Configuración del acceso seguro con el firewall Sophos XG

Contenido

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

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.

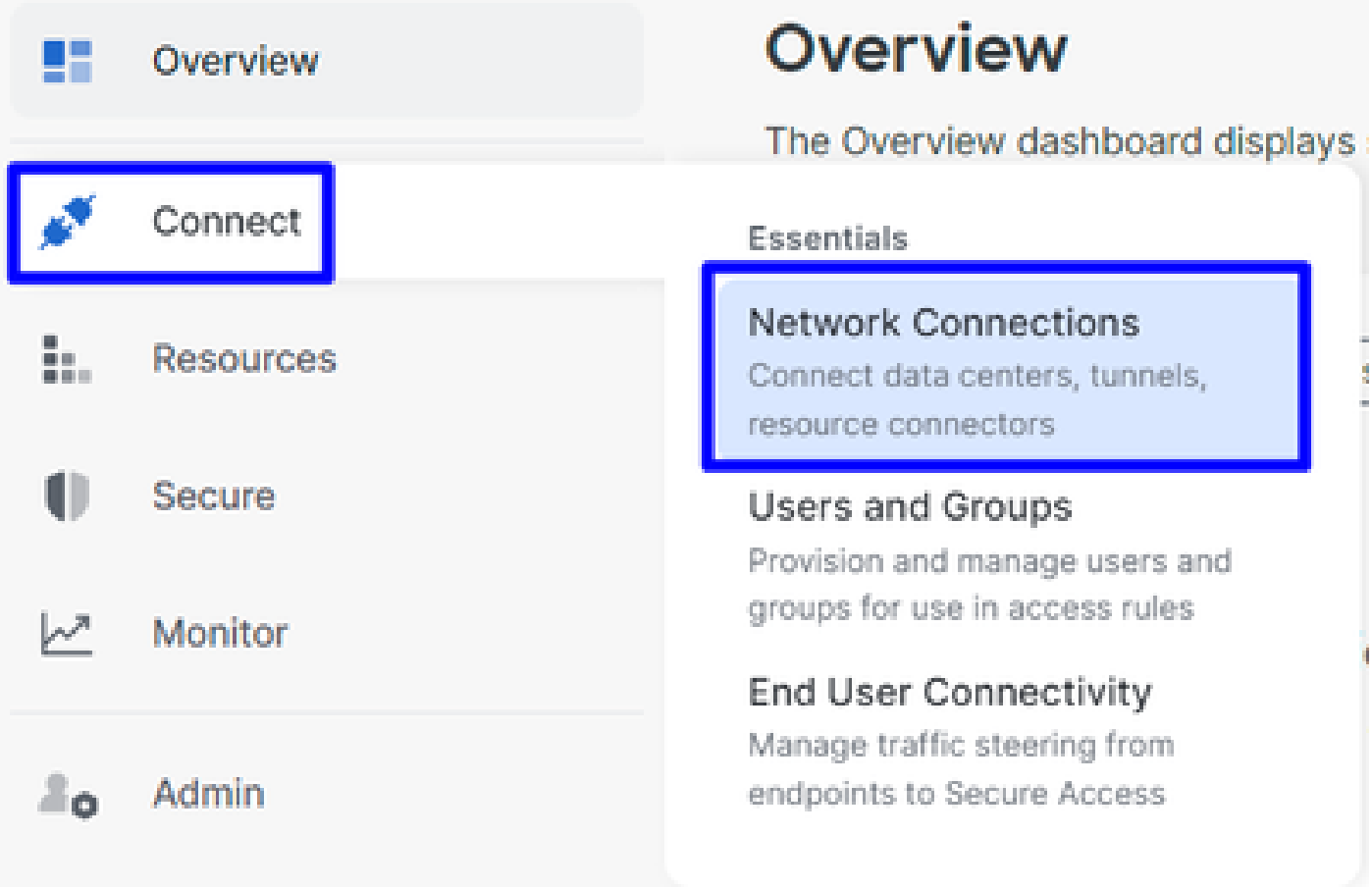
Configurar

Configuración del túnel en Secure Access

Vaya al panel de administración de Secure Access.

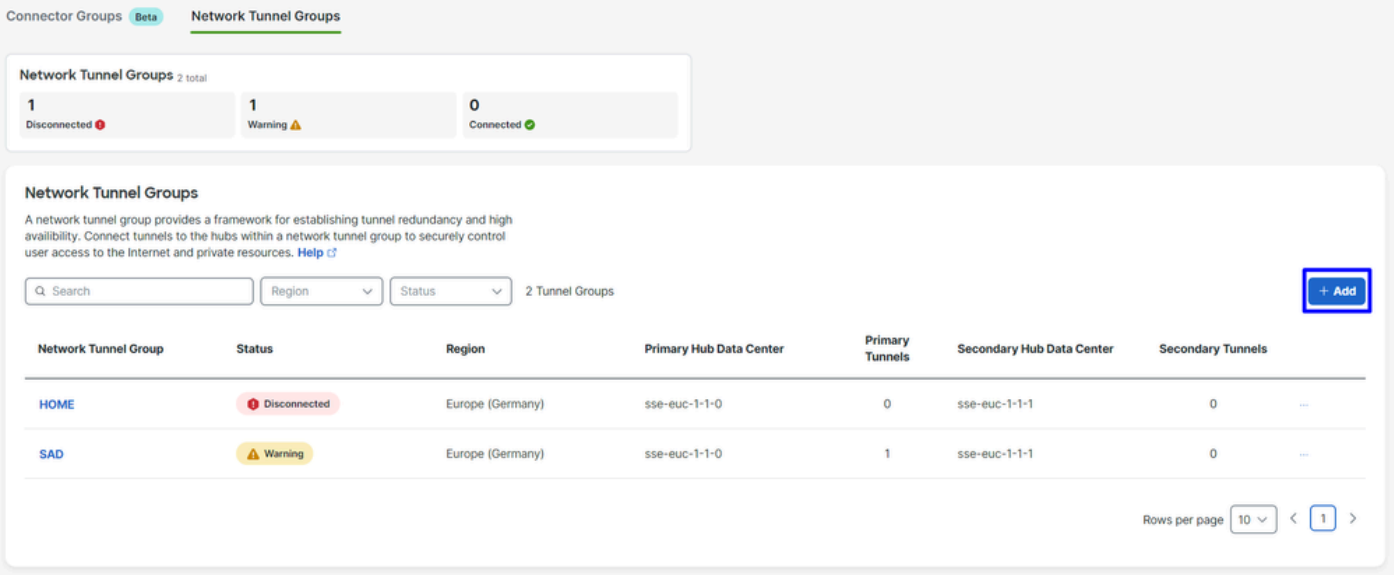
Acceso seguro - Página principal

- 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

SophosFirewall

Region

Europe (Germany)

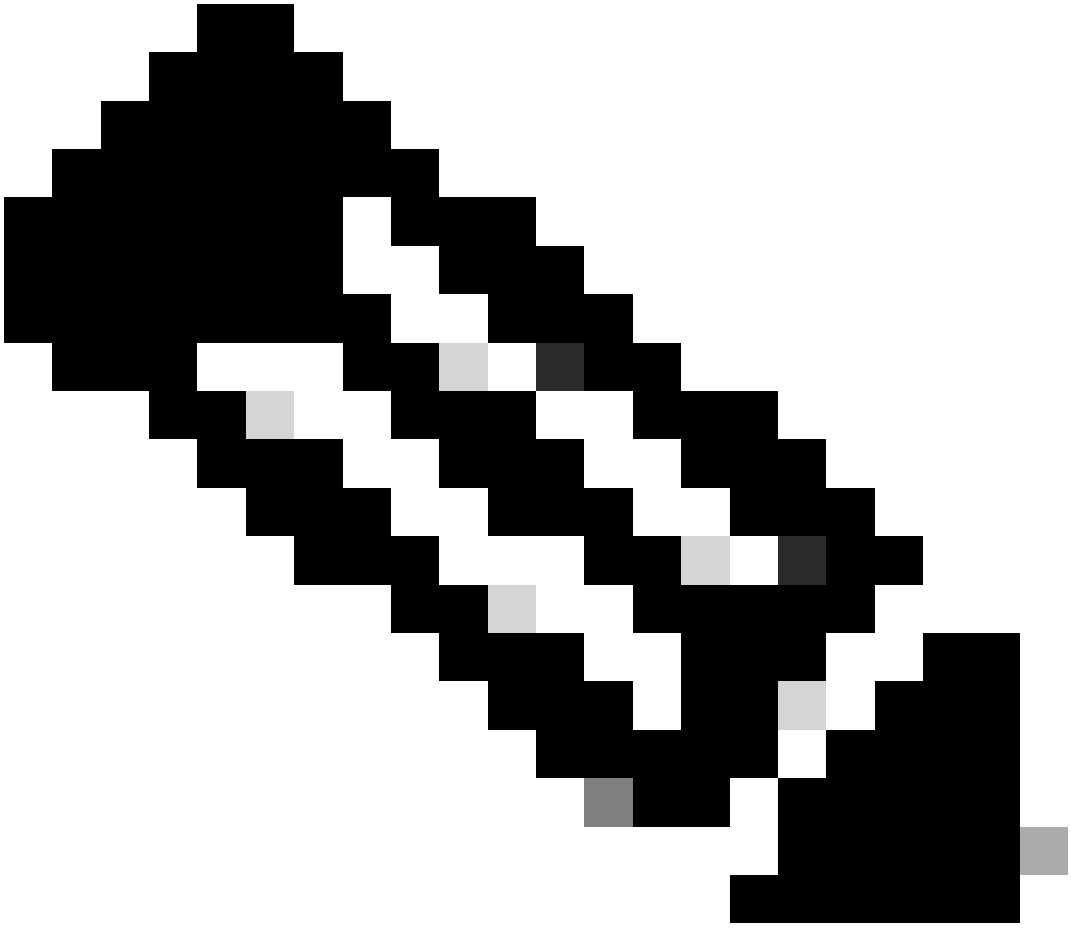
Device Type

Other

Cancel

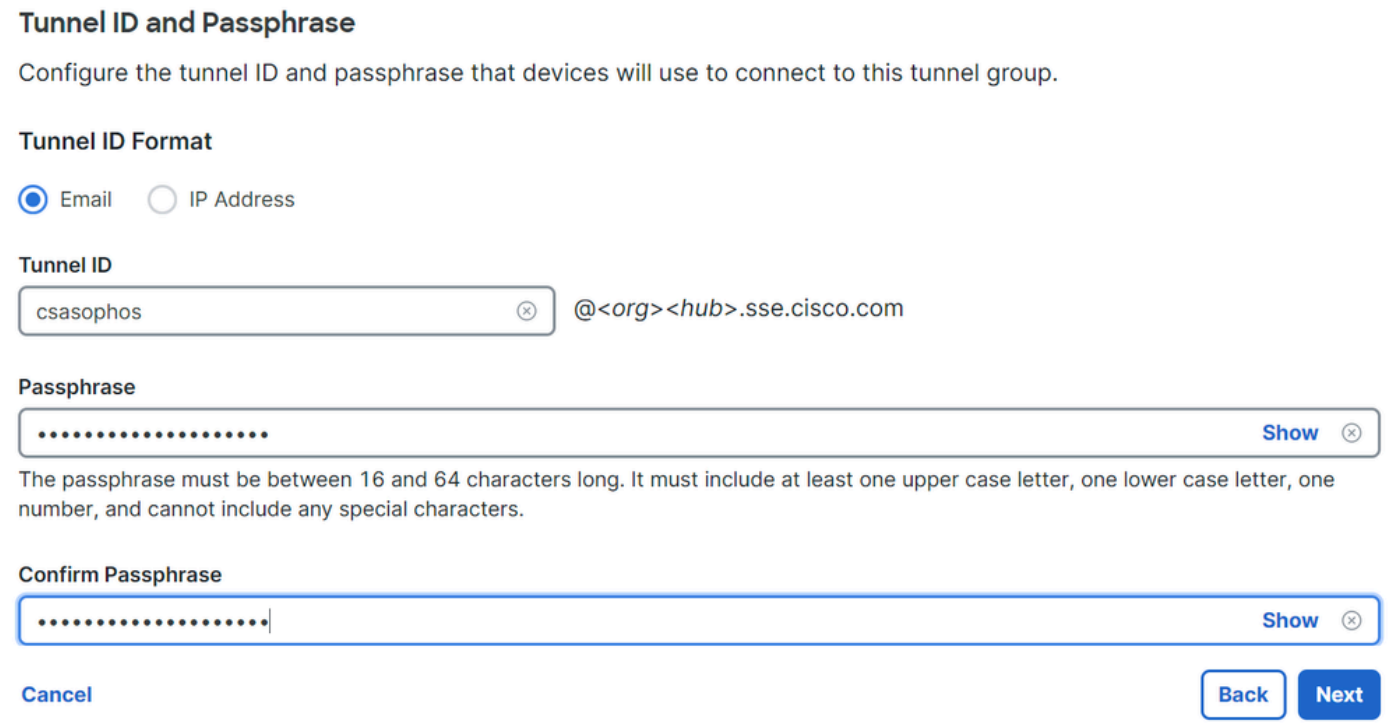
Next

Acceso seguro - Grupos de túnel - Configuración general



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

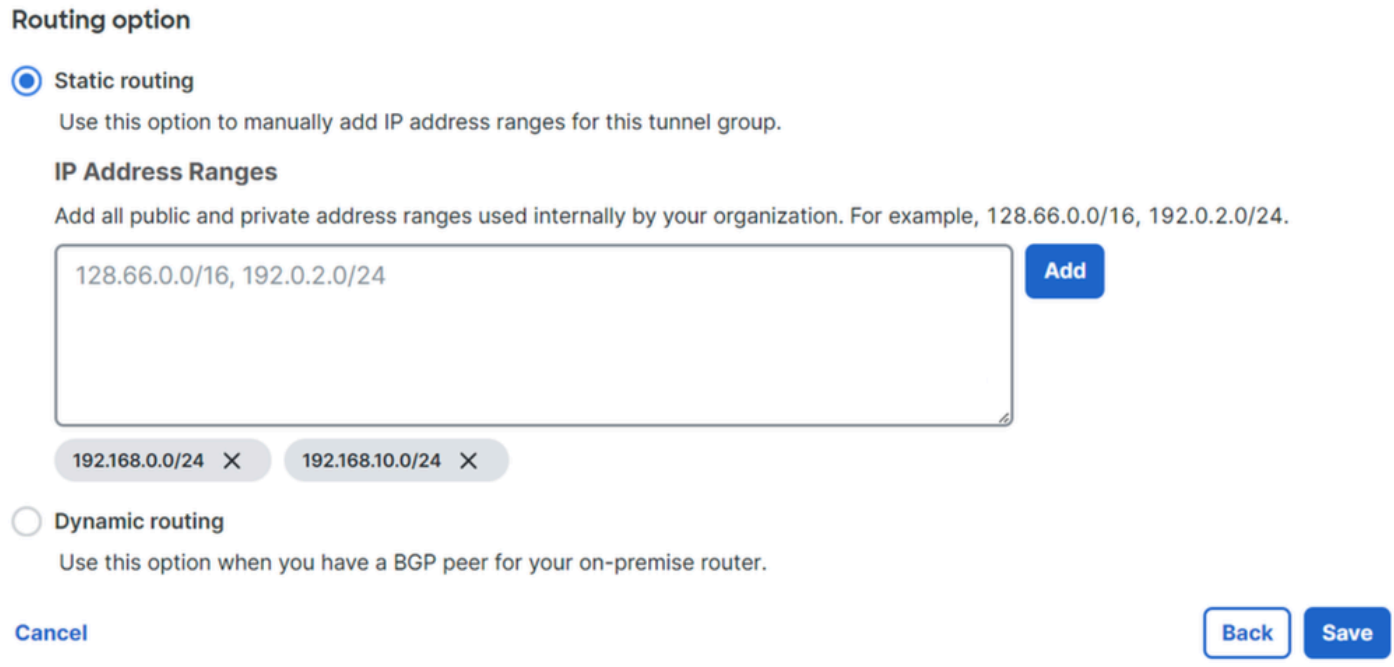
- Configure el Tunnel ID Format y Passphrase.
- Haga clic en Next.



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.

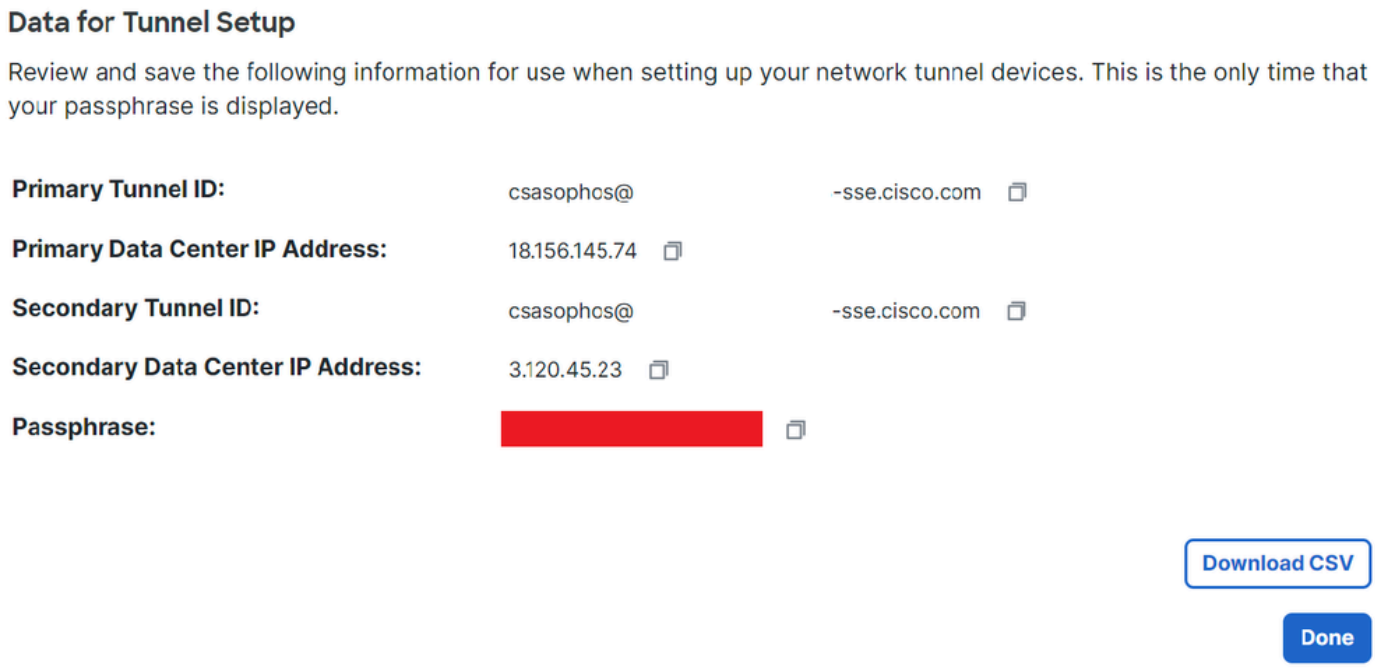
- Haga clic en **Save**.



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



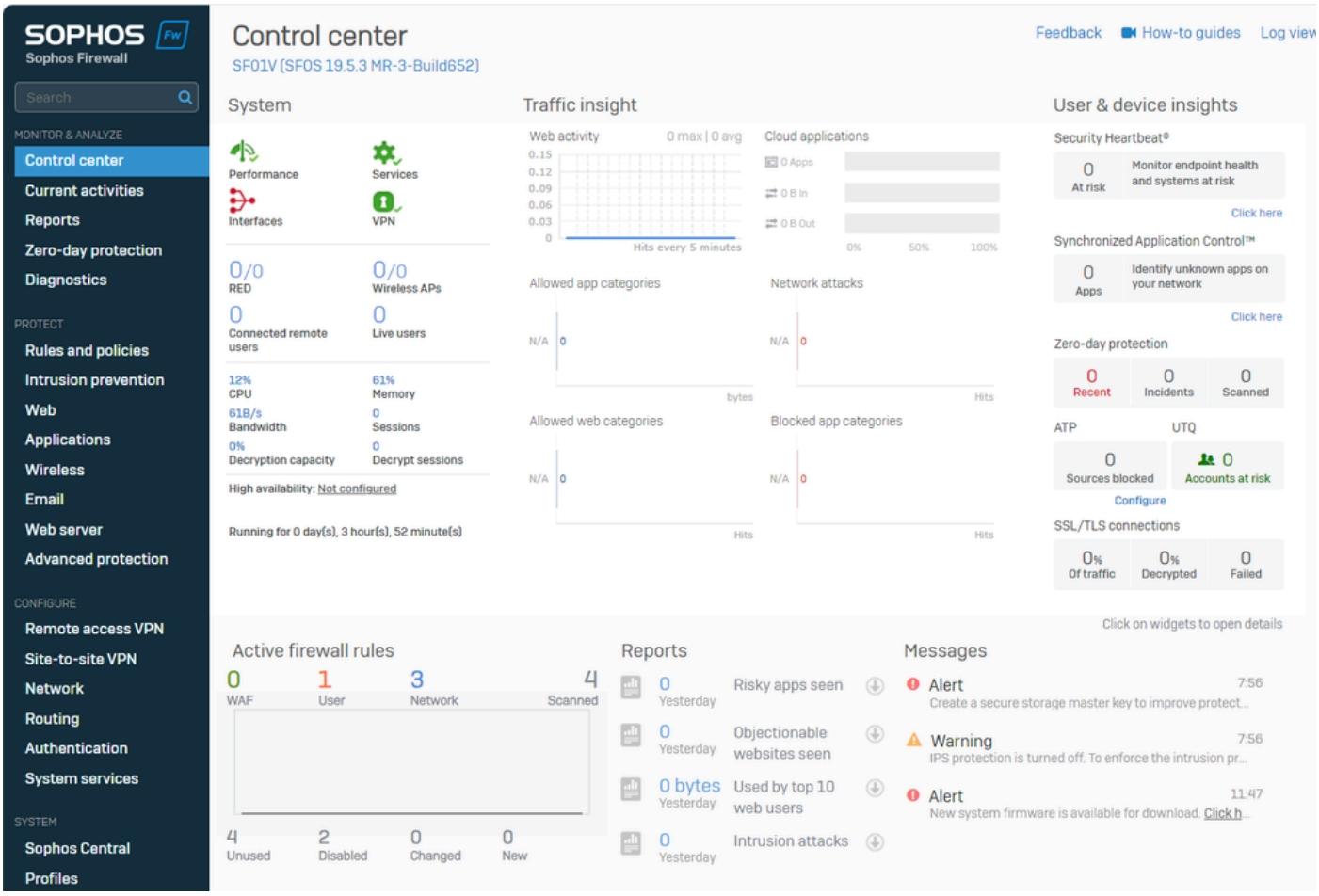
Acceso seguro - Grupos de túnel - Reanudación de la configuración

Configuración del túnel en Sophos

Configurar perfil IPsec

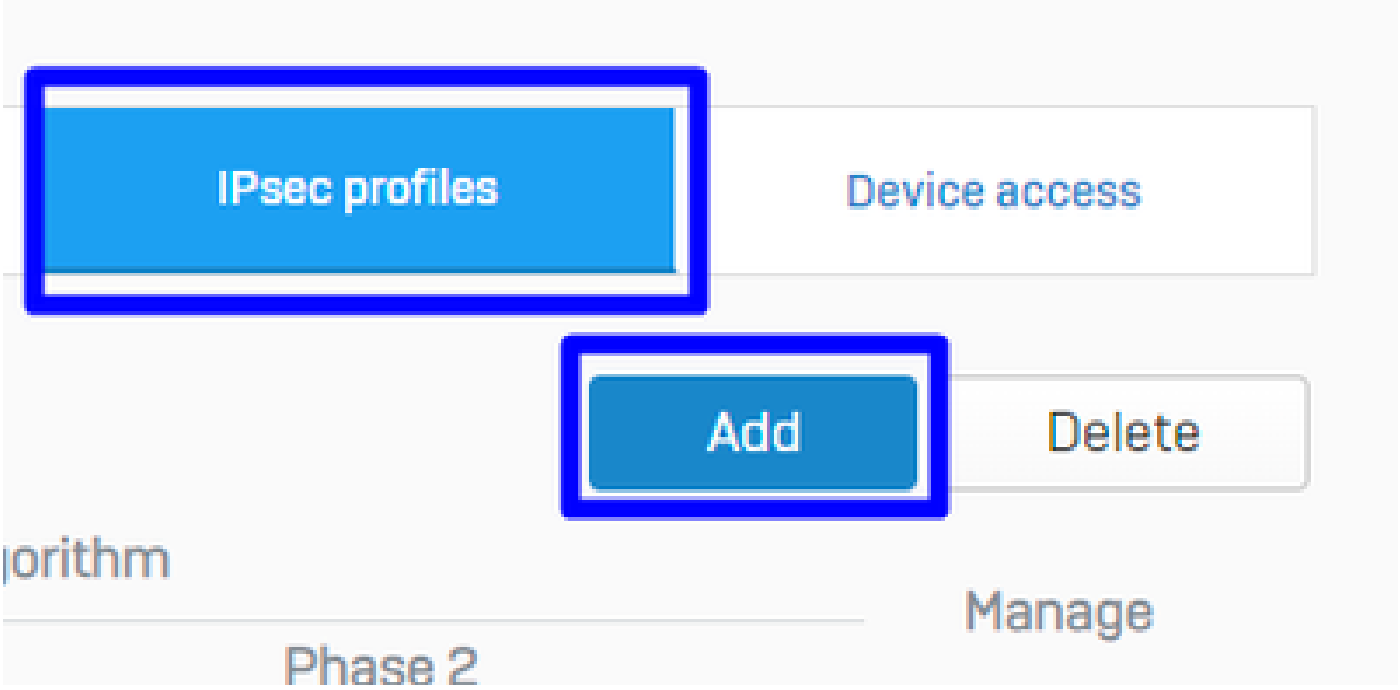
Para configurar el perfil IPsec, navegue hasta el firewall Sophos XG.

Se obtiene algo similar a esto:



Sophos - Panel de administración

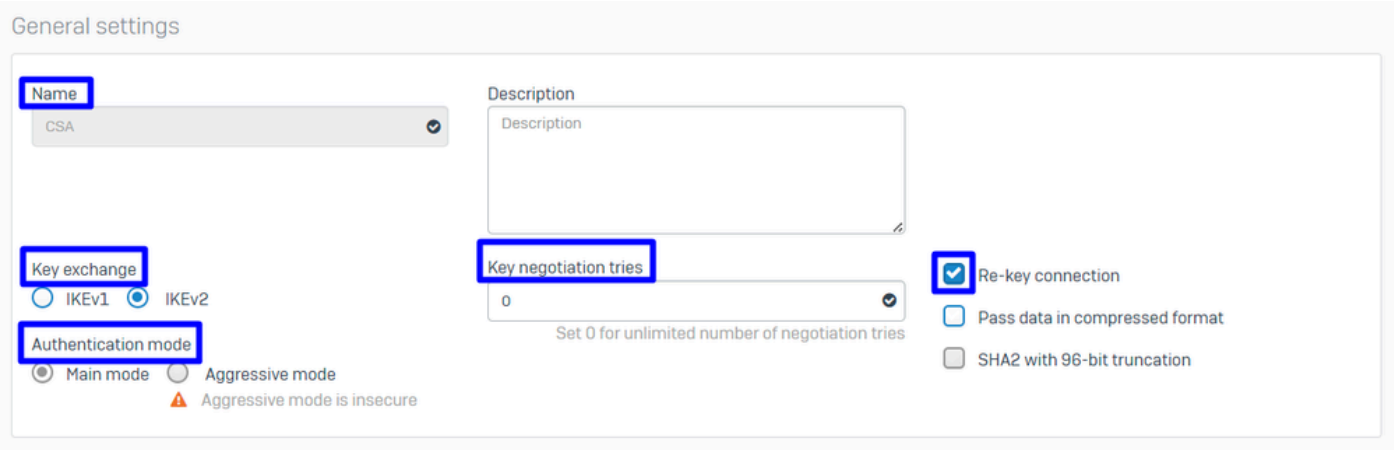
- Desplácese hasta Profiles
- Haga clic en **IPsec Profiles** y después haga clic enAdd



Sophos: perfiles IPsec

En **General Settings** configurar:

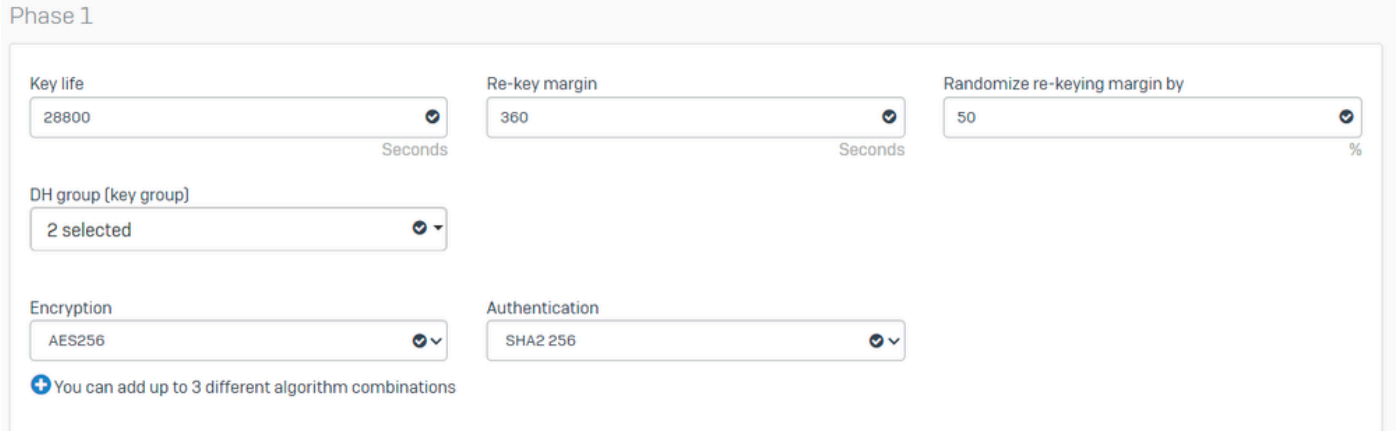
- **Name**: un nombre de referencia a la política de acceso seguro de Cisco
- **Key Exchange**: IKEv2
- **Authentication Mode**: Modo principal
- **Key Negotiation Tries**:0
- **Re-Key connection**: Marque la opción



Sophos - Perfiles IPsec - Configuración general

En **Phase 1** configurar:

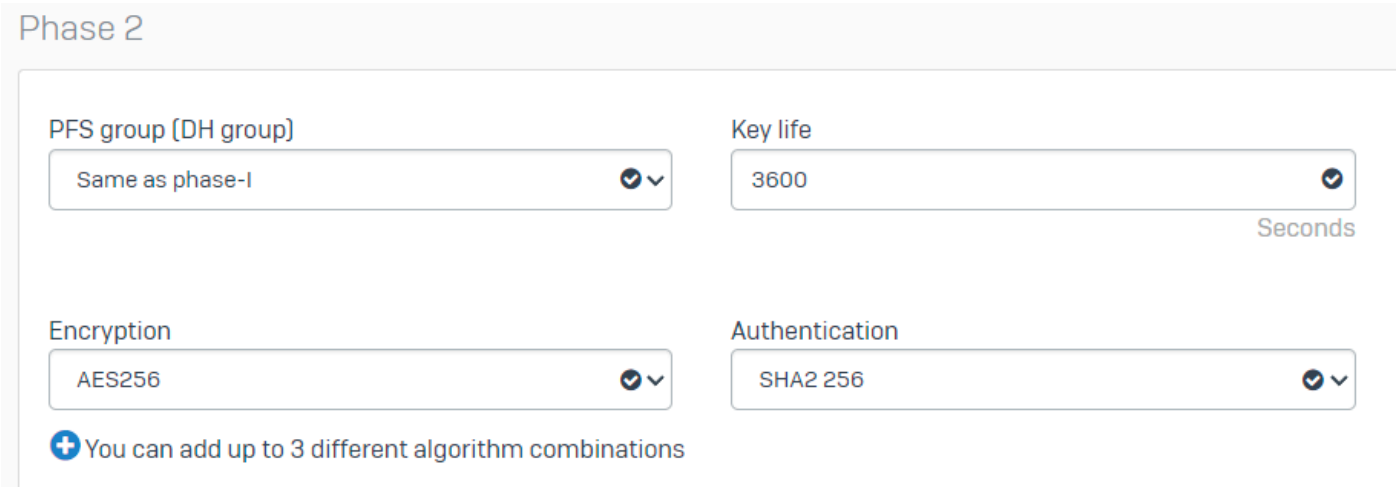
- **Key Life**:28800
- **DH group(key group)**: Seleccione 19 y 20
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin:360 (Default)
- **Randomize re-keying margin by**:50 (Default)



Sophos - Perfiles IPsec - Fase 1

En **Phase 2** configurar:

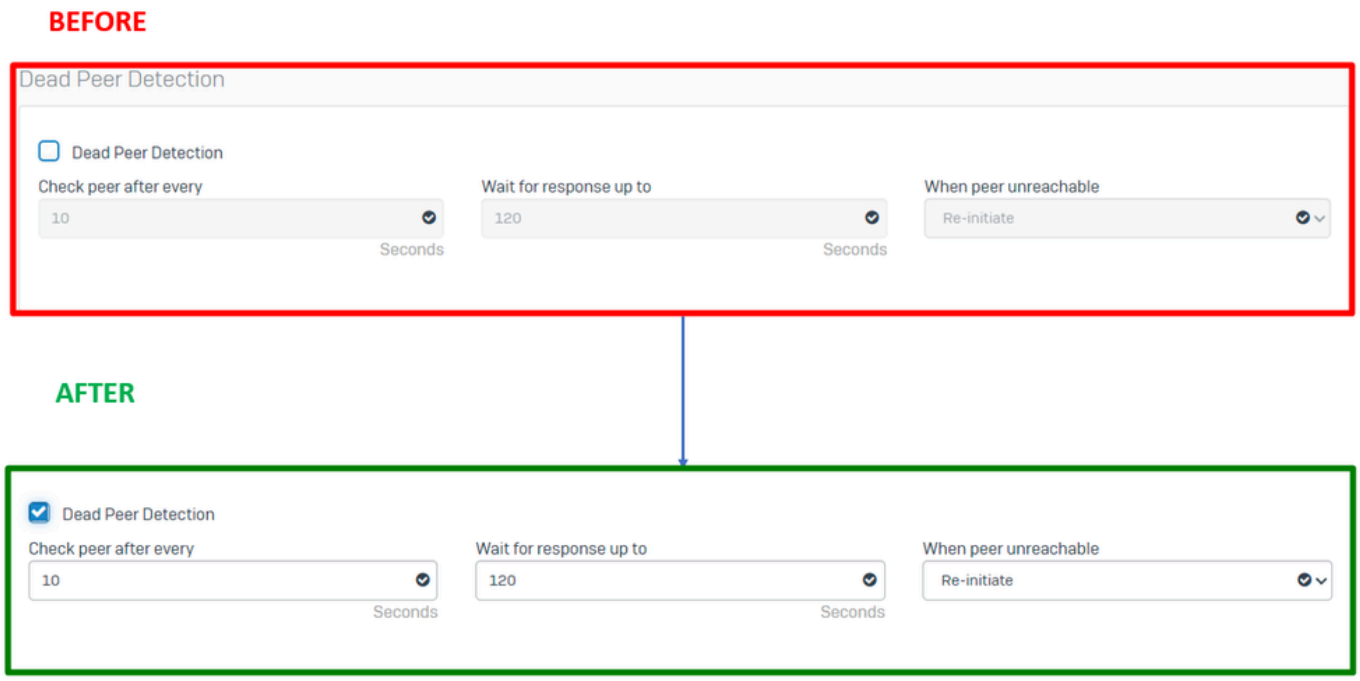
- PFS group (DH group): igual que en la fase I
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256



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)

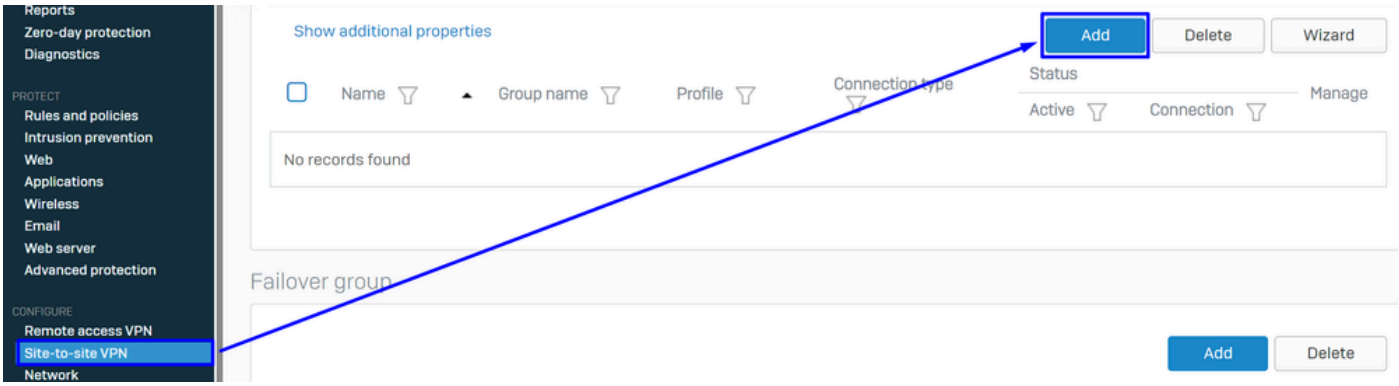


Sophos - Perfiles IPsec - Detección de puntos inactivos

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

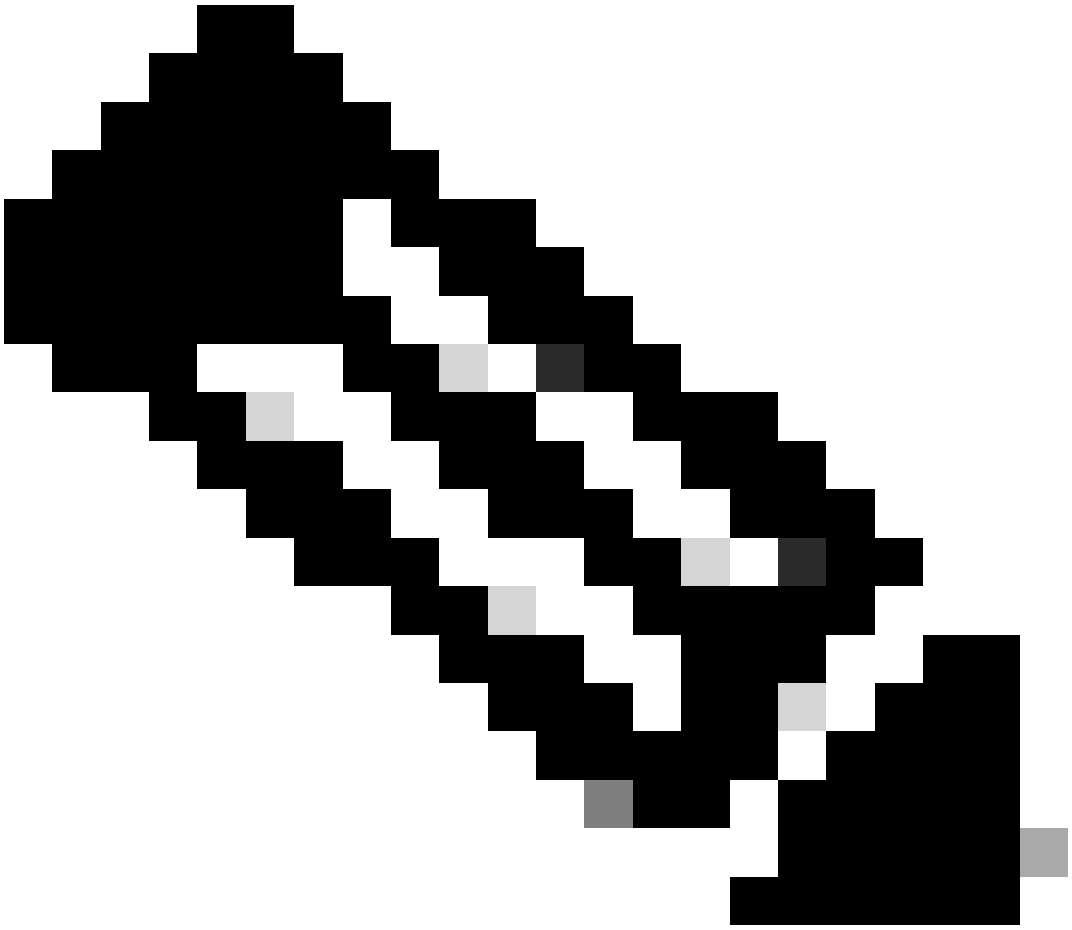
Para iniciar la configuración de la VPN, haga clic en **Site-to-site VPN** y, a continuación, en **Add**.



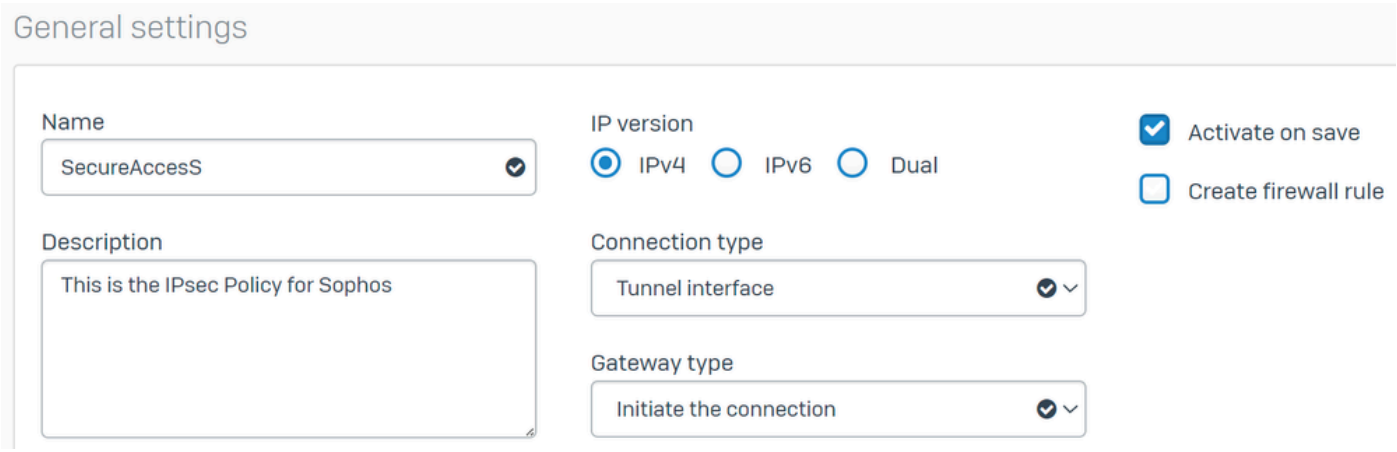
Sophos: VPN de sitio a sitio

En **General Settings** configurar:

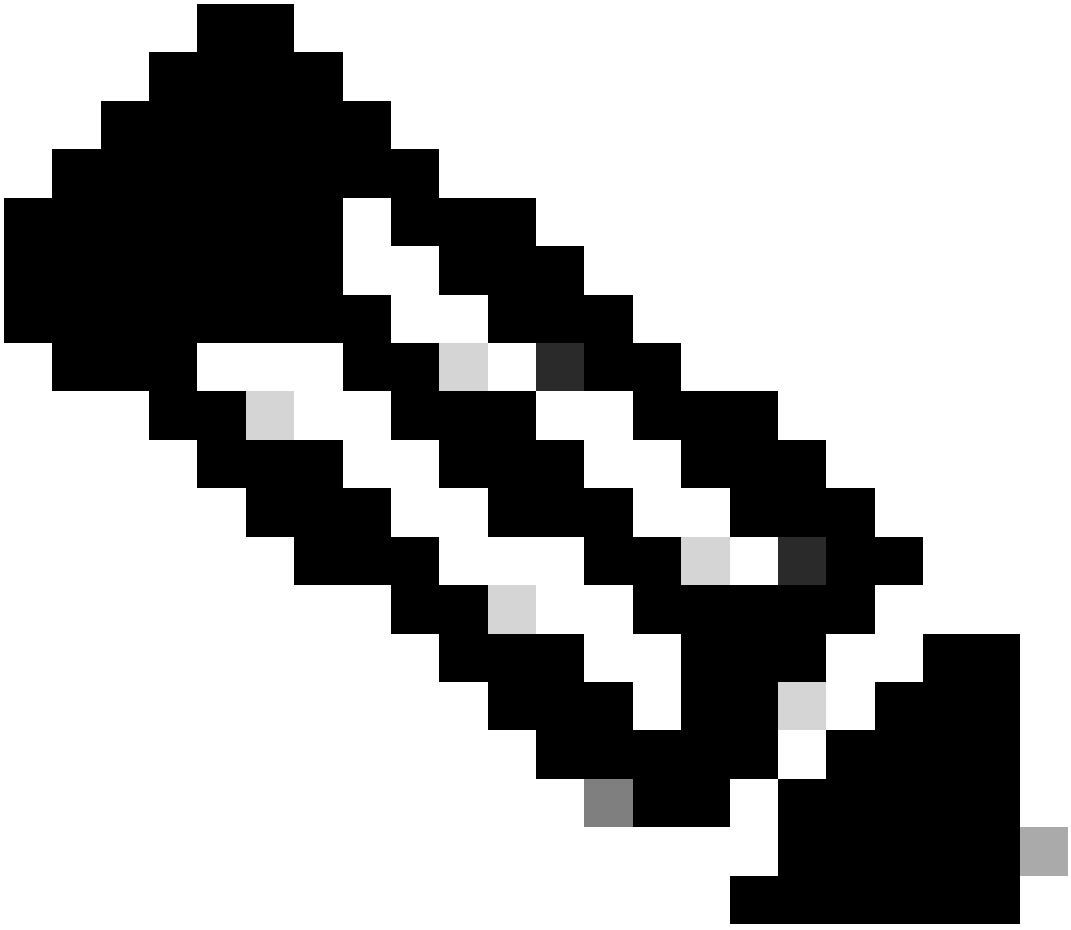
- **Name**: un nombre de referencia a la política IPSec de Cisco Secure Access
- IP version:IPv4
- Connection type: Interfaz de túnel
- Gateway type: inicia la conexión
- Active on save: Marque la opción



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



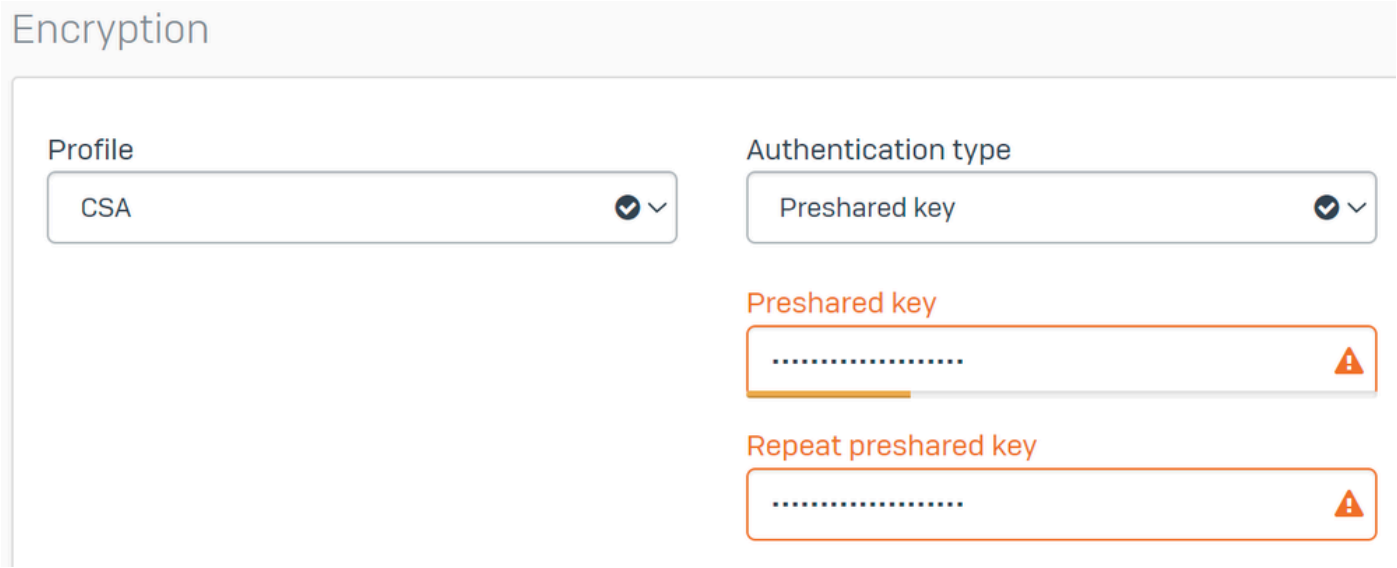
Sophos - VPN de sitio a sitio - Configuración general



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**

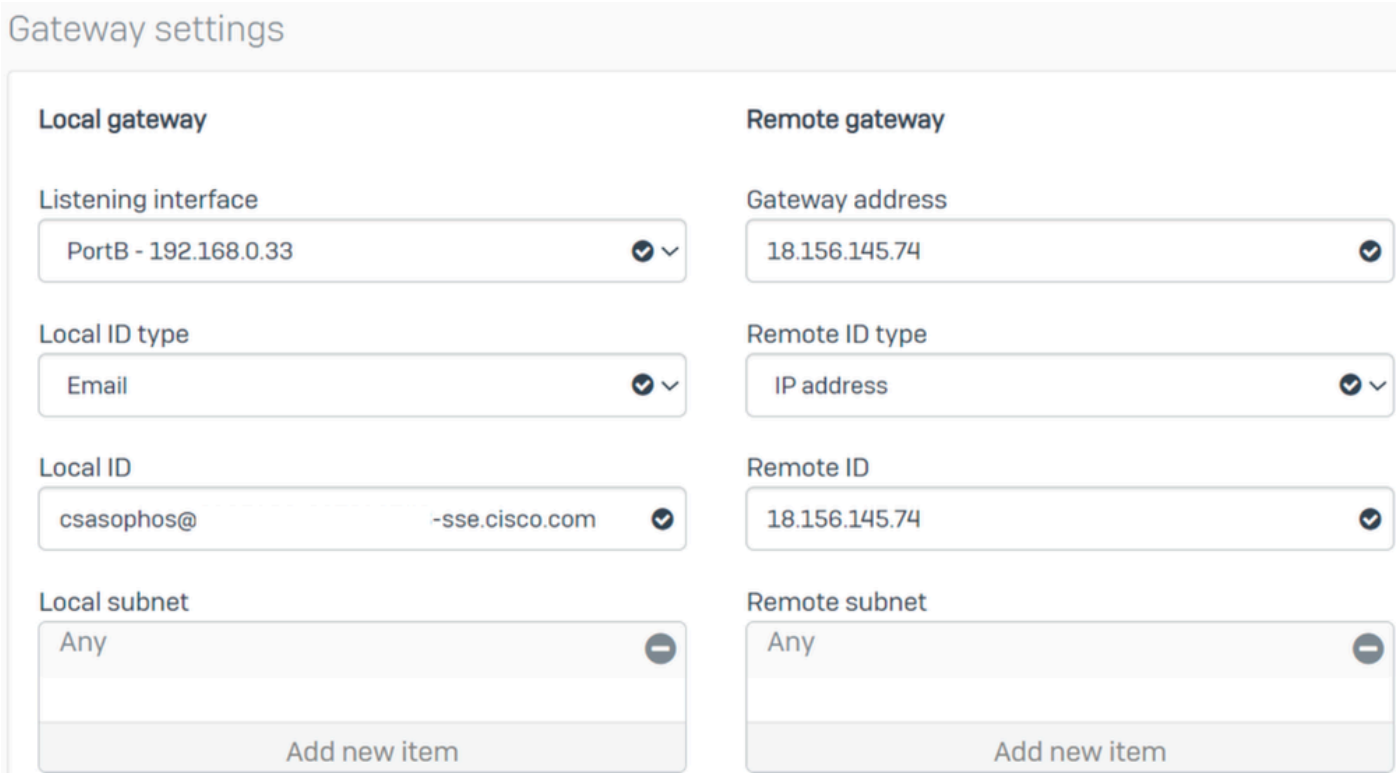


Sophos: VPN de sitio a sitio: cifrado

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

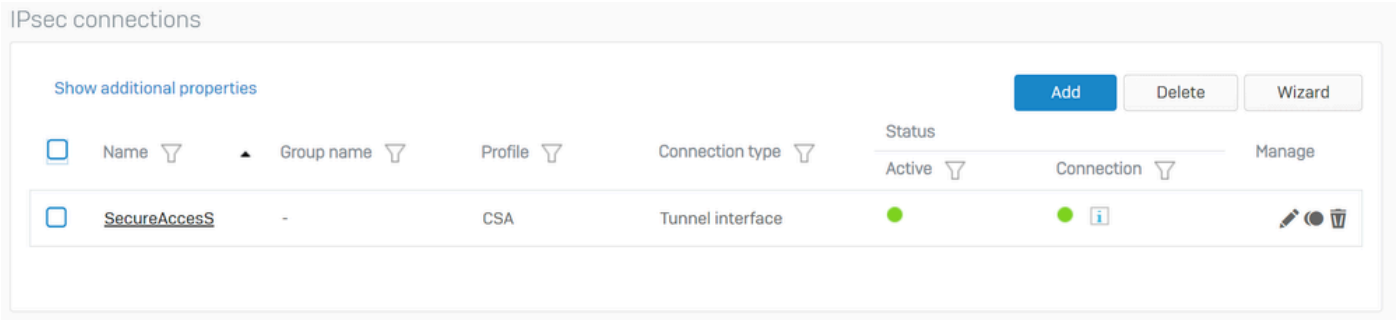
Gateway local	Gateway remoto
Interfaz de escucha Su Interfaz De Internet Wan	Dirección de gateway La IP pública generada en el paso, **Tunnel Data**
Tipo de ID local Correo electrónico	Tipo de ID remoto Dirección IP

ID local El correo electrónico generado en el paso, **Tunnel Data**	ID remoto La IP pública generada en el paso, **Tunnel Data**
Subred local cualquiera	Subred remota cualquiera

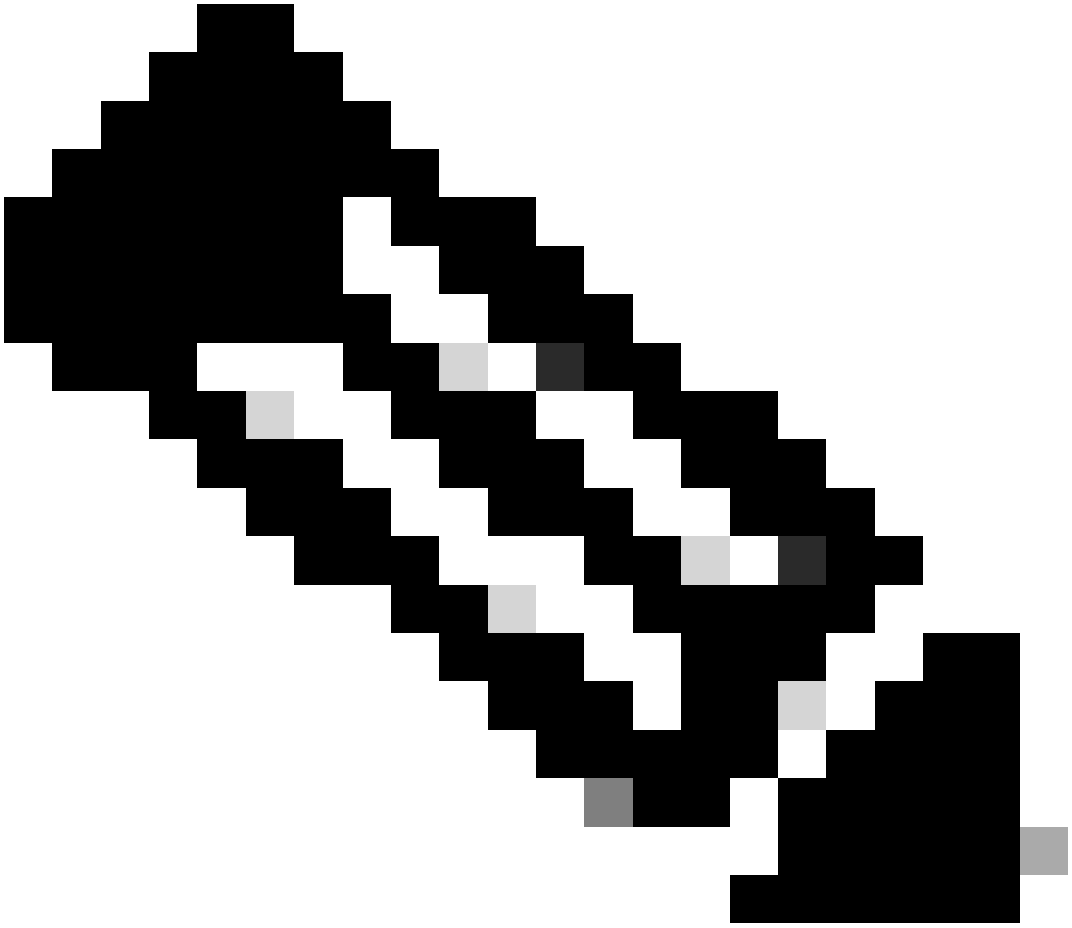


Sophos - VPN de sitio a sitio - Configuración de gateway

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

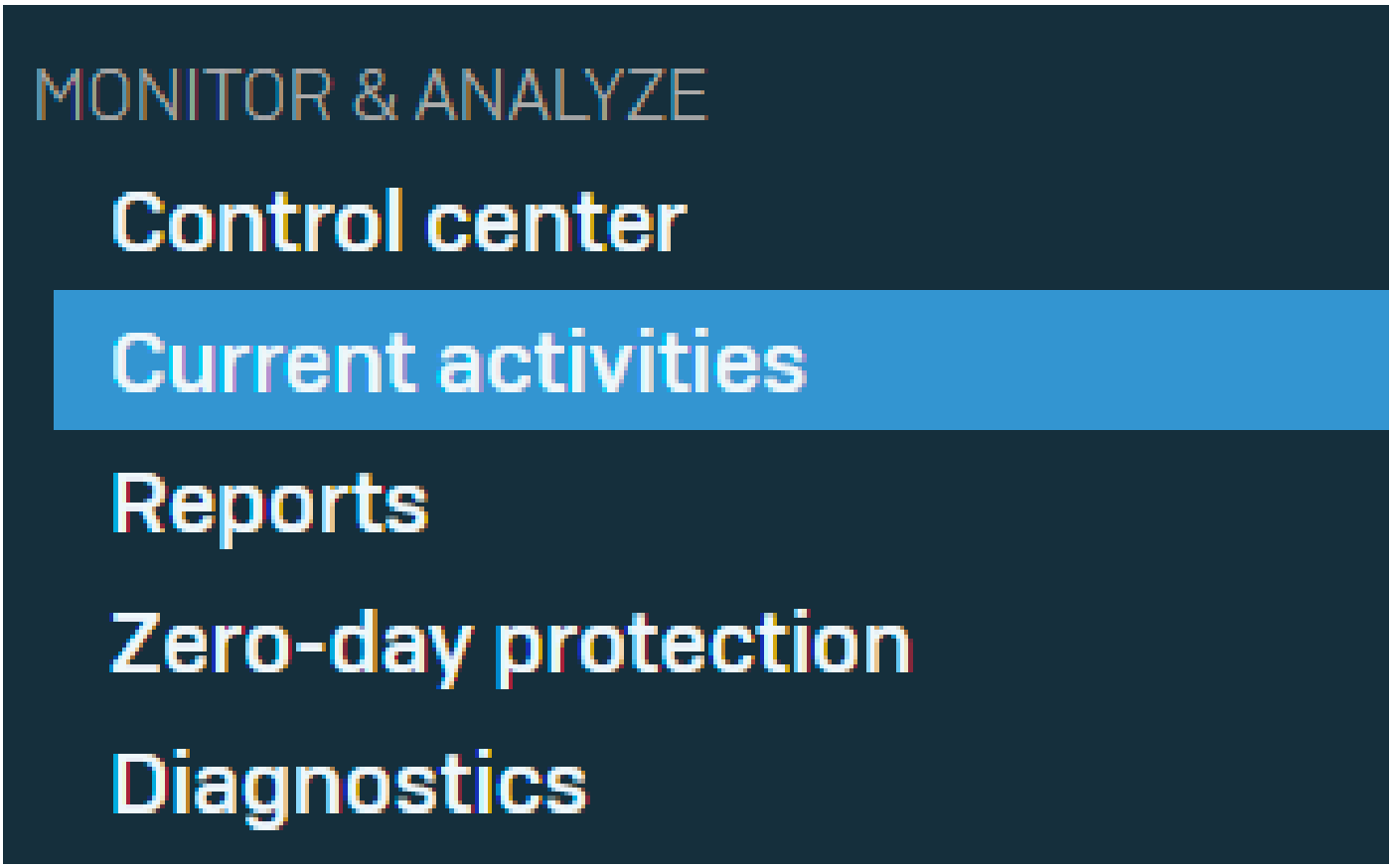


Sophos: VPN de sitio a sitio: conexiones IPsec

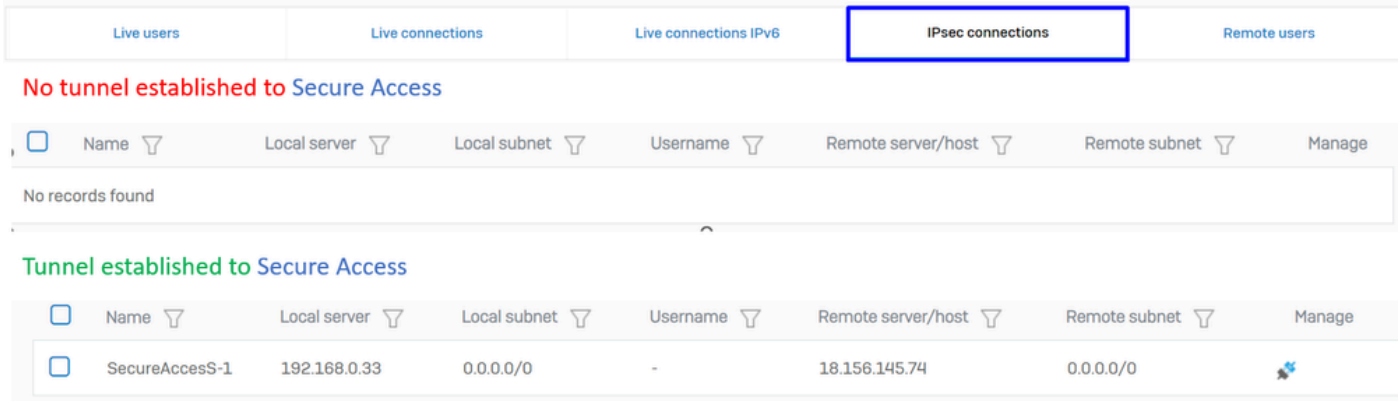


Nota: Para comprobar si el túnel está correctamente activado en la última imagen, puede comprobar el **Connection** estado; si está en verde, el túnel está conectado si no está en verde y el túnel no está conectado.

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



Sophos - Supervisión y análisis - IPsec



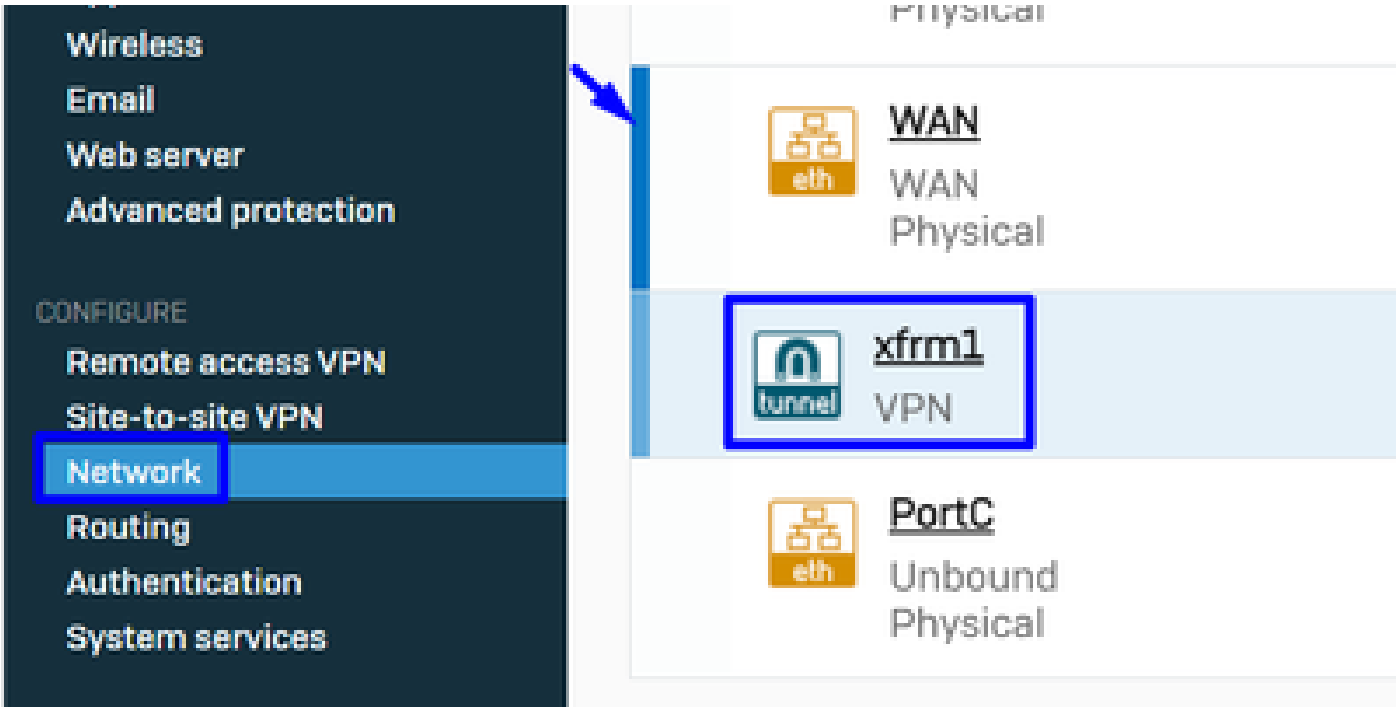
Sophos - Supervisión y análisis - IPSec antes y después

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

Sophos - Red - Interfaz de túnel - Configuración

Configuración de las puertas de enlace

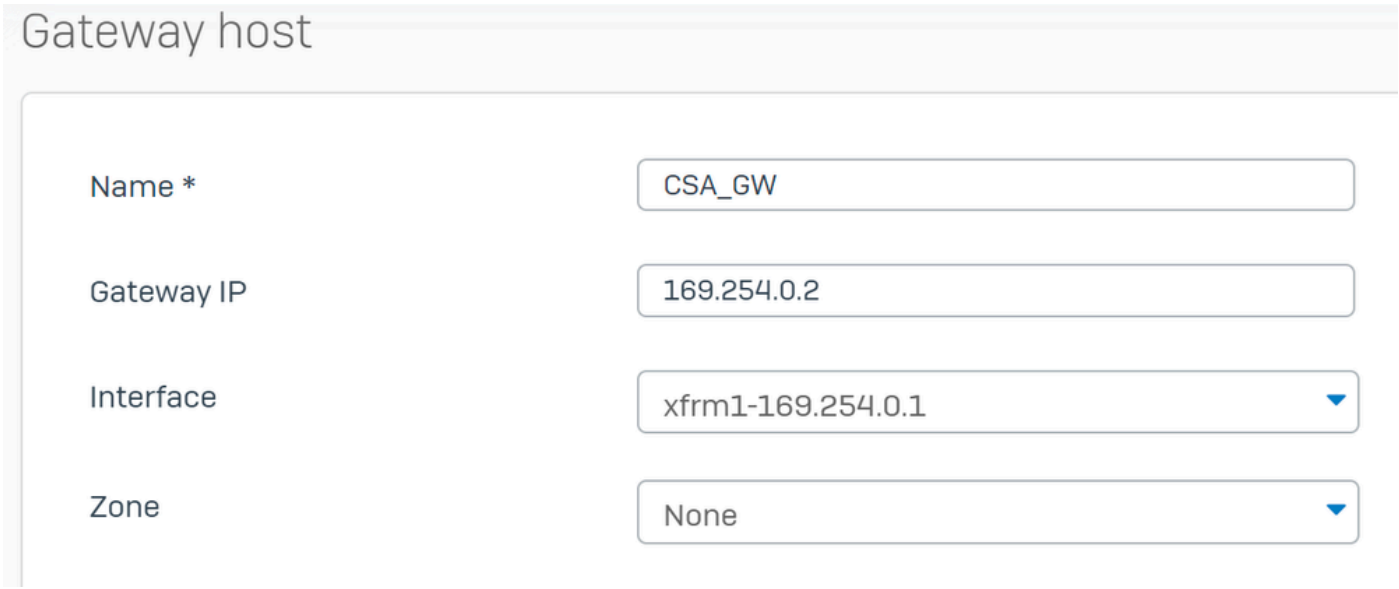
Para configurar el gateway para la interfaz virtual (xfrm)

- Desplácese hasta Routing > Gateways
- Haga clic en Add

Sophos - Routing - Puertas de enlace

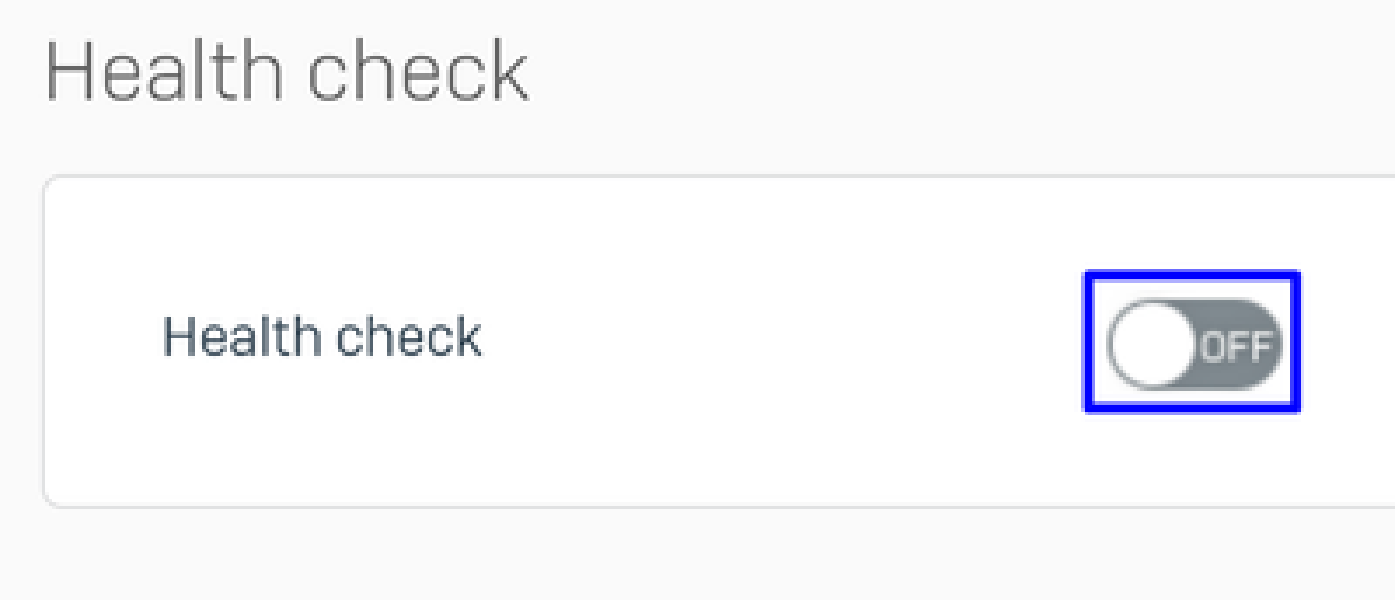
En **Gateway host** configurar:

- **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)



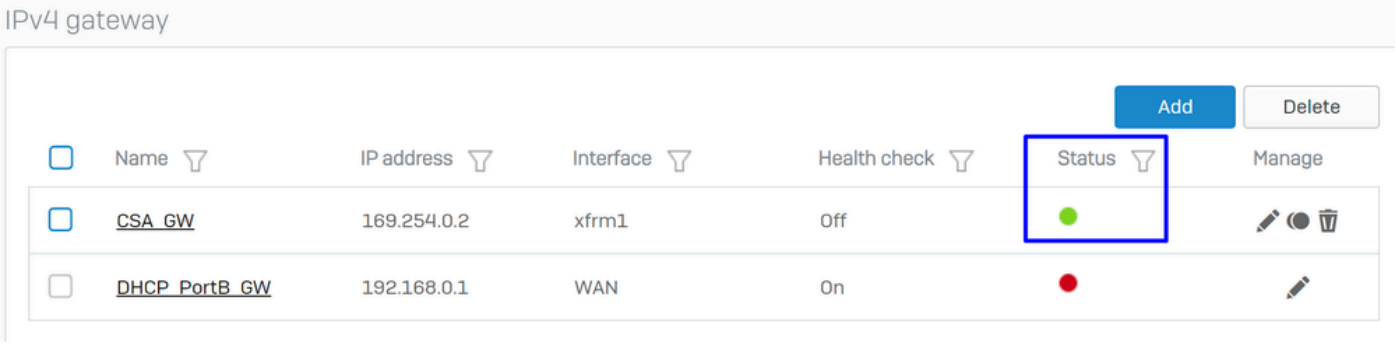
Sophos - Routing - Puertas de enlace - Host de puerta de enlace

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



Sophos - Routing - Gateways - Comprobación de estado

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



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.

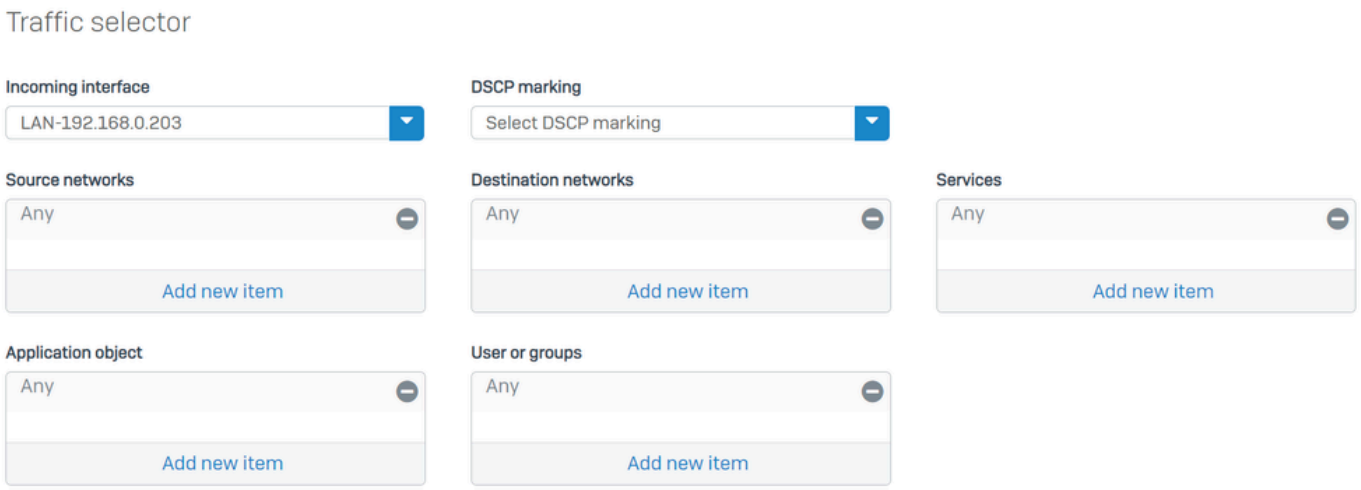
Desplácese hasta **Routing > SD-WAN routes.**

- 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

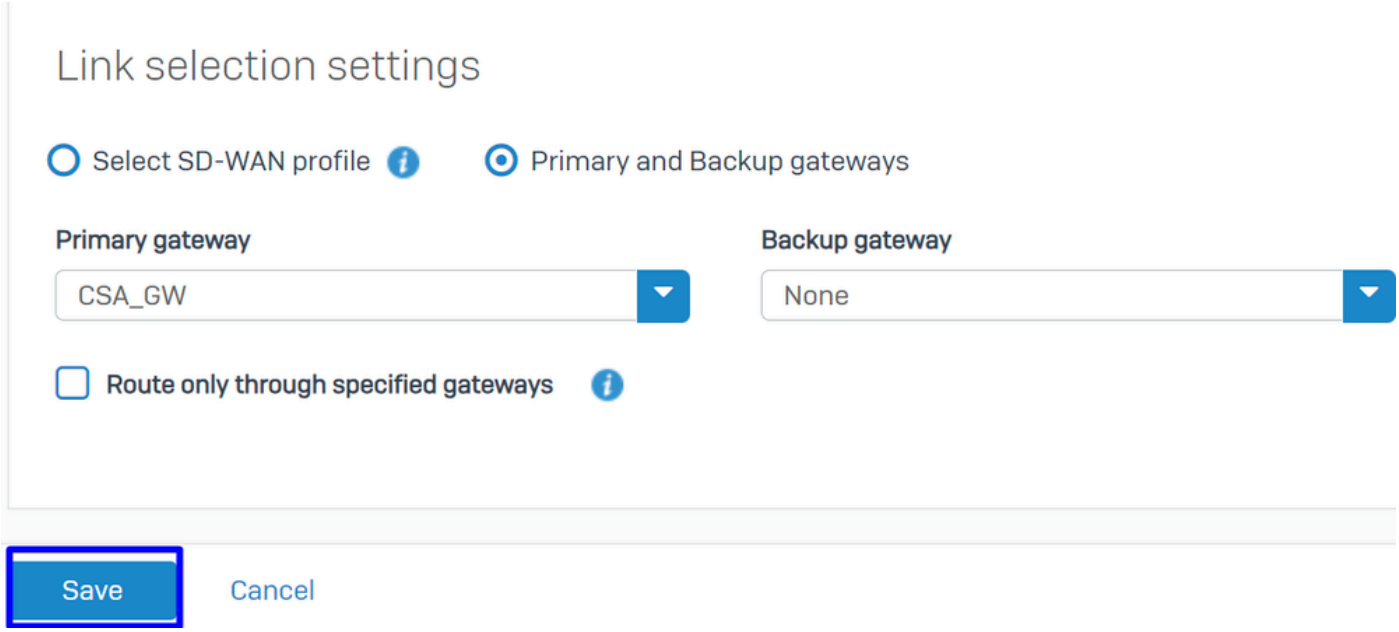


Sophos - Rutas SD-Wan - Selector de tráfico

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**



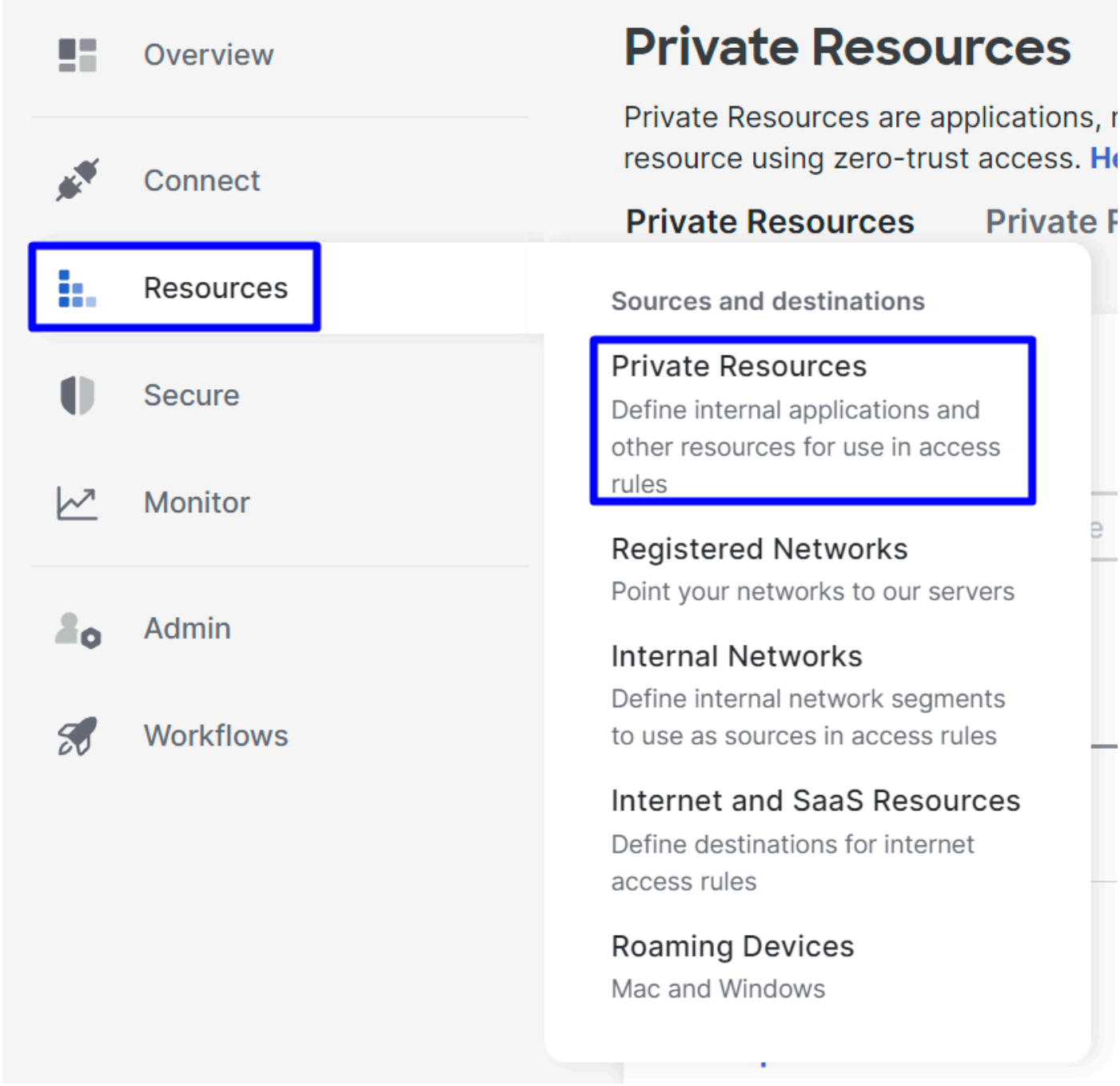
Sophos - Rutas SD-Wan - Selector de tráfico - Gateways primarios y de respaldo

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

Configurar aplicación privada

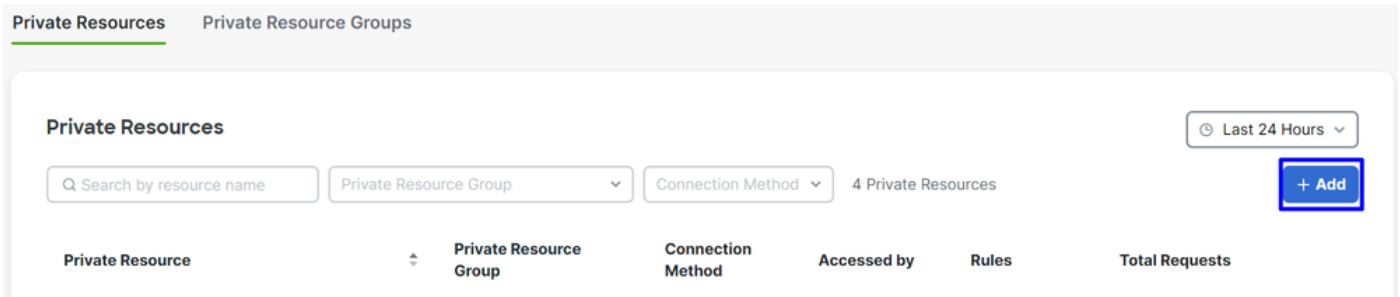
Para configurar el acceso a la aplicación privada, inicie sesión en el Portal de administración.

- Desplácese hasta **Resources > Private Resources**



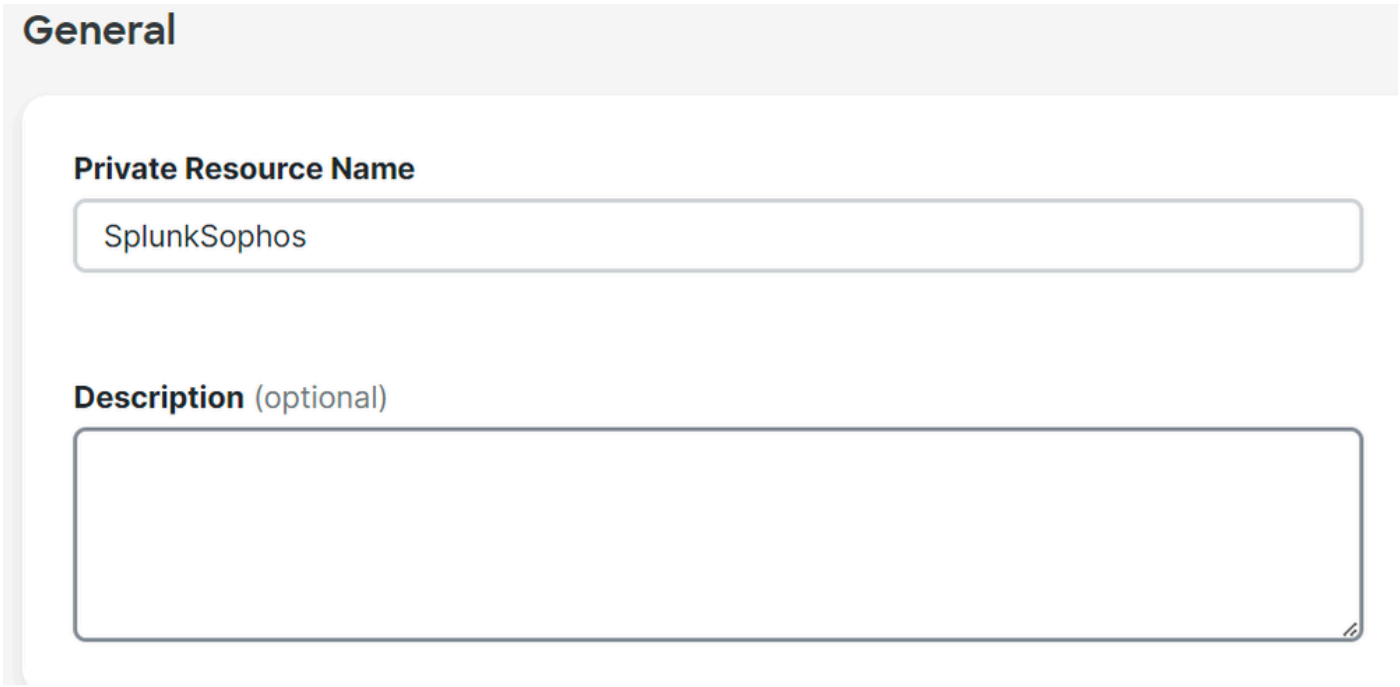
Acceso seguro - Recursos privados

- Haga clic en + Add



Acceso seguro - Recursos privados 2

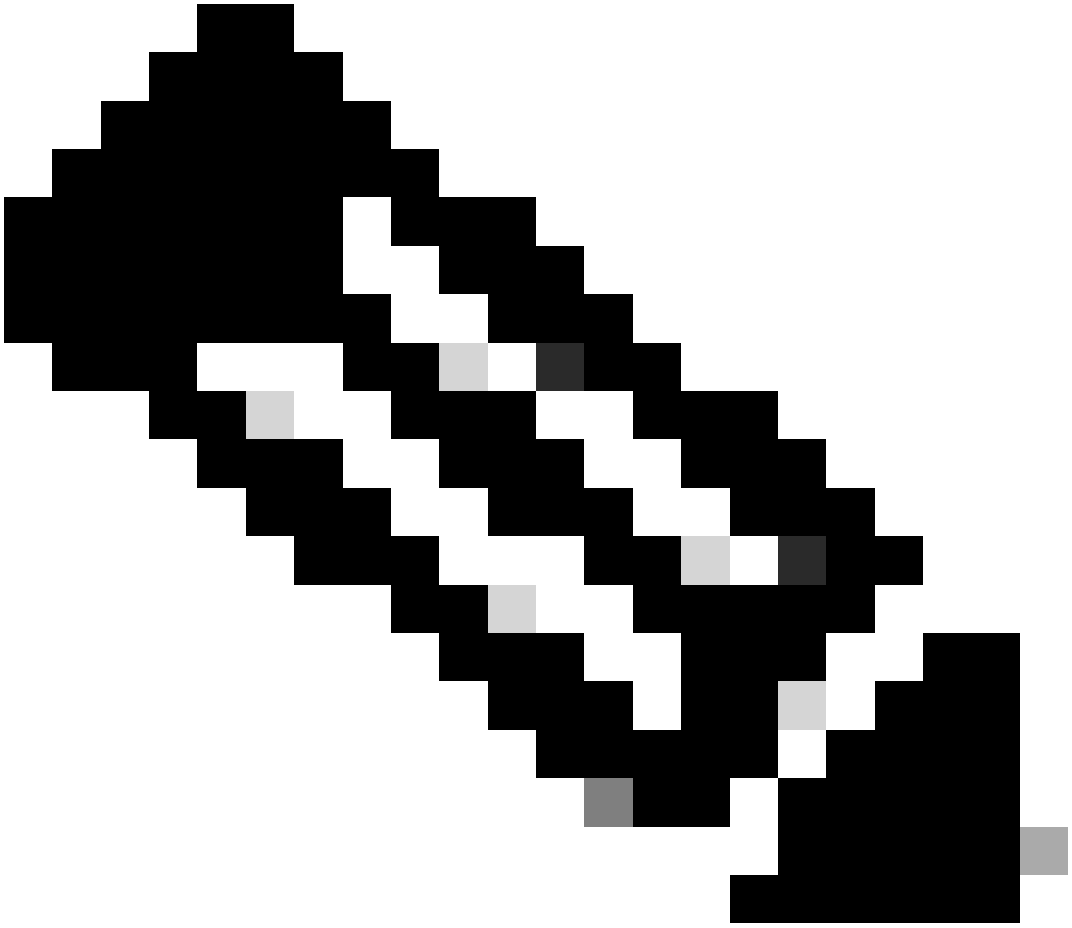
- En **General** Configurar el **Private Resource Name**



Acceso seguro - Recursos privados - General

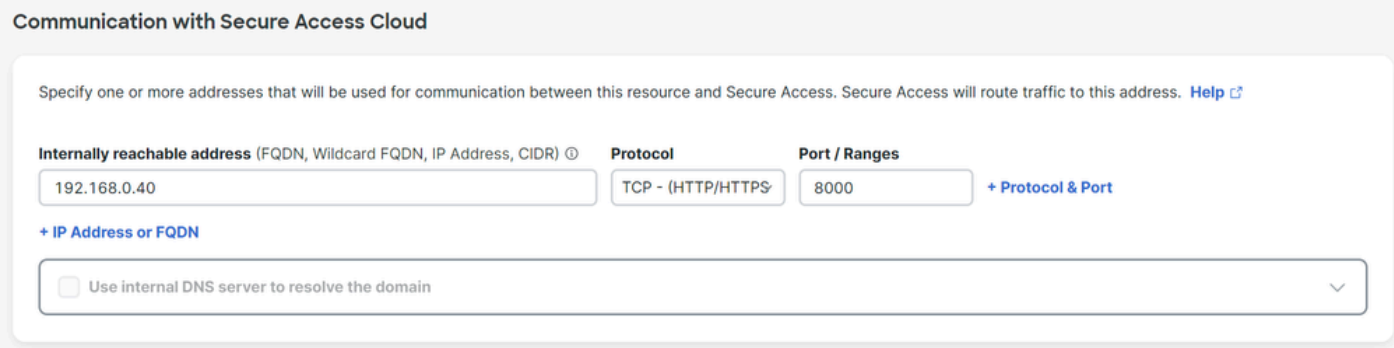
En **Communication with Secure Access Cloud** configurar:

- I**nternally 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**.

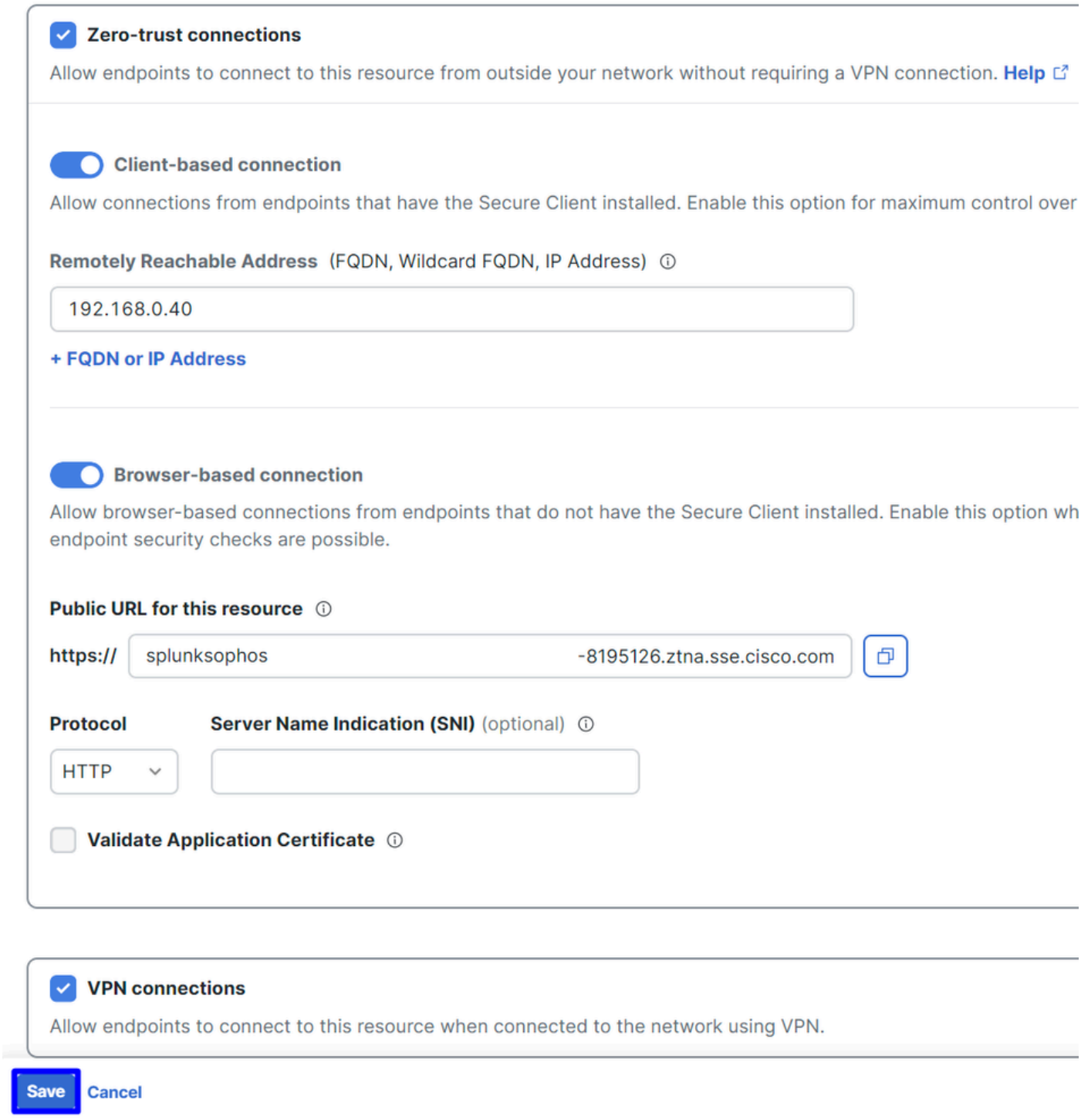
- **Protocol**: seleccione el protocolo que utiliza para acceder a ese recurso
- Port / Ranges : seleccione los puertos que necesita habilitar para acceder a la aplicación



Acceso seguro - Recursos privados - Comunicaciones con acceso seguro Nube

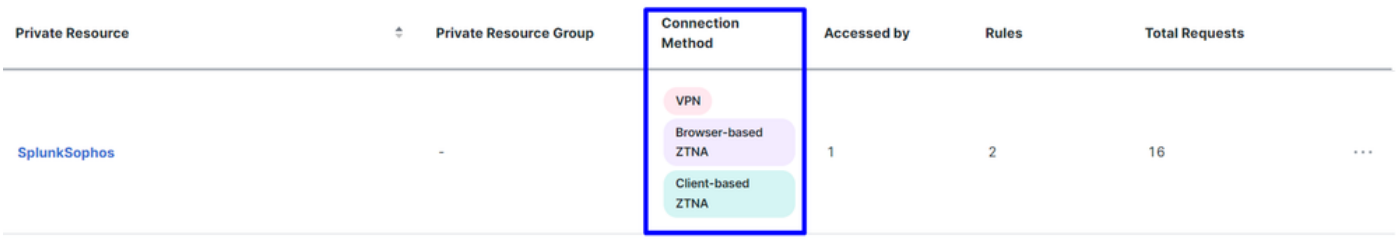
Dentro **Endpoint Connection Methods** de , configure todas las formas posibles de acceder a los recursos privados a través de Secure Access y elija los métodos que desea utilizar para su entorno:

- **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**



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

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

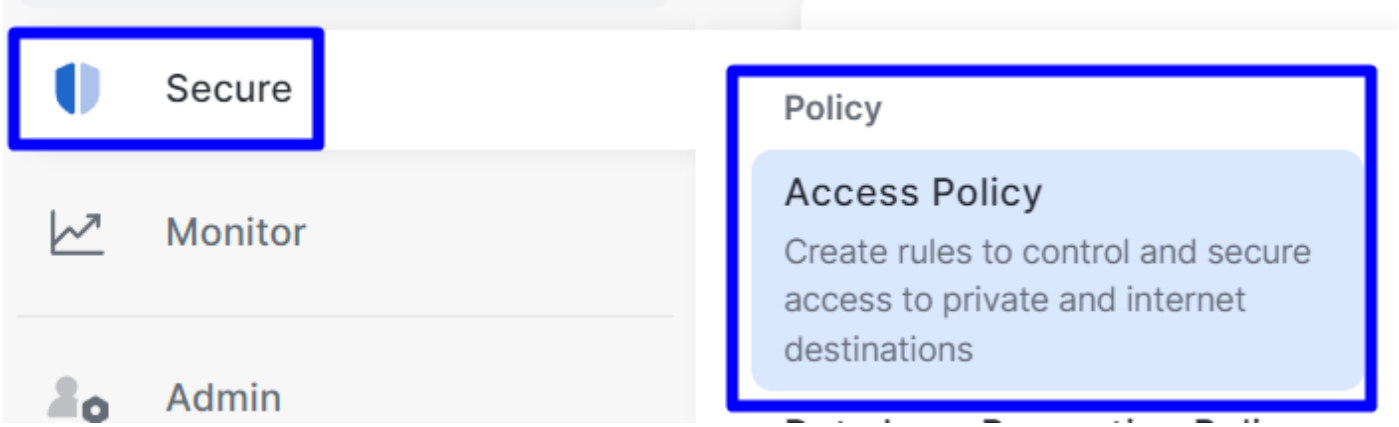


Acceso seguro: recursos privados configurados

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

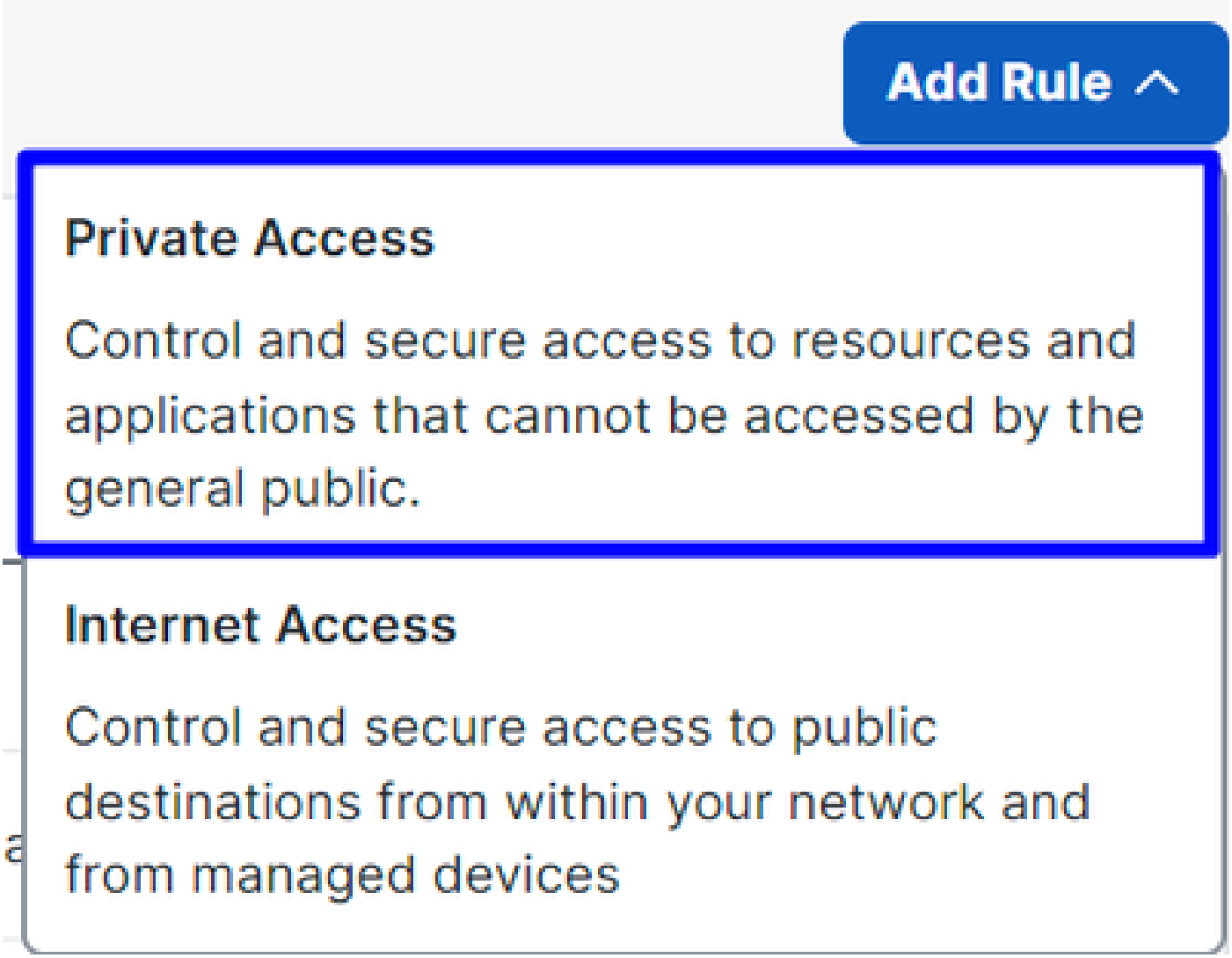
Configuración de la política de acceso

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



Acceso seguro - Política de acceso

- Haga clic en **Add Rule > Private Access**

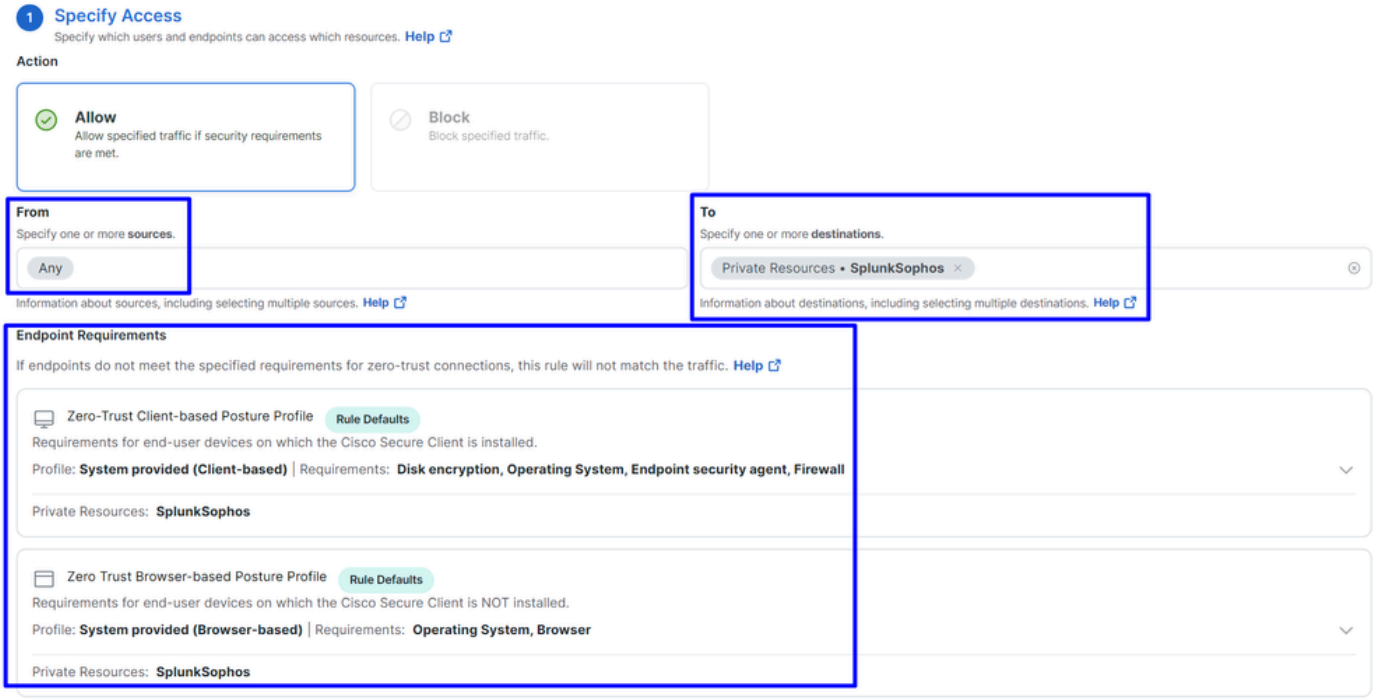


Acceso seguro - Política de acceso - Acceso privado

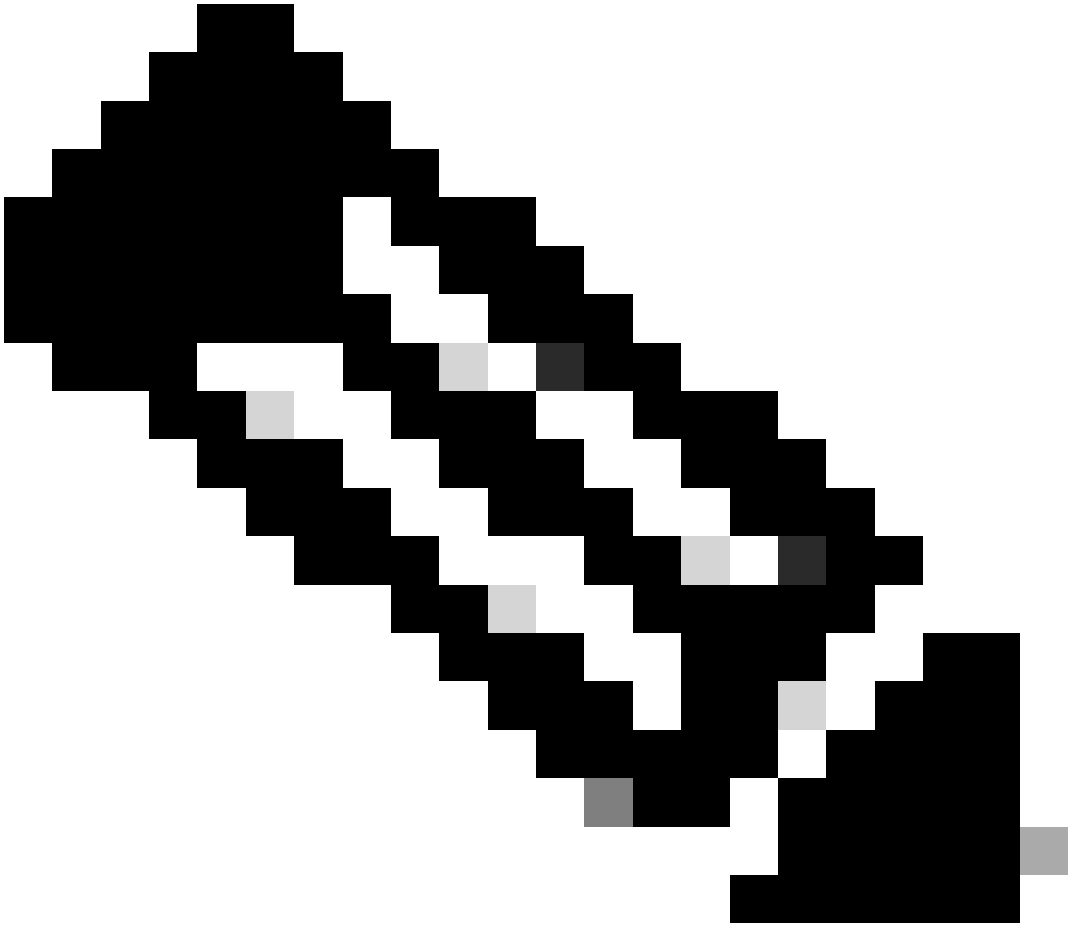
Configure las siguientes opciones para proporcionar acceso a través de varios métodos de autenticación:

- 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**



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

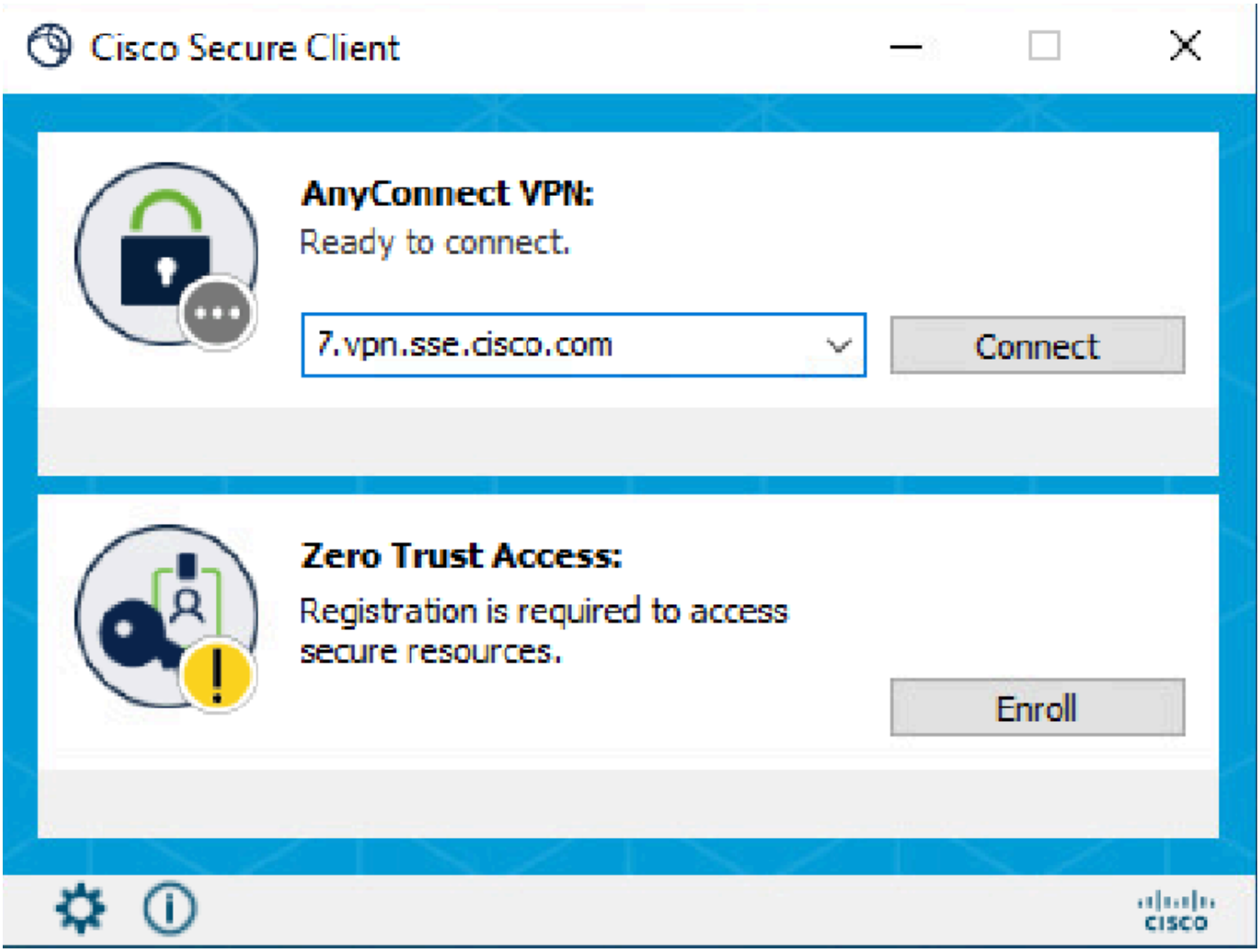
Después de esto, puede continuar con el paso Verify.

Verificación

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

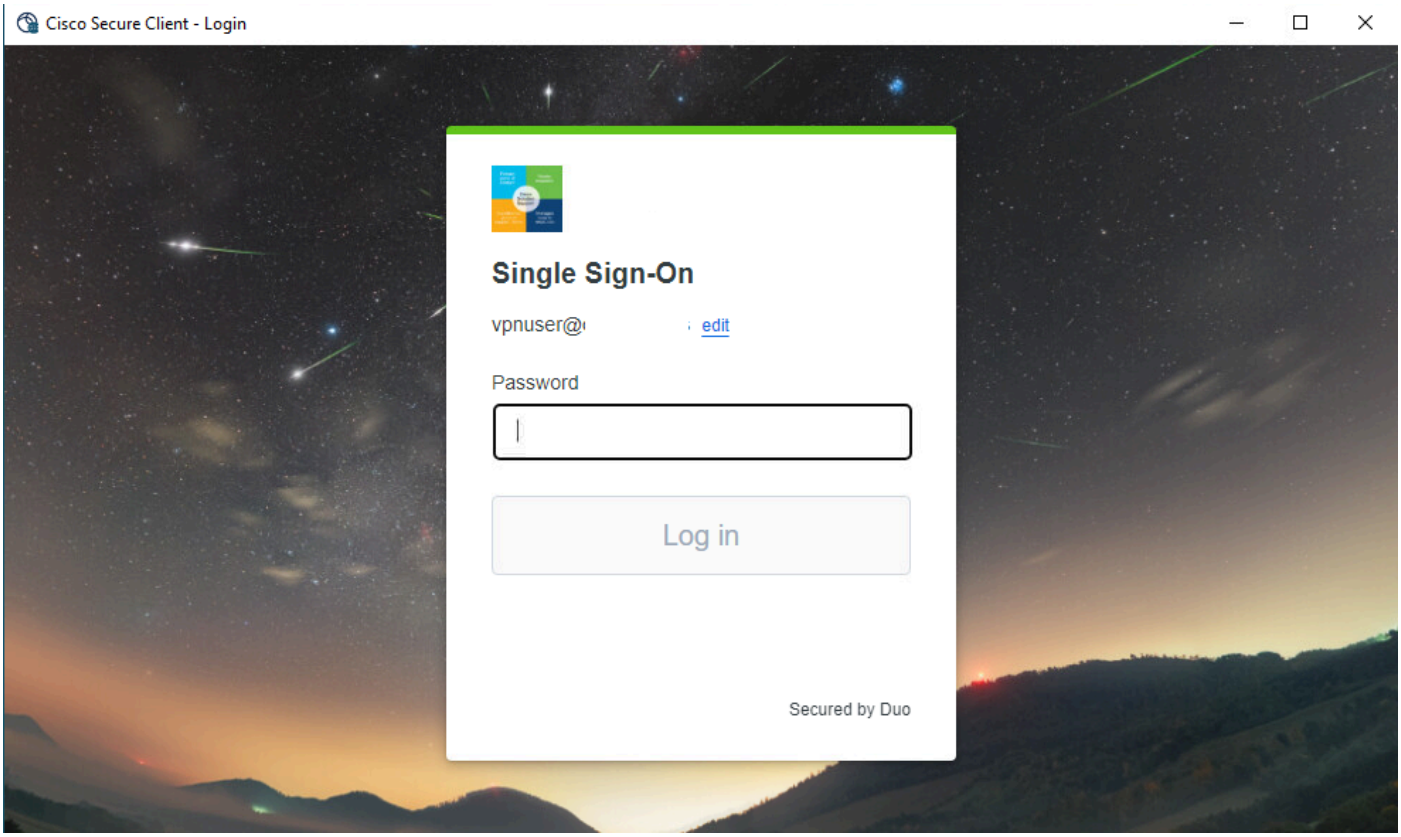
VPN de RA

Inicie sesión mediante Cisco Secure Client Agent-VPN.



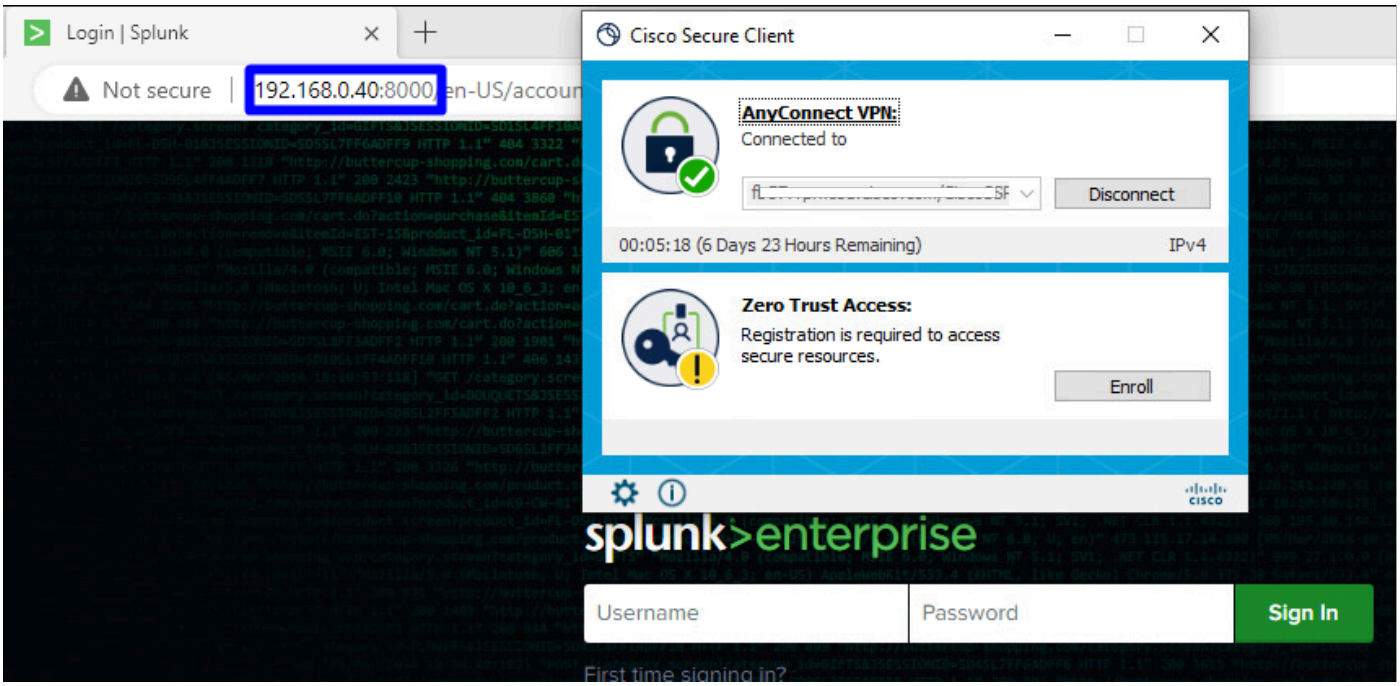
Cliente seguro - VPN

- Autenticar mediante su proveedor de SSO



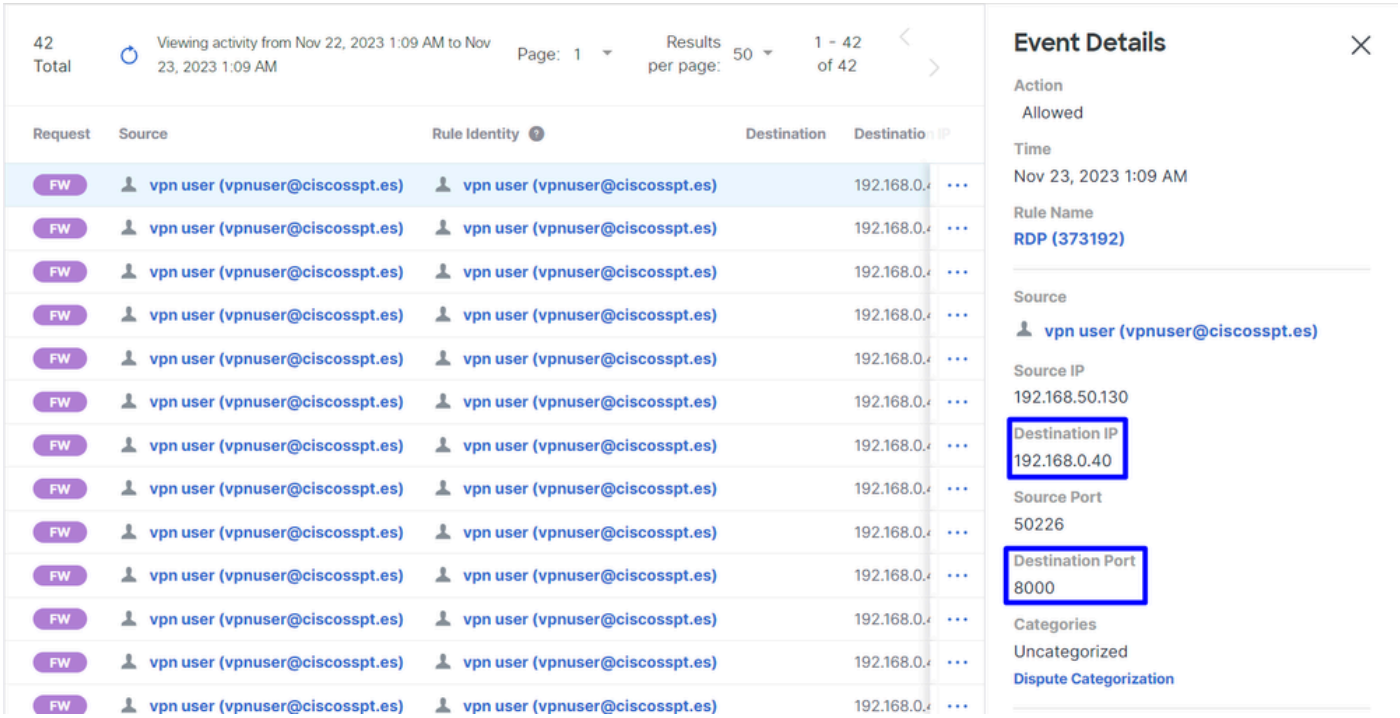
Acceso seguro - VPN - SSO

- Después de autenticarse, acceda al recurso:



Acceso seguro - VPN - Autenticado

Navegue hasta:Monitor > Activity Search

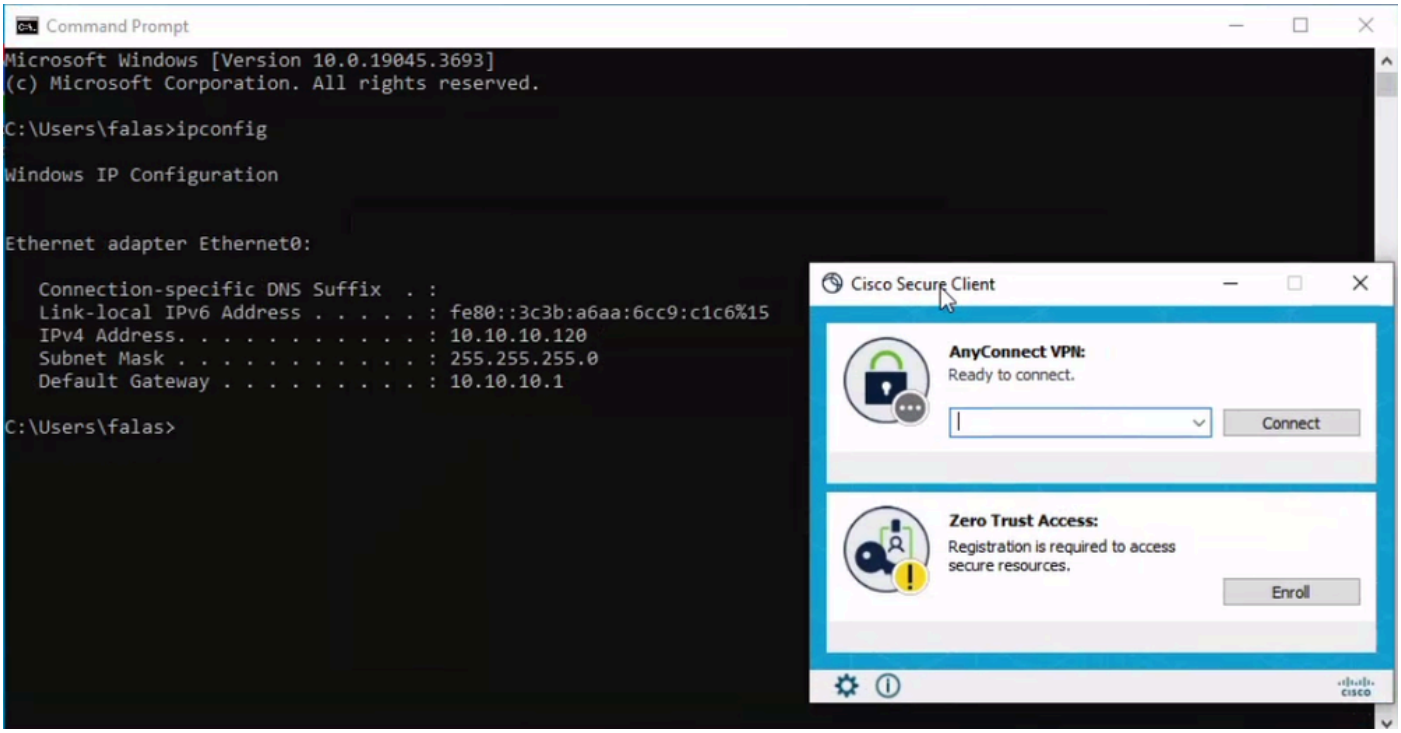


Acceso seguro - Búsqueda de actividad - RA-VPN

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

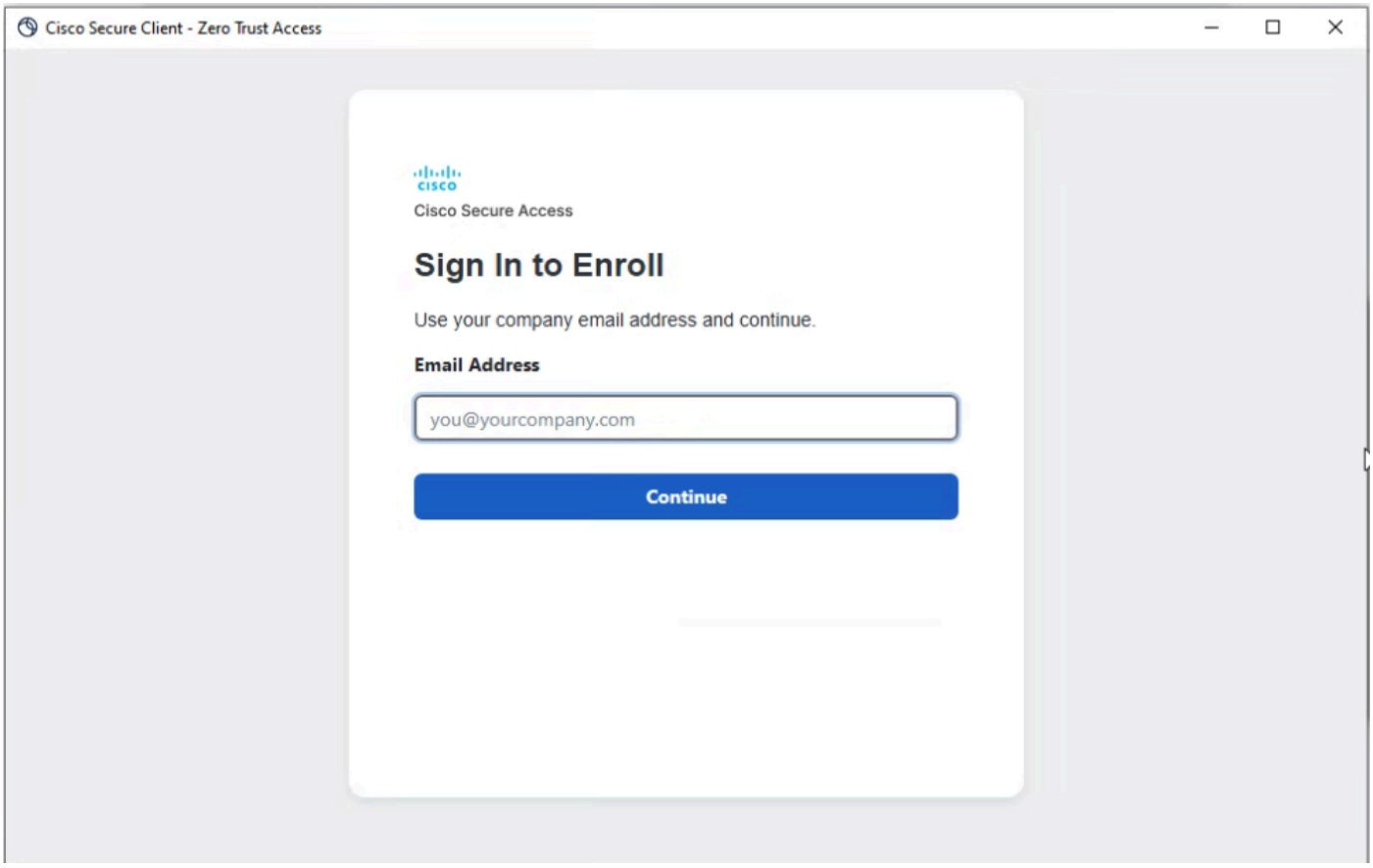
ZTNA de base cliente

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



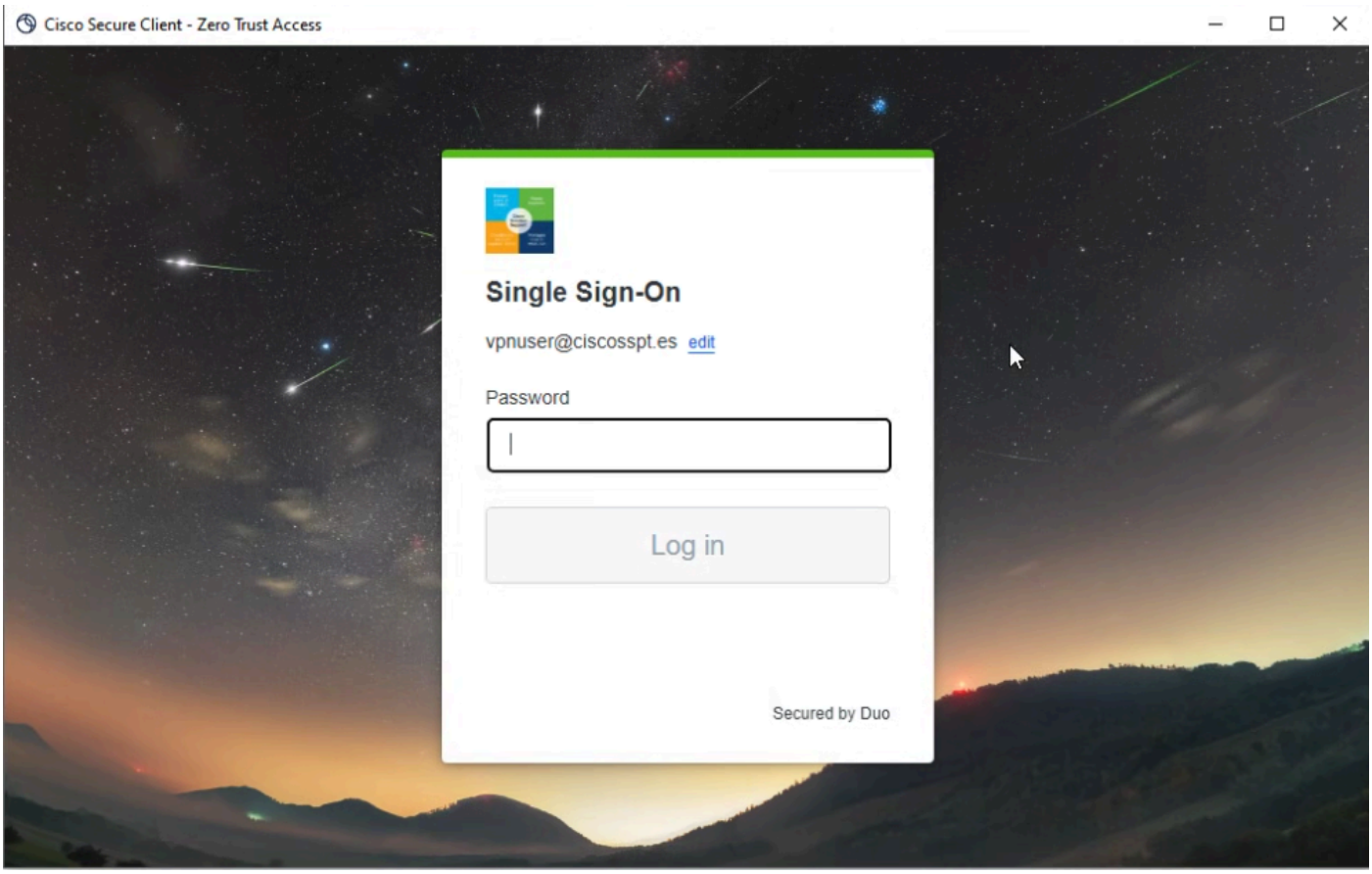
Cliente seguro: ZTNA

- Inscríbase con su nombre de usuario.



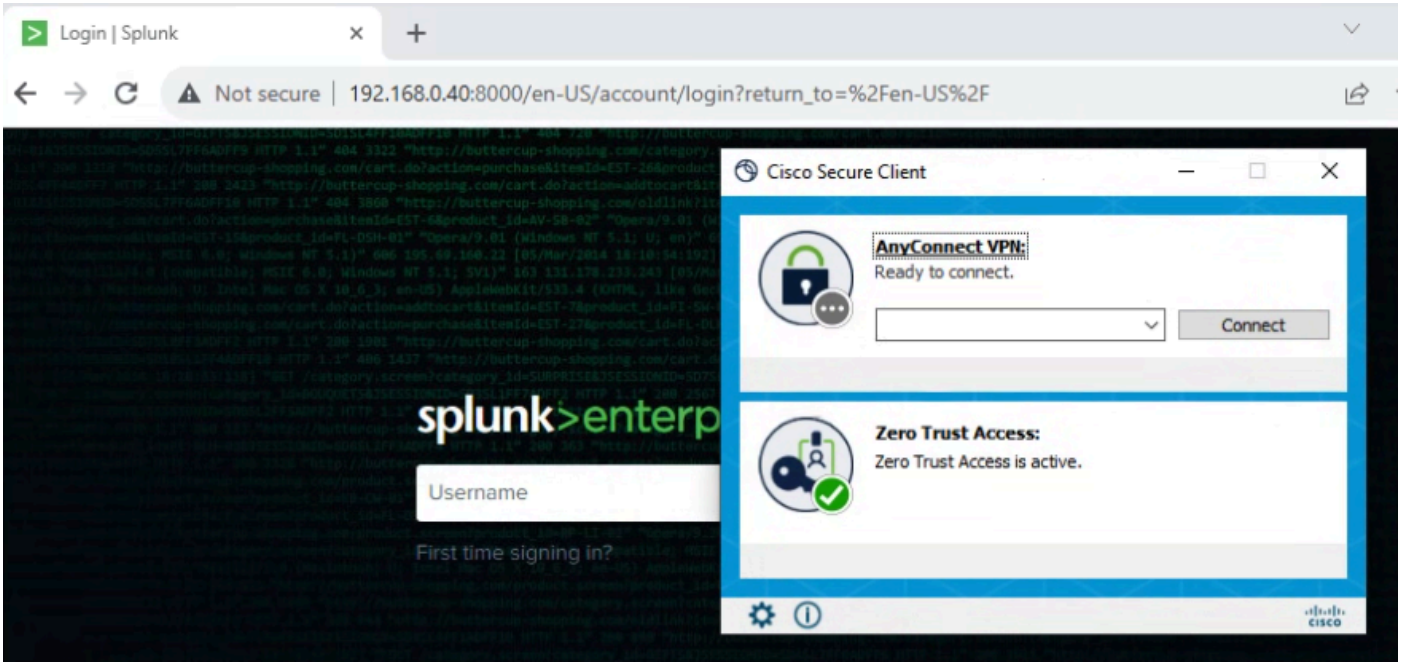
Secure Client - ZTNA - Inscripción

- Autenticar en su proveedor de SSO



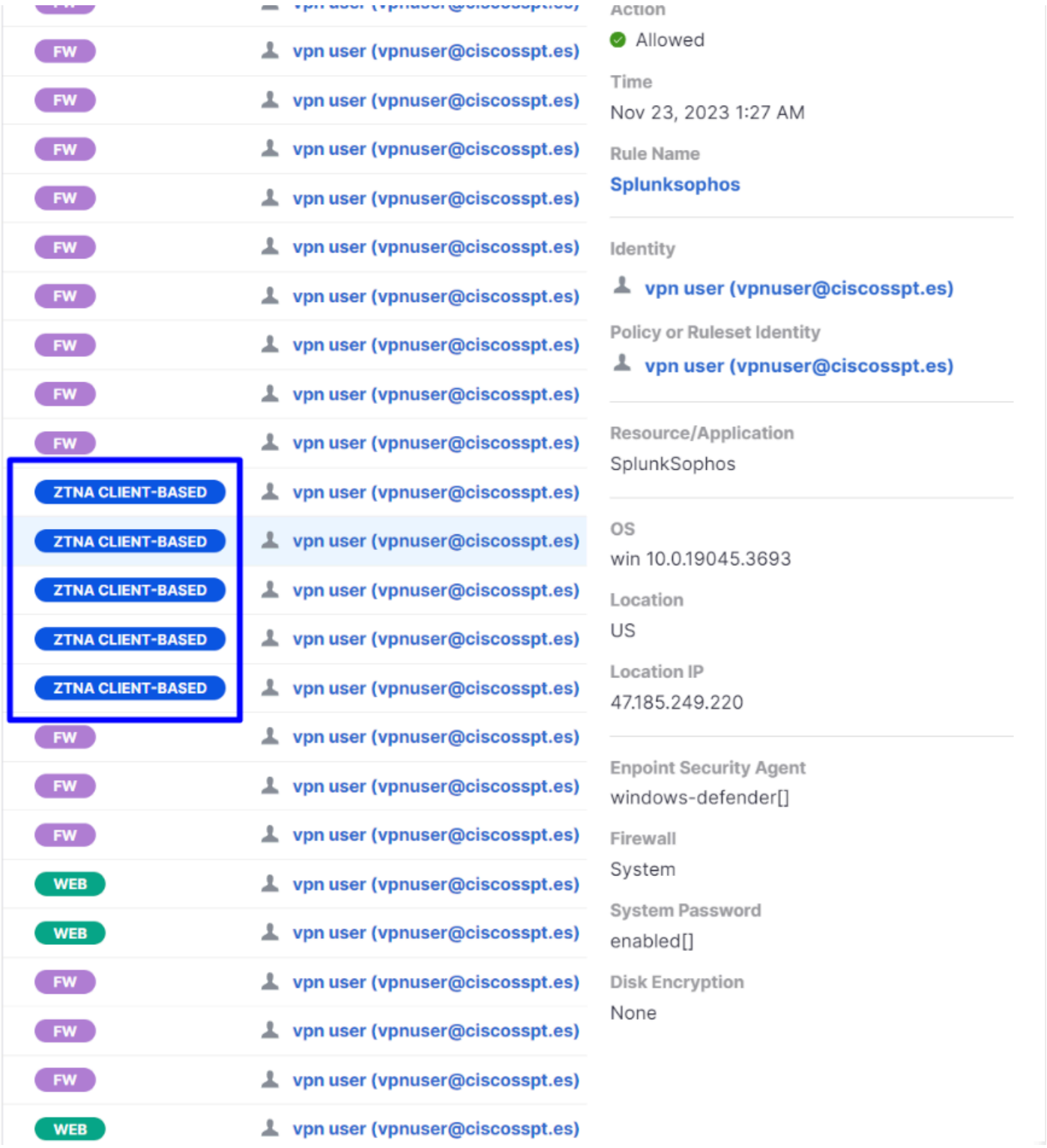
Secure Client - ZTNA - Inicio de sesión de SSO

- Después de autenticarse, acceda al recurso:



Acceso seguro - ZTNA - Registrado

Navegue hasta:Monitor > Activity Search

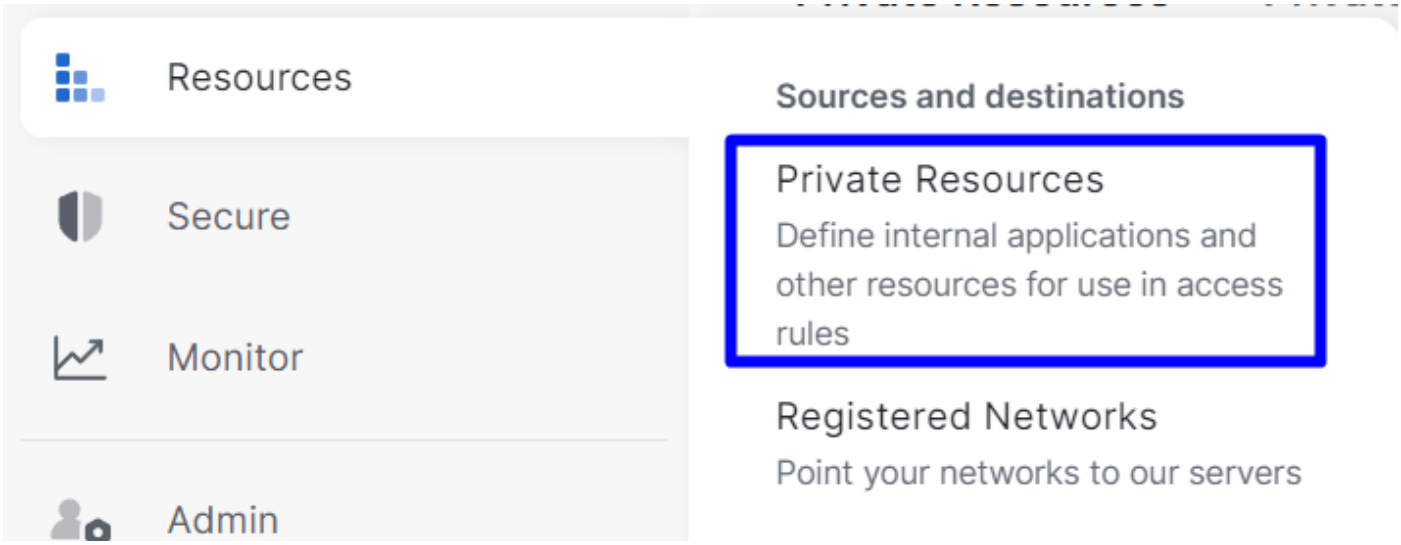


Acceso seguro - Búsqueda de actividad - Basado en cliente ZTNA

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

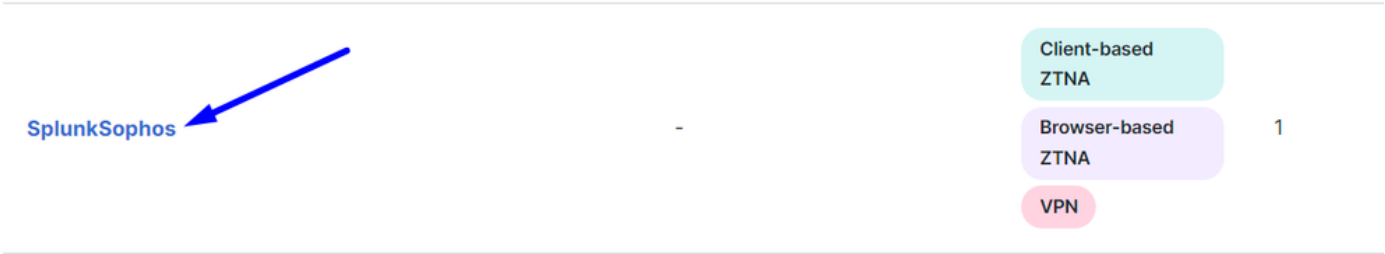
ZTNA basado en navegador

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



Acceso seguro - Recurso privado

- Haga clic en su política



Acceso seguro - Recursos privados - SplunkSophos

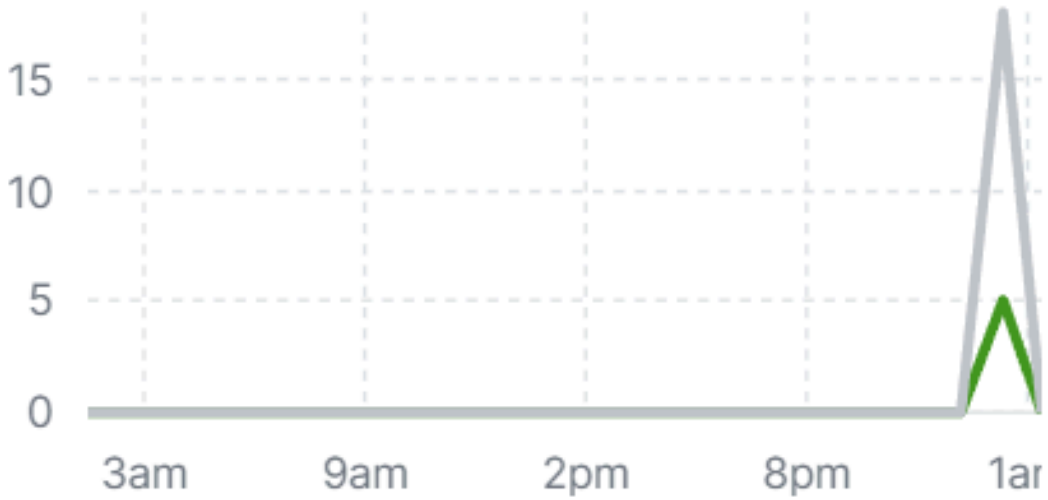
- Desplazarse hacia abajo

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

Acceso seguro - Recurso privado - Desplácese hacia abajo

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).