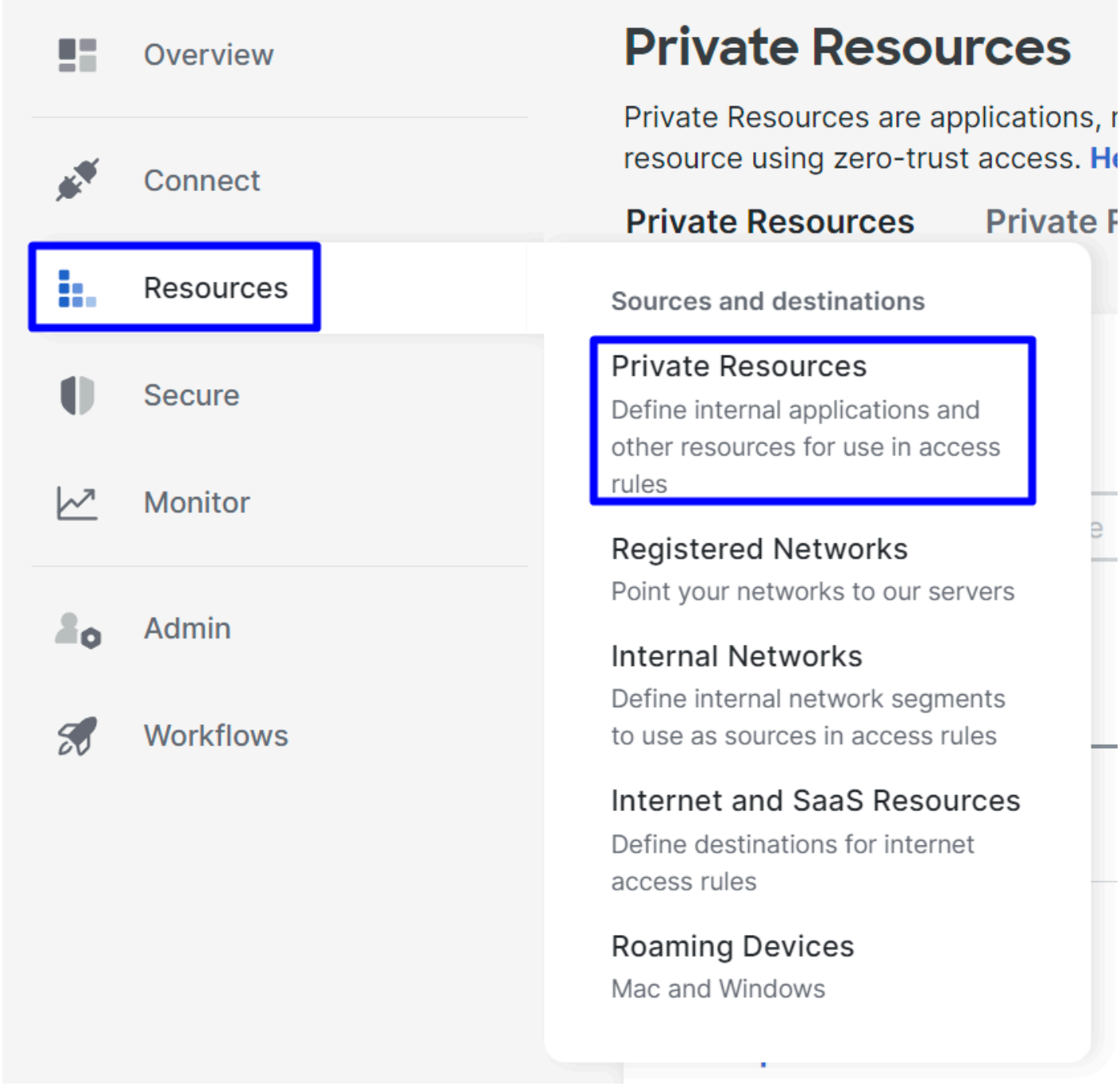
Sophos - Routes SD-Wan - Sélecteur de trafic - Passerelles principale et de secours

Après avoir finalisé la configuration du pare-feu Sophos XG, vous pouvez passer à l'étape suivante : **Configure Private App.**

Configurer une application privée

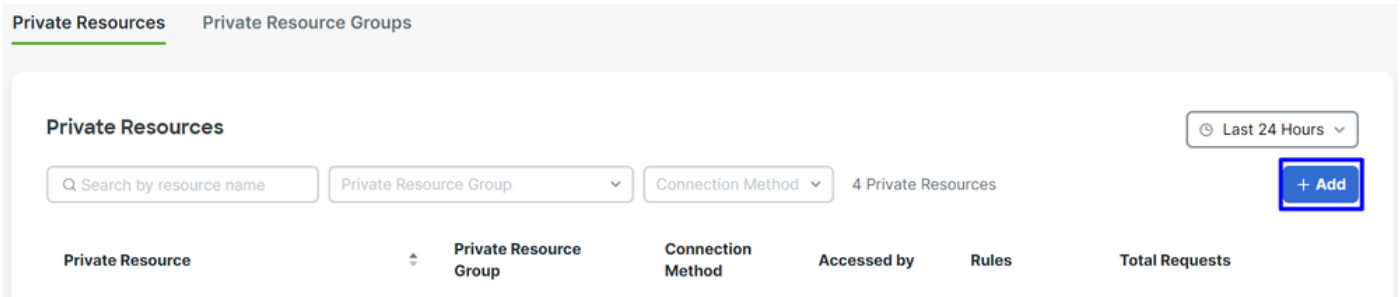
Afin de configurer l'accès à l'application privée, connectez-vous au portail Admin.

- Naviguez jusqu'à **Resources > Private Resources**



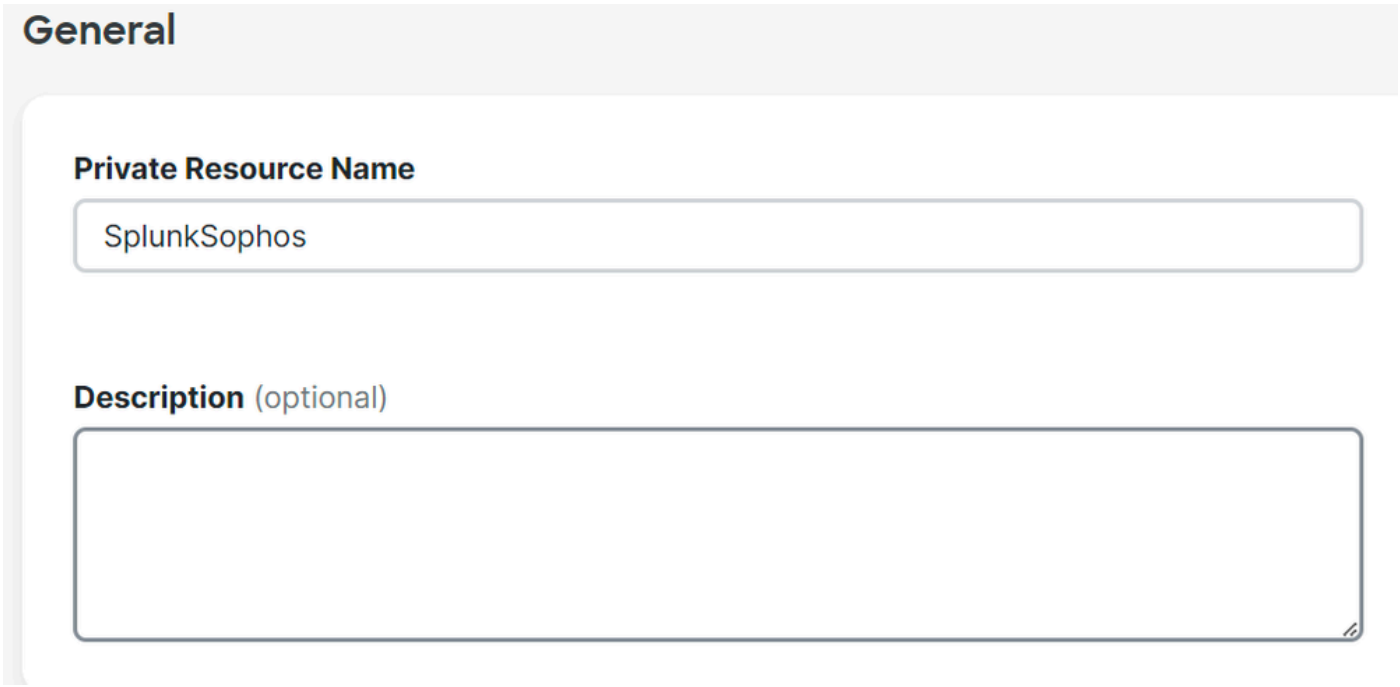
Accès sécurisé - Ressources privées

- Cliquez sur + Add



Accès sécurisé - Ressources privées 2

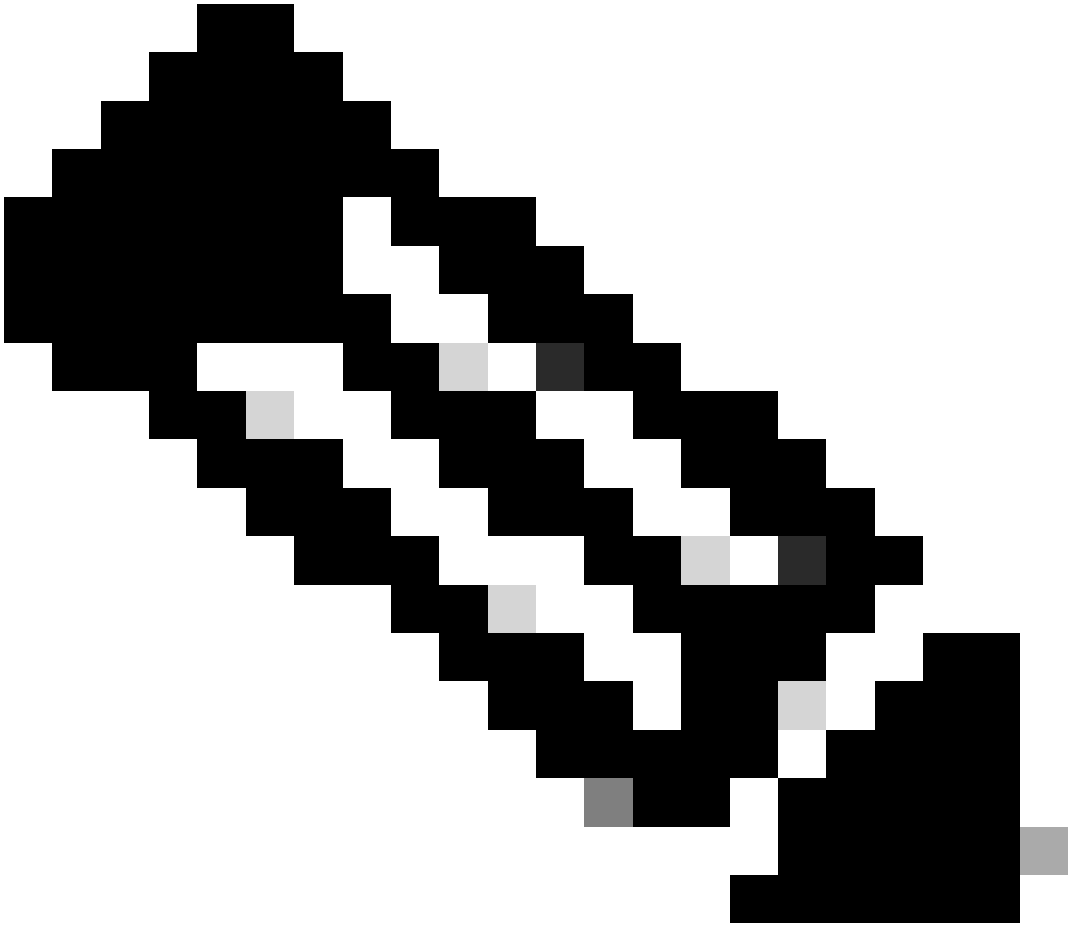
- Sous **General** Configurer le **Private Resource Name**



Accès sécurisé - Ressources privées - Général

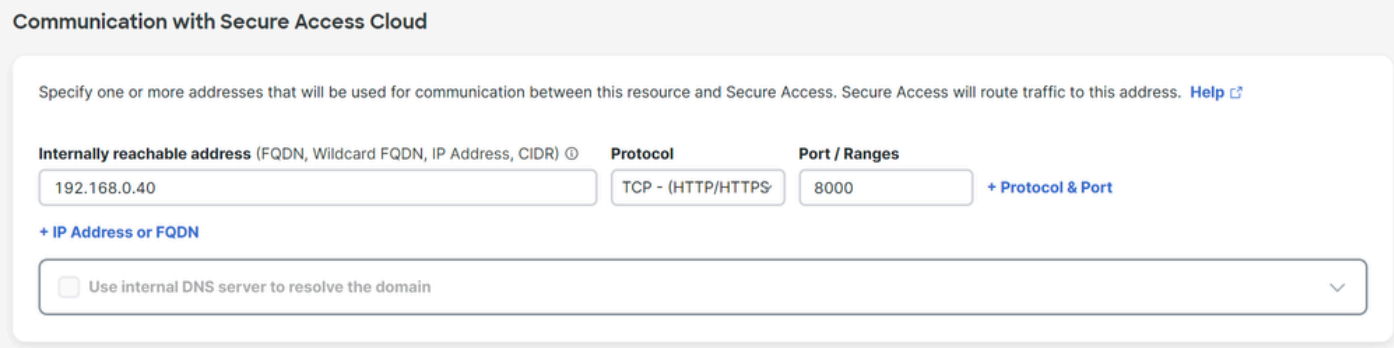
Sous **Communication with Secure Access Cloud** configure :

- I**nternally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: sélectionnez la ressource à laquelle vous souhaitez accéder



Remarque : n'oubliez pas que l'adresse accessible en interne a été attribuée à l'étape **Configure the Tunnel on Secure Access**.

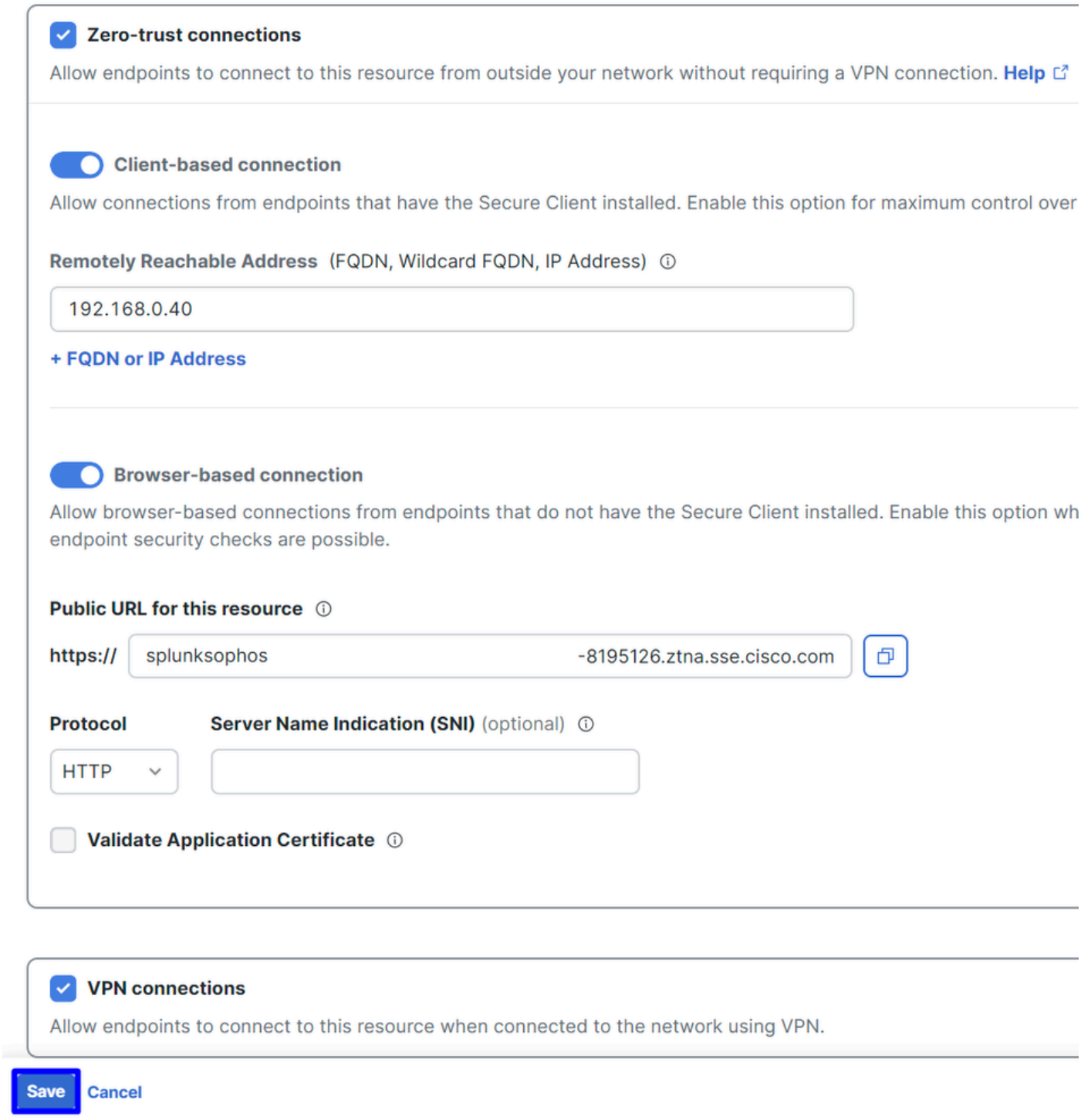
- **Protocol**: sélectionnez le protocole utilisé pour accéder à cette ressource
- Port / Ranges : sélectionnez les ports à activer pour accéder à l'application



Accès sécurisé - Ressources privées - Communications avec le cloud d'accès sécurisé

Dans **Endpoint Connection Methods**, vous configurez toutes les méthodes possibles pour accéder aux ressources privées via l'accès sécurisé et choisissez les méthodes que vous souhaitez utiliser pour votre environnement :

- **Zero-trust connections**: cochez la case pour activer l'accès ZTNA.
    - **Client-based connection**: Activer le bouton pour autoriser le ZTNA client
        - **Remotely Reachable Address**: configurez l'adresse IP de votre application privée
    - **Browser-based connection**: activez le bouton pour autoriser le ZTNA basé sur le navigateur
        - Public URL for this resource: ajoutez un nom à utiliser en association avec le domaine ztna.sse.cisco.com
            - Protocol: sélectionnez HTTP ou HTTPS comme protocole d'accès via le navigateur
    - **VPN connections**: cochez la case pour activer l'accès RA-VPN.
- Cliquer **Save**



Accès sécurisé - Ressources privées - Communications avec accès sécurisé Cloud 2

Une fois la configuration terminée, voici le résultat :

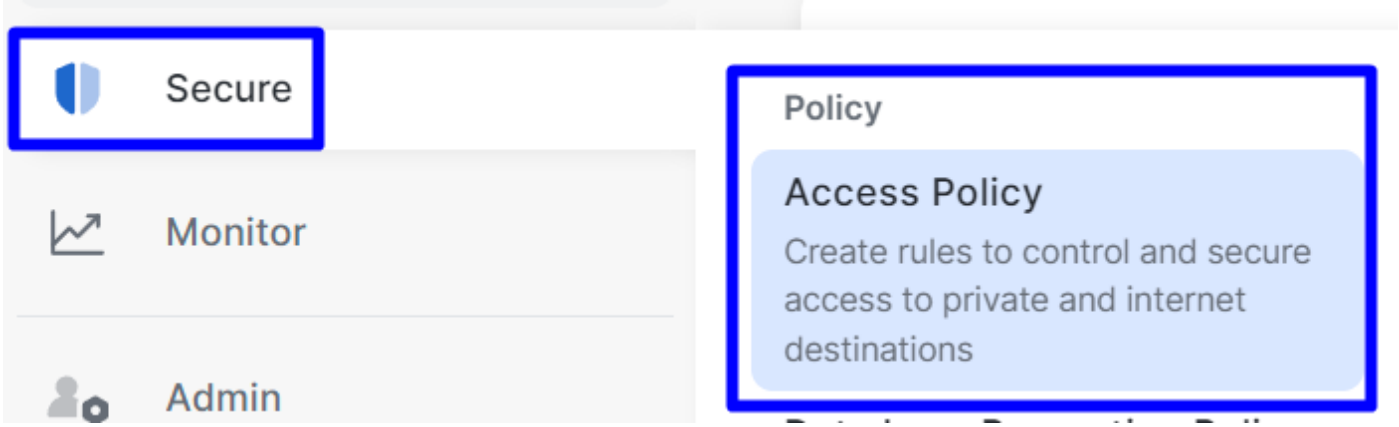
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	VPN Browser-based ZTNA Client-based ZTNA	1	2	16

Accès sécurisé : ressources privées configurées

Vous pouvez maintenant passer à l'étape **Configure the Access Policy**.

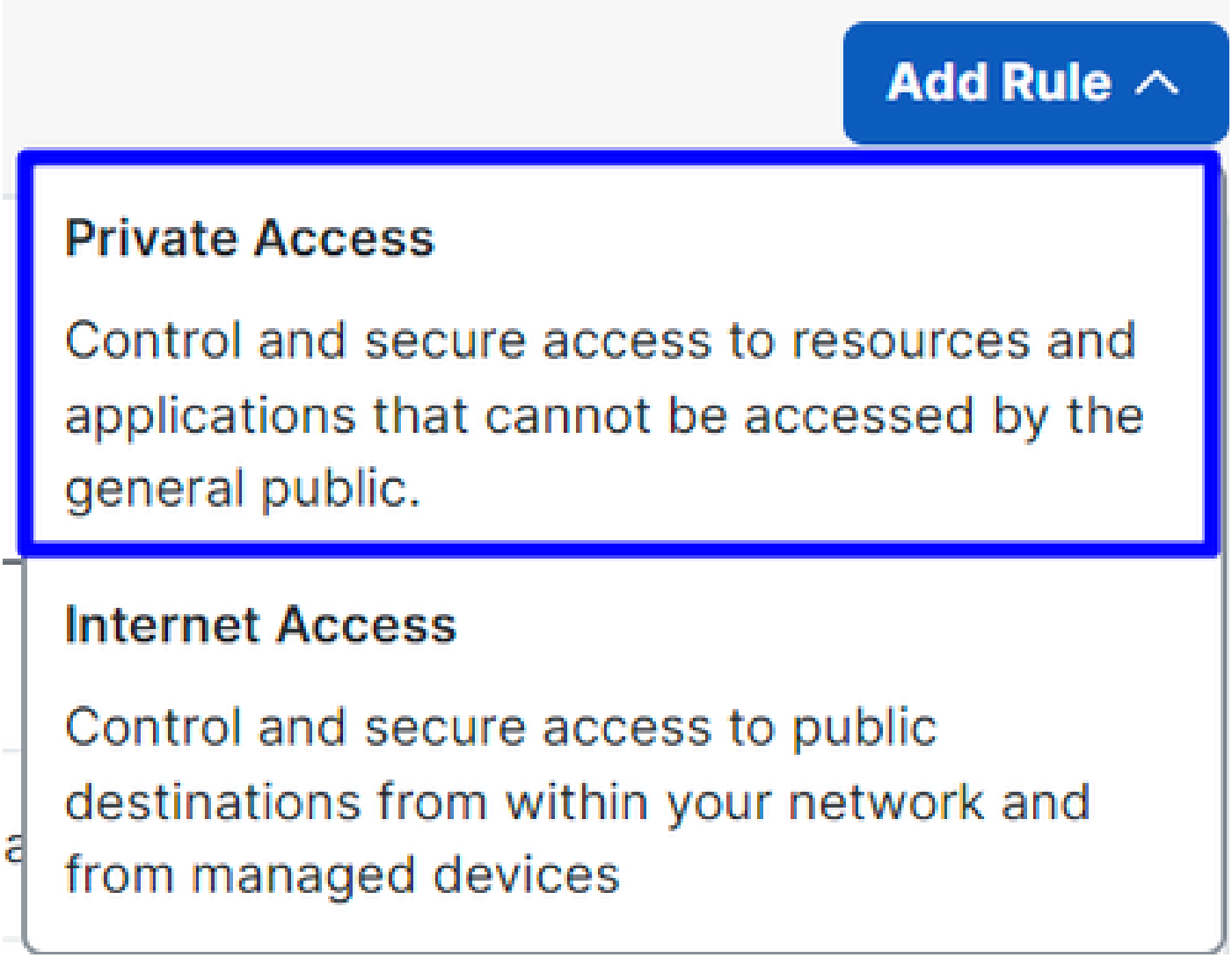
Configurer la stratégie d'accès

Pour configurer la stratégie d'accès, accédez à Secure > Access Policy.



Accès sécurisé - Politique d'accès

- Cliquer **Add Rule > Private Access**

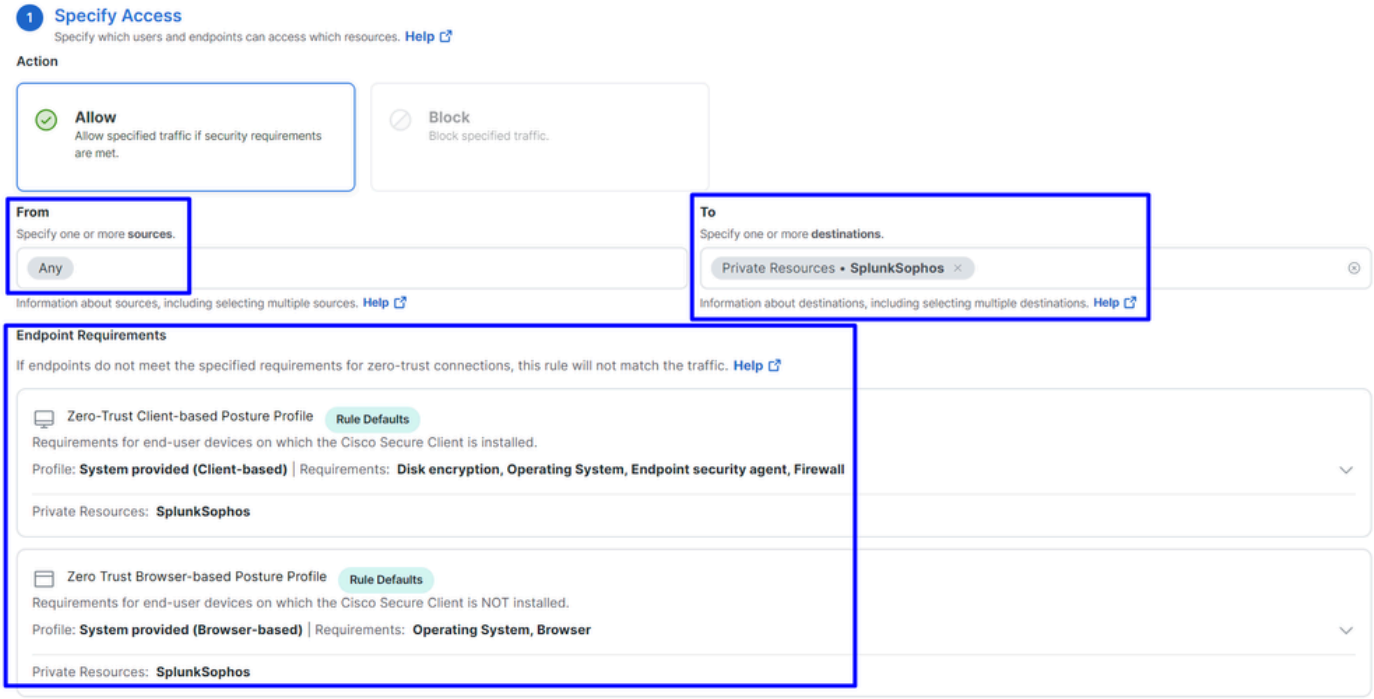


Accès sécurisé - Politique d'accès - Accès privé

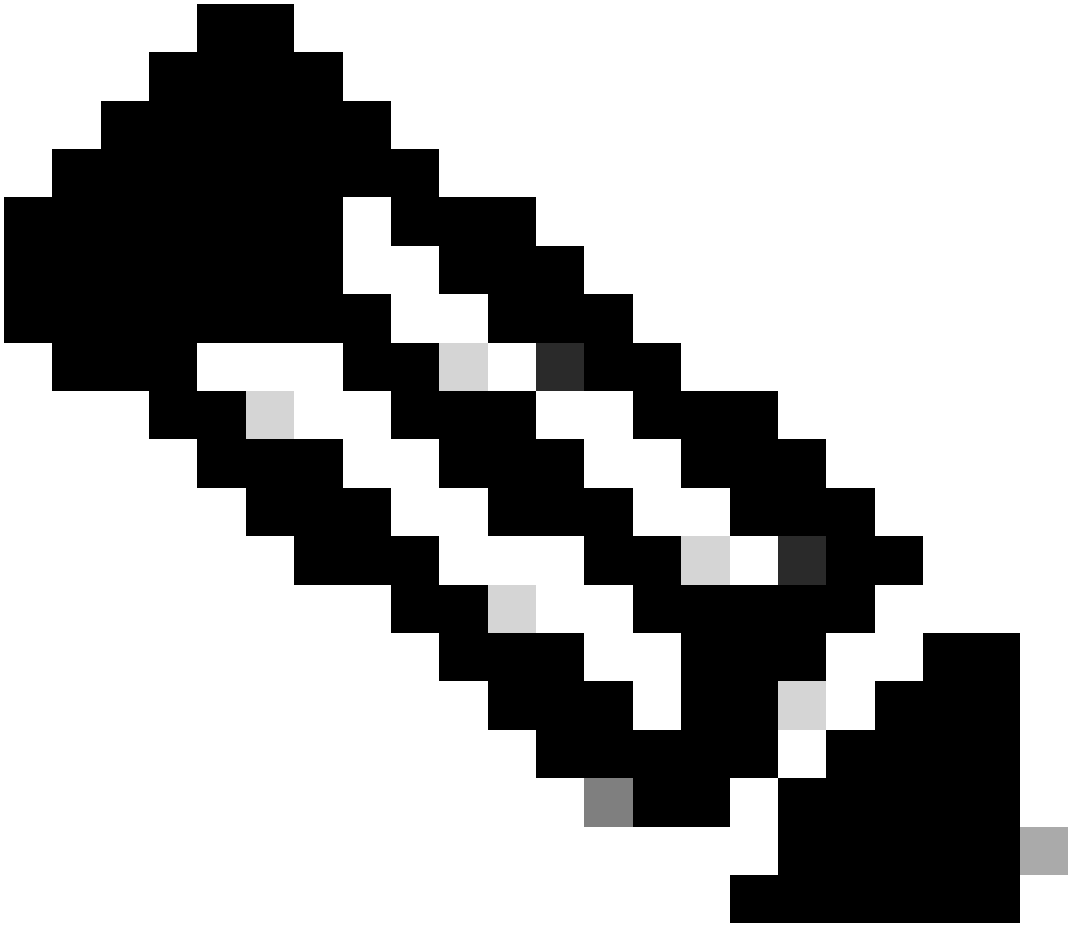
Configurez les options suivantes pour fournir un accès via plusieurs méthodes d'authentification :

- 1. Specify Access
    - Action:Allow
        - **Rule name**: spécifiez un nom pour votre règle d'accès
        - **From**: utilisateurs auxquels vous accordez l'accès
        - **To**: application à laquelle vous souhaitez autoriser l'accès
        - Endpoint Requirements: (par défaut)

- Cliquer **Next**



Accès sécurisé - Stratégie d'accès - Spécifier l'accès



Remarque : pour l'étape **2. Configure Security** si nécessaire, mais dans ce cas, vous n'avez pas activé le **Intrusion Prevention (IPS)**, ou **Tenant Control Profile**.

- Cliquez sur Save, et vous avez :

	#	Rule name	Access	Action	Sources	Destinations	Security	Status
	6	Splunksophos	Private	Allow	Any	SplunkSophos	-	

Accès sécurisé : stratégie d'accès configurée

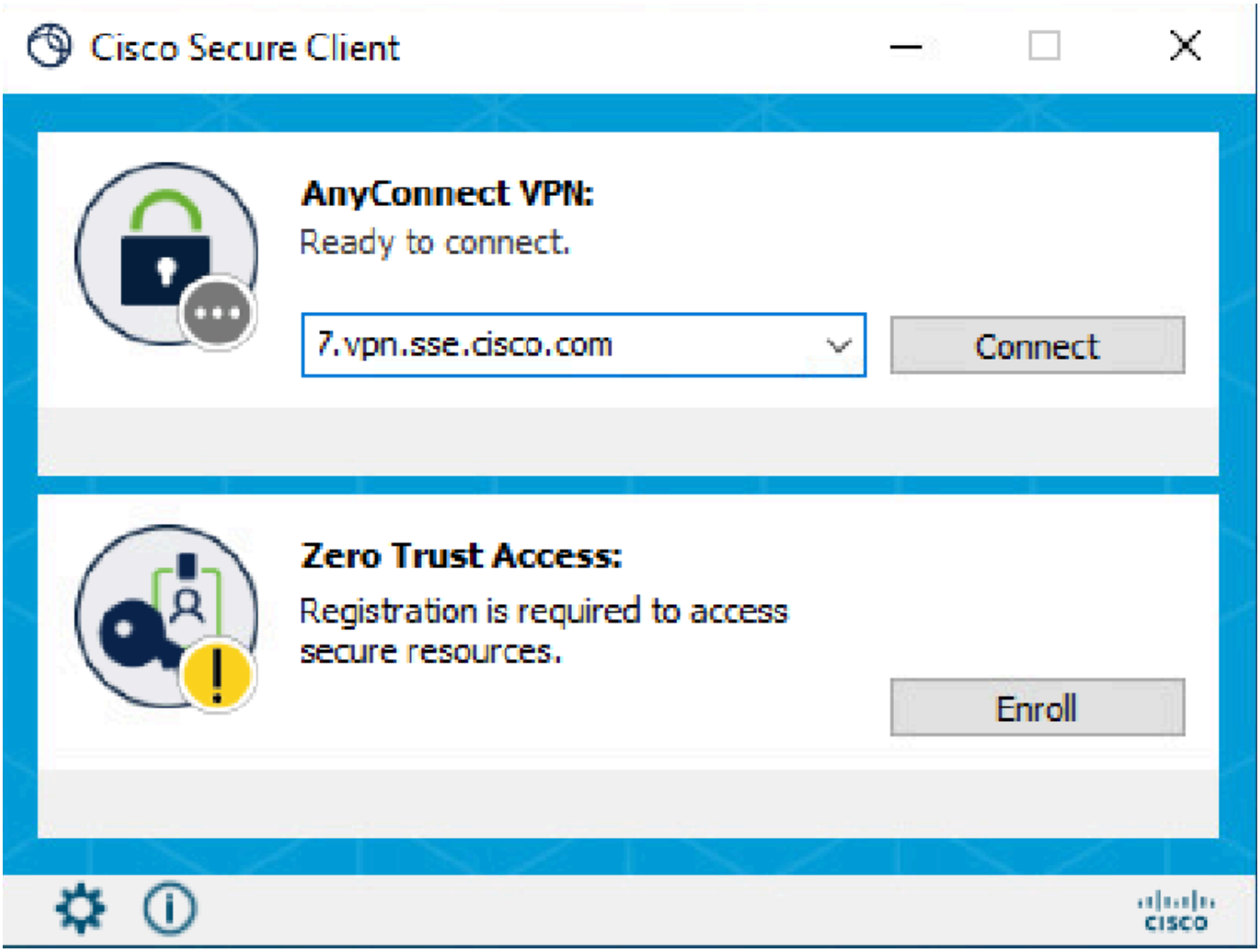
Ensuite, vous pouvez passer à l'étape Verify.

Vérifier

Afin de vérifier l'accès, vous devez avoir installé l'agent de Cisco Secure Client que vous pouvez télécharger à partir de Téléchargement de logiciel - Cisco Secure Client.

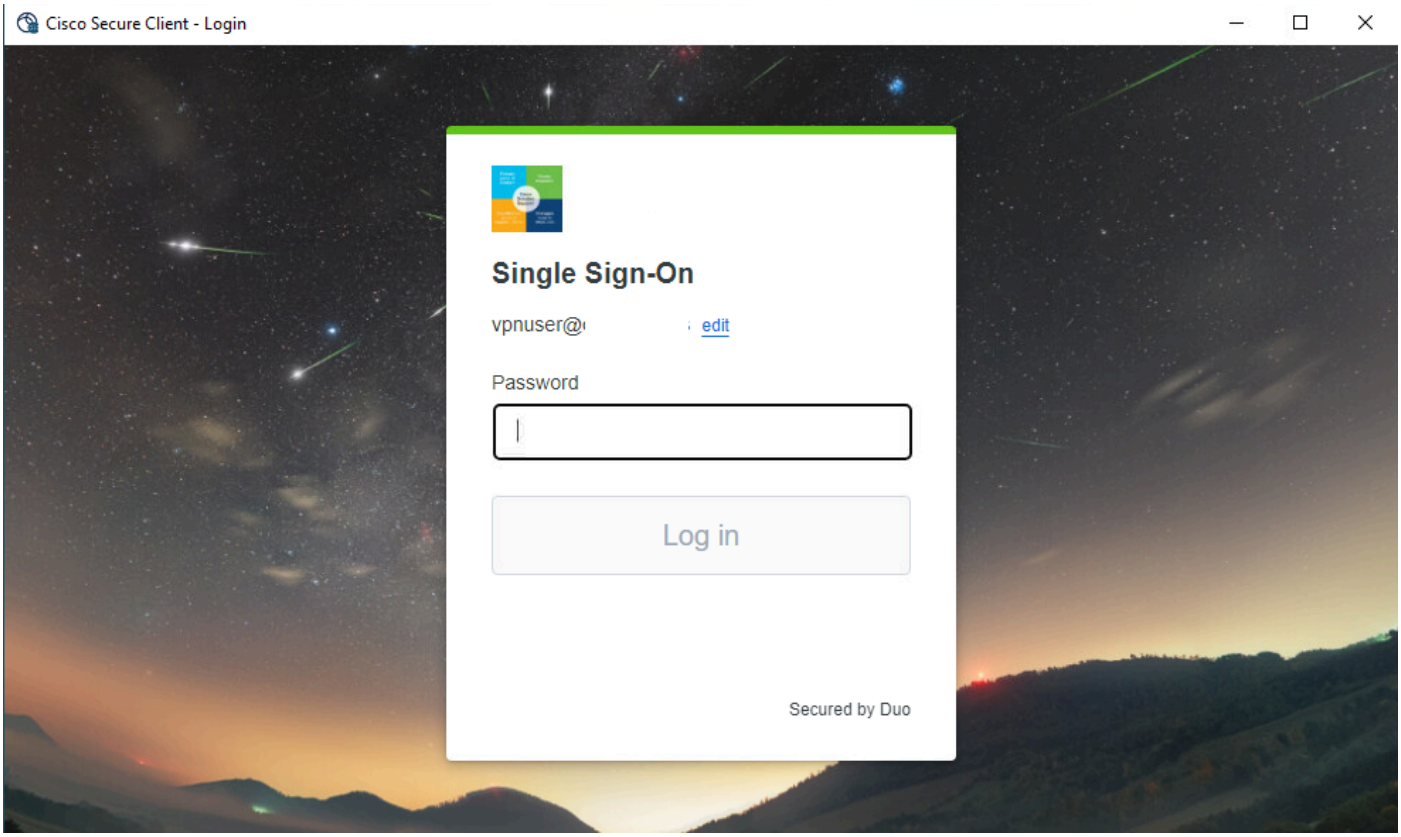
RA-VPN

Connectez-vous via Cisco Secure Client Agent-VPN.



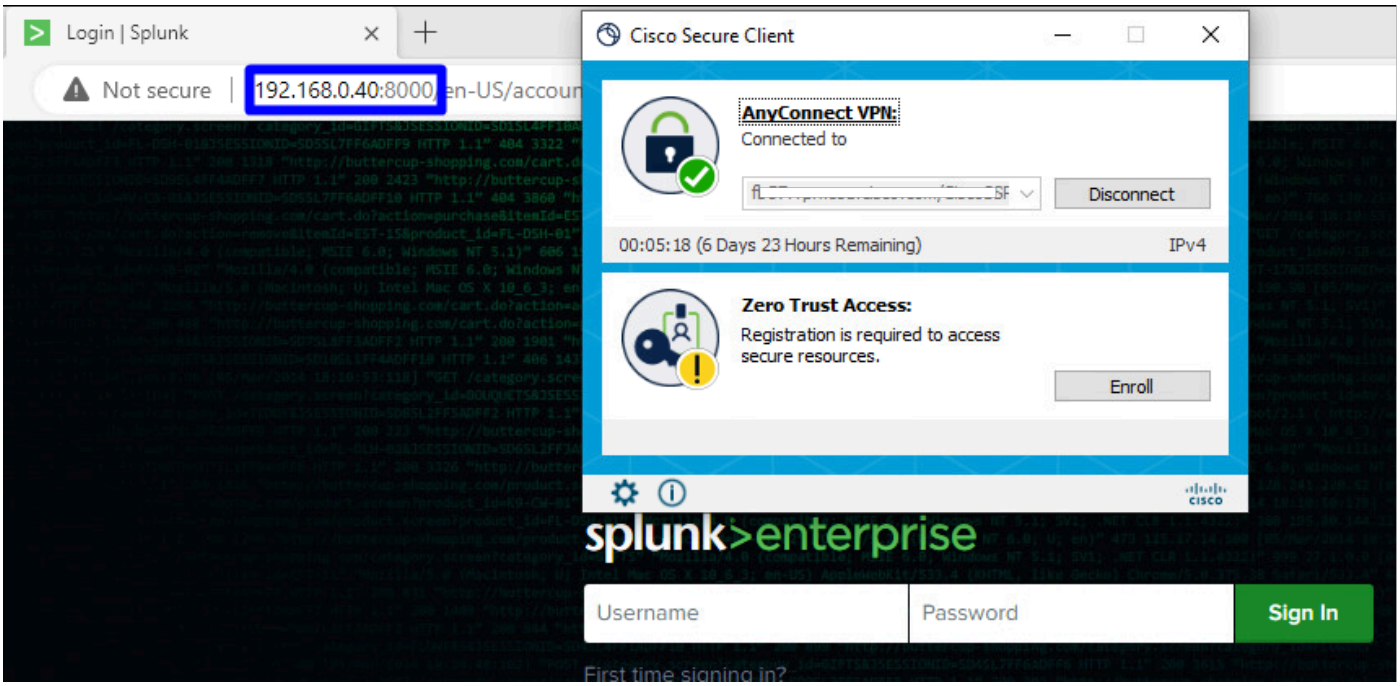
Client sécurisé - VPN

- Authentification via votre fournisseur SSO



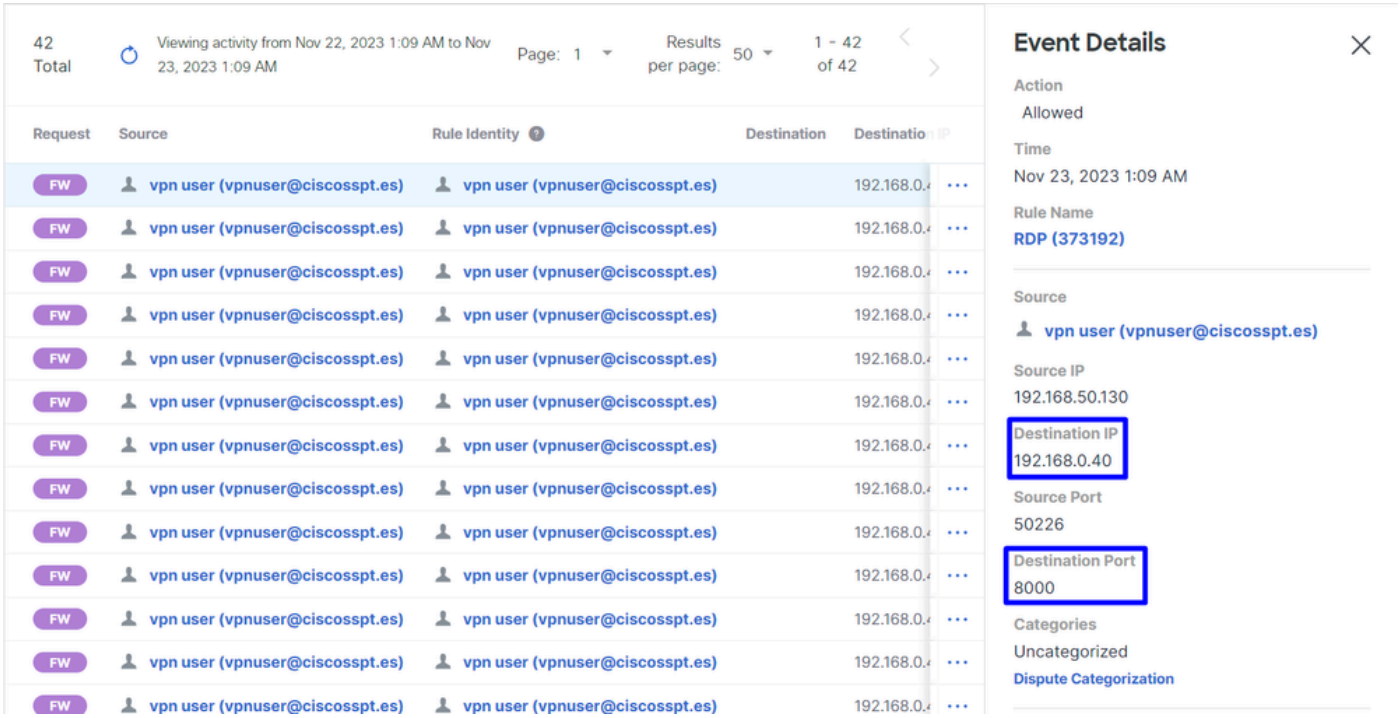
Accès sécurisé - VPN - SSO

- Une fois que vous êtes authentifié, accédez à la ressource :



Accès sécurisé - VPN - Authentifié

Naviguez jusqu'à l'adresse :Monitor > Activity Search

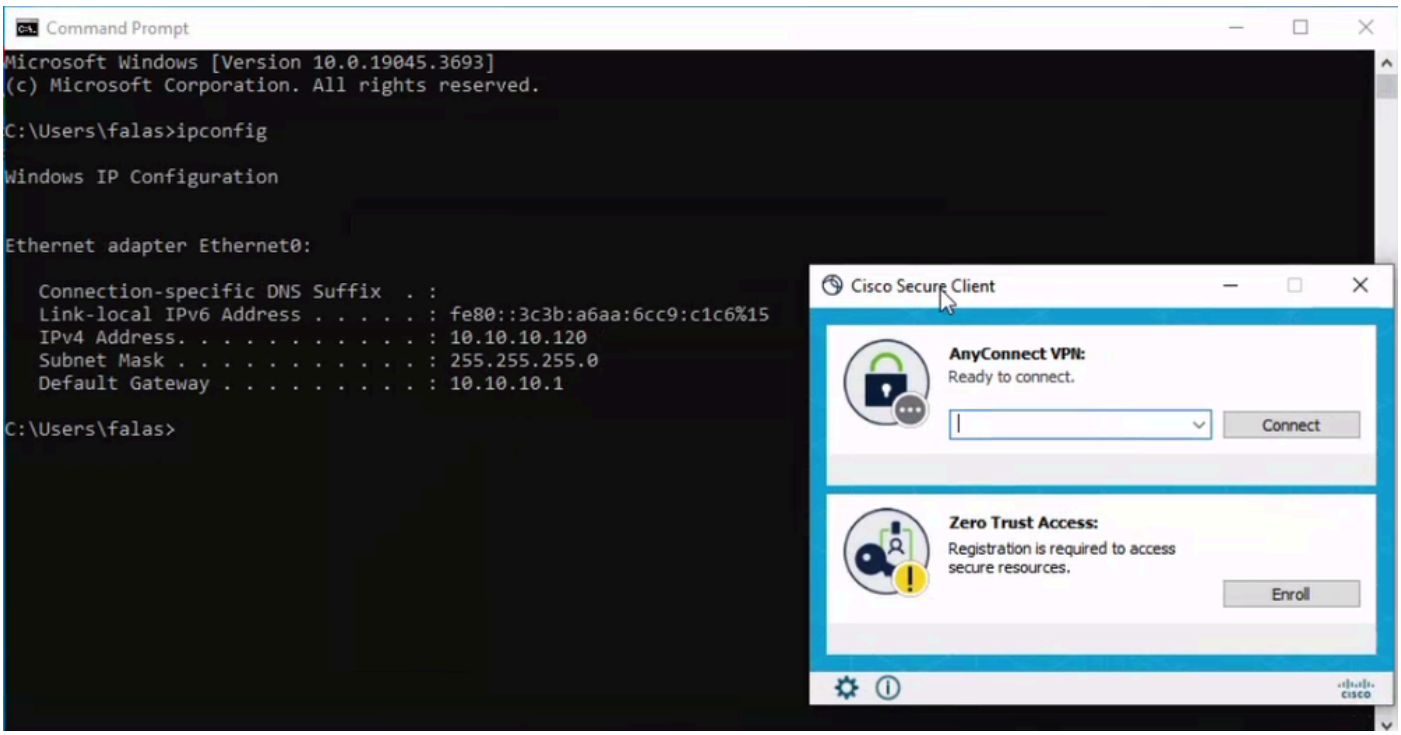


Accès sécurisé - Recherche d'activité - RA-VPN

Vous pouvez voir que l'utilisateur a été autorisé à s'authentifier via RA-VPN.

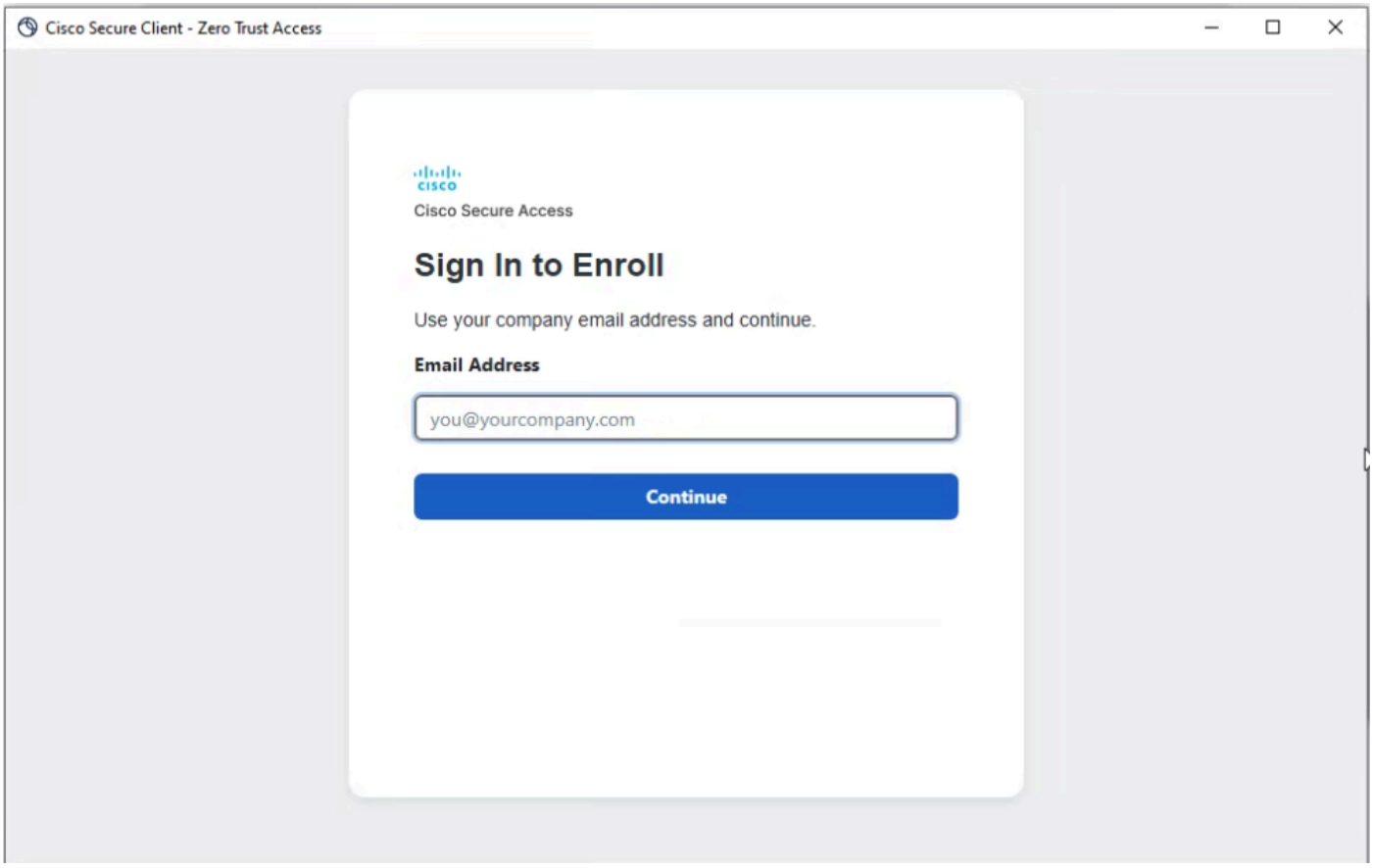
ZTNA client-Base

Connexion via Cisco Secure Client Agent - ZTNA.



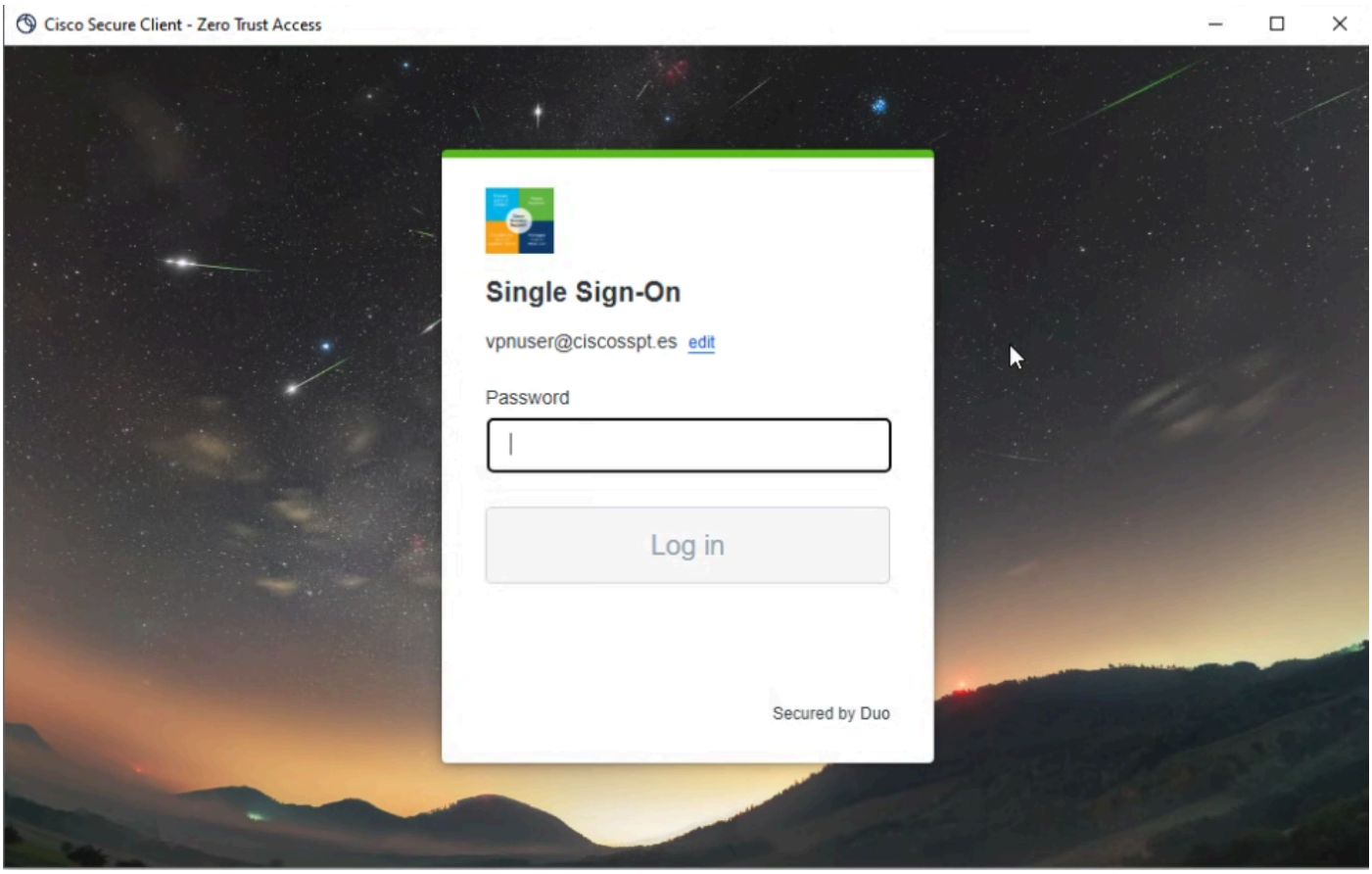
Client sécurisé - ZTNA

- Inscrivez-vous avec votre nom d'utilisateur.



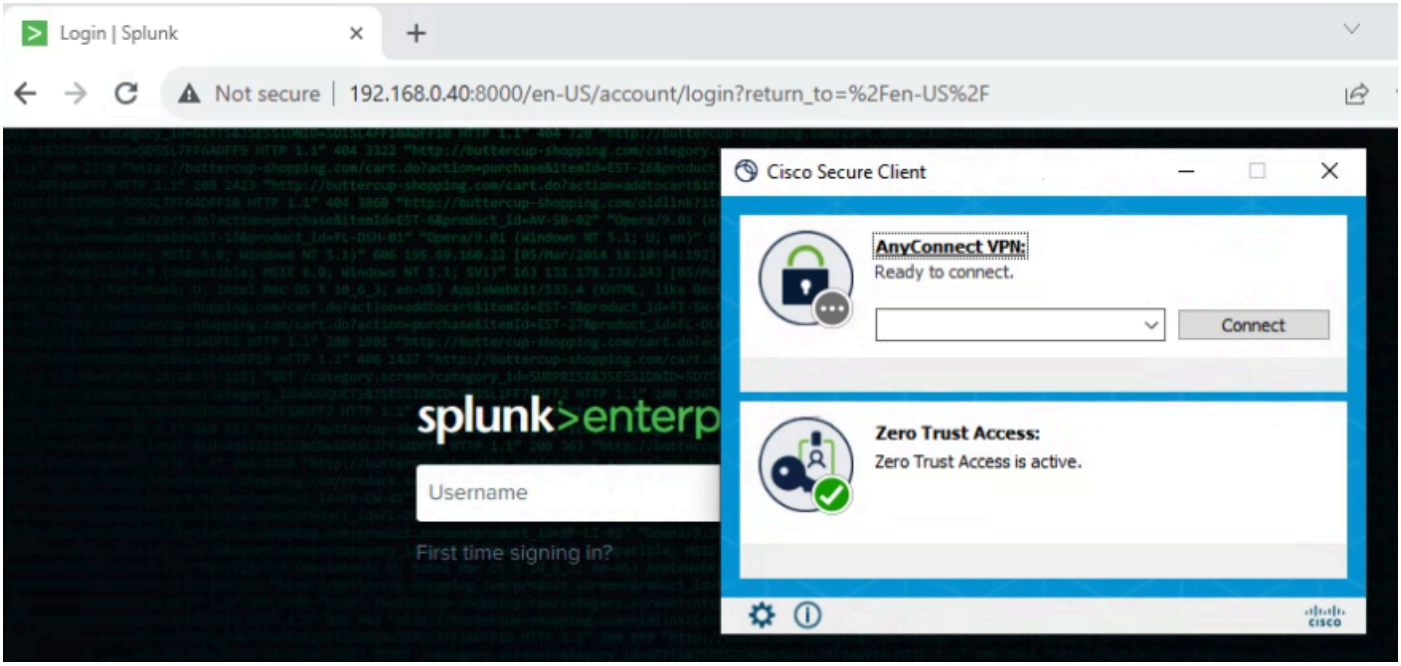
Client sécurisé - ZTNA - Inscription

- Authentification dans votre fournisseur SSO



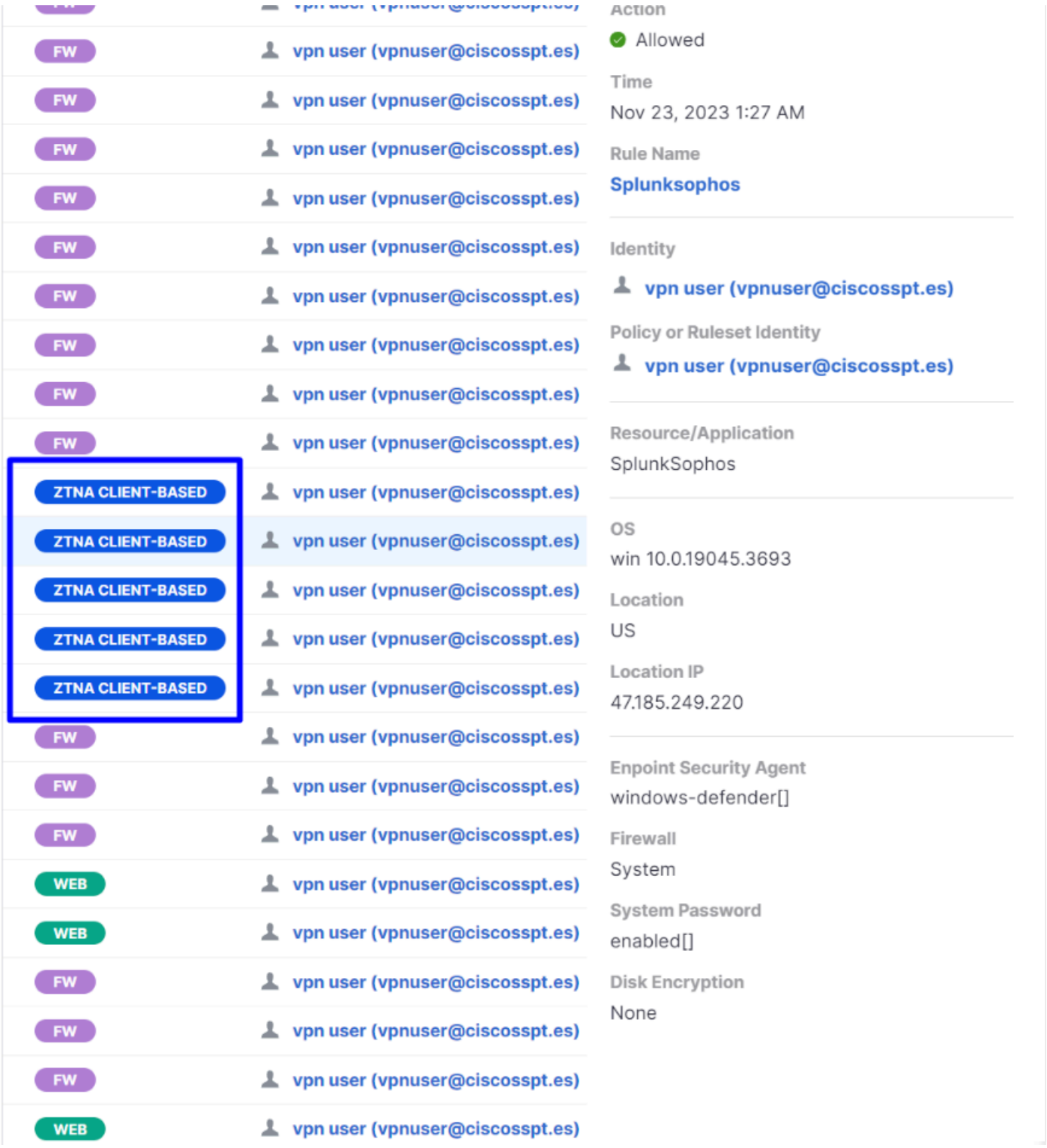
Client sécurisé - ZTNA - Connexion SSO

- Une fois que vous êtes authentifié, accédez à la ressource :



Accès sécurisé - ZTNA - Connecté

Naviguez jusqu'à l'adresse :Monitor > Activity Search

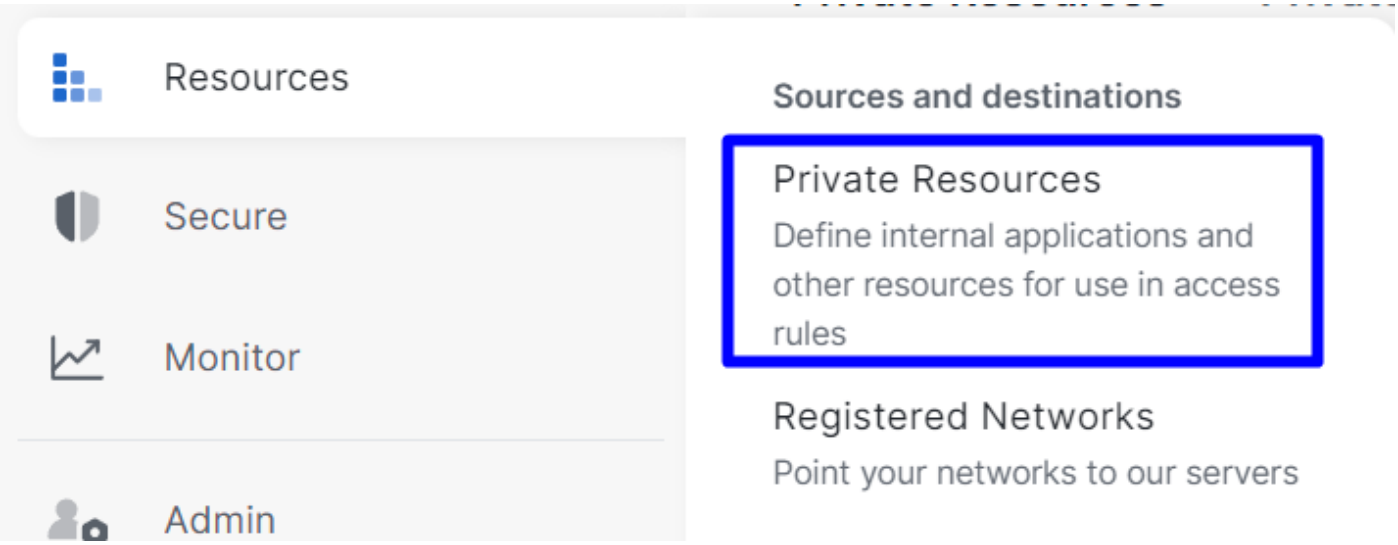


Accès sécurisé - Recherche d'activité - Basé sur le client ZTNA

Vous pouvez voir que l'utilisateur a été autorisé à s'authentifier via ZTNA basé sur le client.

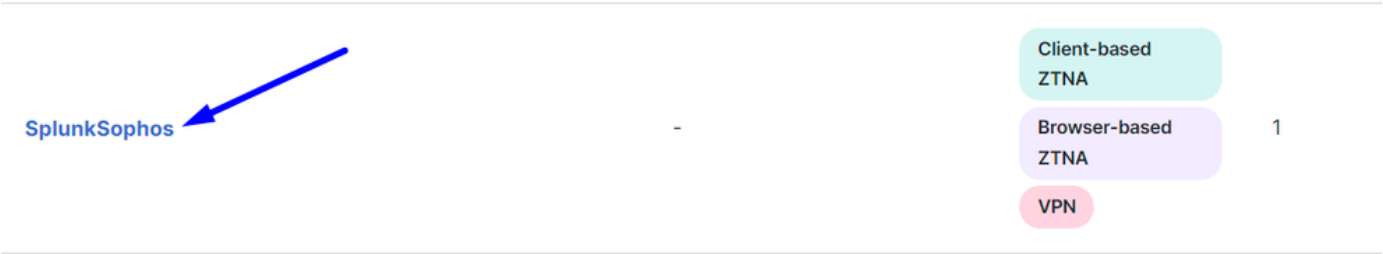
ZTNA basé sur un navigateur

Pour obtenir l'URL, vous devez accéder à **Resources > Private Resources**.



Accès sécurisé - Ressource privée

- Cliquez sur votre politique



Accès sécurisé - Ressource privée - SplunkSophos

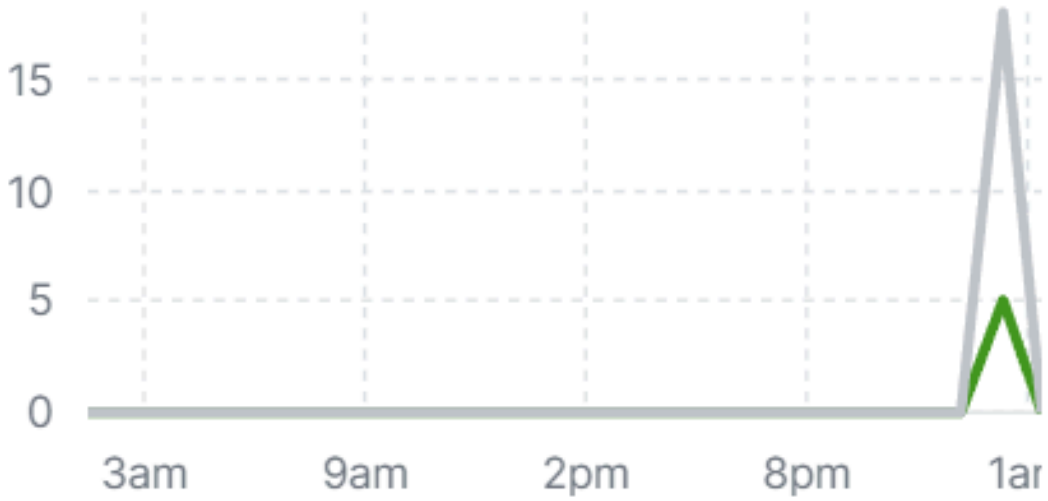
- Faites défiler vers le bas

SplunkSophos

Client-based ZTNA | Browser-based ZTNA | VPN

Total Requests

23 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status	
Success	5
Blocked	18

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.