

Configure o acesso seguro com o firewall Sophos XG

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar o túnel no acesso seguro](#)

[Dados do túnel](#)

[Configurar o túnel no Sophos](#)

[Configurar perfil IPsec](#)

[Configurar VPN site a site](#)

[Configurar a interface do túnel](#)

[Configurar os gateways](#)

[Configurar a rota SD-WAN](#)

[Configurar Aplicativo Privado](#)

[Configurar a política de acesso](#)

[Verificar](#)

[RA-VPN](#)

[ZTNA baseado em cliente](#)

[ZTNA baseado em navegador](#)

[Informações Relacionadas](#)

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



CISCO

Secure

Access

SOPHOS

Acesso seguro - Sophos

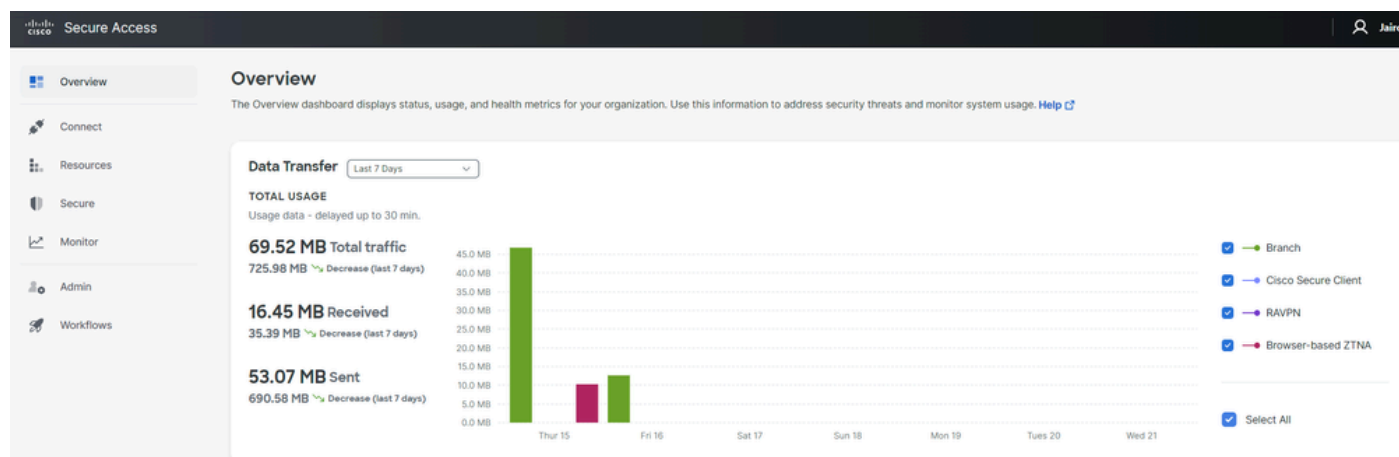
A Cisco projetou o Secure Access para garantir a proteção e o fornecimento de acesso a aplicativos privados, tanto no local quanto baseados em nuvem. Ele também protege a conexão da rede à Internet. Isso é obtido por meio da implementação de vários métodos e camadas de segurança, todos voltados para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

Overview

The Overview dashboard displays

Essentials

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

Connect

Resources

Secure

Monitor

Admin

Acesso seguro - Conexões de rede

- Em Network Tunnel Groups clique em + Add.

Connector Groups Beta **Network Tunnel Groups**

Network Tunnel Groups 2 total

1 Disconnected ● 1 Warning ▲ 0 Connected ●

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Q Search Region Status 2 Tunnel Groups + Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
HOME	● Disconnected	Europe (Germany)	sse-euc-1-1-0	0	sse-euc-1-1-1	0
SAD	▲ Warning	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1	0

Rows per page 10 < 1 >

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

 ⊗

Region

 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



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

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

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**.

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

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

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.

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

[Download CSV](#)

[Done](#)

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:

SOPHOS Sophos Firewall PW

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

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

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Advanced protection

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

System

Traffic insight

Web activity 0 max | 0 avg

Cloud applications

0 Apps

0 B In

0 B Out

Security Heartbeat®

0 At risk

Monitor endpoint health and systems at risk

Synchronized Application Control™

0 Apps

Identify unknown apps on your network

Zero-day protection

0 Recent

0 Incidents

0 Scanned

ATP

0 Sources blocked

UTQ

0 Accounts at risk

SSL/TLS connections

0% Of traffic

0% Decrypted

0 Failed

Active firewall rules

0 WAF

1 User

3 Network

4 Scanned

4 Unused

2 Disabled

0 Changed

0 New

Reports

0 Risky apps seen

0 Objectionable websites seen

0 bytes Used by top 10 web users

0 Intrusion attacks

Messages

Alert

Warning

Alert

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

Click on widgets to open details

Painel de administração do Sophos

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

IPsec profiles

Device access

Add

Delete

algorithm

Phase 2

Manage

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

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 - 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)

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		
DH group (key group) 2 selected <input checked="" type="checkbox"/>		
Encryption AES256 <input checked="" type="checkbox"/>	Authentication SHA2 256 <input checked="" type="checkbox"/>	
+ You can add up to 3 different algorithm combinations		

Sophos - 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

Phase 2

PFS group (DH group) Same as phase-I <input checked="" type="checkbox"/>	Key life 3600 <input checked="" type="checkbox"/>
Seconds	
Encryption AES256 <input checked="" type="checkbox"/>	Authentication SHA2 256 <input checked="" type="checkbox"/>
+ You can add up to 3 different algorithm combinations	

Sophos - 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)

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 - 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**.

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

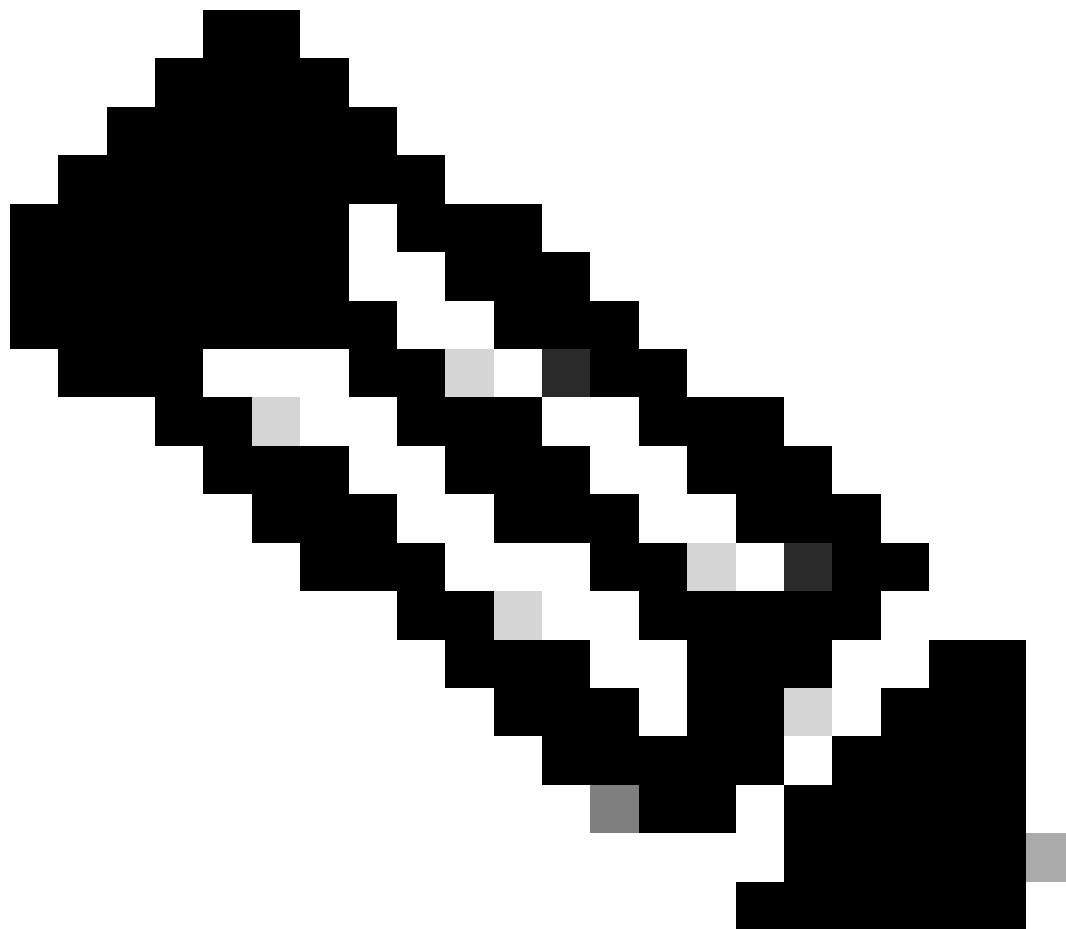
Add Delete Wizard

Add Delete

Sophos - VPN 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.

General settings

Name SecureAccessS	IP version <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
Description This is the IPsec Policy for Sophos	Connection type Tunnel interface	
	Gateway type Initiate the connection	

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

Encryption

Profile	Authentication type
CSA	Preshared key
	Preshared key
	Repeat 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

<p>ID local</p> <p>O e-mail gerado sob a etapa, Tunnel Data</p>	<p>ID remota</p> <p>O IP público gerado sob a etapa, Tunnel Data</p>
<p>Sub-rede local qualquer um</p>	<p>Sub-rede Remota qualquer um</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 site a site - Configurações de gateway

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

IPsec connections

Show additional properties

Name	Group name	Profile	Connection type	Status	Connection	Manage
<input type="checkbox"/> <u>SecureAccessS</u>	-	CSA	Tunnel interface	● Active	● <input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Stop"/> <input type="button" value="Delete"/>

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**.

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

Sophos - Monitorar e analisar - IPsec

Live users	Live connections	Live connections IPv6	IPsec connections	Remote users			
No tunnel established to Secure Access							
<input type="checkbox"/>	Name ▾	Local server ▾	Local subnet ▾	Username ▾	Remote server/host ▾	Remote subnet ▾	Manage
No records found							
Tunnel established to Secure Access							
<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	

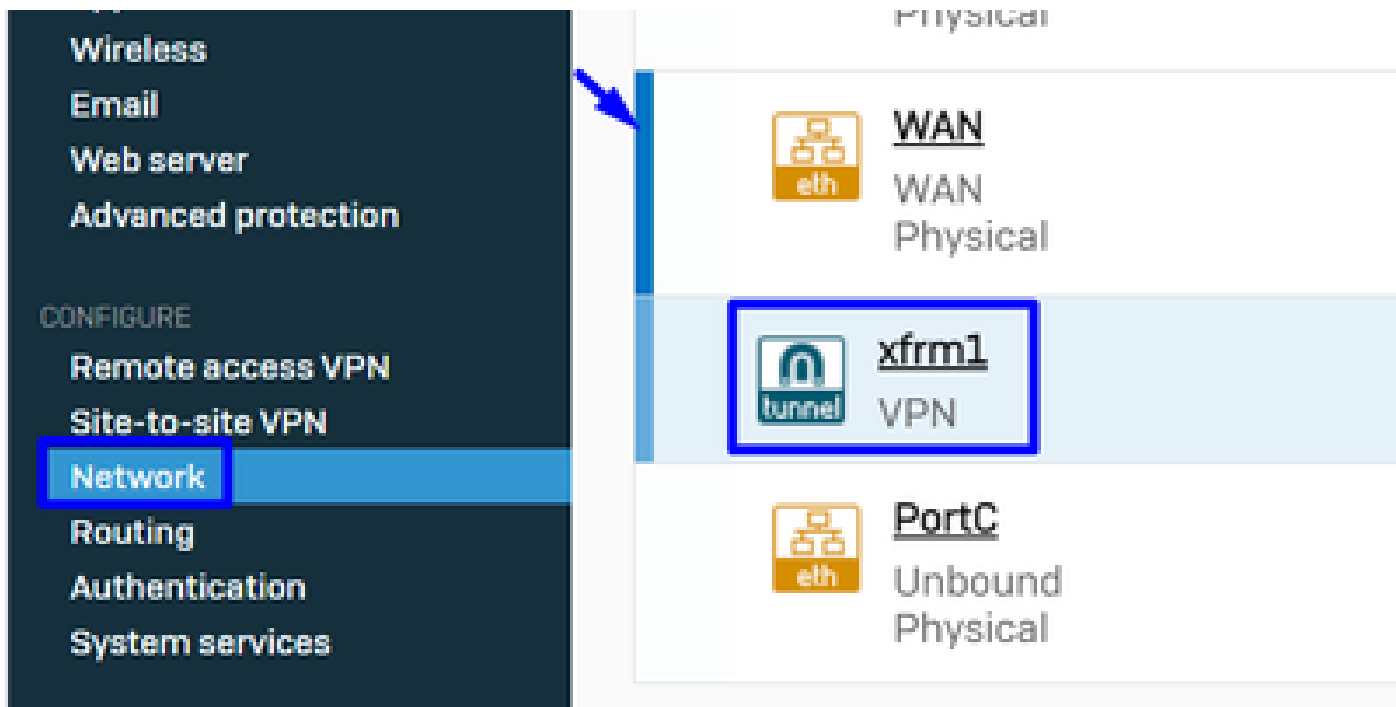
Sophos - Monitorar e analisar - IPsec antes e depois

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

Configurar a interface do túnel

Navegue **Network** e verifique sua WAN 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

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 - Rede - Interface de túnel - Configuração

Configurar os gateways

Para configurar o gateway para a interface virtual (xfrm)

- Navegue até Routing > Gateways
- Clique em Add

The screenshot shows the Sophos Gateway configuration page. The 'Gateways' tab is active. Under the 'IPv4 gateway' section, a table lists the configured gateways. One gateway is shown: 'DHCP_PortB_GW' with IP address '192.168.0.1', Interface 'WAN', Health check 'On', and Status 'Down' (indicated by a red dot). Buttons for 'Add' and 'Delete' are visible at the top right of the table.

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)

The screenshot shows the 'Gateway host' configuration form. The fields are: Name * (CSA_GW), Gateway IP (169.254.0.2), Interface (xfrm1-169.254.0.1), and Zone (None).

Sophos - Roteamento - Gateways - Host do gateway

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

Health check

Health check



Sophos - Roteamento - Gateways - Verificação de integridade

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

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		

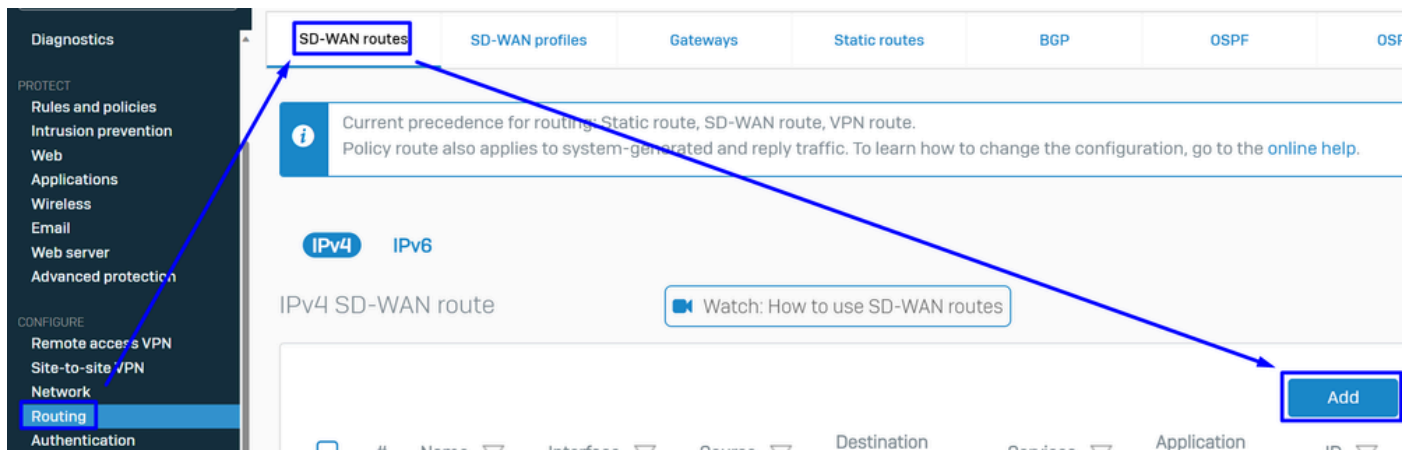
Sophos - Roteamento - Gateways - Status

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

Traffic selector

Incoming interface: LAN-192.168.0.203

DSCP marking: Select DSCP marking

Source networks: Any

Destination networks: Any

Services: Any

Application object: Any

User or groups: Any

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**

Link selection settings

Select SD-WAN profile ⓘ Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

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**

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

Acesso seguro - Recursos privados

- Clique em + Add

Private Resources Private Resource Groups

Private Resources

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

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

Acesso seguro - Recursos privados 2

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

General

Private Resource Name

SplunkSophos

Description (optional)

Acesso seguro - Recursos privados - Geral

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

- **Internally 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

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

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**

Zero-trust connections

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

Client-based connection

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

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

192.168.0.40

+ FQDN or IP Address

Browser-based connection

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

Public URL for this resource ⓘ

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



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

HTTP

Validate Application Certificate ⓘ

VPN connections

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

Save Cancel

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

Após a conclusão da configuração, este é o resultado:

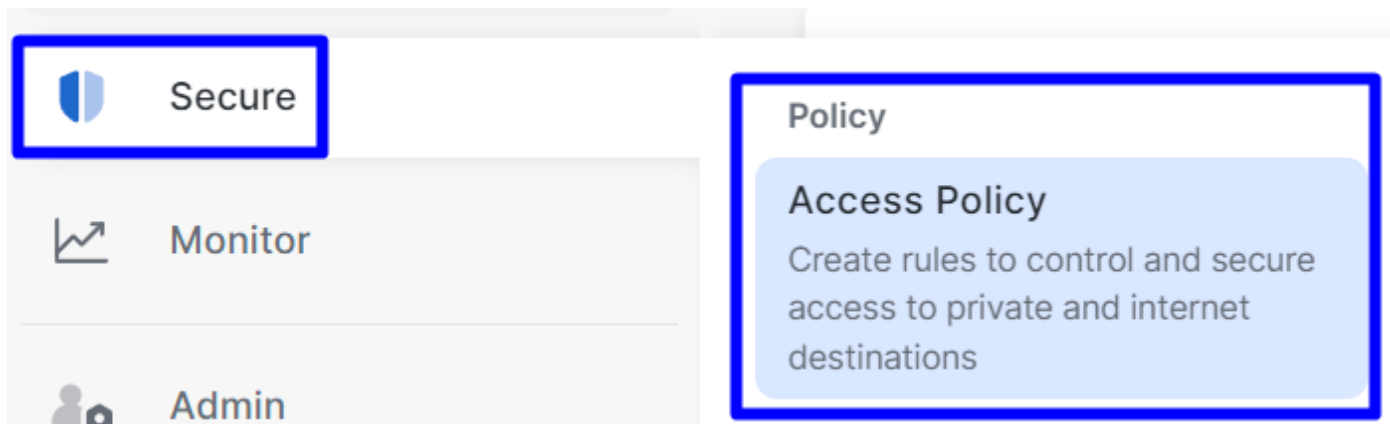
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none">VPNBrowser-based ZTNAClient-based ZTNA	1	2	16

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**

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

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**

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

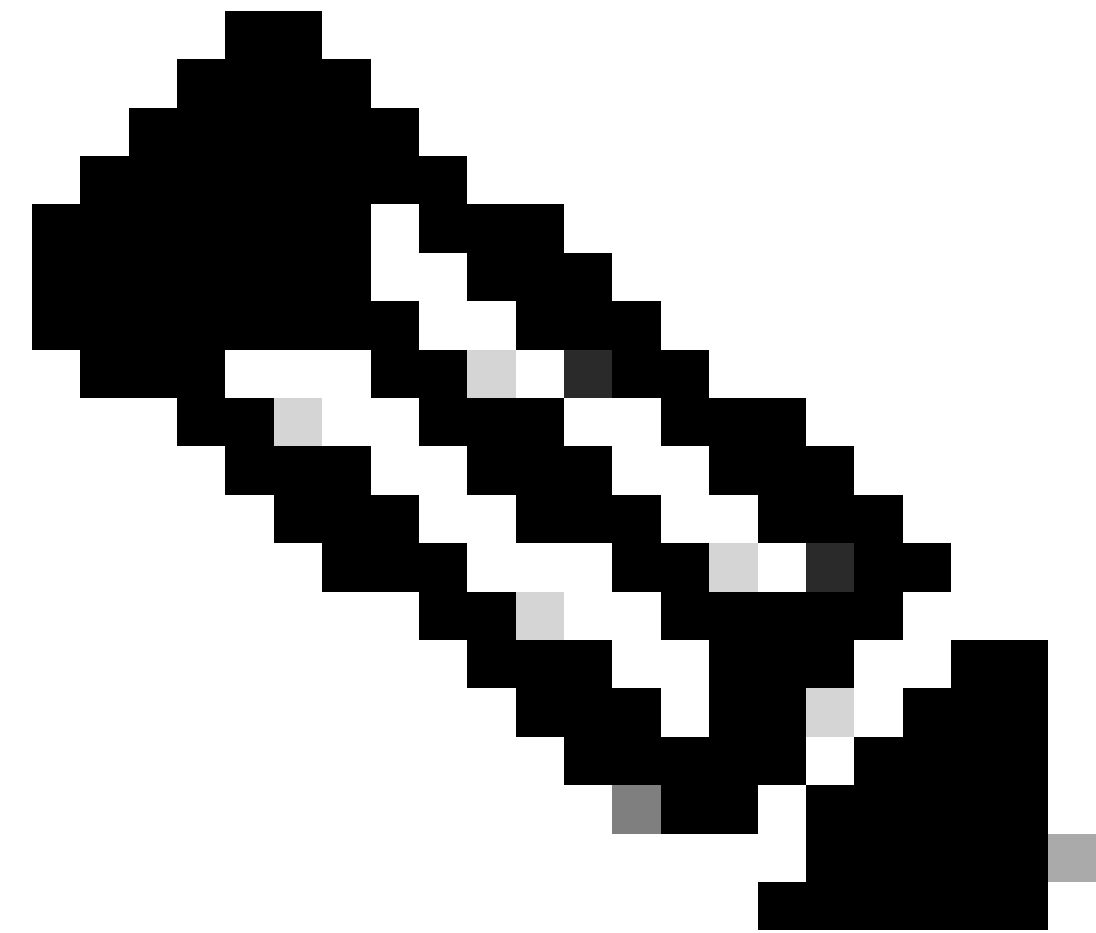
Rule Defaults

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**

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:

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

Acesso seguro - Política de acesso configurada

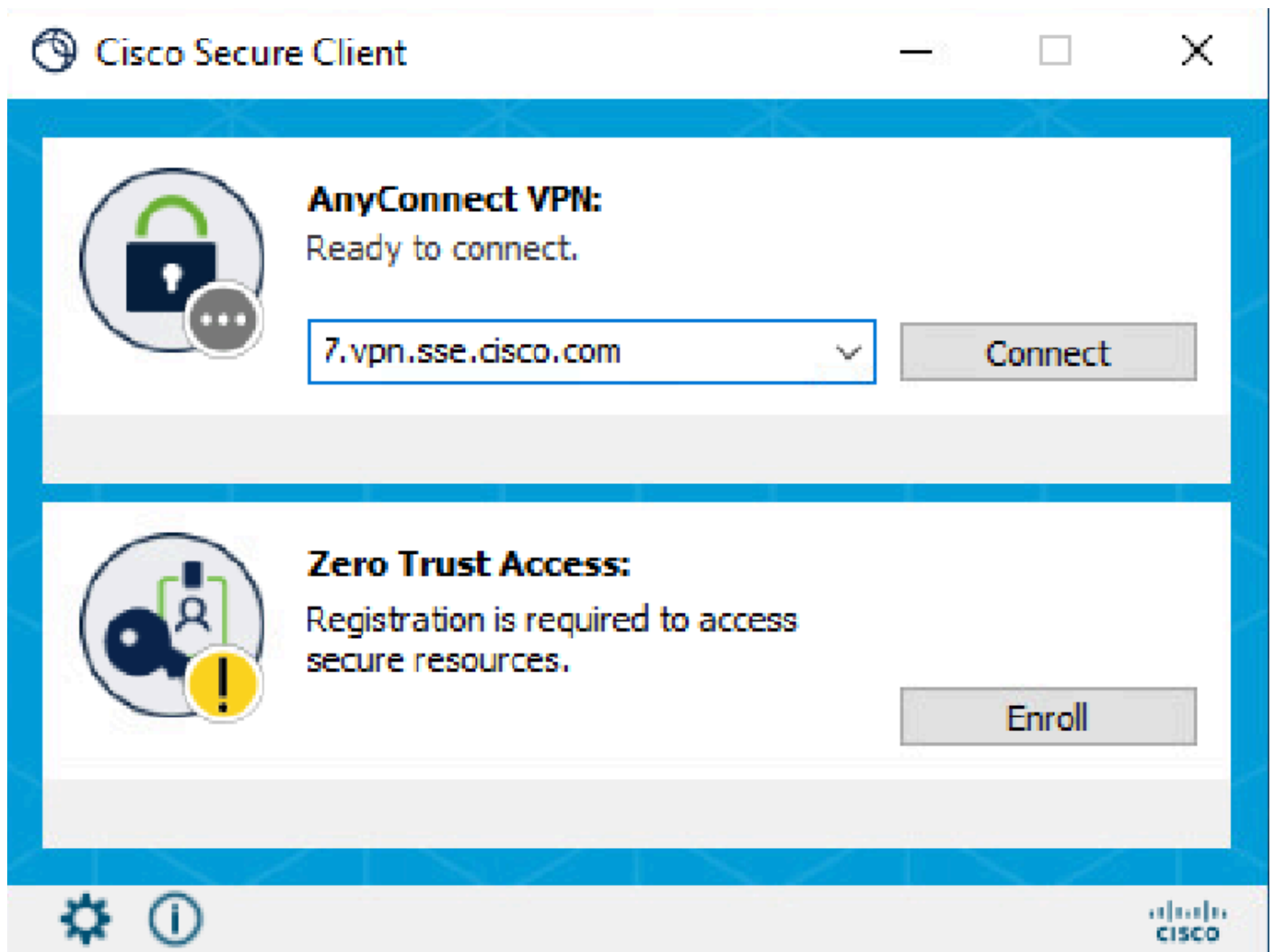
Depois disso, você poderá prosseguir com a etapa Verify.

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](#).

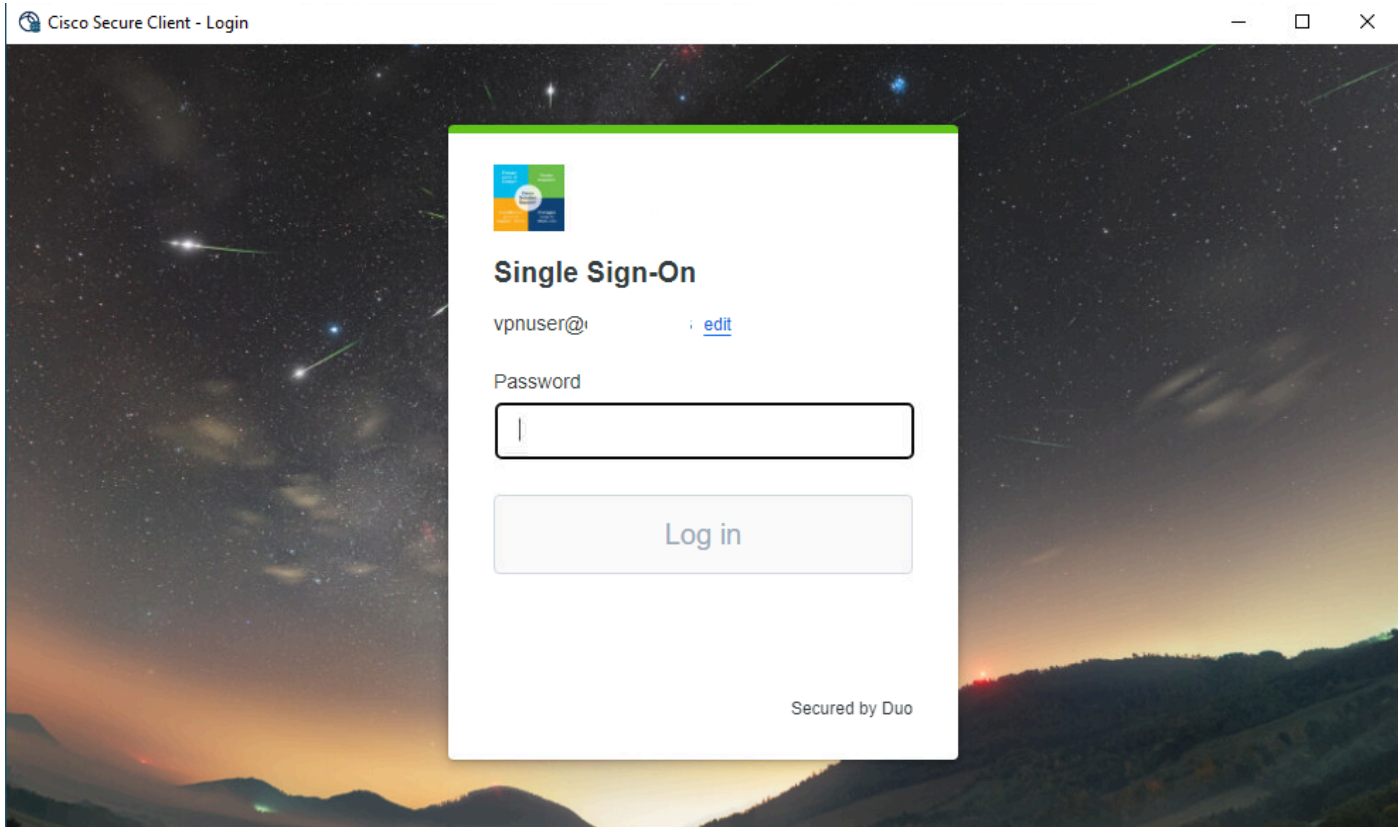
RA-VPN

Faça login através do Cisco Secure Client Agent-VPN.



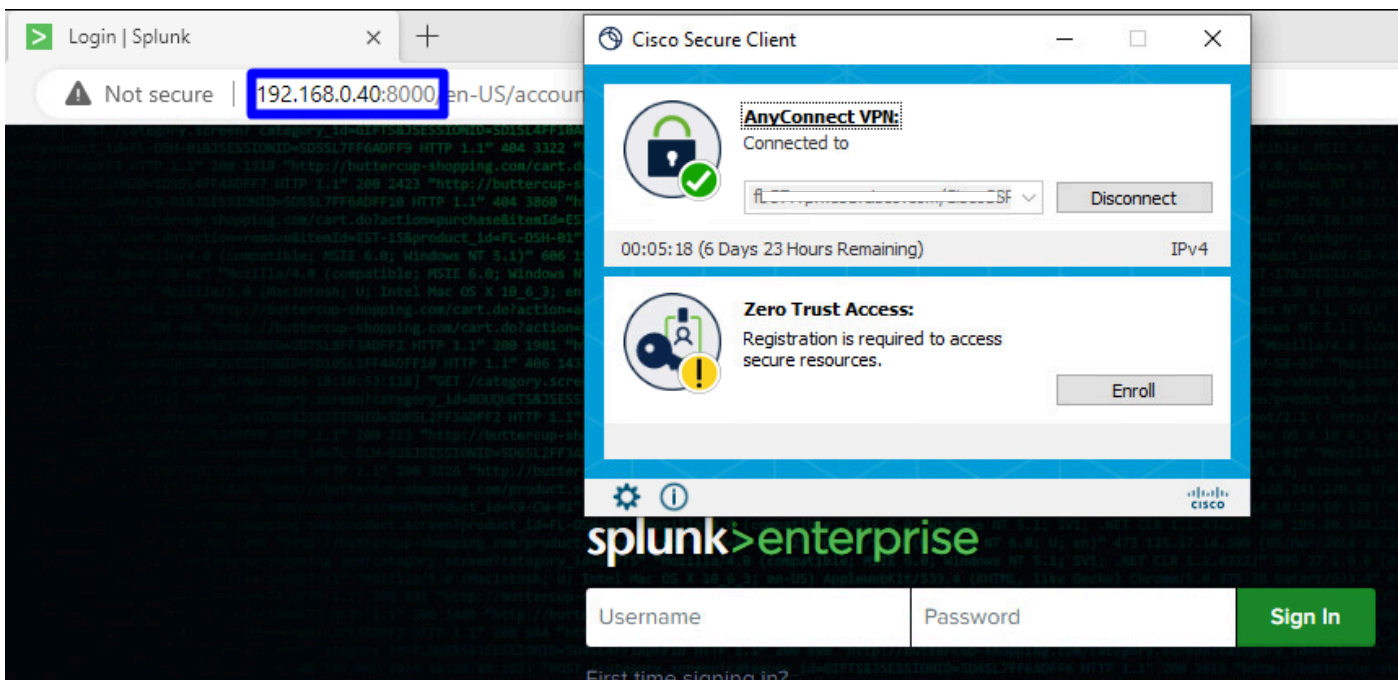
Cliente seguro - VPN

- Autenticar através do provedor SSO



Acesso seguro - VPN - SSO

- Depois de autenticado, acesse o recurso:



Acesso seguro - VPN - Autenticado

Navegue até: Monitor > Activity Search

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

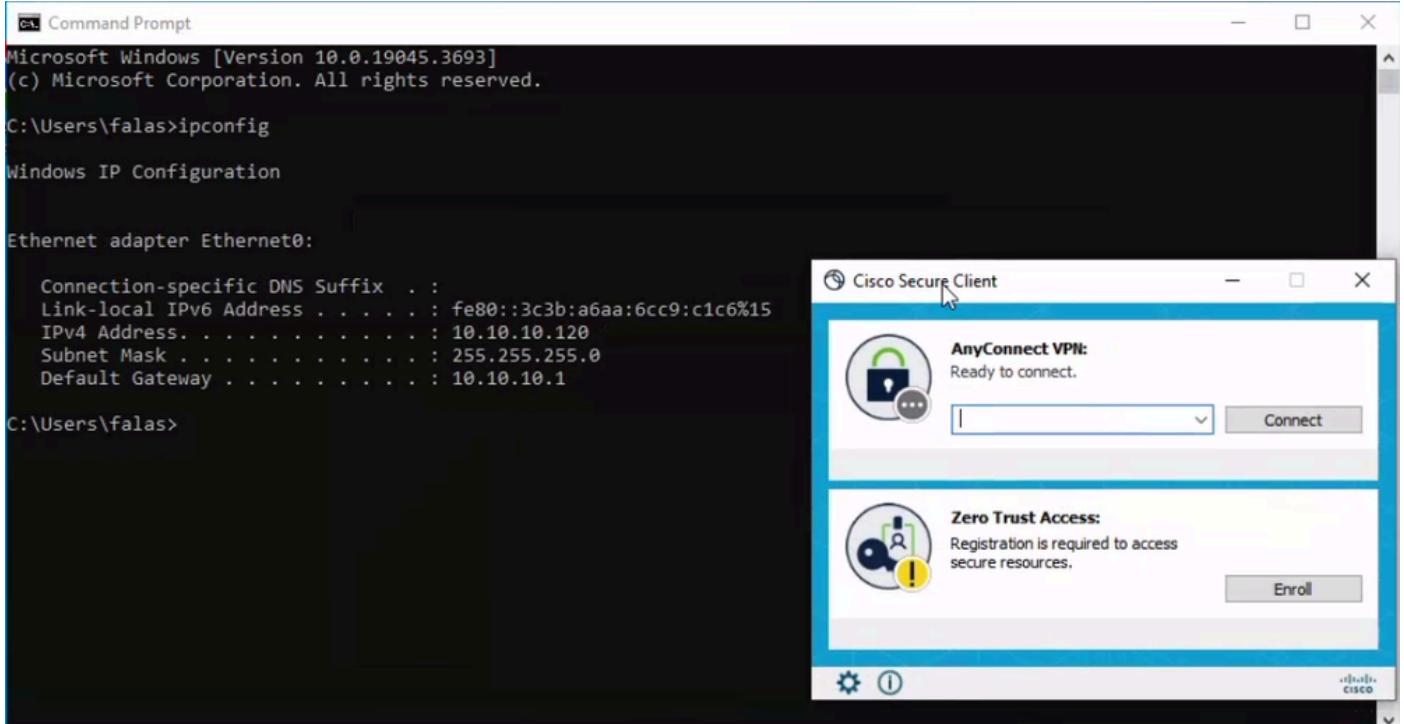
Categories: Uncategorized, Dispute Categorization

Acesso seguro - Pesquisa de atividades - RA-VPN

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

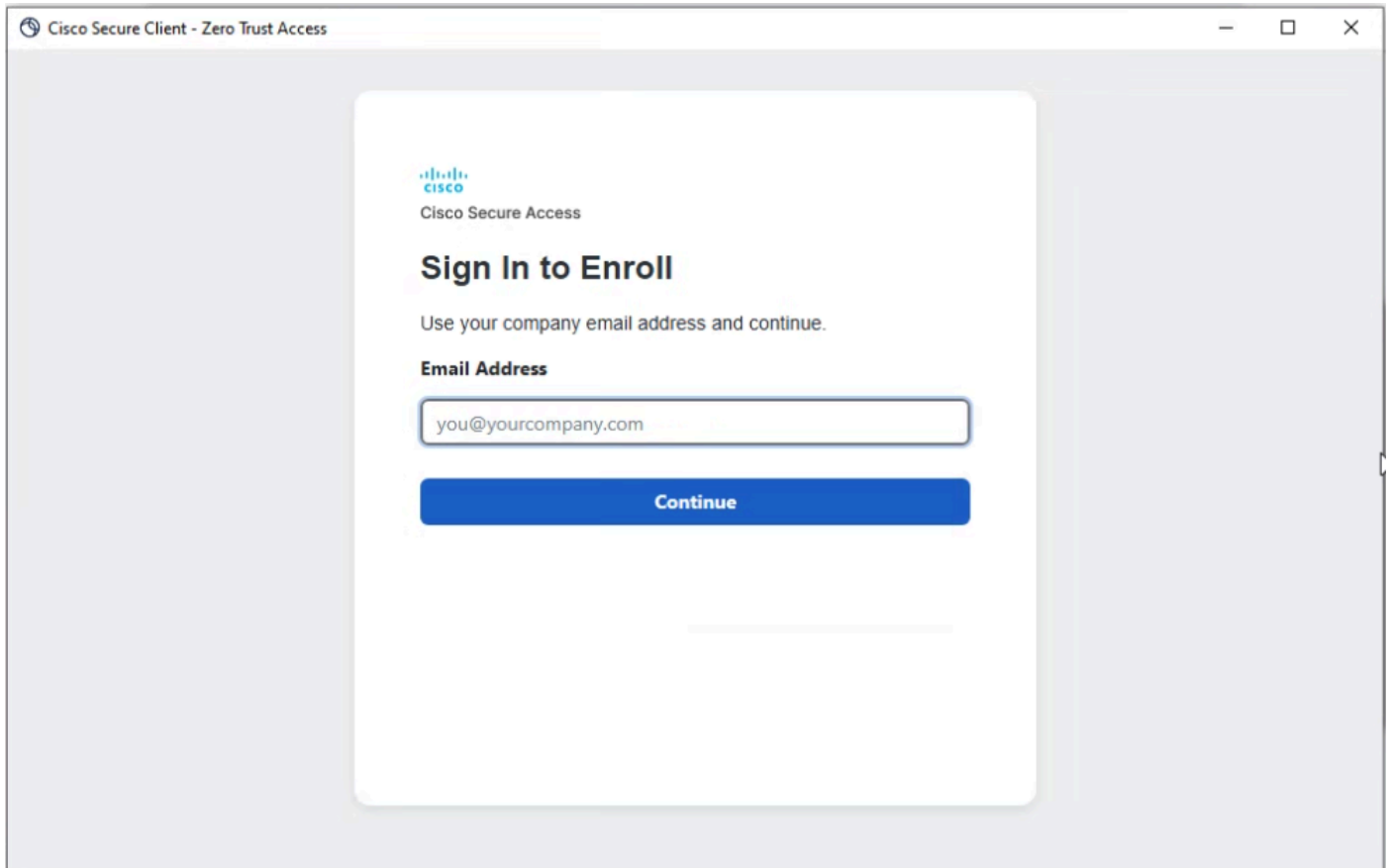
ZTNA baseado em cliente

Faça login através do Cisco Secure Client Agent - ZTNA.



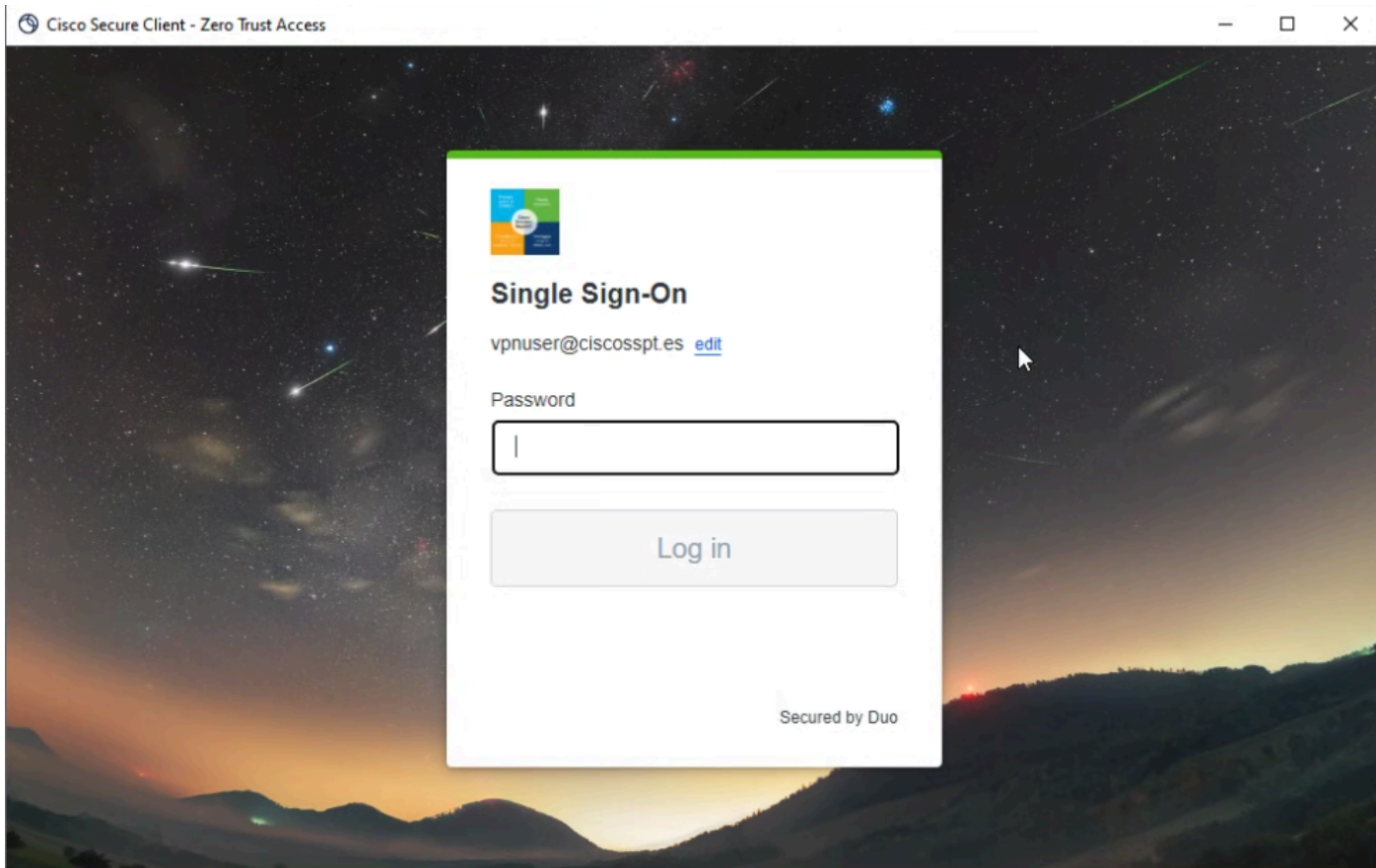
Cliente seguro - ZTNA

- Inscreva-se com seu nome de usuário.



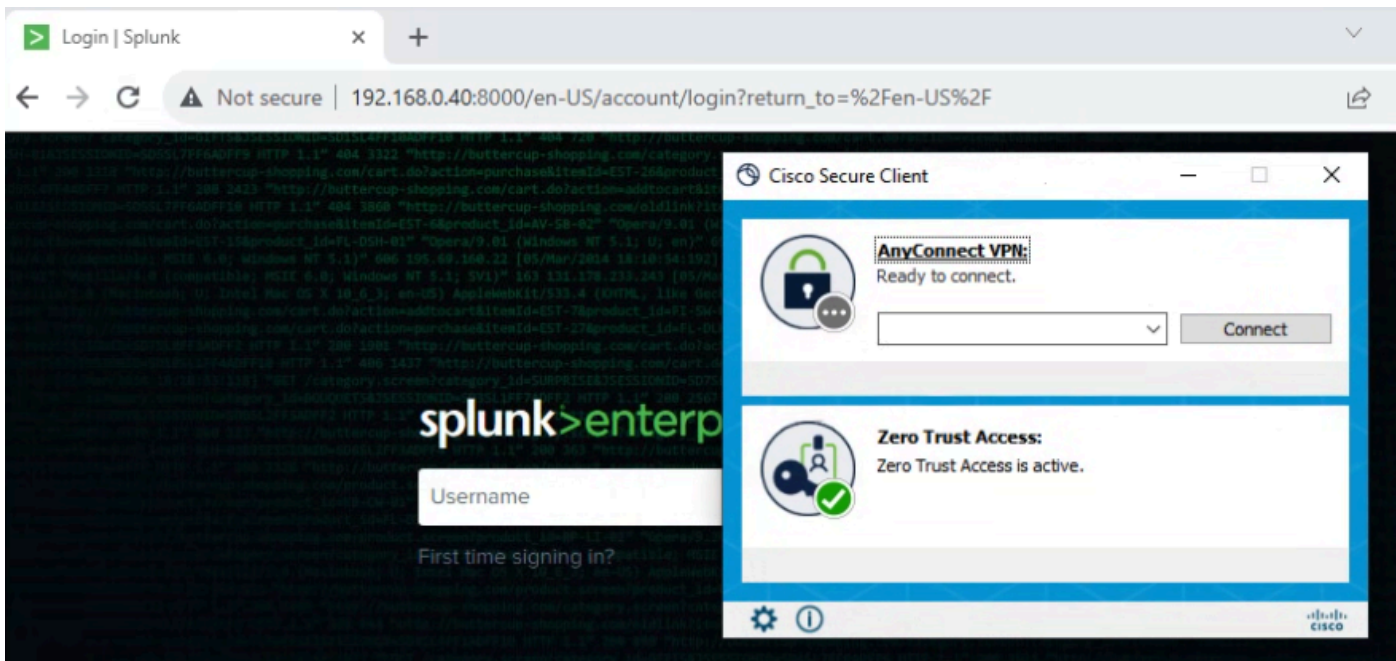
Secure Client - ZTNA - Inscrever

- 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

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)		
FW	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
WEB	vpn user (vpnuser@ciscospt.es)		

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**.

The screenshot shows the Splunk Sophos interface. On the left is a sidebar with the following items: 'Resources' (with a grid icon), 'Secure' (with a shield icon), 'Monitor' (with a line graph icon), and 'Admin' (with a person icon). The main content area is titled 'Sources and destinations' and contains two options: 'Private Resources' (with the subtext 'Define internal applications and other resources for use in access rules') and 'Registered Networks' (with the subtext 'Point your networks to our servers'). The 'Private Resources' option is enclosed in a blue rectangular box.

Acesso seguro - Recurso privado

- Clique em sua política

The screenshot shows a table with one row. The first cell contains the text 'SplunkSophos'. A blue arrow points from the top right towards the 'SplunkSophos' text. To the right of the table, there are three stacked buttons: 'Client-based ZTNA' (teal), 'Browser-based ZTNA' (purple), and 'VPN' (pink). The number '1' is positioned to the right of these buttons.

Acesso seguro - Recurso privado - SplunkSophos

- Rolar para baixo

SplunkSophos

Client-based ZTNA

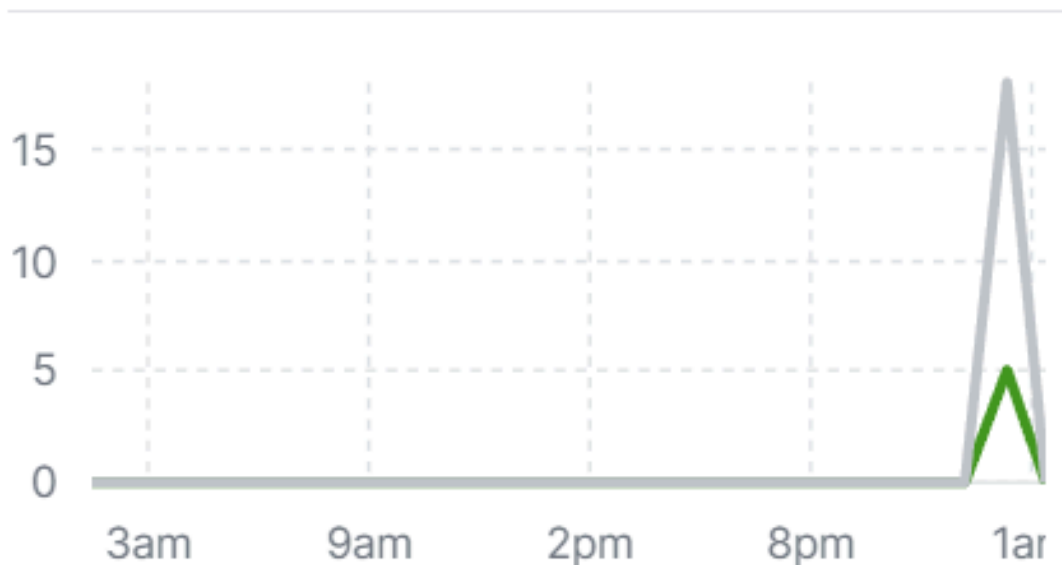
Browser-based ZTNA



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.