Configure o acesso seguro com o firewall Sophos XG

Contents

Introdução

Este documento descreve como configurar o acesso seguro com o Sophos XG Firewall.

Pré-requisitos

- Configurar Provisionamento de Usuário
- Configuração de Autenticação ZTNA SSO
- Configurar o acesso seguro da VPN de acesso remoto

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firewall Sophos XG
- Acesso seguro

- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA sem cliente

Componentes Utilizados

As informações neste documento são baseadas em:

- Firewall Sophos XG
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Acesso seguro - Sophos

A Cisco projetou o Secure Access para garantir a proteção e o fornecimento de acesso a aplicativos privados, tanto no local quanto baseados em nuvem. Ele também protege a conexão da rede à Internet. Isso é obtido por meio da implementação de vários métodos e camadas de segurança, todos voltados para preservar as informações à medida que elas são acessadas pela

nuvem.

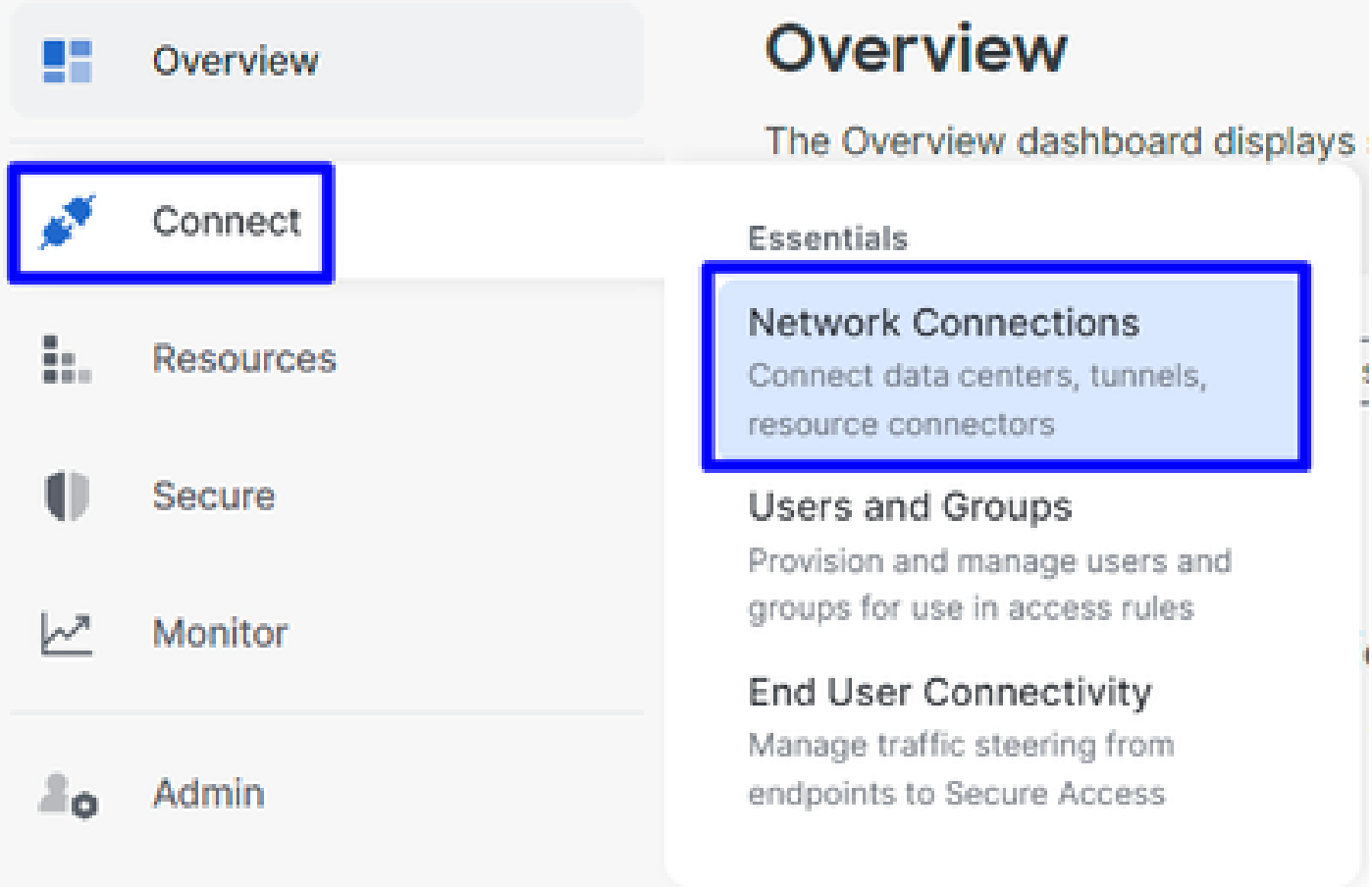
Configurar

Configurar o túnel no acesso seguro

Navegue até o painel de administração do Secure Access.

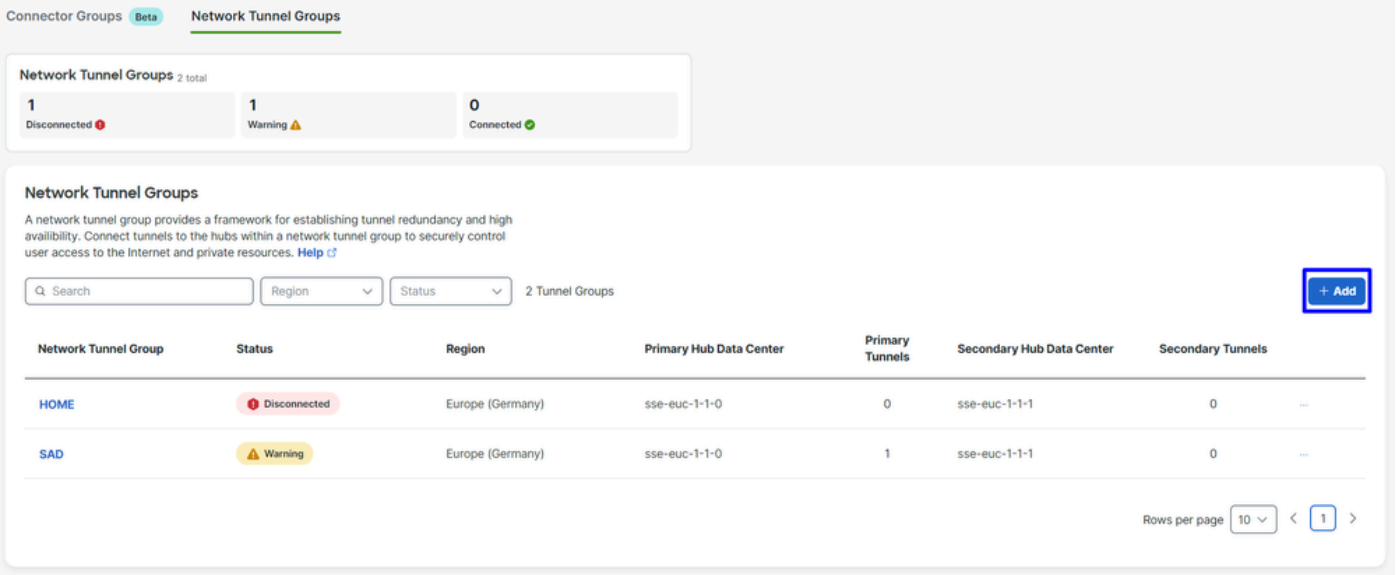
Acesso seguro - Página principal

- Clique em Connect > Network Connections.



Acesso seguro - Conexões de rede

- Em Network Tunnel Groups clique em + Add.



Acesso seguro - Grupos de túnel de rede

- Configure Tunnel Group Name, Region e Device Type.
- Clique **Next** em.

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)

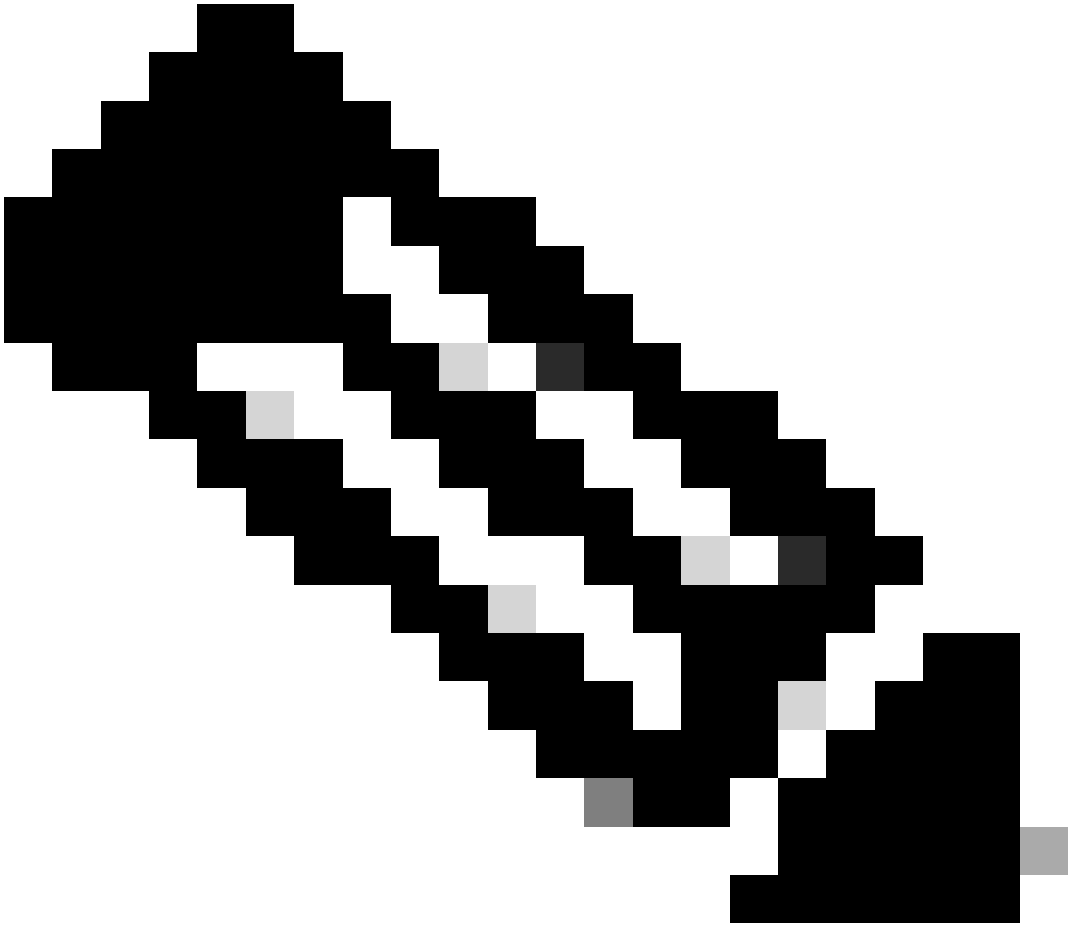
Device Type

Other

Cancel

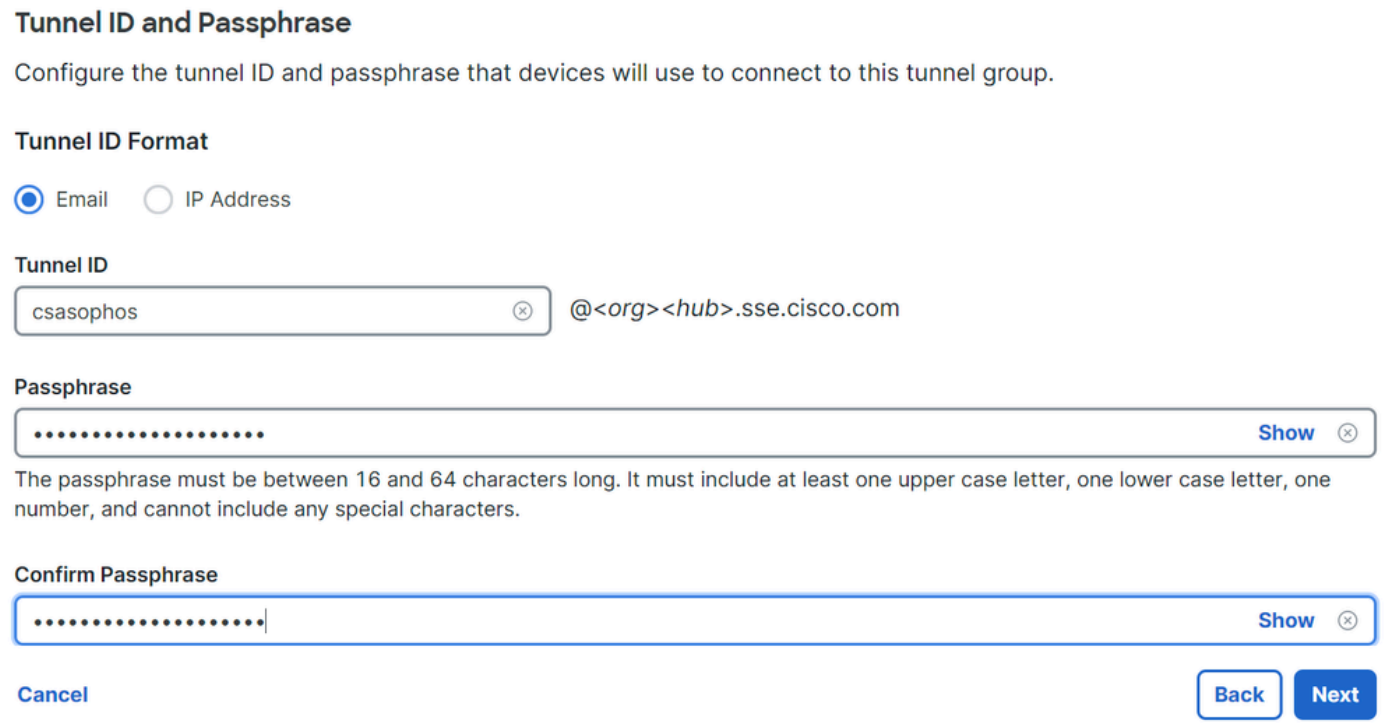
Next

Acesso seguro - Grupos de túneis - Configurações gerais



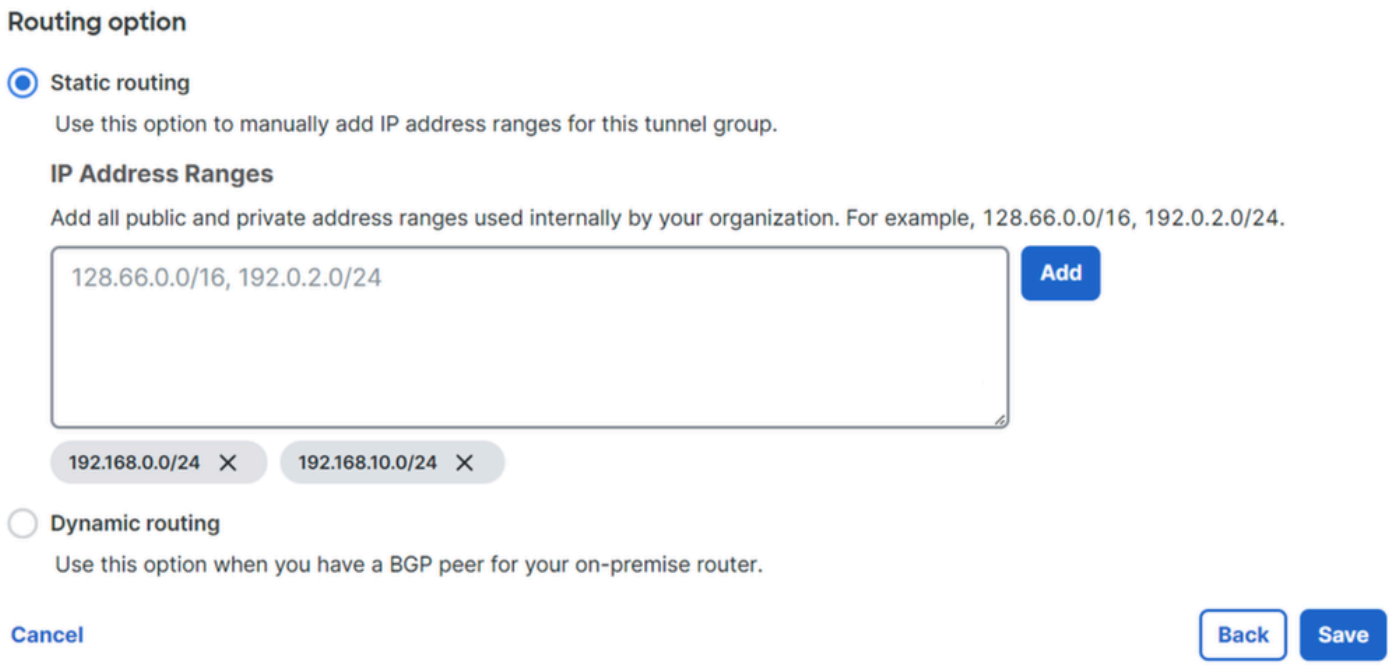
Observação: escolha a região mais próxima ao local do firewall.

- Configure o Tunnel ID Format e Passphrase.
- Clique em Next.



Acesso seguro - Grupos de túneis - ID e senha do túnel

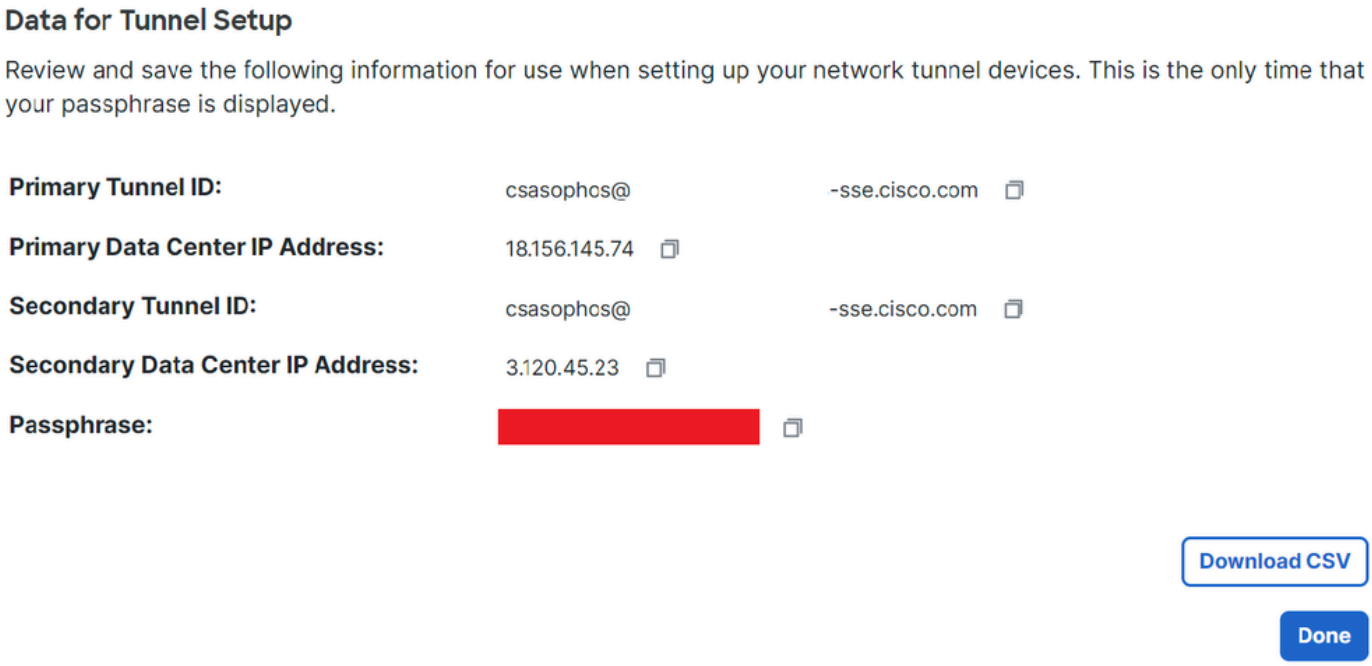
- Configure os intervalos de endereços IP ou hosts que você configurou na rede e deseja passar o tráfego pelo Secure Access.
- Clique em **Save**.



Acesso seguro - Grupos de túneis - Opções de roteamento

Depois de clicar nas informações sobre **Save** o túnel que são exibidas, salve essas informações para a próxima etapa, **Configure the tunnel on Sophos**.

Dados do túnel



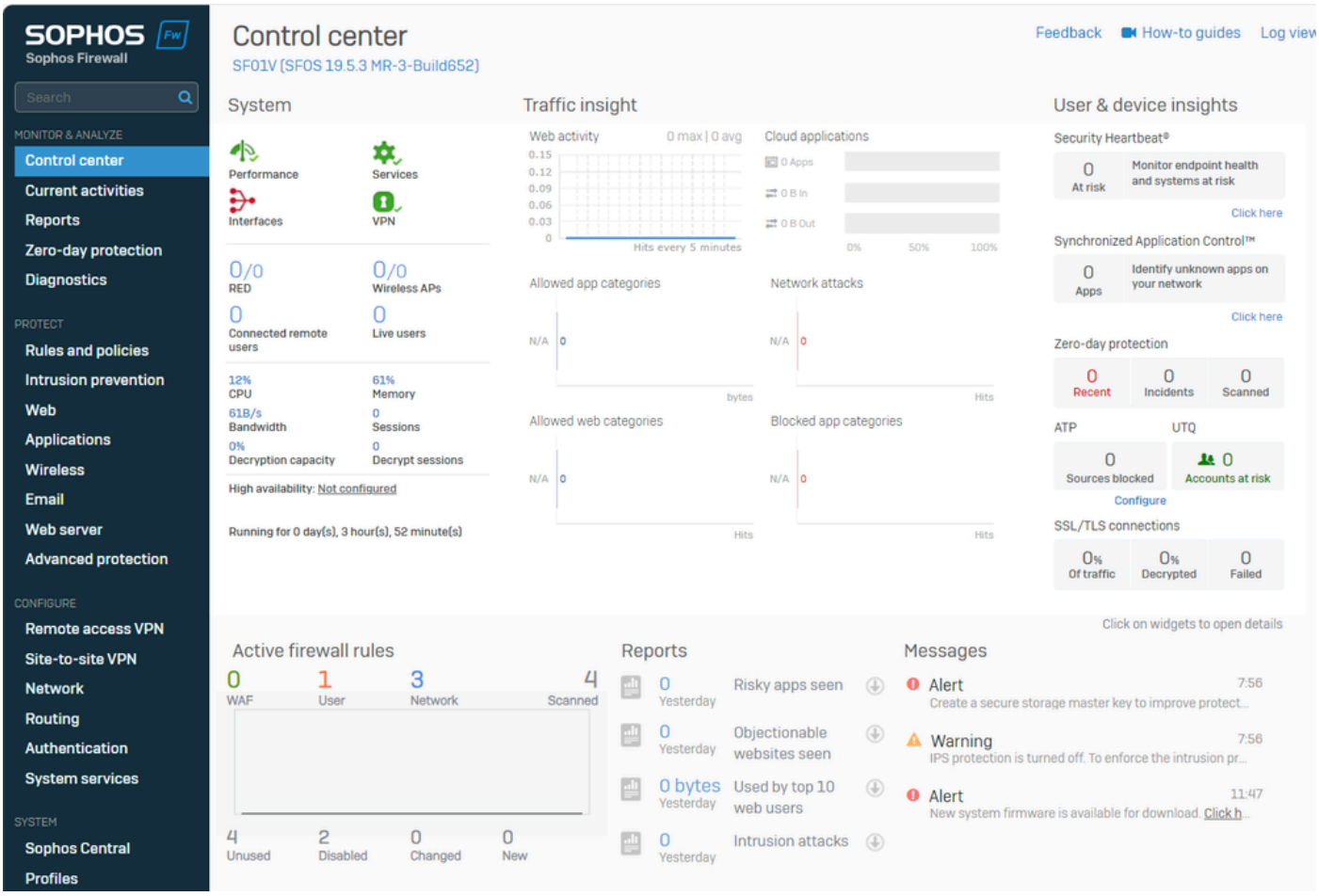
Secure Access - Tunnel Groups - Resume of configuration (Acesso seguro - Grupos de túneis - Retomar a configuração)

Configurar o túnel no Sophos

Configurar perfil IPsec

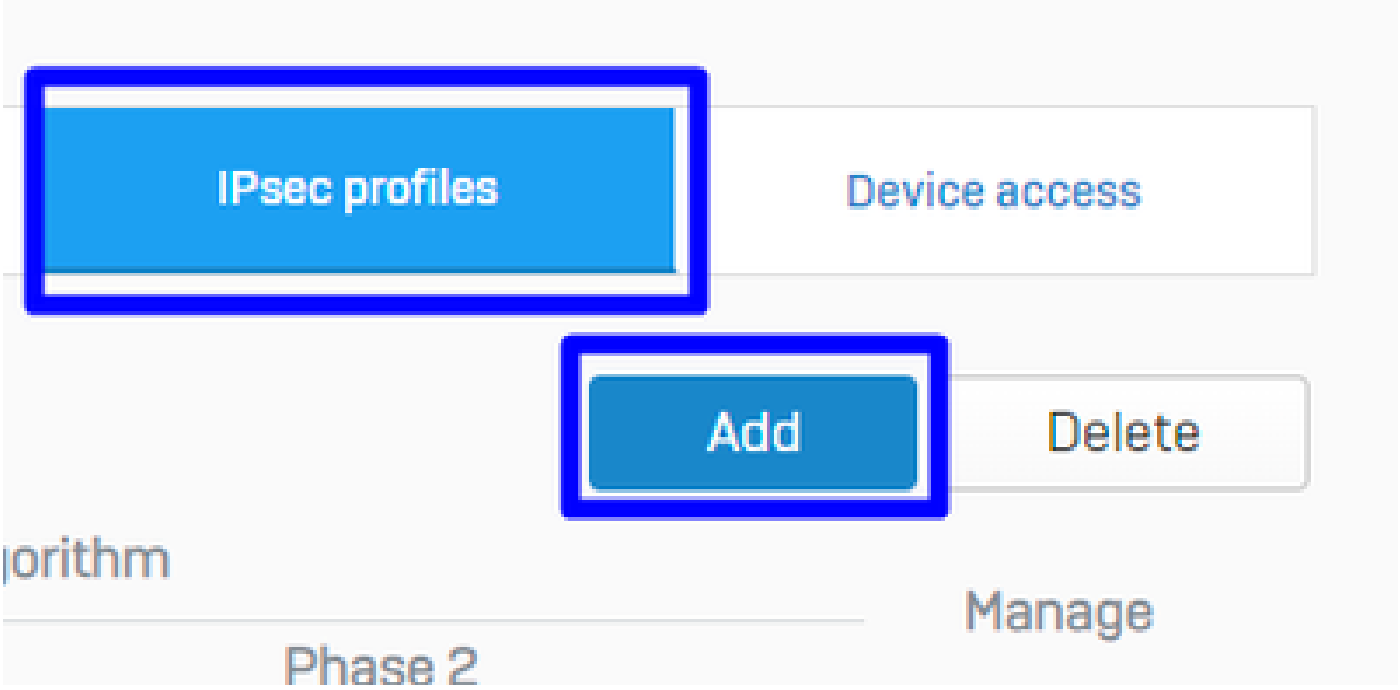
Para configurar o perfil IPsec, navegue para o firewall do Sophos XG.

Você obtém algo semelhante a isto:



Painel de administração do Sophos

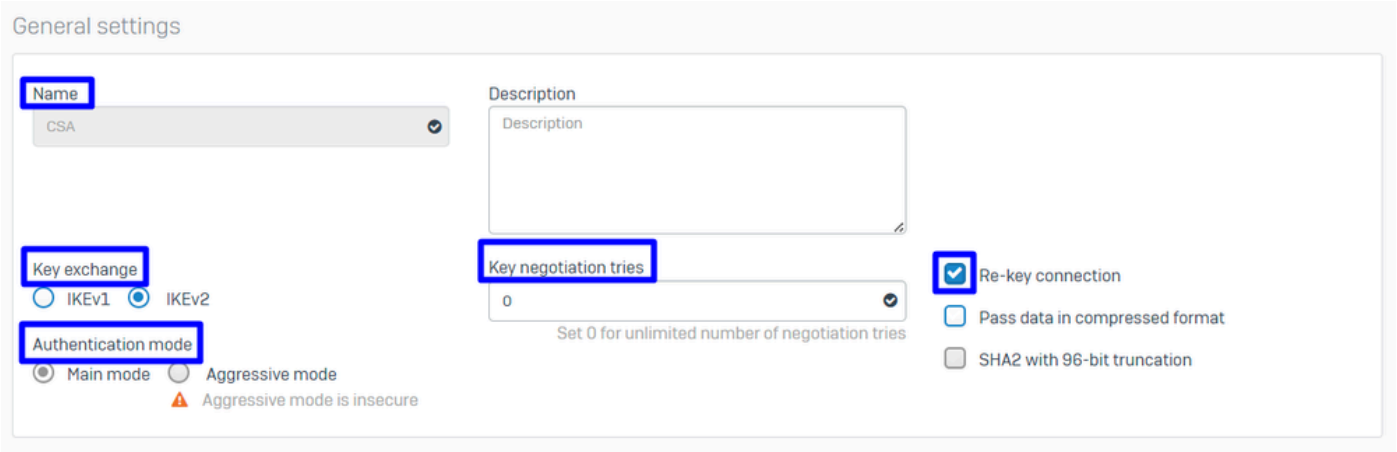
- Navegue até Profiles
- Clique em **IPsec Profiles** e depois clique emAdd



Sophos - Perfis IPsec

Em **General Settings** configurar:

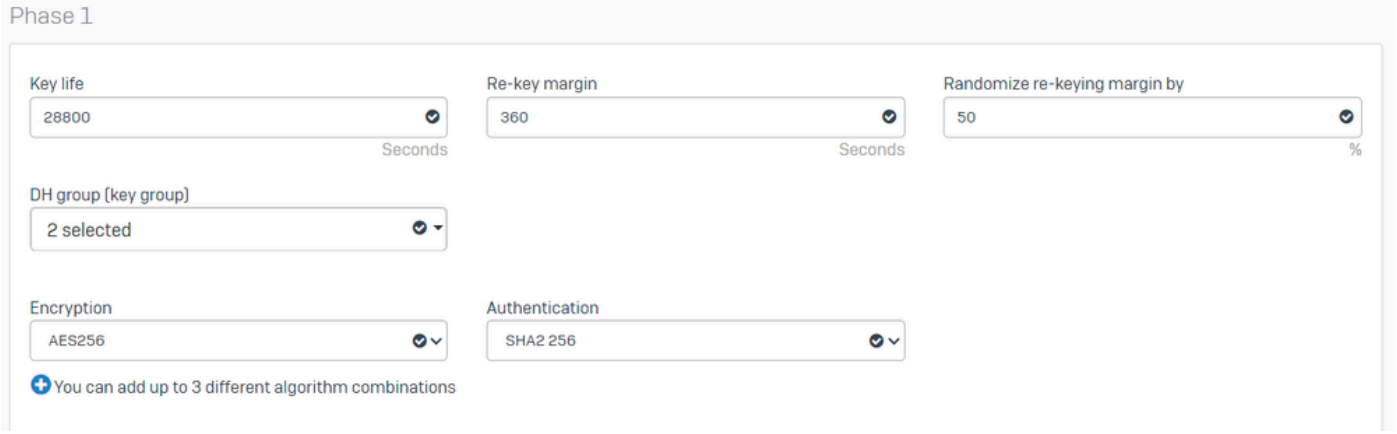
- **Name**: um nome de referência para a Política de acesso seguro da Cisco
- **Key Exchange**: IKEv2
- **Authentication Mode**: Modo principal
- **Key Negotiation Tries**:0
- **Re-Key connection**: Marque a opção



Sophos - Perfis IPsec - Configurações gerais

Em **Phase 1** configurar:

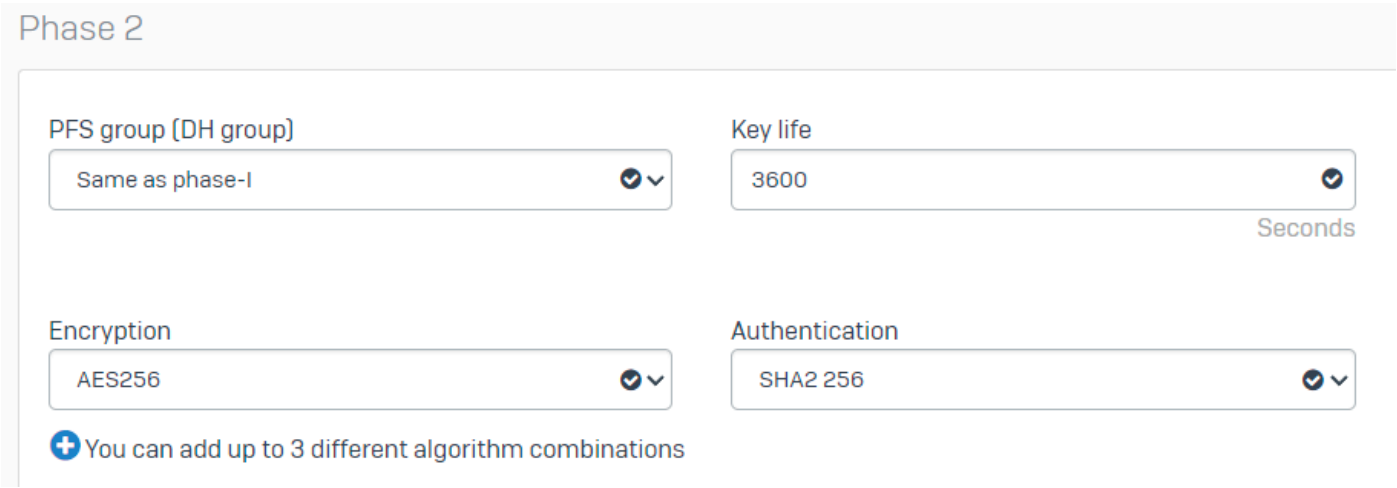
- **Key Life**:28800
- **DH group(key group)**: Selecione 19 e 20
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin:360 (Padrão)
- **Randomize re-keying margin by**:50 (Padrão)



Sophos - Perfis IPsec - Fase 1

Em **Phase 2** configurar:

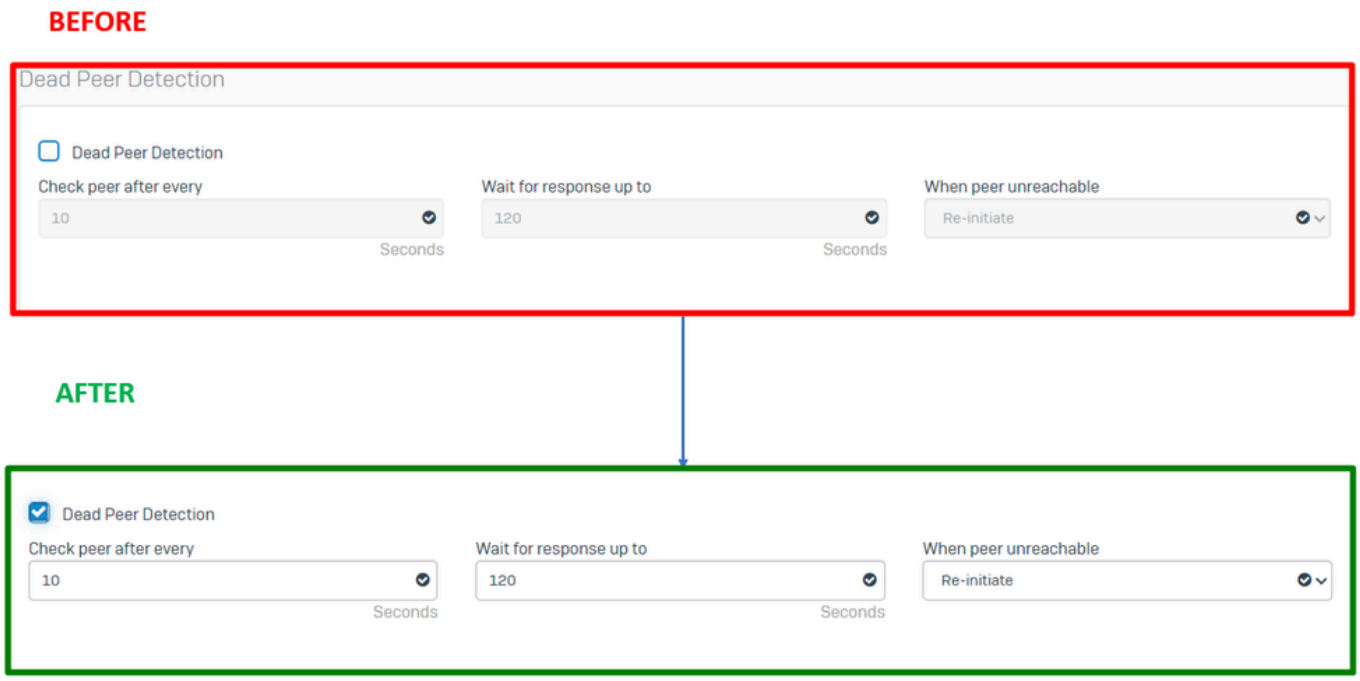
- PFS group (DH group): Igual à fase I
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256



Sophos - Perfis IPsec - Fase 2

Em **Dead Peer Detection** configurar:

- **Dead Peer Detection**: Marque a opção
- **Check peer after every**:10
- **Wait for response up to**:120 (Padrão)
- **When peer unreachable**: Reiniciar (Padrão)

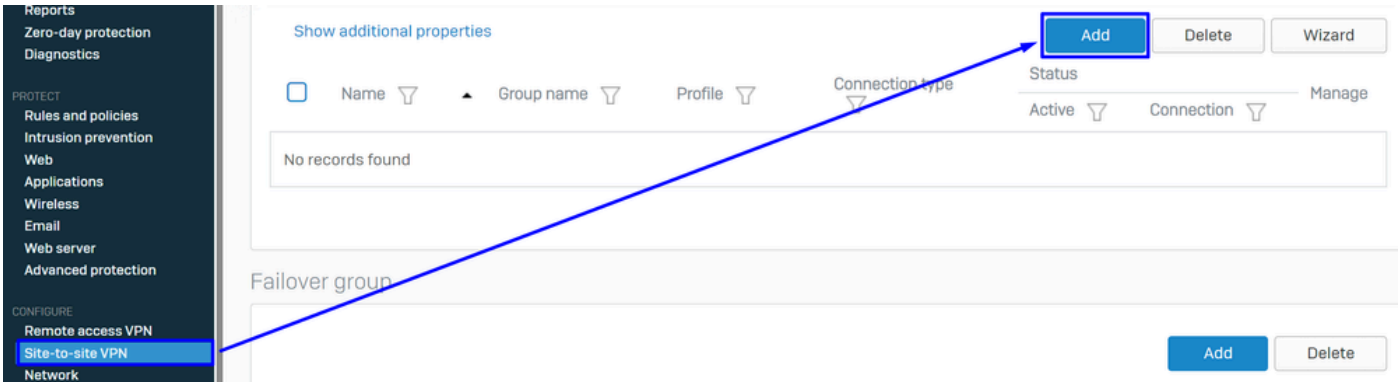


Sophos - Perfis IPsec - Detecção Dead Peer

Depois disso, clique em **Save** and proceed with the next step, Configure Site-to-site VPN.

Configurar VPN site a site

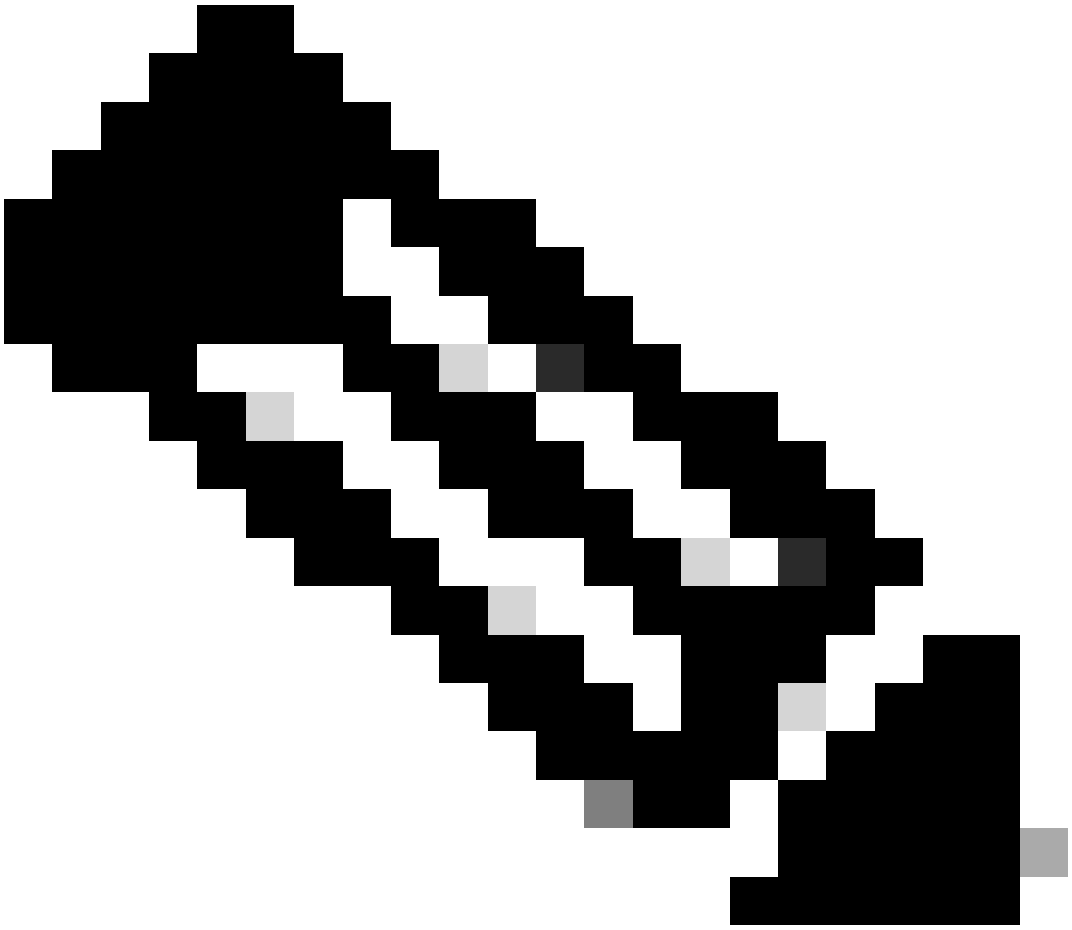
Para iniciar a configuração da VPN, clique em **Site-to-site VPN** e em **Add**.



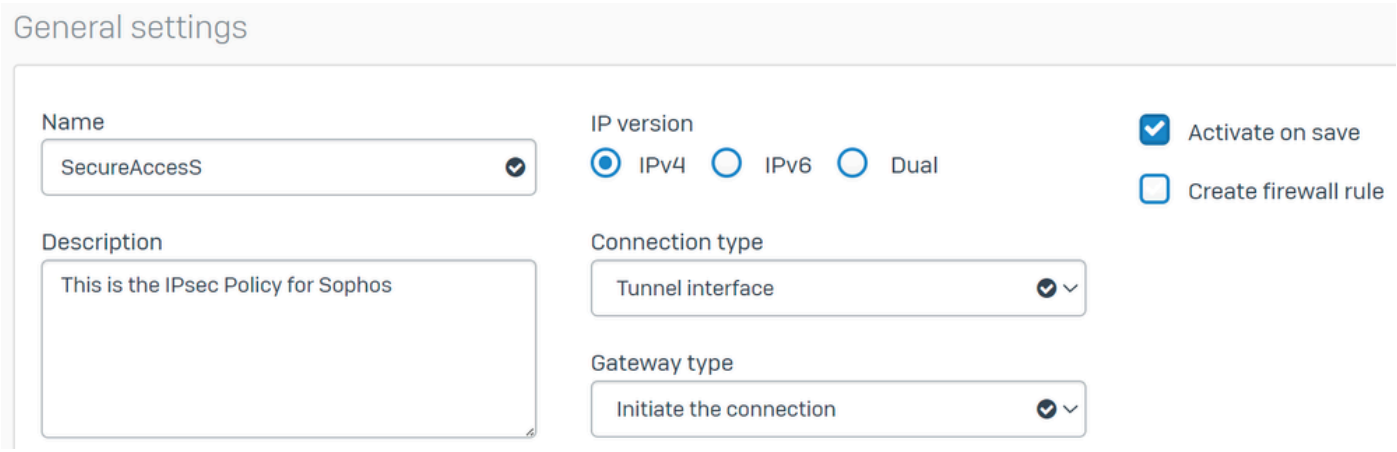
Sophos - VPN site a site

Em **General Settings** configurar:

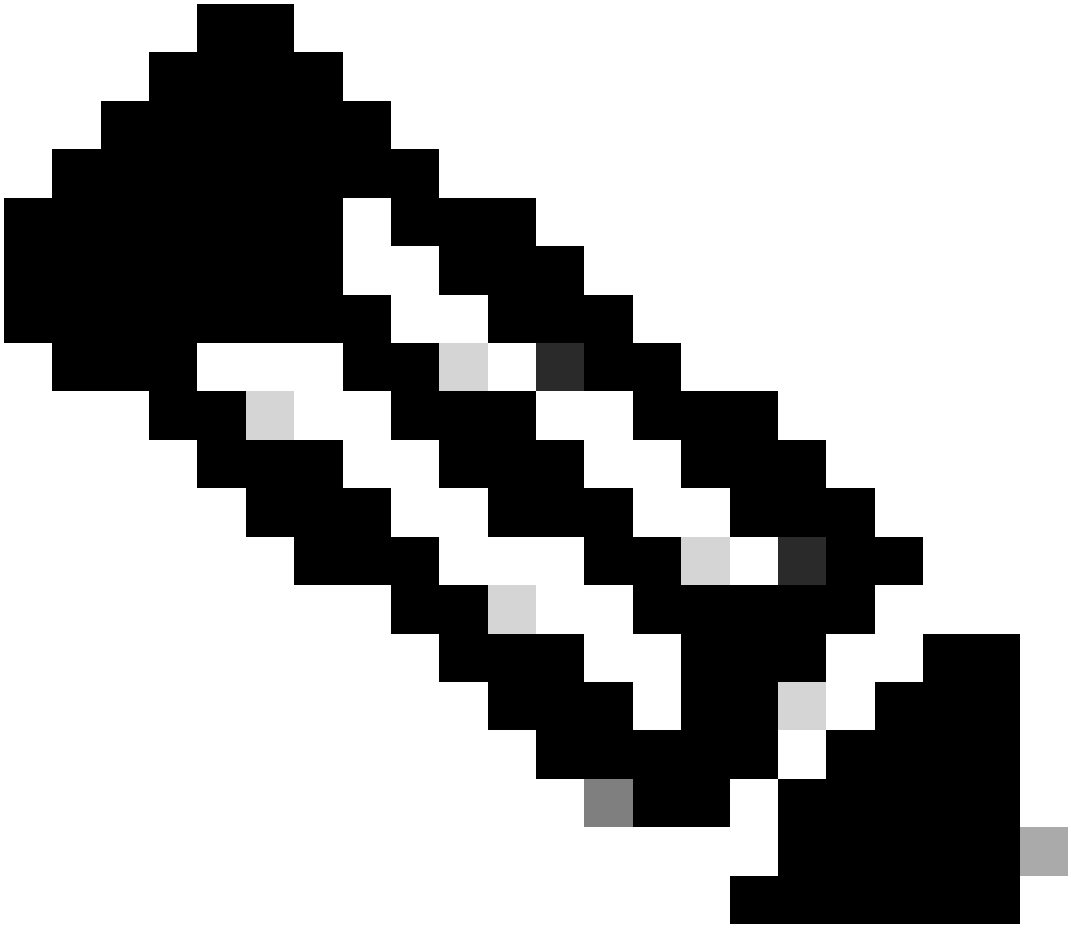
- **Name**: Um nome de referência para a Política IPsec do Cisco Secure Access
- IP version:IPv4
- Connection type: interface de túnel
- Gateway type: Inicie a conexão
- Active on save: Marque a opção



Observação: a opção **Active on save** habilita a VPN automaticamente depois que você termina de configurar a VPN site a site.



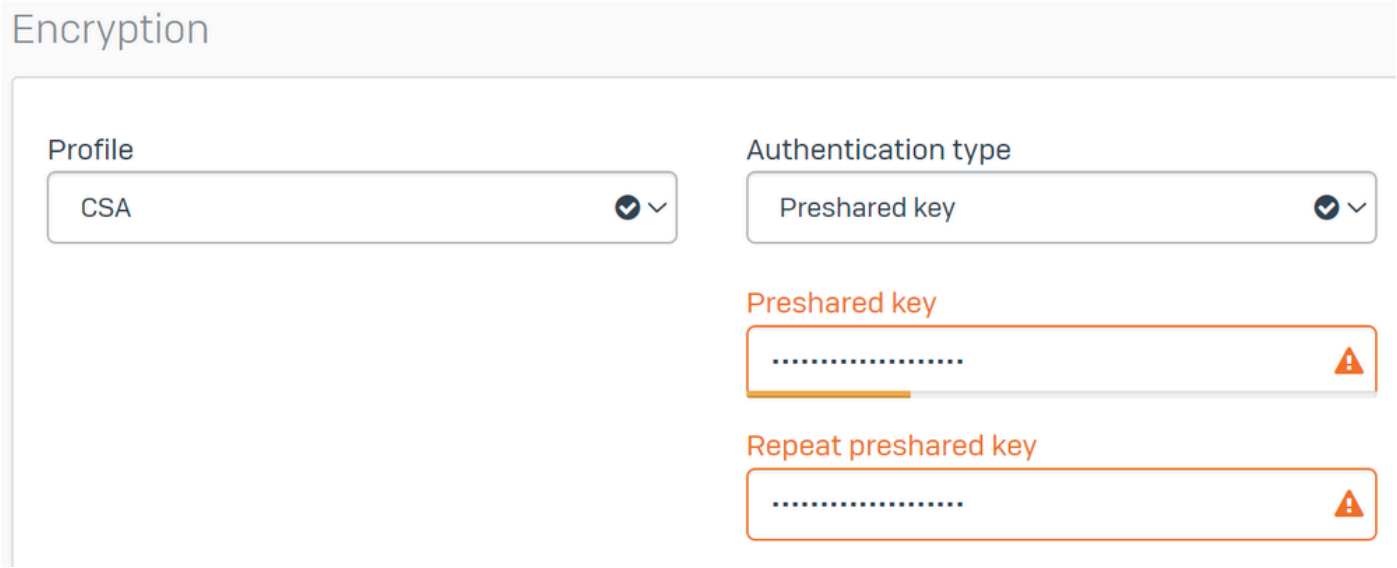
Sophos - VPN site a site - Configurações gerais



Observação: a opção Tunnel interface cria uma interface de túnel virtual para o Sophos XG Firewall com o nome XFRM.

Em **Encryption** configurar:

- **Profile**: o perfil que você cria na etapa, **Configure IPsec Profile**
- **Authentication type**: Chave pré-compartilhada
- **Preshared key**: A chave configurada na etapa, Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**

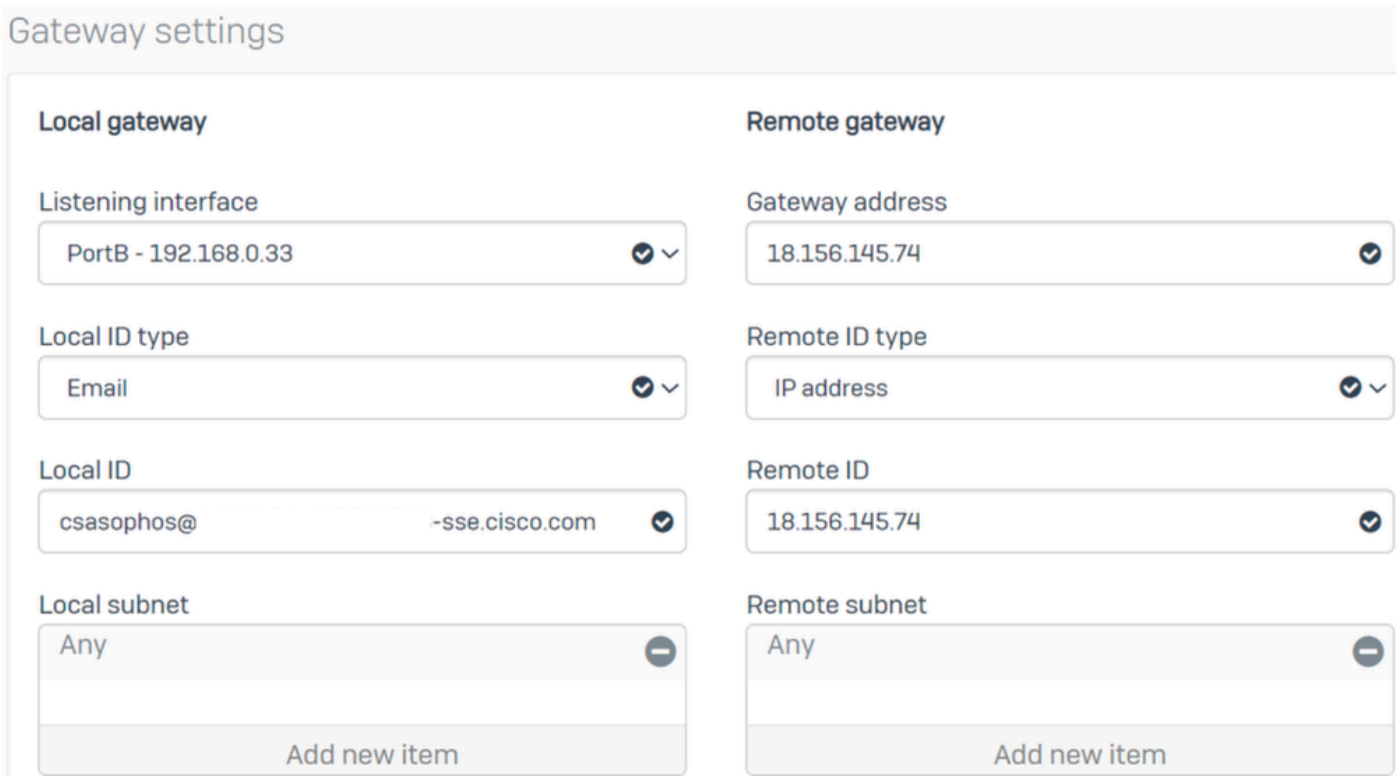


Sophos - VPN site a site - Criptografia

Nas opções **Gateway Settings** configure Local Gateway e Remote Gateway, use esta tabela como referência.

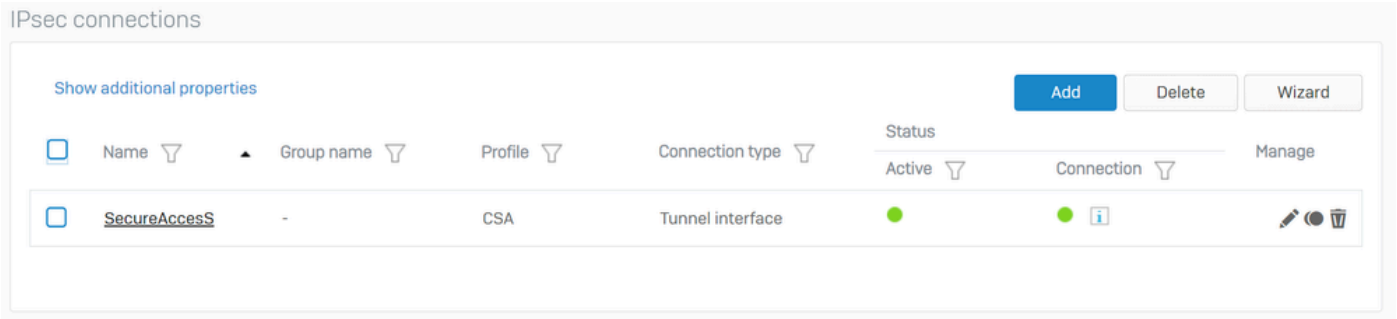
Gateway local	Gateway remoto
Interface de escuta Sua Interface Wan-Internet	Endereço do gateway O IP público gerado sob a etapa, **Tunnel Data**
Tipo de ID local E-mail	Tipo de ID remota Endereço IP

ID local O e-mail gerado sob a etapa, **Tunnel Data**	ID remota O IP público gerado sob a etapa, **Tunnel Data**
Sub-rede local qualquer um	Sub-rede Remota qualquer um

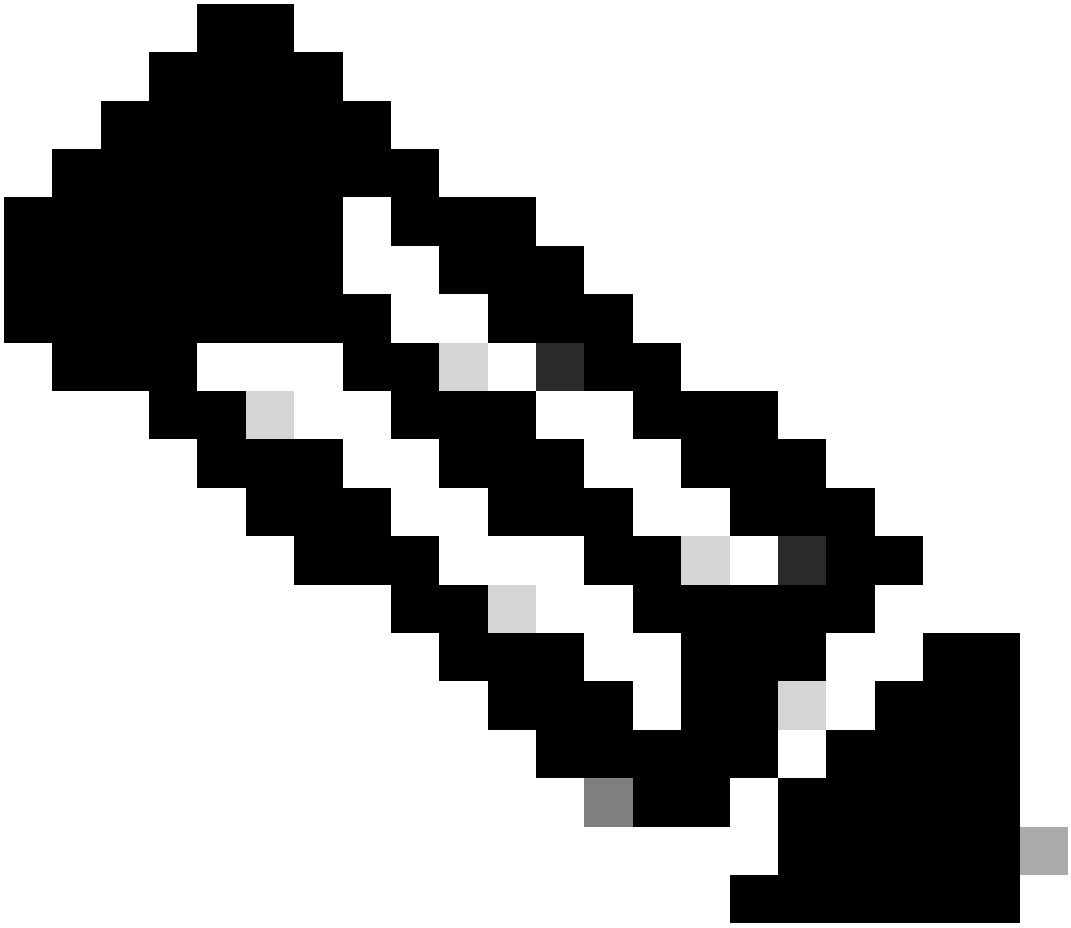


Sophos - VPN site a site - Configurações de gateway

Depois disso, clique em **Save**, e você poderá ver que o túnel foi criado.

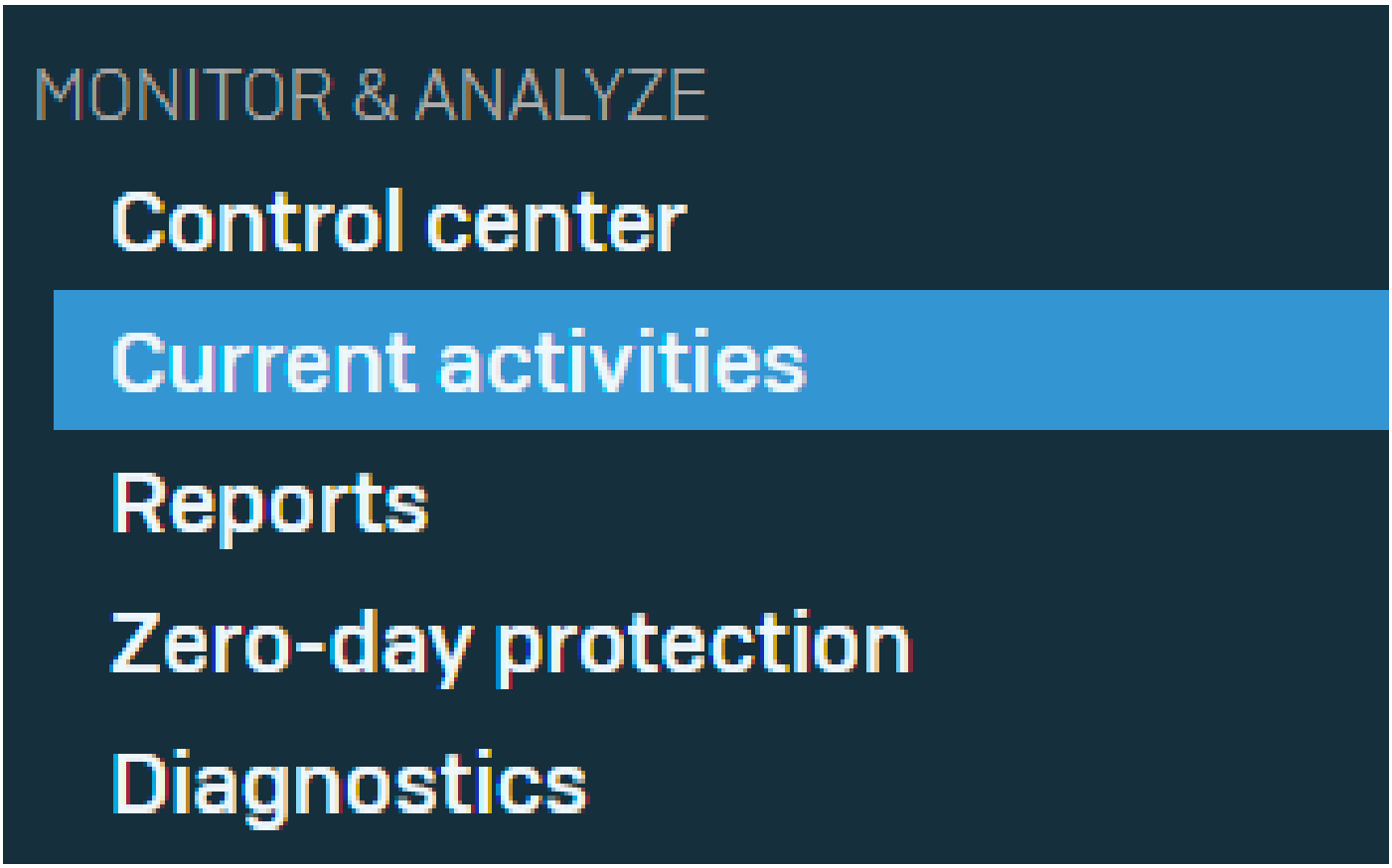


Sophos - VPN site a site - Conexões IPsec

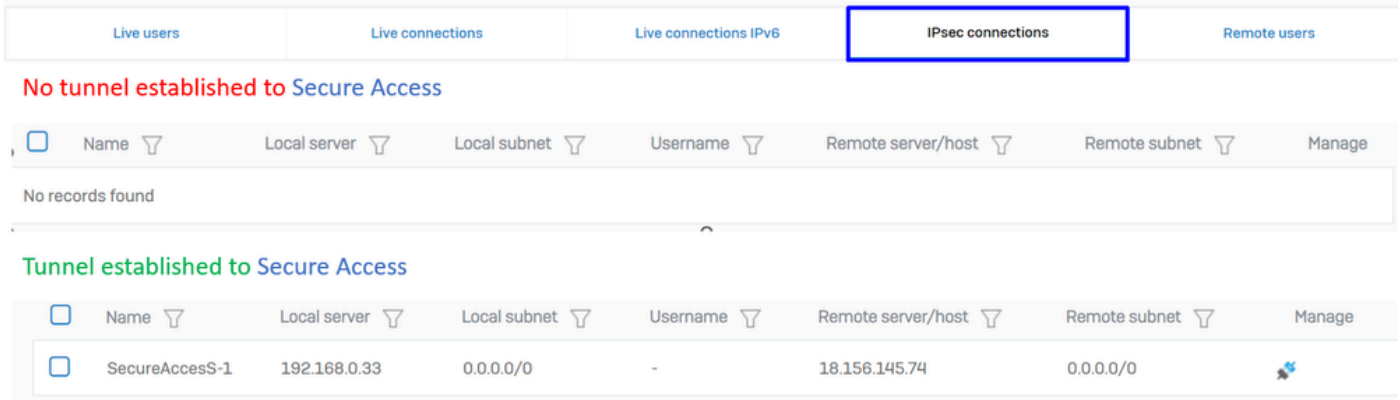


Observação: para verificar se o túnel está habilitado corretamente na última imagem, você pode verificar o **Connection** status; se estiver verde, o túnel está conectado; se não estiver verde, o túnel não está conectado.

Para verificar se um túnel está estabelecido, navegue até **Current Activities > IPsec Connections**.



Sophos - Monitorar e analisar - IPsec



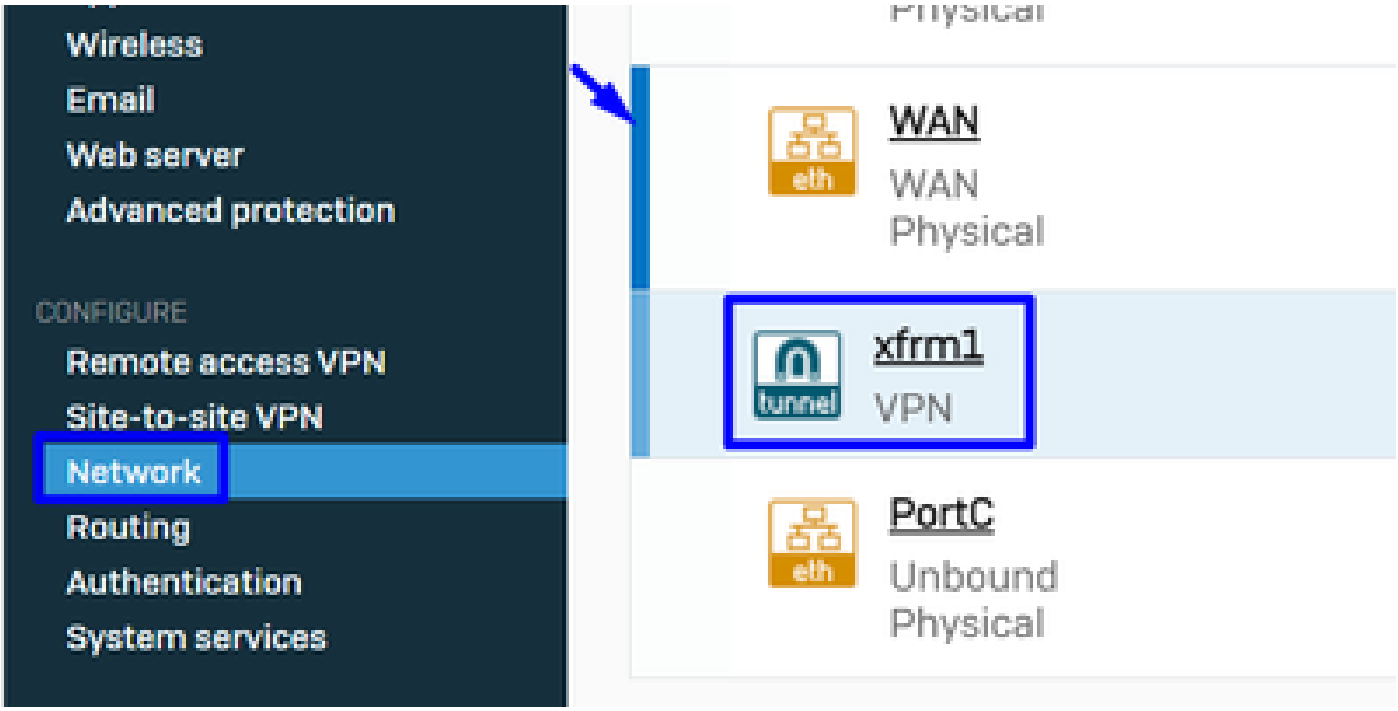
Sophos - Monitorar e analisar - IPsec antes e depois

Depois disso, podemos continuar com a etapa, **Configure Tunnel Interface Gateway**.

Configurar a interface do túnel

Navegue **Network** e verifique suaWAN interface configurada na VPN para editar a interface do túnel virtual com o nome xfrm.

- Clique na **xfrm** interface.



Sophos - Rede - Interface de túnel

- Configure a interface com um IP não-roteável em sua rede. Por exemplo, você pode usar 169.254.x.x/30, que é um IP em um espaço não-roteável normalmente, em nosso exemplo, usamos 169.254.0.1/30

Sophos - Rede - Interface de túnel - Configuração

Configurar os gateways

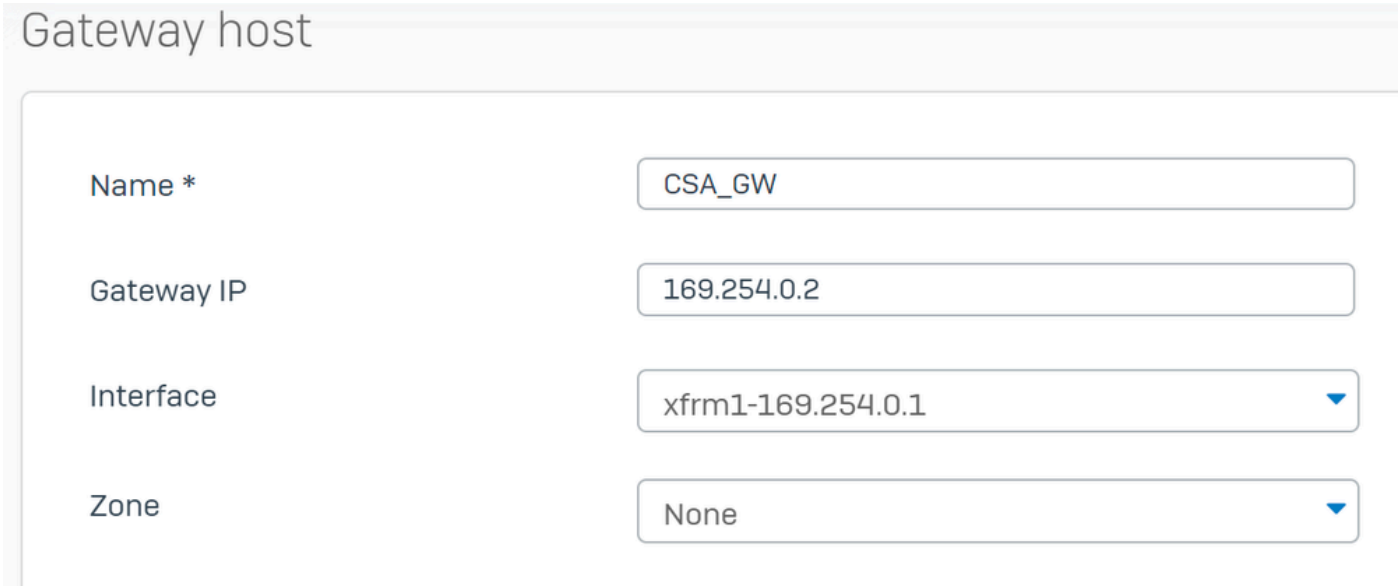
Para configurar o gateway para a interface virtual (xfrm)

- Navegue até Routing > Gateways
- Clique em Add

Sophos - Roteamento - Gateways

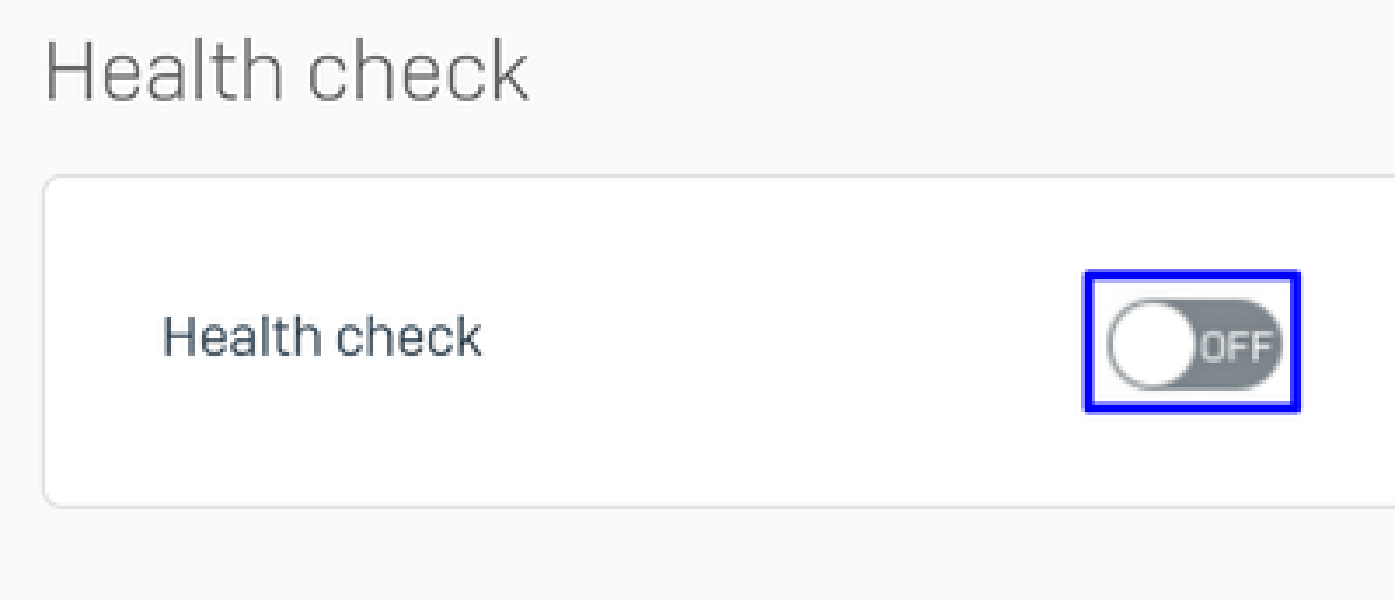
Em **Gateway host** configurar:

- **Name**: um nome que faz referência à interface virtual criada para a VPN
- **Gateway IP**: No nosso caso 169.254.0.2, esse é o IP na rede 169.254.0.1/30 que já atribuímos na etapa, Configure Tunnel Interface
- Interface: Interface virtual VPN
- **Zone**: Nenhum (Padrão)



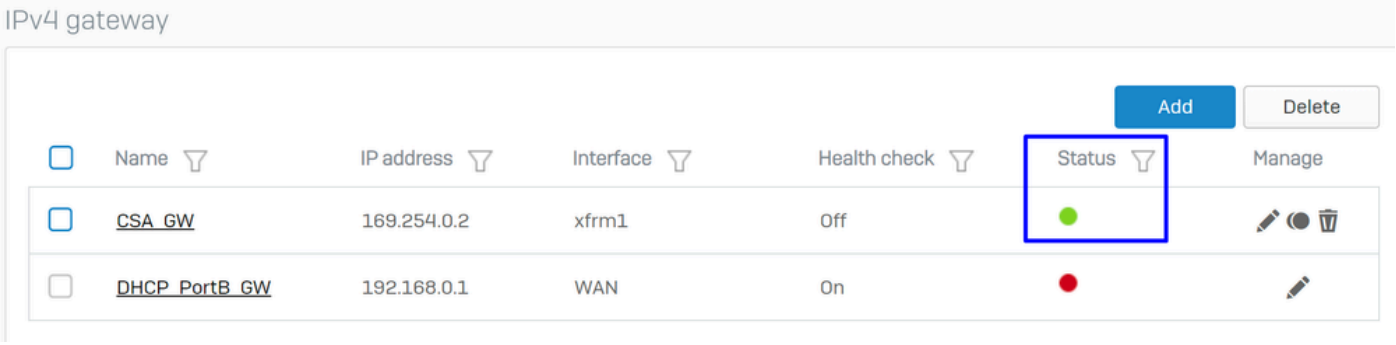
Sophos - Roteamento - Gateways - Host do gateway

- Em **Health check** desativar a verificação
- Clique em **Save**



Sophos - Roteamento - Gateways - Verificação de integridade

Você pode observar o status do gateway depois de salvar a configuração:



Sophos - Roteamento - Gateways - Status

Configurar a rota SD-WAN

Para finalizar o processo de configuração, você precisa criar a rota que permite encaminhar o tráfego para o Secure Access.

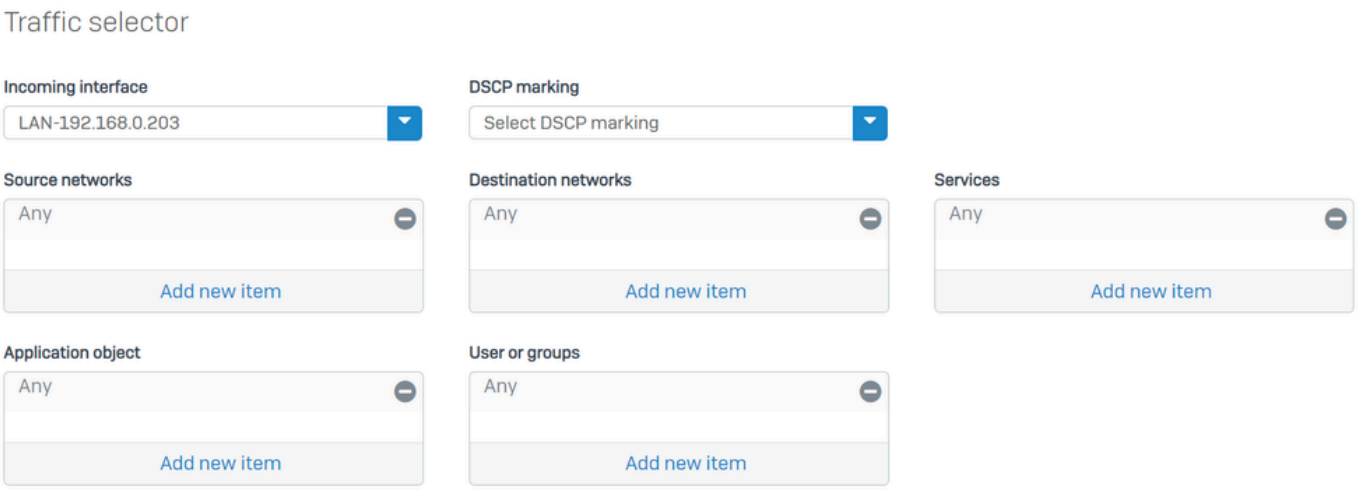
Navegue até **Routing > SD-WAN routes.**

- Clique em **Add**

Sophos - Rotas SD-Wan

Em **Traffic Selector** configurar:

- Incoming interface: selecione a interface de onde deseja enviar o tráfego ou os usuários que acessam de RA-VPN, ZTNA ou Clientless-ZTNA
- DSCP marking: Nada para este exemplo
- **Source networks**: selecione o endereço que você deseja rotear pelo túnel
- **Destination networks**: Qualquer um ou você pode especificar um destino
- **Services**: Qualquer um ou você pode especificar os serviços
- **Application object**: um aplicativo se você tiver o objeto configurado
- User or groups: se desejar adicionar um grupo específico de usuários para rotear o tráfego para o acesso seguro

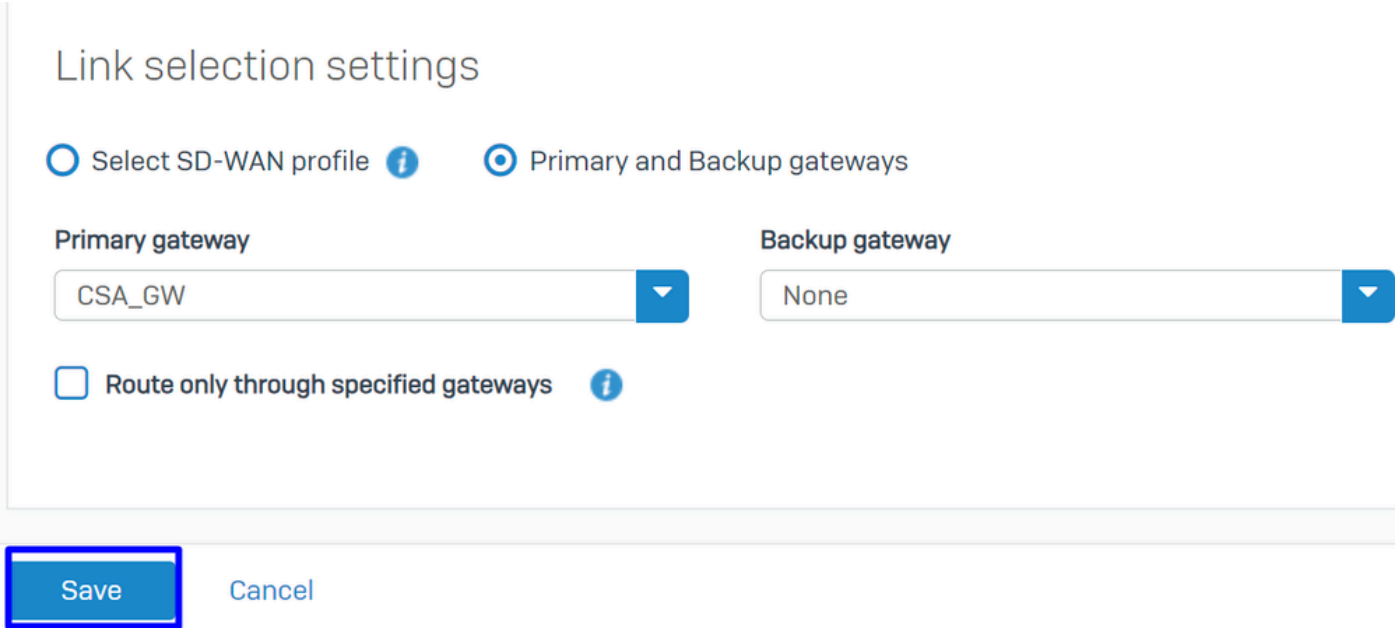


Sophos - Rotas SD-Wan - Seletor de tráfego

Em **Link selection settings** configurar o gateway:

- Primary and Backup gateways: Marque a opção

- **Primary gateway**: selecione o gateway configurado na etapa, Configure the Gateways
- Clique em **Save**



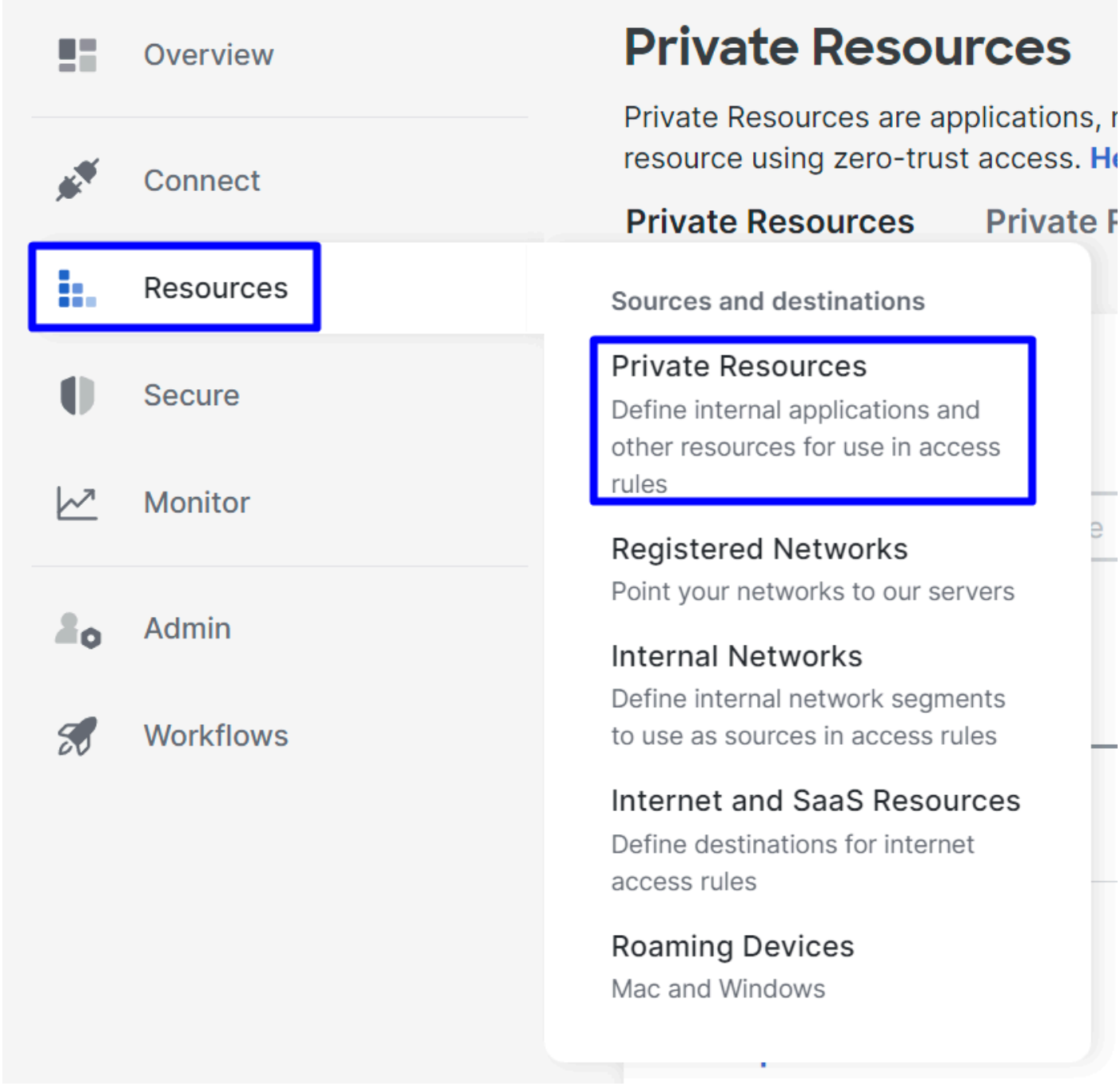
Sophos - Rotas SD-Wan - Seletor de tráfego - Gateways primários e de backup

Depois de finalizar a configuração no Sophos XG Firewall, você pode prosseguir com a etapa, **Configure Private App.**

Configurar Aplicativo Privado

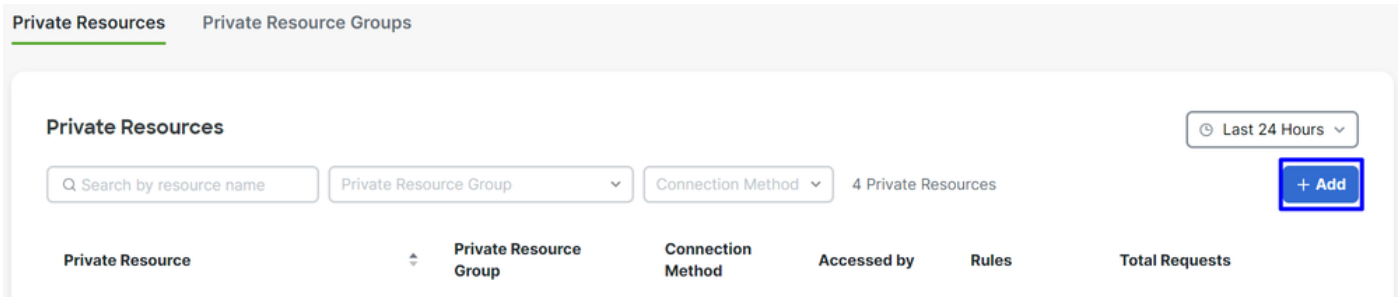
Para configurar o acesso ao aplicativo privado, faça login no Portal de administração.

- Navegue até **Resources > Private Resources**



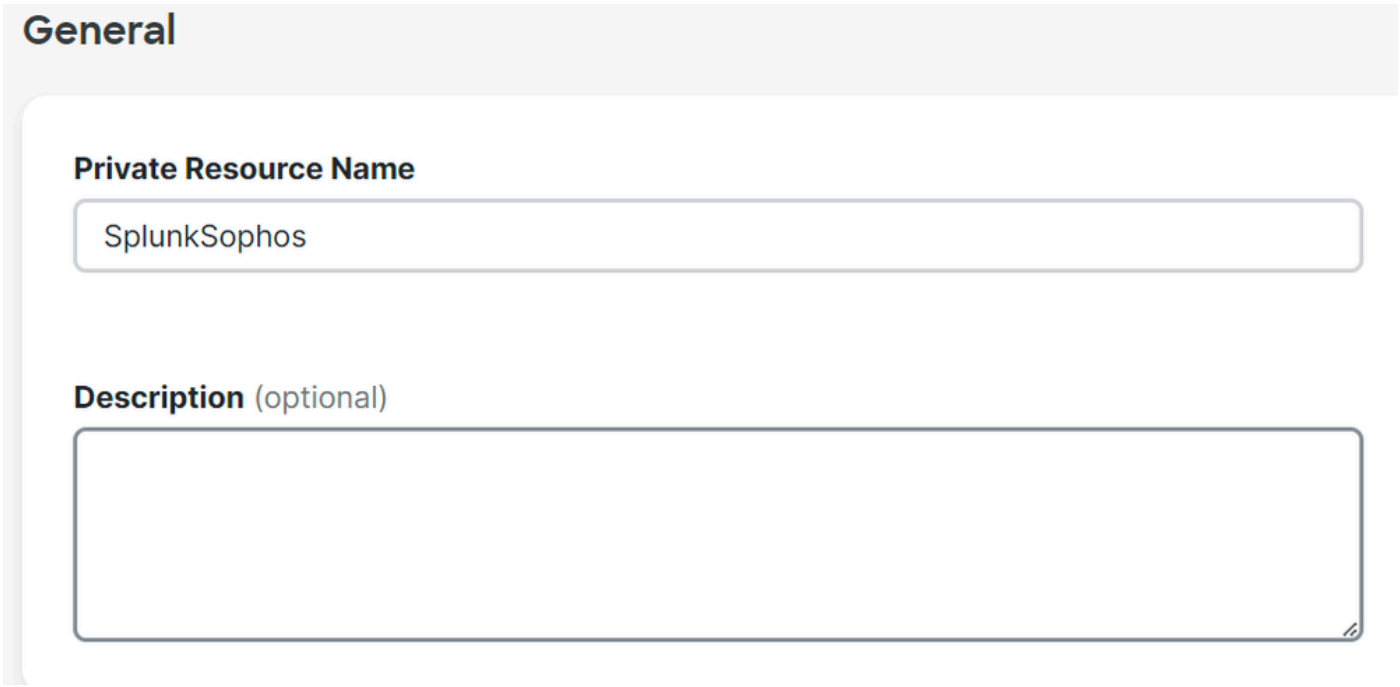
Acesso seguro - Recursos privados

- Clique em + Add



Acesso seguro - Recursos privados 2

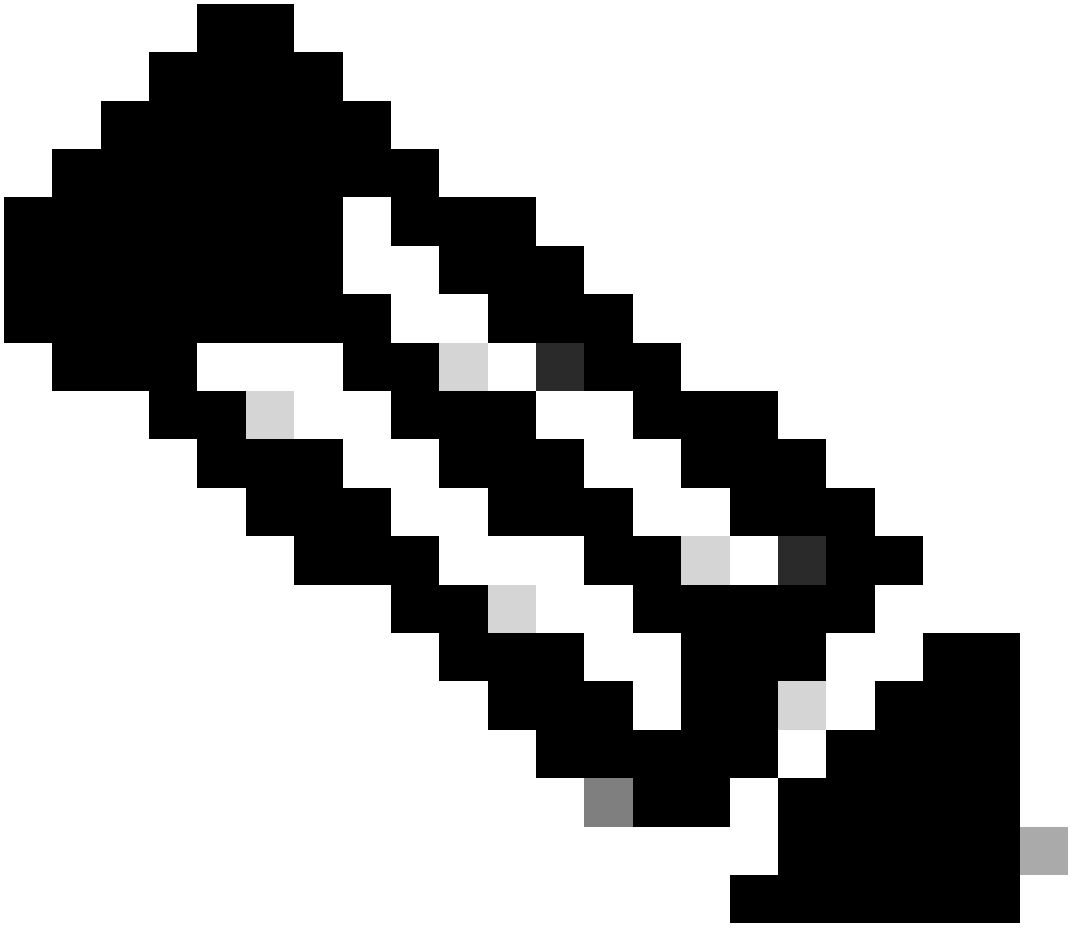
- Em **General** Configurar, **Private Resource Name**



Acesso seguro - Recursos privados - Geral

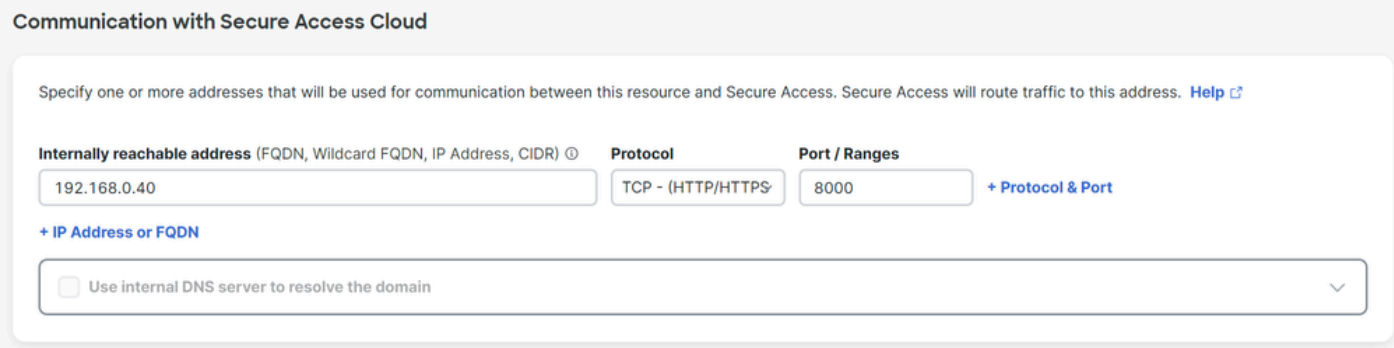
Em **Communication with Secure Access Cloud** configurar:

- I**nternally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: selecione o recurso que deseja acessar



Observação: lembre-se de que o endereço acessível internamente foi atribuído na etapa, **Configure the Tunnel on Secure Access**.

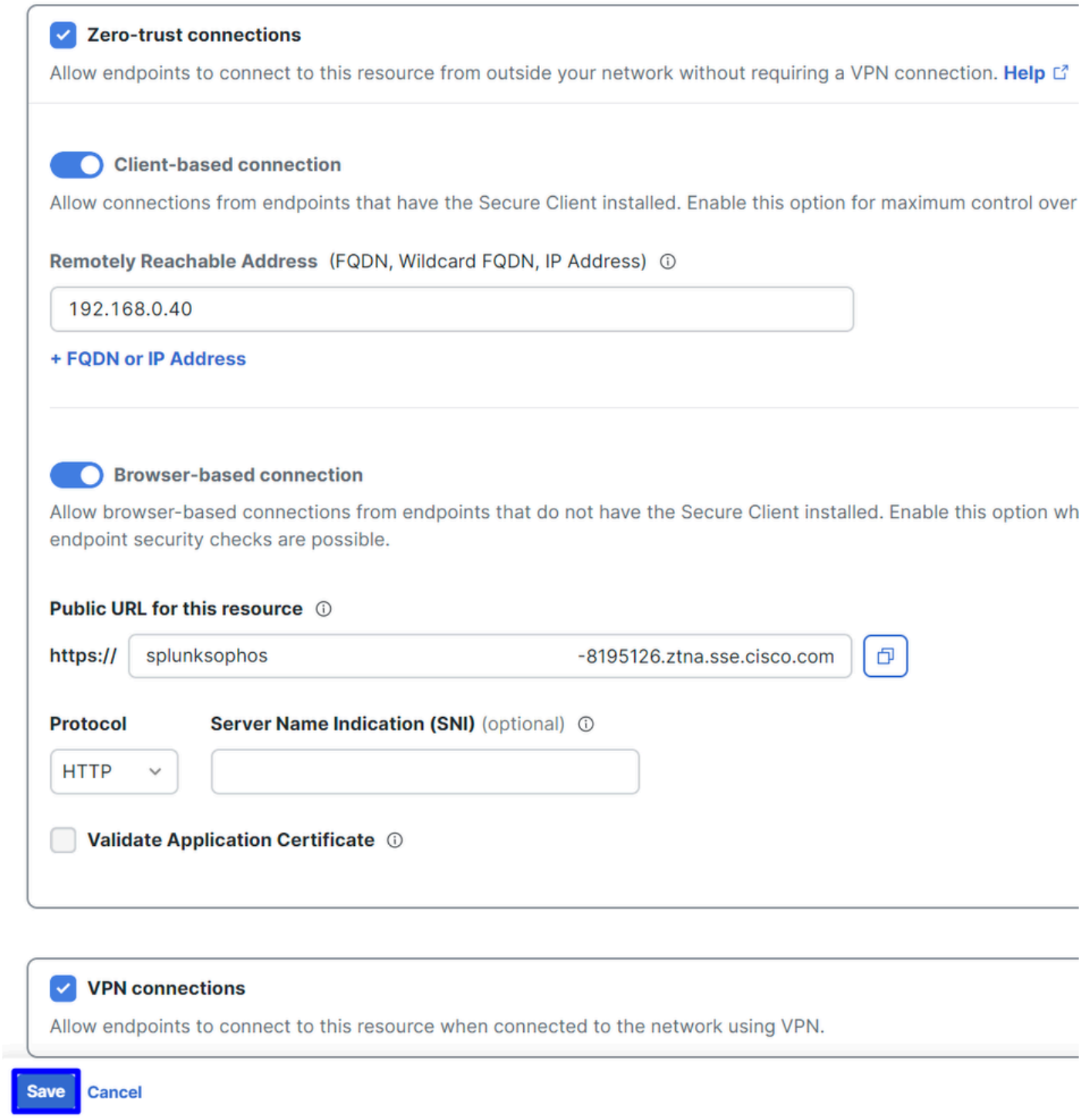
- **Protocol**: selecione o protocolo que você usa para acessar esse recurso
- Port / Ranges : selecione as portas que você precisa habilitar para acessar o aplicativo



Acesso seguro - Recursos privados - Comunicações com Secure Access Cloud

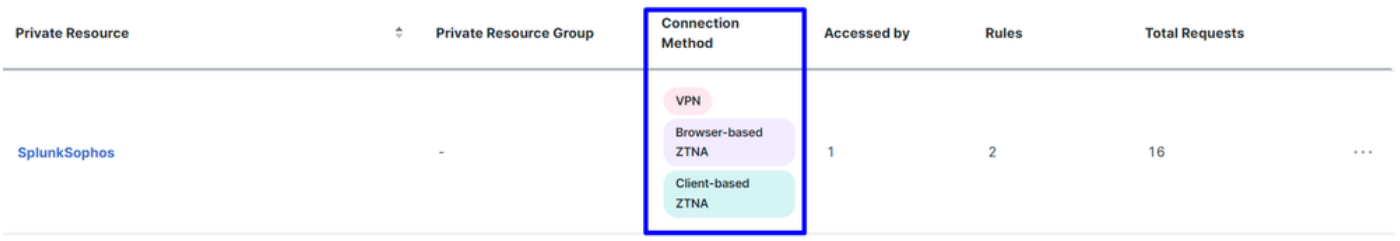
No, você configura todas as formas possíveis de acessar recursos privados por meio do Secure Access e escolhe os métodos que deseja usar para seu ambiente **Endpoint Connection Methods**:

- **Zero-trust connections**: Marque a caixa para habilitar o acesso ZTNA.
    - **Client-based connection**: Habilite o botão para permitir ZTNA de base de cliente
        - **Remotely Reachable Address**: Configure o IP do seu aplicativo privado
    - **Browser-based connection**: Habilite o botão para permitir ZTNA baseado em navegador
        - Public URL for this resource: Adicione um nome para usar em conjunto com o domínio ztna.sse.cisco.com
            - Protocol: escolha HTTP ou HTTPS como protocolo para acessar por meio do navegador
    - **VPN connections**: Marque a caixa para habilitar o acesso RA-VPN.
- Clique em **Save**



Acesso seguro - Recursos privados - Comunicações com Secure Access Cloud 2

Após a conclusão da configuração, este é o resultado:

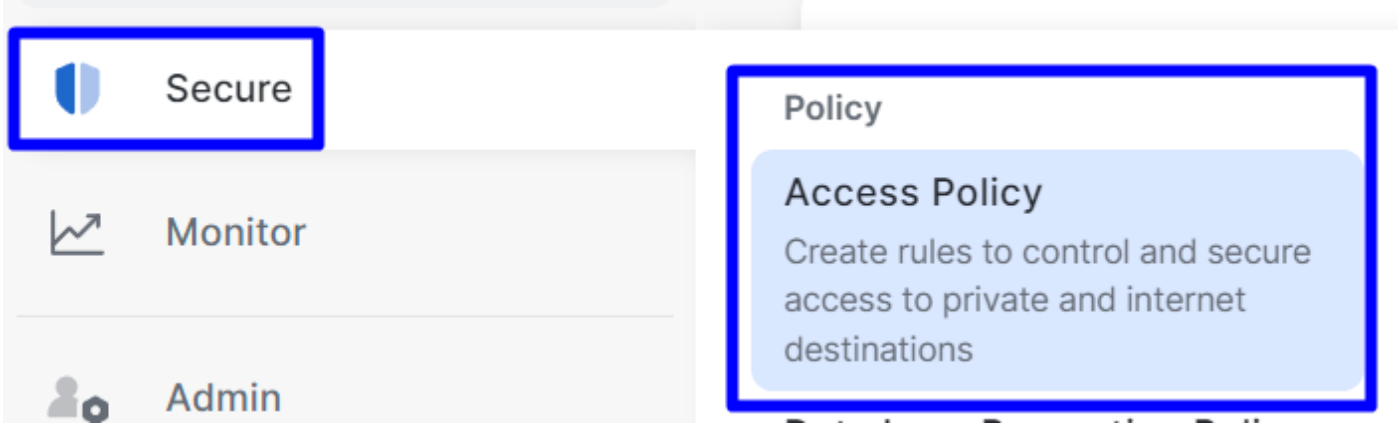


Acesso seguro - Recursos privados configurados

Agora você pode prosseguir com a etapa, **Configure the Access Policy**.

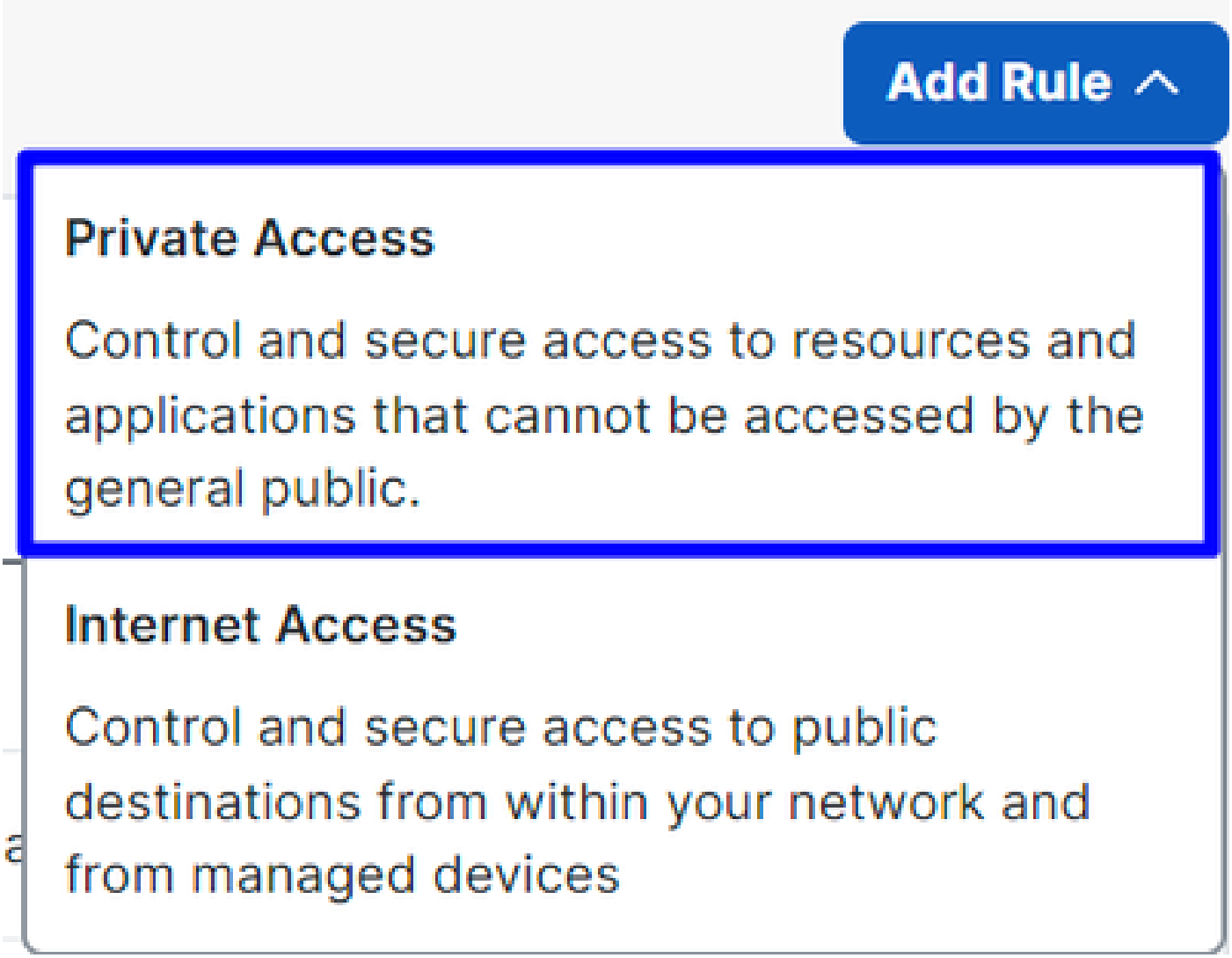
Configurar a política de acesso

Para configurar a política de acesso, navegue até Secure > Access Policy.



Acesso seguro - Política de acesso

- Clique em **Add Rule > Private Access**

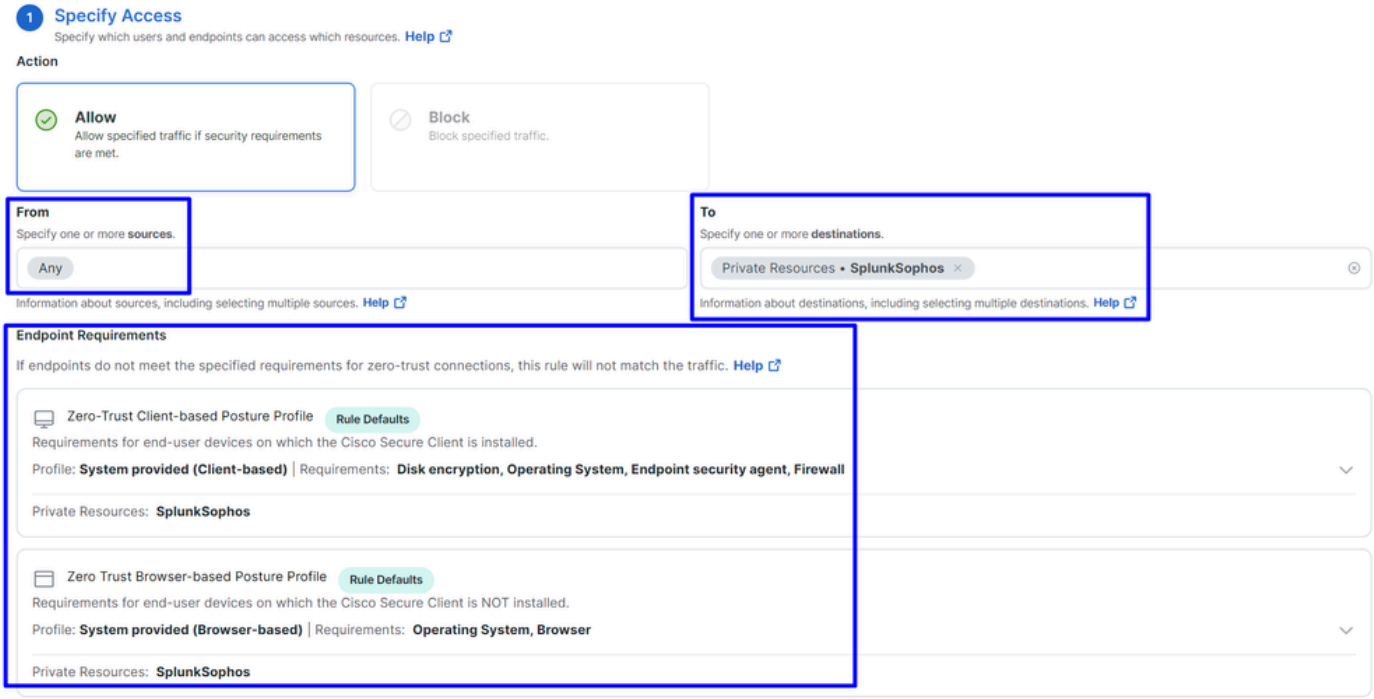


Acesso seguro - Política de acesso - Acesso privado

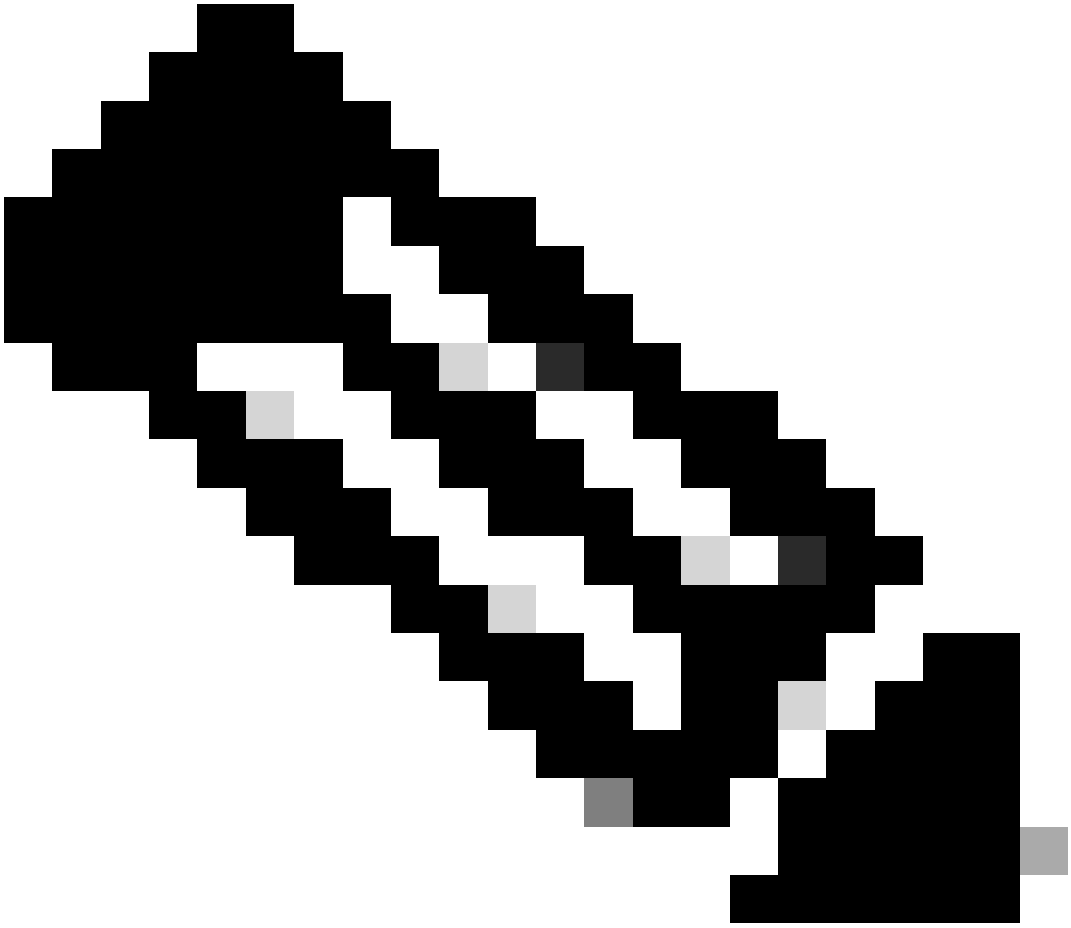
Configure as próximas opções para fornecer acesso por meio de vários métodos de autenticação:

- 1. Specify Access
    - Action:Permissão
        - **Rule name**: especifique um nome para sua regra de acesso
        - **From**: Os usuários aos quais você concede acesso
        - **To**: o aplicativo ao qual você deseja permitir acesso
        - Endpoint Requirements: (Padrão)

- Clique em **Next**

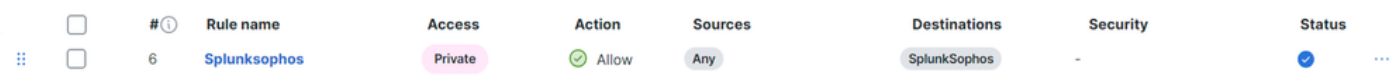


Acesso seguro - Política de acesso - Especificar acesso



Observação: para a etapa **2. Configure Security** conforme necessário, mas nesse caso, você não habilitou o **Intrusion Prevention (IPS)**, ou **Tenant Control Profile**.

- Clique em Save e você terá:



Acesso seguro - Política de acesso configurada

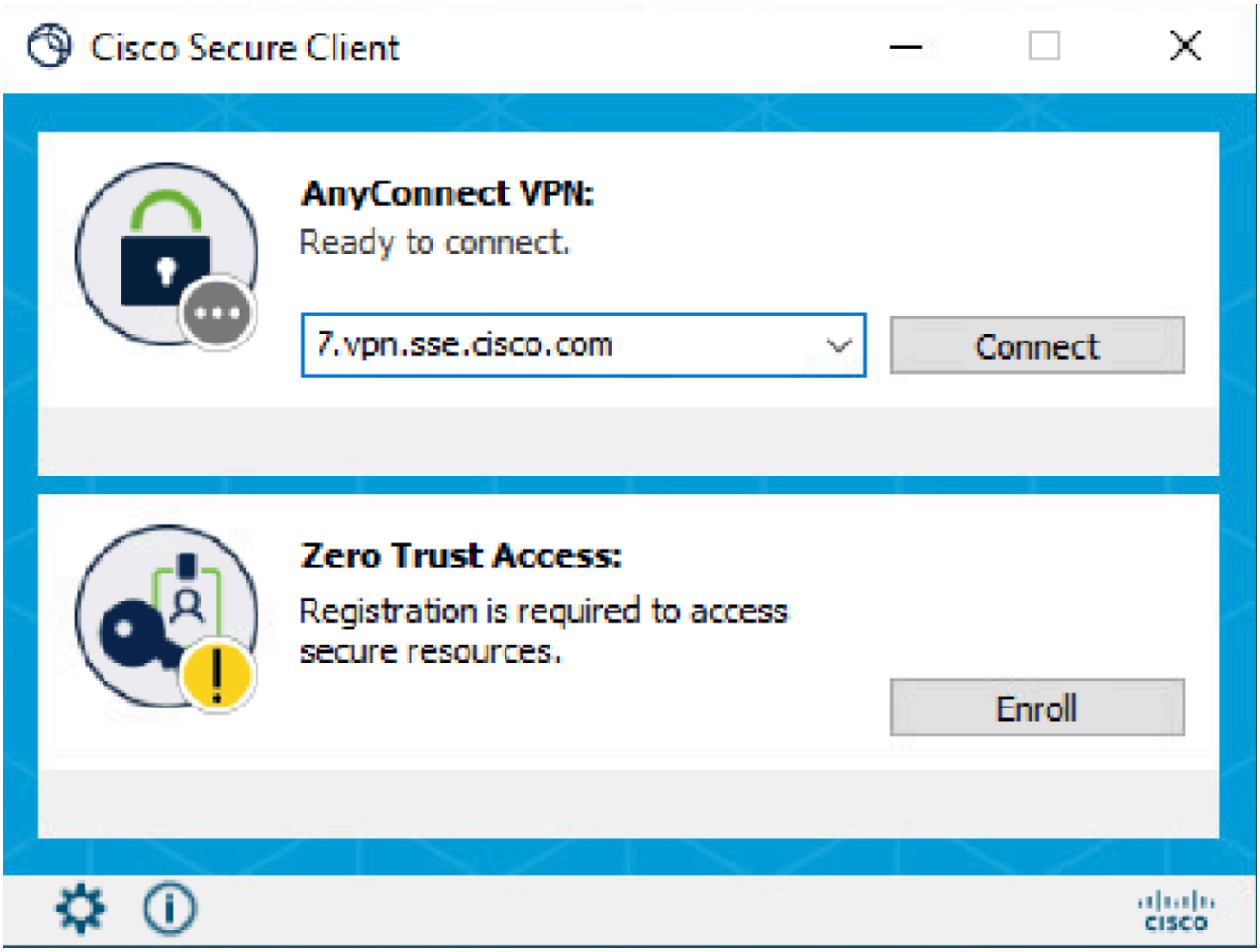
Depois disso, você poderá prosseguir com a etapa Verify.

Verificar

Para verificar o acesso, você deve ter instalado o agente do Cisco Secure Client que pode ser baixado em Download de Software - Cisco Secure Client.

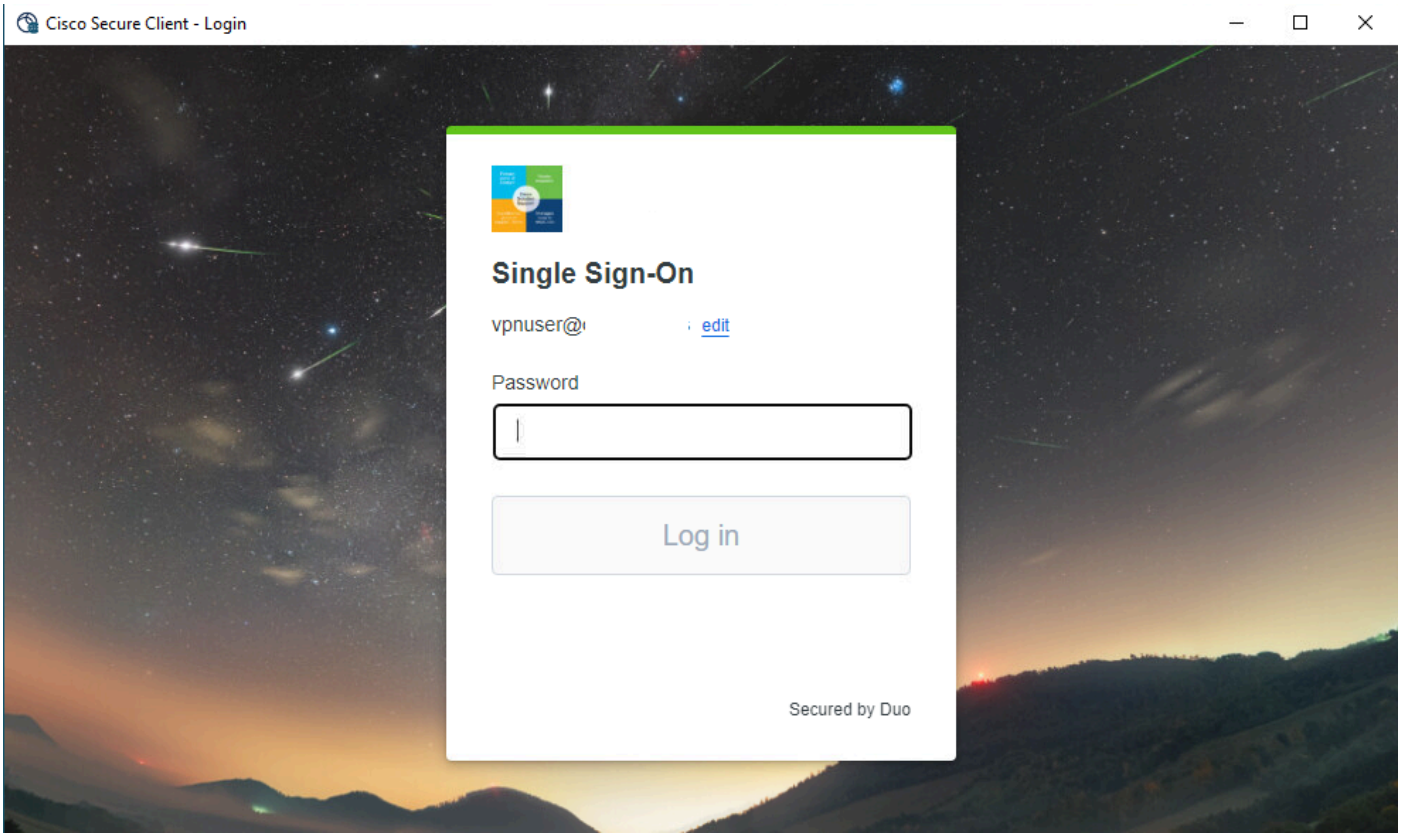
RA-VPN

Faça login através do Cisco Secure Client Agent-VPN.



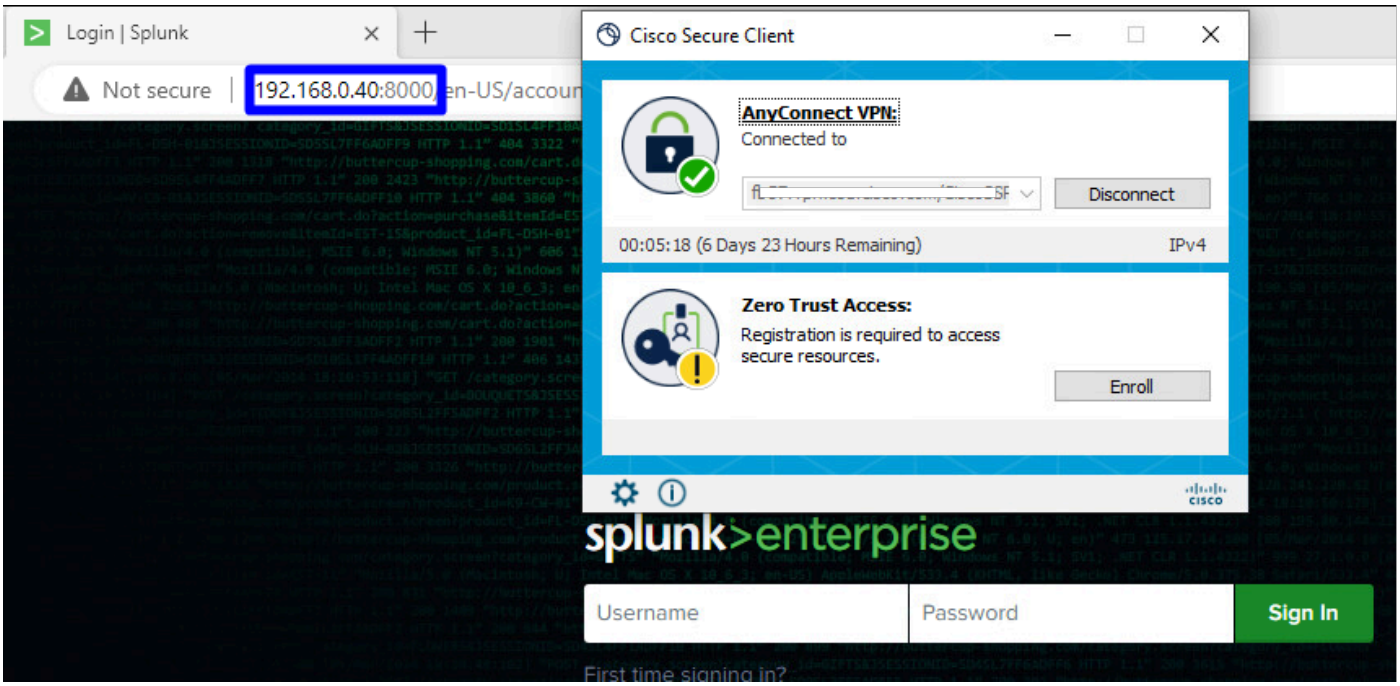
Cliente seguro - VPN

- Autenticar através do provedor SSO



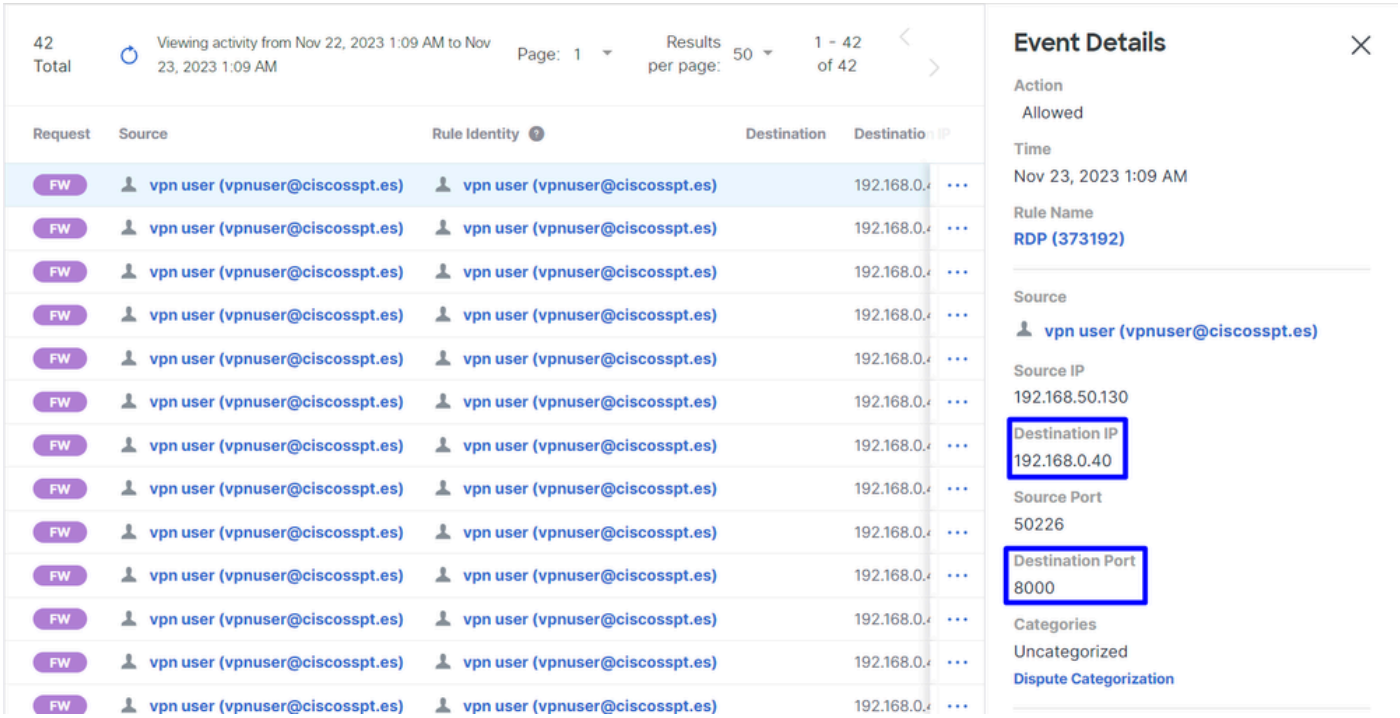
Acesso seguro - VPN - SSO

- Depois de autenticado, acesse o recurso:



Acesso seguro - VPN - Autenticado

Navegue até:Monitor > Activity Search

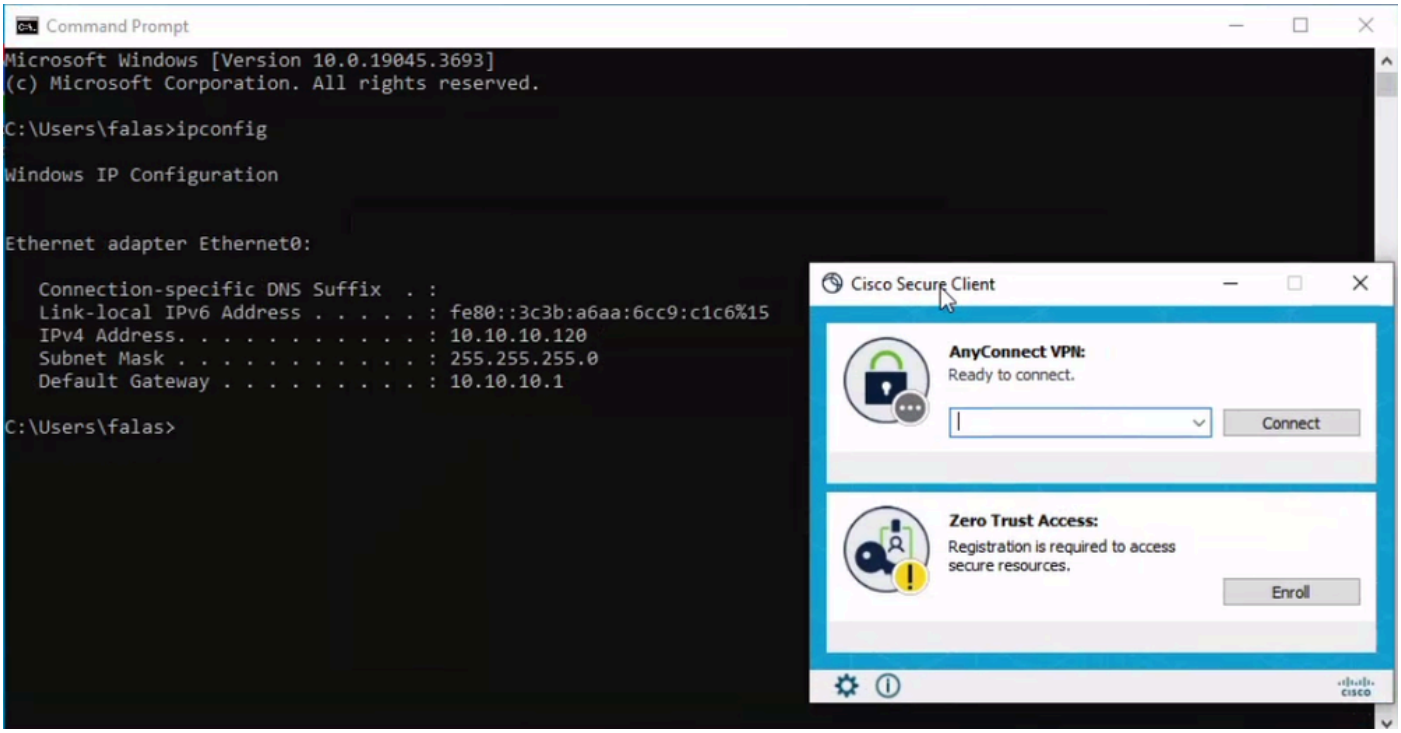


Acesso seguro - Pesquisa de atividades - RA-VPN

Você pode ver que o usuário teve permissão para se autenticar por meio de RA-VPN.

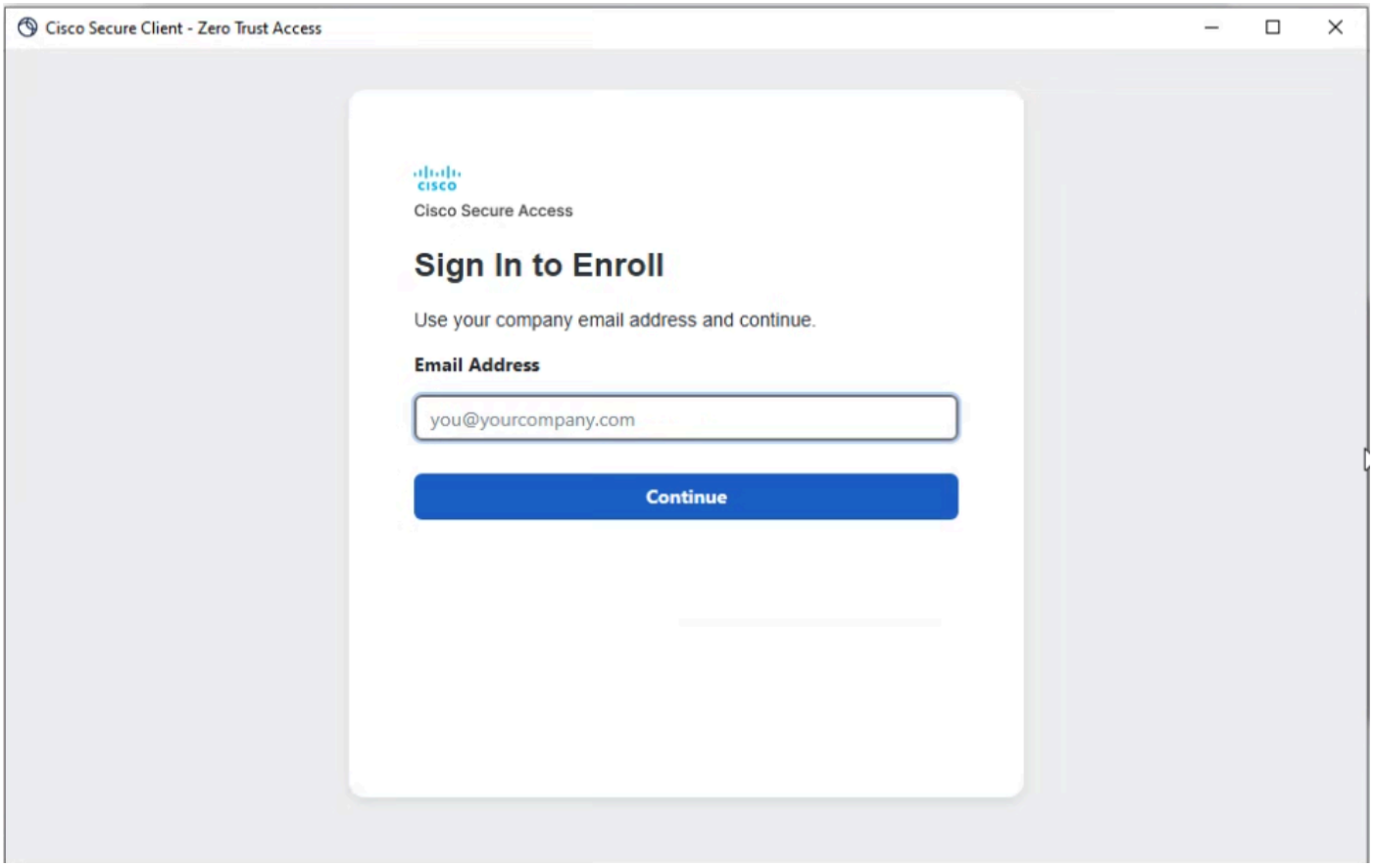
ZTNA baseado em cliente

Faça login através do Cisco Secure Client Agent - ZTNA.



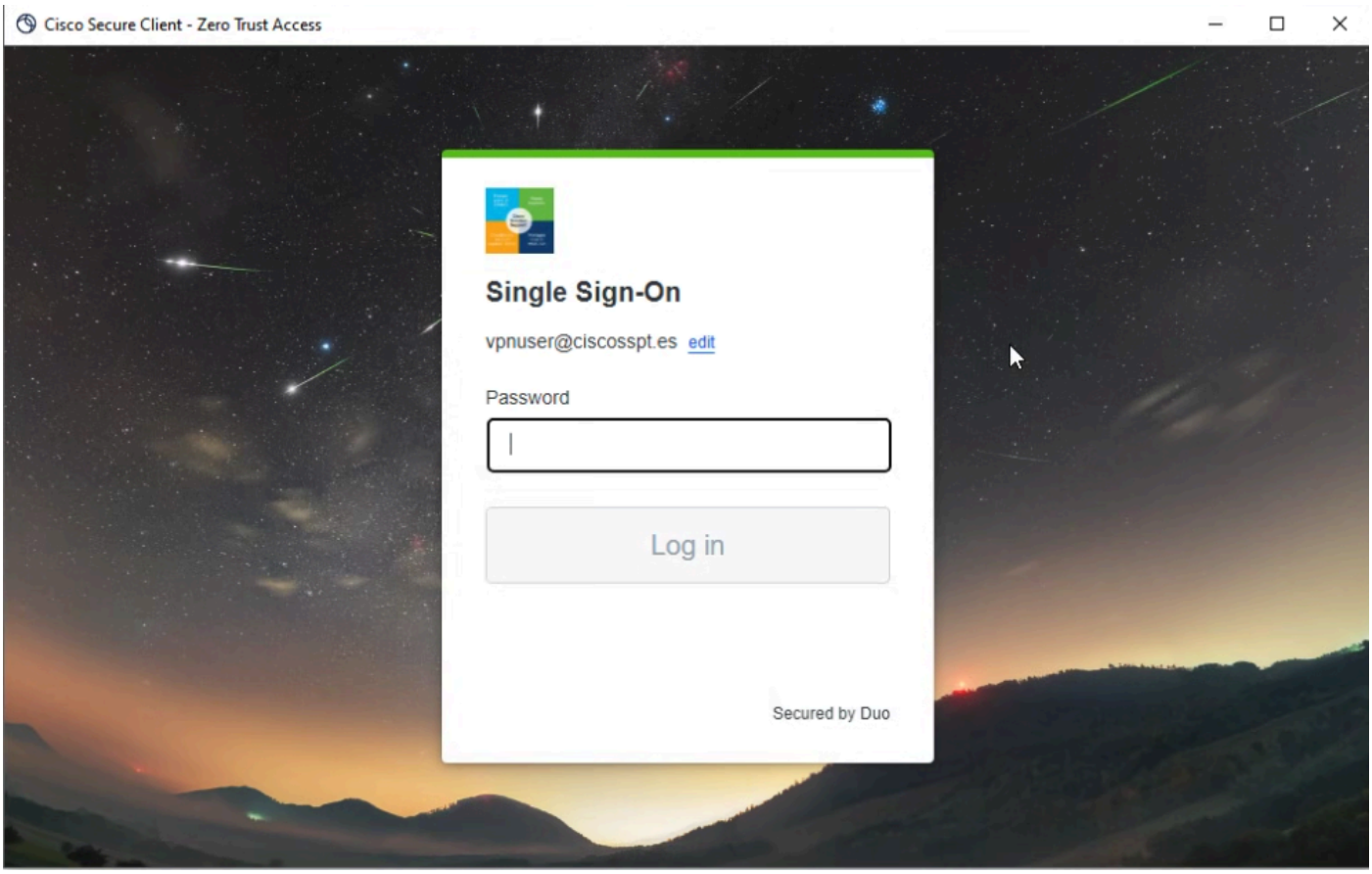
Cliente seguro - ZTNA

- Inscreva-se com seu nome de usuário.



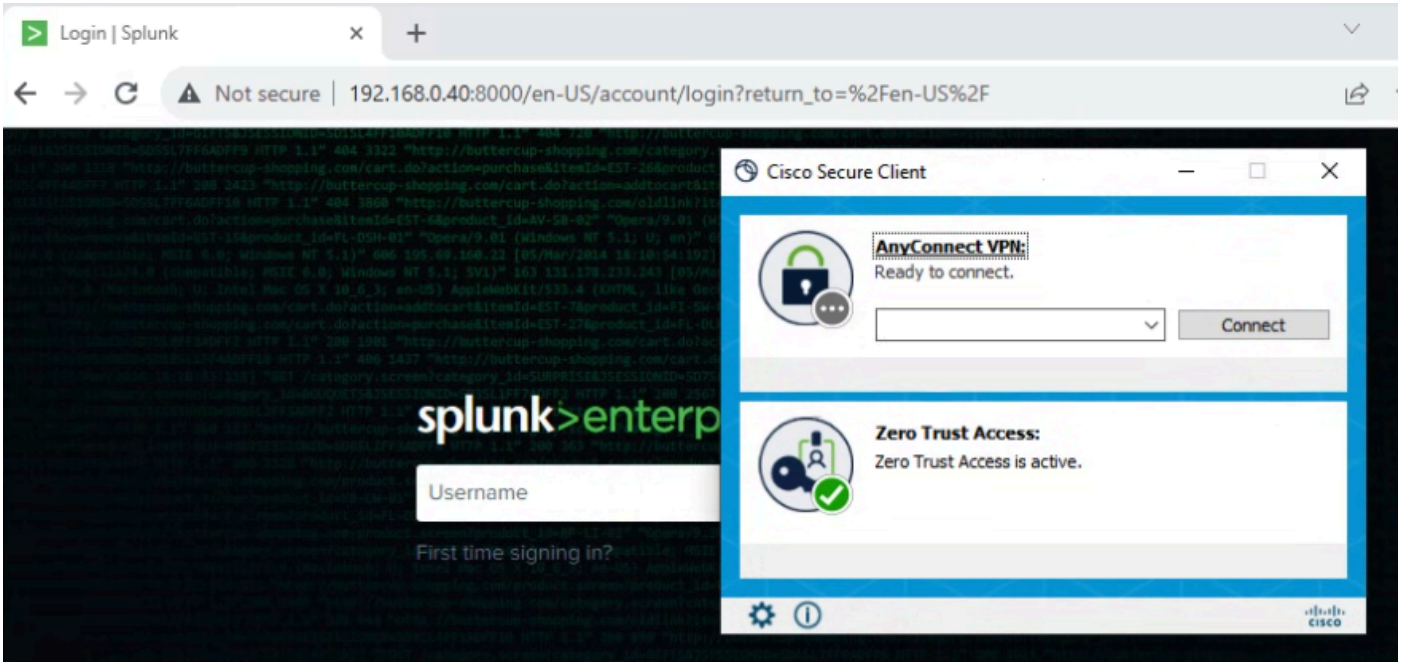
Secure Client - ZTNA - Inscrever

- Autenticar em seu Provedor de SSO



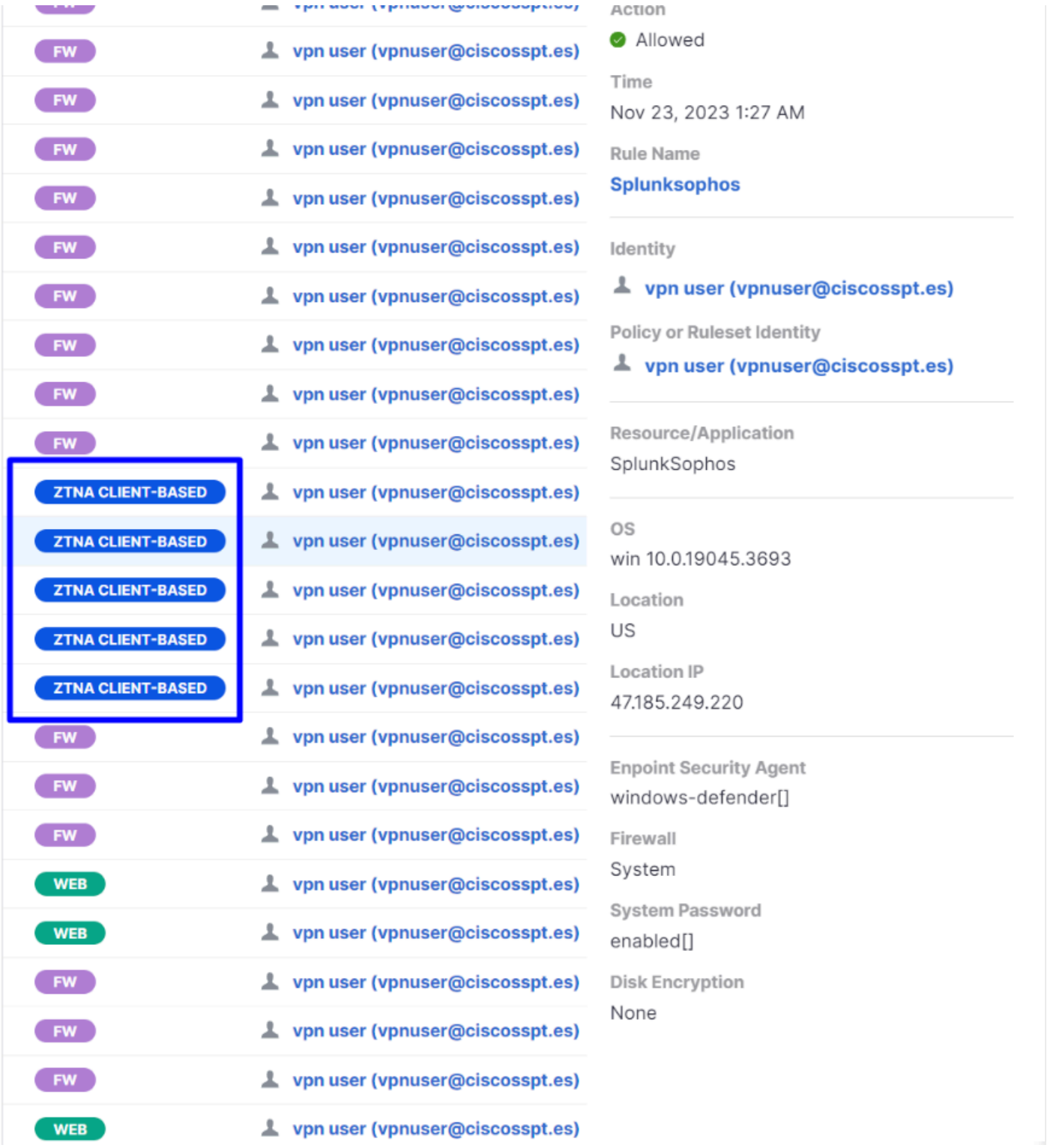
Cliente seguro - ZTNA - Login SSO

- Depois de autenticado, acesse o recurso:



Acesso seguro - ZTNA - Conectado

Navegue até:Monitor > Activity Search

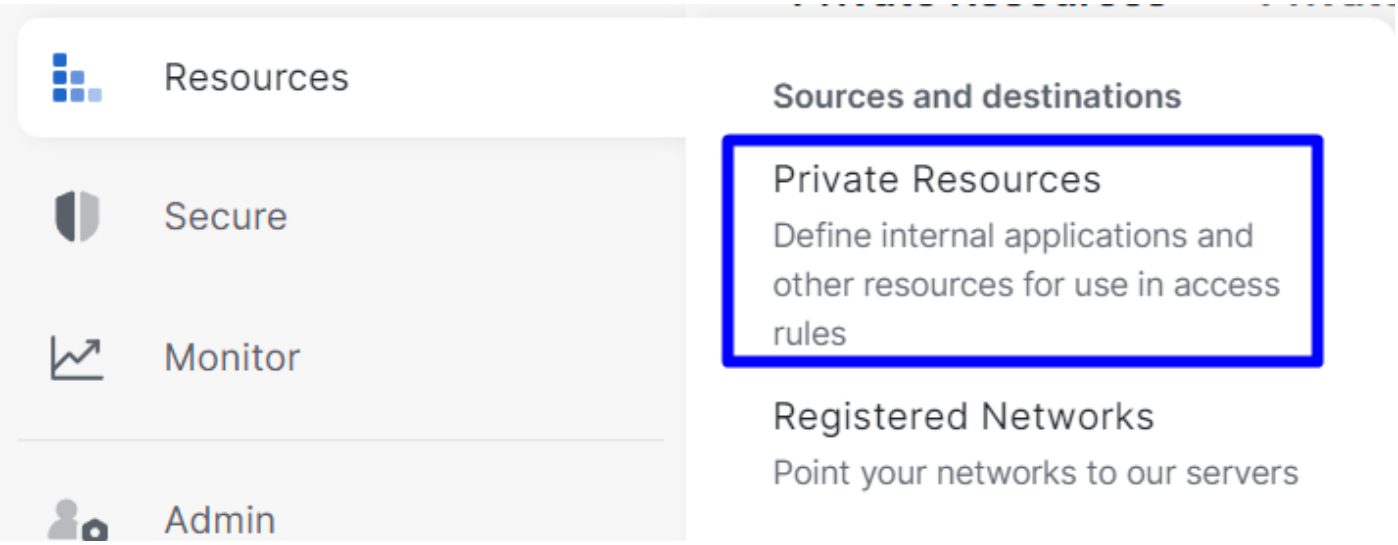


Acesso seguro - Pesquisa de atividades - Baseado em cliente ZTNA

Você pode ver que o usuário teve permissão para se autenticar por meio do ZTNA baseado em cliente.

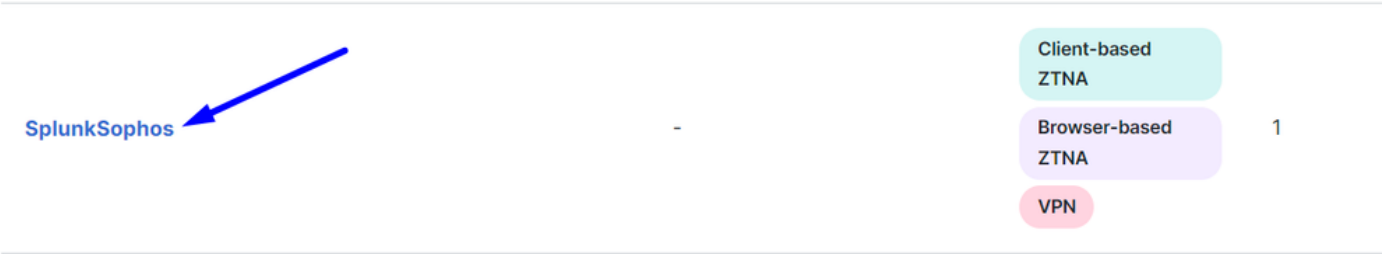
ZTNA baseado em navegador

Para obter o URL, você precisa ir para **Resources > Private Resources**.



Acesso seguro - Recurso privado

- Clique em sua política



Acesso seguro - Recurso privado - SplunkSophos

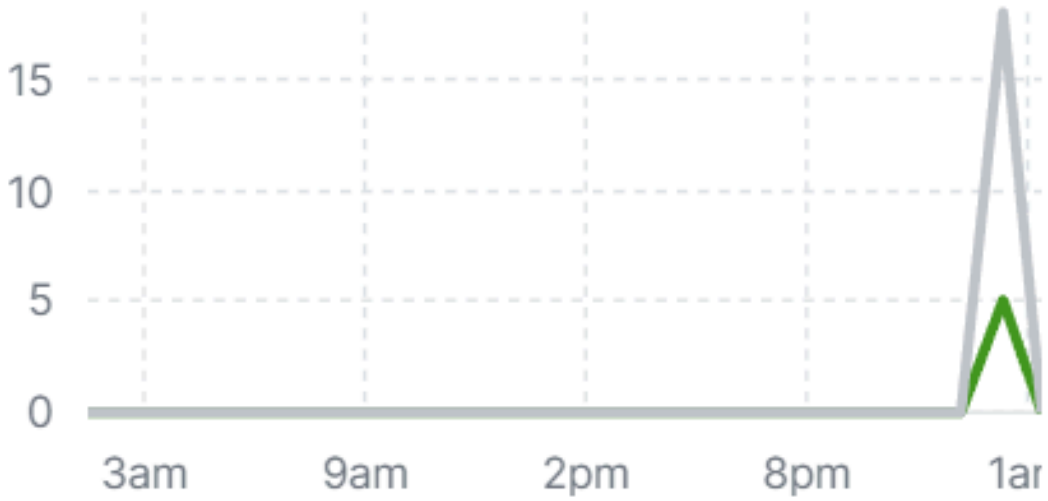
- Rolar para baixo

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.