

# Configurer un accès sécurisé avec le pare-feu Sophos XG

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configuration du tunnel sur l'accès sécurisé](#)

[Données du tunnel](#)

[Configuration du tunnel sur Sophos](#)

[Configurer le profil IPsec](#)

[Configuration d'un VPN site à site](#)

[Configurer l'interface du tunnel](#)

[Configuration des passerelles](#)

[Configuration de la route SD-WAN](#)

[Configurer une application privée](#)

[Configurer la stratégie d'accès](#)

[Vérifier](#)

[RA-VPN](#)

[ZTNA client-Base](#)

[ZTNA basé sur un navigateur](#)

[Informations connexes](#)

---

## 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



**CISCO**

Secure

Access

**SOPHOS**

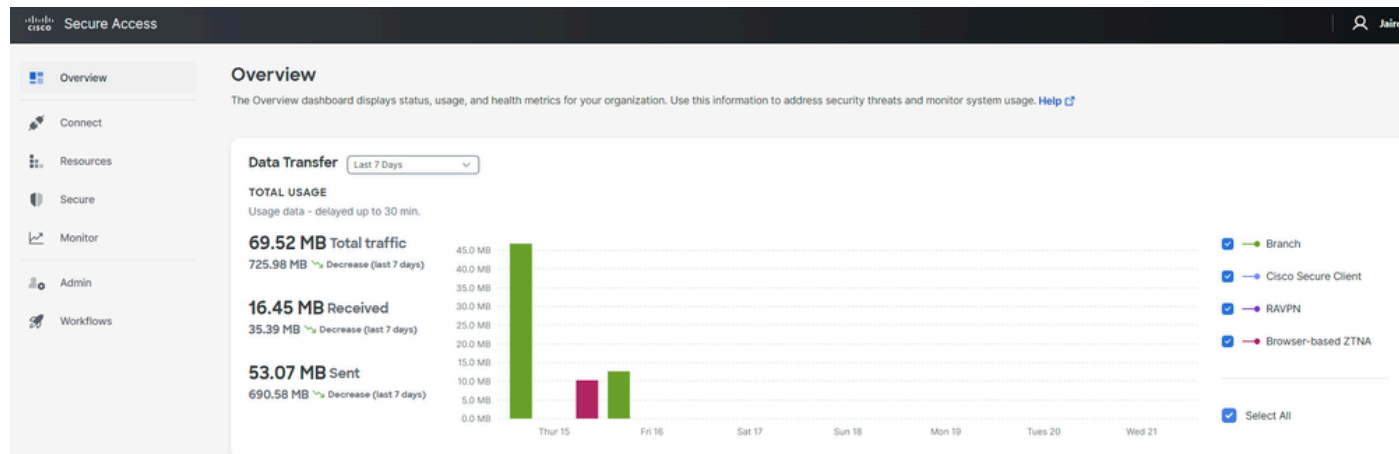
Accès sécurisé - Sophos

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.

The Overview dashboard displays the following sections:

- Connect** (highlighted)
- Resources**
- Secure**
- Monitor**
- Admin**

**Essentials**

- Network Connections** (highlighted): Connect data centers, tunnels, resource connectors
- Users and Groups**: Provision and manage users and groups for use in access rules
- End User Connectivity**: Manage traffic steering from endpoints to Secure Access

Accès sécurisé - Connexions réseau

- Sous Network Tunnel Groups cliquez sur + Add.

Connector Groups Beta **Network Tunnel Groups**

Network Tunnel Groups 2 total

1 Disconnected ● 1 Warning ▲ 0 Connected ●

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](#)

Q Search Region Status 2 Tunnel Groups + Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
<a href="#">HOME</a>	<span>●</span> Disconnected	Europe (Germany)	sse-euc-1-1-0	0	sse-euc-1-1-1	0
<a href="#">SAD</a>	<span>▲</span> Warning	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1	0

Rows per page 10 < 1 >

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

 ⊗

### Region

 ∨

### Device Type

 ∨

[Cancel](#)

[Next](#)



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

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

## Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

### Tunnel ID Format

Email  IP Address

### Tunnel ID

csasophos @<org><hub>.sse.cisco.com

### Passphrase

..... Show

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

### Confirm Passphrase

..... Show

Cancel

Back

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**.

## Routing option

Static routing

Use this option to manually add IP address ranges for this tunnel group.

### IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24 Add

192.168.0.0/24 X

192.168.10.0/24 X

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Cancel

Back

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

### Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

<b>Primary Tunnel ID:</b>	csasophcs@	-sse.cisco.com	📄
<b>Primary Data Center IP Address:</b>	18.156.145.74		📄
<b>Secondary Tunnel ID:</b>	csasophcs@	-sse.cisco.com	📄
<b>Secondary Data Center IP Address:</b>	3.120.45.23		📄
<b>Passphrase:</b>	<div style="background-color: red; width: 150px; height: 15px;"></div>		📄

[Download CSV](#)

[Done](#)

*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** Sophos Firewall Feedback [How-to guides](#) [Log view](#)

**Control center**  
SF01V (SFOS 19.5.3 MR-3-Build652)

**System** | **Traffic insight** | **User & device insights**

**MONITOR & ANALYZE**

- Control center**
- Current activities
- Reports
- Zero-day protection
- Diagnostics

**PROTECT**

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced protection

**CONFIGURE**

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

**SYSTEM**

- Sophos Central
- Profiles

**Performance** | **Services** | **Interfaces** | **VPN**

0/0 RED | 0/0 Wireless APs  
0 Connected remote users | 0 Live users

12% CPU | 61% Memory  
61B/s Bandwidth | 0 Sessions  
0% Decryption capacity | 0 Decrypt sessions

High availability: **Not configured**

Running for 0 day(s), 3 hour(s), 52 minute(s)

**Traffic insight**

Web activity: 0 max | 0 avg  
Cloud applications: 0 Apps, 0 B In, 0 B Out

Allowed app categories | Network attacks  
Allowed web categories | Blocked app categories

**User & device insights**

Security Heartbeat®: 0 At risk | Monitor endpoint health and systems at risk

Synchronized Application Control™: 0 Apps | Identify unknown apps on your network

Zero-day protection: 0 Recent, 0 Incidents, 0 Scanned

ATP: 0 Sources blocked | UTQ: 0 Accounts at risk

SSL/TLS connections: 0% Of traffic, 0% Decrypted, 0 Failed

**Active firewall rules**

0 WAF | 1 User | 3 Network | 4 Scanned

4 Unused | 2 Disabled | 0 Changed | 0 New

**Reports**

- 0 Risky apps seen (Yesterday)
- 0 Objectionable websites seen (Yesterday)
- 0 bytes Used by top 10 web users (Yesterday)
- 0 Intrusion attacks (Yesterday)

**Messages**

- Alert: Create a secure storage master key to improve protect... (7:56)
- Warning: IPS protection is turned off. To enforce the intrusion pr... (7:56)
- Alert: New system firmware is available for download. [Click h...](#) (11:47)

Click on widgets to open details

Sophos - Panneau d'administration

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

**IPsec profiles** | **Device access**

**Add** | **Delete**

algorithm | **Manage**

**Phase 2**

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

General settings

**Name**  
CSA

**Description**  
Description

**Key exchange**  
 IKEv1  IKEv2

**Authentication mode**  
 Main mode  Aggressive mode  
⚠ Aggressive mode is insecure

**Key negotiation tries**  
0  
Set 0 for unlimited number of negotiation tries

Re-key connection  
 Pass data in compressed format  
 SHA2 with 96-bit truncation

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)

## Phase 1

Key life 28800 <input checked="" type="checkbox"/> Seconds	Re-key margin 360 <input checked="" type="checkbox"/> Seconds	Randomize re-keying margin by 50 <input checked="" type="checkbox"/> %
DH group (key group) 2 selected <input checked="" type="checkbox"/>		
Encryption AES256 <input checked="" type="checkbox"/>	Authentication SHA2 256 <input checked="" type="checkbox"/>	

You can add up to 3 different algorithm combinations

*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

## Phase 2

PFS group (DH group) Same as phase-I <input checked="" type="checkbox"/>	Key life 3600 <input checked="" type="checkbox"/> Seconds
Encryption AES256 <input checked="" type="checkbox"/>	Authentication SHA2 256 <input checked="" type="checkbox"/>

You can add up to 3 different algorithm combinations

*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)

## BEFORE

Dead Peer Detection

Dead Peer Detection

Check peer after every: 10 Seconds

Wait for response up to: 120 Seconds

When peer unreachable: Re-initiate

## AFTER

Dead Peer Detection

Check peer after every: 10 Seconds

Wait for response up to: 120 Seconds

When peer unreachable: Re-initiate

*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**.

Reports

- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced protection

CONFIGURE

- Remote access VPN
- Site-to-site VPN**
- Network

Show additional properties

Name ▾ ▲ Group name ▾ Profile ▾ Connection type ▾ Status

Active ▾ Connection ▾ Manage

No records found

Failover group

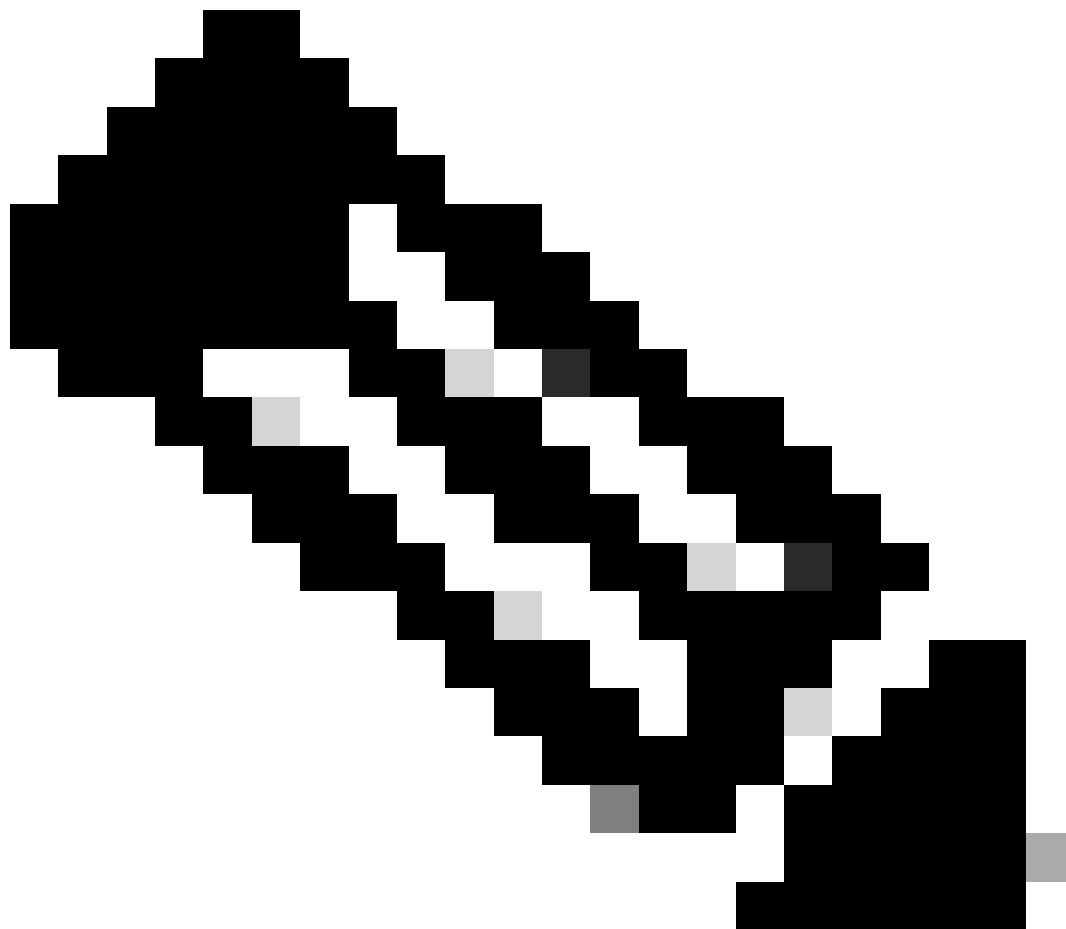
Add Delete Wizard

Add Delete

*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.

---

## General settings

<b>Name</b> SecureAccessS	<b>IP version</b> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Dual	<input checked="" type="checkbox"/> Activate on save <input type="checkbox"/> Create firewall rule
<b>Description</b> This is the IPsec Policy for Sophos	<b>Connection type</b> Tunnel interface	
	<b>Gateway type</b> Initiate the connection	

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

Encryption

Profile	Authentication type
CSA	Preshared key
	Preshared key
	Repeat preshared key

Sophos - VPN de site à site - Cryptage

Sous **Gateway Settings** configure Local Gateway et options Remote 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, <a href="#">Tunnel Data</a>
Type d'ID local Courriel	Type d'ID distant



	Adresse IP
ID local L'e-mail généré à l'étape, <a href="#">Tunnel Data</a>	ID distant L'adresse IP publique générée lors de l'étape, <a href="#">Tunnel Data</a>
Sous-réseau local tous les modèles	Sous-réseau distant tous les modèles

## Gateway settings

Local gateway	Remote gateway
<b>Listening interface</b> <input type="text" value="PortB - 192.168.0.33"/>	<b>Gateway address</b> <input type="text" value="18.156.145.74"/>
<b>Local ID type</b> <input type="text" value="Email"/>	<b>Remote ID type</b> <input type="text" value="IP address"/>
<b>Local ID</b> <input type="text" value="csasophos@"/> <input type="text" value="-sse.cisco.com"/>	<b>Remote ID</b> <input type="text" value="18.156.145.74"/>
<b>Local subnet</b> <input type="text" value="Any"/>	<b>Remote subnet</b> <input type="text" value="Any"/>
<a href="#">Add new item</a>	<a href="#">Add new item</a>

Sophos - VPN site à site - Paramètres de passerelle

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

## IPsec connections

Show additional properties							Add	Delete	Wizard
Name	Group name	Profile	Connection type	Status	Connection	Manage			
<input type="checkbox"/> <u>SecureAccesS</u>	-	CSA	Tunnel interface	<span style="color: green;">●</span>	<span style="color: green;">●</span> <a href="#">i</a>	<a href="#">✎</a> <a href="#">🔌</a> <a href="#">🗑️</a>			

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**.

MONITOR & ANALYZE

# Control center


Current activities

Reports

Zero-day protection

Diagnostics

*Sophos - Surveillance et analyse - IPsec*

Live users	Live connections	Live connections IPv6	IPsec connections	Remote users			
<b>No tunnel established to Secure Access</b>							
<input type="checkbox"/>	Name ▾	Local server ▾	Local subnet ▾	Username ▾	Remote server/host ▾	Remote subnet ▾	Manage
No records found							
<b>Tunnel established to Secure Access</b>							
<input type="checkbox"/>	Name ▾	Local server ▾	Local subnet ▾	Username ▾	Remote server/host ▾	Remote subnet ▾	Manage
<input type="checkbox"/>	SecureAccesS-1	192.168.0.33	0.0.0.0/0	-	18.156.145.74	0.0.0.0/0	

*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

#### General settings

Name *	<input type="text" value="xfrm1"/>
Hardware	xfrm1
IPsec connection	SecureAccessS
Network zone	VPN
<input checked="" type="checkbox"/> IPv4 configuration	
IPv4/netmask *	<input type="text" value="169.254.0.1"/> <input type="text" value="/30 (255.255.255.252)"/>

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

The screenshot shows the 'Gateways' configuration page in Sophos Routing. The 'IPv4 gateway' section contains a table with the following data:

Name	IP address	Interface	Health check	Status	Manage
<input type="checkbox"/> DHCP_PortB_GW	192.168.0.1	WAN	On	Down (red dot)	

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)

The 'Gateway host' configuration form contains the following fields:

- Name \*:** CSA\_GW
- Gateway IP:** 169.254.0.2
- Interface:** xfrm1-169.254.0.1
- Zone:** None

Sophos - Routage - Passerelles - Hôte de passerelle

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

# Health check

Health check



*Sophos - Routage - Passerelles - Contrôle d'intégrité*

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

## IPv4 gateway

<input type="checkbox"/>	Name	IP address	Interface	Health check	Status	Manage
<input type="checkbox"/>	<u>CSA_GW</u>	169.254.0.2	xfrm1	Off		
<input type="checkbox"/>	<u>DHCP_PortB_GW</u>	192.168.0.1	WAN	On		

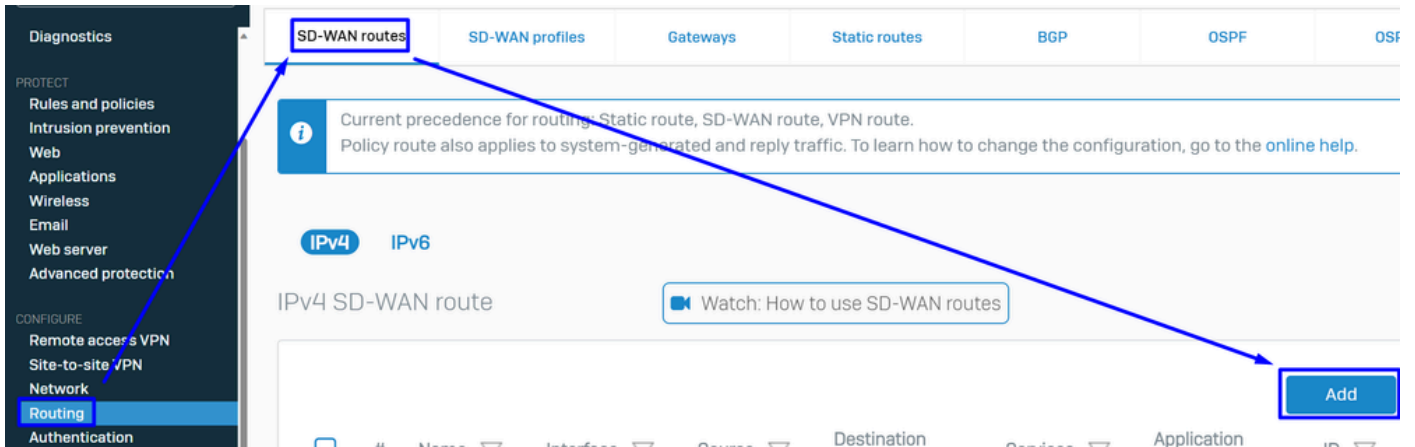
*Sophos - Routage - Passerelles - État*

## 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

### Traffic selector

<b>Incoming interface</b> <input type="text" value="LAN-192.168.0.203"/>	<b>DSCP marking</b> <input type="text" value="Select DSCP marking"/>	
<b>Source networks</b> <input type="text" value="Any"/> <input type="button" value="Add new item"/>	<b>Destination networks</b> <input type="text" value="Any"/> <input type="button" value="Add new item"/>	<b>Services</b> <input type="text" value="Any"/> <input type="button" value="Add new item"/>
<b>Application object</b> <input type="text" value="Any"/> <input type="button" value="Add new item"/>	<b>User or groups</b> <input type="text" value="Any"/> <input type="button" value="Add new item"/>	

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**

### Link selection settings

Select SD-WAN profile ⓘ  Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

*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**



**Private Resources**

Private Resources are applications, r  
resource using zero-trust access. Ho

**Private Resources**    Private F

Sources and destinations

**Private Resources**  
Define internal applications and  
other resources for use in access  
rules

**Registered Networks**  
Point your networks to our servers

**Internal Networks**  
Define internal network segments  
to use as sources in access rules

**Internet and SaaS Resources**  
Define destinations for internet  
access rules

**Roaming Devices**  
Mac and Windows

Accès sécurisé - Ressources privées

- Cliquez sur + Add

**Private Resources**    Private Resource Groups

Private Resources

Q Search by resource name    Private Resource Group    Connection Method    4 Private Resources    Last 24 Hours    + Add

Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
------------------	------------------------	-------------------	-------------	-------	----------------

Accès sécurisé - Ressources privées 2

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

## General

### Private Resource Name

SplunkSophos

### Description (optional)

*Accès sécurisé - Ressources privées - Général*

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

- **Internally 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

## Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address. [Help](#)

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)

192.168.0.40

Protocol

TCP - (HTTP/HTTPS)

Port / Ranges

8000

[+ Protocol & Port](#)

[+ IP Address or FQDN](#)

Use internal DNS server to resolve the domain

*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**

**Zero-trust connections**

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

**Client-based connection**

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over

**Remotely Reachable Address** (FQDN, Wildcard FQDN, IP Address) ⓘ

192.168.0.40

+ FQDN or IP Address

**Browser-based connection**

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when endpoint security checks are possible.

**Public URL for this resource** ⓘ

https:// splunksophos -8195126.ztna.sse.cisco.com



**Protocol**

**Server Name Indication (SNI)** (optional) ⓘ

HTTP

**Validate Application Certificate** ⓘ

**VPN connections**

Allow endpoints to connect to this resource when connected to the network using VPN.

**Save** Cancel

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

Une fois la configuration terminée, voici le résultat :

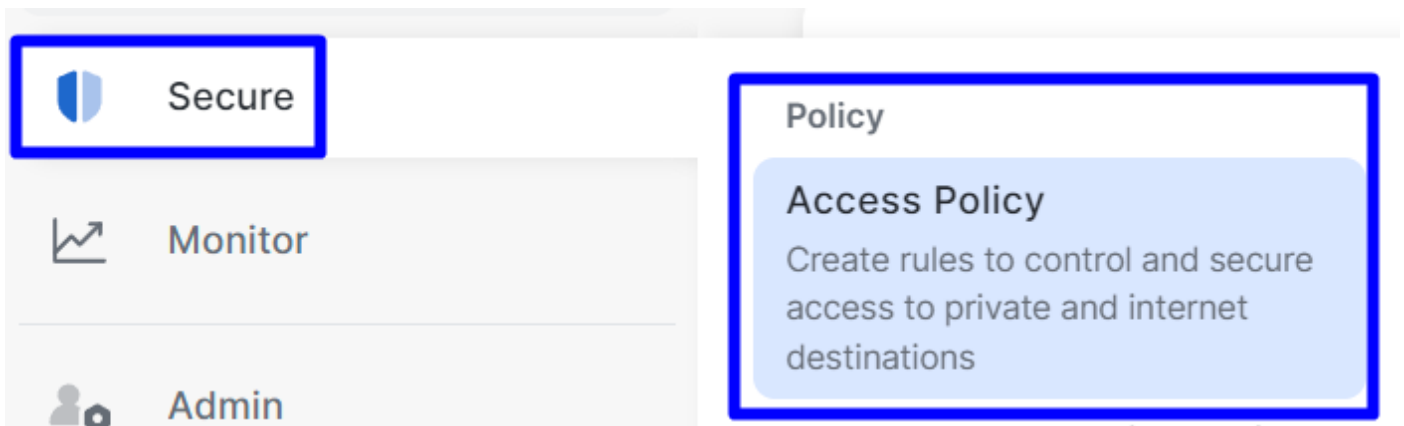
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none"><li>VPN</li><li>Browser-based ZTNA</li><li>Client-based ZTNA</li></ul>	1	2	16

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**

Add Rule ^

## Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

## Internet Access

Control and secure access to public destinations from within your network and from managed devices

*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**

## 1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

### Action



#### Allow

Allow specified traffic if security requirements are met.



#### Block

Block specified traffic.

### From

Specify one or more sources.

Any

Information about sources, including selecting multiple sources. [Help](#)

### To

Specify one or more destinations.

Private Resources • SplunkSophos

Information about destinations, including selecting multiple destinations. [Help](#)

### Endpoint Requirements

If endpoints do not meet the specified requirements for zero-trust connections, this rule will not match the traffic. [Help](#)



#### Zero-Trust Client-based Posture Profile

Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

Profile: **System provided (Client-based)** | Requirements: **Disk encryption, Operating System, Endpoint security agent, Firewall**

Private Resources: **SplunkSophos**



#### Zero Trust Browser-based Posture Profile

Rule Defaults

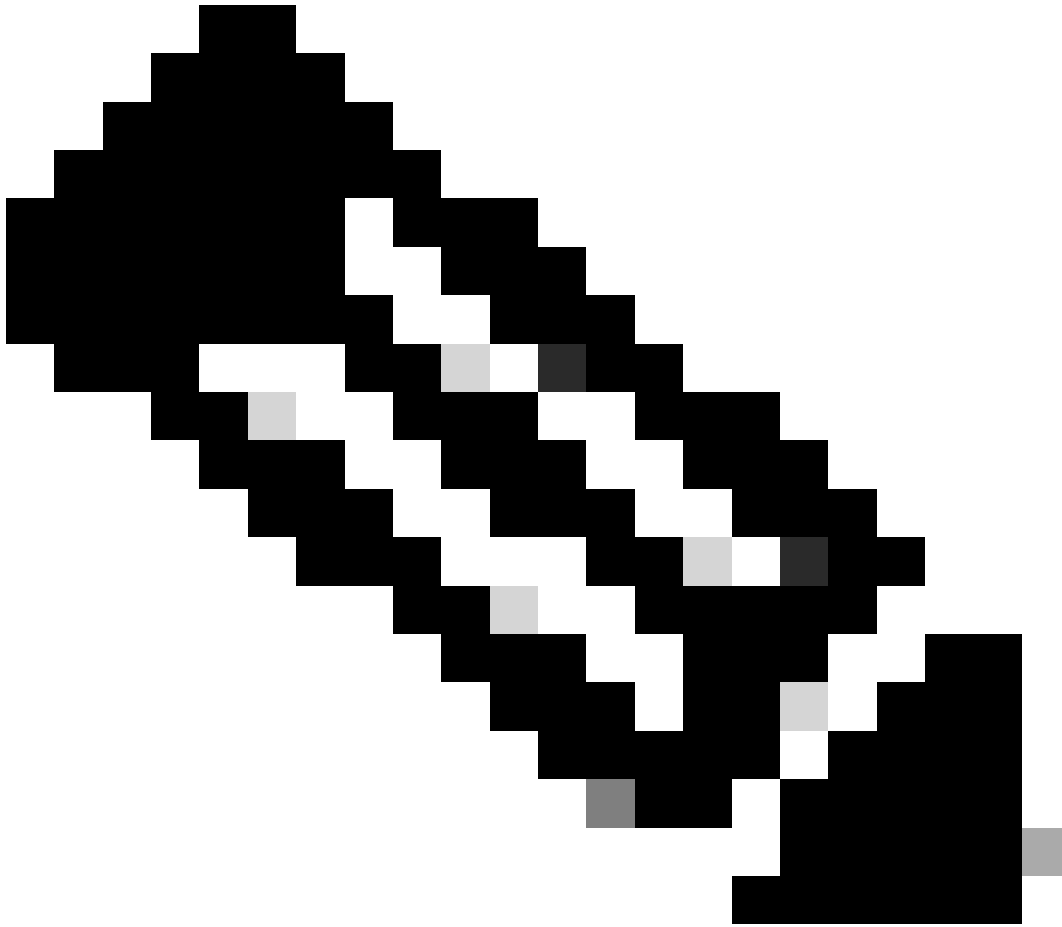
Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

Profile: **System provided (Browser-based)** | Requirements: **Operating System, Browser**

Private Resources: **SplunkSophos**

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 :

<input type="checkbox"/>	# ⓘ	Rule name	Access	Action	Sources	Destinations	Security	Status
<input type="checkbox"/>	6	SplunkSophos	Private	✓ Allow	Any	SplunkSophos	-	✓ ...

*Accès sécurisé : stratégie d'accès configurée*

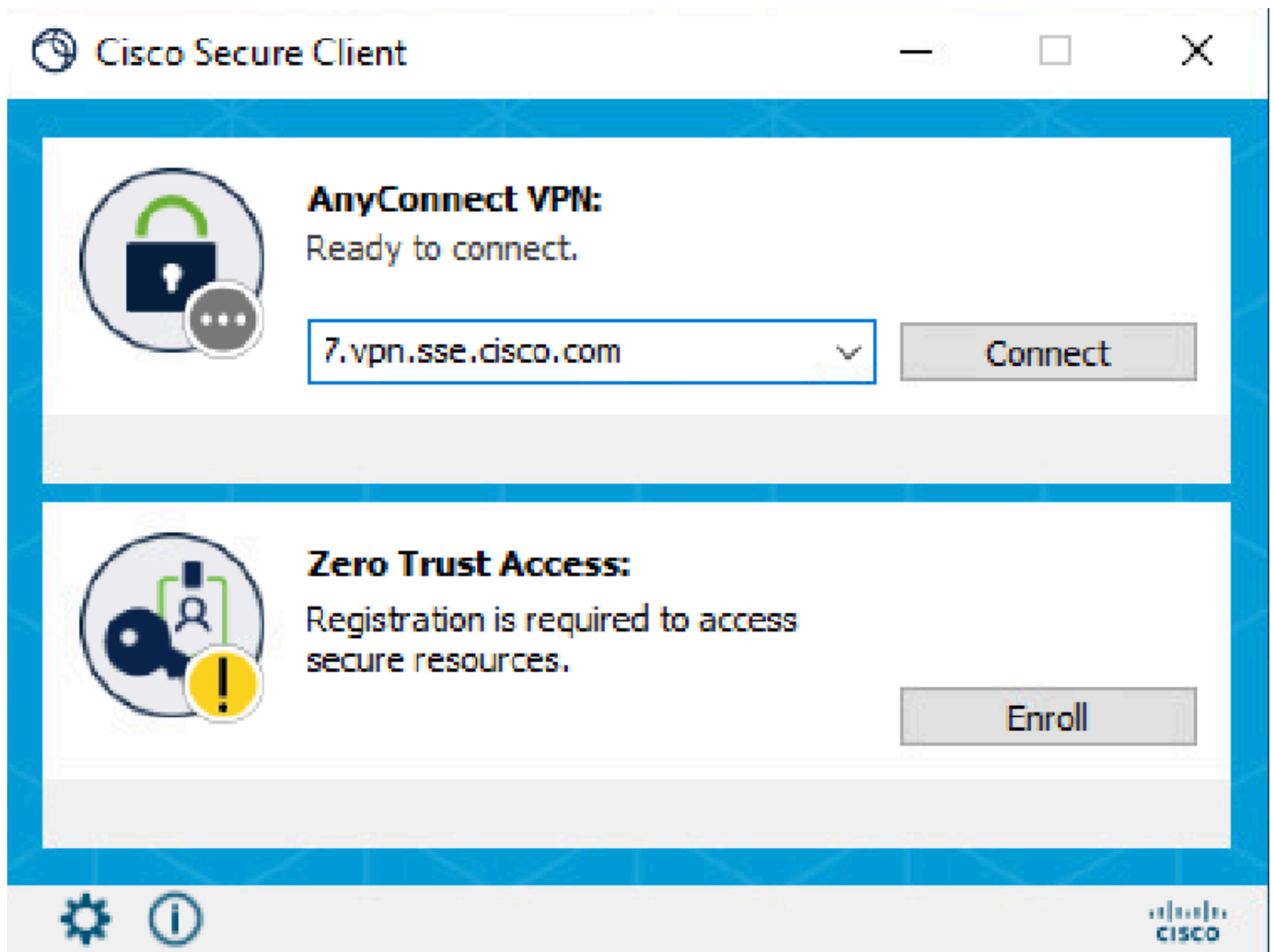
Ensuite, vous pouvez passer à l'étape Verify.

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](#).

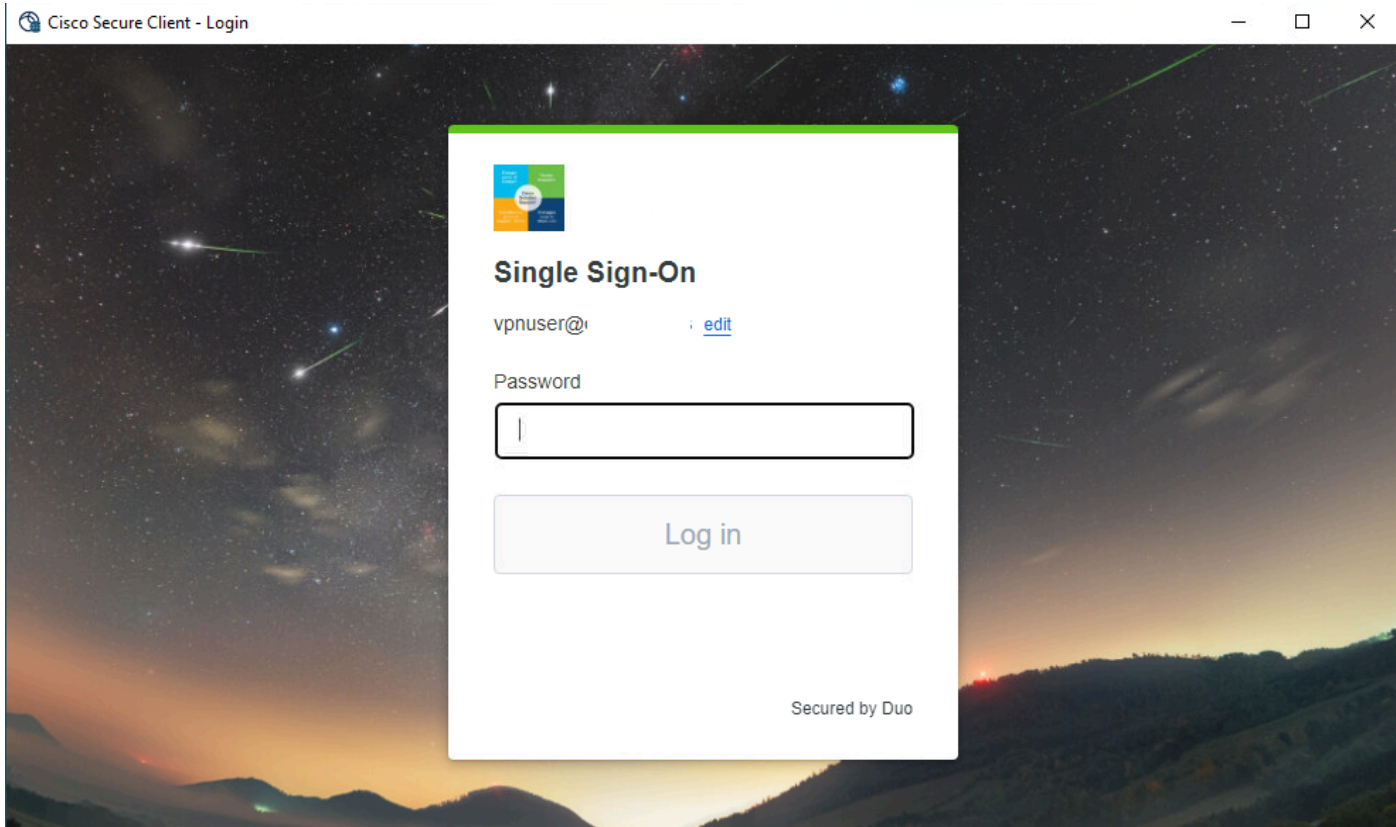
RA-VPN

Connectez-vous via Cisco Secure Client Agent-VPN.



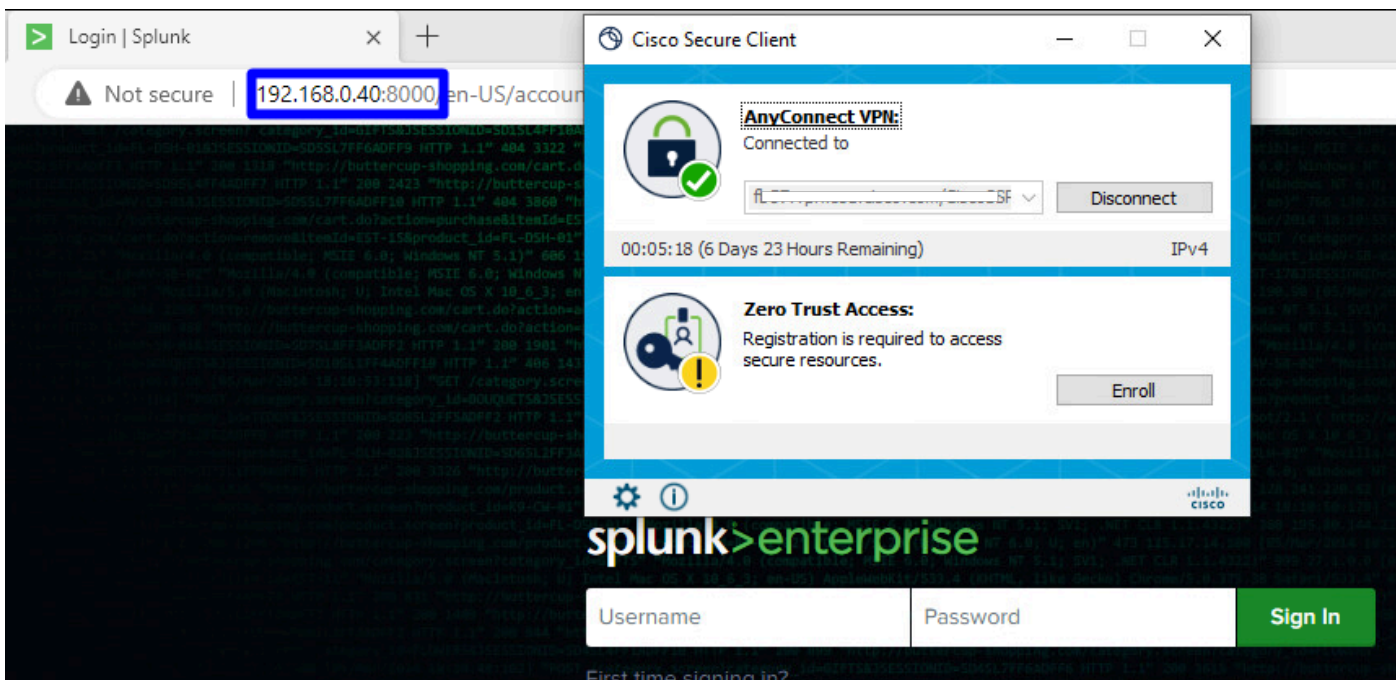
Client sécurisé - VPN

- 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

42 Total Viewing activity from Nov 22, 2023 1:09 AM to Nov 23, 2023 1:09 AM Page: 1 Results per page: 50 1 - 42 of 42

Request	Source	Rule Identity	Destination	Destination IP
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...

### Event Details

Action: Allowed

Time: Nov 23, 2023 1:09 AM

Rule Name: RDP (373192)

Source: vpn user (vpnuser@ciscospt.es)

Source IP: 192.168.50.130

Destination IP: 192.168.0.40

Source Port: 50226

Destination Port: 8000

Categories: Uncategorized, Dispute Categorization

Accès sécurisé - Recherche d'activité - RA-VPN

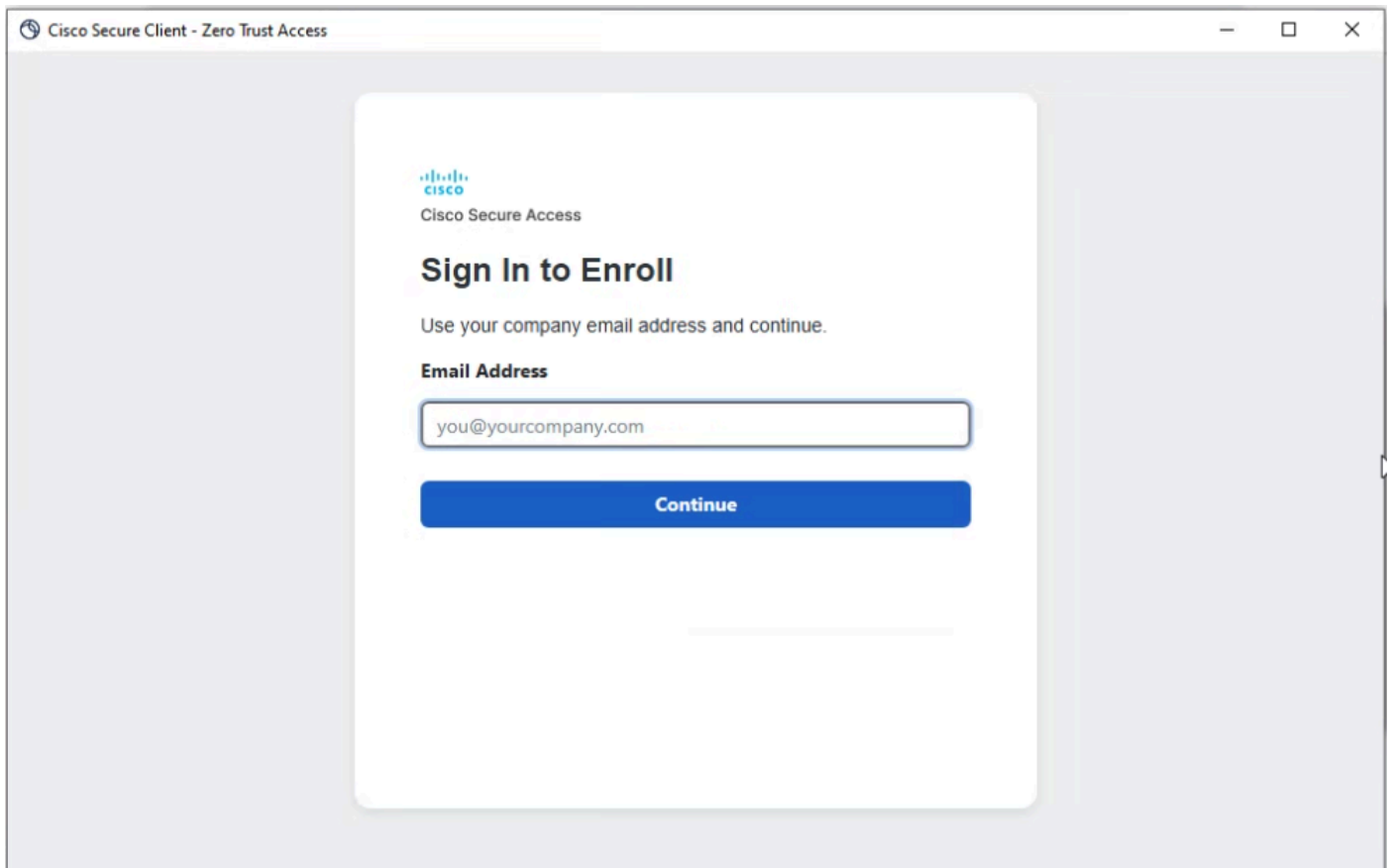
Vous pouvez voir que l'utilisateur a été autorisé à s'authentifier via RA-VPN.

ZTNA client-Base

Connexion via Cisco Secure Client Agent - ZTNA.

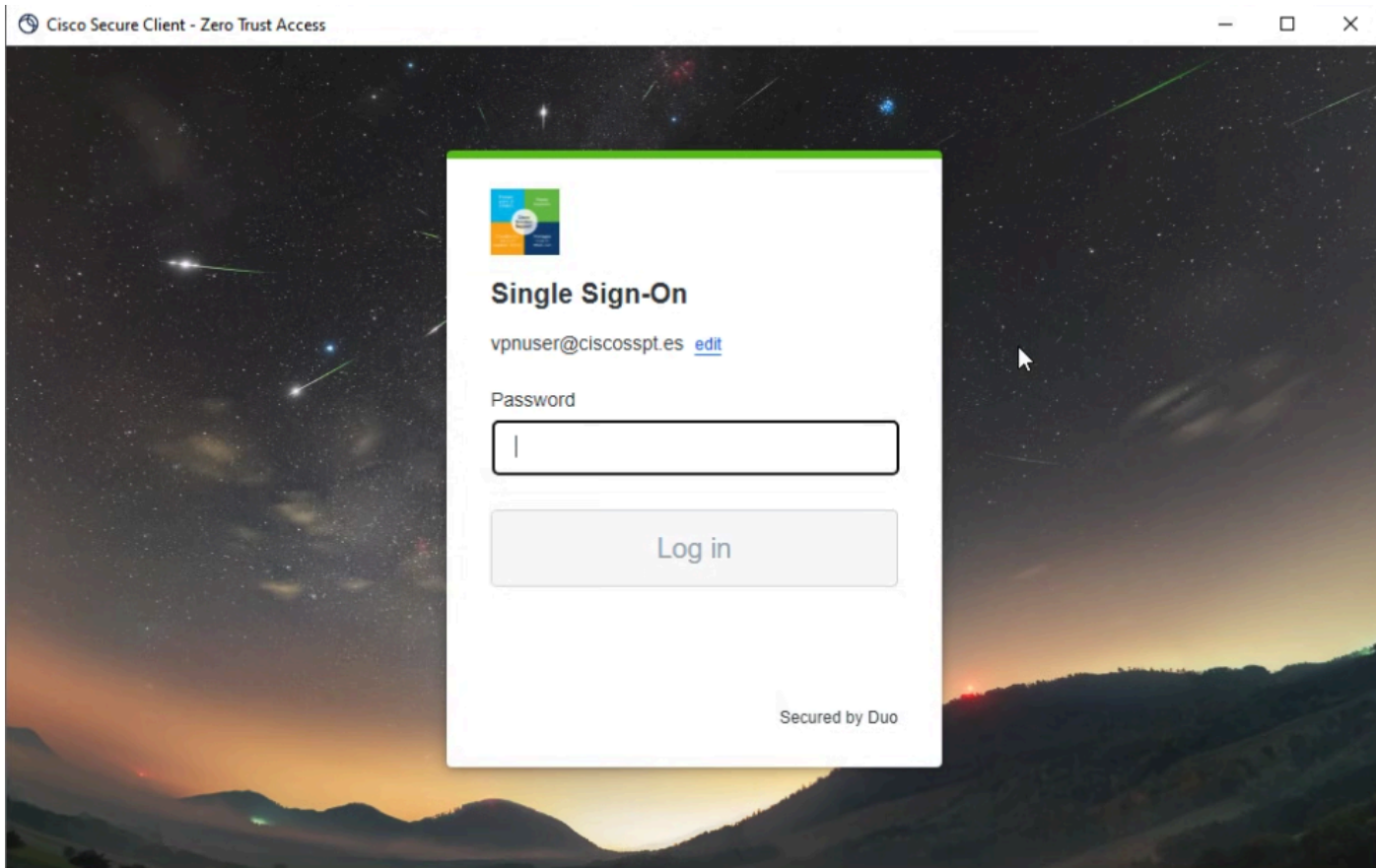
Client sécurisé - ZTNA

- Inscrivez-vous avec votre nom d'utilisateur.



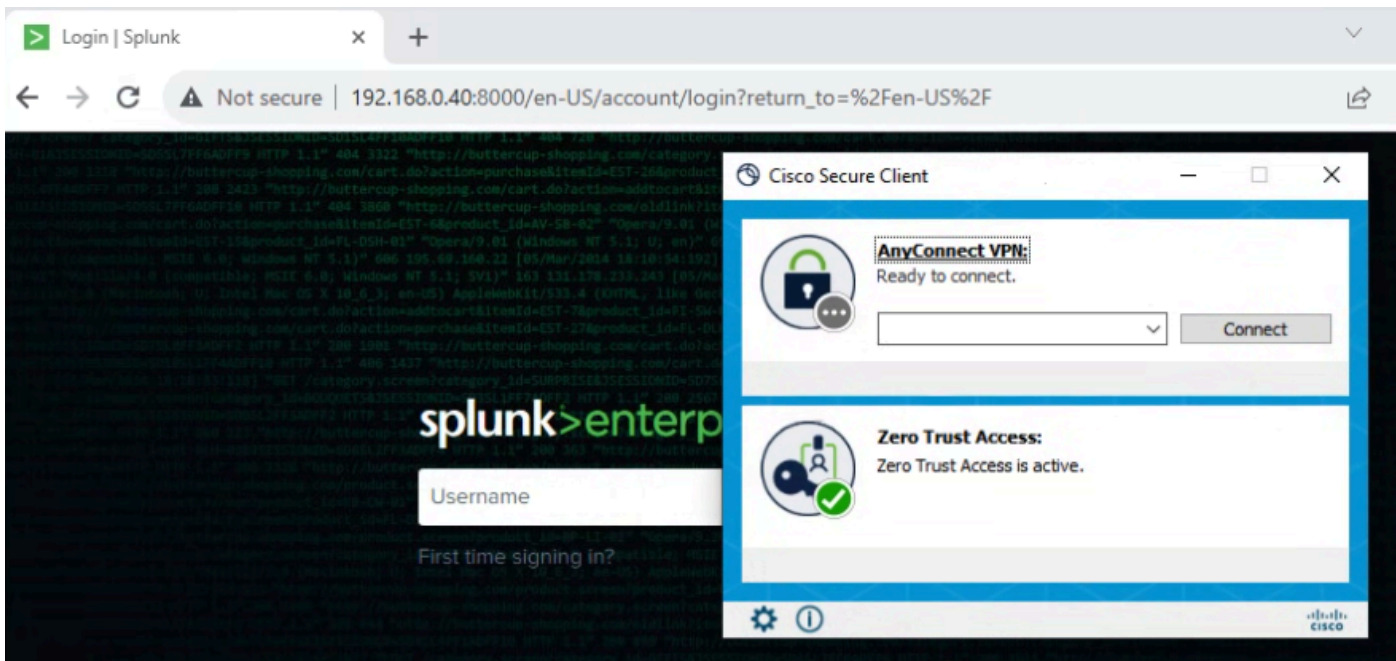
*Client sécurisé - ZTNA - Inscription*

- 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

FW	vpn user (vpnuser@ciscosspt.es)	Action	Allowed
FW	vpn user (vpnuser@ciscosspt.es)	Time	Nov 23, 2023 1:27 AM
FW	vpn user (vpnuser@ciscosspt.es)	Rule Name	Splunksophos
FW	vpn user (vpnuser@ciscosspt.es)	Identity	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)	Policy or Ruleset Identity	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)	Resource/Application	SplunkSophos
FW	vpn user (vpnuser@ciscosspt.es)	OS	win 10.0.19045.3693
FW	vpn user (vpnuser@ciscosspt.es)	Location	US
FW	vpn user (vpnuser@ciscosspt.es)	Location IP	47.185.249.220
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	Endpoint Security Agent	windows-defender[]
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	Firewall	System
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	System Password	enabled[]
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	Disk Encryption	None
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
WEB	vpn user (vpnuser@ciscosspt.es)		
WEB	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
FW	vpn user (vpnuser@ciscosspt.es)		
WEB	vpn user (vpnuser@ciscosspt.es)		

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**.

The screenshot shows a sidebar on the left with four main navigation items: 'Resources' (with a grid icon), 'Secure' (with a shield icon), 'Monitor' (with a line graph icon), and 'Admin' (with a person icon). To the right, under the heading 'Sources and destinations', there are two sections: 'Private Resources' (described as 'Define internal applications and other resources for use in access rules') and 'Registered Networks' (described as 'Point your networks to our servers'). The 'Private Resources' section is highlighted with a blue rectangular border.

Accès sécurisé - Ressource privée

- Cliquez sur votre politique

The screenshot shows a list of resources. On the left, the text 'SplunkSophos' is displayed in blue. A blue arrow points from the top right towards this text. To the right of the list, there are three colored buttons: a light blue button labeled 'Client-based ZTNA', a light purple button labeled 'Browser-based ZTNA', and a light pink button labeled 'VPN'. The number '1' is visible to the right of the 'Browser-based ZTNA' button.

Accès sécurisé - Ressource privée - SplunkSophos

- Faites défiler vers le bas



# SplunkSophos

Client-based ZTNA

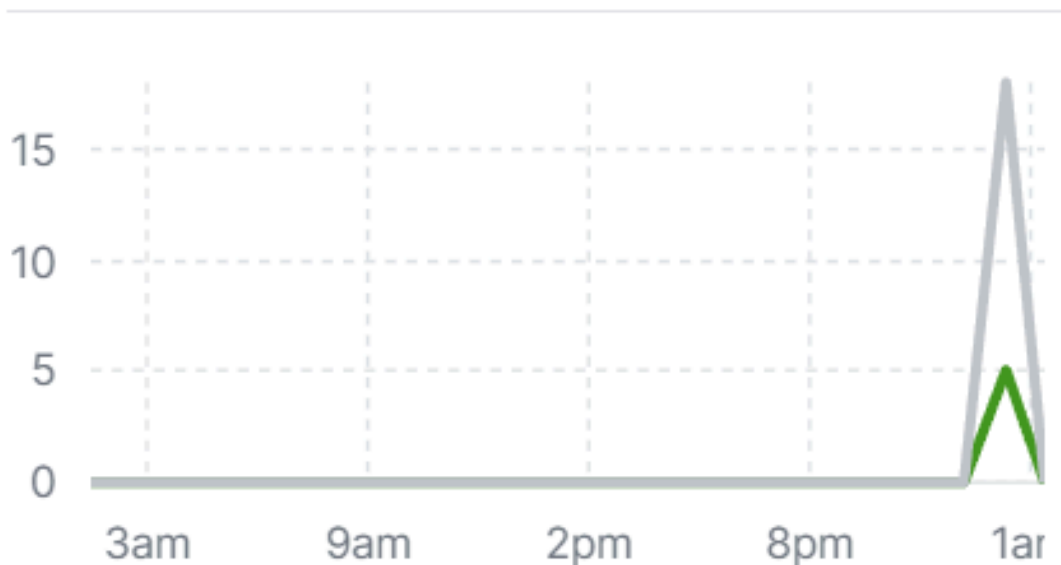
Browser-based ZTNA



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.