

# Configuración del acceso seguro con el firewall Sophos XG

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración del túnel en Secure Access](#)

[Datos del túnel](#)

[Configuración del túnel en Sophos](#)

[Configurar perfil IPsec](#)

[Configuración de VPN de sitio a sitio](#)

[Configurar interfaz de túnel](#)

[Configuración de las puertas de enlace](#)

[Configuración de la ruta SD-WAN](#)

[Configurar aplicación privada](#)

[Configuración de la política de acceso](#)

[Verificación](#)

[VPN de RA](#)

[ZTNA de base cliente](#)

[ZTNA basado en navegador](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar Secure Access con Sophos XG Firewall.

## Prerequisites

- [Configurar aprovisionamiento de usuarios](#)
- [Configuración de Autenticación SSO de ZTNA](#)
- [Configurar acceso seguro VPN de acceso remoto](#)

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall Sophos XG
- Acceso seguro

- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA
- ZTNA sin cliente

## Componentes Utilizados

La información de este documento se basa en:

- Firewall Sophos XG
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes



**CISCO**

Secure

Access

**SOPHOS**

Acceso seguro: Sophos

Cisco ha diseñado Secure Access para garantizar la protección y la provisión de acceso a aplicaciones privadas, tanto en las instalaciones como en la nube. También protege la conexión de la red a Internet. Esto se consigue mediante la implementación de varios métodos y capas de seguridad, todo ello con el objetivo de preservar la información a medida que acceden a ella a

través de la nube.

# Configurar

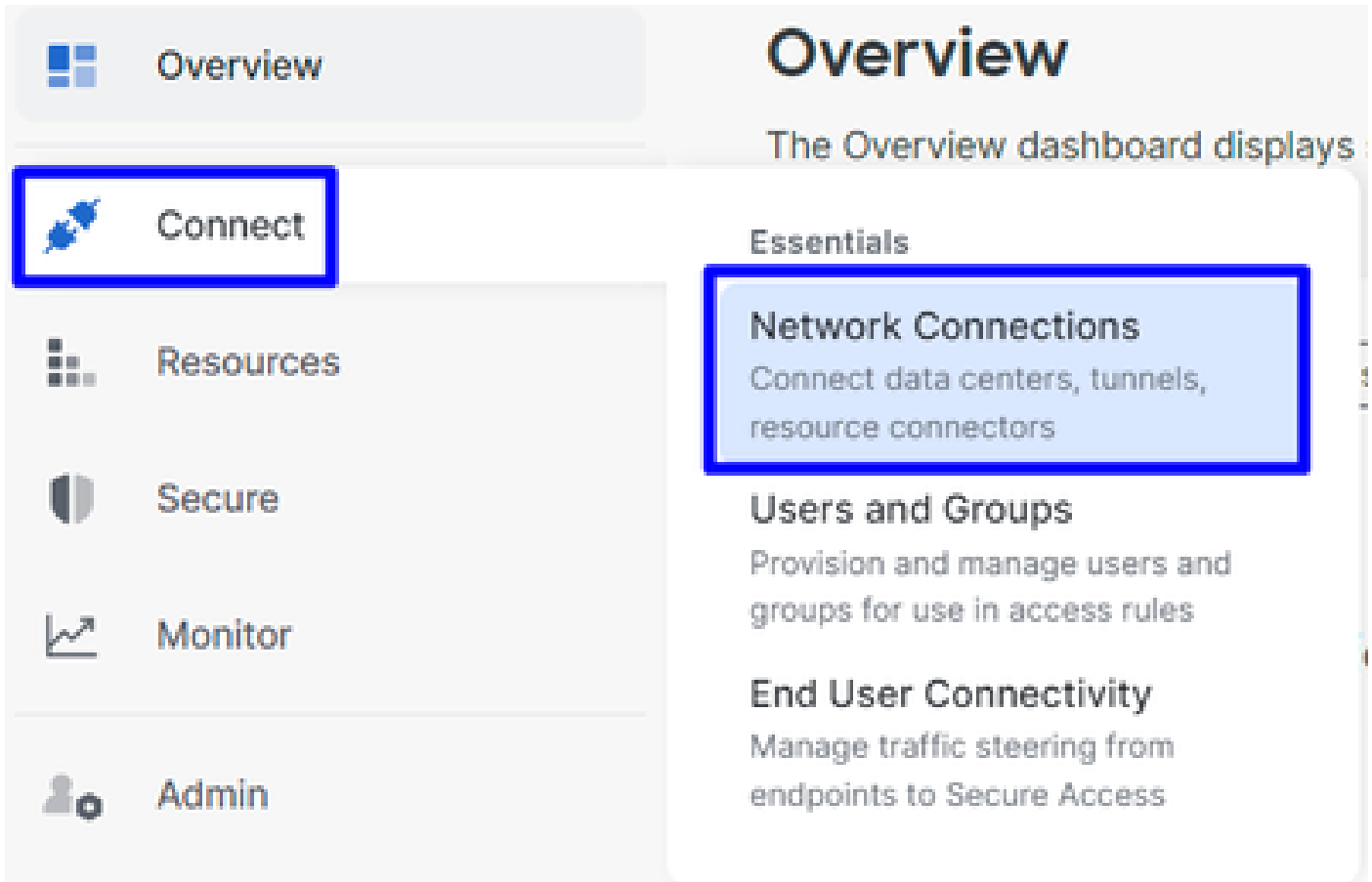
## Configuración del túnel en Secure Access

Vaya al panel de administración de [Secure Access](#).



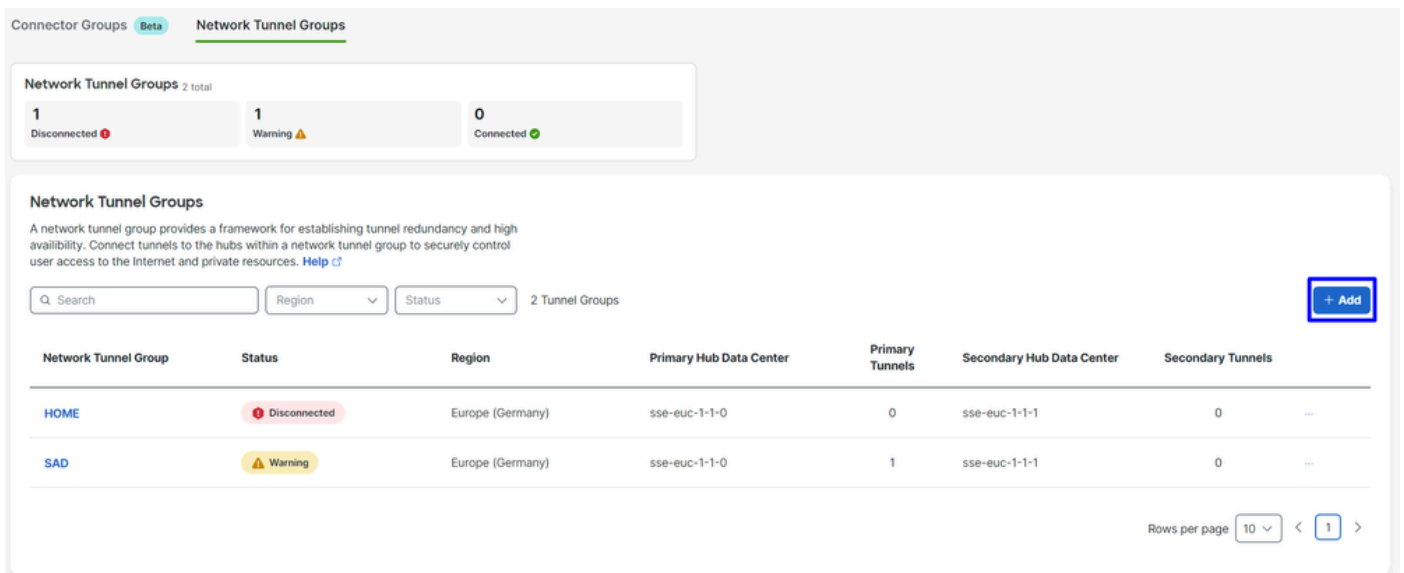
Acceso seguro - Página principal

- Haga clic en **Connect > Network Connections**.



Acceso seguro - Conexiones de red

- En Network Tunnel Groups haga clic en + Add.



Acceso seguro - Grupos de túnel de red

- Configure Tunnel Group Name, Region y Device Type.
- Haga Next clic.

## 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

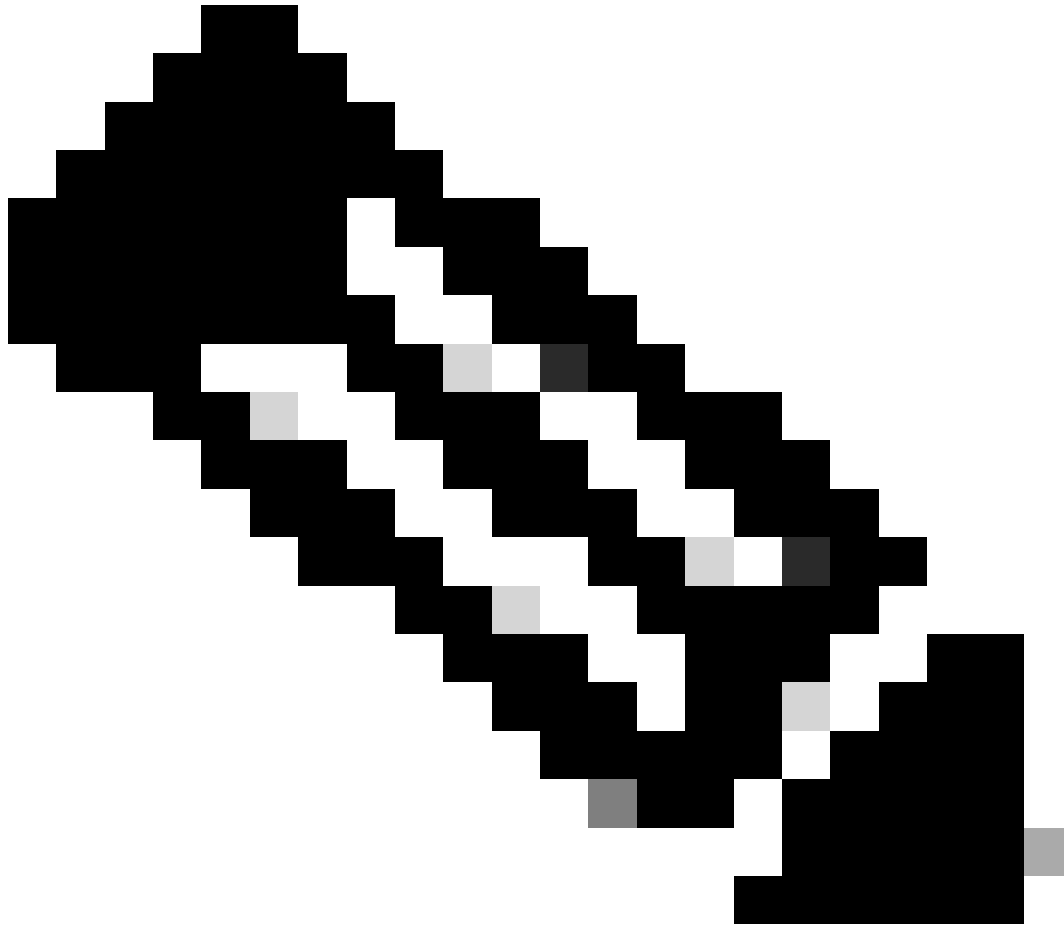
 ∨

### Device Type

 ∨

[Cancel](#)

[Next](#)



**Nota:** Seleccione la región más cercana a la ubicación del firewall.

- 
- Configure el Tunnel ID Format y Passphrase.
  - Haga clic en 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

Acceso seguro - Grupos de túnel - ID de túnel y frase de paso

- Configure los rangos de direcciones IP o los hosts que ha configurado en la red y que desea que el tráfico pase a través de Secure Access.
- Haga clic en **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

Acceso seguro - Grupos de túnel - Opciones de routing

Después de hacer clic en **Save** la información sobre el túnel se muestra, guarde esa información para el siguiente paso, **Configure the tunnel on Sophos**.



## Datos del túnel

### 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](#)

*Acceso seguro - Grupos de túnel - Reanudación de la configuración*

Configuración del túnel en Sophos

Configurar perfil IPsec

Para configurar el perfil IPsec, navegue hasta el firewall Sophos XG.

Se obtiene algo similar a esto:

**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**

**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 [Click here](#)

**Synchronized Application Control™**  
0 Apps Identify unknown apps on your network [Click here](#)

**Zero-day protection**  
0 Recent 0 Incidents 0 Scanned

**ATP** **UTQ**  
0 Sources blocked 0 Accounts at risk [Configure](#)

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

Click on widgets to open details

Sophos - Panel de administración

- Desplácese hasta **Profiles**
- Haga clic en **IPsec Profiles** y después haga clic en **Add**

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

**Add** **Delete**

**Manage**

algorithm

Phase 2

En **General Settings** configurar:

- **Name:** un nombre de referencia a la política de acceso seguro de Cisco
- **Key Exchange:** IKEv2
- **Authentication Mode:** Modo principal
- **Key Negotiation Tries:**0
- **Re-Key connection:** Marque la opción

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

Sophos - Perfiles IPsec - Configuración general

En **Phase 1** configurar:

- **Key Life:**28800
- **DH group(key group):** Seleccione 19 y 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"/>	Re-key margin 360 <input checked="" type="checkbox"/>	Randomize re-keying margin by 50 <input checked="" type="checkbox"/>
Seconds		Seconds
DH group (key group) 2 selected <input checked="" type="checkbox"/>		
Encryption AES256 <input checked="" type="checkbox"/>	Authentication SHA2 256 <input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> You can add up to 3 different algorithm combinations		

*Sophos - Perfiles IPsec - Fase 1*

En **Phase 2** configurar:

- PFS group (DH group): igual que en la 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"/>
<input checked="" type="checkbox"/> You can add up to 3 different algorithm combinations	

*Sophos - Perfiles IPsec - Fase 2*

En **Dead Peer Detection** configurar:

- **Dead Peer Detection:** Marque la opción
- **Check peer after every:**10
- **Wait for response up to:**120 (Default)
- **When peer unreachable:** Reiniciar (predeterminado)

## 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 - Perfiles IPsec - Detección de puntos inactivos*

Después de eso, haga clic en **Save** and proceed with the next step, Configure Site-to-site VPN.

Configuración de VPN de sitio a sitio

Para iniciar la configuración de la VPN, haga clic en **Site-to-site VPN** y, a continuación, en **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 ▾ Manage

Active ▾ Connection ▾

No records found

Failover group

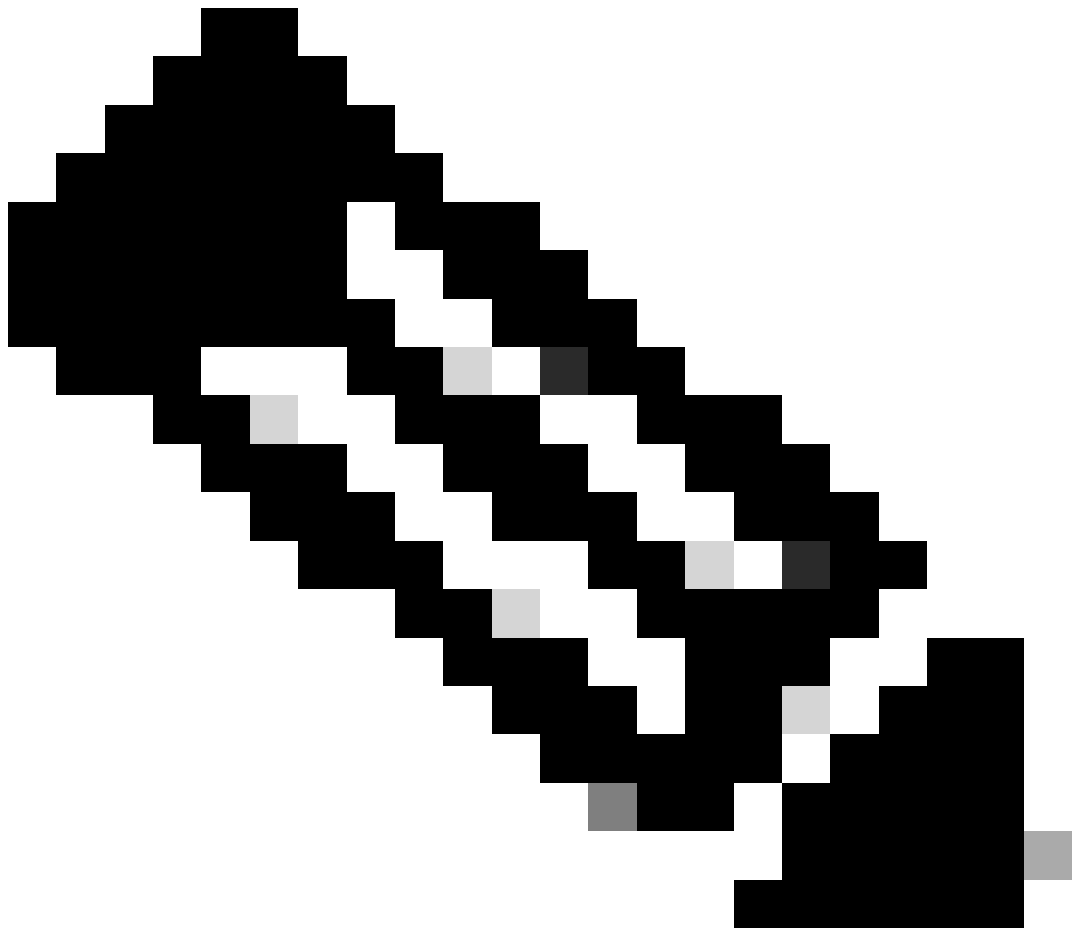
Add Delete Wizard

Add Delete

*Sophos: VPN de sitio a sitio*

En **General Settings** configurar:

- **Name:** un nombre de referencia a la política IPsec de Cisco Secure Access
- IP version: IPv4
- Connection type: Interfaz de túnel
- Gateway type: inicia la conexión
- Active on save: Marque la opción



**Nota:** La opción **Active on save** habilita la VPN automáticamente después de que termine de configurar la VPN de sitio a sitio.

---

## 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 de sitio a sitio - Configuración general

**Nota:** La opción Interfaz de túnel crea una interfaz de túnel virtual para el firewall Sophos XG con el nombre XFRM.

En **Encryption** configurar:

- **Profile:** el perfil que se crea en el paso, **Configure IPsec Profile**
- **Authentication type:** Clave previamente compartida
- **Preshared key:** la clave que configure en el paso, [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key:** Preshared key

Encryption

Profile: CSA

Authentication type: Preshared key

Preshared key: .....

Repeat preshared key: .....

*Sophos: VPN de sitio a sitio: cifrado*

En **Gateway Settings** configurar Local Gateway y Remote Gateway opciones, utilice esta tabla como referencia.

Gateway local	Gateway remoto
Interfaz de escucha Su Interfaz De Internet Wan	Dirección de gateway La IP pública generada en el paso, <a href="#">Tunnel Data</a>
Tipo de ID local Correo electrónico	Tipo de ID remoto Dirección IP



<p>ID local</p> <p>El correo electrónico generado en el paso, <a href="#">Tunnel Data</a></p>	<p>ID remoto</p> <p>La IP pública generada en el paso, <a href="#">Tunnel Data</a></p>
<p>Subred local cualquiera</p>	<p>Subred remota cualquiera</p>

## Gateway settings

Local gateway	Remote gateway
<p>Listening interface</p> <p>PortB - 192.168.0.33 <input checked="" type="checkbox"/></p>	<p>Gateway address</p> <p>18.156.145.74 <input checked="" type="checkbox"/></p>
<p>Local ID type</p> <p>Email <input checked="" type="checkbox"/></p>	<p>Remote ID type</p> <p>IP address <input checked="" type="checkbox"/></p>
<p>Local ID</p> <p>csasophos@ -sse.cisco.com <input checked="" type="checkbox"/></p>	<p>Remote ID</p> <p>18.156.145.74 <input checked="" type="checkbox"/></p>
<p>Local subnet</p> <p>Any <input type="checkbox"/></p> <p>Add new item</p>	<p>Remote subnet</p> <p>Any <input type="checkbox"/></p> <p>Add new item</p>

Sophos - VPN de sitio a sitio - Configuración de gateway

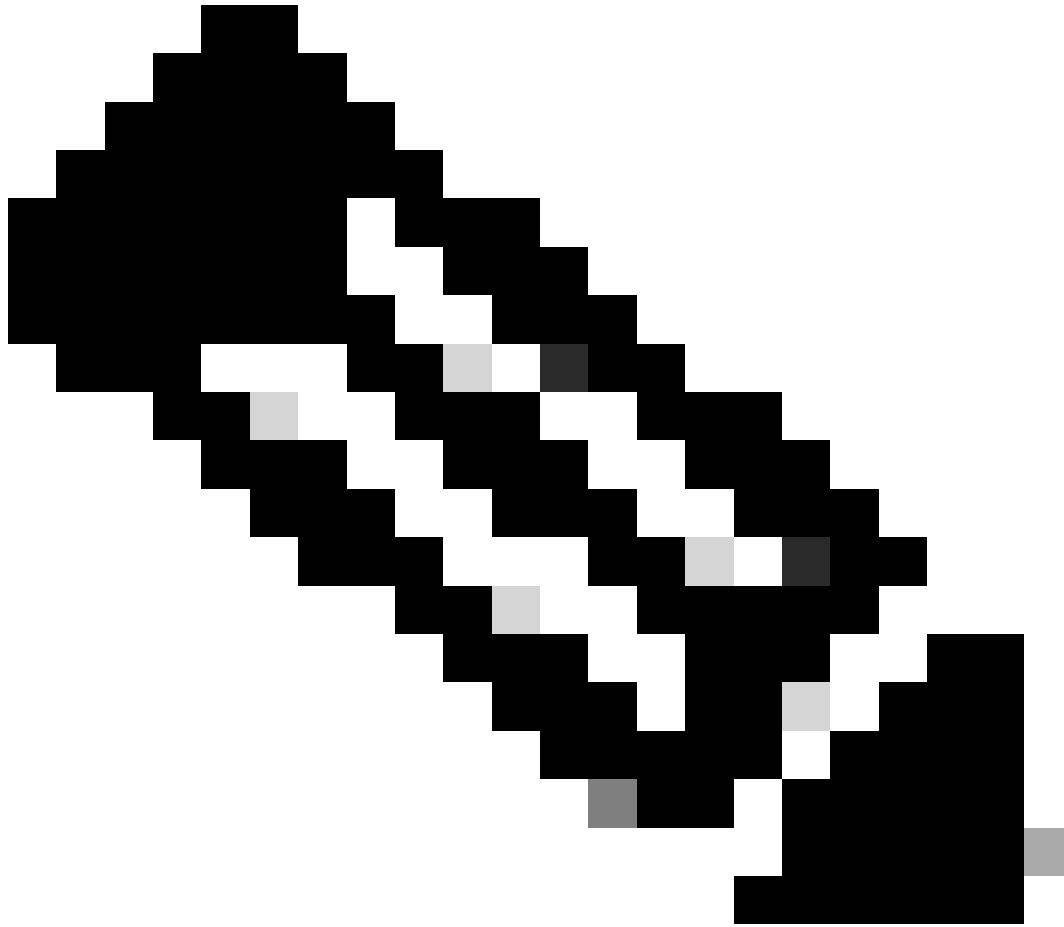
Después de hacer clic en **Save**, y se puede ver que el túnel fue creado.

### IPsec connections

Show additional properties Add Delete Wizard

<input type="checkbox"/>	Name <input type="text"/>	Group name <input type="text"/>	Profile <input type="text"/>	Connection type <input type="text"/>	Status	Connection <input type="text"/>	Manage
<input type="checkbox"/>	SecureAccesS	-	CSA	Tunnel interface	<span style="color: green;">●</span> Active <input type="text"/>	<span style="color: green;">●</span> <input type="text"/>	<input type="text"/> <input type="text"/> <input type="text"/>

Sophos: VPN de sitio a sitio: conexiones IPsec



**Nota:** Para comprobar si el túnel está correctamente activado en la última imagen, puede comprobar el **Connection** estado; si está en verde, el túnel está conectado si no está en verde y el túnel no está conectado.

---

Para comprobar si se ha establecido un túnel, vaya a **Current Activities > IPsec Connections**.

MONITOR & ANALYZE

# Control center


Current activities

Reports

Zero-day protection

Diagnostics

*Sophos - Supervisión y análisis - 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	

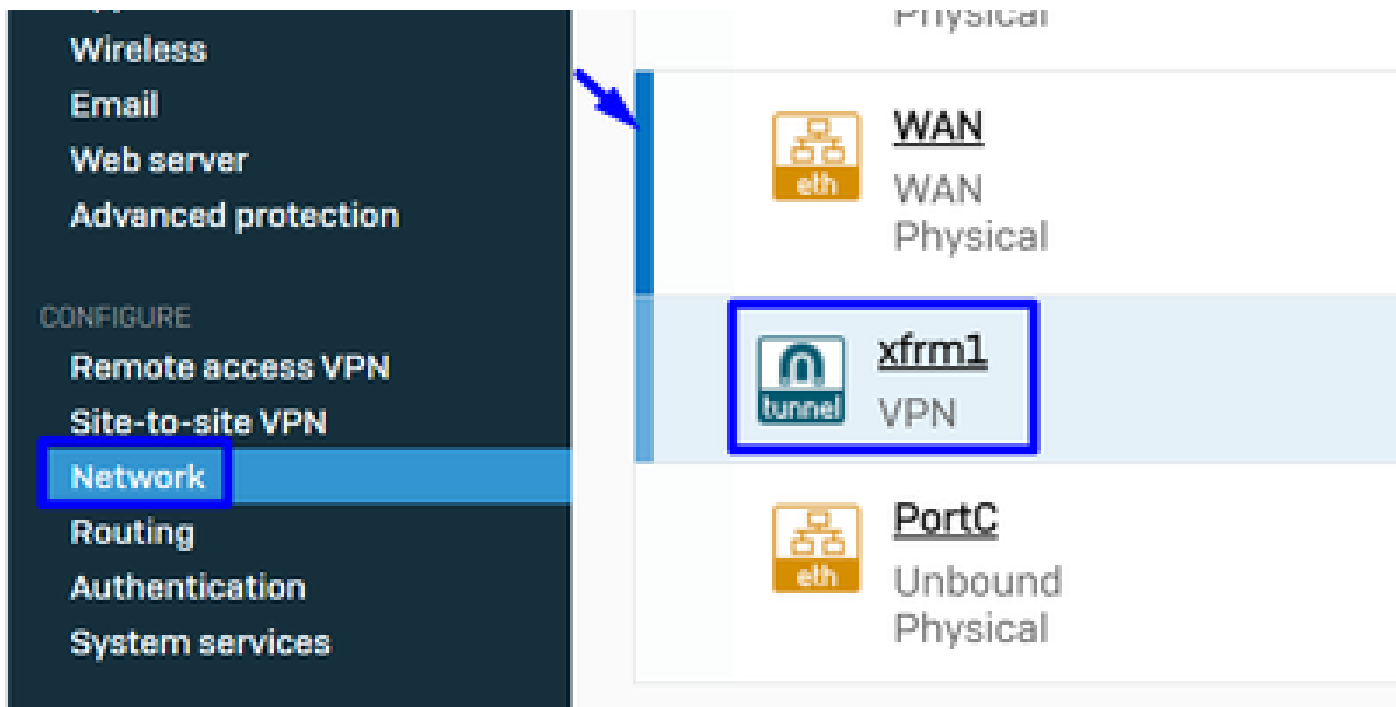
*Sophos - Supervisión y análisis - IPsec antes y después*

Después de eso, podemos continuar con el paso, **Configure Tunnel Interface Gateway**.

Configurar interfaz de túnel

Desplácese hasta **Network** la interfaz configurada en la VPN y compruébela WAN para editar la interfaz de túnel virtual con el nombre xfrm.

- Haga clic en **xfrm** la interfaz.



Sophos - Red - Interfaz de túnel

- Configure la interfaz con una IP no enrutable en su red; por ejemplo, puede utilizar 169.254.x.x/30, que es una IP en un espacio no enrutable; en nuestro ejemplo, utilizamos 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 - Red - Interfaz de túnel - Configuración

#### Configuración de las puertas de enlace

Para configurar el gateway para la interfaz virtual (xfrm)

- Desplácese hasta Routing > Gateways
- Haga clic en Add

Sophos - Routing - Puertas de enlace

En **Gateway host** configurar:

- **Name:** un nombre que hace referencia a la interfaz virtual creada para la VPN
- **Gateway IP:** En nuestro caso 169.254.0.2, esa es la IP bajo la red 169.254.0.1/30 que ya asignamos bajo el paso, Configure Tunnel Interface
- **Interface:** Interfaz virtual de VPN
- **Zone:** Ninguno (valor predeterminado)

Sophos - Routing - Puertas de enlace - Host de puerta de enlace

- En **Health check** deshabilitar la comprobación
- Haga clic en **Save**

# Health check

Health check



*Sophos - Routing - Gateways - Comprobación de estado*

Puede observar el estado del gateway después de guardar la configuración:

## 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 - Estado*

## Configuración de la ruta SD-WAN

Para finalizar el proceso de configuración, debe crear la ruta que le permita reenviar el tráfico a Secure Access.

Desplácese hasta **Routing > SD-WAN routes**.

- Haga clic en **Add**



Rutas Sophos - SD-Wan

En **Traffic Selector** configurar:

- Incoming interface: seleccione la interfaz desde la que desea enviar el tráfico o los usuarios que acceden desde RA-VPN, ZTNA o Clientless-ZTNA
- DSCP marking: Nada para este ejemplo
- **Source networks**: seleccione la dirección que desea rutear a través del túnel
- **Destination networks**: Cualquiera o puede especificar un destino
- **Services**: Cualquiera o puede especificar los servicios
- **Application object**: una aplicación si tiene el objeto configurado
- User or groups: si desea agregar un grupo específico de usuarios para enrutar el tráfico a Secure Access

### Traffic selector

<p><b>Incoming interface</b></p> <p>LAN-192.168.0.203</p>	<p><b>DSCP marking</b></p> <p>Select DSCP marking</p>	
<p><b>Source networks</b></p> <p>Any</p> <p>Add new item</p>	<p><b>Destination networks</b></p> <p>Any</p> <p>Add new item</p>	<p><b>Services</b></p> <p>Any</p> <p>Add new item</p>
<p><b>Application object</b></p> <p>Any</p> <p>Add new item</p>	<p><b>User or groups</b></p> <p>Any</p> <p>Add new item</p>	

Sophos - Rutas SD-Wan - Selector de tráfico

En **Link selection settings** configurar la puerta de enlace:

- Primary and Backup gateways: Marque la opción

- **Primary gateway:** seleccione la puerta de enlace configurada en el paso [Configure the Gateways](#)
- Haga clic en **Save**

Link selection settings

Select SD-WAN profile ⓘ  Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

*Sophos - Rutas SD-Wan - Selector de tráfico - Gateways primarios y de respaldo*

Después de finalizar la configuración en el firewall Sophos XG, puede continuar con el paso, **Configure Private App.**

Configurar aplicación privada

Para configurar el acceso a la aplicación privada, inicie sesión en el [Portal de administración](#).

- Desplácese hasta **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

Acceso seguro - Recursos privados

- Haga clic en + Add

**Private Resources**    Private Resource Groups

Private Resources Last 24 Hours

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

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

Acceso seguro - Recursos privados 2

- En **General** Configurar el **Private Resource Name**

## General

### Private Resource Name

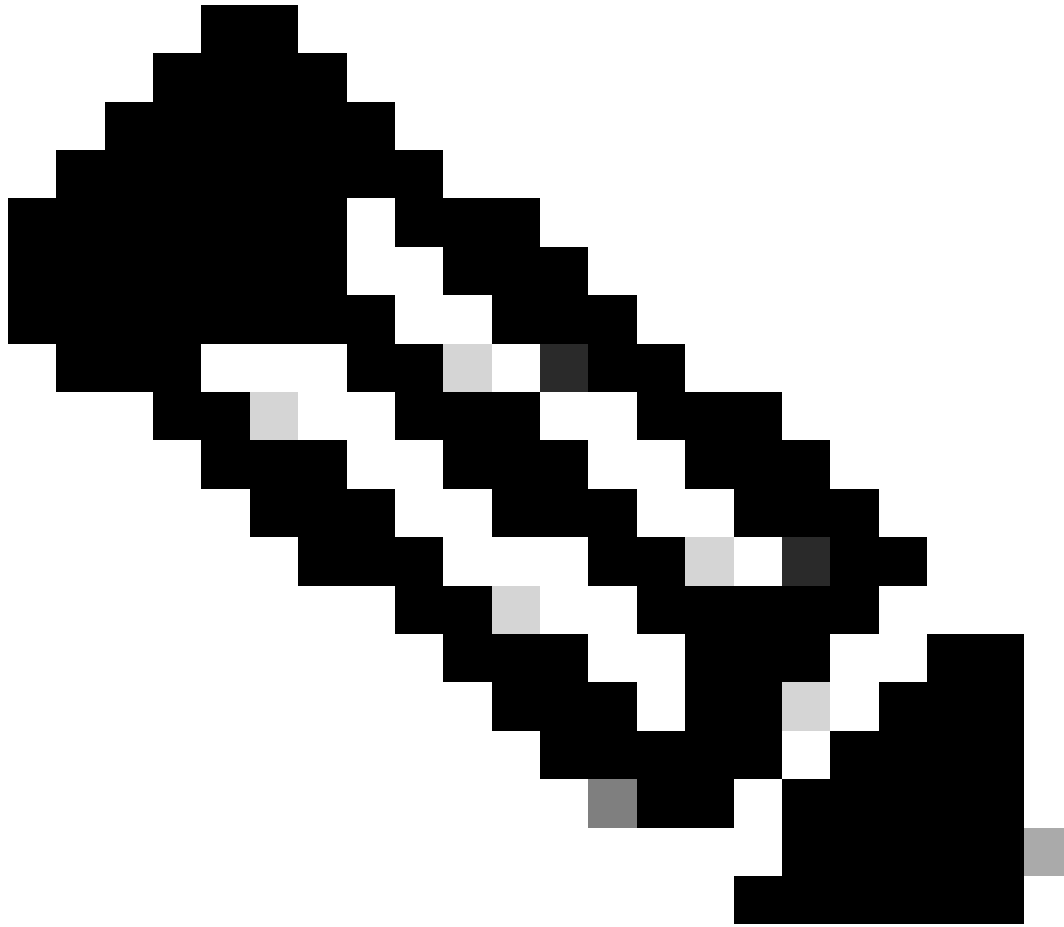
SplunkSophos

### Description (optional)

*Acceso seguro - Recursos privados - General*

En **Communication with Secure Access Cloud** configurar:

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: seleccione el recurso al que desea acceder



**Nota:** Recuerde que la dirección de acceso interno se asignó en el paso [Configure the Tunnel on Secure Access](#).

- 
- **Protocol:** seleccione el protocolo que utiliza para acceder a ese recurso
  - **Port / Ranges :** seleccione los puertos que necesita habilitar para acceder a la aplicación

## 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

*Acceso seguro - Recursos privados - Comunicaciones con acceso seguro Nube*

Dentro **Endpoint Connection Methods** de , configure todas las formas posibles de acceder a los recursos privados a través de Secure Access y elija los métodos que desea utilizar para su entorno:

- **Zero-trust connections:** marque la casilla para activar el acceso ZTNA.
  - **Client-based connection:** active el botón para permitir la base de clientes ZTNA
    - **Remotely Reachable Address:** configure la IP de su aplicación privada
  - **Browser-based connection:** active el botón para permitir ZTNA basado en explorador
    - Public URL for this resource: agregue un nombre para utilizarlo junto con el dominio ztna.sse.cisco.com
      - Protocol: elija HTTP o HTTPS como protocolo al que acceder a través del navegador
- **VPN connections:** marque la casilla para habilitar el acceso RA-VPN.
- Haga clic en **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) ⓘ  
  
[+ 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://  -8195126.ztna.sse.cisco.com

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

**Validate Application Certificate** ⓘ

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

**Save** [Cancel](#)

Acceso seguro - Recursos privados - Comunicaciones con la nube de acceso seguro 2

Una vez finalizada la configuración, se obtiene el siguiente resultado:

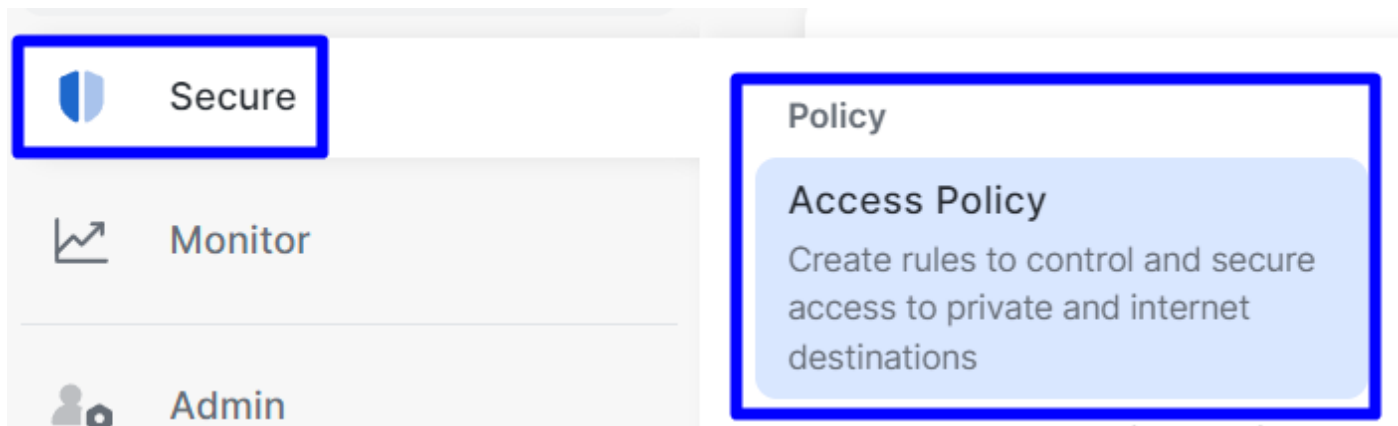
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none"> <li>VPN</li> <li>Browser-based ZTNA</li> <li>Client-based ZTNA</li> </ul>	1	2	16

Acceso seguro: recursos privados configurados

Ahora puede continuar con el paso **Configure the Access Policy**.

Configuración de la política de acceso

Para configurar la política de acceso, navegue hasta **Secure > Access Policy**.



*Acceso seguro - Política de acceso*

- Haga clic en **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

*Acceso seguro - Política de acceso - Acceso privado*

Configure las siguientes opciones para proporcionar acceso a través de varios métodos de autenticación:

- 1. Specify Access
  - Action:Permiso
    - **Rule name:** especifique un nombre para la regla de acceso
    - **From:** los usuarios a los que concede acceso
    - **To:** la aplicación a la que deseaba permitir el acceso
    - Endpoint Requirements: (Valor predeterminado)
- Haga clic en **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

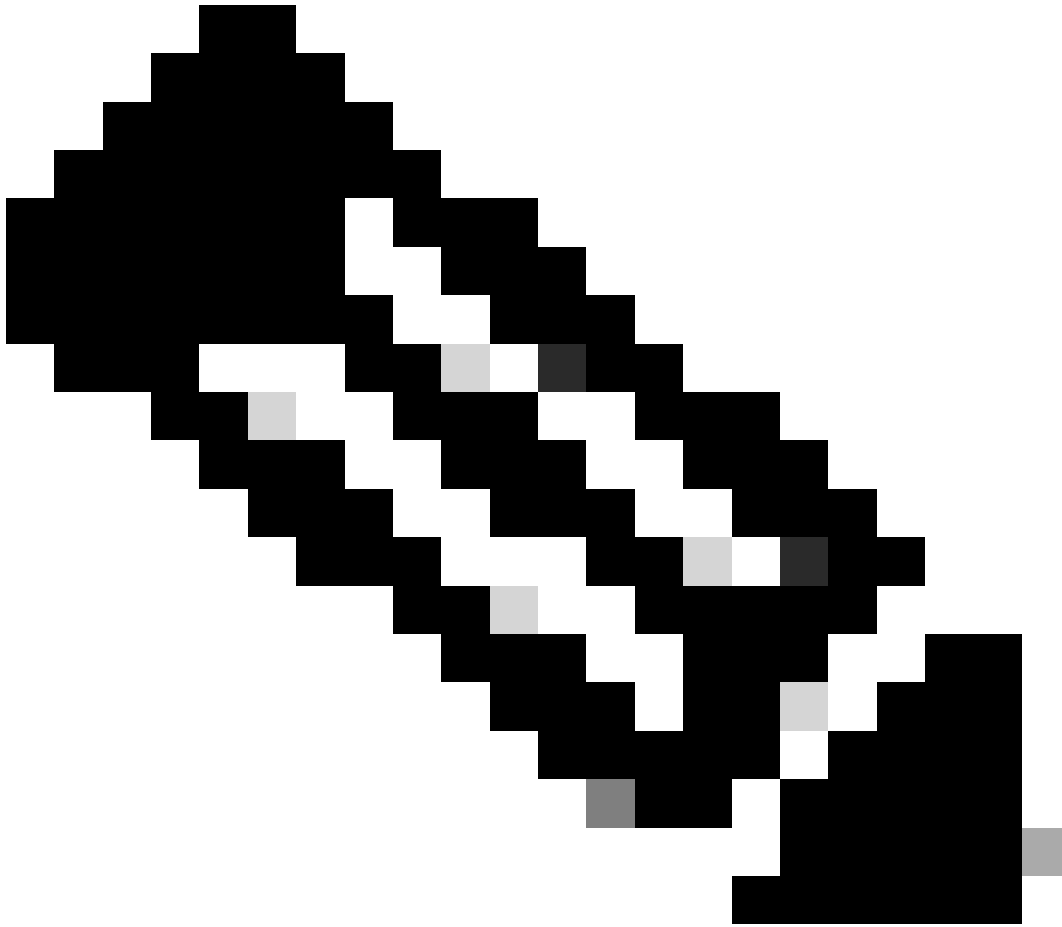
Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

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

Private Resources: **SplunkSophos**

Acceso seguro - Directiva de acceso - Especificar acceso





**Nota:** Para el paso 2. **Configure Security** según sea necesario, pero en este caso, no ha activado el **Intrusion Prevention (IPS)**, o **Tenant Control Profile**.

- Haga clic en Save y obtendrá lo siguiente:

	# ⓘ	Rule name	Access	Action	Sources	Destinations	Security	Status
⋮	6	SplunkSophos	Private	Allow	Any	SplunkSophos	-	✓ ...

*Acceso seguro: política de acceso configurada*

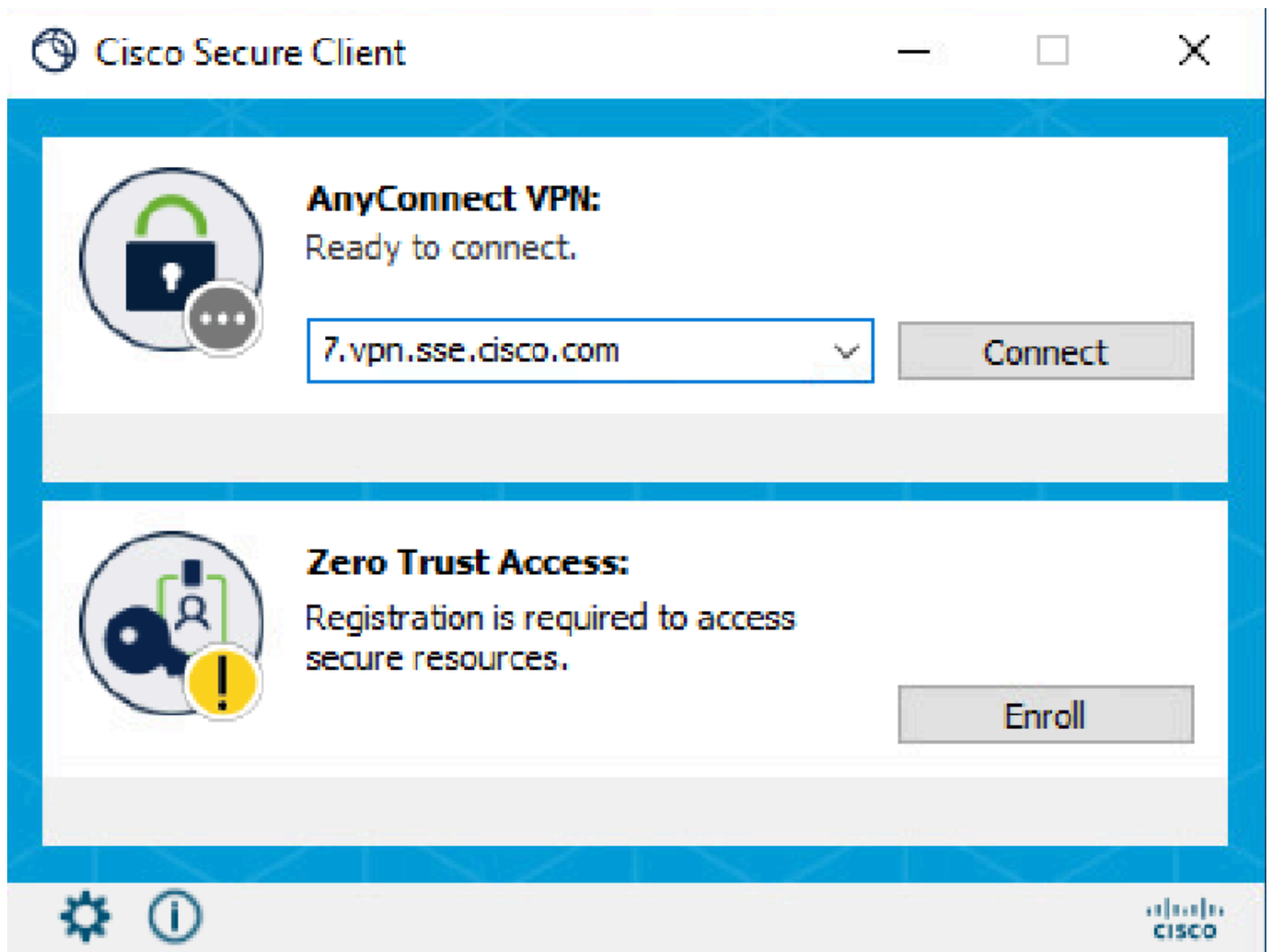
Después de esto, puede continuar con el paso Verify.

Verificación

Para verificar el acceso, debe tener instalado el agente de Cisco Secure Client que puede descargar de [Descarga de Software - Cisco Secure Client](#).

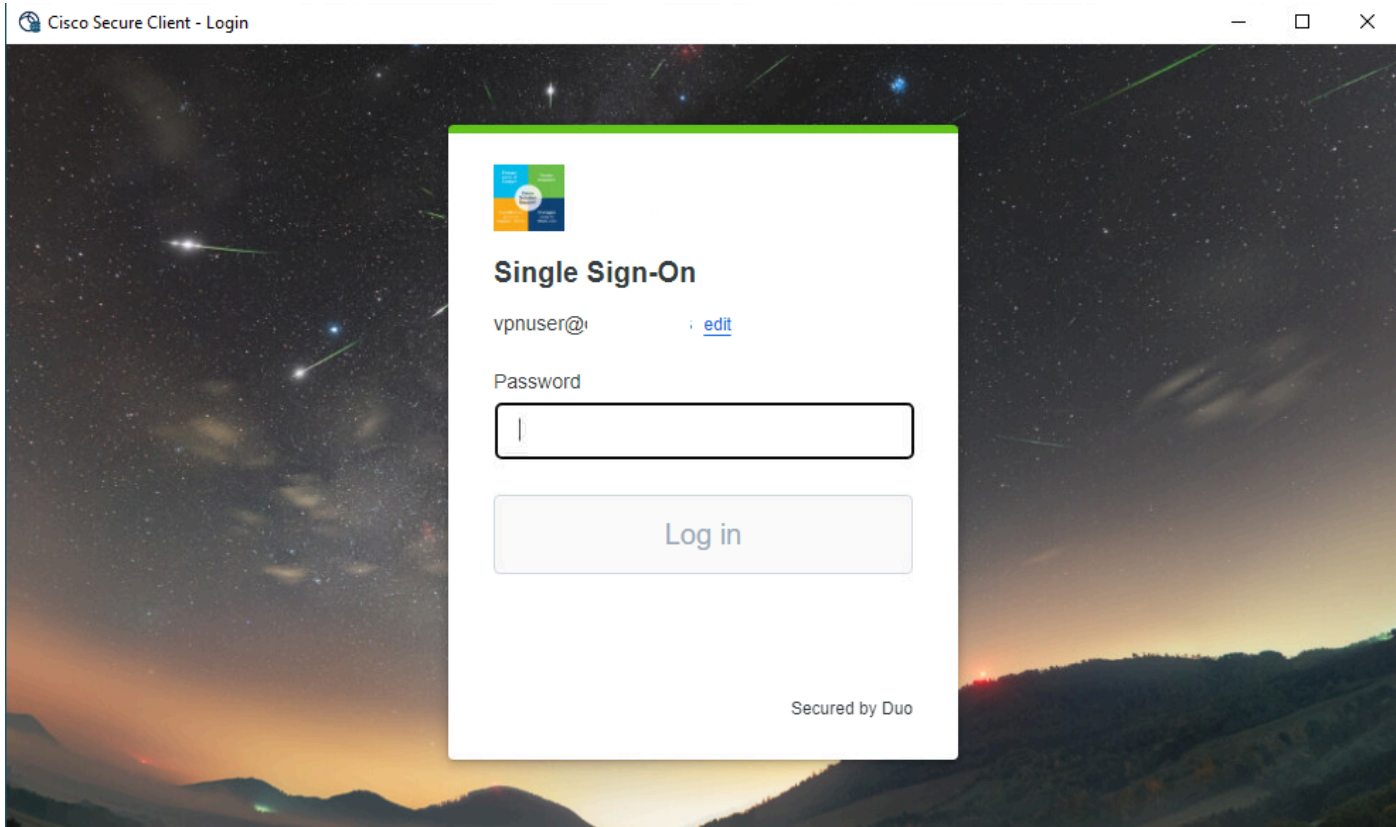
VPN de RA

Inicie sesión mediante Cisco Secure Client Agent-VPN.



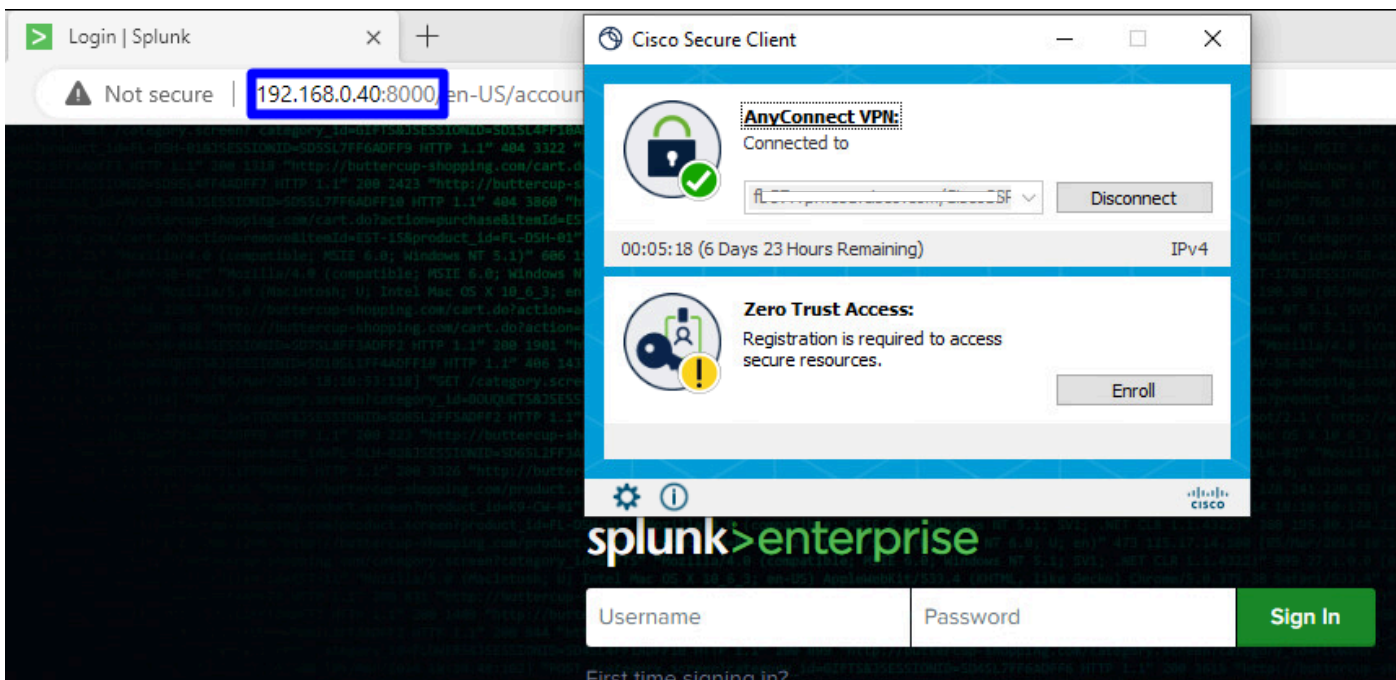
*Cliente seguro - VPN*

- Autenticar mediante su proveedor de SSO



Acceso seguro - VPN - SSO

- Después de autenticarse, acceda al recurso:



Acceso seguro - VPN - Autenticado

Navegue hasta: 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

Acceso seguro - Búsqueda de actividad - RA-VPN

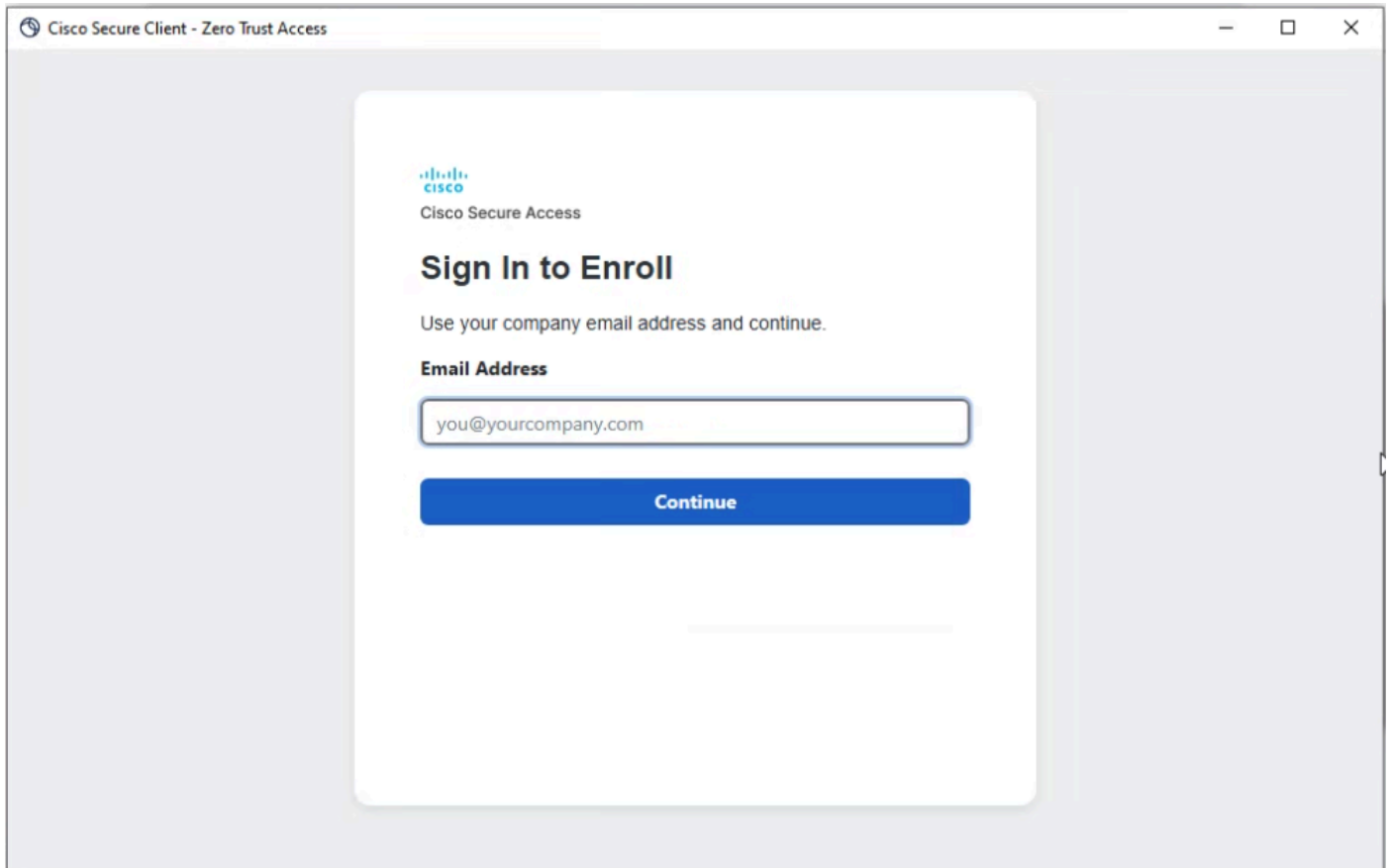
Puede ver que al usuario se le permitió autenticarse a través de RA-VPN.

ZTNA de base cliente

Inicie sesión a través de Cisco Secure Client Agent - ZTNA.

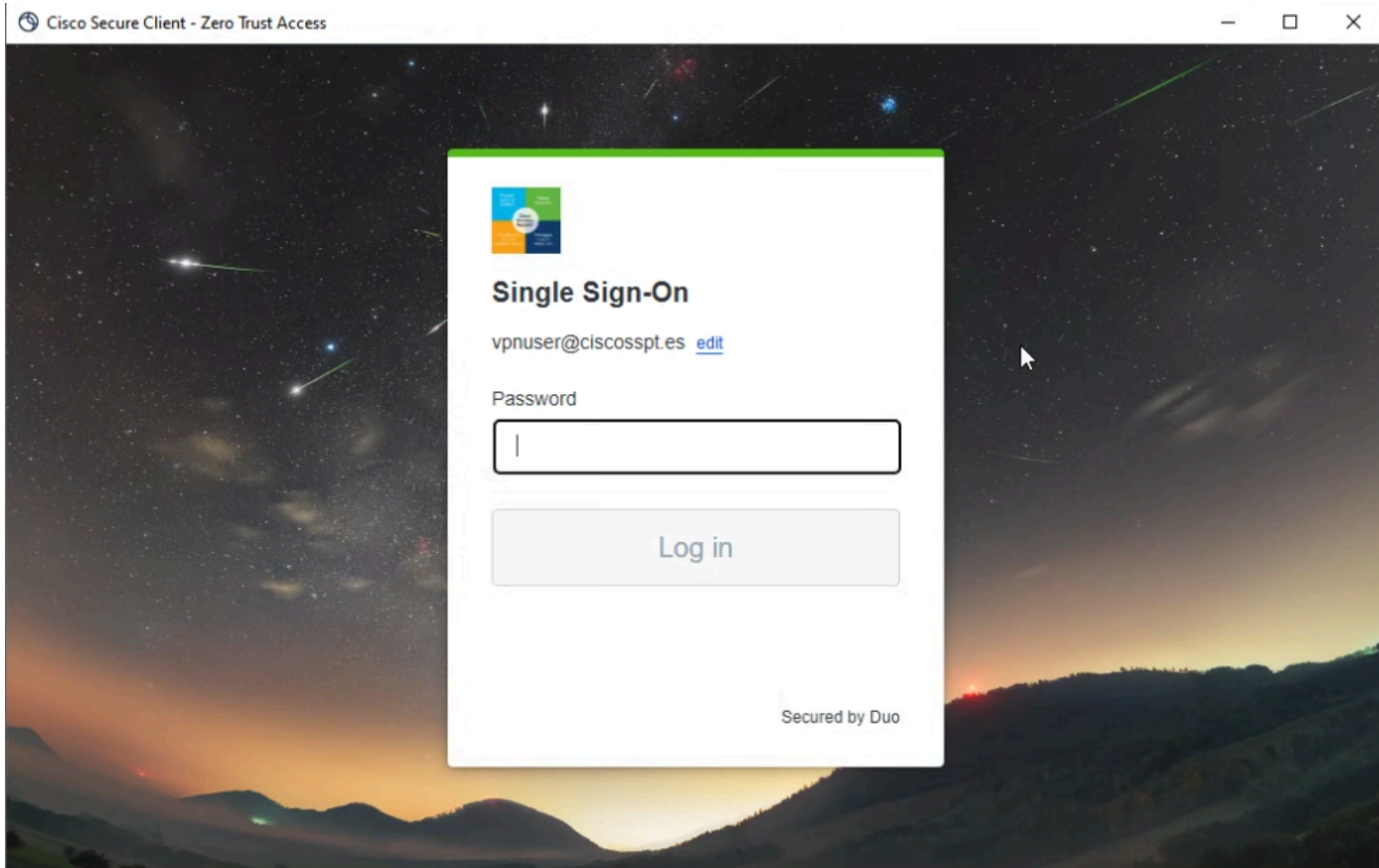
Cliente seguro: ZTNA

- Insíbase con su nombre de usuario.



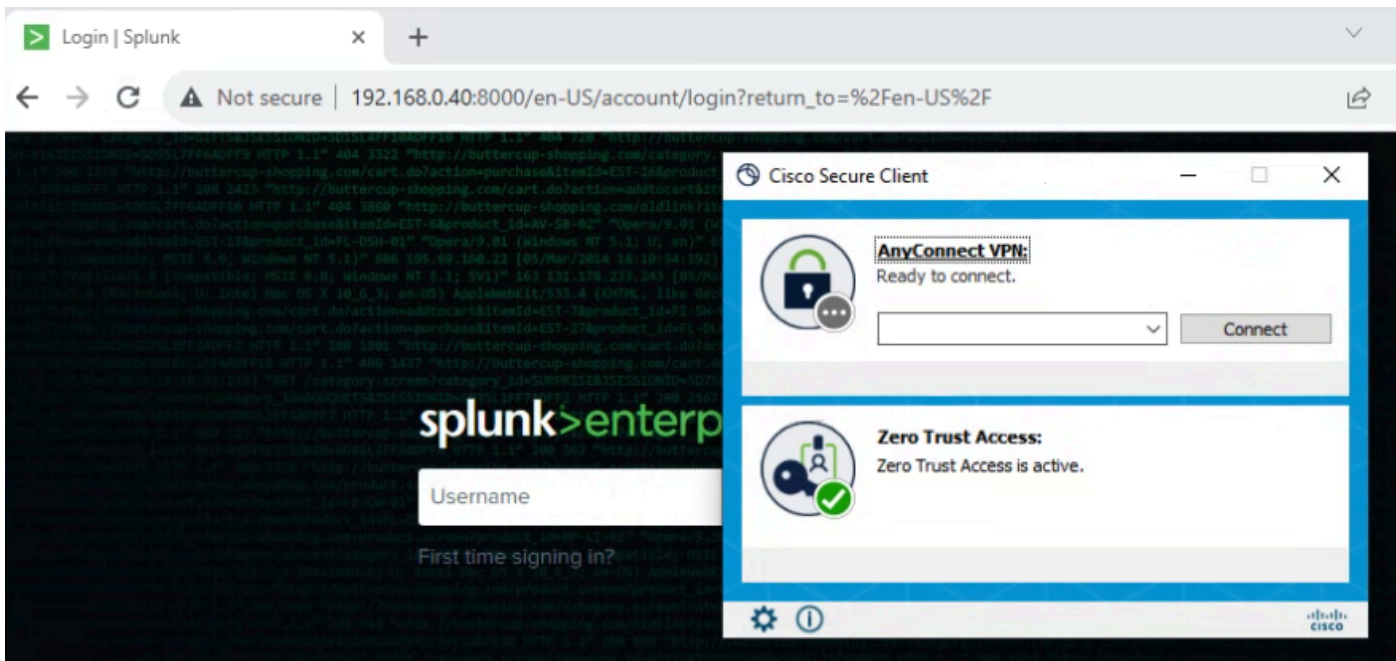
*Secure Client - ZTNA - Inscripción*

- Autenticar en su proveedor de SSO



Secure Client - ZTNA - Inicio de sesión de SSO

- Después de autenticarse, acceda al recurso:



Acceso seguro - ZTNA - Registrado

Navegue hasta: Monitor > Activity Search

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

Acceso seguro - Búsqueda de actividad - Basado en cliente ZTNA

Puede ver que al usuario se le permitió autenticarse a través de ZTNA basado en cliente.

ZTNA basado en navegador

Para obtener la URL, debe ir a **Resources > Private Resources**.

The screenshot shows the Splunk Sophos interface. On the left is a navigation menu 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). On the right, under the heading 'Sources and destinations', there are two options: 'Private Resources' (highlighted with a blue box) and 'Registered Networks'. The 'Private Resources' option includes the text 'Define internal applications and other resources for use in access rules'. Below it, 'Registered Networks' includes the text 'Point your networks to our servers'.

*Acceso seguro - Recurso privado*

- Haga clic en su política

The screenshot shows a table with one row. The first column contains the text 'SplunkSophos', with a blue arrow pointing to it from the right. The second column contains a hyphen '-'. The third column contains a legend with three items: 'Client-based ZTNA' (in a light blue rounded rectangle), 'Browser-based ZTNA' (in a light purple rounded rectangle), and 'VPN' (in a light pink rounded rectangle). To the right of the legend is the number '1'.

*Acceso seguro - Recursos privados - SplunkSophos*

- Desplazarse hacia abajo



# SplunkSophos

Client-based ZTNA

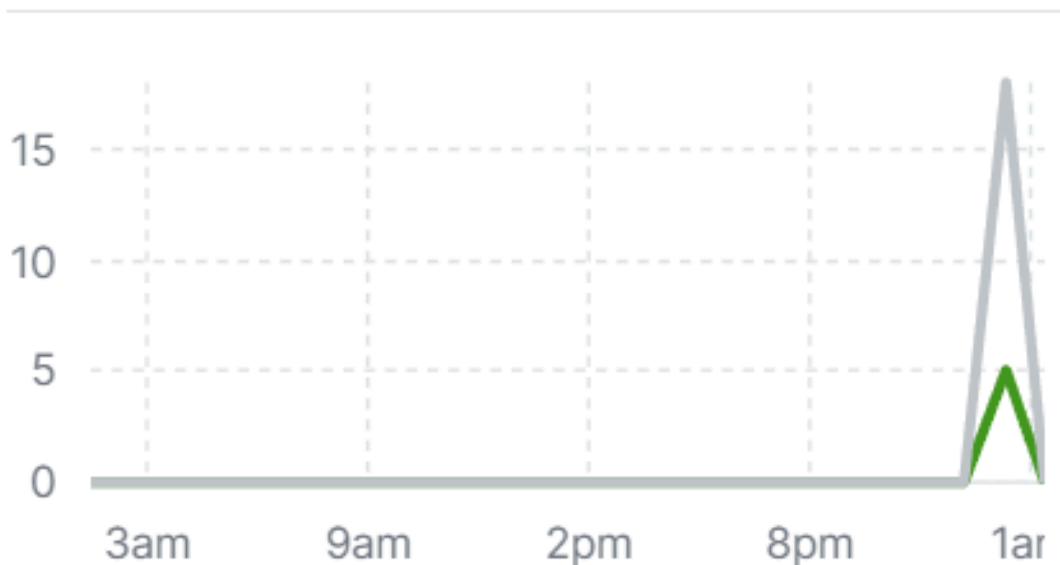
Browser-based ZTNA



VPN

Total Requests

**23** ↗ 44% from previous 24 hours



## TOTAL REQUESTS BY STATUS

### Status

✓	Success	5
⊘	Blocked	18



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).