Configure Secure Access with Sophos XG Firewall

Contents

Introduction

This document describes how to configure Secure Access with Sophos XG Firewall.

Prerequisites

- Configure User Provisioning
- ZTNA SSO Authentication Configuration
- Configure Remote Access VPN Secure Access

Requirements

Cisco recommends that you have knowledge of these topics:

- Sophos XG Firewall
- Secure Access
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless ZTNA

Components Used

The information in this document is based on:

- Sophos XG Firewall
- Secure Access
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

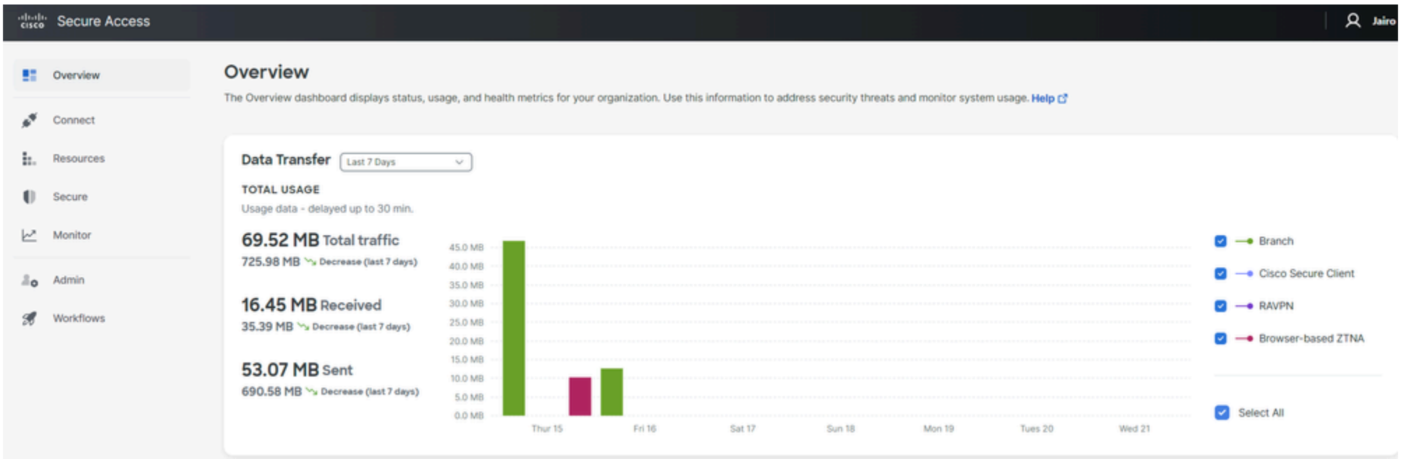
Secure Access - Sophos

Cisco has designed Secure Access to ensure the protection and provision of access to private applications, both on-premise and cloud-based. It also safeguards the connection from the network to the internet. This is achieved through the implementation of multiple security methods and layers, all aimed at preserving the information as they access it via the cloud.

Configure

Configure the Tunnel on Secure Access

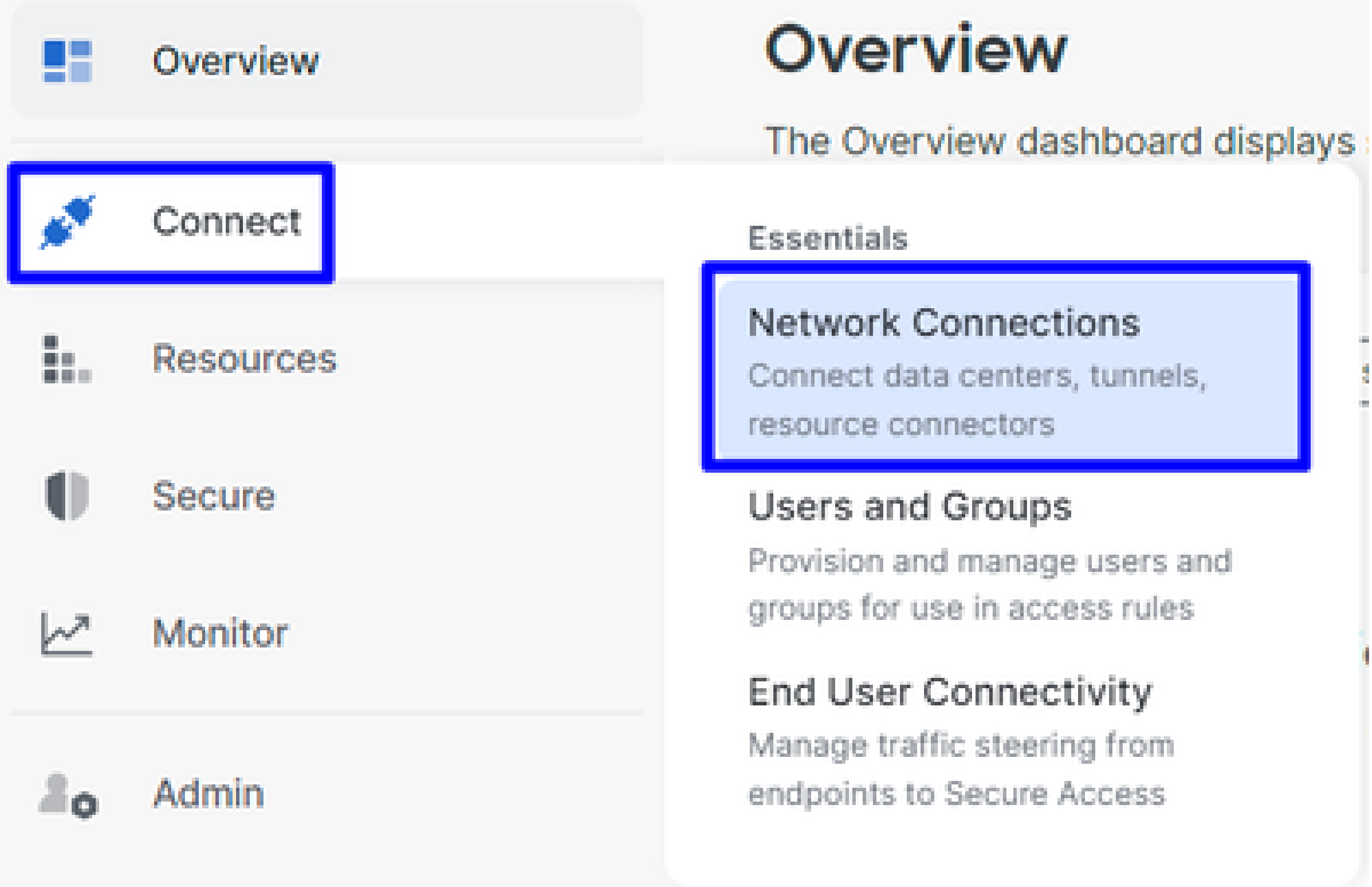
Navigate to the admin panel of Secure Access.



The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

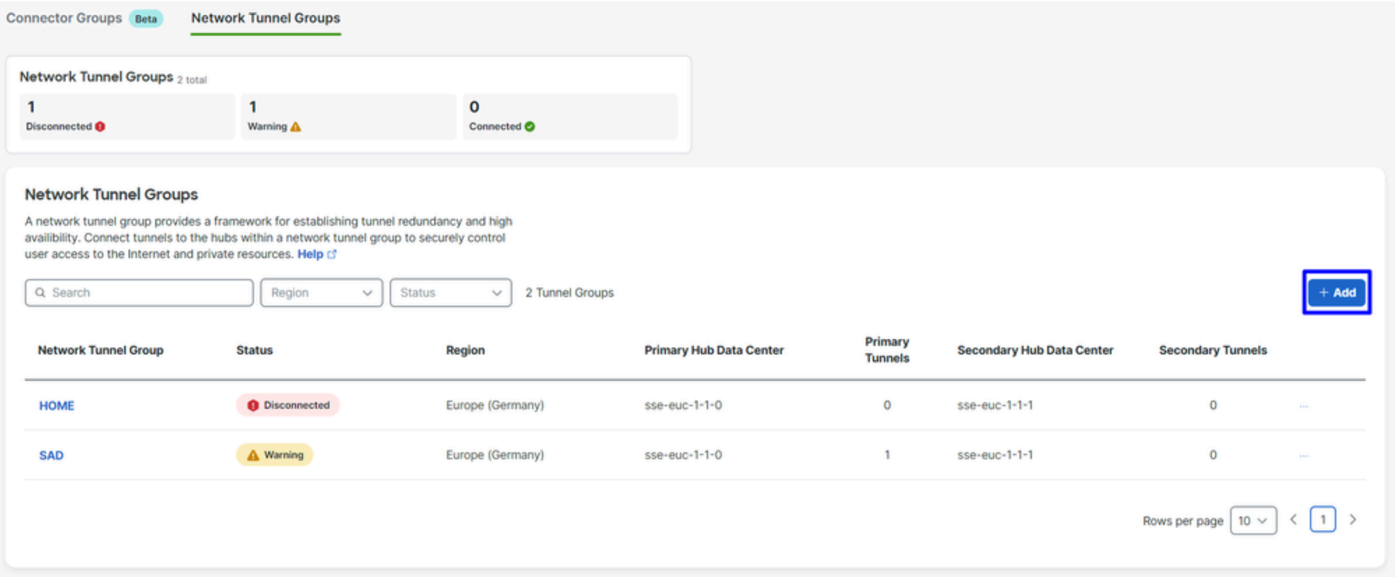
Secure Access - Main Page

- Click on Connect > Network Connections.


Overview
Connect
Resources
Secure
Monitor
Admin
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

Secure Access - Network Connections

- Under Network Tunnel Groups click on + Add.



Network Tunnel Groups 2 total

1 Disconnected | 1 Warning | 0 Connected

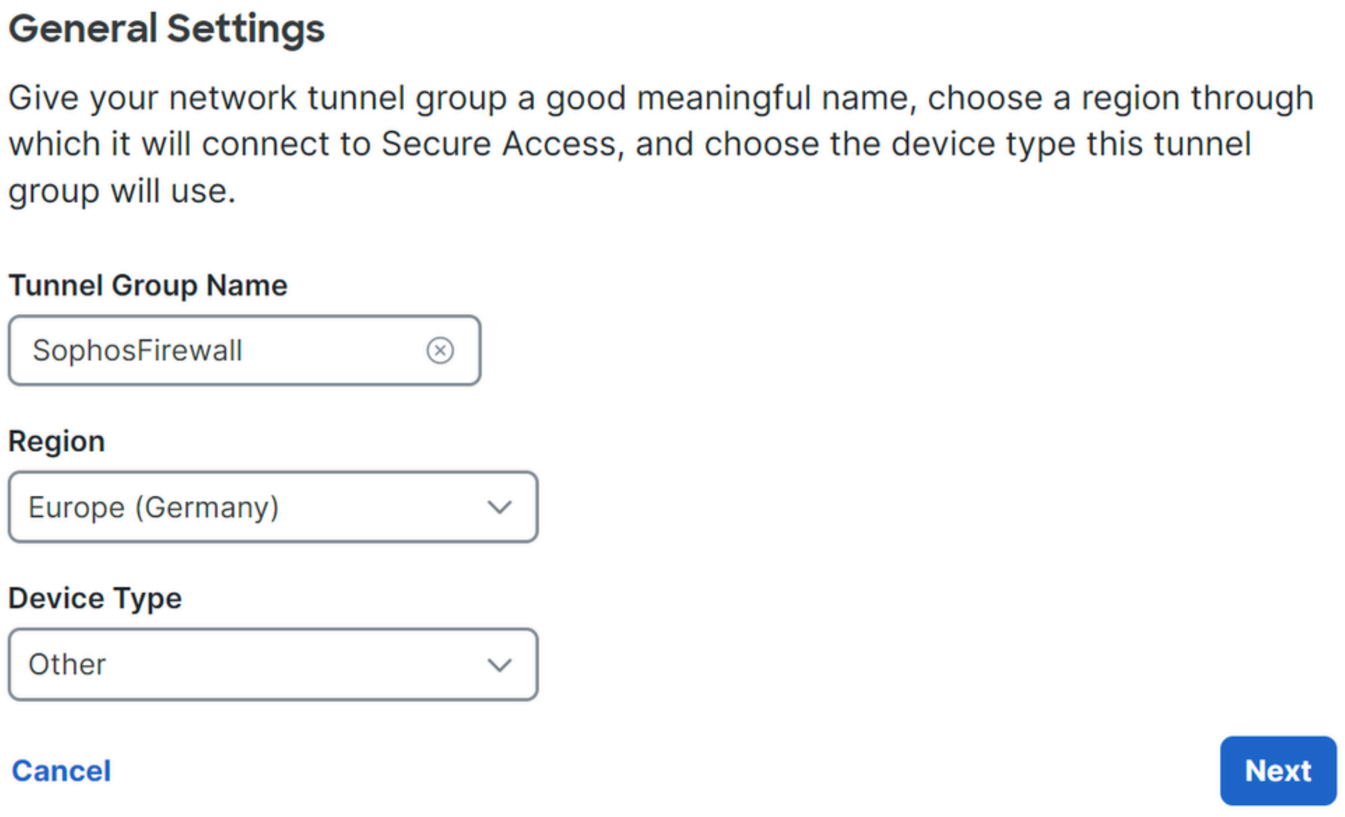
Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availibility. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. Help

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

Secure Access - Network Tunnel Groups

- Configure Tunnel Group Name, Region and Device Type.
- Click **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: SophosFirewall

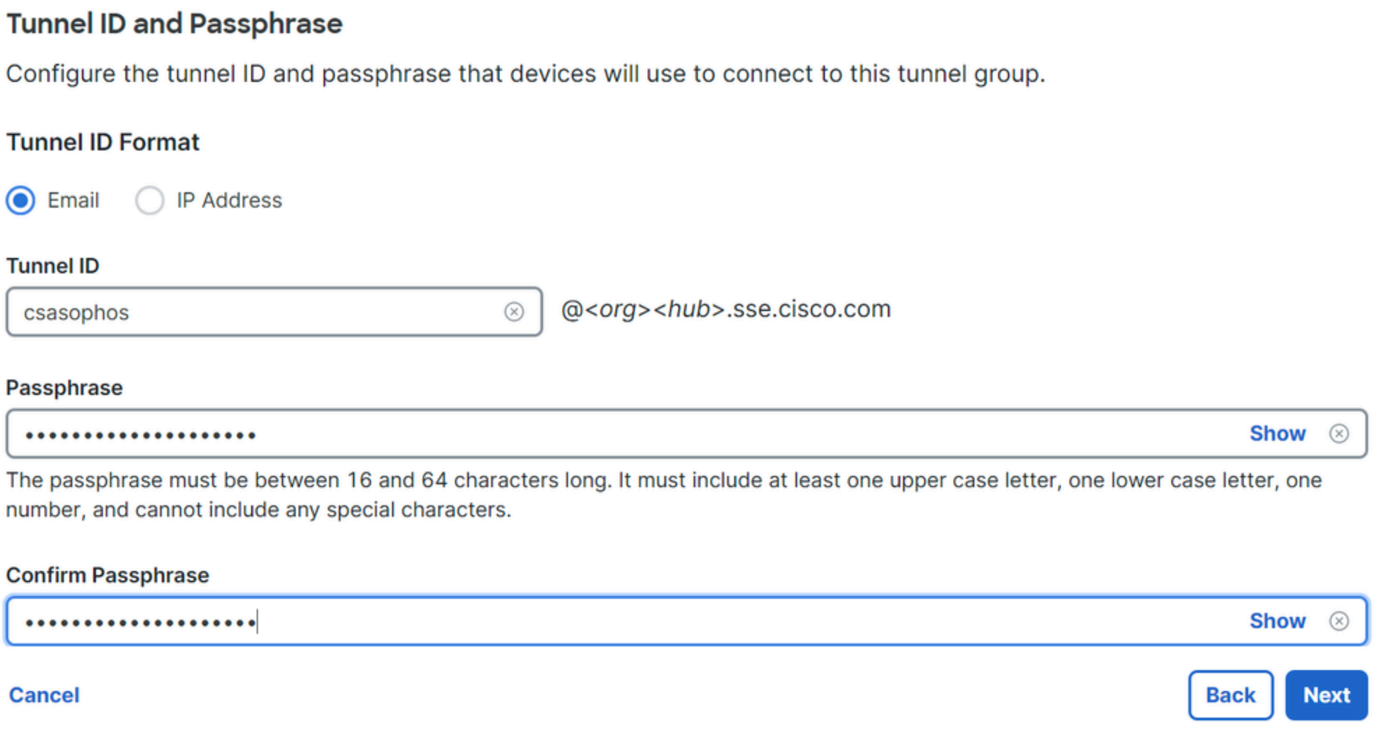
Region: Europe (Germany)

Device Type: Other

Secure Access - Tunnel Groups - General Settings

Note: Choose the region nearest to the location of your firewall.

- Configure the Tunnel ID Format and Passphrase.
- Click 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

••••••••••••••••••••

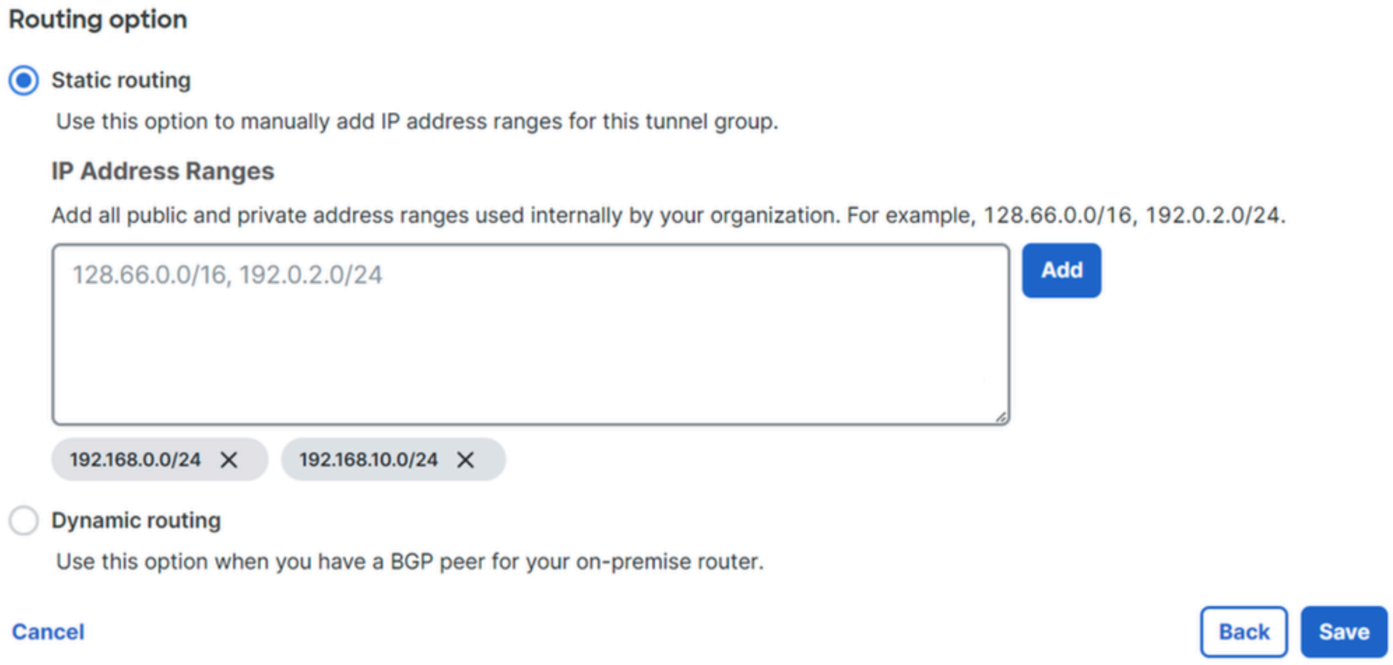
The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

••••••••••••••••••••

Secure Access - Tunnel Groups - Tunnel ID and Passphrase

- Configure the IP address ranges or hosts that you have configured on your network and want to pass the traffic through Secure Access.
- Click **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

192.168.0.0/24 ✕ 192.168.10.0/24 ✕

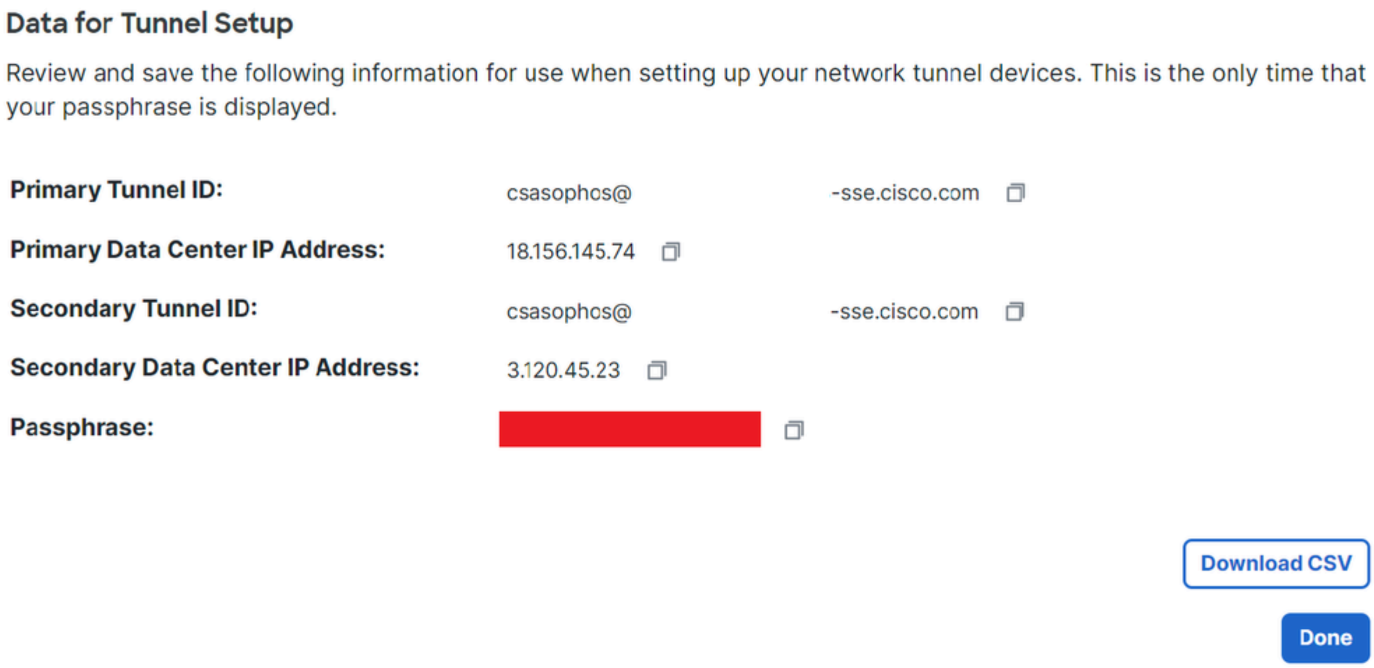
○ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Secure Access - Tunnel Groups - Routing Options

After you click on **Save** the information about the tunnel gets displayed, please save that information for the next step, **Configure the tunnel on Sophos.**

Tunnel Data



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:	csasophos@ -sse.cisco.com
Primary Data Center IP Address:	18.156.145.74
Secondary Tunnel ID:	csasophos@ -sse.cisco.com
Secondary Data Center IP Address:	3.120.45.23
Passphrase:	[redacted]

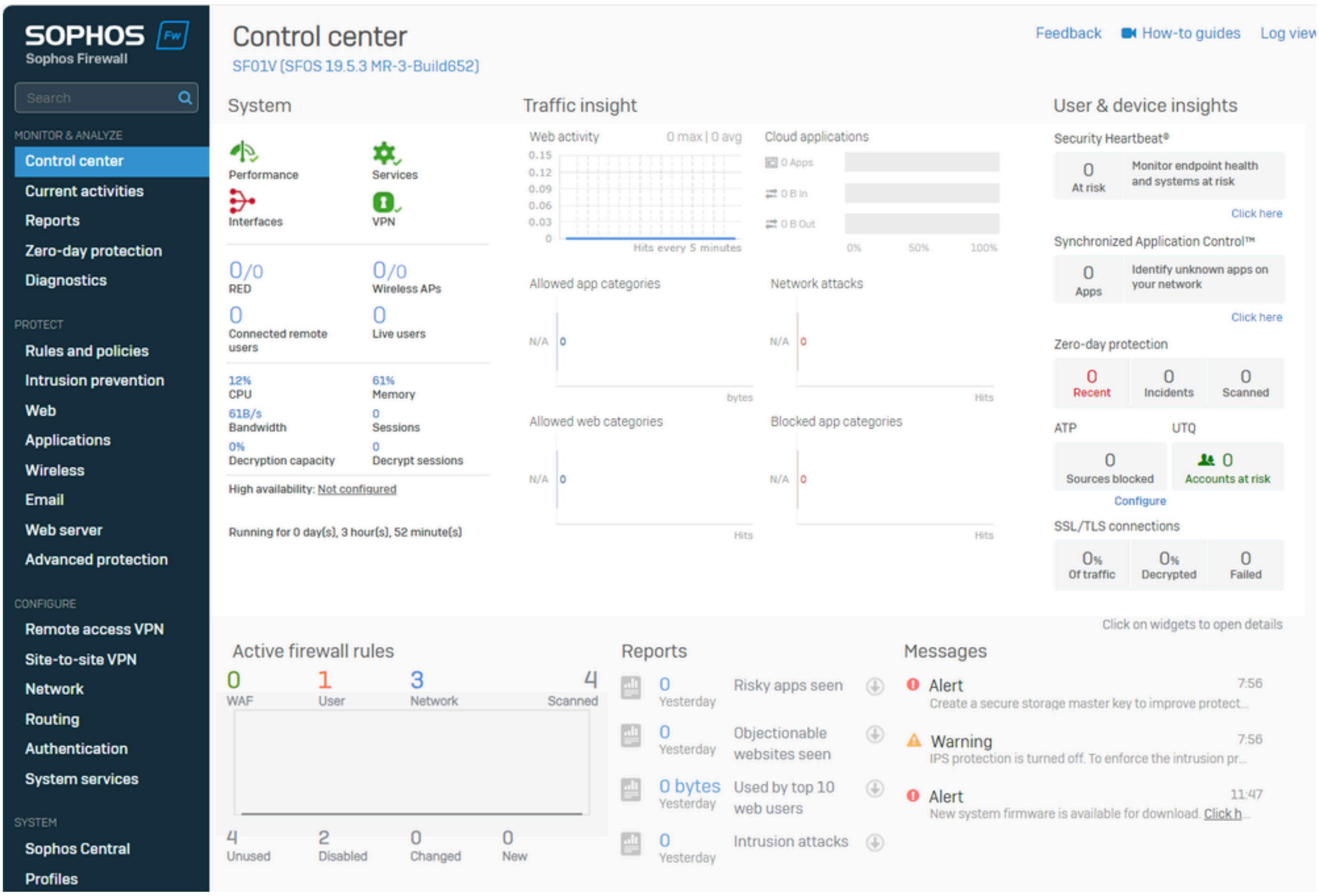
Secure Access - Tunnel Groups - Resume of configuration

Configure the Tunnel on Sophos

Configure IPsec Profile

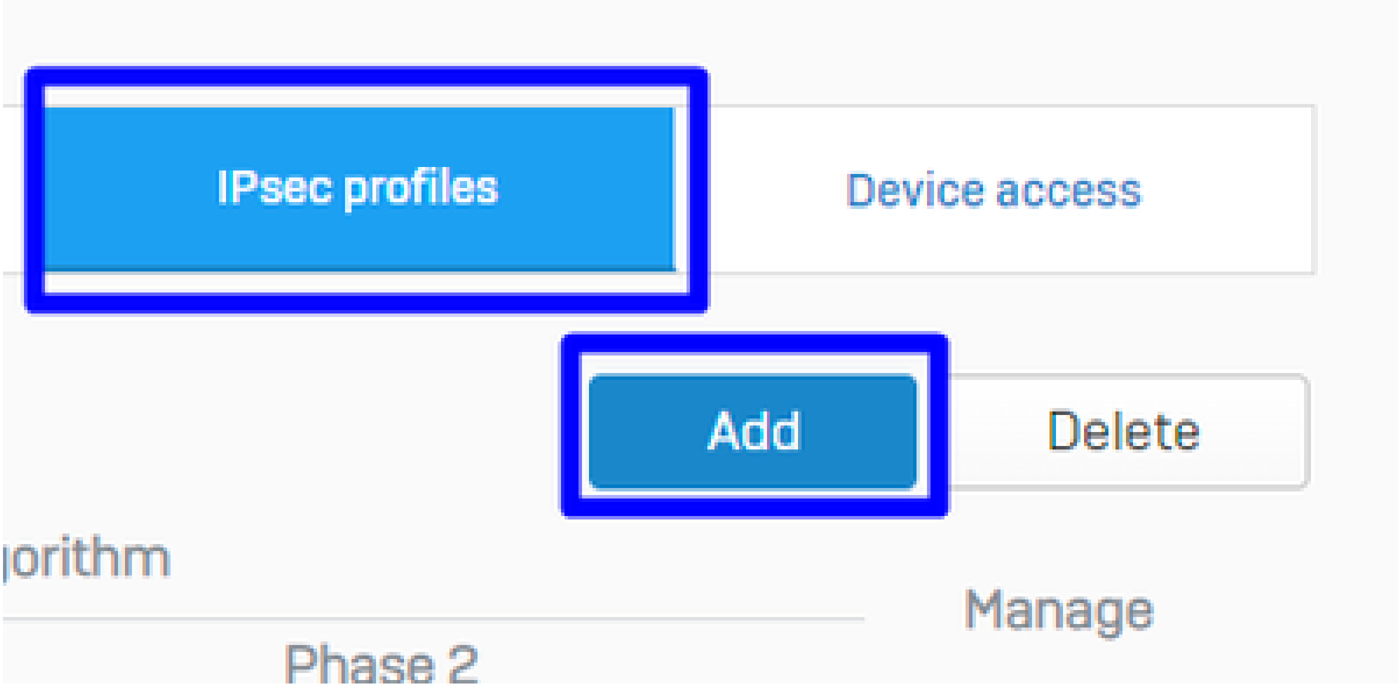
In order to configure the IPsec Profile, navigate to your Sophos XG Firewall.

You obtain something similar to this:



Sophos - Admin Panel

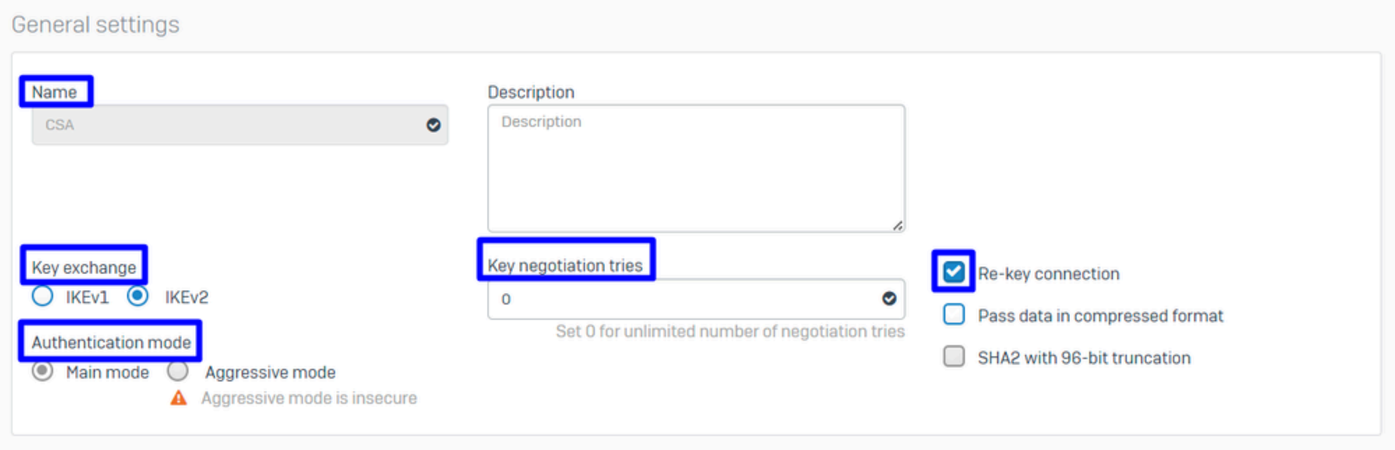
- Navigate to Profiles
- Click on **IPsec Profiles** and after that click onAdd



Sophos - IPsec Profiles

Under **General Settings** configure:

- **Name**: A reference name to the Cisco Secure Access Policy
- **Key Exchange**: IKEv2
- **Authentication Mode**: Main Mode
- **Key Negotiation Tries**: 0
- **Re-Key connection**: Check the option



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

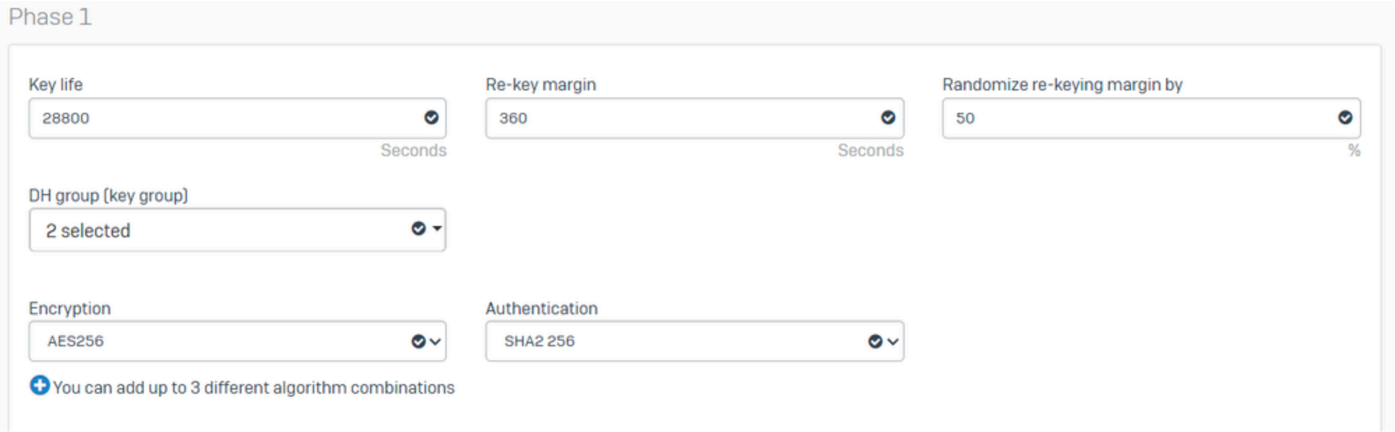
□ Pass data in compressed format

□ SHA2 with 96-bit truncation

Sophos - IPsec Profiles - General Settings

Under **Phase 1** configure:

- **Key Life**: 28800
- **DH group(key group)**: Select 19 and 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

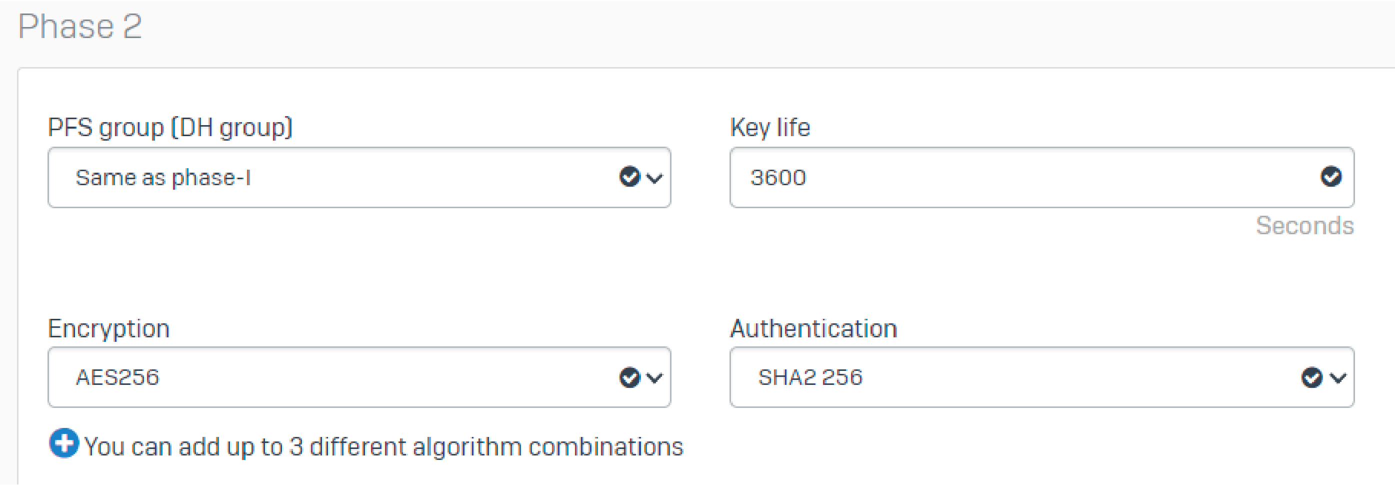
Authentication: SHA2 256

You can add up to 3 different algorithm combinations

Sophos - IPsec Profiles - Phase 1

Under **Phase 2** configure:

- PFS group (DH group): Same as phase-I
- **Key life**: 3600
- **Encryption**: AES 256
- Authentication: SHA2 256



Phase 2

PFS group (DH group): Same as phase-I

Key life: 3600 Seconds

Encryption: AES256

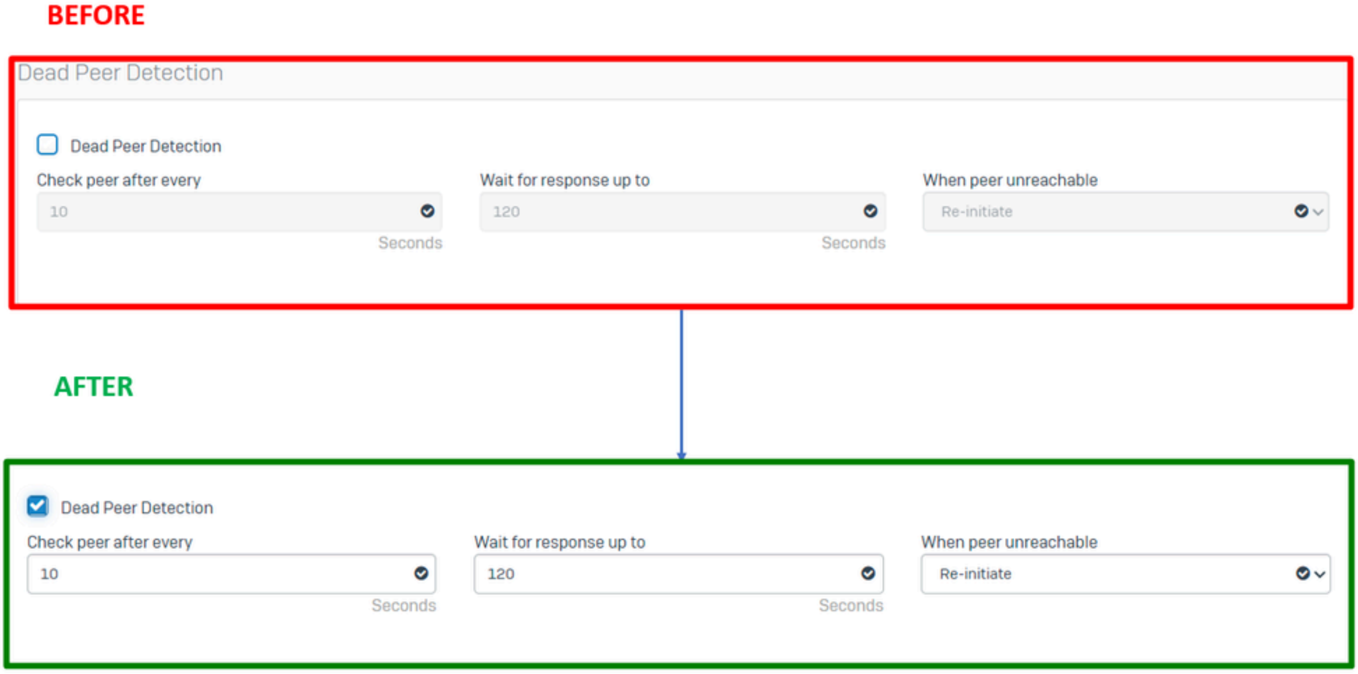
Authentication: SHA2 256

You can add up to 3 different algorithm combinations

Sophos - IPsec Profiles - Phase 2

Under **Dead Peer Detection** configure:

- **Dead Peer Detection**: Check the option
- **Check peer after every**: 10
- **Wait for response up to**: 120 (Default)
- **When peer unreachable**: Re-initiate (Default)



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

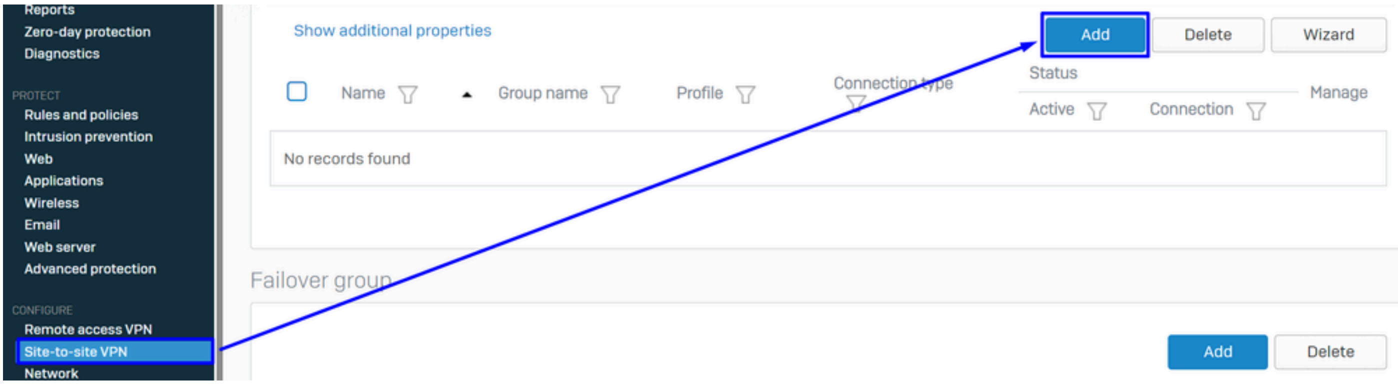
When peer unreachable: Re-initiate

Sophos - IPsec Profiles - Dead Peer Detection

After that click on **Save** and proceed with the next step, Configure Site-to-site VPN.

Configure Site-to-site VPN

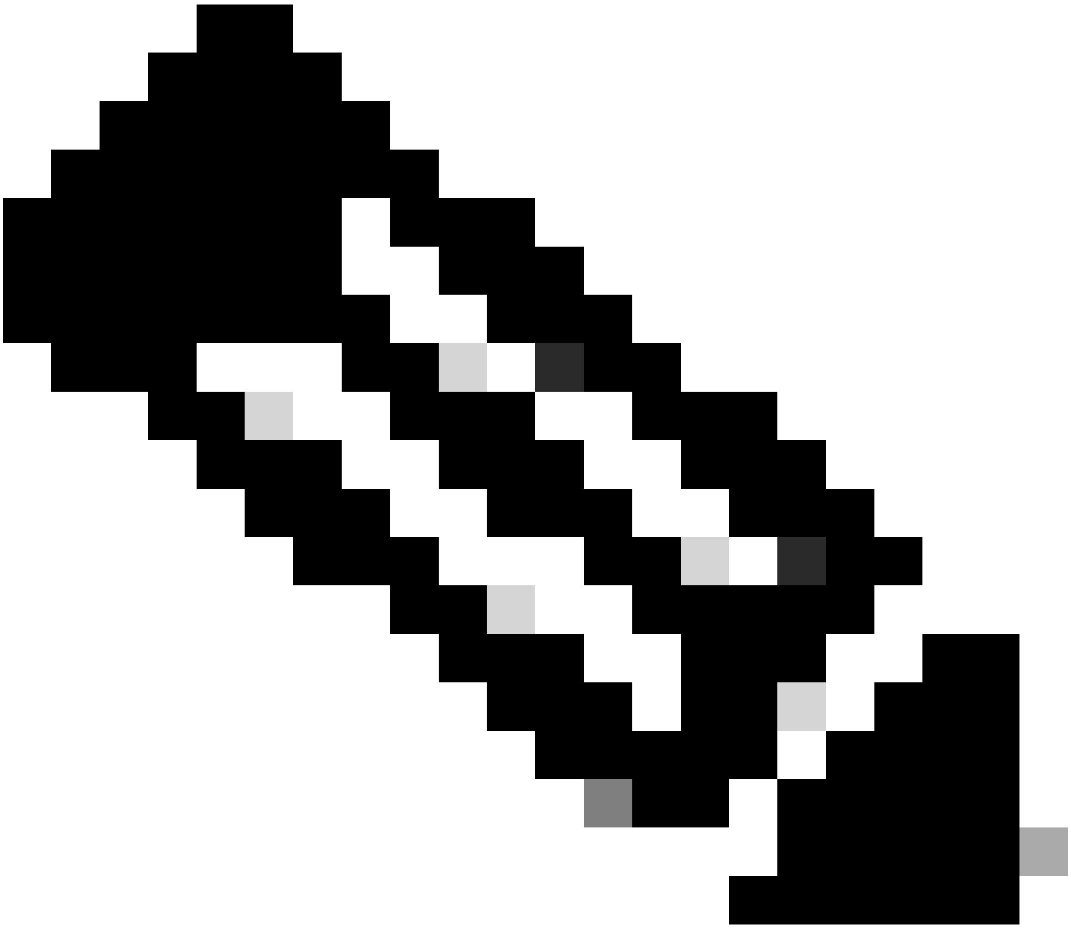
To initiate the configuration of the VPN, click on **Site-to-site VPN** and click on **Add**.



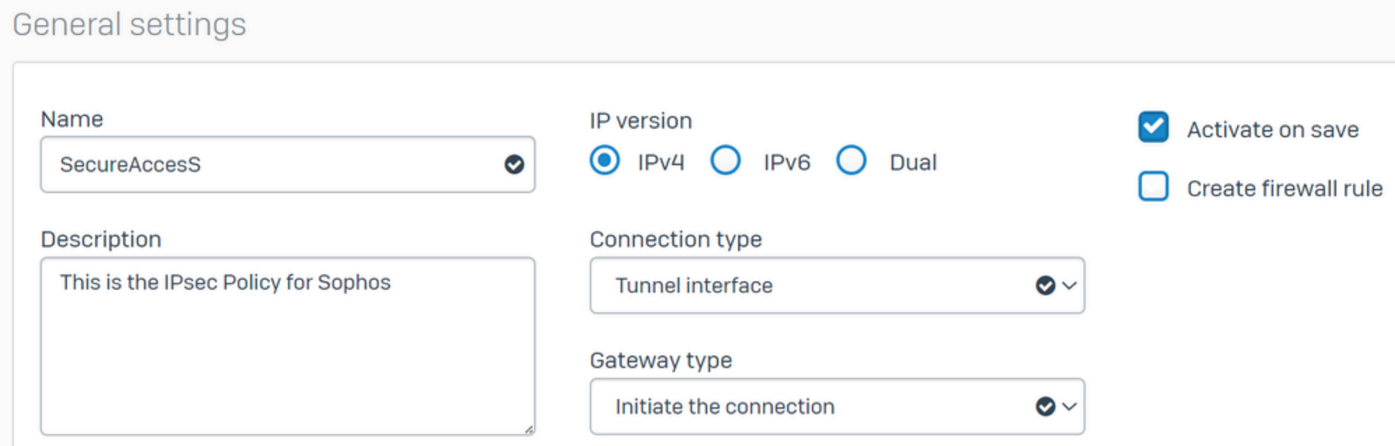
Sophos - Site-to-site VPN

Under **General Settings** configure:

- **Name**: A reference name to the Cisco Secure Access IPsec Policy
- IP version: IPv4
- Connection type: Tunnel interface
- Gateway type: Initiate the connection
- Active on save: Check the option



Note: The option **Active on save** enables the VPN automatically after you end up configuring the site-to-site VPN.



General settings

Name

SecureAccesS

Description

This is the IPsec Policy for Sophos

IP version

● IPv4 ○ IPv6 ○ Dual

Connection type

Tunnel interface

Gateway type

Initiate the connection

☑ Activate on save

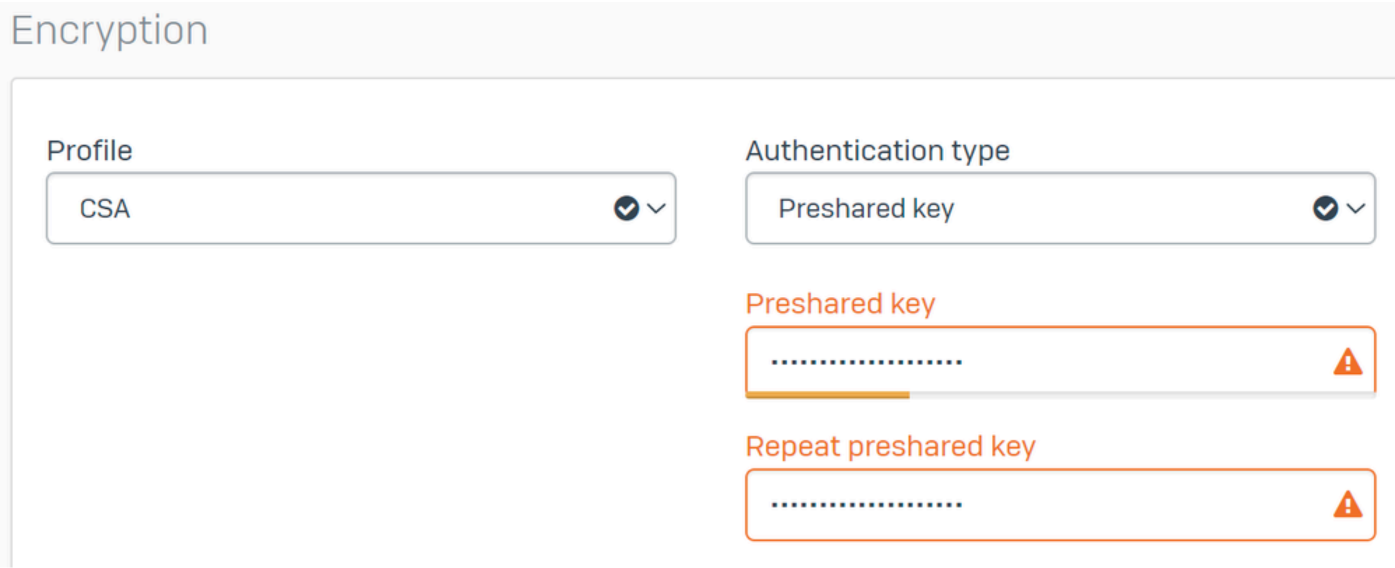
□ Create firewall rule

Sophos - Site-to-site VPN - General Settings

Note: The option Tunnel interface creates a virtual tunnel interface for the Sophos XG Firewall with the name XFRM.

Under **Encryption** configure:

- **Profile**: The profile that you create on the step, **Configure IPsec Profile**
- **Authentication type**: Preshared key
- **Preshared key**: The key that you configure on the step, Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**



Encryption

Profile: CSA

Authentication type: Preshared key

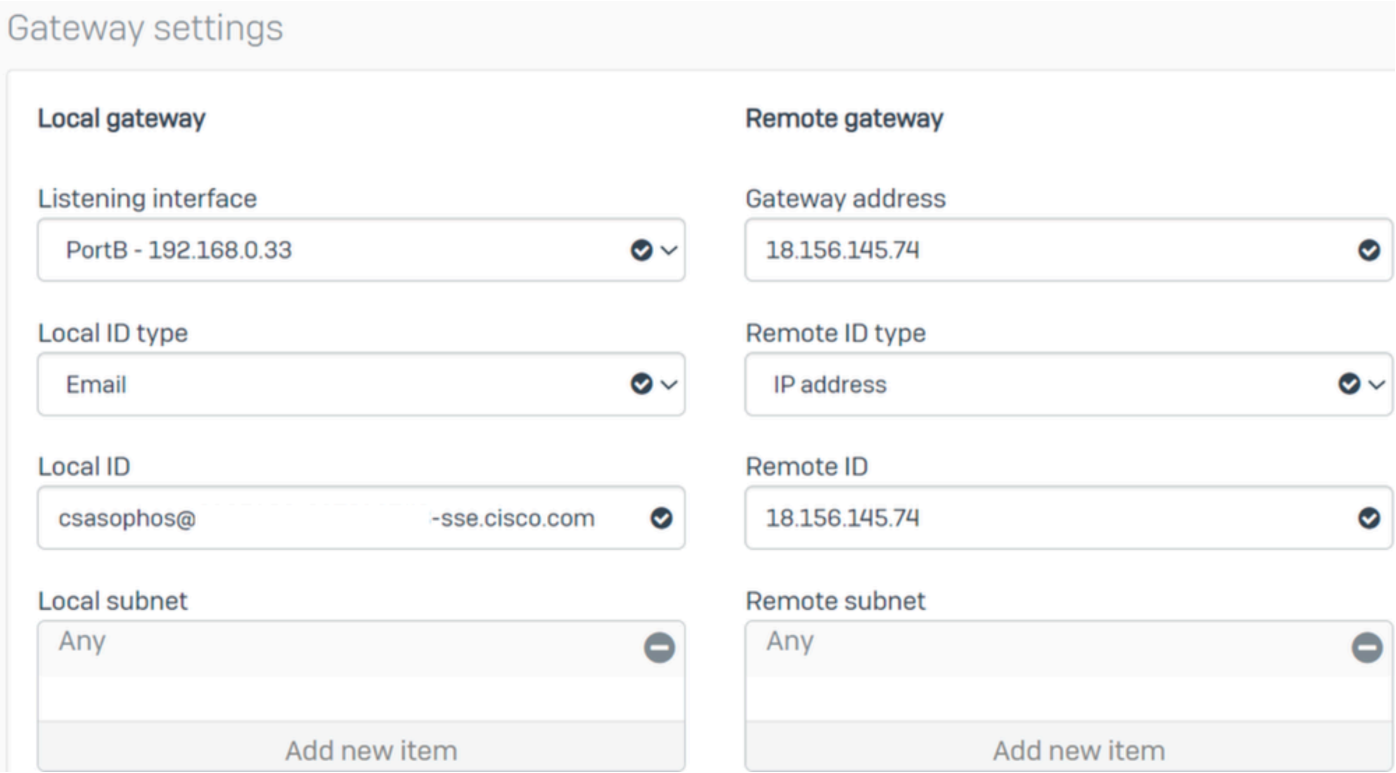
Preshared key: ••••••••••••••••••••

Repeat preshared key: ••••••••••••••••••••

Sophos - Site-to-site VPN - Encryption

Under **Gateway Settings** configure Local Gateway and Remote Gateway options, use this table as a reference.

Local Gateway	Remote Gateway
Listening interface Your Wan-Internet Interface	**Gateway address** The public IP generated under the step, **Tunnel Data**
Local ID type Email	**Remote ID type** IP address
Local ID The Email generated under the step, **Tunnel Data**	**Remote ID** The public IP generated under the step, **Tunnel Data**
Local subnet Any	**Remote Subnet** Any



Gateway settings

Local gateway

Listening interface: PortB - 192.168.0.33

Local ID type: Email

Local ID: csasophos@[redacted]-sse.cisco.com

Local subnet: Any

Add new item

Remote gateway

Gateway address: 18.156.145.74

Remote ID type: IP address

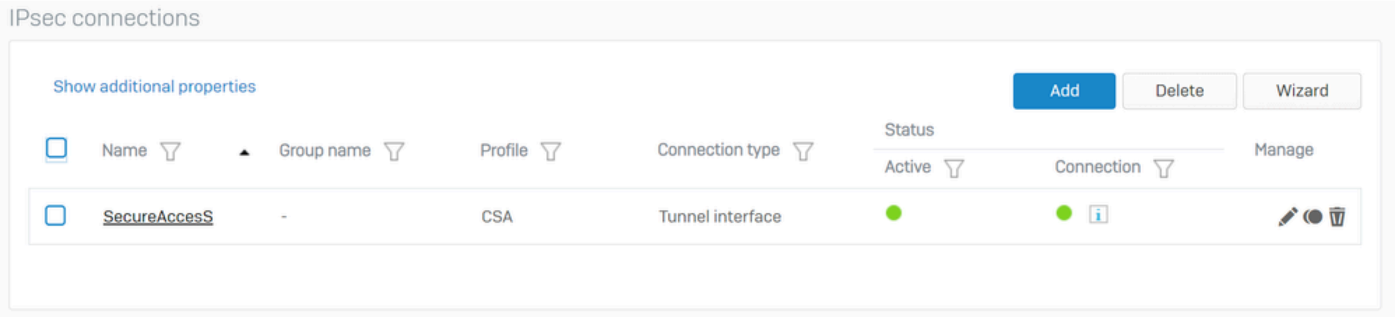
Remote ID: 18.156.145.74

Remote subnet: Any

Add new item

Sophos - Site-to-site VPN - Gateway Settings

After that click on **Save**, and you can see that the tunnel was created.



IPsec connections

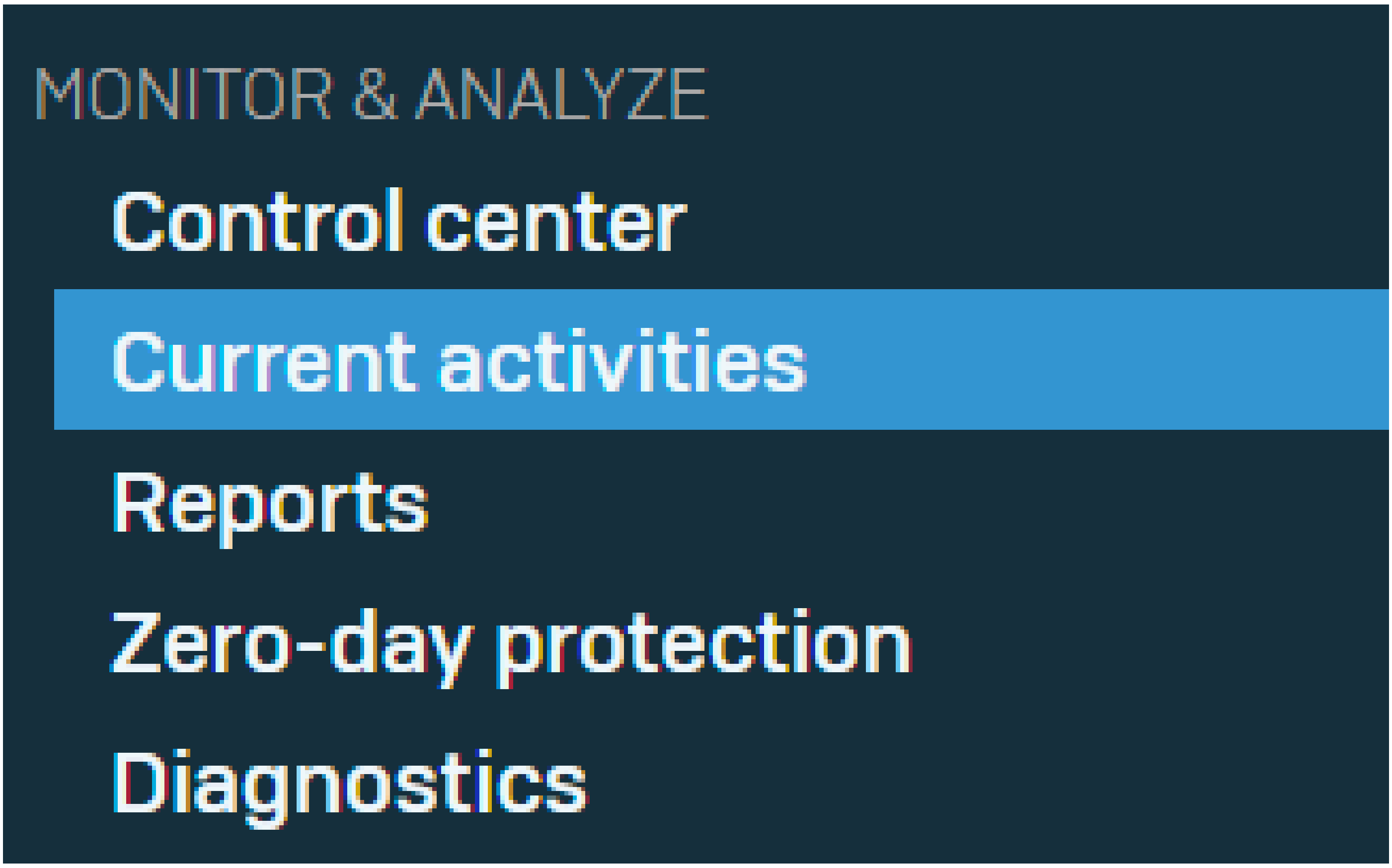
Show additional properties

□	Name	Group name	Profile	Connection type	Status		Manage
					Active	Connection	
□	SecureAccesS	-	CSA	Tunnel interface	●	●	

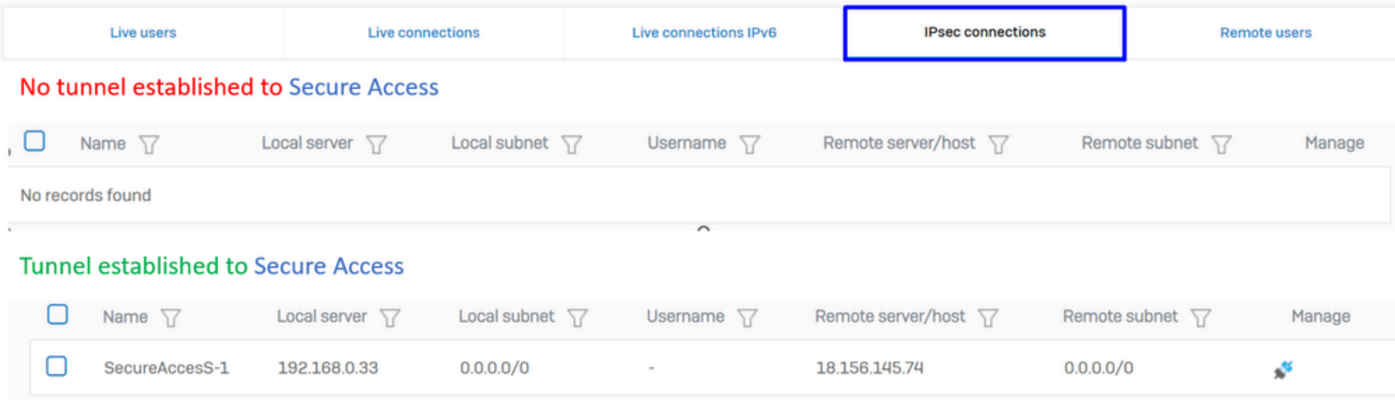
Sophos - Site-to-site VPN - IPsec Connections

Note: To check if the tunnel is correctly enabled on the last image you can check **Connection** status, if it is green, the tunnel is connected if it is not green the tunnel is not connected.

To check if a tunnel is established navigate to **Current Activities > IPsec Connections**.



Sophos - Monitor and Analyze - IPsec



No tunnel established to Secure Access

□	Name	Local server	Local subnet	Username	Remote server/host	Remote subnet	Manage
No records found							

Tunnel established to Secure Access

□	Name	Local server	Local subnet	Username	Remote server/host	Remote subnet	Manage
□	SecureAccesS-1	192.168.0.33	0.0.0.0/0	-	18.156.145.74	0.0.0.0/0	

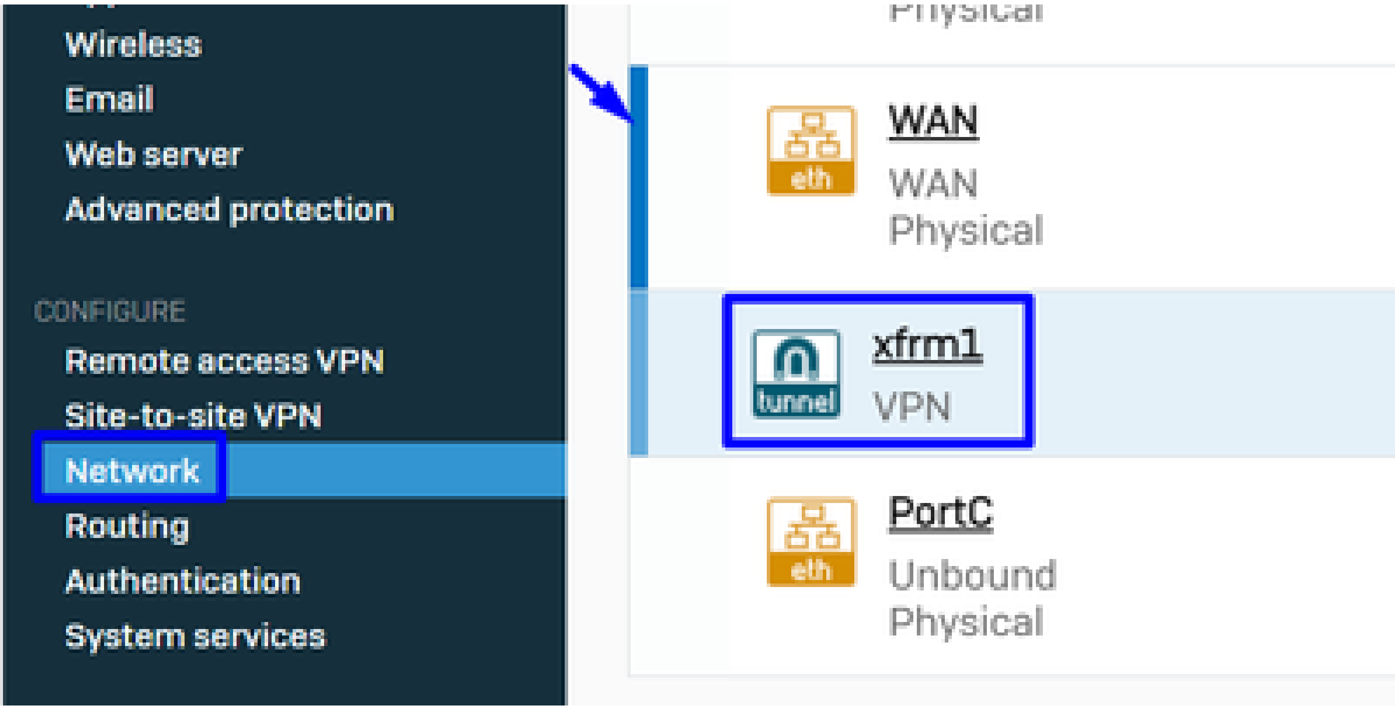
Sophos - Monitor and Analyze - IPsec before and after

After that, we can continue with the step, **Configure Tunnel Interface Gateway**.

Configure Tunnel Interface

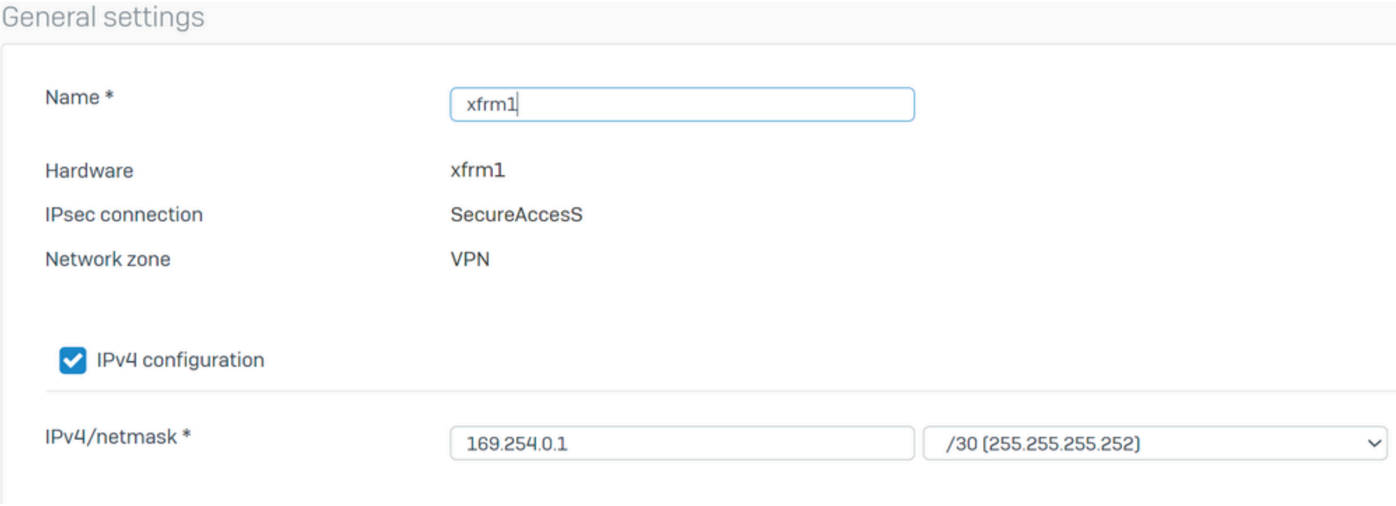
Navigate to **Network** and check your WAN interface configured on the VPN to edit the virtual tunnel interface with the name xfrm.

- Click on the**xfrm** interface.



Sophos - Network - Tunnel Interface

- Configure the interface with an IP non-routable in your network, for example, you can use 169.254.x.x/30 which is an IP in a non-routable space usually, in our example we use 169.254.0.1/30


General settings

Name * xfrm1

Hardware xfrm1

IPsec connection SecureAccesS

Network zone VPN

☑ IPv4 configuration

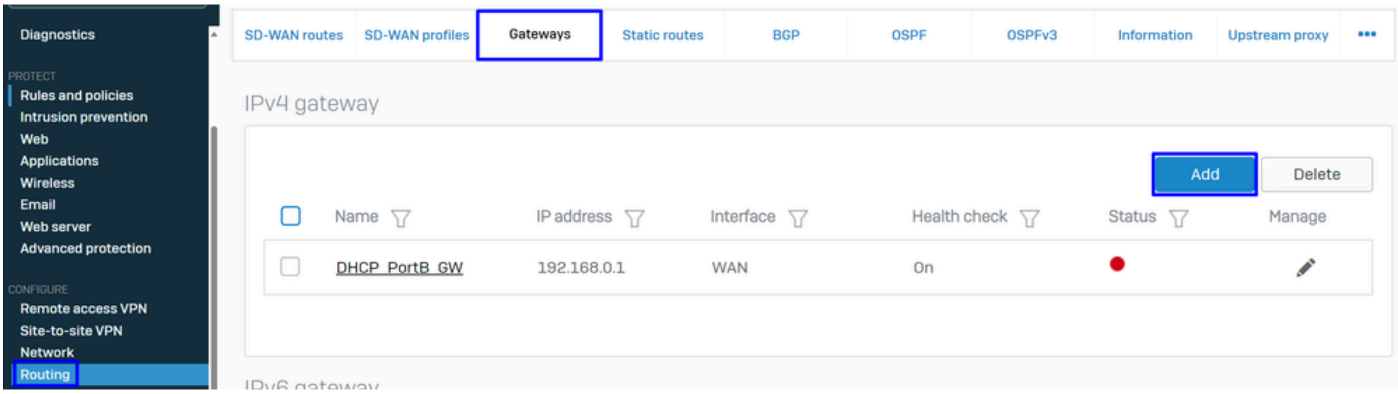
IPv4/netmask * 169.254.0.1 /30 (255.255.255.252)

Sophos - Network - Tunnel Interface - Configuration

Configure the Gateways

In order to configure the gateway for the virtual interface (xfrm)

- Navigate to Routing > Gateways
- Click Add



IPv4 gateway

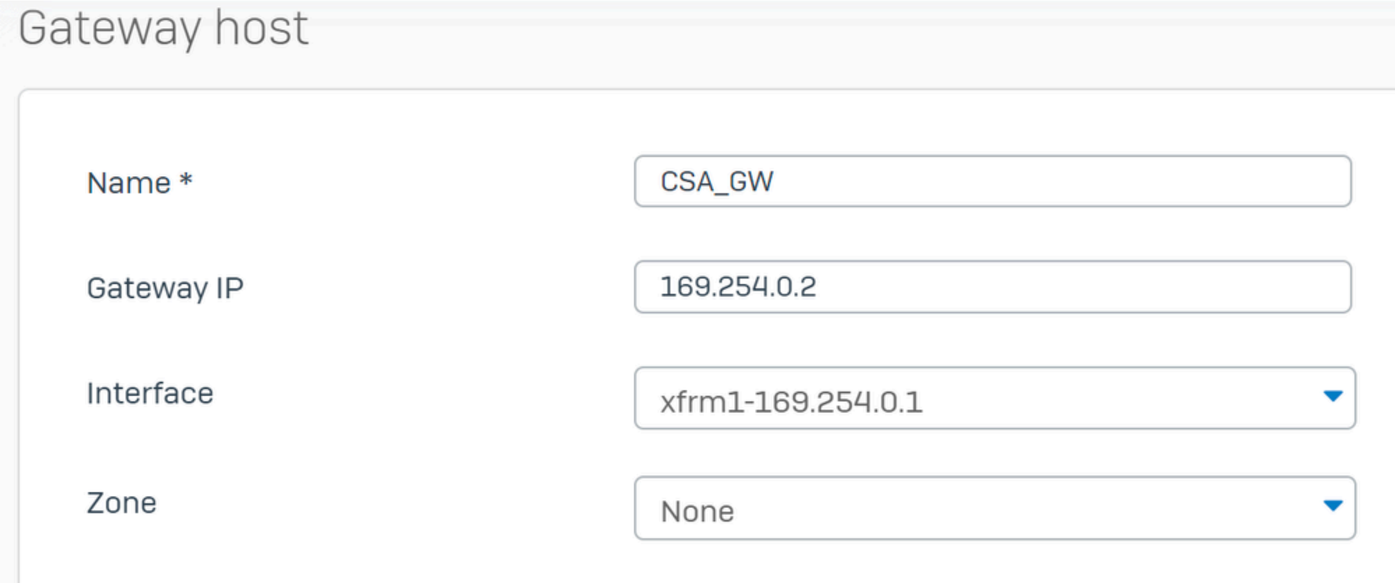
□	Name	IP address	Interface	Health check	Status	Manage
□	DHCP_PortB_GW	192.168.0.1	WAN	On	●	✎

IPv6 gateway

Sophos - Routing - Gateways

Under **Gateway host** configure:

- **Name**: A name that makes reference to the virtual interface created for the VPN
- **Gateway IP**: In our case 169.254.0.2, that is the IP under the network 169.254.0.1/30 that already we assigned under the step, [Configure Tunnel Interface]
- Interface: VPN Virtual Interface
- **Zone**: None (Default)

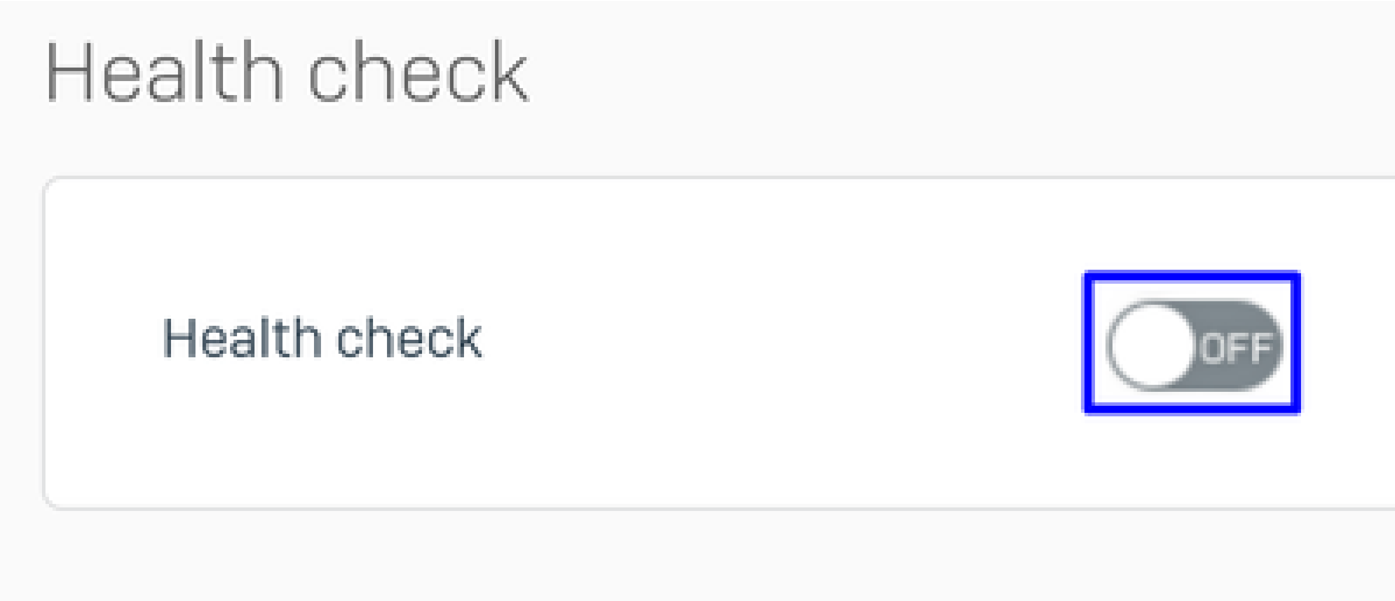


Gateway host

Name *	CSA_GW
Gateway IP	169.254.0.2
Interface	xfrm1-169.254.0.1
Zone	None

Sophos - Routing - Gateways - Gateway Host

- Under **Health check** disable the check
- Click **Save**

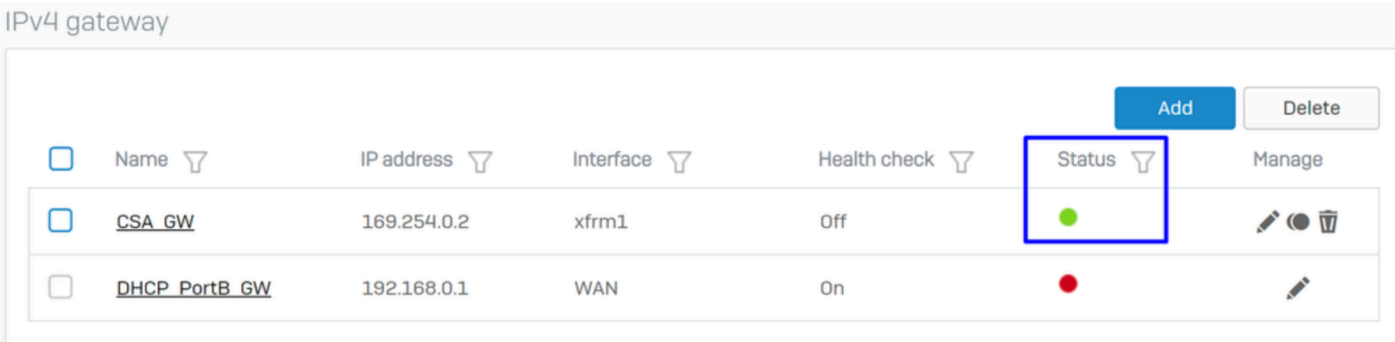


Health check

Health check

Sophos - Routing - Gateways - Health-check

You can observe the status of the gateway after you save the configuration:



IPv4 gateway

□	Name	IP address	Interface	Health check	Status	Manage
□	CSA_GW	169.254.0.2	xfrm1	Off	🟢	✎ ◐ 🗑
□	DHCP_PortB_GW	192.168.0.1	WAN	On	🔴	✎

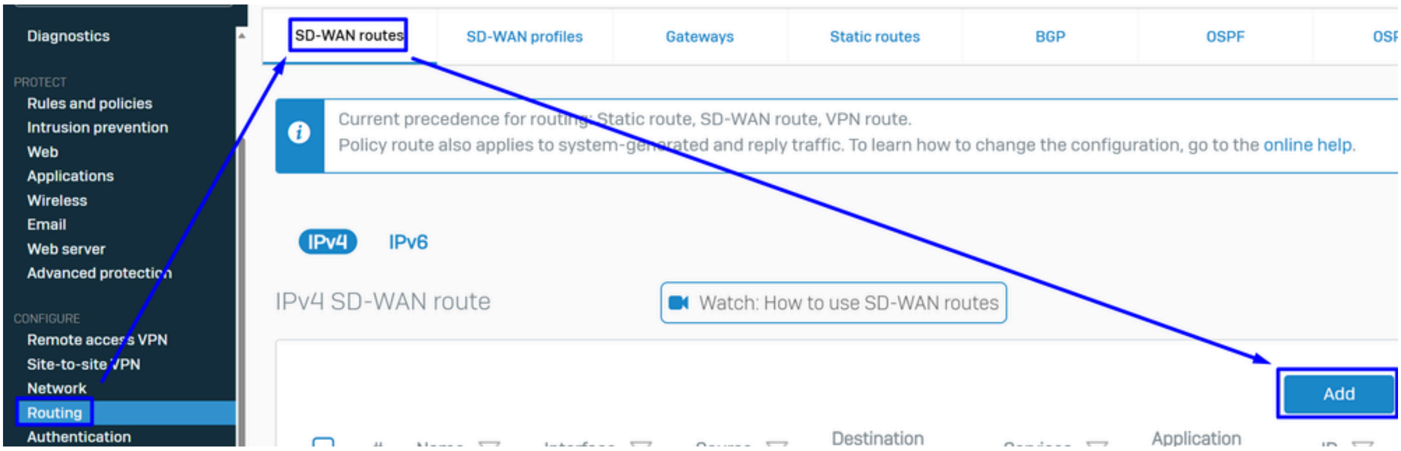
Sophos - Routing - Gateways - Status

Configure the SD-WAN Route

To finalize the process of configuration, you need to create the route that permits you to forward the traffic to Secure Access.

Navigate to **Routing** > **SD-WAN routes.**

- Click on **Add**



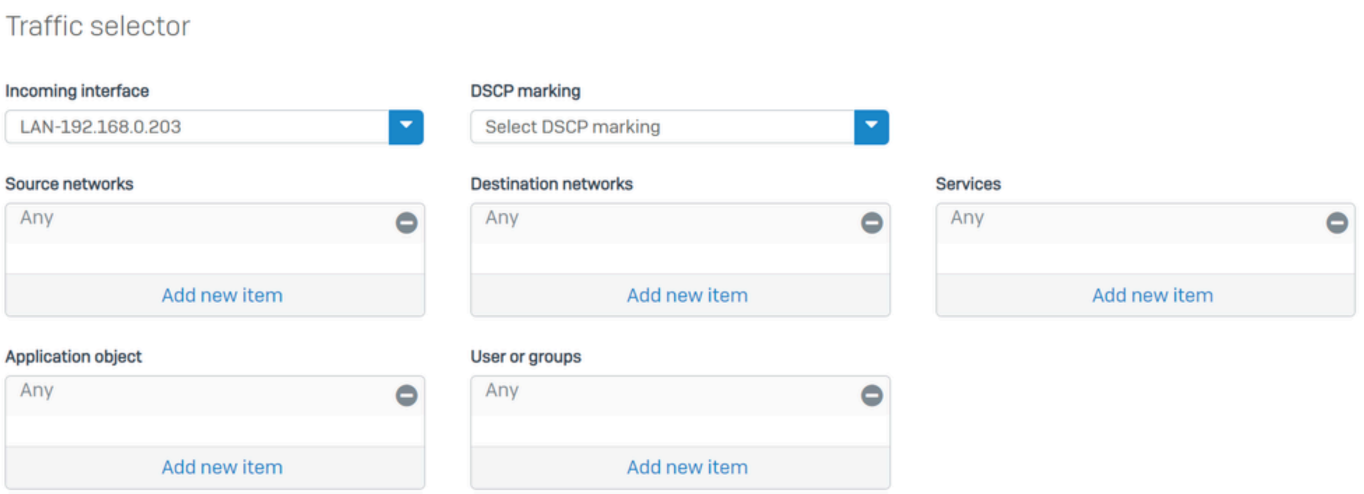
Current precedence for routing: Static route, SD-WAN route, VPN route.
Policy route also applies to system-generated and reply traffic. To learn how to change the configuration, go to the online help.

IPv4 SD-WAN route

Sophos - SD-Wan Routes

Under **Traffic Selector** configure:

- Incoming interface: Select the interface from where you want to send the traffic or the users that access from RA-VPN, ZTNA, or Clientless-ZTNA
- DSCP marking: Nothing for this example
- **Source networks**: Select the address that you want to route through the tunnel
- **Destination networks**: Any or you can specify a destination
- **Services**: Any or you can specify the services
- **Application object**: An application if you have the object configured
- User or groups: If you want to add a specific group of users to route the traffic to Secure Access



Traffic selector

Incoming interface: LAN-192.168.0.203

DSCP marking: Select DSCP marking

Source networks: Any

Destination networks: Any

Services: Any

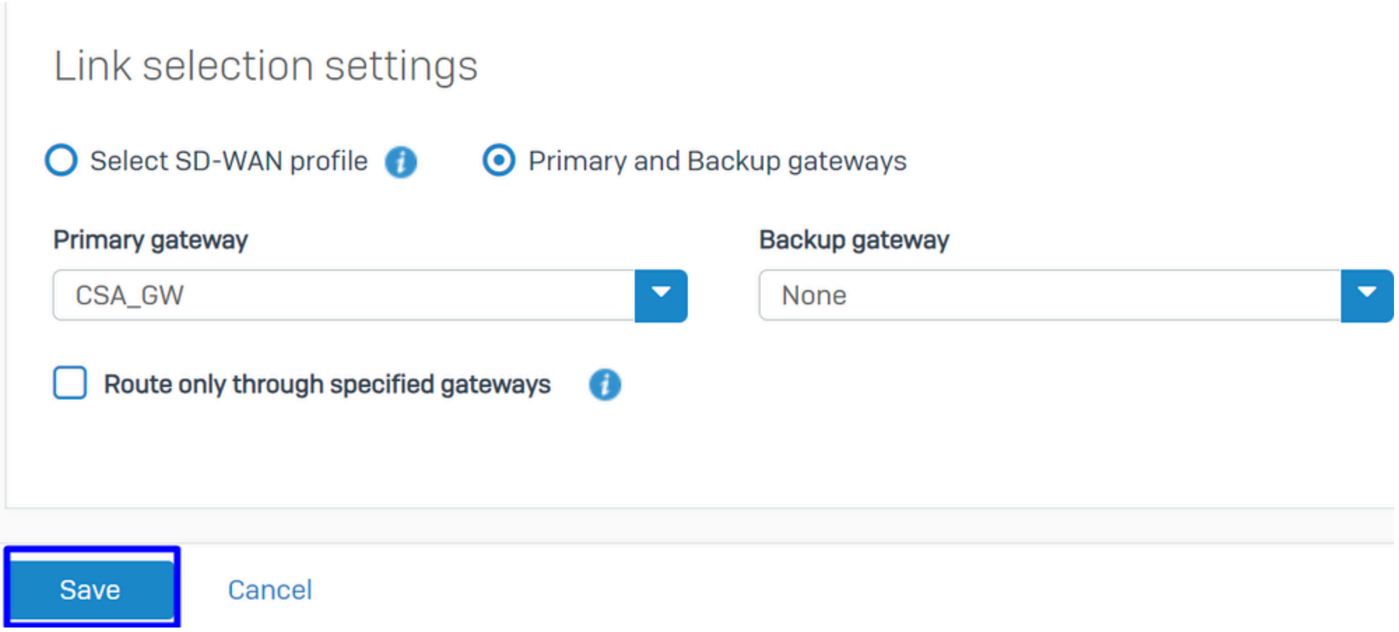
Application object: Any

User or groups: Any

Sophos - SD-Wan Routes - Traffic Selector

Under **Link selection settings** configure the gateway:

- Primary and Backup gateways: Check the option
- **Primary gateway**: Select the gateway configured under the step, [Configure the Gateways]()
- Click on **Save**



Link selection settings

○ Select SD-WAN profile ● Primary and Backup gateways

Primary gateway: CSA_GW

Backup gateway: None

□ Route only through specified gateways

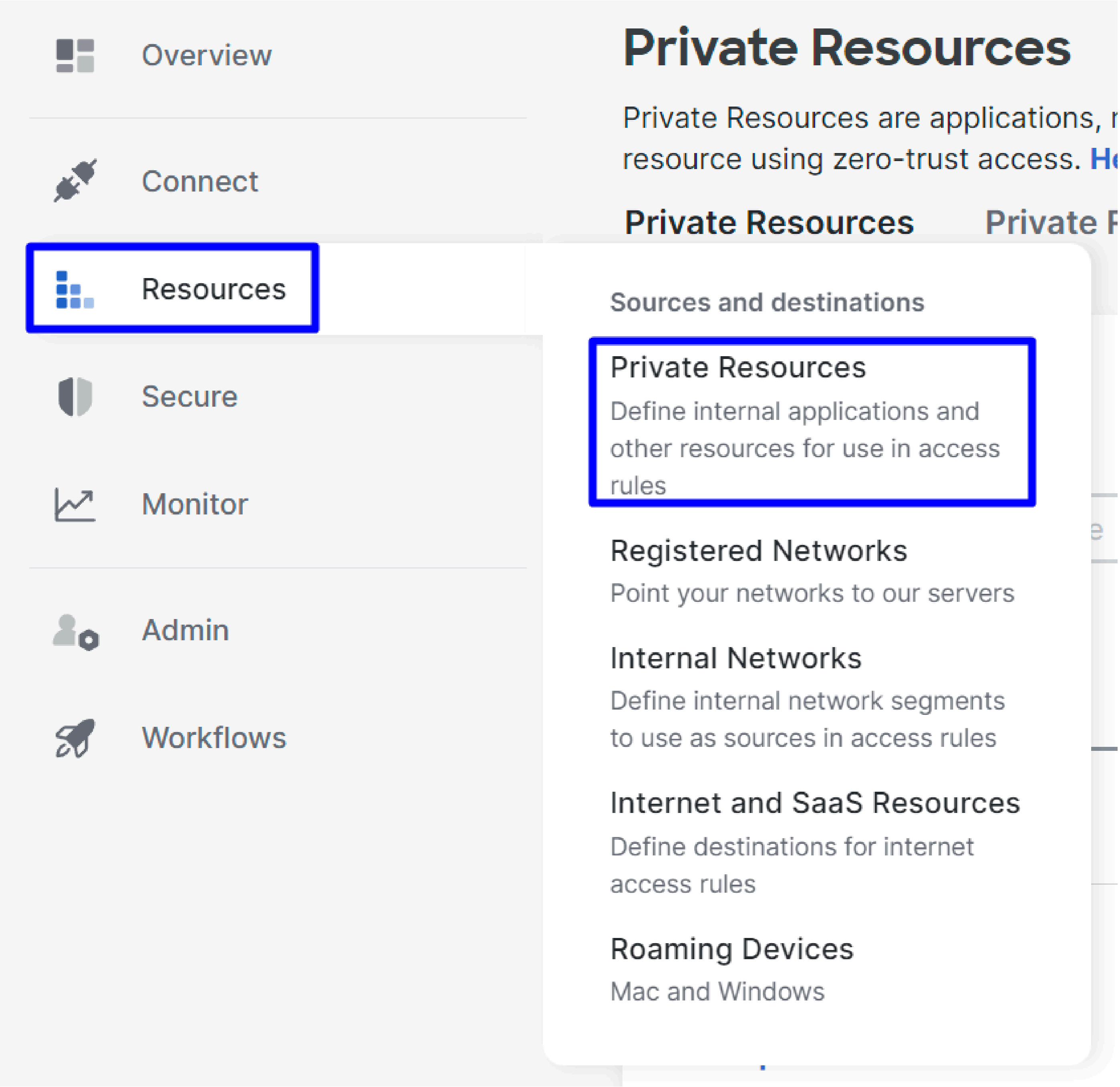
Sophos - SD-Wan Routes - Traffic Selector - Primary and Backup gateways

After you finalize the configuration on the Sophos XG Firewall you can proceed with the step, **Configure Private App.**

Configure Private App

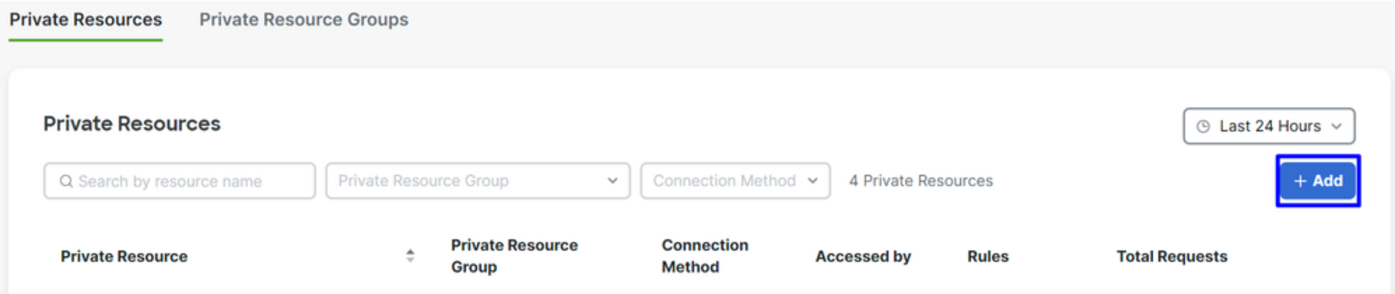
In order to configure the Private App access, log in to the Admin Portal.

- Navigate to **Resources > Private Resources**


Overview
Connect
Resources
Secure
Monitor
Admin
Workflows
Private Resources
Private Resources are applications, r
resource using zero-trust access. He
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

Secure Access - Private Resources

- Click on + Add



Private Resources | Private Resource Groups

Private Resources

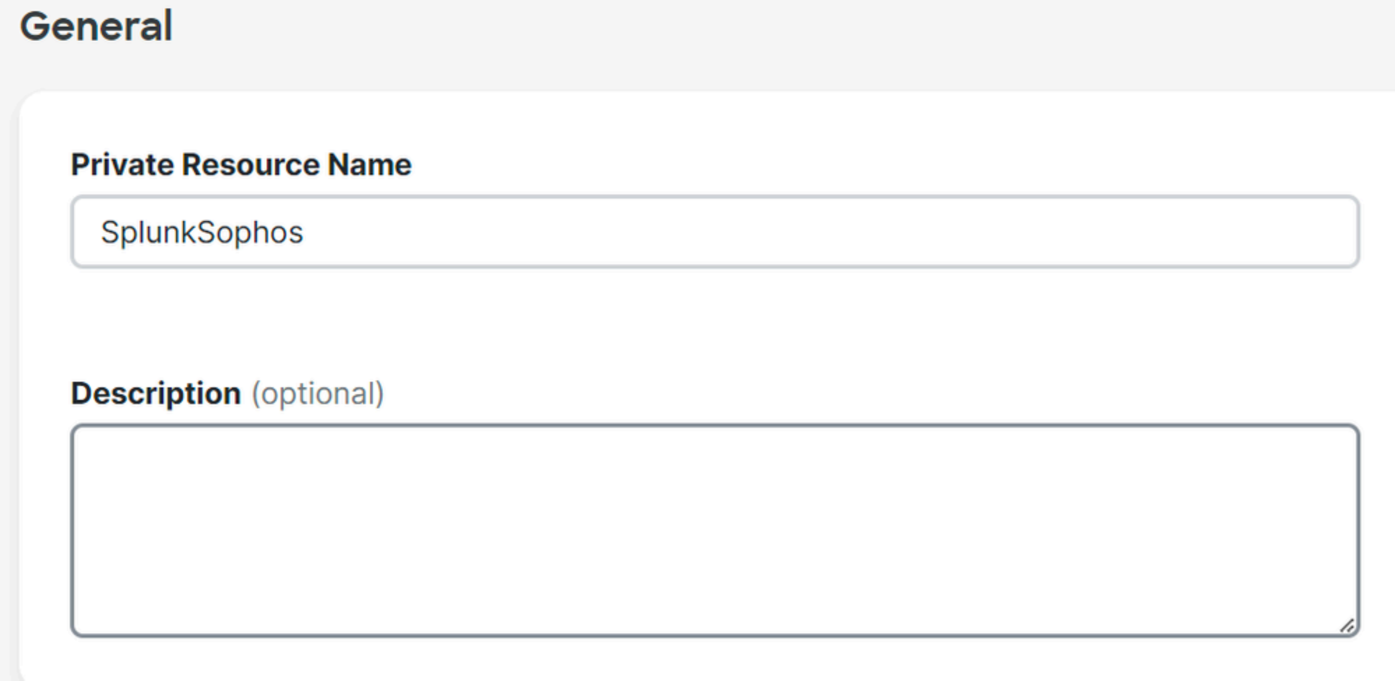
Last 24 Hours

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

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

Secure Access - Private Resources 2

- Under **General** Configure the **Private Resource Name**



General

Private Resource Name: SplunkSophos

Description (optional)

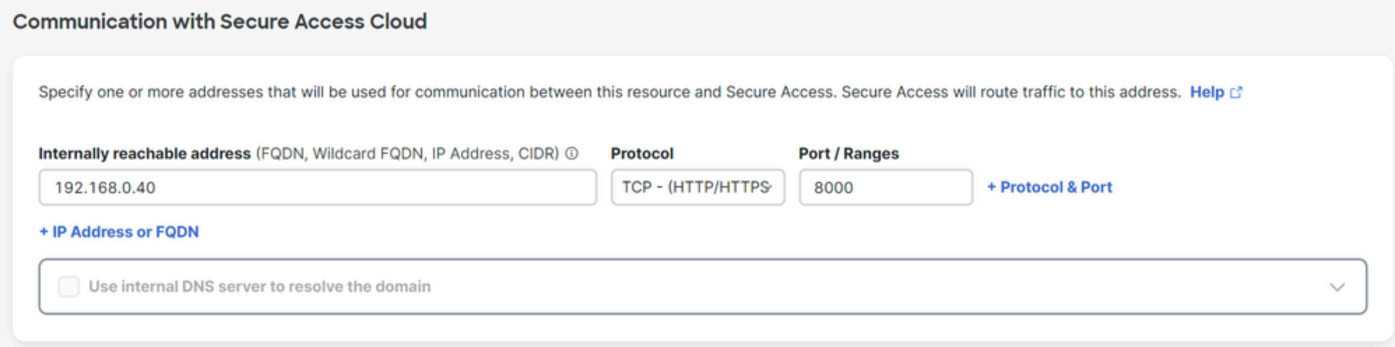
Secure Access - Private Resources - General

Under **Communication with Secure Access Cloud** configure:

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: Select the resource that you want to access

Note: Remember the internally reachable address was assigned on the step, **[Configure the Tunnel on Secure Access](#)**.

- **Protocol**: Select the protocol that you use to access that resource
- Port / Ranges : Select the ports that you need to enable to access the app



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

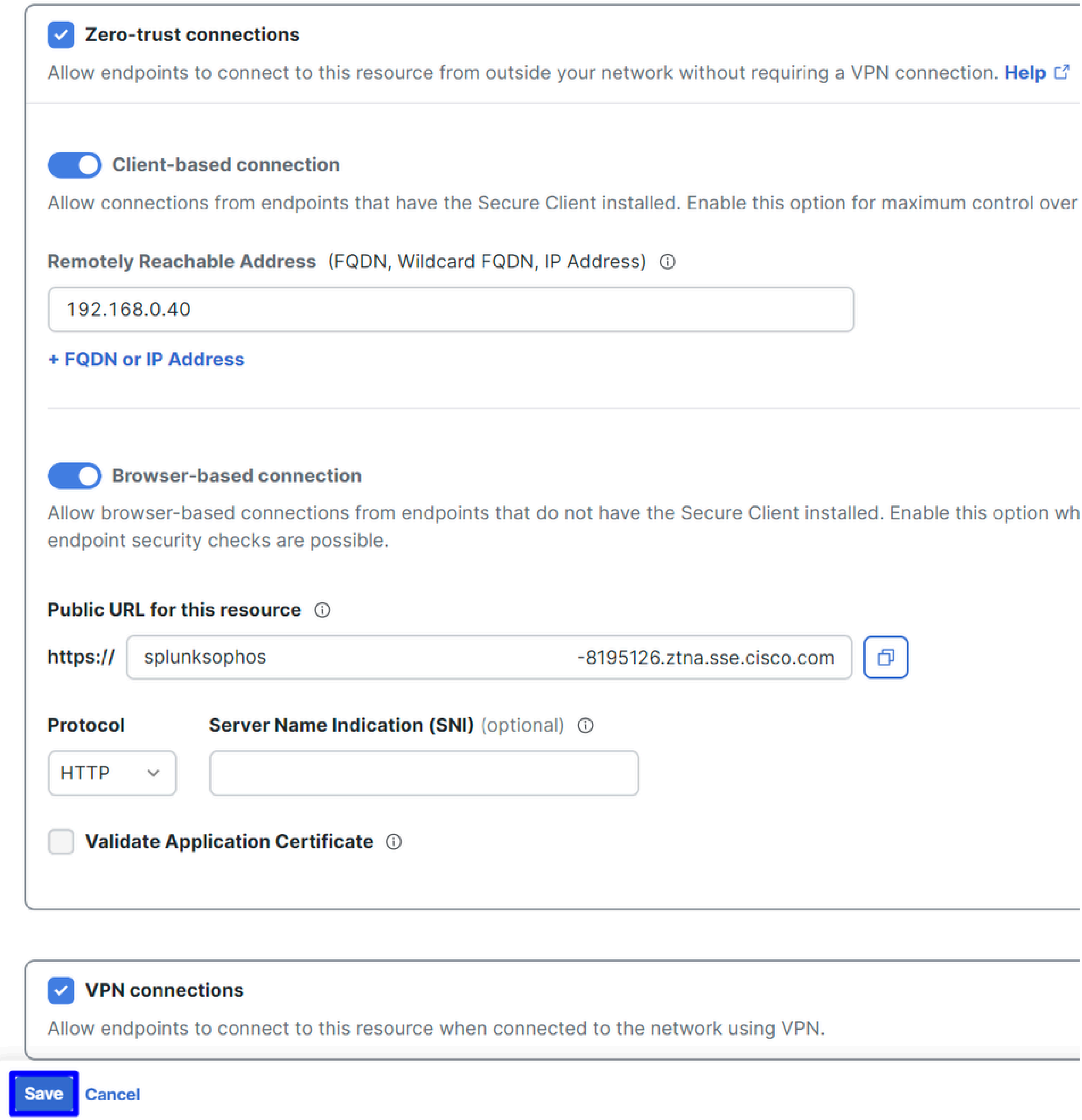
□ Use internal DNS server to resolve the domain

Secure Access - Private Resources - Communications with Secure Access Cloud

Within **Endpoint Connection Methods**, you configure all the ways possible to access private resources via Secure

Access, and choose the methods that you want to use for your environment:

- **Zero-trust connections**: Check the box to enable ZTNA access.
  - **Client-based connection**: Enable the button to permit client base ZTNA
    - **Remotely Reachable Address**: Configure the IP of your private App
  - **Browser-based connection**: Enable the button to permit browser-based ZTNA
    - Public URL for this resource: Add a name to use in conjunction with the domain ztna.sse.cisco.com
    - Protocol: Choose HTTP or HTTPS as a protocol to access through the browser
  - **VPN connections**: Check the box to enable RA-VPN Access.
- Click **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

Browser-based connection

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

Public URL for this resource

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

Protocol: HTTP

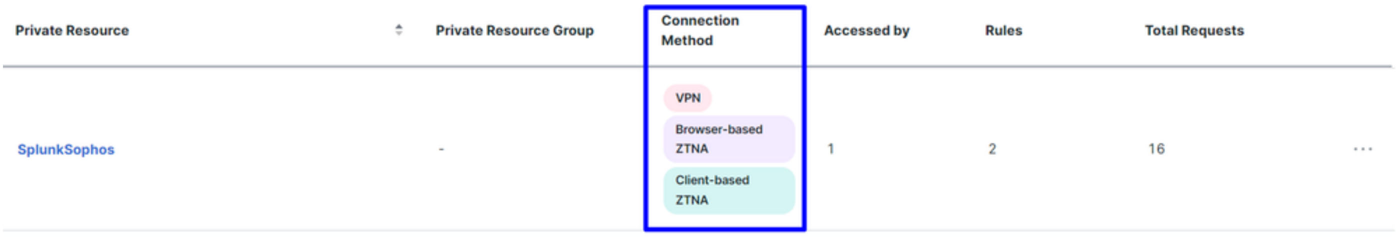
Server Name Indication (SNI) (optional):

□ Validate Application Certificate

☑ **VPN connections**

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

After the configuration is complete, this is the result:



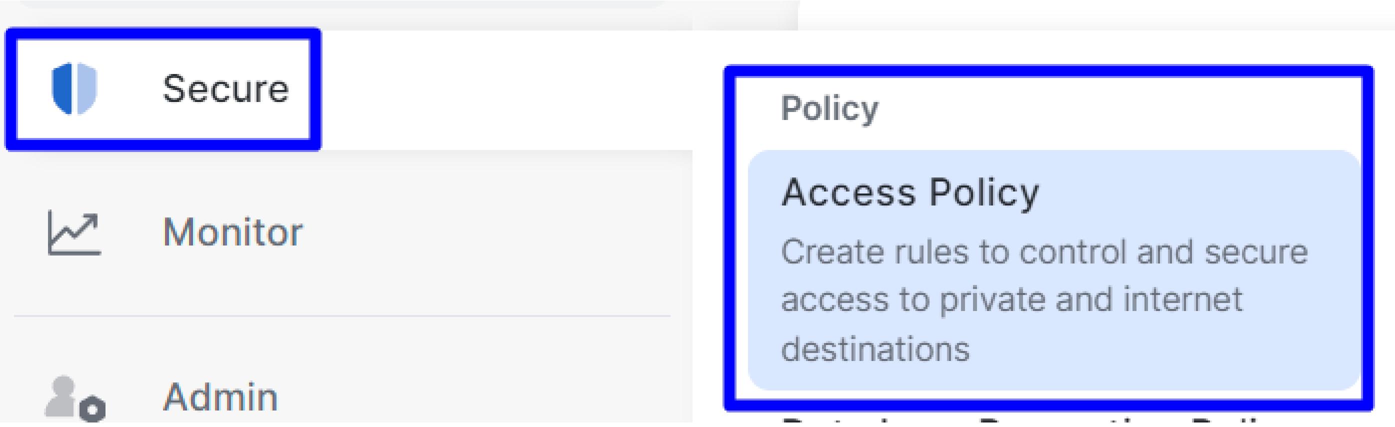
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	VPN Browser-based ZTNA Client-based ZTNA	1	2	16

Secure Access - Private Resources Configured

Now you can proceed with the step, **Configure the Access Policy**.

Configure the Access Policy

In order to configure the access policy navigate to Secure > Access Policy.

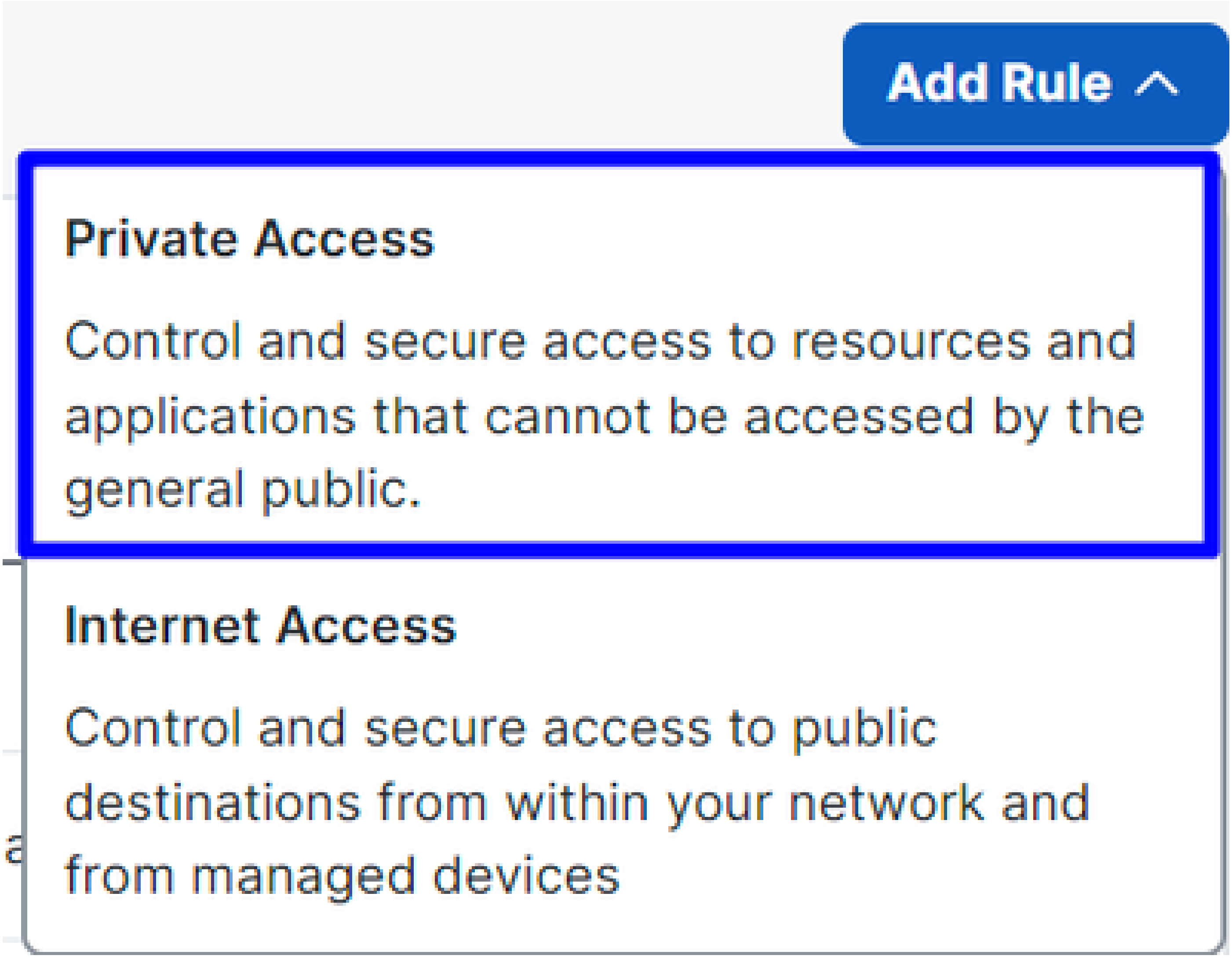


Access Policy

Create rules to control and secure access to private and internet destinations

Secure Access - Access Policy

- Click **Add Rule** > **Private Access**



Add Rule

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

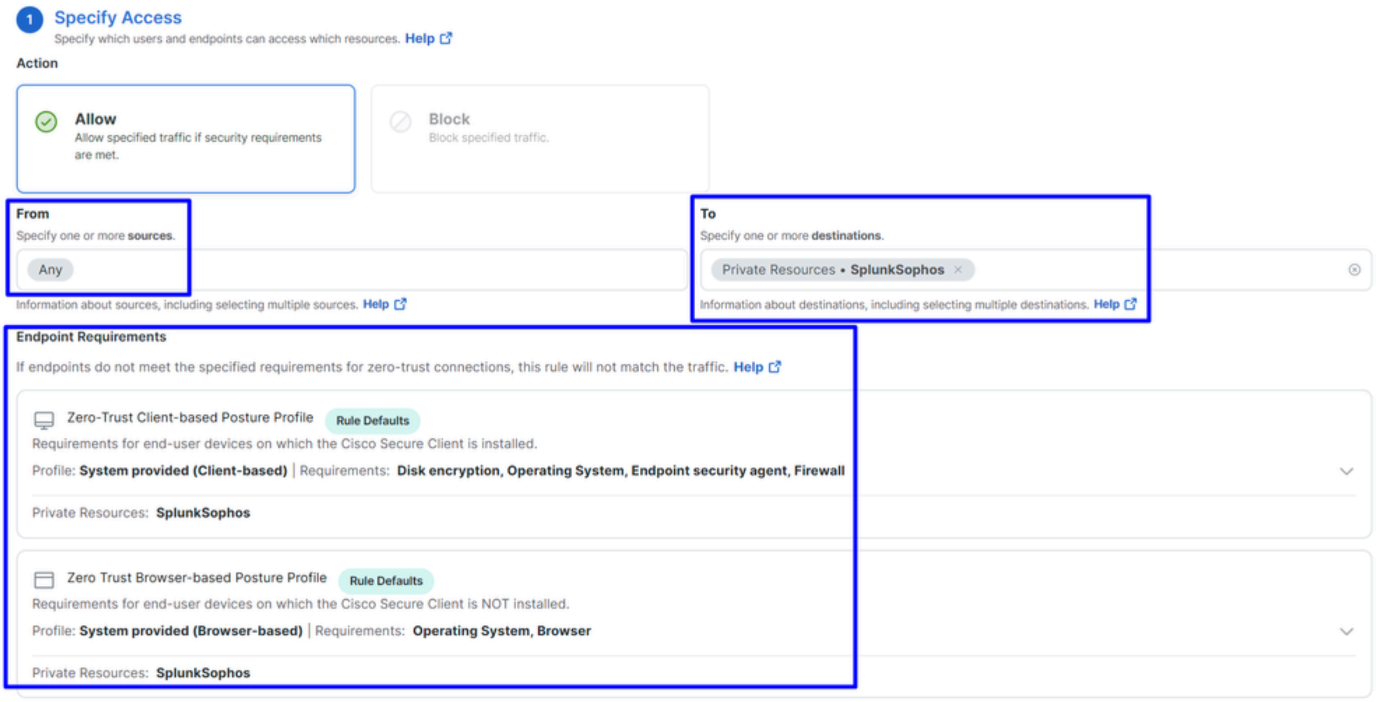
Internet Access

Control and secure access to public destinations from within your network and from managed devices

Secure Access - Access Policy - Private Access

Configure the next options to provide access through multiple methods of authentication:

- 1. Specify Access
  - Action: Allow
  - **Rule name**: Specify a name for your access rule
  - **From**: The users that you grant access to
  - **To**: The application that you wanted to permit access
  - Endpoint Requirements: (Default)
- Click **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.

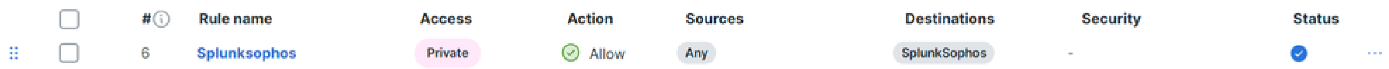
Profile: **System provided (Browser-based)** | Requirements: **Operating System, Browser**

Private Resources: **SplunkSophos**

Secure Access - Access Policy - Specify Access

Note: For step **2. Configure Security** as needed, but in this case, you did not enable the **Intrusion Prevention (IPS)**, or **Tenant Control Profile.**

- Click Save, and you have:



☐	#	Rule name	Access	Action	Sources	Destinations	Security	Status
☐	6	Splunksophos	Private	✓ Allow	Any	SplunkSophos	-	✓

Secure Access - Access Policy Configured

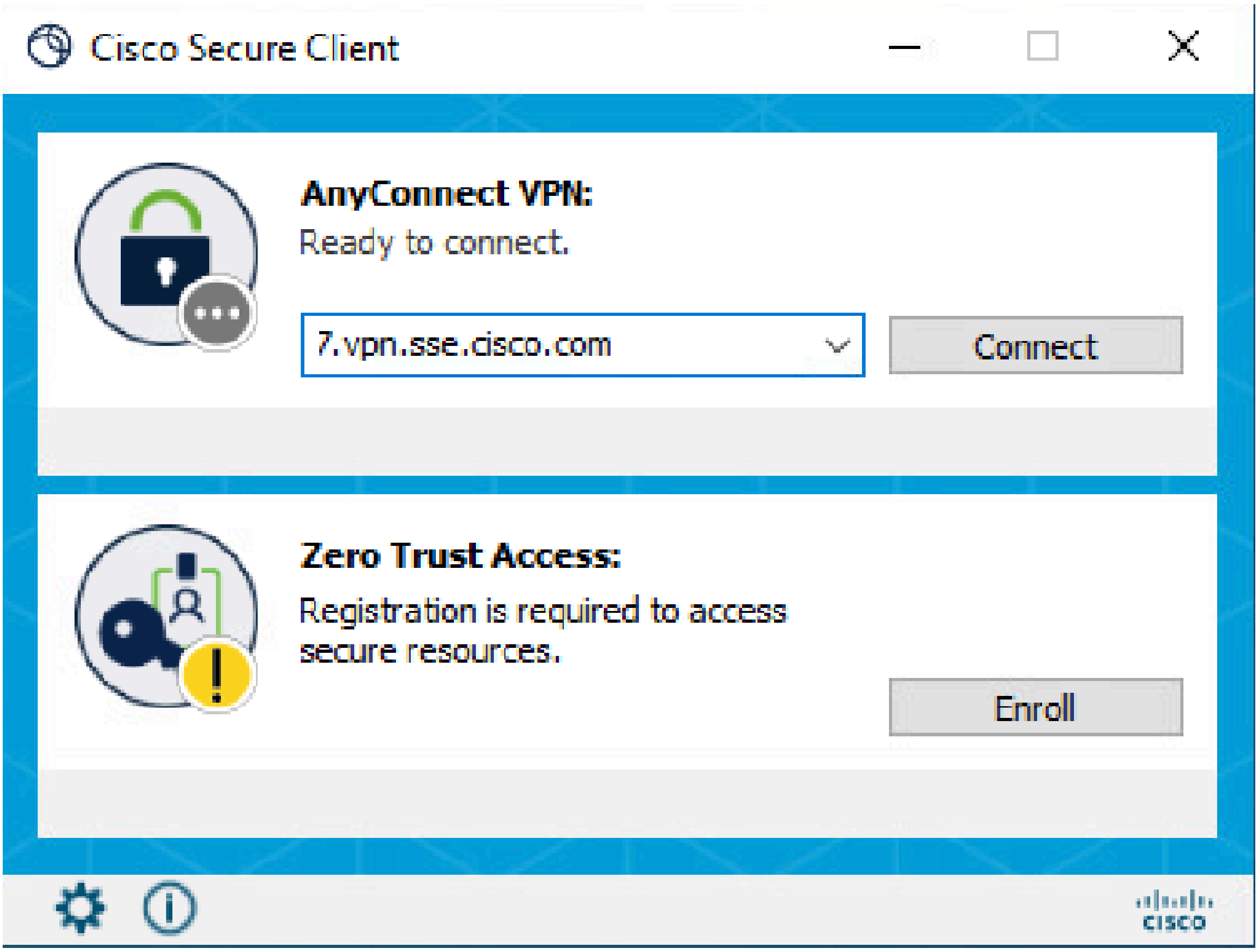
After that, you can proceed with the step Verify.

Verify

In order to verify the access you must have installed the agent of Cisco Secure Client that you can download from Software Download - Cisco Secure Client.

RA-VPN

Login through Cisco Secure Client Agent-VPN.


Cisco Secure Client

AnyConnect VPN:

Ready to connect.

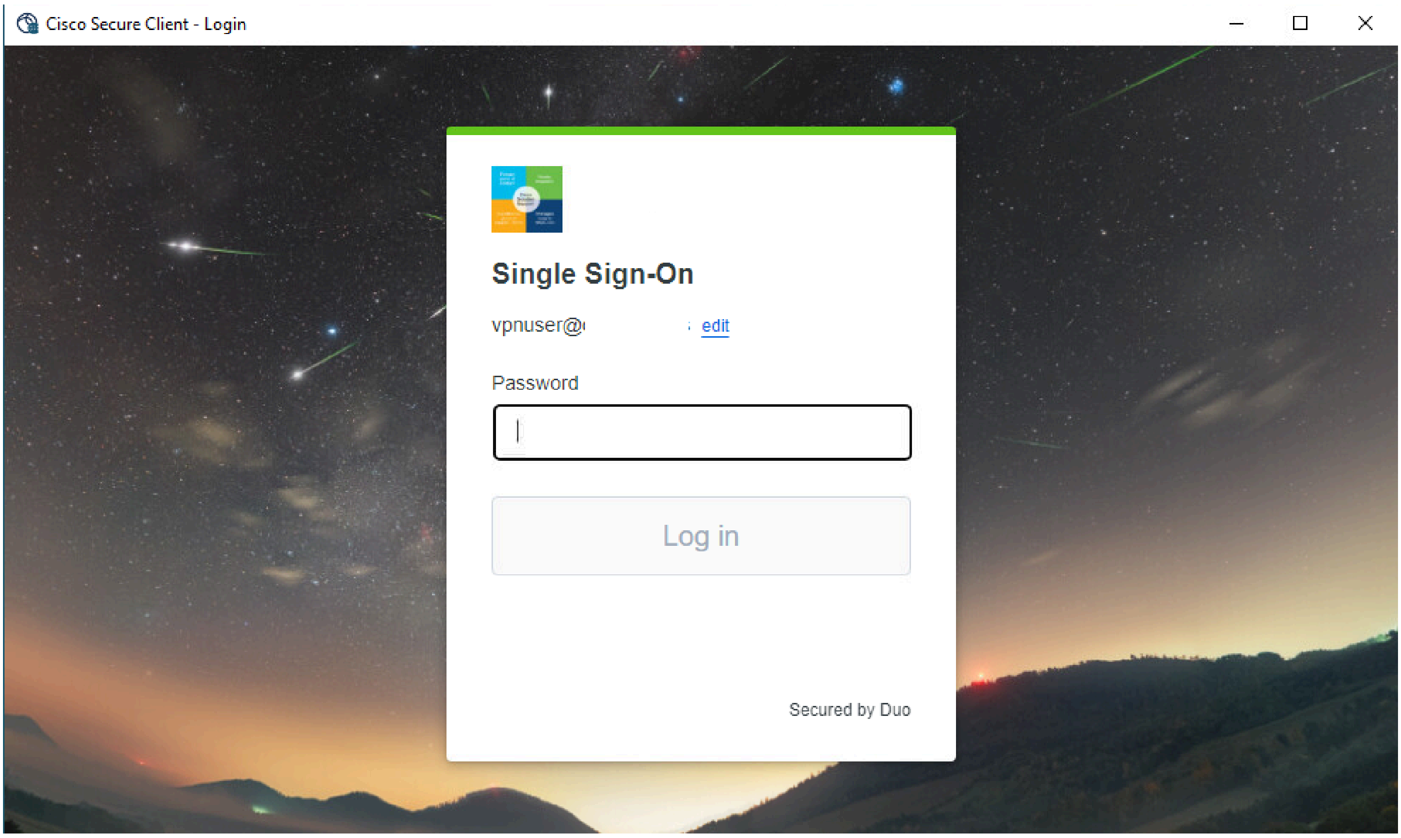
7.vpn.sse.cisco.com

Zero Trust Access:

Registration is required to access secure resources.

Secure Client - VPN

- Authenticate through your SSO provider



Cisco Secure Client - Login

Single Sign-On

vpnuser@ edit

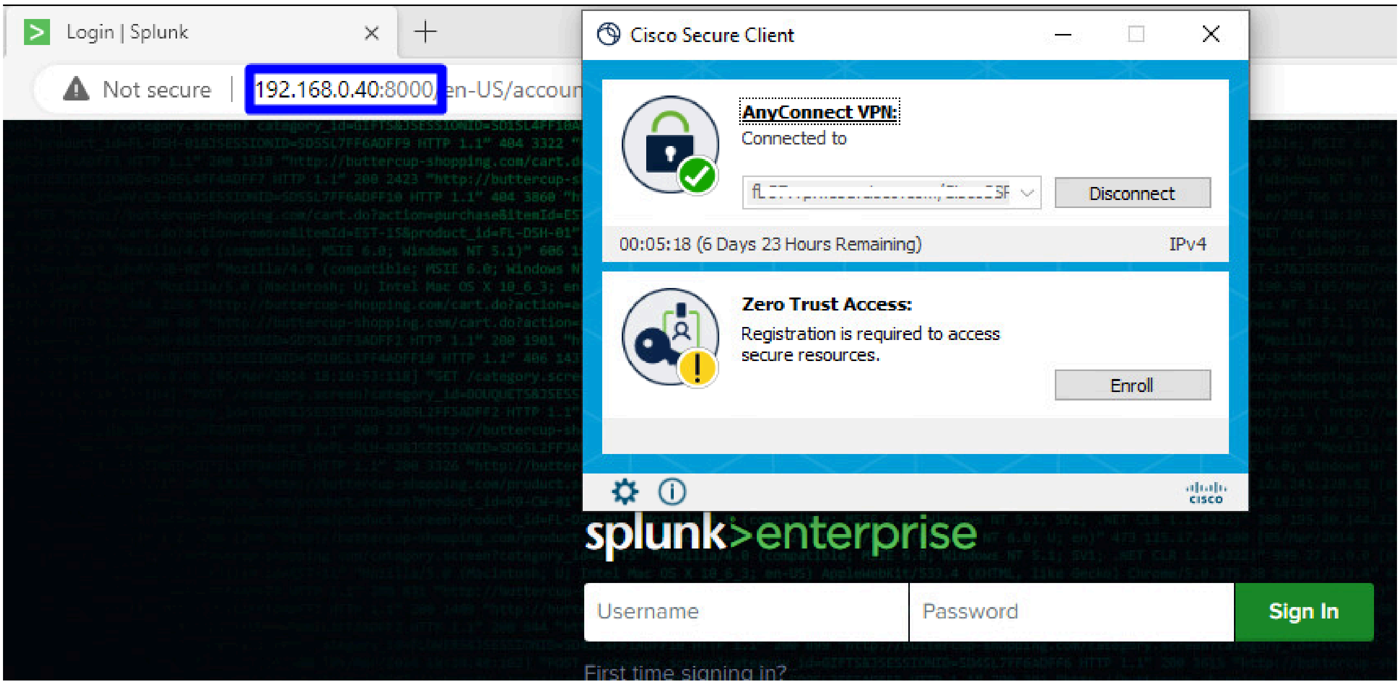
Password

Log in

Secured by Duo

Secure Access - VPN - SSO

- After you get authenticated, access to the resource:



Login | Splunk

Not secure | 192.168.0.40:8000/en-US/accoun

Cisco Secure Client

AnyConnect VPN:
Connected to

Disconnect

00:05:18 (6 Days 23 Hours Remaining) IPv4

Zero Trust Access:
Registration is required to access secure resources.

Enroll

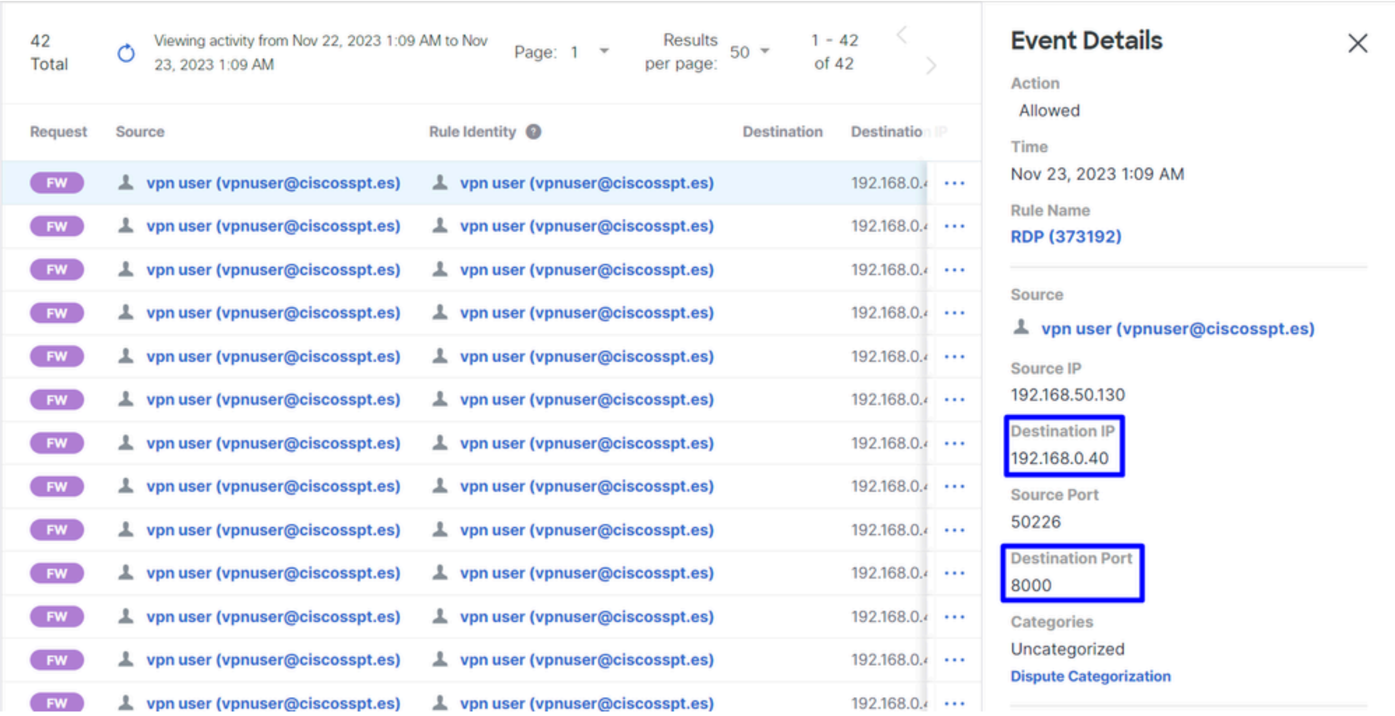
splunk>enterprise

Username | Password | Sign In

First time signing in?

Secure Access - VPN - Authenticated

Navigate to 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	Destinatio
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)		192.168.0.4

Event Details

Action
Allowed

Time
Nov 23, 2023 1:09 AM

Rule Name
RDP (373192)

Source
vpn user (vpnuser@ciscosspt.es)

Source IP
192.168.50.130

Destination IP
192.168.0.40

Source Port
50226

Destination Port
8000

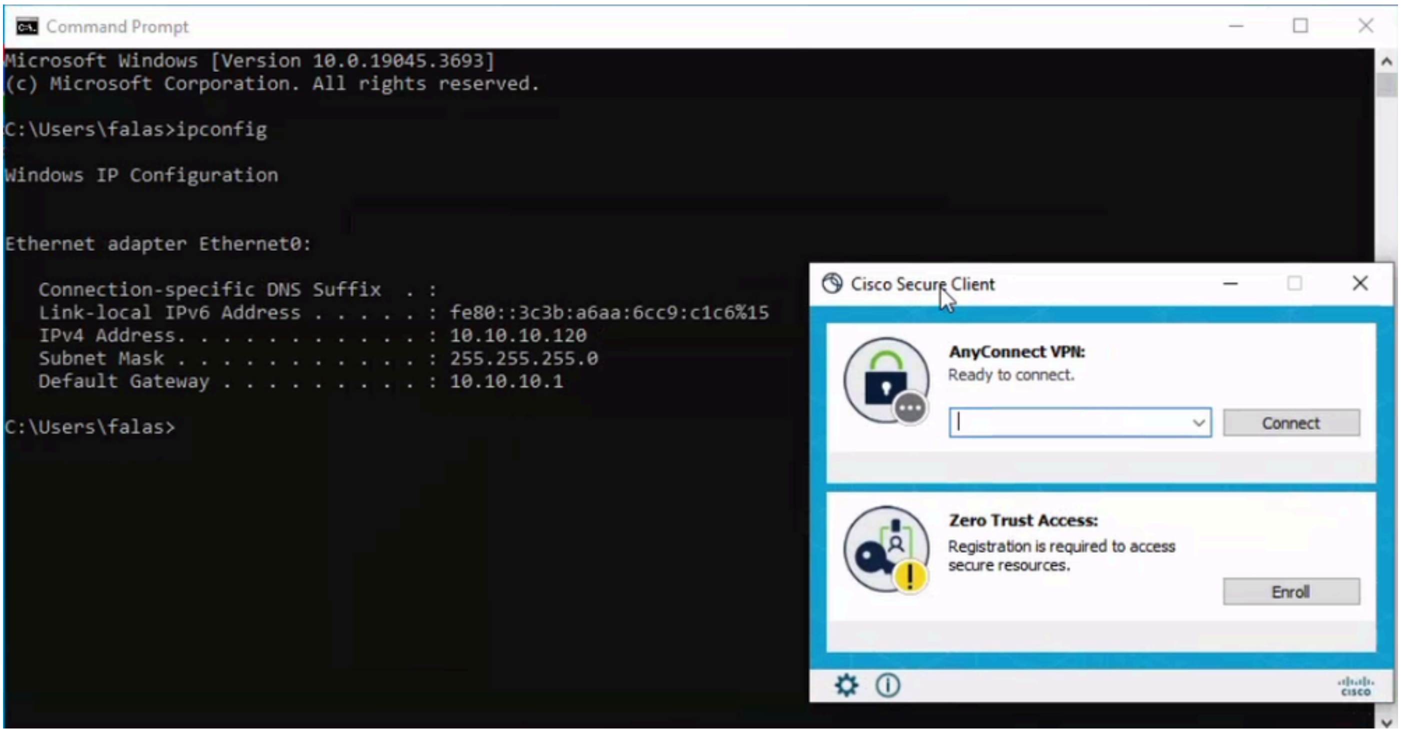
Categories
Uncategorized
Dispute Categorization

Secure Access - Activity Search - RA-VPN

You are able to see the user was allowed to authenticate through RA-VPN.

Client-Base ZTNA

Login through Cisco Secure Client Agent - ZTNA.



Command Prompt

```
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>
```

Cisco Secure Client

AnyConnect VPN:
Ready to connect.

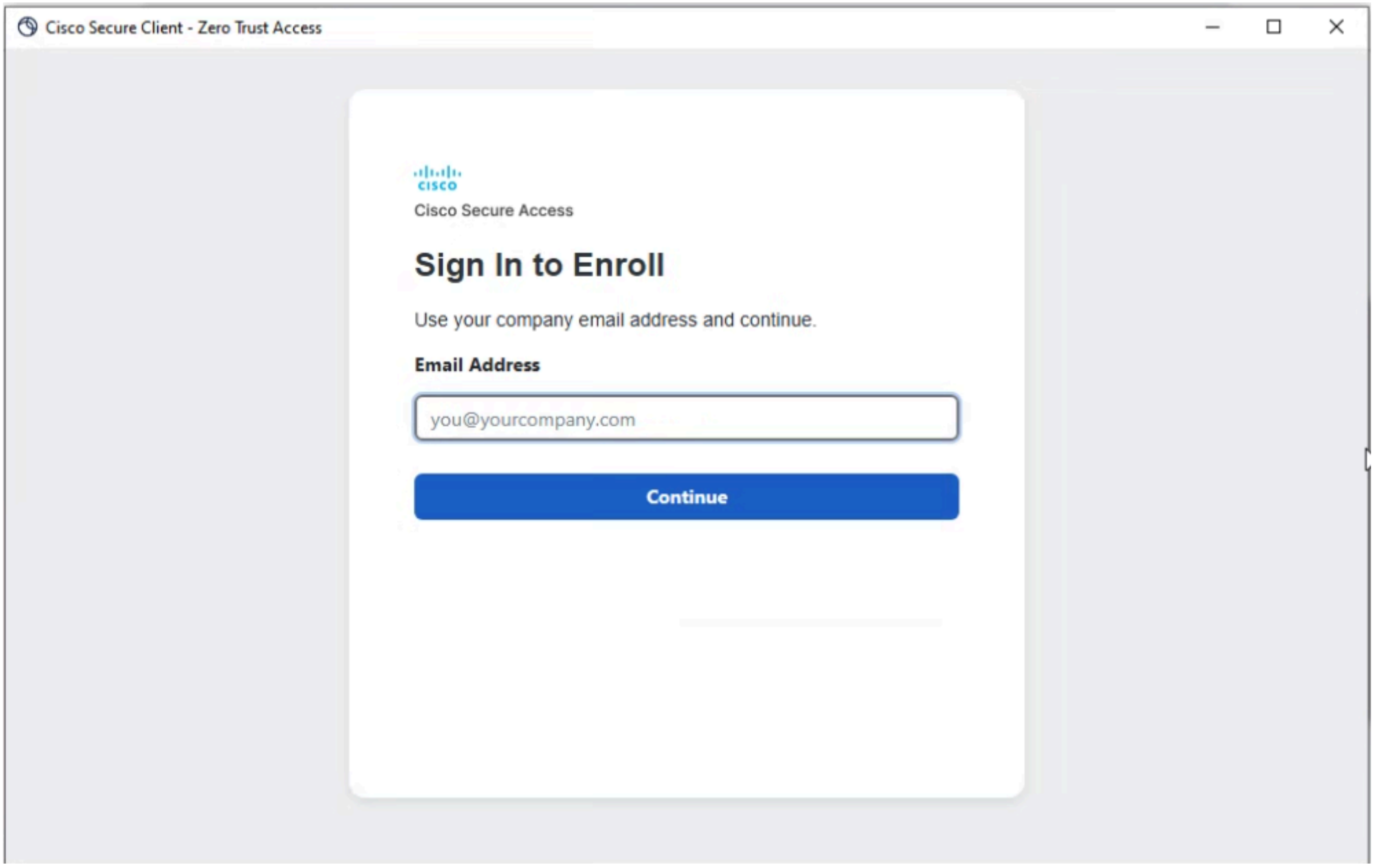
Connect

Zero Trust Access:
Registration is required to access secure resources.

Enroll

Secure Client - ZTNA

- Enroll with your username.



Cisco Secure Client - Zero Trust Access

Cisco Secure Access

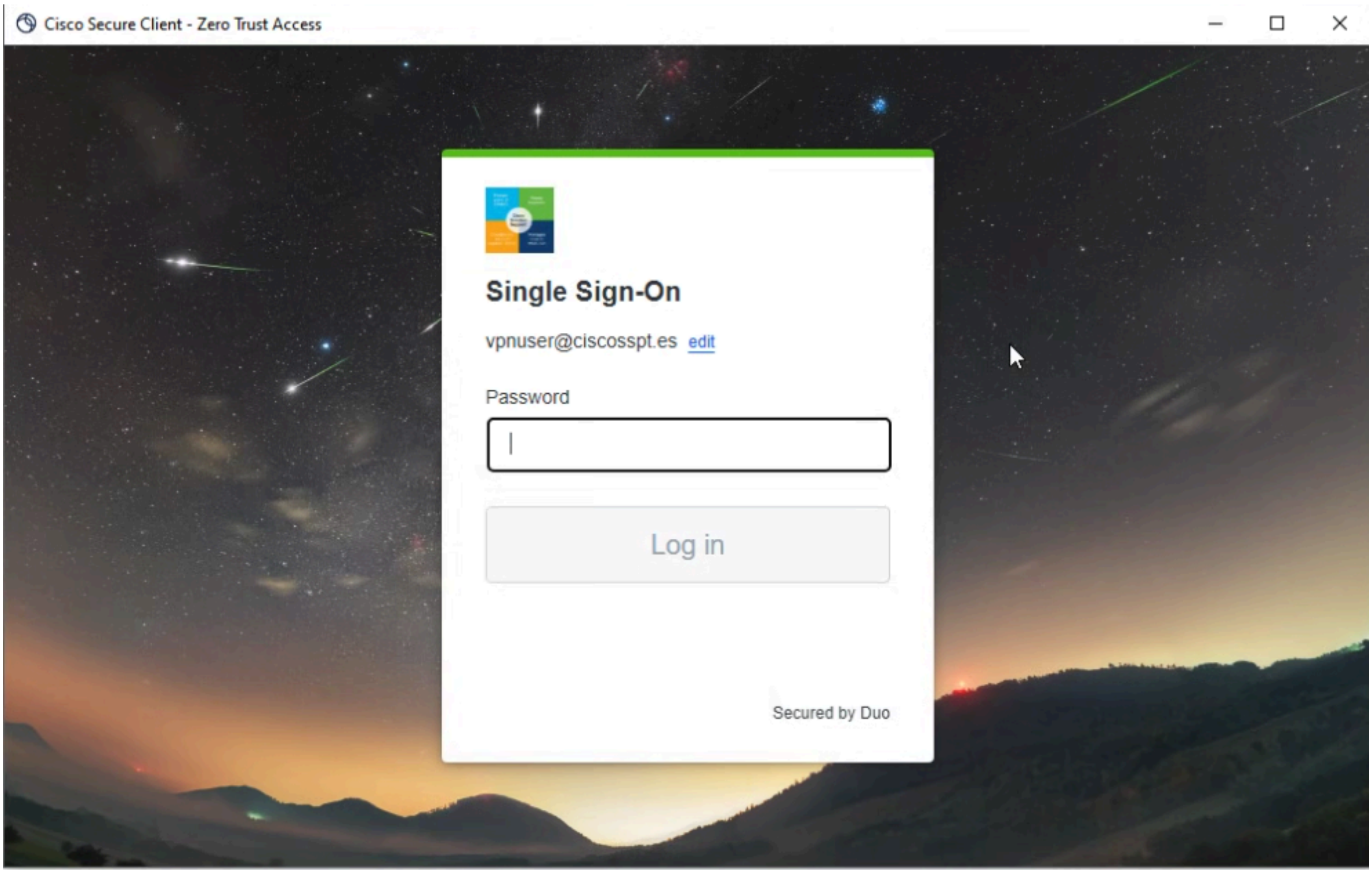
Sign In to Enroll

Use your company email address and continue.

Email Address: you@yourcompany.com

Secure Client - ZTNA - Enroll

- Authenticate in your SSO Provider



Cisco Secure Client - Zero Trust Access

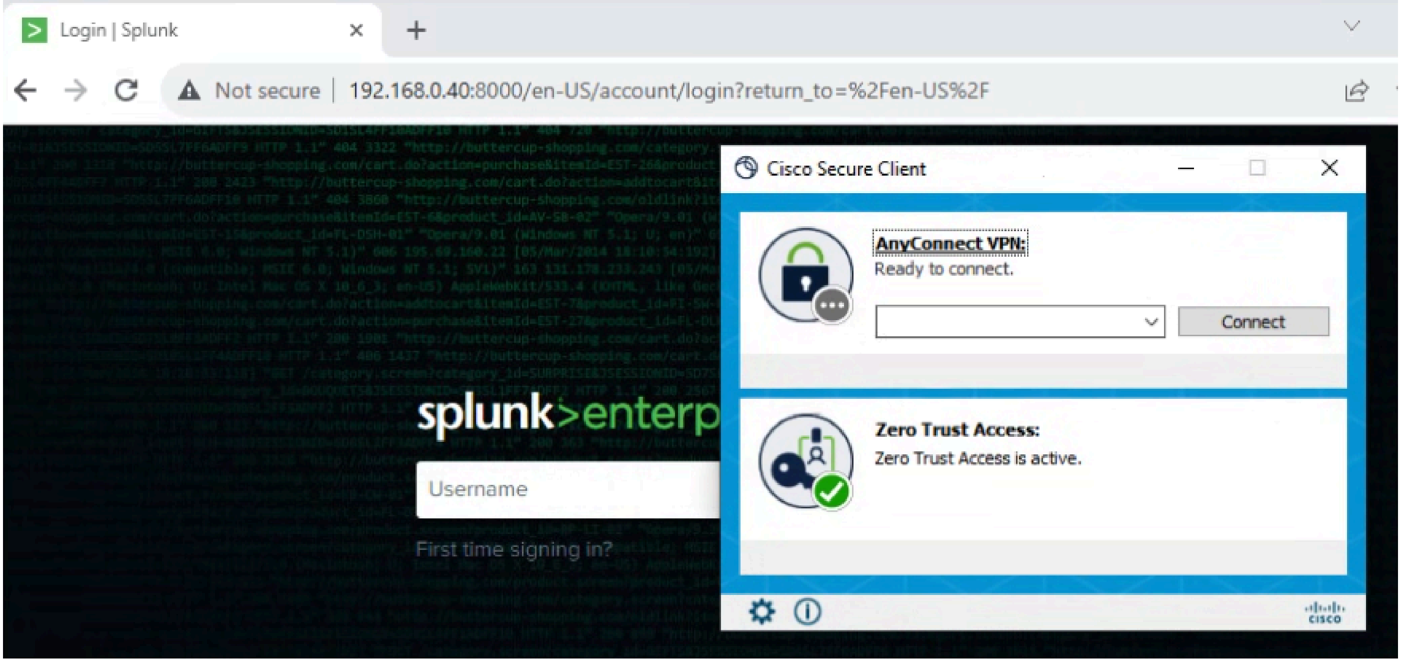
Single Sign-On

vpnuser@ciscosspt.es edit

Password:

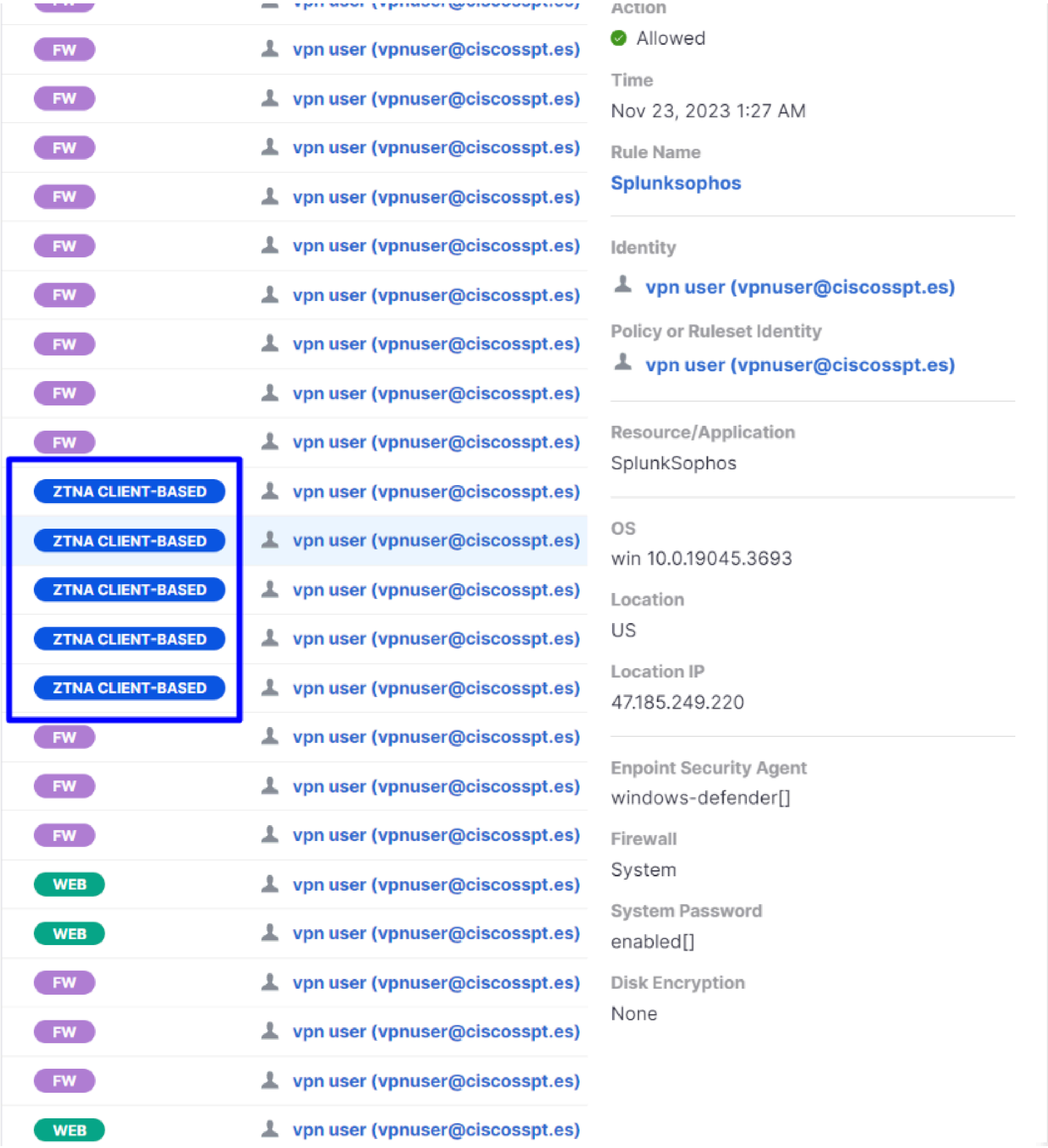
Secure Client - ZTNA - SSO Login

- After you get authenticated, access to the resource:



Secure Access - ZTNA - Logged

Navigate to Monitor > Activity Search:



FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)
ZTNA CLIENT-BASED	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)
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)

Action
● Allowed

Time
Nov 23, 2023 1:27 AM

Rule Name
Splunksophos

Identity
vpn user (vpnuser@ciscosspt.es)

Policy or Ruleset Identity
vpn user (vpnuser@ciscosspt.es)

Resource/Application
SplunkSophos

OS
win 10.0.19045.3693

Location
US

Location IP
47.185.249.220

Enpoint Security Agent
windows-defender[]

Firewall
System

System Password
enabled[]

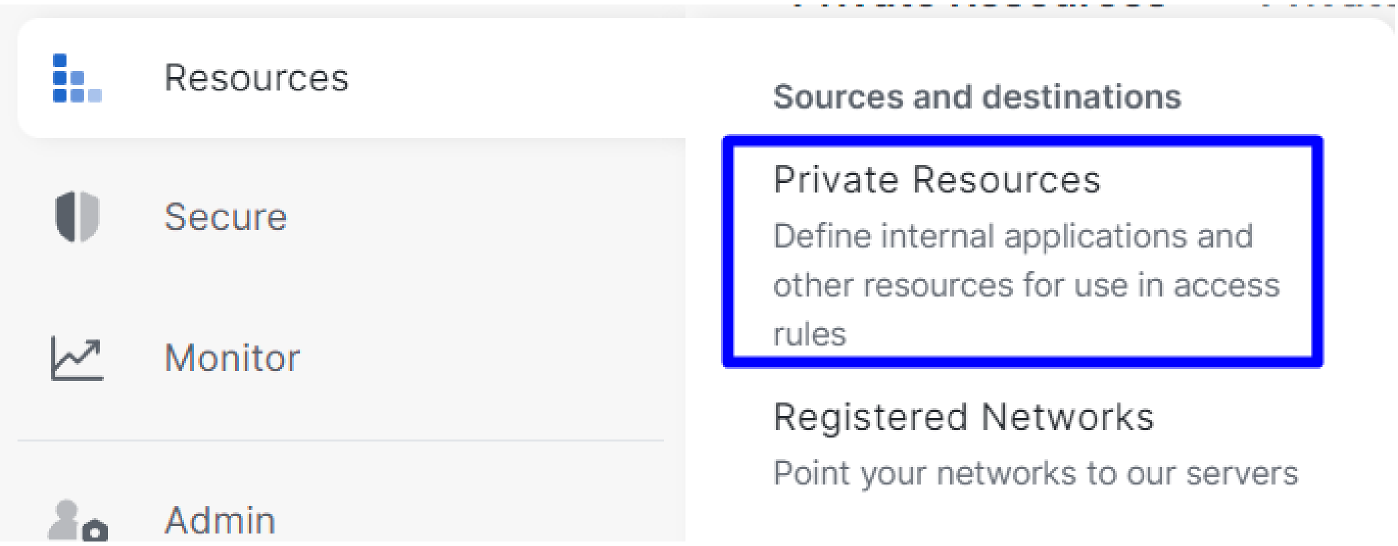
Disk Encryption
None

Secure Access - Activity Search - ZTNA Client-Based

You are able to see the user was allowed to authenticate through client-based ZTNA.

Browser-based ZTNA

In order to get the URL, you need to go to **Resources** > **Private Resources**.



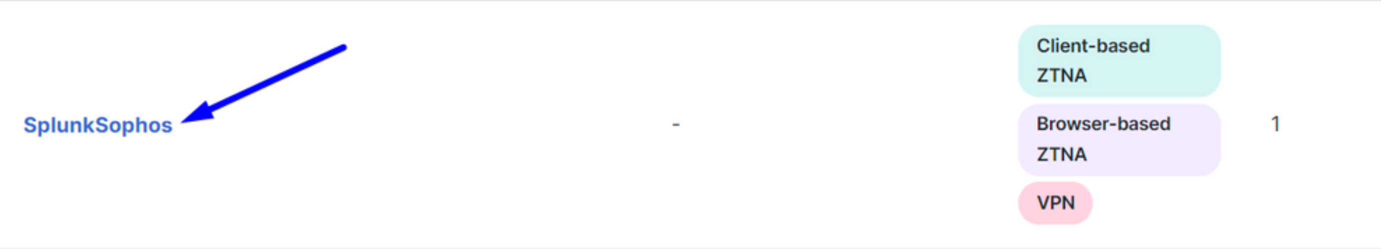
Sources and destinations

Private Resources
Define internal applications and other resources for use in access rules

Registered Networks
Point your networks to our servers

Secure Access - Private Resource

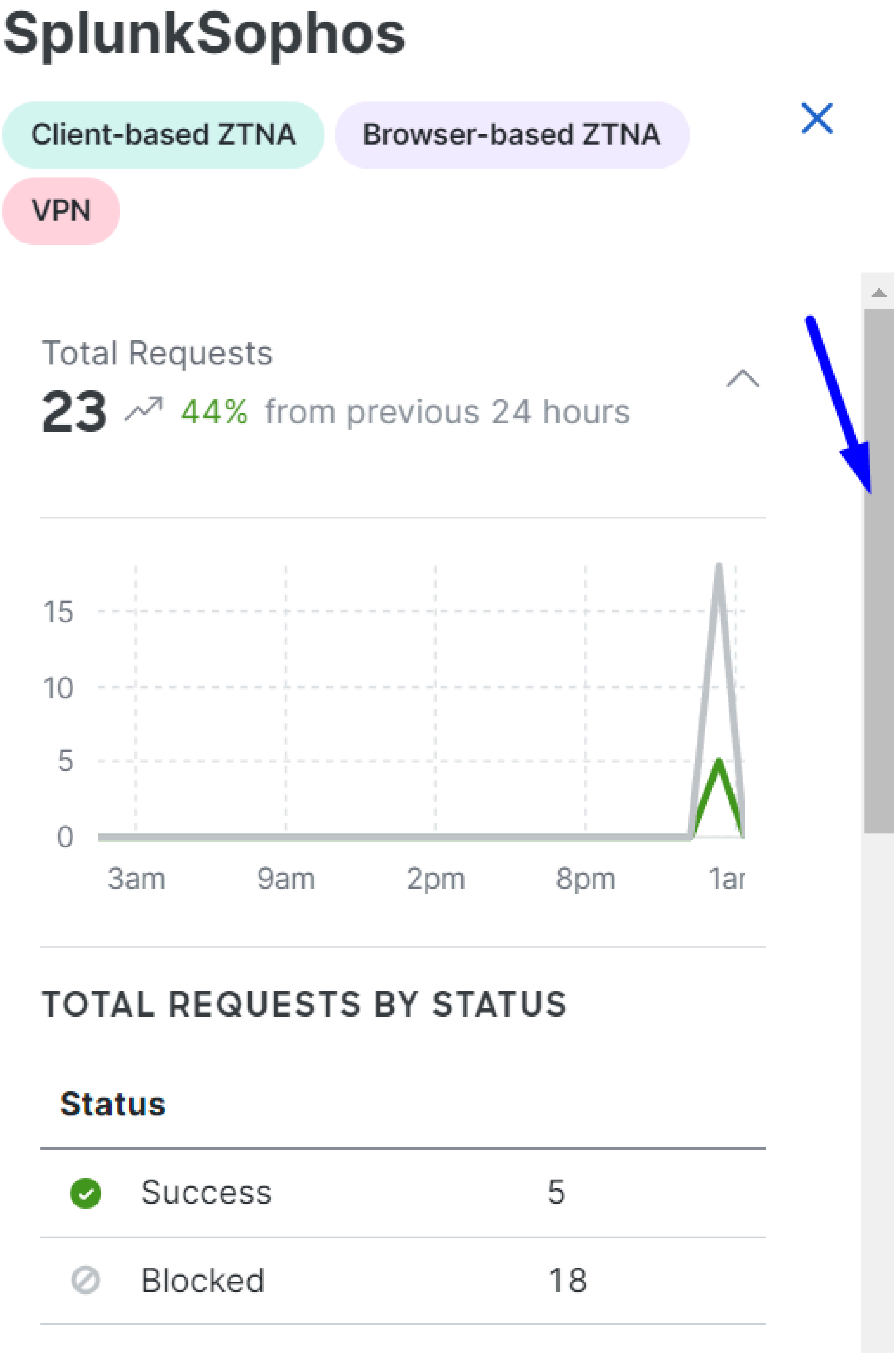
- Click on your Policy



SplunkSophos	-	Client-based ZTNA Browser-based ZTNA VPN	1

Secure Access - Private Resource - SplunkSophos

- Scroll down



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

Secure Access - Private Resource - Scroll Down