

# Beveiligde toegang configureren met Sophos XG-firewall

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[De tunnel op beveiligde toegang configureren](#)

[Tunnelgegevens](#)

[De tunnel op Sophos configureren](#)

[IPsec-profiel configureren](#)

[Site-to-site VPN configureren](#)

[Tunnelinterface configureren](#)

[De gateways configureren](#)

[De SD-WAN router configureren](#)

[Privé-app configureren](#)

[Het toegangsbeleid configureren](#)

[Verifiëren](#)

[RA-VPN](#)

[Op client gebaseerde ZTNA](#)

[Op browser gebaseerde ZTNA](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u Secure Access kunt configureren met de Sophos XG-firewall.

## Voorwaarden

- [Gebruikersprovisioning configureren](#)
- [Configuratie ZTNA SSO-verificatie](#)
- [Beveiligde toegang tot VPN configureren](#)

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Sophos XG-firewall
- Beveiligde toegang

- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA
- Clientloze ZTNA

## Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Sophos XG-firewall
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie



**CISCO**

Secure

Access

**SOPHOS**

Beveiligde toegang - Sophos

Cisco heeft Secure Access ontworpen om de bescherming en levering van toegang tot particuliere toepassingen te waarborgen, zowel op locatie als in de cloud. Het beschermt ook de verbinding van het netwerk met het internet. Dit wordt bereikt door de implementatie van meerdere beveiligingsmethoden en -lagen, die allemaal gericht zijn op het bewaren van de informatie zoals

ze deze via de cloud benaderen.

## Configureren

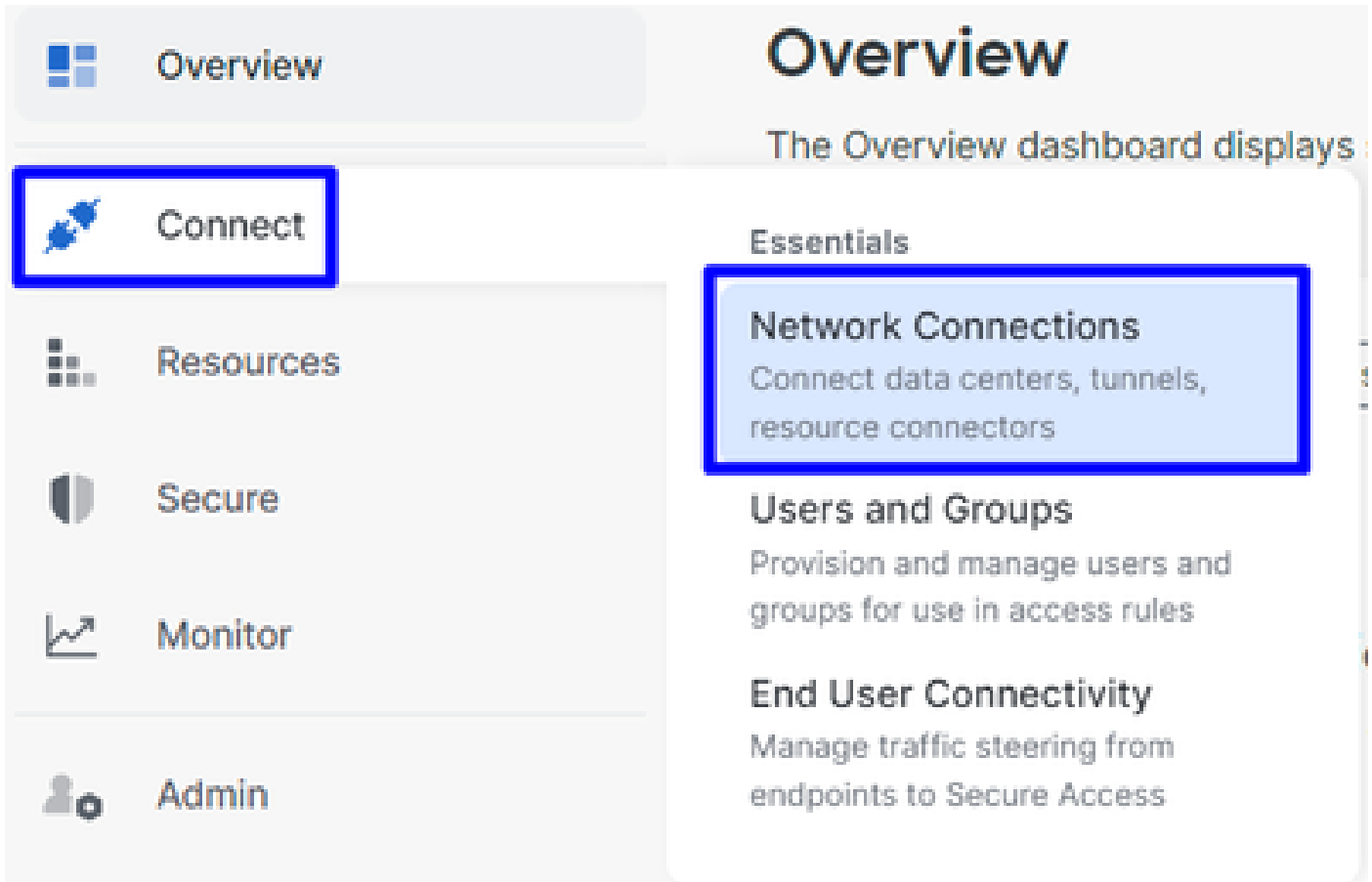
De tunnel op beveiligde toegang configureren

Navigeer naar het beheerderspaneel van [Secure Access](#).



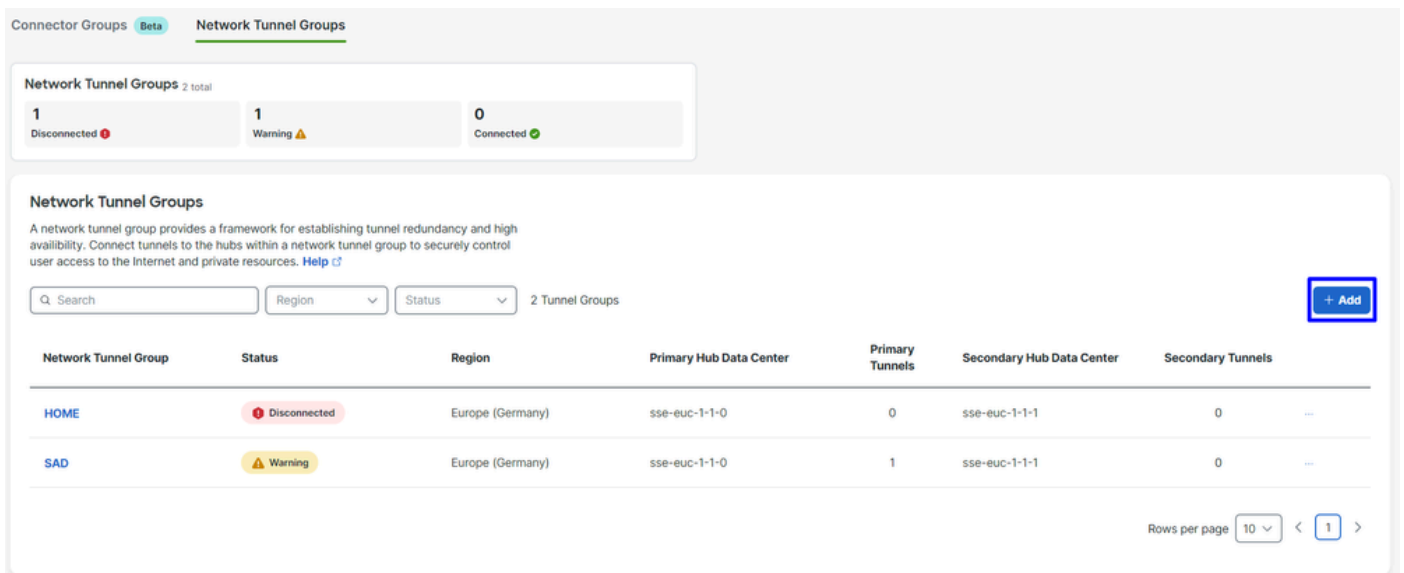
Secure Access - hoofdpagina

- **Klik op** Connect > Network Connections.



Secure Access - netwerkverbindingen

- Klik onder Network Tunnel Groups + Add op.



Secure Access - netwerktunnelgroepen

- Configureren Tunnel Group Name, Region en Device Typegebruiken.
- Klik op de knop . 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

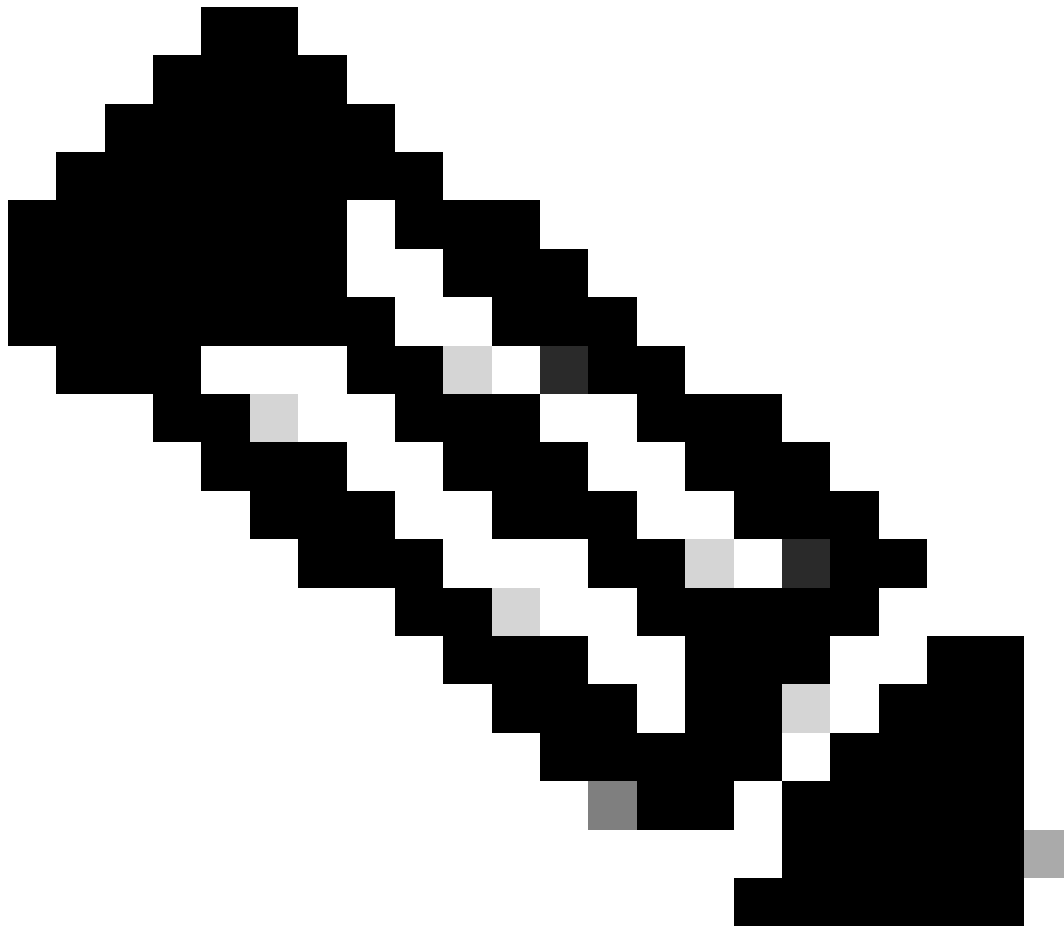
 ∨

### Device Type

 ∨

[Cancel](#)

[Next](#)



**Opmerking:** kies de regio die het dichtst bij de locatie van uw firewall ligt.

- 
- Configureer de instellingen Tunnel ID Format en Passphrase.
  - Klik op de knop .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

Secure Access - tunnelgroepen - tunnelid en wachtwoord

- Configureer het IP-adresbereik of de hosts die u op uw netwerk hebt geconfigureerd en u wilt het verkeer via Secure Access doorgeven.
- Klik op de knop . **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

Secure Access - tunnelgroepen - routingopties

Nadat u op **Save** de informatie over de tunnel wordt weergegeven, bewaar die informatie voor de volgende stap, **Configure the tunnel on Sophos**.



## Tunnelgegevens

### 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](#)

*Secure Access - tunnelgroepen - hervatting van configuratie*

De tunnel op Sophos configureren

IPsec-profiel configureren

Om het IPsec-profiel te configureren navigeer je naar de Sophos XG-firewall.

U verkrijgt iets gelijkaardigs:

**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)

**Web activity** 0 max | 0 avg  
Hits every 5 minutes

**Cloud applications**  
0 Apps | 0 B In | 0 B Out

**Allowed app categories** | **Network attacks**  
N/A | 0 | N/A | 0

**Allowed web categories** | **Blocked app categories**  
N/A | 0 | N/A | 0

**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** | **UTQ**  
0 Sources blocked | 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

Softwarepaneel - Beheerderspaneel

- Naar navigeren Profiles
- Klik op **IPsec Profiles** en klik daarna op Add

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

**Add** | **Delete**

**Manage**

algorithm

Phase 2

Onder **General Settings** configureren:

- **Name:** Een referentiernaam voor het Cisco Secure Access Policy
- **Key Exchange:** IKEv2
- **Authentication Mode:** Hoofdmodus
- **Key Negotiation Tries:**0
- **Re-Key connection:** Controleer de optie

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

Onder **Phase 1** configureren:

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

## 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 - IPsec-profielen - fase 1*

Onder **Phase 2** configureren:

- PFS group (DH group): Hetzelfde als fase-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 - IPsec-profielen - fase 2*

Onder **Dead Peer Detection** configureren:

- **Dead Peer Detection:** Controleer de optie
- **Check peer after every:**10
- **Wait for response up to:**120 (Standaard)
- **When peer unreachable:** Opnieuw initiëren (standaard)

## BEFORE

Dead Peer Detection

Dead Peer Detection

Check peer after every  Seconds

Wait for response up to  Seconds

When peer unreachable

## AFTER

Dead Peer Detection

Check peer after every  Seconds

Wait for response up to  Seconds

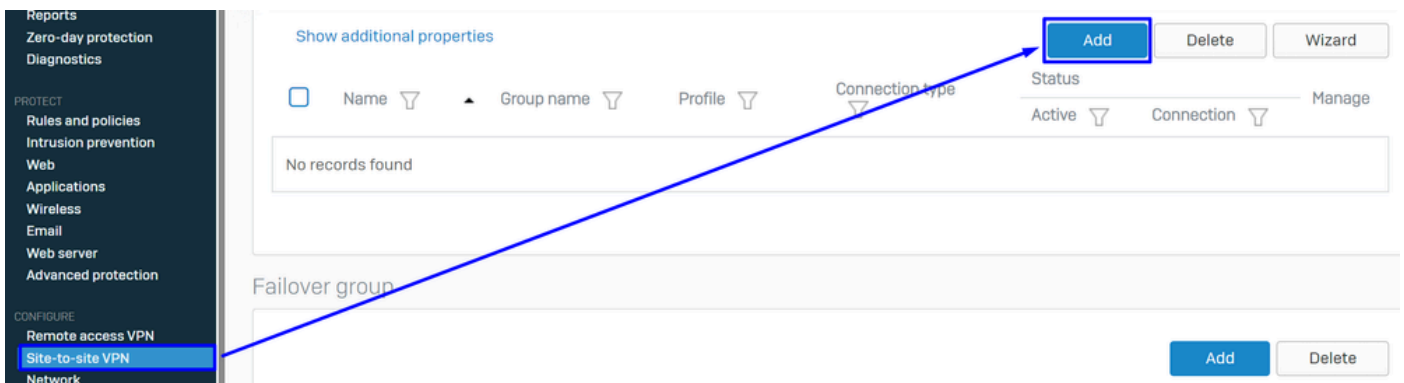
When peer unreachable

*Sophos - IPsec-profielen - detectie van dode peers*

Klik daarna op **Save** and proceed with the next step, Configure Site-to-site VPN.

Site-to-site VPN configureren

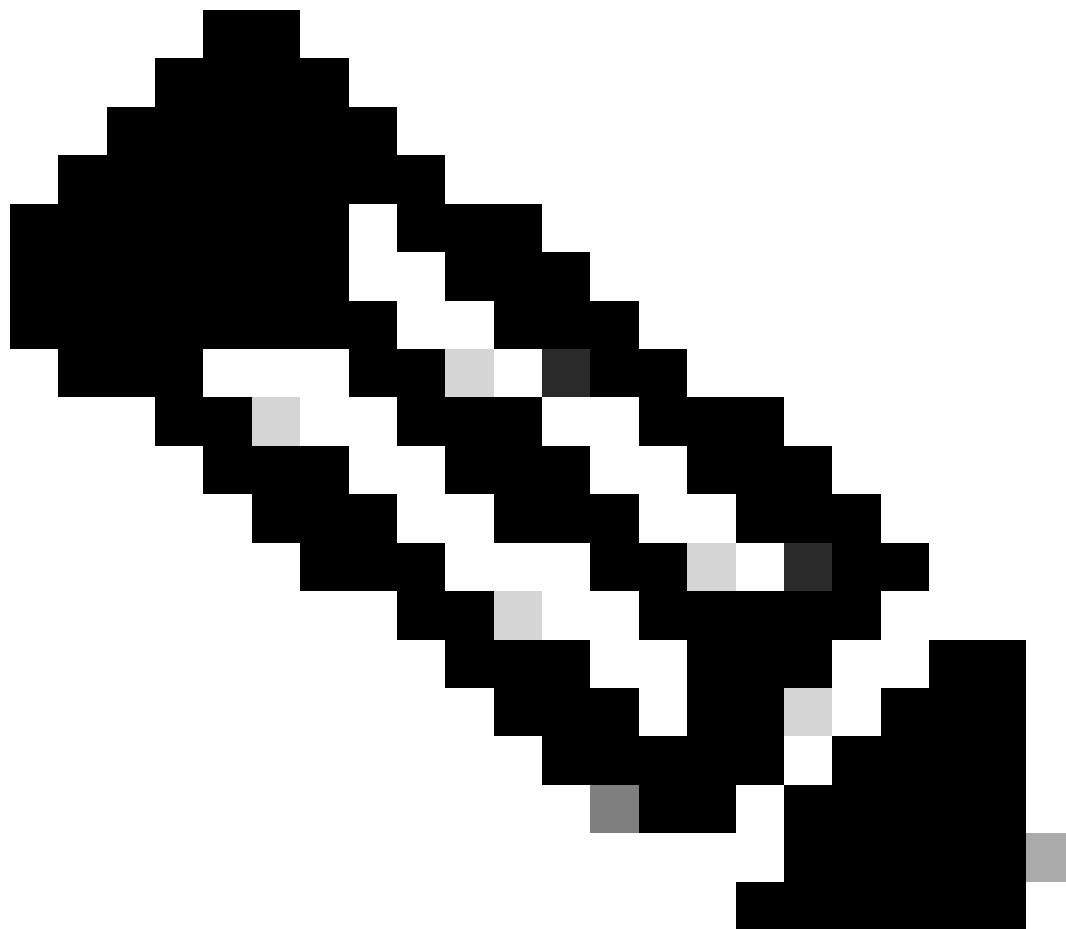
Om de configuratie van VPN te initiëren, klik op **Site-to-site VPN** en klik op **Add**.



*Sophos - Site-to-site VPN*

Onder **General Settings** configureren:

- **Name:** Een referentienaam voor het Cisco Secure Access IPsec-beleid
- IP version: IPv4
- Connection type: Tunnelinterface
- Gateway type: Verbinding starten
- Active on save: Controleer de optie



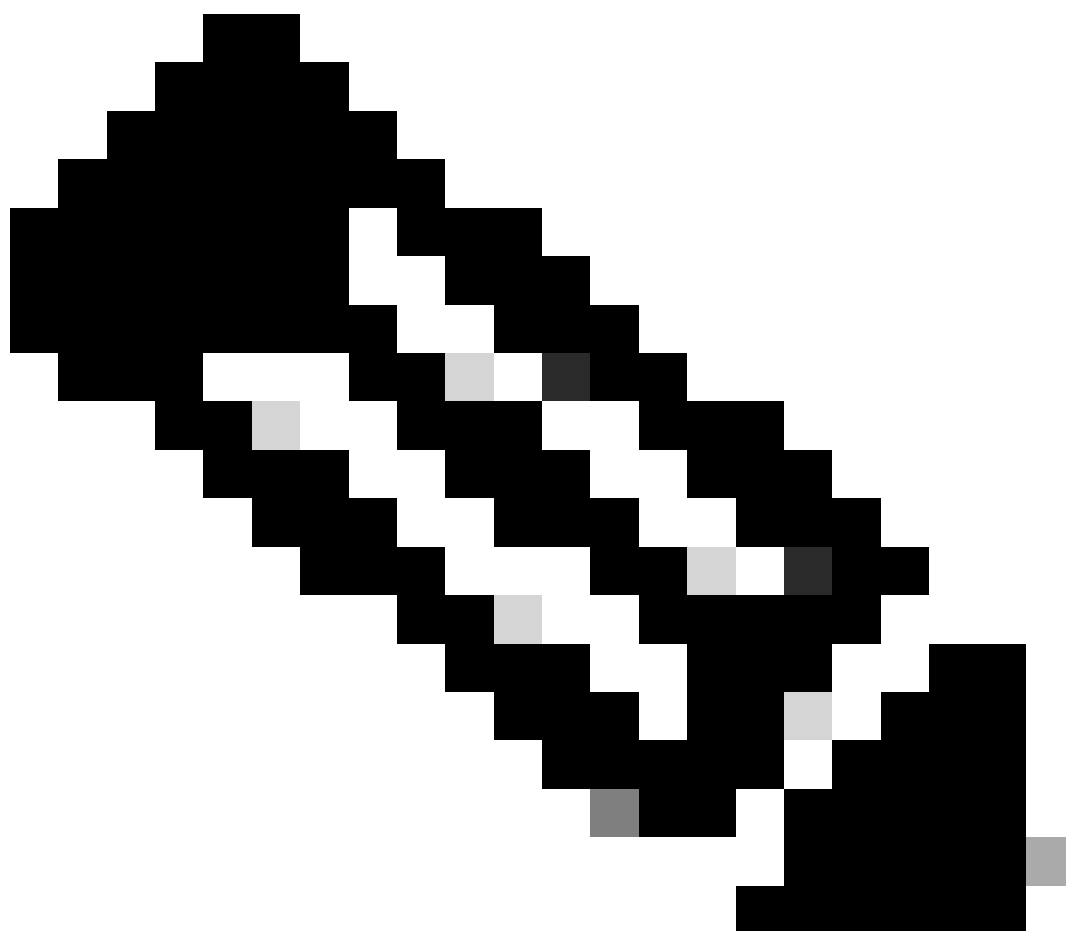
**Opmerking:** de optie **Active on save** schakelt de VPN automatisch in nadat u de site-to-site VPN hebt geconfigureerd.

---

## 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 - Site-to-site VPN - Algemene instellingen



**Opmerking:** de optie Tunnel interface maakt een virtuele tunnelinterface voor de Sophos XG Firewall met de naam XFRM.

Onder **Encryption** configureren:

- **Profile:** Het profiel dat u op de stap maakt, **Configure IPsec Profile**
- **Authentication type:** Preshared sleutel
- **Preshared key:** De toets die u instelt op de stap, [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key:** Preshared key

### Encryption

<b>Profile</b> CSA	<b>Authentication type</b> Preshared key
	<b>Preshared key</b> .....
	<b>Repeat preshared key</b> .....

Sophos - Site-to-site VPN - Encryptie

Gebruik onder **Gateway Settings** Configure Local Gateway and Remote Gateway Options deze tabel als referentie.

Lokale gateway	Externe gateway
Luisterinterface Uw WAN-internetinterface	Gatewayadres Het openbare IP dat tijdens de stap wordt gegenereerd, <a href="#">Tunnel Data</a>
Type plaatselijke id Email	Type Remote-id



	IP-adres
Lokale id De e-mail die onder de stap is gegenereerd, <a href="#">Tunnel Data</a>	Remote-id Het openbare IP dat tijdens de stap wordt gegenereerd, <a href="#">Tunnel Data</a>
Lokale subnetverbinding Alle	Remote-subnet Alle

## 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"/>
<input type="button" value="Add new item"/>	<input type="button" value="Add new item"/>

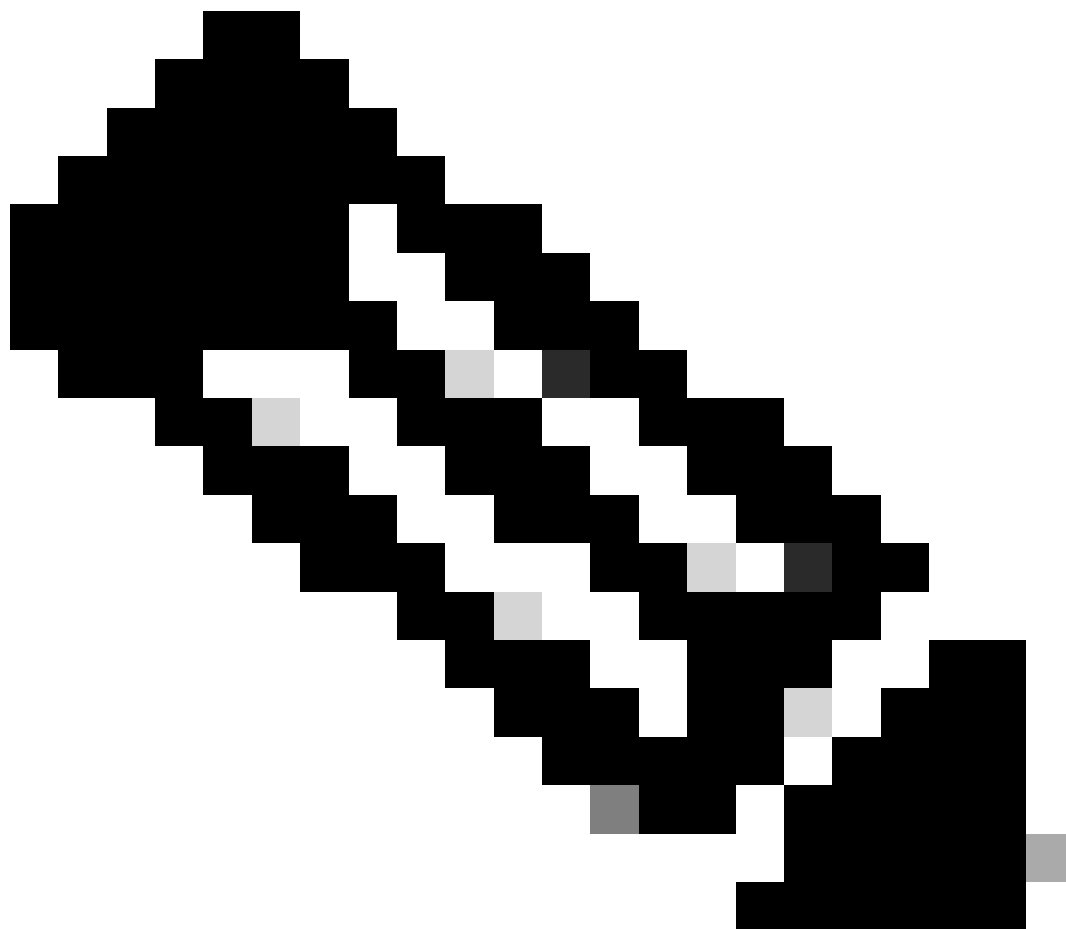
Sophos - Site-to-site VPN - Gateway-instellingen

Daarna klik je op **Save**, en je kunt zien dat de tunnel gemaakt is.

## IPsec connections

Show additional properties							<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Wizard"/>
<input type="checkbox"/>	Name	Group name	Profile	Connection type	Status	Connection	Manage		
					Active				
<input type="checkbox"/>	SecureAccesS	-	CSA	Tunnel interface	<span style="color: green;">●</span>	<span style="color: green;">●</span> <input type="button" value="i"/>	<input type="button" value="edit"/>	<input type="button" value="stop"/>	<input type="button" value="trash"/>

Snoop - Site-to-site VPN - IPsec-verbindingen



**Opmerking:** Om te controleren of de tunnel op de laatste afbeelding correct is ingeschakeld, kunt u de **Connection** status controleren, als deze groen is, wordt de tunnel aangesloten als deze niet groen is.

---

Om te controleren of er een tunnel is geopend, gaat u naar **Current Activities > IPsec Connections**.

MONITOR & ANALYZE

# Control center


Current activities

Reports

Zero-day protection

Diagnostics

*Sophos - Monitor en 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	

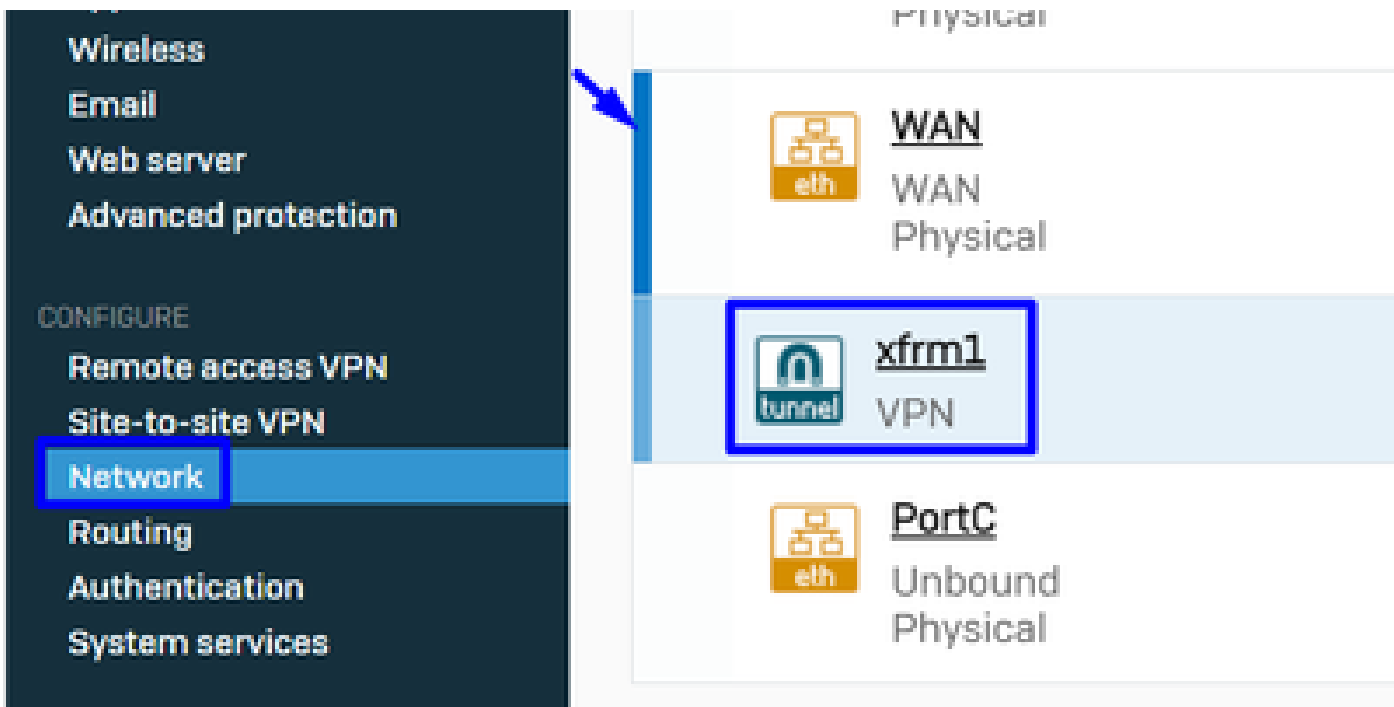
*Sophos - Monitor en Analyse - IPsec voor en na*

Daarna kunnen we doorgaan met de stap, **Configure Tunnel Interface Gateway**.

Tunnelinterface configureren

Navigeer naar **Network** en controleer uw WAN interface die is geconfigureerd op VPN om de virtuele tunnelinterface met de naam te bewerken xfrm.

- Klik op **xfrm** de interface.



Sophos - netwerk - tunnelinterface

- Configureer de interface met een IP niet-routable in uw netwerk, bijvoorbeeld, kunt u 169.254.x.x/30 gebruiken die een IP is in een niet-routable ruimte meestal, in ons voorbeeld gebruiken wij 169.254.0.1/30

### General settings

Name *	<input type="text" value="xfrm1"/>
Hardware	xfrm1
IPsec connection	SecureAccess
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 - Network - Tunnel Interface - configuratie

### De gateways configureren

Zo configureert u de gateway voor de virtuele interface (xfrm)

- Naar navigeren Routing > Gateways
- Klik op de knop Add

The screenshot shows the Sophos management console interface. On the left is a dark sidebar with navigation options under 'PROTECT' (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced protection) and 'CONFIGURE' (Remote access VPN, Site-to-site VPN, Network, Routing). The 'Routing' option is highlighted. The top navigation bar includes tabs for SD-WAN routes, SD-WAN profiles, Gateways (selected), Static routes, BGP, OSPF, OSPFv3, Information, and Upstream proxy. The main content area is titled 'IPv4 gateway' and 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	<span style="color: red;">●</span>	

Sophos - routing - gateways

Onder **Gateway host** configureren:

- **Name:** Een naam die verwijst naar de virtuele interface die voor VPN is gemaakt
- **Gateway IP:** In ons geval 169.254.0.2, dat is het IP onder het netwerk 169.254.0.1/30 dat wij reeds onder de stap hebben toegewezen, Configure Tunnel Interface
- InterfaceVPN virtuele interface
- **Zone:** Geen (standaard)

The screenshot shows the 'Gateway host' configuration form. The fields are as follows:

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

Sophos - Routing - Gateways - Gateway-host

- Schakel onder **Health check** Uitschakelen
- Klik op de knop **Save**

# Health check

Health check



*Sophos - Routing - Gateways - gezondheidscontrole*

U kunt de status van de gateway waarnemen nadat u de configuratie hebt opgeslagen:

## 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		

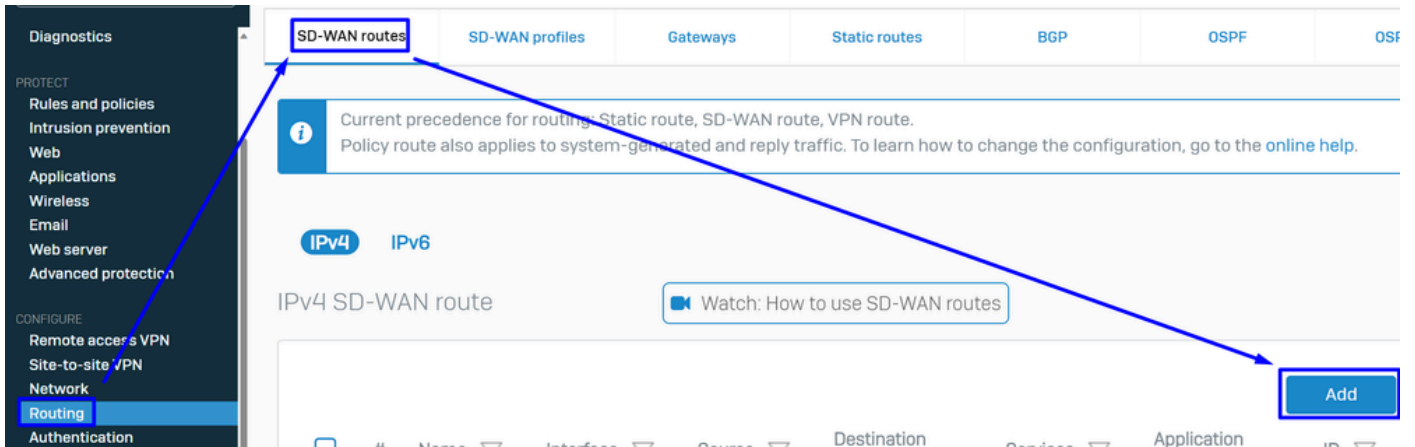
*Sophos - Routing - Gateways - status*

De SD-WAN router configureren

Om het configuratieproces te voltooien, moet u de route creëren die u toelaat om het verkeer door te sturen naar Secure Access.

Naar navigeren **Routing > SD-WAN routes**.

- Klik op **Add**



Sophos - SD-WAN routers

Onder **Traffic Selector** configureren:

- **Incoming interface:** Selecteer de interface van waar u het verkeer of de gebruikers wilt verzenden die van RA-VPN, ZTNA, of Clientless-ZTNA toegang hebben
- **DSCP marking:** Niets voor dit voorbeeld
- **Source networks:** Selecteer het adres dat u door de tunnel wilt leiden
- **Destination networks:** Om het even welk of u kunt een bestemming specificeren
- **Services:** Om het even welk of u kunt de diensten specificeren
- **Application object:** Een toepassing als u het object geconfigureerd hebt
- **User or groups:** Als u een specifieke groep gebruikers wilt toevoegen om het verkeer naar Secure Access te leiden

### 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 - SD-WAN routers - Traffic Selector

Onder **Link selection settings** configureer de gateway:

- **Primary and Backup gateways:** Controleer de optie

- **Primary gateway:** Selecteer de gateway die onder de stap is geconfigureerd, [Configure the Gateways](#)
- Klik op **Save**

Link selection settings

Select SD-WAN profile ⓘ  Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

*Sophos - SD-WAN routers - Traffic Selector - Primaire en back-upgateways*

Nadat u de configuratie op de Sophos XG Firewall hebt voltooid, kunt u doorgaan met de stap, **Configure Private App**.

Privé-app configureren

Meld u aan bij het [Admin Portal](#) om de Private App-toegang te configureren.

- Naar navigeren **Resources > Private Resources**



The image shows the navigation menu on the left with the following items: Overview, Connect, Resources (highlighted with a blue box), Secure, Monitor, Admin, and Workflows. The main content area is titled "Private Resources" and contains a description: "Private Resources are applications, r resource using zero-trust access. Ho". Below this, there are two tabs: "Private Resources" (selected) and "Private F". A white panel on the right lists several categories, with "Private Resources" highlighted by a blue box. The categories listed are: Sources and destinations, Private Resources (with description: "Define internal applications and other resources for use in access rules"), Registered Networks (with description: "Point your networks to our servers"), Internal Networks (with description: "Define internal network segments to use as sources in access rules"), Internet and SaaS Resources (with description: "Define destinations for internet access rules"), and Roaming Devices (with description: "Mac and Windows").

Secure Access - particuliere bronnen

- Klik op + Add

The image shows the "Private Resources" table in the Secure Access console. At the top, there are tabs for "Private Resources" (selected) and "Private Resource Groups". Below the tabs, there is a search bar "Q Search by resource name", a dropdown for "Private Resource Group", a dropdown for "Connection Method", and a count "4 Private Resources". A blue "+ Add" button is located on the right. A date filter "Last 24 Hours" is also present. The table has the following columns: Private Resource, Private Resource Group, Connection Method, Accessed by, Rules, and Total Requests.

Secure Access - particuliere bronnen 2

- Onder **General** Configureren **Private Resource Name**

## General

### Private Resource Name

SplunkSophos

### Description (optional)

*Beveiligde toegang - particuliere bronnen - algemeen*

Onder **Communication with Secure Access Cloud** configureren:

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR):** Selecteer de resource die u wilt openen



**Opmerking:** Onthoud dat het intern bereikbare adres is toegewezen op de stap, [Configure the Tunnel on Secure Access](#).

- 
- **Protocol:** Selecteer het protocol dat u gebruikt om toegang te krijgen tot die bron
  - **Port / Ranges :** Selecteer de poorten die u nodig hebt om toegang te krijgen tot de app

## 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

*Secure Access - Private Resources - Communicatie met Secure Access Cloud*

Binnen **Endpoint Connection Methods**, vormt u alle manieren mogelijk om tot privé middelen via Veilige Toegang toegang te hebben, en kiest de methodes die u voor uw milieu wilt gebruiken:

- **Zero-trust connections:** Schakel het vakje in om ZTNA-toegang in te schakelen.
  - **Client-based connection:** Schakel de knop in om client base ZTNA toe te laten
    - **Remotely Reachable Address:** Het IP-adres van uw privé-app configureren
  - **Browser-based connection:** Schakel de knop in om op de browser gebaseerde ZTNA toe te staan
    - **Public URL for this resource:** Voeg een naam toe om te gebruiken in combinatie met het domein `ztna.sse.cisco.com`
      - **Protocol:** Kies HTTP of HTTPS als een protocol voor toegang via de browser
- **VPN connections:** Vink het vakje aan om RA-VPN Access in te schakelen.
- Klik op de knop **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

Secure Access - Private Resources - Communicatie met Secure Access Cloud 2

Nadat de configuratie is voltooid, is dit het resultaat:

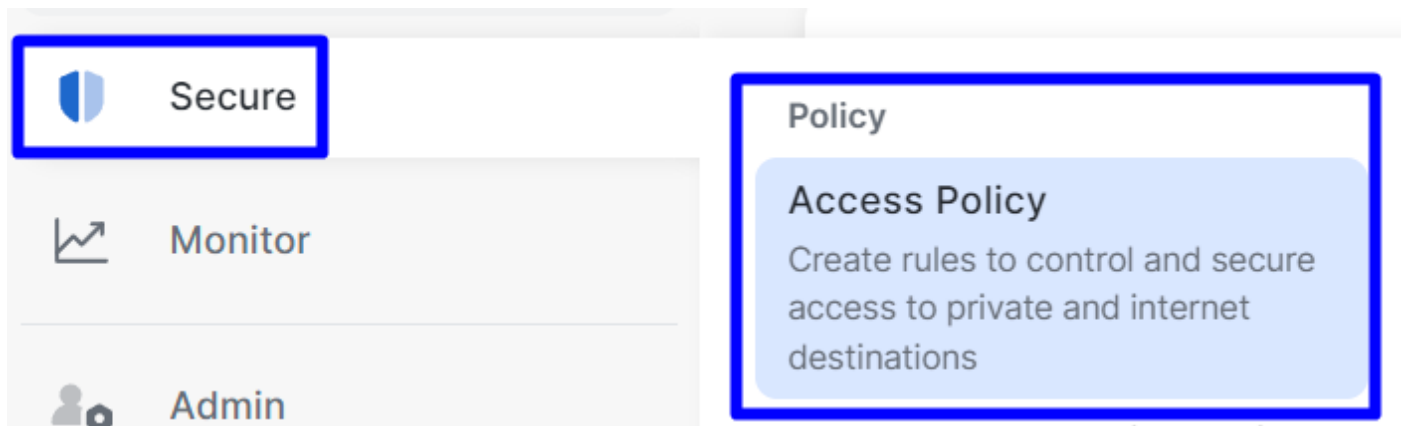
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests	
SplunkSophos	-	<ul style="list-style-type: none"><li>VPN</li><li>Browser-based ZTNA</li><li>Client-based ZTNA</li></ul>	1	2	16	...

Secure Access - geconfigureerd voor privé-bronnen

Nu kunt u doorgaan met de stap, **Configure the Access Policy**.

Het toegangsbeleid configureren

Om het toegangsbeleid te configureren navigeer je naar Secure > Access Policy.



*Secure Access - toegangsbeleid*

- Klik op de knop **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

*Secure Access - toegangsbeleid - privé-toegang*

Configureer de volgende opties om toegang te bieden via meerdere verificatiemethoden:

- 1. Specify Access
  - Action: Allow (toestaan)
    - **Rule name:** Geef een naam op voor uw toegangsregel
    - **From:** De gebruikers die u toegang verleent tot
    - **To:** De toepassing die u toegang wilde verlenen
    - Endpoint Requirements: (standaard)
- Klik op de knop **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

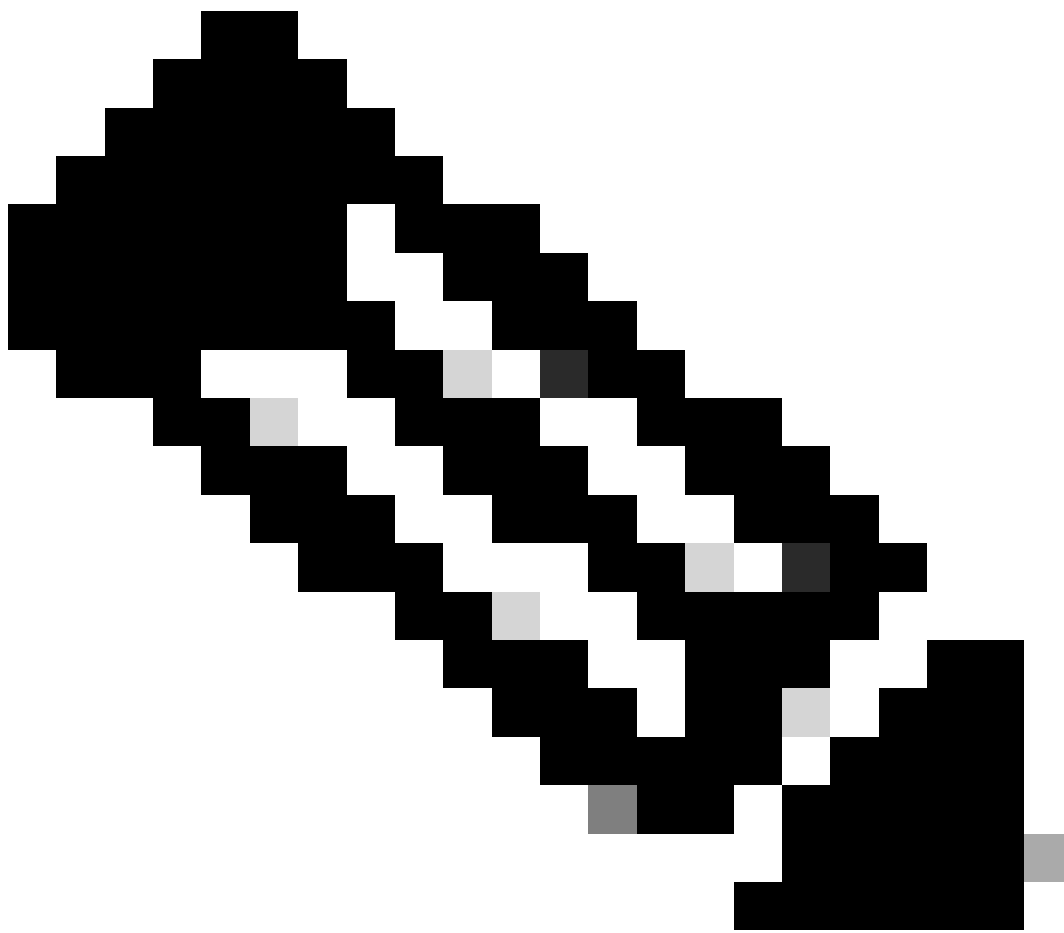
Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

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

Private Resources: **SplunkSophos**

Secure Access - toegangsbeleid - toegang opgeven





**Opmerking:** voor de stap **2. Configure Security** die u moet uitvoeren, maar in dit geval hebt u de **Intrusion Prevention (IPS)**, of **Tenant Control Profiel** niet ingeschakeld.

- Klik Save en je hebt:

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

*Secure Access - geconfigureerd toegangsbeleid*

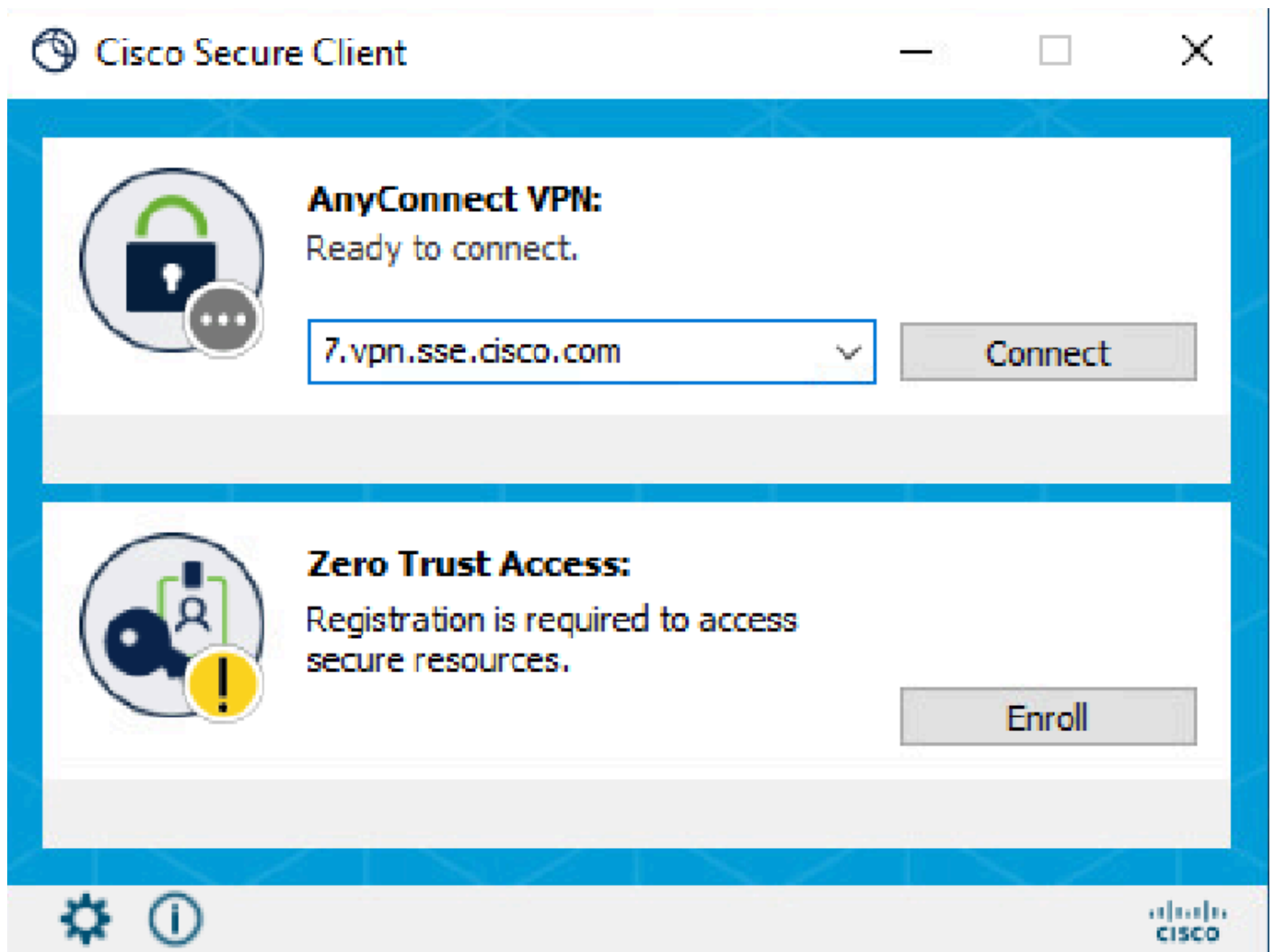
Daarna kunt u doorgaan met de stap Verify.

Verifiëren

Om de toegang te verifiëren moet u de agent van Cisco Secure Client hebben geïnstalleerd die u kunt downloaden van [Software Download - Cisco Secure Client](#).

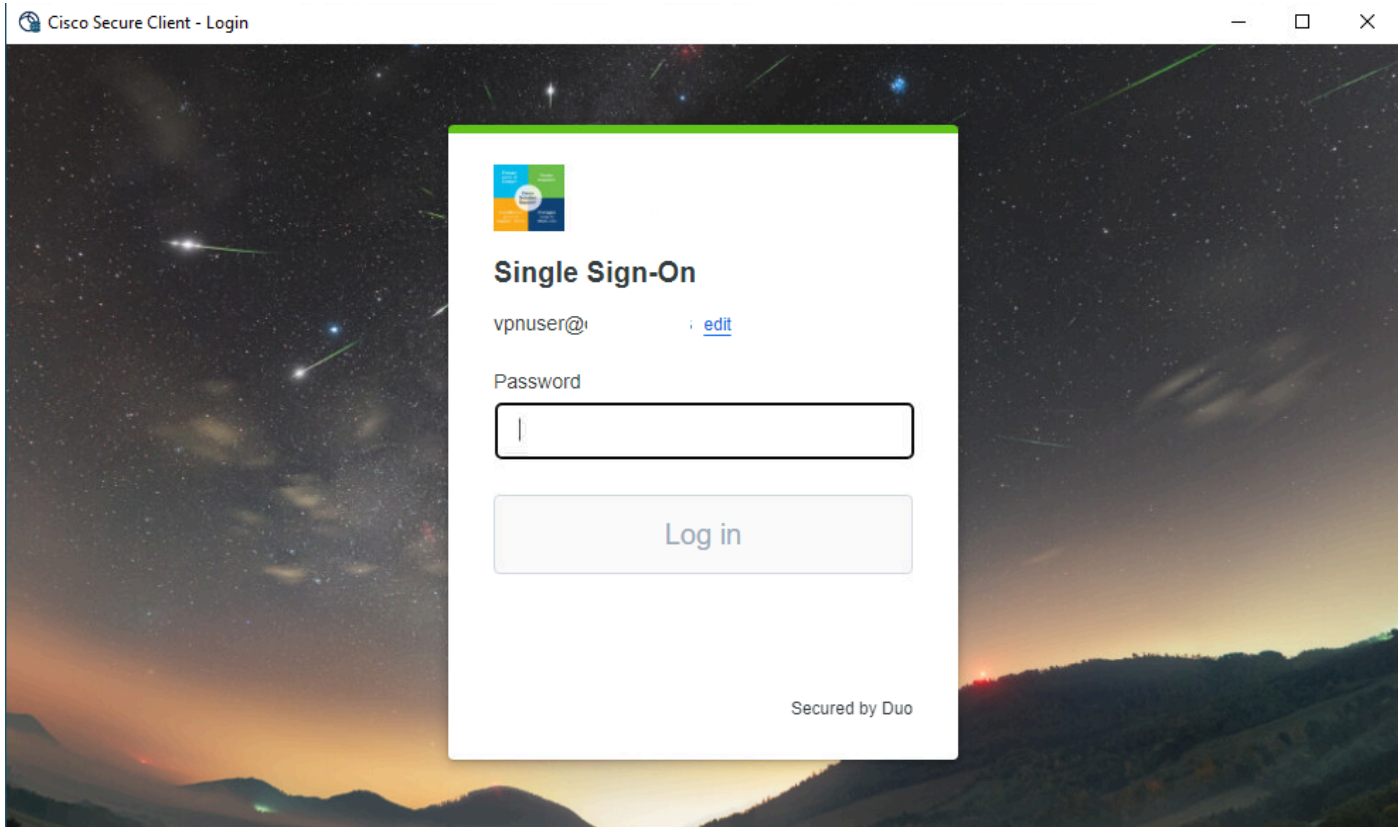
RA-VPN

Aanmelden via Cisco Secure Client Agent-VPN.



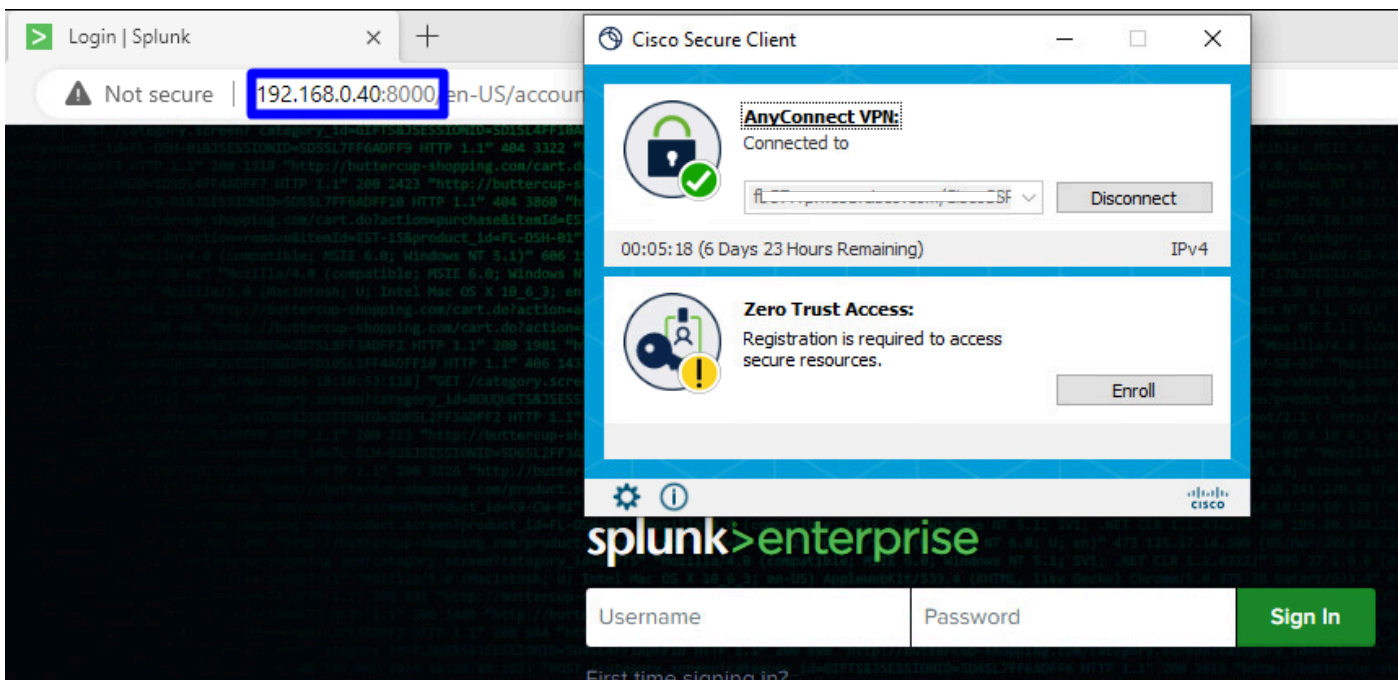
*Beveiligde client - VPN*

- Verifiëren via uw SSO-provider



Secure Access - VPN - SSO

- Nadat u wordt geverifieerd, toegang tot de bron:



Secure Access - VPN - geverifieerd

Navigeer naar 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

Beveiligde toegang - Zoeken naar activiteiten - RA-VPN

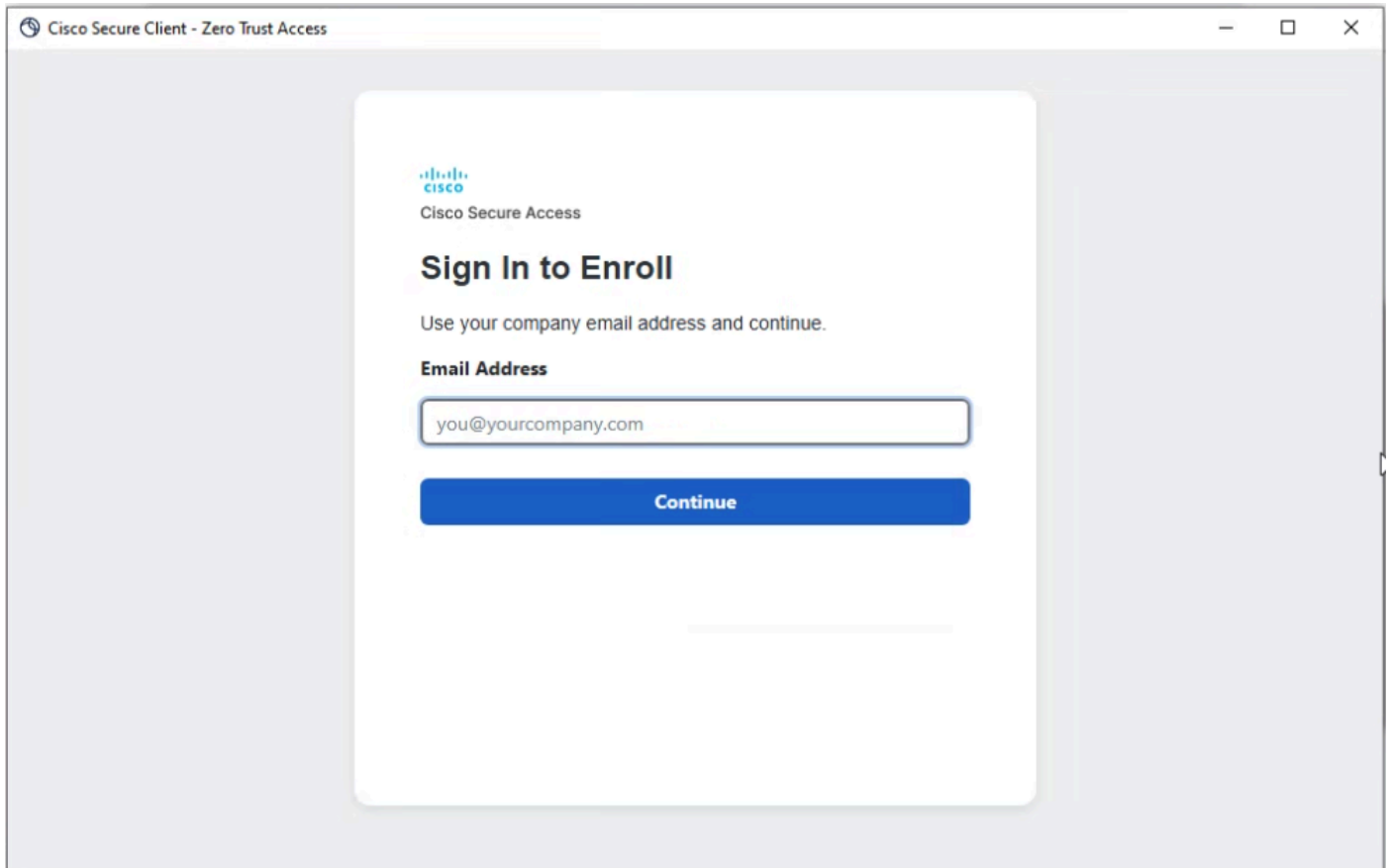
Je kunt zien dat de gebruiker toestemming heeft gekregen om te authenticeren via RA-VPN.

Op client gebaseerde ZTNA

Aanmelden via Cisco Secure Client Agent - ZTNA.

Secure-client - ZTNA

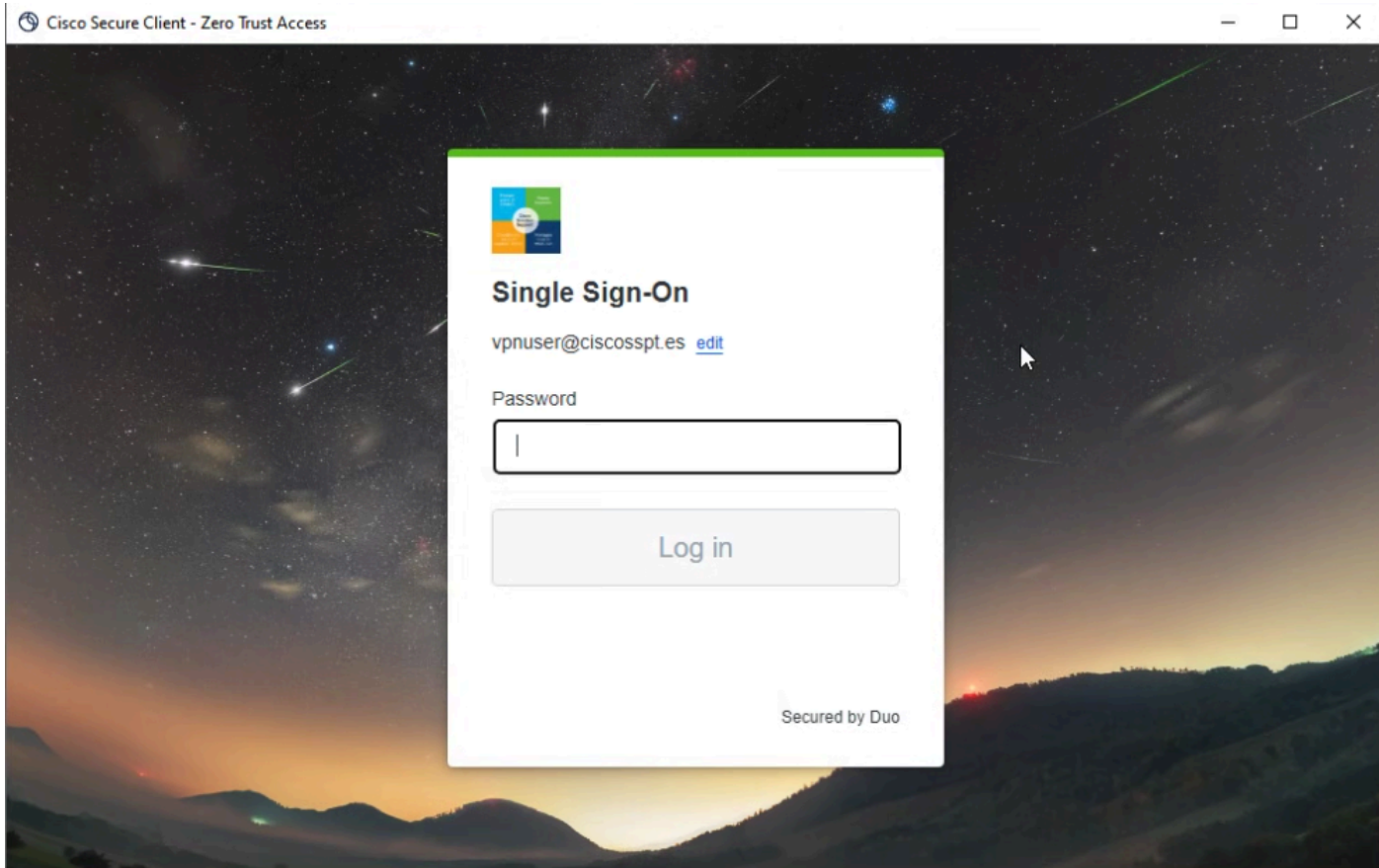
- Schrijf je in met je gebruikersnaam.



*Secure-client - ZTNA - inschrijven*

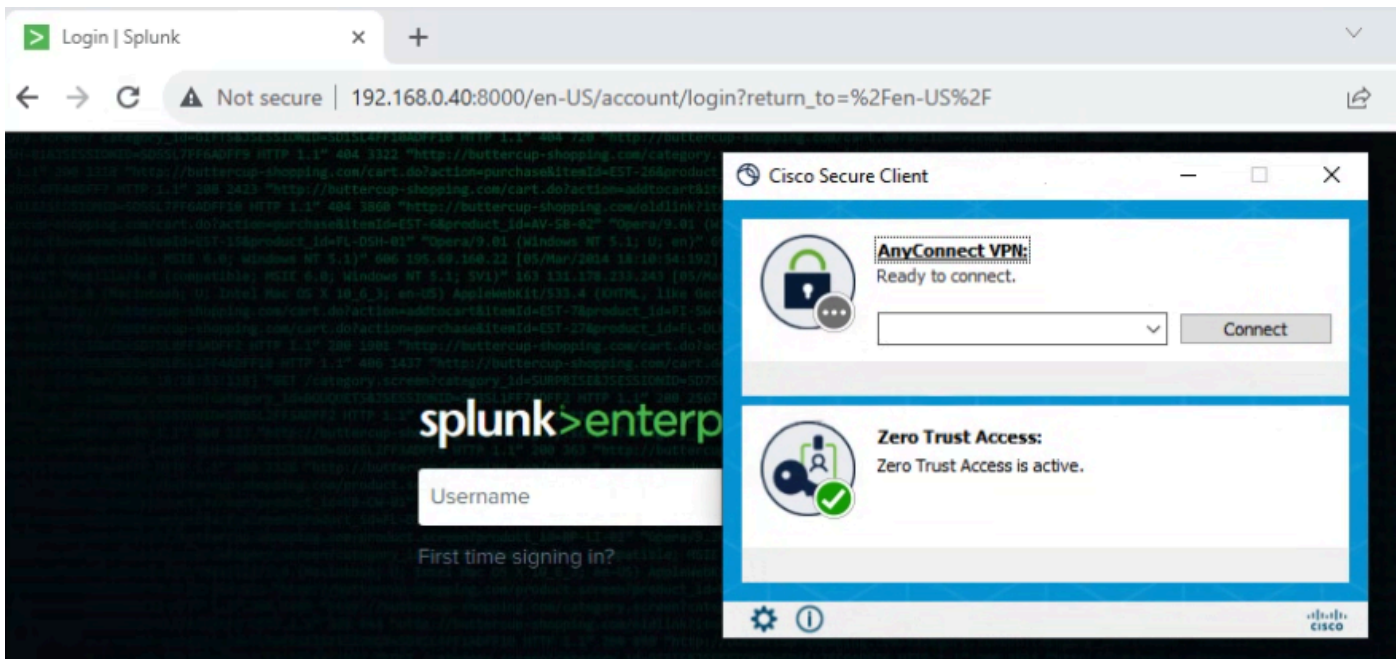
- Verifiëren in uw SSO-provider





Secure-client - ZTNA - SSO-aanmelding

- Nadat u wordt geverifieerd, toegang tot de bron:



Secure Access - ZTNA - vastlegging

Navigeer naar Monitor > Activity Search:



The screenshot shows the Splunk Sophos interface. On the left is a navigation sidebar with four items: 'Resources' (with a grid icon), 'Secure' (with a shield icon), 'Monitor' (with a line graph icon), and 'Admin' (with a person icon). The main content area is titled 'Sources and destinations' and contains two sections: 'Private Resources' (highlighted with a blue border) and 'Registered Networks'. The 'Private Resources' section includes the text 'Define internal applications and other resources for use in access rules'. The 'Registered Networks' section includes the text 'Point your networks to our servers'.

Secure Access - privé-bron

- Klik op uw beleid

The screenshot shows a table with one row. The first column contains the text 'SplunkSophos', which is highlighted with a blue arrow pointing to it from the right. The second column contains a hyphen '-'. To the right of the table is a filter menu with three options: 'Client-based ZTNA' (light blue), 'Browser-based ZTNA' (light purple), and 'VPN' (pink). The number '1' is displayed to the right of the filter menu.

Secure Access - privé-bron - SplunkSophos

- Omlaag scrollen



# SplunkSophos

Client-based ZTNA

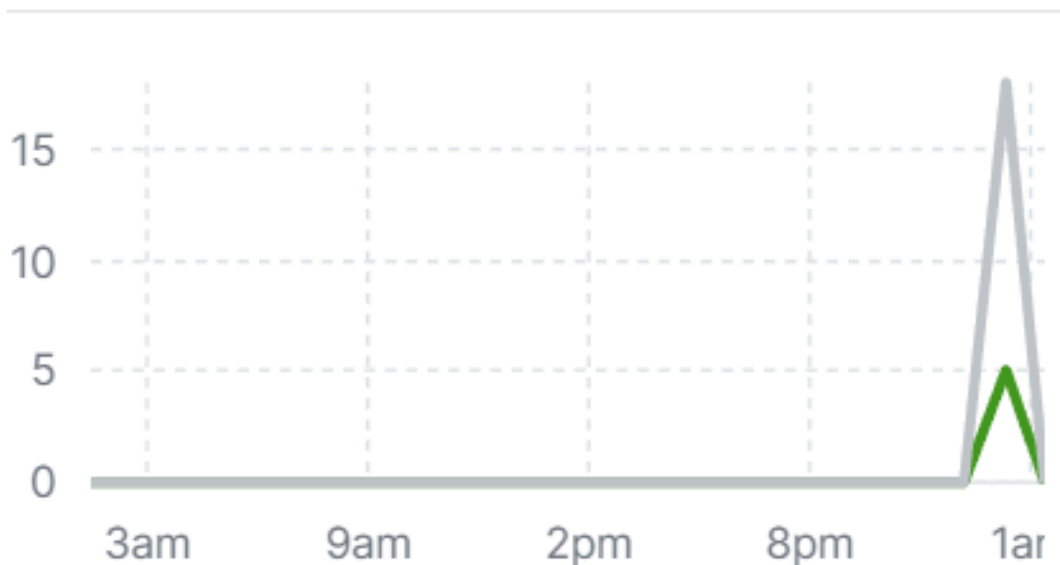
Browser-based ZTNA



VPN

Total Requests

**23** ↗ 44% from previous 24 hours



## TOTAL REQUESTS BY STATUS

### Status

✓	Success	5
⊘	Blocked	18



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.