

使用Sophos XG防火墙配置安全访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[在安全访问时配置隧道](#)

[隧道数据](#)

[在Sophos上配置隧道](#)

[配置IPsec配置文件](#)

[配置站点到站点VPN](#)

[配置隧道接口](#)

[配置网关](#)

[配置SD-WAN路由](#)

[配置专用应用](#)

[配置访问策略](#)

[验证](#)

[RA-VPN](#)

[基于客户端的ZTNA](#)

[基于浏览器的ZTNA](#)

[相关信息](#)

简介

本文档介绍如何使用Sophos XG防火墙配置安全访问。

先决条件

- [配置用户调配](#)
- [ZTNA SSO身份验证配置](#)
- [配置远程访问VPN安全访问](#)

要求

Cisco 建议您了解以下主题：

- Sophos XG防火墙
- 安全访问
- 思科安全客户端- VPN
- 思科安全客户端- ZTNA

- 无客户端ZTNA

使用的组件

本文档中的信息基于：

- Sophos XG防火墙
- 安全访问
- 思科安全客户端- VPN
- 思科安全客户端- ZTNA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息



CISCO

Secure

Access

SOPHOS

安全访问- Sophos

思科设计了安全访问(Secure Access)，以确保对内部和基于云的私有应用的访问得到保护和调配。它还可以保护从网络到Internet的连接。这通过实施多种安全方法和层来实现，所有 these 方法都旨在保护通过云访问信息时所需的信息。

配置

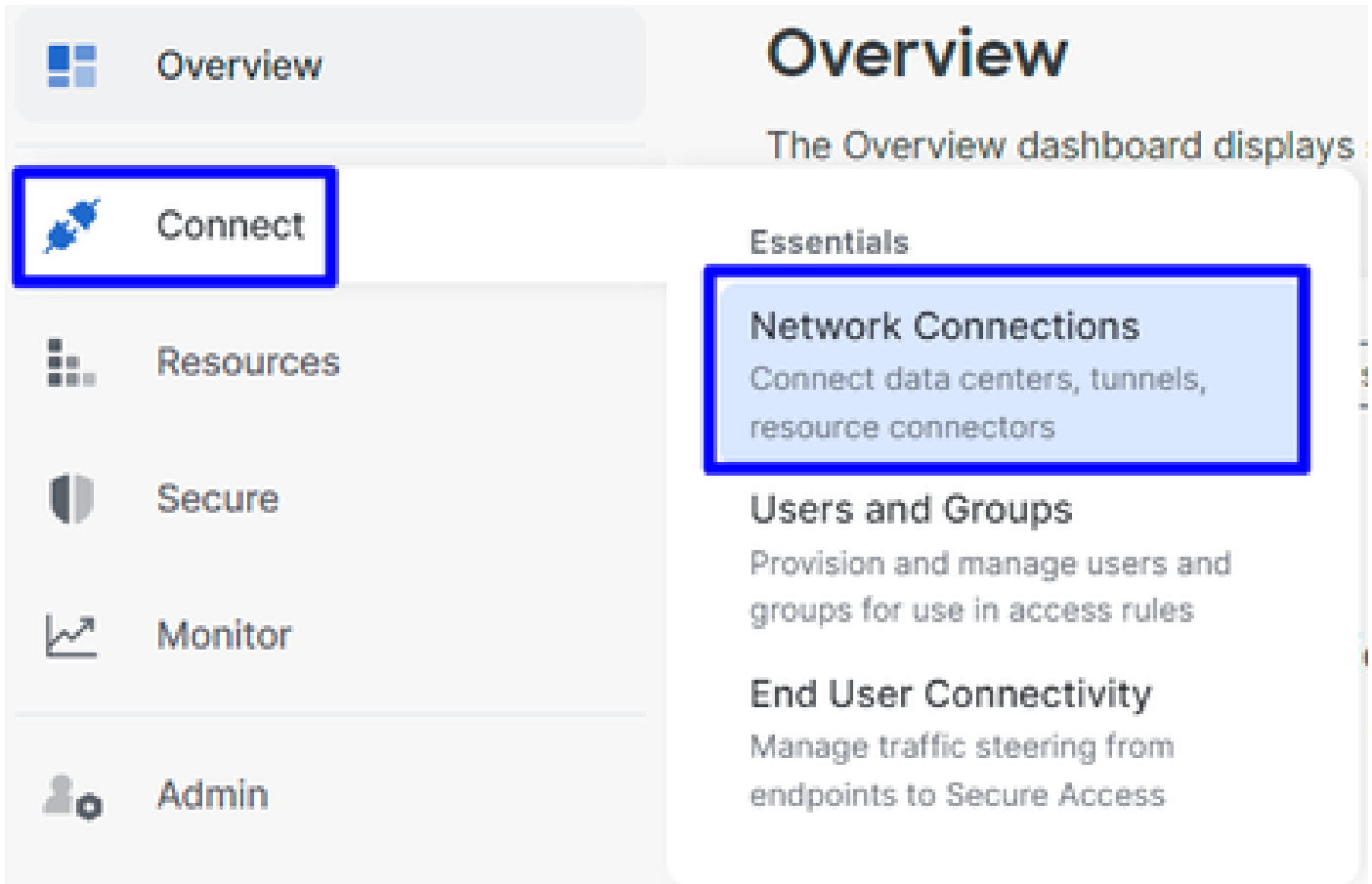
在安全访问时配置隧道

导航到[安全访问](#)的管理面板。



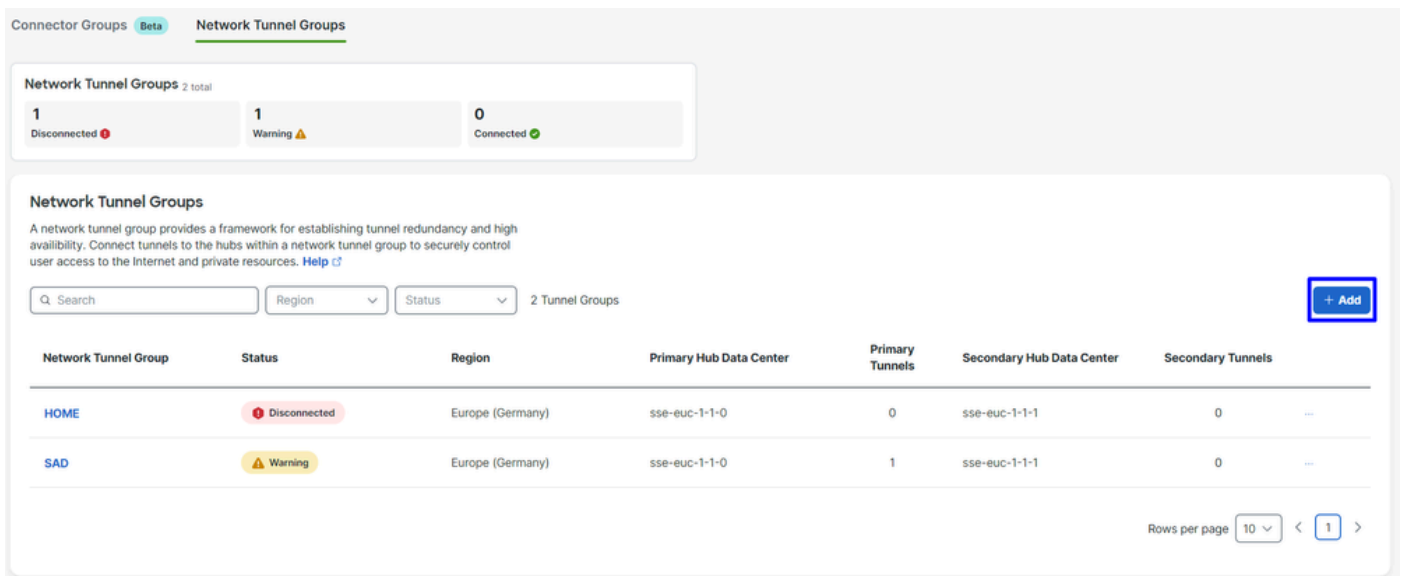
安全访问-主页

- 点击 Connect > Network Connections.



安全访问-网络连接

- 在Network Tunnel Groups下，单击+ Add。



安全访问-网络隧道组

- 配置Tunnel Group Name、Region和Device Type。
- 单击。Next

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

 ⊗

Region

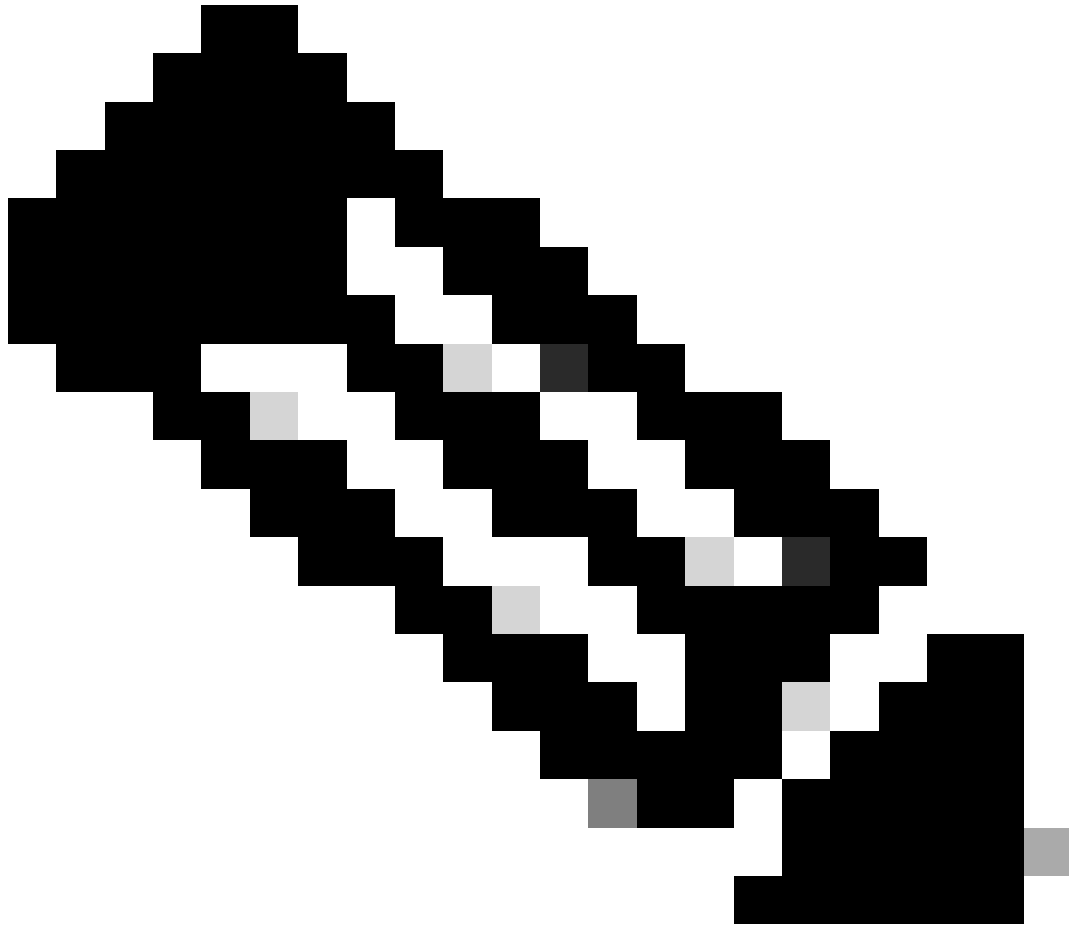
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



注意：选择距离防火墙位置最近的区域。

-
- 配置Tunnel ID Format和Passphrase。
 - 单击。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

安全访问-隧道组-隧道ID和密码

- 配置已在网络上配置并要通过安全访问传递流量的IP地址范围或主机。
- 单击。 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

安全访问-隧道组-路由选项

单击显示的Save 有关隧道的信息后，请保存该信息，以便执行下一步Configure the tunnel on Sophos。

隧道数据

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](#)

安全访问-隧道组-恢复配置

在Sophos上配置隧道

配置IPsec配置文件

要配置IPsec配置文件，请导航到您的Sophos XG防火墙。

您将获得类似以下内容：

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
Cloud applications
Allowed app categories Network attacks
Allowed web categories Blocked app categories

Security Heartbeat®
0 At risk Monitor endpoint health and systems at risk

Synchronized Application Control™
0 Apps Identify unknown apps on your network

Zero-day protection
0 Recent 0 Incidents 0 Scanned

ATP UTQ
0 Sources blocked 0 Accounts at risk

SSL/TLS connections
0% Of traffic 0% Decrypted 0 Failed

Active firewall rules
0 WAF 1 User 3 Network 4 Scanned

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...](#)

4 Unused 2 Disabled 0 Changed 0 New

Click on widgets to open details

Sophos - 管理面板

- 导航至 Profiles
- 点击 IPsec Profiles 并在之后点击Add

algorithm Manage

IPsec profiles **Device access**

Add **Delete**

Phase 2

在**General Settings** configure下：

- **Name**：思科安全访问策略的参考名称
- **Key Exchange**：IKEv2
- **Authentication Mode**：主模式
- **Key Negotiation Tries**:0
- **Re-Key connection**：选中选项

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

在**Phase 1** configure下：

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

Phase 1

Key life 28800 Seconds	Re-key margin 360 Seconds	Randomize re-keying margin by 50 %
DH group (key group) 2 selected		
Encryption AES256	Authentication SHA2 256	

+ You can add up to 3 different algorithm combinations

Sophos - IPsec配置文件-第1阶段

在Phase 2 configure下：

- PFS group (DH group) : 与I阶段相同
- **Key life**:3600
- **Encryption** : AES 256
- Authentication : SHA2 256

Phase 2

PFS group (DH group) Same as phase-1	Key life 3600 Seconds
Encryption AES256	Authentication SHA2 256

+ You can add up to 3 different algorithm combinations

Sophos - IPsec配置文件-第2阶段

在 Dead Peer Detection configure下：

- **Dead Peer Detection** : 选中选项
- **Check peer after every**:10
- **Wait for response up to**:120 (Default)
- **When peer unreachable** : 重新启动 (默认)

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

Dead Peer Detection

Check peer after every: 10 Seconds

Wait for response up to: 120 Seconds

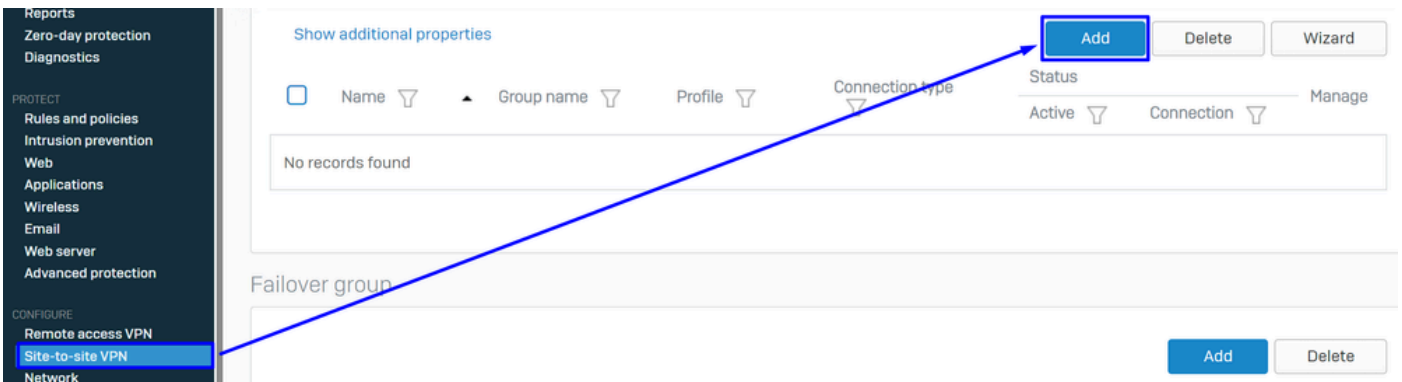
When peer unreachable: Re-initiate

Sophos - IPsec配置文件-失效对等体检测

之后，单击 **Save** and proceed with the next step, Configure Site-to-site VPN。

配置站点到站点VPN

要启动VPN配置，请点击**Site-to-site VPN**，然后点击 **Add**。

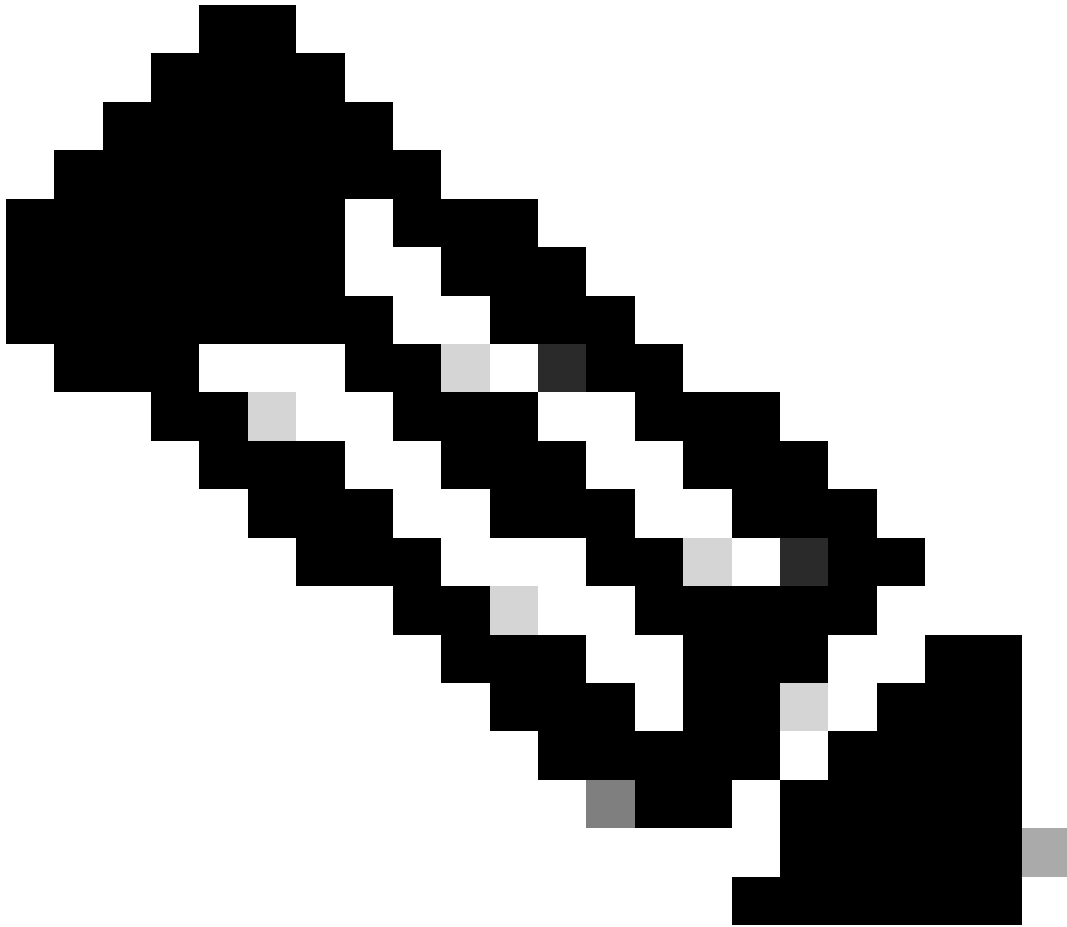


Sophos - 站点到站点VPN

在**General Settings** configure下：

- **Name**：思科安全访问IPsec策略的参考名称
- IP version：IPv4
- Connection type:通道接口
- Gateway type：启动连接

- Active on save : 选中选项
-



注意：在您最终配置站点到站点VPN后，该选项会自动启Active on save 用VPN。

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 - 站点到站点VPN - 常规设置

注意：选项Tunnel interface为名为XFRM的Sophos XG防火墙创建虚拟隧道接口。

在Encryption configure下：

- **Profile**：您在步骤中创建的配置文件， **Configure IPsec Profile**
- **Authentication type**:预共享密钥
- **Preshared key**：在步骤中配置的密钥， [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key**：Preshared key

Encryption

Profile CSA	Authentication type Preshared key
	Preshared key
	Repeat preshared key

Sophos - 站点到站点VPN - 加密

在**Gateway Settings** configure Local Gateway和Remote Gateway options下，使用此表作为参考。

本地网关	远程网关
侦听接口 您的Wan-Internet接口	网关地址 在步骤中生成的公共IP， Tunnel Data
本地ID类型 发送邮件	远程ID类型 IP 地址

本地ID 步骤下生成的邮件， Tunnel Data	远程ID 在步骤中生成的公共IP， Tunnel Data
本地子网 any	远程子网 any

Gateway settings

Local gateway	Remote gateway
Listening interface PortB - 192.168.0.33	Gateway address 18.156.145.74
Local ID type Email	Remote ID type IP address
Local ID csasophos@ -sse.cisco.com	Remote ID 18.156.145.74
Local subnet Any	Remote subnet Any
Add new item	Add new item

Sophos - 站点到站点VPN - 网关设置

之后单击Save按钮，您可以看到隧道已创建。

IPsec connections

Show additional properties

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

Sophos - 站点到站点VPN - IPsec连接



注：要检查隧道是否已在上一个映像上正确启用，您可以检查**Connection** 状态；如果它是绿色的，则表示隧道已连接；如果它不是绿色的，则表示隧道未连接。

要检查是否建立了隧道，请导航到 **Current Activities > IPsec Connections**。

MONITOR & ANALYZE

Control center


Current activities

Reports

Zero-day protection

Diagnostics

Sophos - 监控和分析- 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 - 监控和分析- IPsec前后

之后，我们可以继续执行 **Configure Tunnel Interface Gateway** 步骤。

配置隧道接口

导航到 **Network** 并检查VPN上配置的接口WAN，以编辑名称为xfrm的虚拟隧道接口。

- 单击接xfrm 口。



Sophos -网络-隧道接口

- 在网络中配置不可路由的IP接口，例如，您可以使用169.254.x.x/30，它通常是不可路由空间中的IP，在我们的示例中，我们使用169.254.0.1/30

General settings

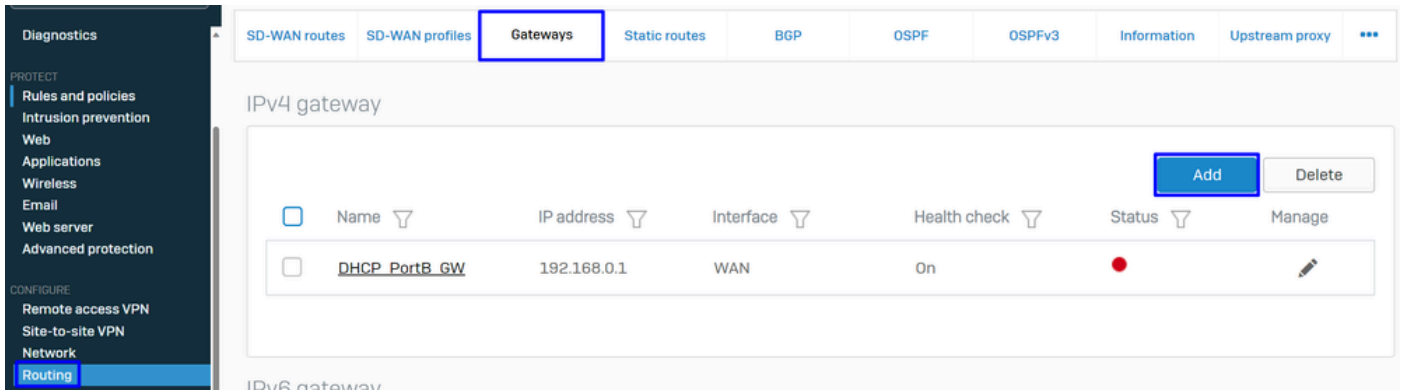
Name *	<input type="text" value="xfrm1"/>
Hardware	xfrm1
IPsec connection	SecureAccessS
Network zone	VPN
<input checked="" type="checkbox"/> IPv4 configuration	
IPv4/netmask *	<input type="text" value="169.254.0.1"/> <input type="text" value="/30 (255.255.255.252)"/>

Sophos -网络-隧道接口-配置

配置网关

为虚拟接口配置网关(xfrm)

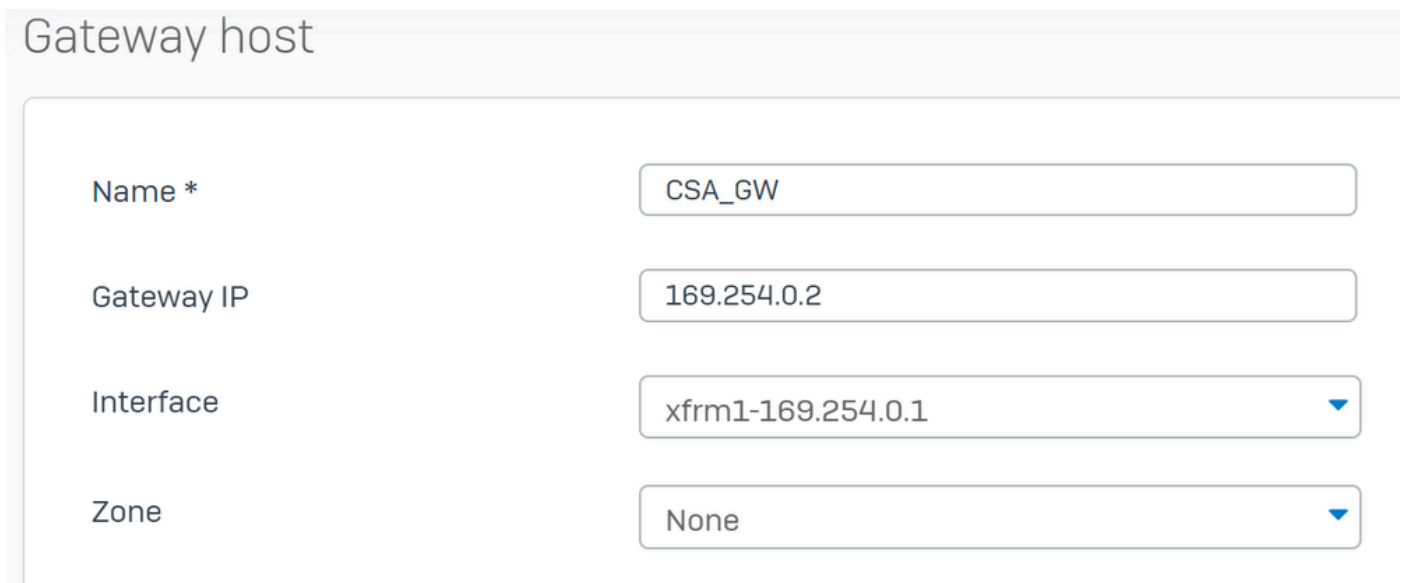
- 导航至 Routing > Gateways
- 点击 Add



Sophos -路由-网关

在Gateway host configure下：

- **Name**：引用为VPN创建的虚拟接口的名称
- **Gateway IP**：在本例中，169.254.0.2是我们在步骤中已分配的网络169.254.0.1/30下的IP，Configure Tunnel Interface
- **Interface**：VPN虚拟接口
- **Zone**：无（默认）



Sophos -路由-网关-网关主机

- 在Health check 禁用检查下
- 点击 Save

Health check

Health check



Sophos -路由-网关-运行状况检查

保存配置后，您可以观察网关的状态：

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		

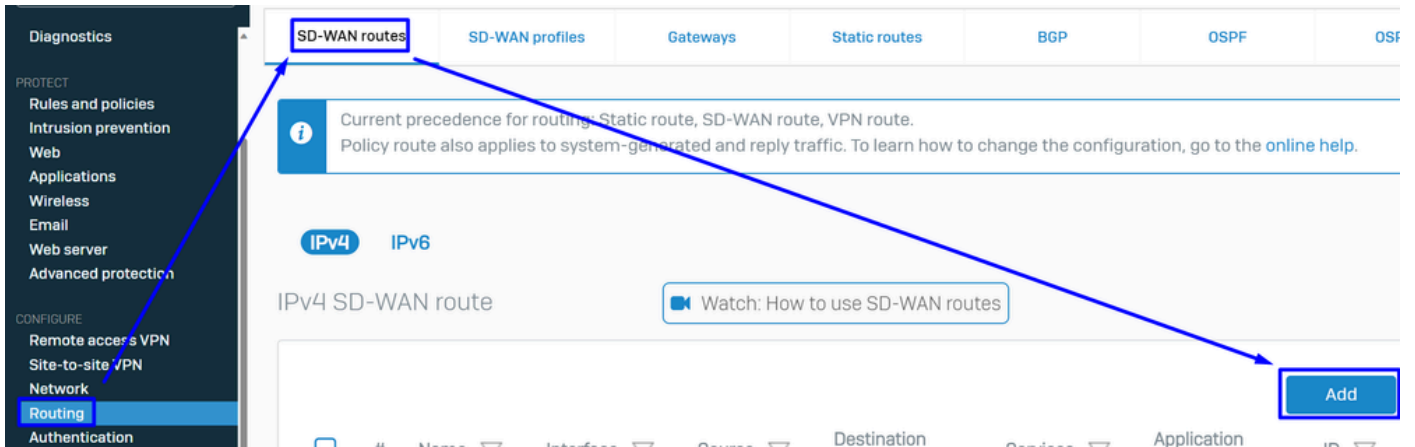
Sophos -路由-网关-状态

配置SD-WAN路由

要完成配置过程，您需要创建允许您将流量转发到安全访问的路由。

导航至 **Routing > SD-WAN routes**.

- 点击 **Add**



Sophos - SD-Wan路由

在Traffic Selector configure下：

- Incoming interface：选择要从中发送流量的接口或从RA-VPN、ZTNA或无客户端ZTNA访问的用户
- DSCP marking：此示例没有任何内容
- **Source networks**：选择要通过隧道路由的地址
- **Destination networks**：任意，或者您可以指定目标
- **Services**：任意，或者您可以指定服务
- **Application object**：如果已配置对象，则为应用程序
- User or groups：如果要添加特定用户组以将流量路由到安全访问

Traffic selector

Incoming interface <input type="text" value="LAN-192.168.0.203"/>	DSCP marking <input type="text" value="Select DSCP marking"/>	
Source networks <input type="text" value="Any"/> <input type="button" value="Add new item"/>	Destination networks <input type="text" value="Any"/> <input type="button" value="Add new item"/>	Services <input type="text" value="Any"/> <input type="button" value="Add new item"/>
Application object <input type="text" value="Any"/> <input type="button" value="Add new item"/>	User or groups <input type="text" value="Any"/> <input type="button" value="Add new item"/>	

Sophos - SD-Wan路由-流量选择器

在Link selection settings 配置网关下：

- Primary and Backup gateways：选中选项

- **Primary gateway** : 选择在步骤中配置的网关 , [Configure the Gateways](#)
- 点击 **Save**

Link selection settings

Select SD-WAN profile ⓘ Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

Sophos - SD-Wan路由-流量选择器-主网关和备份网关

完成Sophos XG防火墙的配置后，您可以继续执行此步骤。 **Configure Private App.**

配置专用应用

要配置专用应用访问，请登录到[管理员门户](#)。

- 导航至 **Resources > Private Resources**

安全访问-私有资源

- 点击 + Add

安全访问-私有资源2

- 在General 配置下， Private Resource Name

General

Private Resource Name

SplunkSophos

Description (optional)

安全访问-私有资源-常规

在Communication with Secure Access Cloud configure下：

- Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)：选择要访问的资源



注意：请记住，内部可到达地址是在步骤 [Configure the Tunnel on Secure Access](#) 中分配的。

-
- **Protocol**：选择用于访问该资源的协议
 - **Port / Ranges**：选择需要启用以访问应用的端口

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

安全访问-私有资源-通过安全访问云进行通信

在 **Endpoint Connection Methods** ，您可以配置通过安全访问访问私有资源的所有可能方式，并选择您想要用于您的环境的方法：

- **Zero-trust connections** ：选中此复选框可启用ZTNA访问。
 - **Client-based connection** ：启用该按钮以允许客户端基本ZTNA
 - **Remotely Reachable Address** ：配置专用应用的IP
 - **Browser-based connection** ：启用该按钮以允许基于浏览器的ZTNA
 - **Public URL for this resource** ：添加要与域ztna.sse.cisco.com结合使用的名称
 - **Protocol** ：选择HTTP或HTTPS作为通过浏览器访问的协议
- **VPN connections** ：选中此复选框可启用RA-VPN访问。
- 点击 **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

安全访问-私有资源-通过安全访问云进行通信2

配置完成后，结果如下：

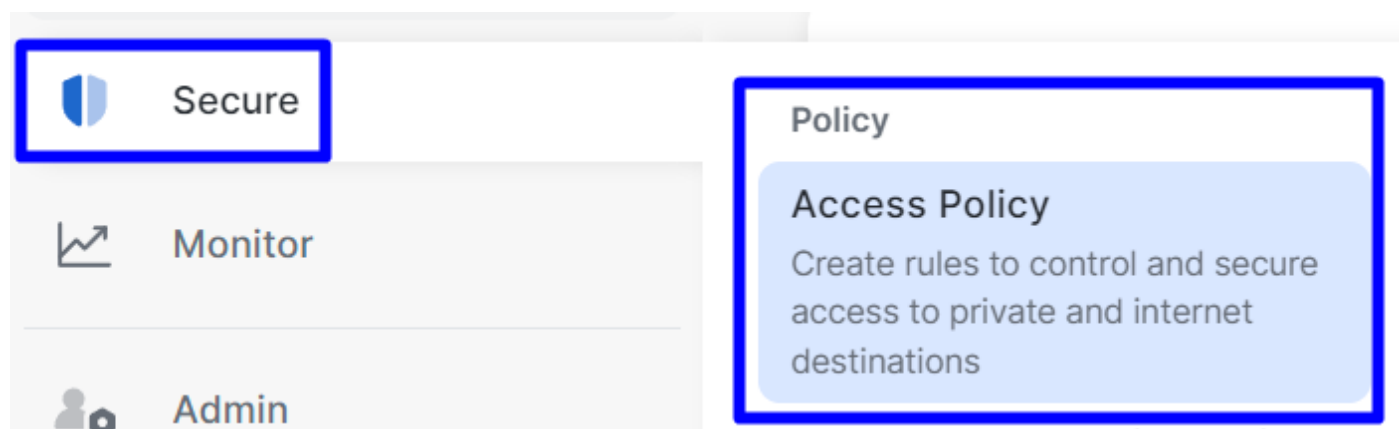
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none">VPNBrowser-based ZTNAClient-based ZTNA	1	2	16

安全访问-已配置私有资源

现在您可以继续执行 **Configure the Access Policy** 步骤。

配置访问策略

要配置访问策略，请导航到 **Secure > Access Policy**。



安全访问-访问策略

- 点击 **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

安全访问-访问策略-专用访问

配置以下选项，以通过多种身份验证方法提供访问权限：

- 1. Specify Access
 - Action:允许
 - **Rule name**：指定访问规则的名称
 - **From**：您授予访问权限的用户
 - **To**：您要允许访问的应用
 - **Endpoint Requirements**：（默认值）
- 点击 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**

安全访问-访问策略-指定访问

注意： 2. Configure Security 对于所需的步骤，但在本例中，您未启用 Intrusion Prevention (IPS)或 Tenant Control Profile。

- 单击Save，您可以：

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

安全访问-已配置访问策略

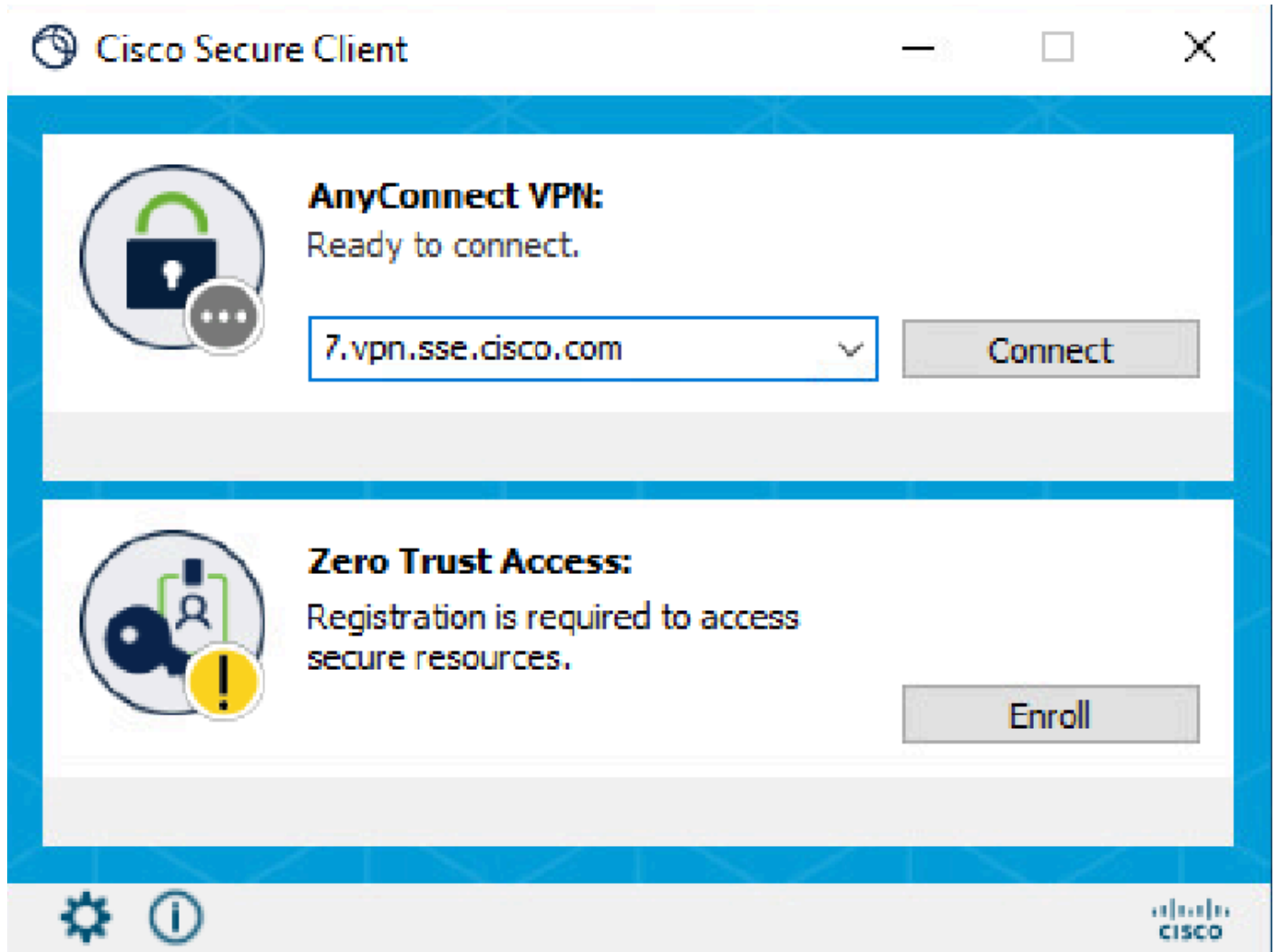
之后，您可以继续执行步骤Verify。

验证

要验证访问，必须已安装可以从[软件下载- Cisco安全客户端](#)下载的Cisco安全客户端代理。

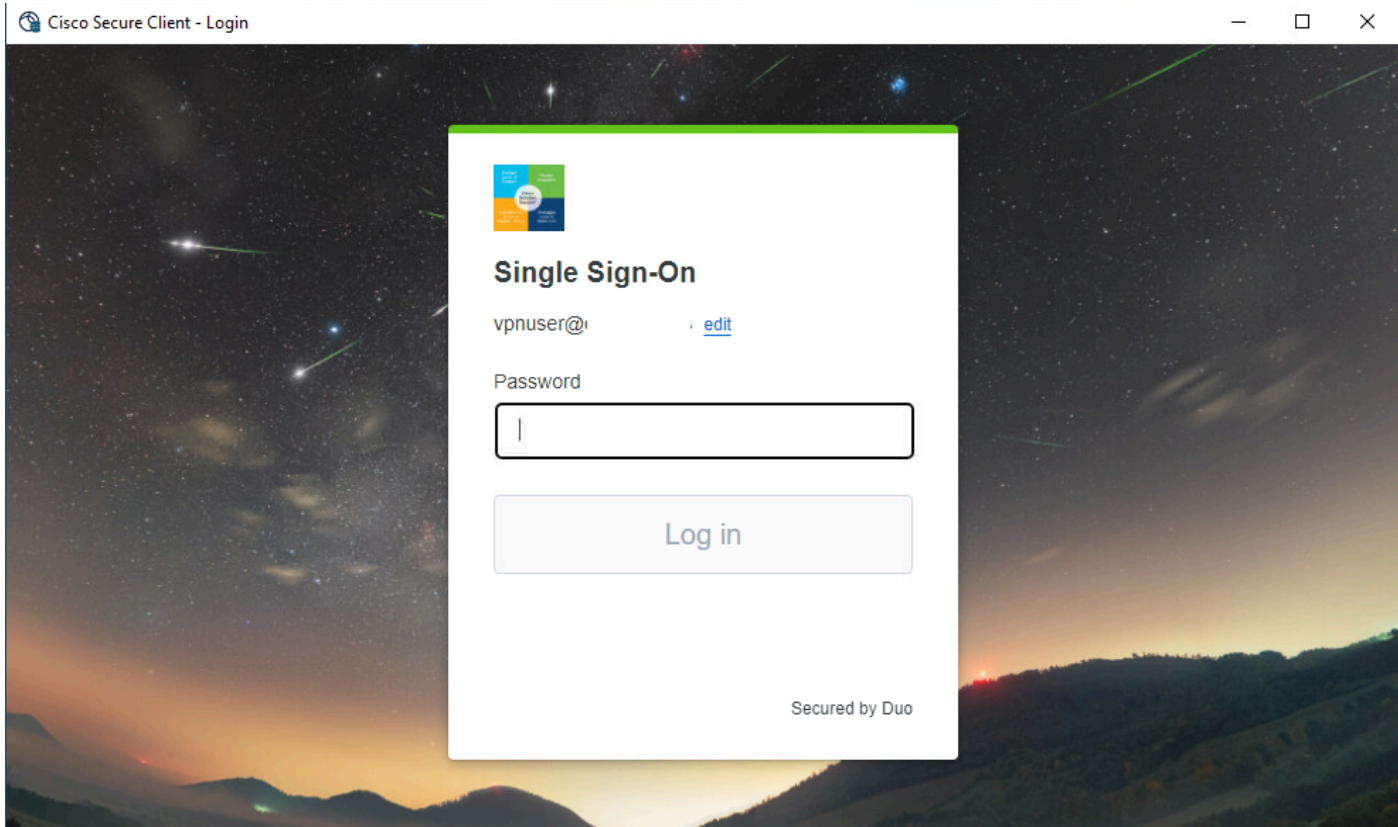
RA-VPN

通过Cisco Secure Client Agent-VPN登录。



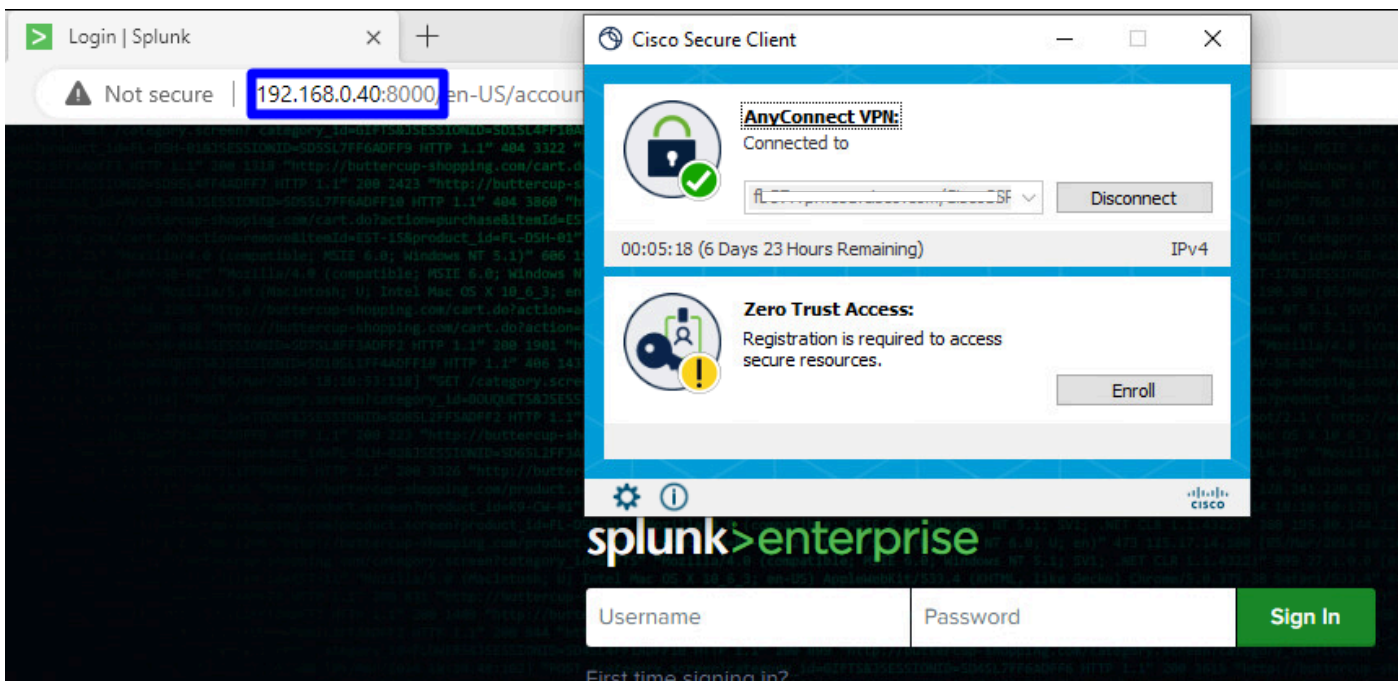
安全客户端- VPN

- 通过您的SSO提供程序进行身份验证



安全访问-VPN-SSO

- 在经过身份验证后，请访问以下资源：



安全访问-VPN-身份验证

导航至：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

安全访问-活动搜索- RA-VPN

您可以看到，允许用户通过RA-VPN进行身份验证。

基于客户端的ZTNA

通过Cisco安全客户端代理- ZTNA登录。

```

Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Users\falas>ipconfig

Windows IP Configuration

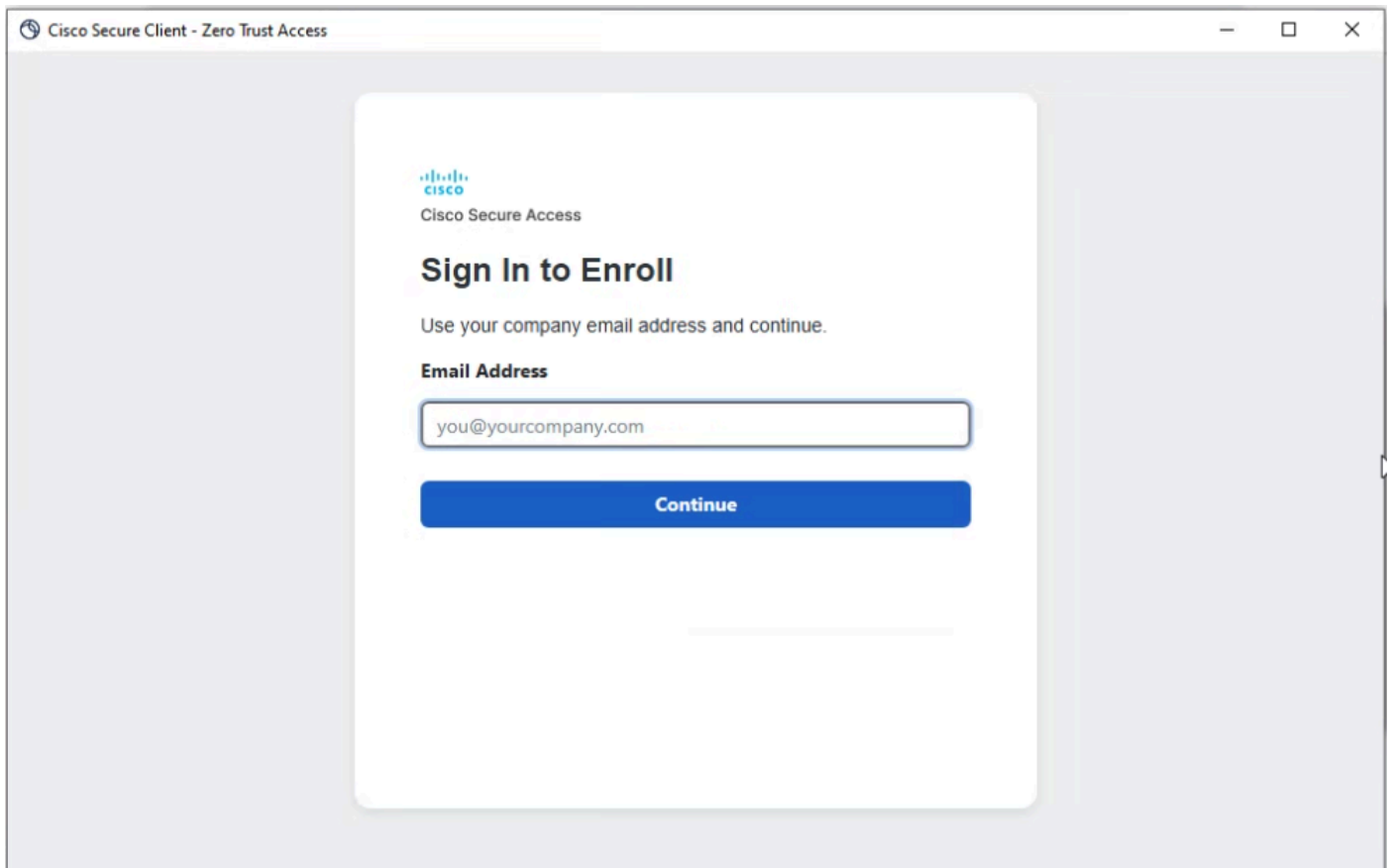
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3c3b:a6aa:6cc9:c1c6%15
    IPv4 Address. . . . . : 10.10.10.120
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1

C:\Users\falas>
  
```

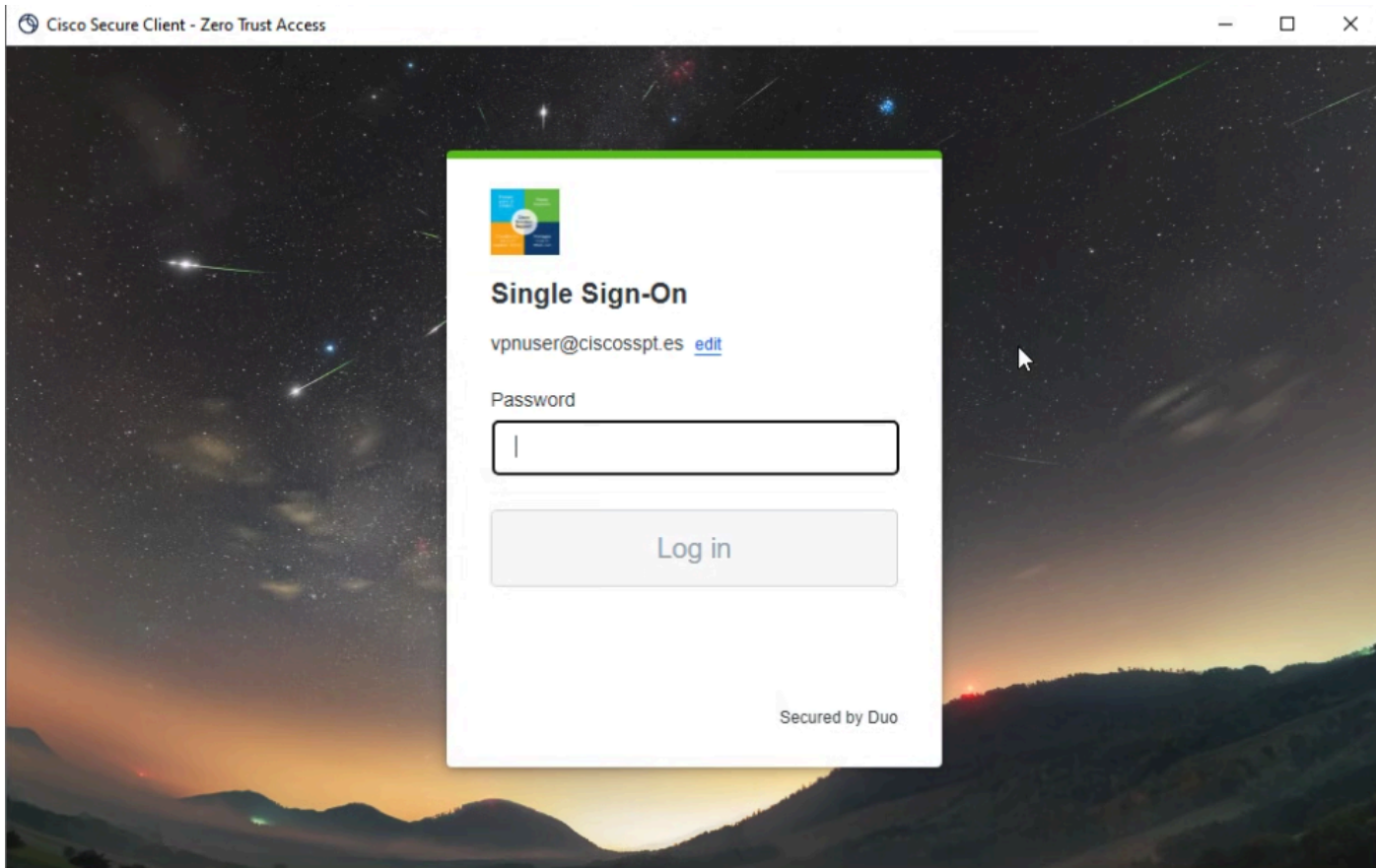
安全客户端- ZTNA

- 使用您的用户名注册。



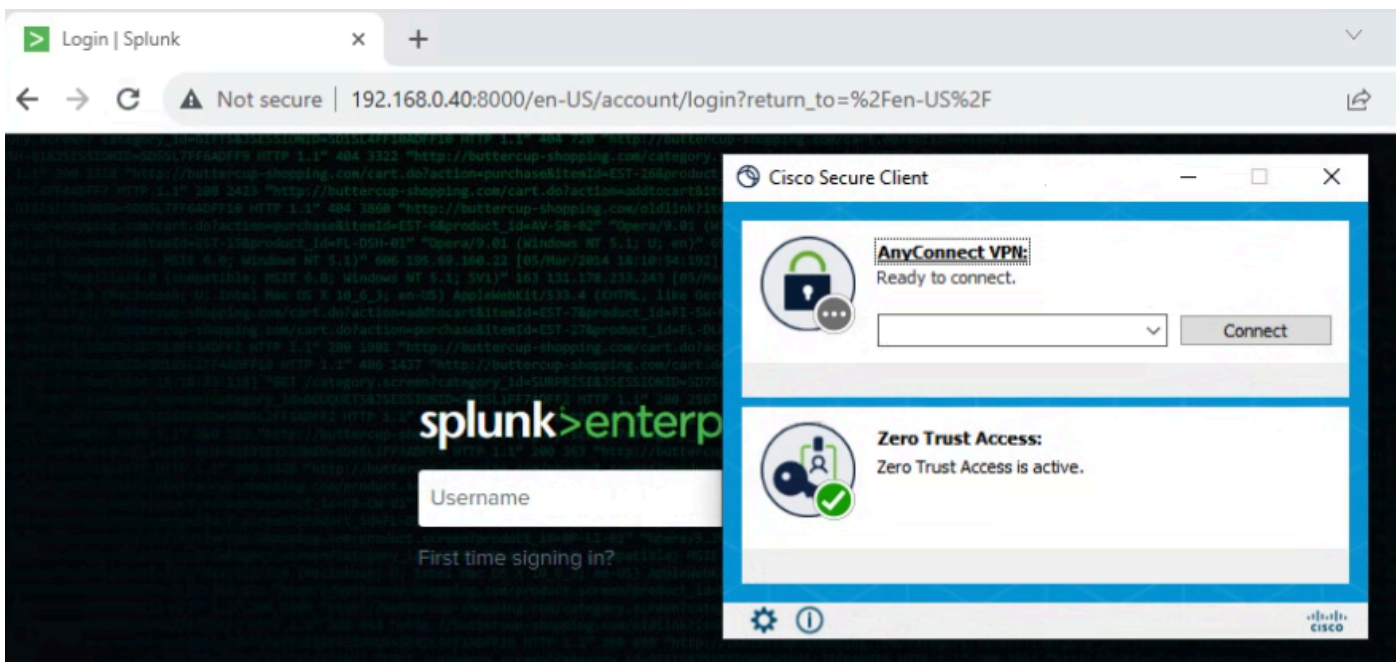
安全客户端- ZTNA -注册

- 在SSO提供程序中进行身份验证



安全客户端- ZTNA - SSO登录

- 在经过身份验证后，请访问以下资源：



安全访问- ZTNA -已记录

导航至：Monitor > Activity Search

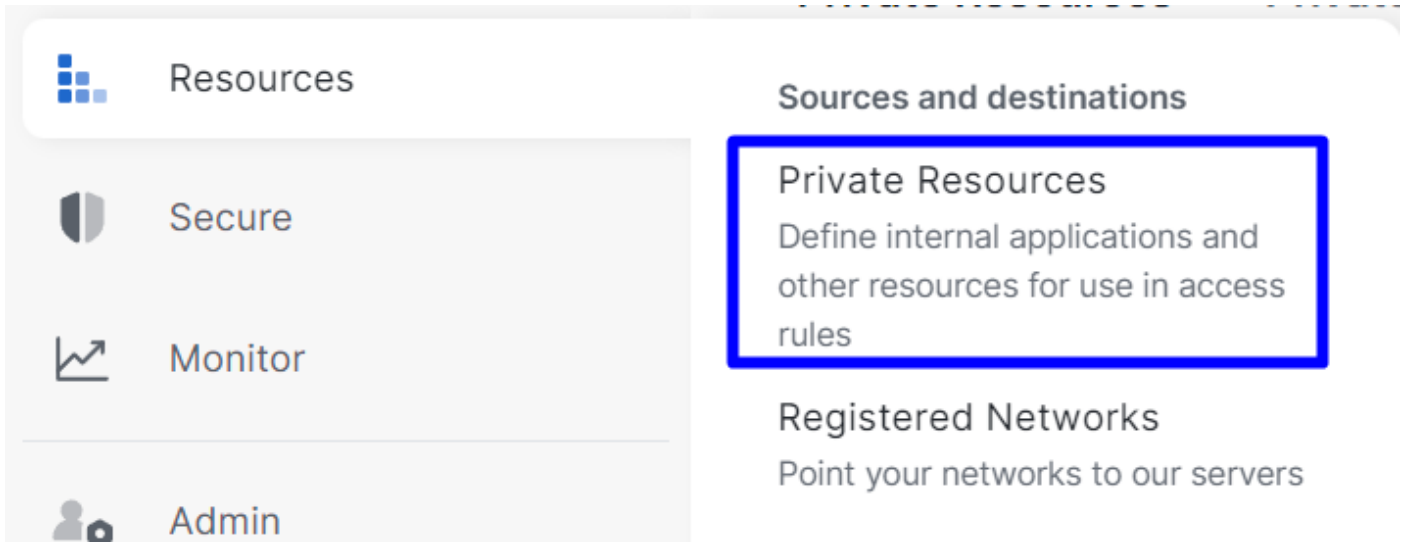
FW	vpn user (vpnuser@ciscosspt.es)	Action	Allowed
FW	vpn user (vpnuser@ciscosspt.es)	Time	Nov 23, 2023 1:27 AM
FW	vpn user (vpnuser@ciscosspt.es)	Rule Name	Splunksophos
FW	vpn user (vpnuser@ciscosspt.es)	Identity	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)	Policy or Ruleset Identity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

安全访问-活动搜索-基于ZTNA客户端

您可以看到用户能够通过基于客户端的ZTNA进行身份验证。

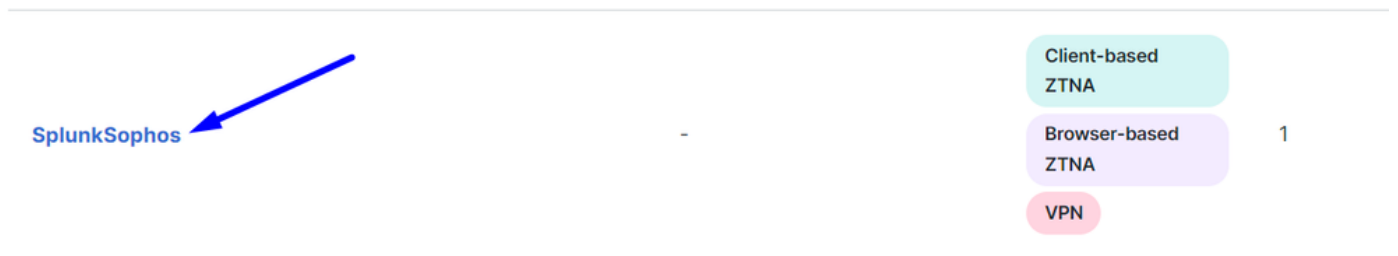
基于浏览器的ZTNA

要获取URL，您需要转到Resources > Private Resources。



安全访问-私有资源

- 单击您的策略



安全访问-私有资源- SplunkSophos

- 下滚

SplunkSophos

Client-based ZTNA

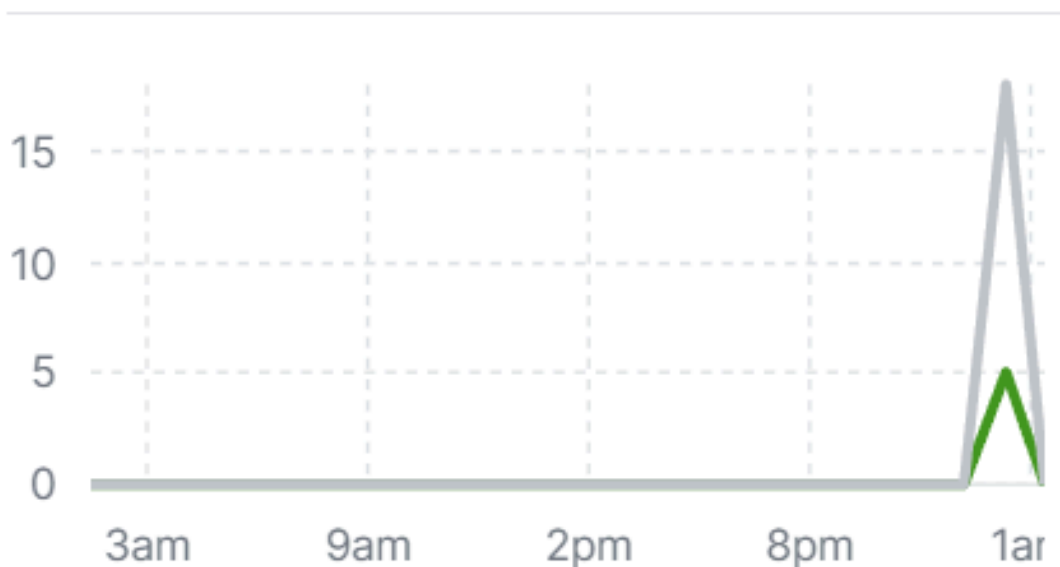
Browser-based ZTNA



VPN

Total Requests

23 ↗ 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status

✓	Success	5
⊘	Blocked	18

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。