

# Configurazione di Secure Access con Sophos XG Firewall

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione del tunnel su accesso sicuro](#)

[Dati tunnel](#)

[Configurazione del tunnel su Sophos](#)

[Configura profilo IPsec](#)

[Configura VPN da sito a sito](#)

[Configura interfaccia tunnel](#)

[Configurazione dei gateway](#)

[Configurazione del router SD-WAN](#)

[Configura app privata](#)

[Configurare i criteri di accesso](#)

[Verifica](#)

[RA-VPN](#)

[ZTNA basata su client](#)

[ZTNA basata su browser](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare Secure Access con Sophos XG Firewall.

## Prerequisiti

- [Configura assegnazione ruoli utente](#)
- [Configurazione autenticazione SSO ZTNA](#)
- [Configura accesso sicuro VPN di accesso remoto](#)

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Sophos XG Firewall
- Accesso sicuro

- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

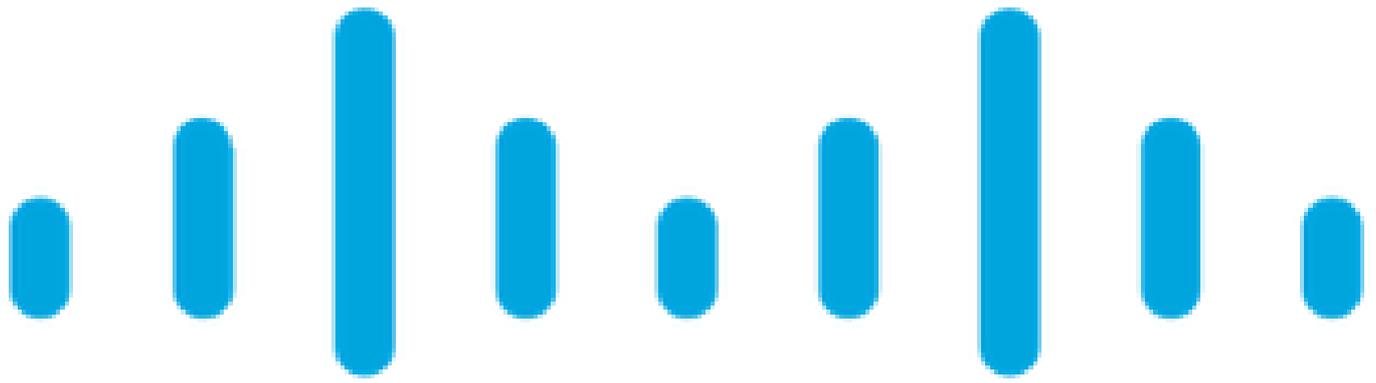
## Componenti usati

Le informazioni fornite in questo documento si basano su:

- Sophos XG Firewall
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse



**CISCO**

Secure

Access

**SOPHOS**

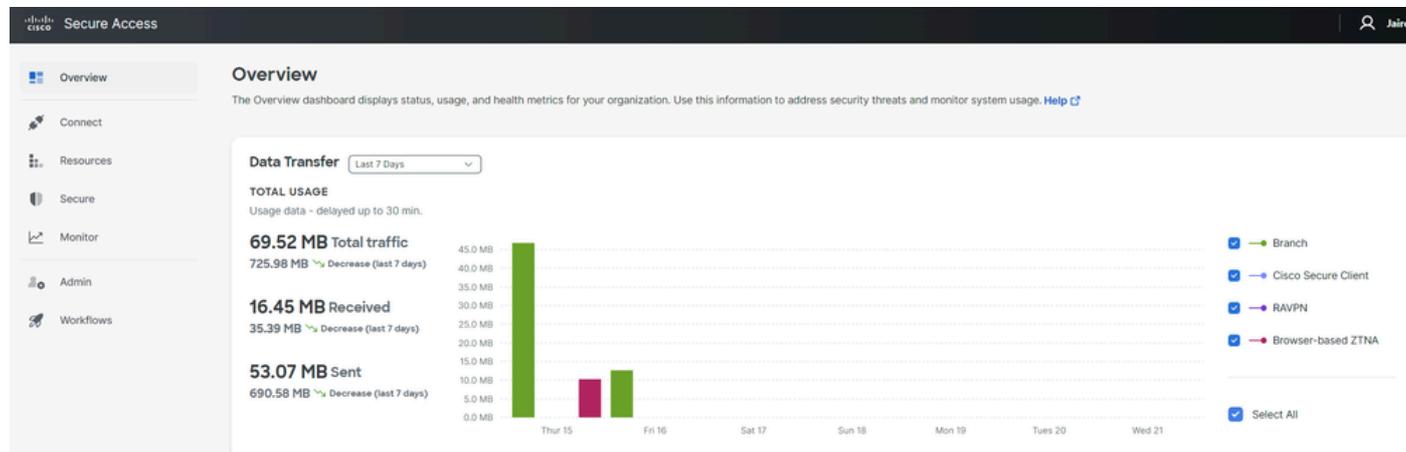
Secure Access - Sophos

Cisco ha progettato Secure Access per garantire la protezione e la fornitura dell'accesso alle applicazioni private, sia in sede che basate su cloud. Inoltre, garantisce il collegamento dalla rete a Internet. Questo risultato è ottenuto attraverso l'implementazione di più metodi e livelli di sicurezza, il tutto finalizzato a preservare le informazioni mentre vi accedono tramite il cloud.

# Configurazione

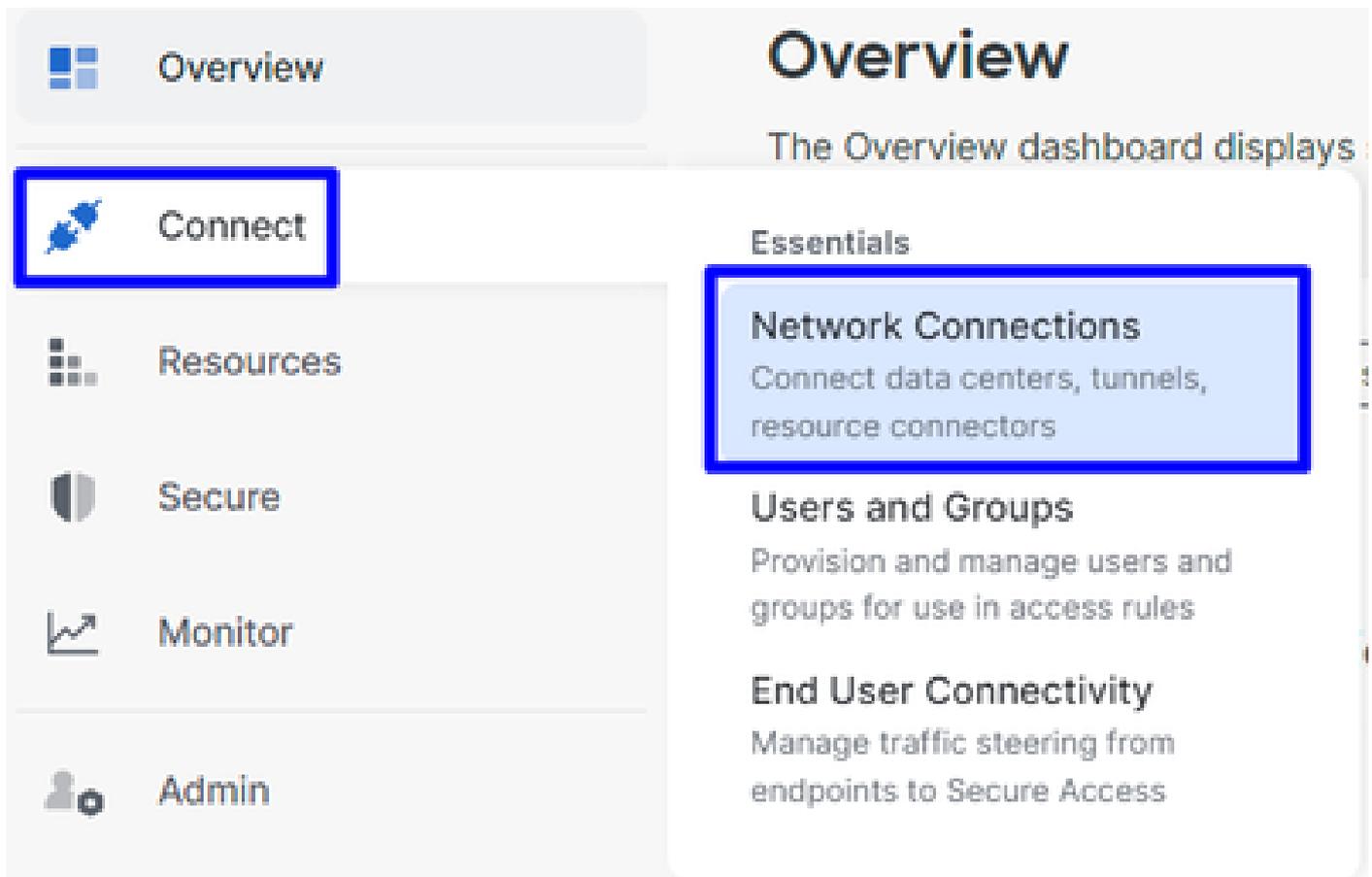
## Configurazione del tunnel su accesso sicuro

Passare al pannello di amministrazione di [Accesso sicuro](#).



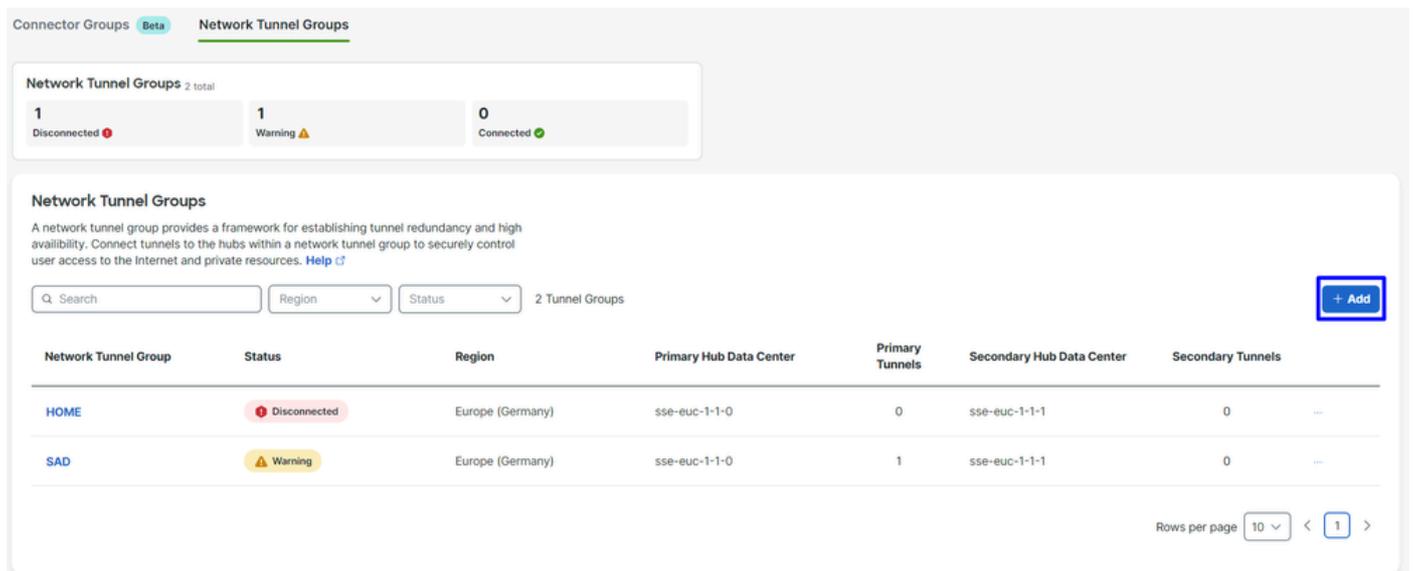
Secure Access - Pagina principale

- Fare clic su **Connect > Network Connections**.



Accesso sicuro - Connessioni di rete

- In fareNetwork Tunnel Groups clic su + Add.



Accesso sicuro - Gruppi di tunnel di rete

- Configurare Tunnel Group Name, Region e Device Type.
- Fare clic su . 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](#)



**Nota:** scegliere la regione più vicina alla posizione del firewall.

- 
- Configurare Tunnel ID Format e Passphrase.
  - Fare clic su .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

Accesso sicuro - Gruppi di tunnel - ID tunnel e passphrase

- Configurare gli intervalli di indirizzi IP o gli host configurati nella rete e che si desidera passare il traffico attraverso l'accesso sicuro.
- Fare clic su **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

Accesso sicuro - Gruppi di tunnel - Opzioni di routing

Dopo aver fatto clic sulle informazioni **Save** del tunnel che vengono visualizzate, salvare le informazioni per il passaggio successivo, **Configure the tunnel on Sophos**.

Dati tunnel

## 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.

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

[Download CSV](#)

[Done](#)

*Accesso sicuro - Gruppi di tunnel - Ripresa della configurazione*

Configurazione del tunnel su Sophos

Configura profilo IPsec

Per configurare il profilo IPsec, passare al firewall Sophos XG.

Si ottiene qualcosa di simile al seguente:

**SOPHOS** Sophos Firewall

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

User & device insights

Security Heartbeat®: 0 At risk

Synchronized Application Control™: 0 Apps

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

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)

High availability: Not configured

Click on widgets to open details

Sophos - Pannello di amministrazione

- Passa a Profiles
- Fare clic su **IPsec Profiles** e quindi su Add

IPsec profiles

Device access

Add

Delete

algorithm

Phase 2

Manage

In **General Settings** Configura:

- **Name:** nome di riferimento ai criteri di accesso sicuro Cisco
- **Key Exchange:** IKEv2
- **Authentication Mode:** Modalità principale
- **Key Negotiation Tries:**0
- **Re-Key connection:** selezionare l'opzione

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 - Profili IPsec - Impostazioni generali

In **Phase 1** Configura:

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

## Phase 1

Key life 28800 <input type="checkbox"/>	Re-key margin 360 <input type="checkbox"/>	Randomize re-keying margin by 50 <input type="checkbox"/>
Seconds		
DH group (key group) 2 selected <input type="checkbox"/>		
Encryption AES256 <input type="checkbox"/>	Authentication SHA2 256 <input type="checkbox"/>	
+ You can add up to 3 different algorithm combinations		

*Sophos - Profili IPsec - Fase 1*

In **Phase 2** Configura:

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

## Phase 2

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

*Sophos - Profili IPsec - Fase 2*

In **Dead Peer Detection** Configura:

- **Dead Peer Detection:** selezionare l'opzione
- **Check peer after every:**10
- **Wait for response up to:** 120 (predefinito)
- **When peer unreachable:** riavvio (predefinito)

## 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 - Profili IPsec - Rilevamento peer inattivi*

Dopodiché, fate clic su **Save** and proceed with the next step, Configure Site-to-site VPN.

Configura VPN da sito a sito

Per avviare la configurazione della VPN, fare clic su **Site-to-site VPN** e su **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

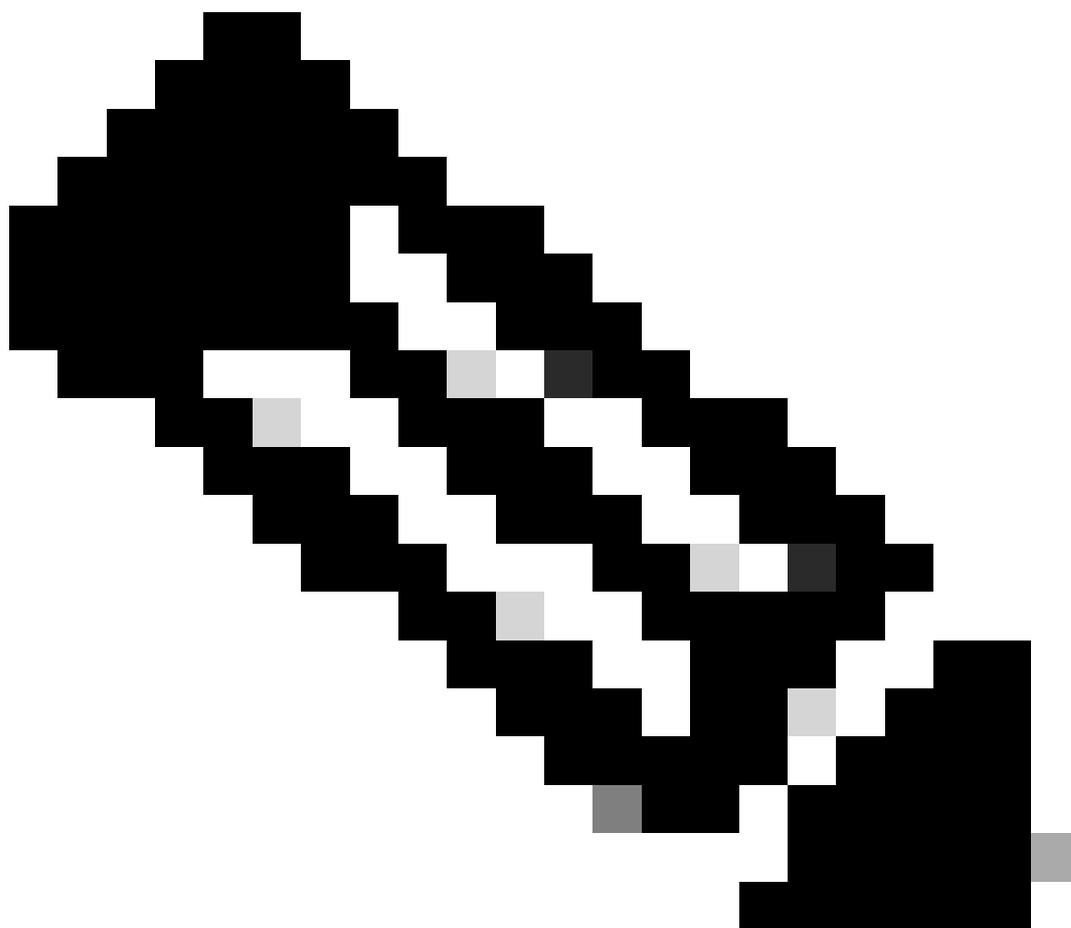
Add Delete Wizard

Add Delete

*Sophos - VPN da sito a sito*

In **General Settings** Configura:

- **Name:** nome di riferimento al criterio IPsec di Cisco Secure Access
- IP version: IPv4
- Connection type: Interfaccia tunnel
- Gateway type: avvia la connessione
- Active on save: selezionare l'opzione



**Nota:** l'opzione **Active on save** abilita la VPN automaticamente dopo la configurazione della VPN da sito a sito.

---

## General settings

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

Sophos - VPN da sito a sito - Impostazioni generali

**Nota:** l'opzione Tunnel interface (interfaccia tunnel) crea un'interfaccia tunnel virtuale per il firewall Sophos XG con il nome XFRM.

In **Encryption** Configura:

- **Profile:** il profilo creato sulla fase, **Configure IPsec Profile**
- **Authentication type:** chiave già condivisa
- **Preshared key:** il campo che si configura nella fase, [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 da sito a sito - Crittografia

In **Gateway Settings** Configura opzioni Local Gateway Remote Gateway utilizzare questa tabella come riferimento.

Gateway locale	Gateway remoto
Interfaccia di ascolto Interfaccia Wan-Internet	Indirizzo gateway L'indirizzo IP pubblico generato nella fase, <a href="#">Tunnel Data</a>
Tipo ID locale Email	Tipo ID remoto

	Indirizzo IP
ID locale L'e-mail generata nella fase, <a href="#">Tunnel Data</a>	ID remoto L'indirizzo IP pubblico generato nella fase, <a href="#">Tunnel Data</a>
Subnet locale Qualsiasi	Subnet remota Qualsiasi

## Gateway settings

Local gateway	Remote gateway
<b>Listening interface</b> <input type="text" value="PortB - 192.168.0.33"/>	<b>Gateway address</b> <input type="text" value="18.156.145.74"/>
<b>Local ID type</b> <input type="text" value="Email"/>	<b>Remote ID type</b> <input type="text" value="IP address"/>
<b>Local ID</b> <input type="text" value="csasophos@"/> <input type="text" value="-sse.cisco.com"/>	<b>Remote ID</b> <input type="text" value="18.156.145.74"/>
<b>Local subnet</b> <input type="text" value="Any"/>	<b>Remote subnet</b> <input type="text" value="Any"/>
<a href="#">Add new item</a>	<a href="#">Add new item</a>

Sophos - VPN da sito a sito - Impostazioni gateway

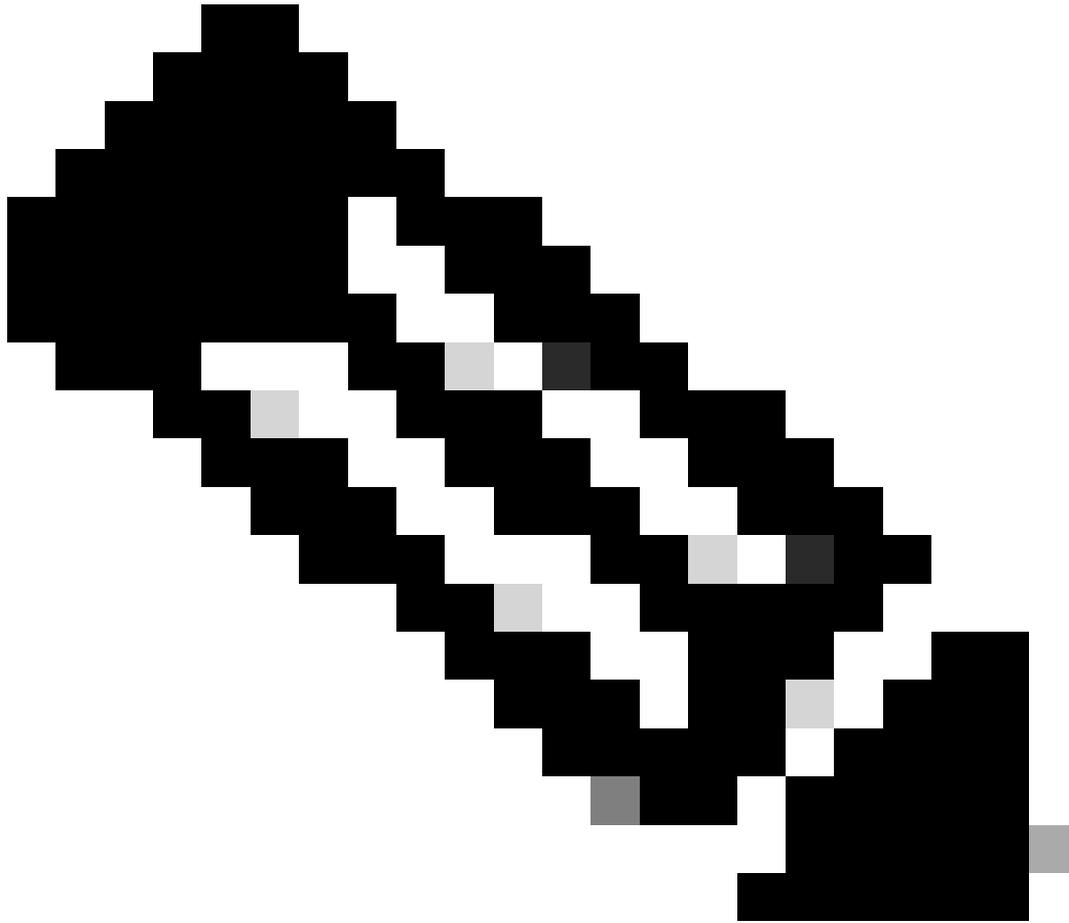
Dopodiché, fare clic su **Save**, e si può vedere che il tunnel è stato creato.

### IPsec connections

[Show additional properties](#) [Add](#) [Delete](#) [Wizard](#)

Name	Group name	Profile	Connection type	Status	Connection	Manage
<input type="checkbox"/> <a href="#">SecureAccesS</a>	-	CSA	Tunnel interface	Active	<input type="checkbox"/>	<a href="#">i</a> <a href="#">edit</a> <a href="#">stop</a> <a href="#">delete</a>

Sophos - VPN da sito a sito - Connessioni IPsec



**Nota:** per verificare se il tunnel è stato abilitato correttamente sull'ultima immagine, è possibile controllare **Connection** lo stato. Se il colore è verde, il tunnel è connesso se non è verde e il tunnel non è connesso.

---

Per verificare se è stato stabilito un tunnel, passare a **Current Activities > IPsec Connections**.

MONITOR & ANALYZE

# Control center

Current activities

Reports

Zero-day protection

Diagnostics

*Sophos - Monitoraggio e analisi - IPsec*

Live users	Live connections	Live connections IPv6	IPsec connections	Remote users			
<b>No tunnel established to Secure Access</b>							
<input type="checkbox"/>	Name ▾	Local server ▾	Local subnet ▾	Username ▾	Remote server/host ▾	Remote subnet ▾	Manage
No records found							
<b>Tunnel established to Secure Access</b>							
<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 - Monitoraggio e analisi - IPsec prima e dopo*

Dopo di che, possiamo continuare con il passo, **Configure Tunnel Interface Gateway**.

Configura interfaccia tunnel

Individuare l'interfaccia configurata sulla VPN **Network** e controllarla perWAN modificare l'interfaccia del tunnel virtuale con il nome xfrm.

- Fare clic su nell'**xfrm** interfaccia.



Sophos - Rete - Interfaccia tunnel

- Configurare l'interfaccia con un IP non instradabile nella rete. Ad esempio, è possibile usare 169.254.x.x/30 che è un IP in uno spazio non instradabile. In genere, nell'esempio riportato viene usato 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 - Rete - Interfaccia tunnel - Configurazione

#### Configurazione dei gateway

Per configurare il gateway per l'interfaccia virtuale (xfrm)

- Passa a Routing > Gateways
- Fare clic su Add

SD-WAN routes SD-WAN profiles **Gateways** Static routes BGP OSPF OSPFv3 Information Upstream proxy ...

IPv4 gateway

<input type="checkbox"/>	Name ▾	IP address ▾	Interface ▾	Health check ▾	Status ▾	Manage
<input type="checkbox"/>	<u>DHCP_PortB_GW</u>	192.168.0.1	WAN	On	●	

IPv6 gateway

Sophos - Routing - Gateway

In **Gateway host** Configura:

- **Name:** nome che fa riferimento all'interfaccia virtuale creata per la VPN
- **Gateway IP:** nel nostro caso 169.254.0.2, ossia l'IP sotto la rete 169.254.0.1/30 che già abbiamo assegnato sotto la fase, Configure Tunnel Interface
- Interface: Interfaccia virtuale VPN
- **Zone:** Nessuno (predefinito)

## Gateway host

Name \*

Gateway IP

Interface

Zone

Sophos - Routing - Gateway - Host gateway

- Sotto **Health check** disattiva controllo
- Fare clic su **Save**

# Health check

Health check



*Sophos - Routing - Gateway - Controllo dello stato*

Dopo aver salvato la configurazione, è possibile osservare lo stato del gateway:

## 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		

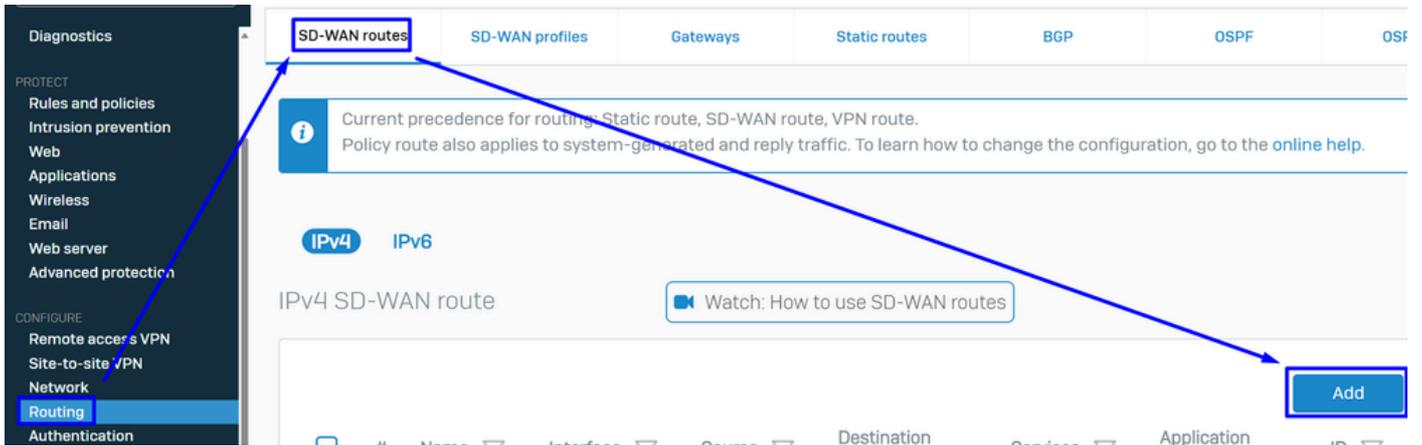
*Sophos - Routing - Gateway - Stato*

## Configurazione del router SD-WAN

Per finalizzare il processo di configurazione, è necessario creare il percorso che consente di inoltrare il traffico a Secure Access.

Passa a **Routing > SD-WAN routes**.

- Fare clic su **Add**



Sophos - Router SD-Wan

### In Traffic Selector Configura:

- Incoming interface: selezionare l'interfaccia da cui inviare il traffico o gli utenti che accedono da RA-VPN, ZTNA o Clientless-ZTNA
- DSCP marking: nessuna informazione per questo esempio
- **Source networks:** selezionare l'indirizzo che si desidera indirizzare attraverso il tunnel
- **Destination networks:** qualsiasi o è possibile specificare una destinazione
- **Services:** qualsiasi o è possibile specificare i servizi
- **Application object:** applicazione se l'oggetto è stato configurato
- User or groups: se si desidera aggiungere un gruppo specifico di utenti per indirizzare il traffico ad Accesso sicuro

### 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

Each field has an "Add new item" button below it.

Sophos - Route SD-Wan - Selettore traffico

### In Link selection settings Configurazione gateway:

- Primary and Backup gateways: selezionare l'opzione

- **Primary gateway:** selezionare il gateway configurato nella fase, [Configure the Gateways](#)
- Fare clic su **Save**

Link selection settings

Select SD-WAN profile ⓘ  Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

*Sophos - Route SD-Wan - Selettore traffico - Gateway principali e di backup*

Dopo aver finalizzato la configurazione sul Sophos XG Firewall, è possibile procedere con la procedura, **Configure Private App**.

Configura app privata

Per configurare l'accesso all'app privata, accedere al [portale](#) di [amministrazione](#).

- Passa a **Resources > Private Resources**

Accesso sicuro - Risorse private

- Fare clic su + Add

Accesso sicuro - Risorse private 2

- In **General** Configurazione **Private Resource Name**

## General

### Private Resource Name

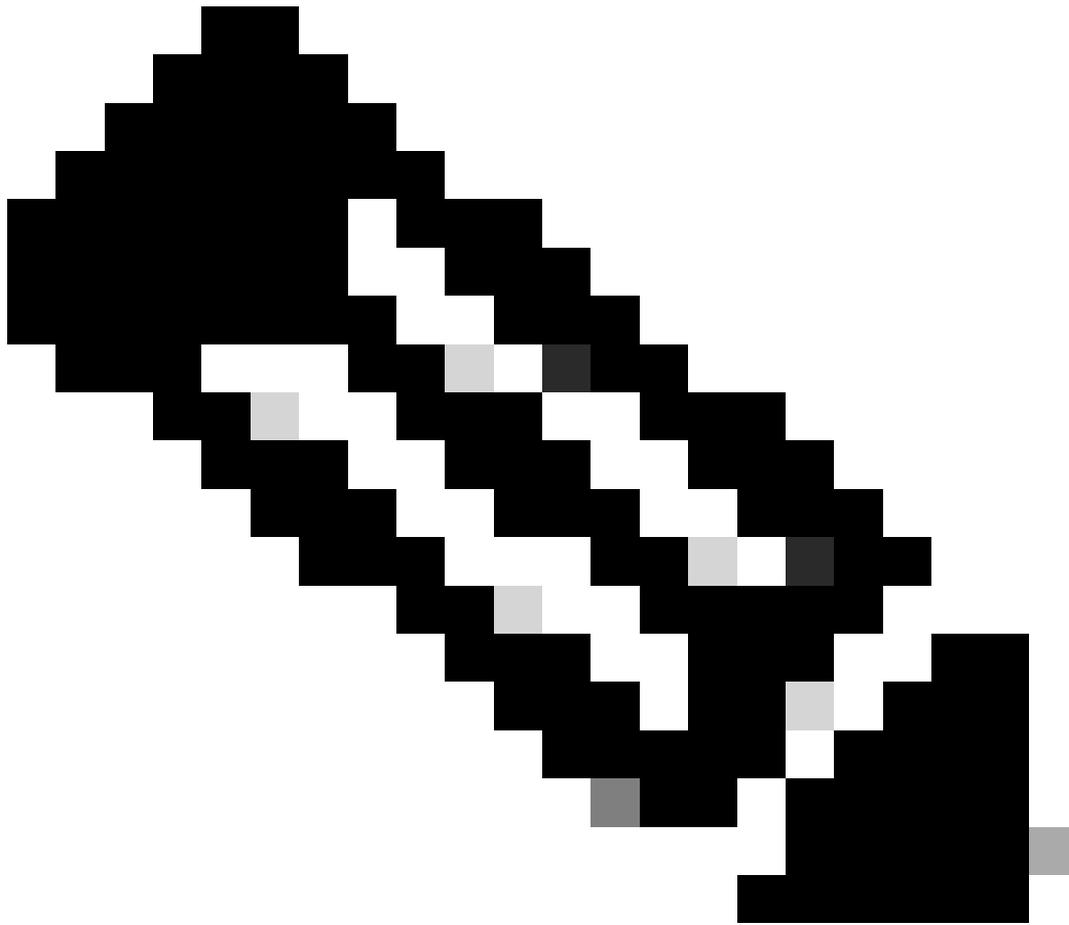
SplunkSophos

### Description (optional)

*Accesso sicuro - Risorse private - Generale*

In **Communication with Secure Access Cloud** Configura:

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: selezionare la risorsa a cui si desidera accedere



**Nota:** ricordare che l'indirizzo raggiungibile internamente è stato assegnato nella fase, [Configure the Tunnel on Secure Access](#).

- 
- **Protocol:** selezionare il protocollo da utilizzare per accedere alla risorsa
  - **Port / Ranges :** selezionare le porte da abilitare per accedere all'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

### Accesso sicuro - Risorse private - Comunicazioni con Secure Access Cloud

All'interno **Endpoint Connection Methods** di è possibile configurare tutte le modalità di accesso alle risorse private tramite Secure Access e scegliere i metodi che si desidera utilizzare per l'ambiente:

- **Zero-trust connections:** selezionare la casella per abilitare l'accesso ZTNA.
  - **Client-based connection:** Abilita il pulsante per consentire l'utilizzo di ZTNA di base client
    - **Remotely Reachable Address:** configurare l'indirizzo IP dell'app privata
  - **Browser-based connection:** Abilita il pulsante per consentire l'utilizzo di ZTNA basato su browser
    - **Public URL for this resource:** aggiungere un nome da utilizzare insieme al dominio `ztna.sse.cisco.com`
      - **Protocol:** scegliere HTTP o HTTPS come protocollo a cui accedere tramite il browser
- **VPN connections:** selezionare la casella per abilitare l'accesso RSA-VPN.
- Fare clic su **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

Accesso sicuro - Risorse private - Comunicazioni con Secure Access Cloud 2

Al termine della configurazione, si ottiene quanto segue:

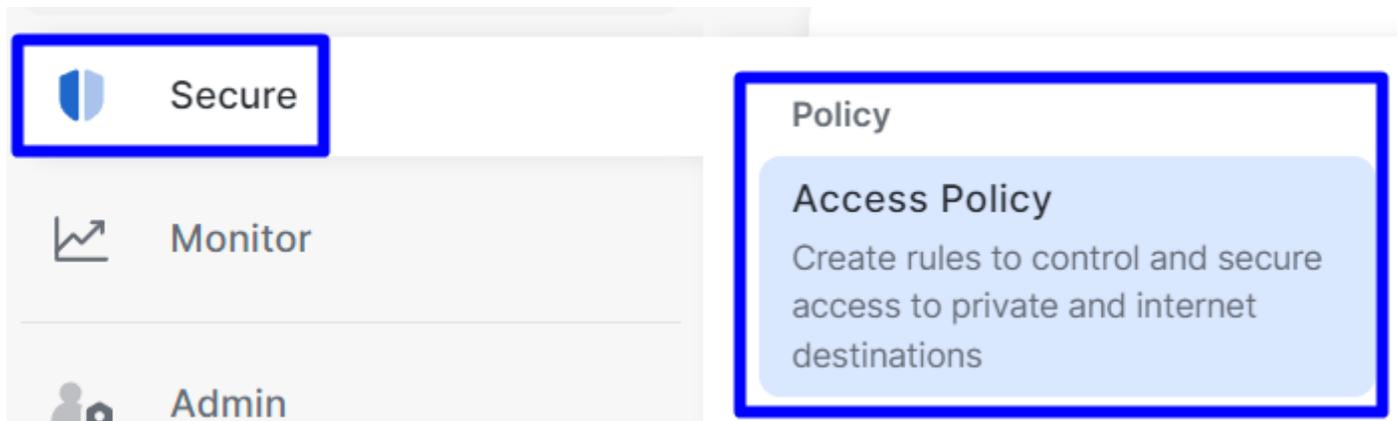
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none"><li>VPN</li><li>Browser-based ZTNA</li><li>Client-based ZTNA</li></ul>	1	2	16

Accesso sicuro - Risorse private configurate

A questo punto è possibile procedere con il passaggio, **Configure the Access Policy**.

Configurare i criteri di accesso

Per configurare i criteri di accesso, passare a Secure > Access Policy.



*Accesso sicuro - Criteri di accesso*

- Fare clic su **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

*Accesso sicuro - Criteri di accesso - Accesso privato*

Configurare le opzioni successive per consentire l'accesso tramite più metodi di autenticazione:

- 1. Specify Access
  - Action:Allow (Autorizza)
    - **Rule name:** specificare un nome per la regola di accesso
    - **From:** gli utenti a cui si concede l'accesso
    - **To:** applicazione alla quale si desidera consentire l'accesso
    - Endpoint Requirements: (predefinito)
- Fare clic su **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

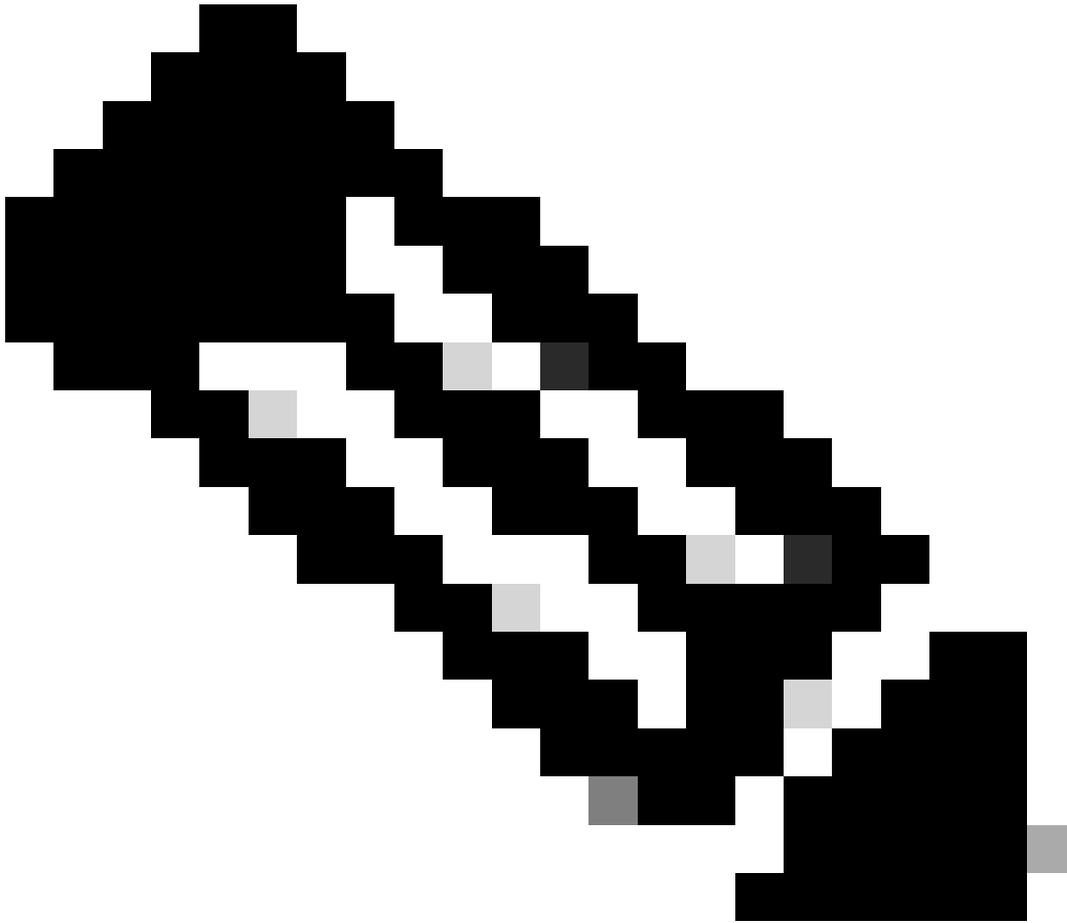
Rule Defaults

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**

Accesso sicuro - Criteri di accesso - Specifica accesso



**Nota:** per il passaggio 2, **Configure Security** in base alle esigenze, ma in questo caso non è stato abilitato il **Intrusion Prevention (IPS)**, o **Tenant Control Profile**.

- Fare clic su Save per:

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

*Accesso protetto - Criteri di accesso configurati*

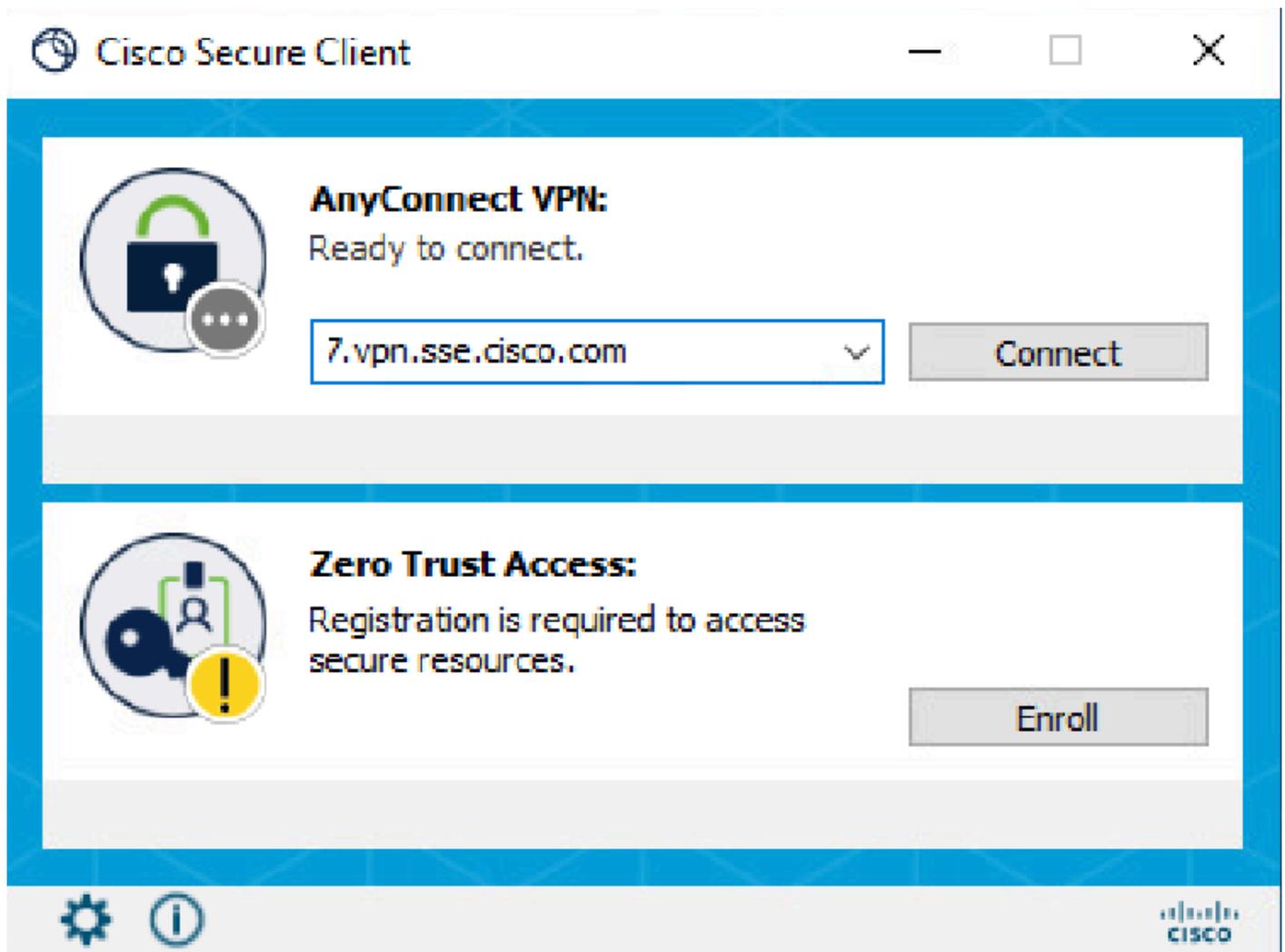
In seguito, è possibile procedere con il passaggio Verify.

Verifica

Per verificare l'accesso, è necessario aver installato l'agente di Cisco Secure Client che è possibile scaricare da [Software Download - Cisco Secure Client](#).

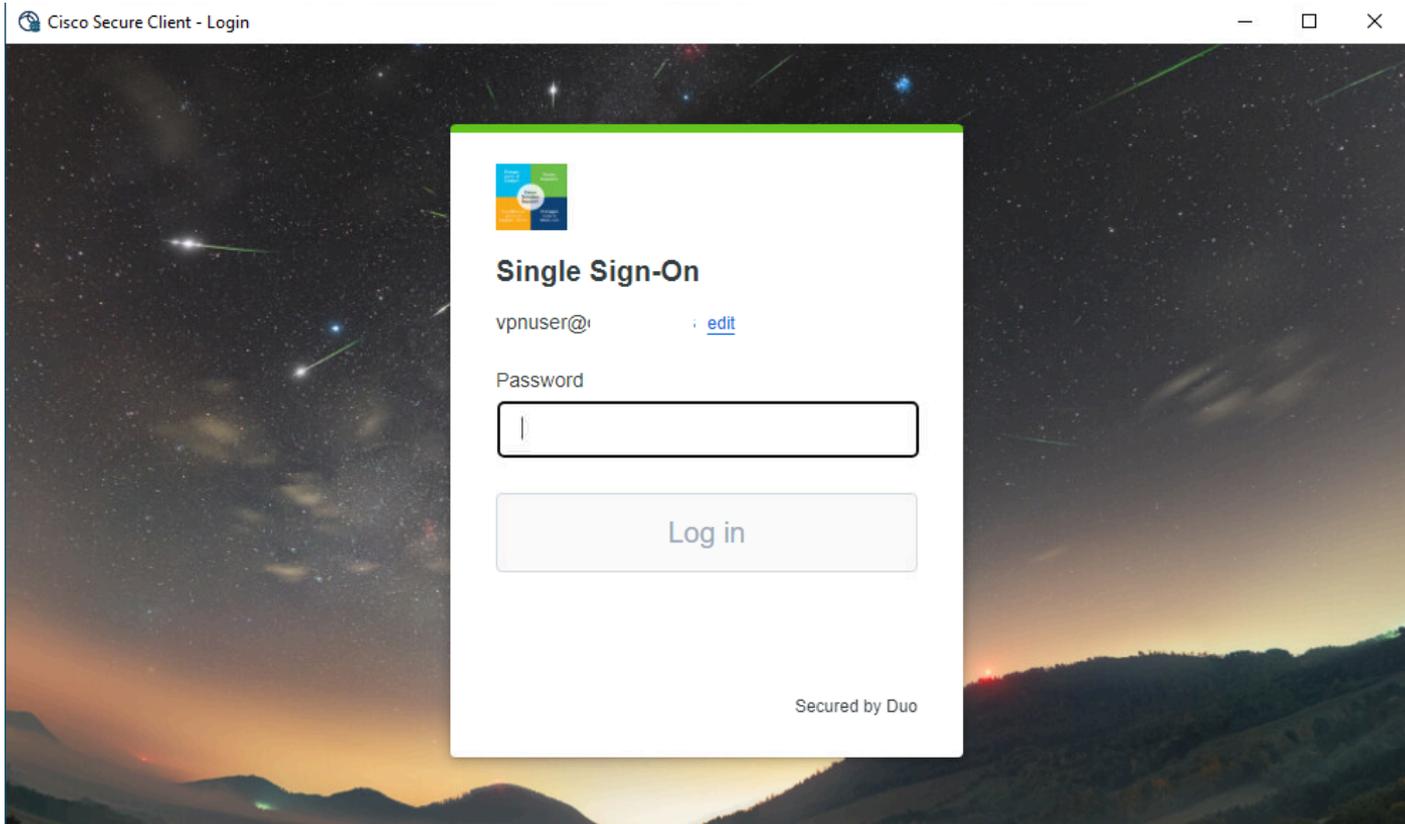
RA-VPN

Accedere tramite Cisco Secure Client Agent-VPN.



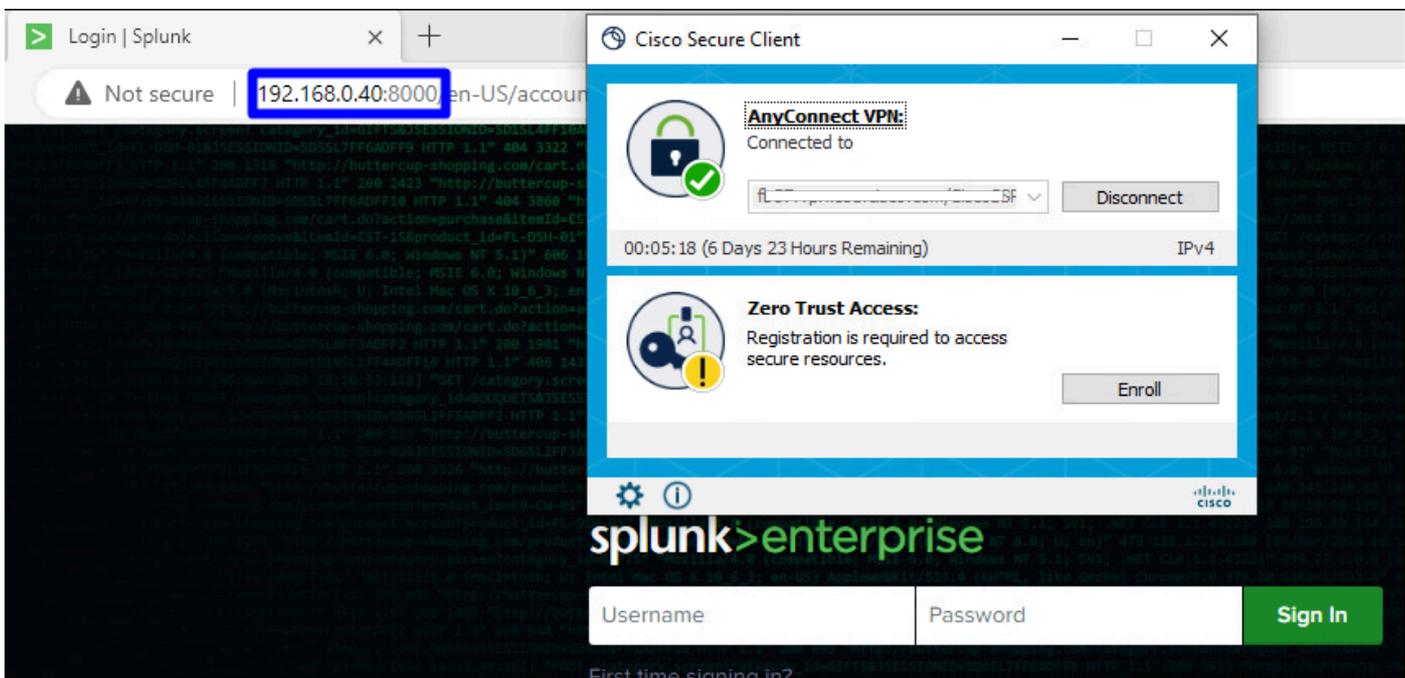
Secure Client - VPN

- Autenticazione tramite il provider SSO



Accesso sicuro - VPN - SSO

- Dopo l'autenticazione, accedere alla risorsa:



Accesso sicuro - VPN - Autenticato

Accedere a: 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@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosst.es)	vpn user (vpnuser@ciscosst.es)	192.168.0.4	...

### Event Details

Action: Allowed

Time: Nov 23, 2023 1:09 AM

Rule Name: RDP (373192)

Source: vpn user (vpnuser@ciscosst.es)

Source IP: 192.168.50.130

Destination IP: 192.168.0.40

Source Port: 50226

Destination Port: 8000

Categories: Uncategorized, Dispute Categorization

Accesso sicuro - Ricerca attività - RA-VPN

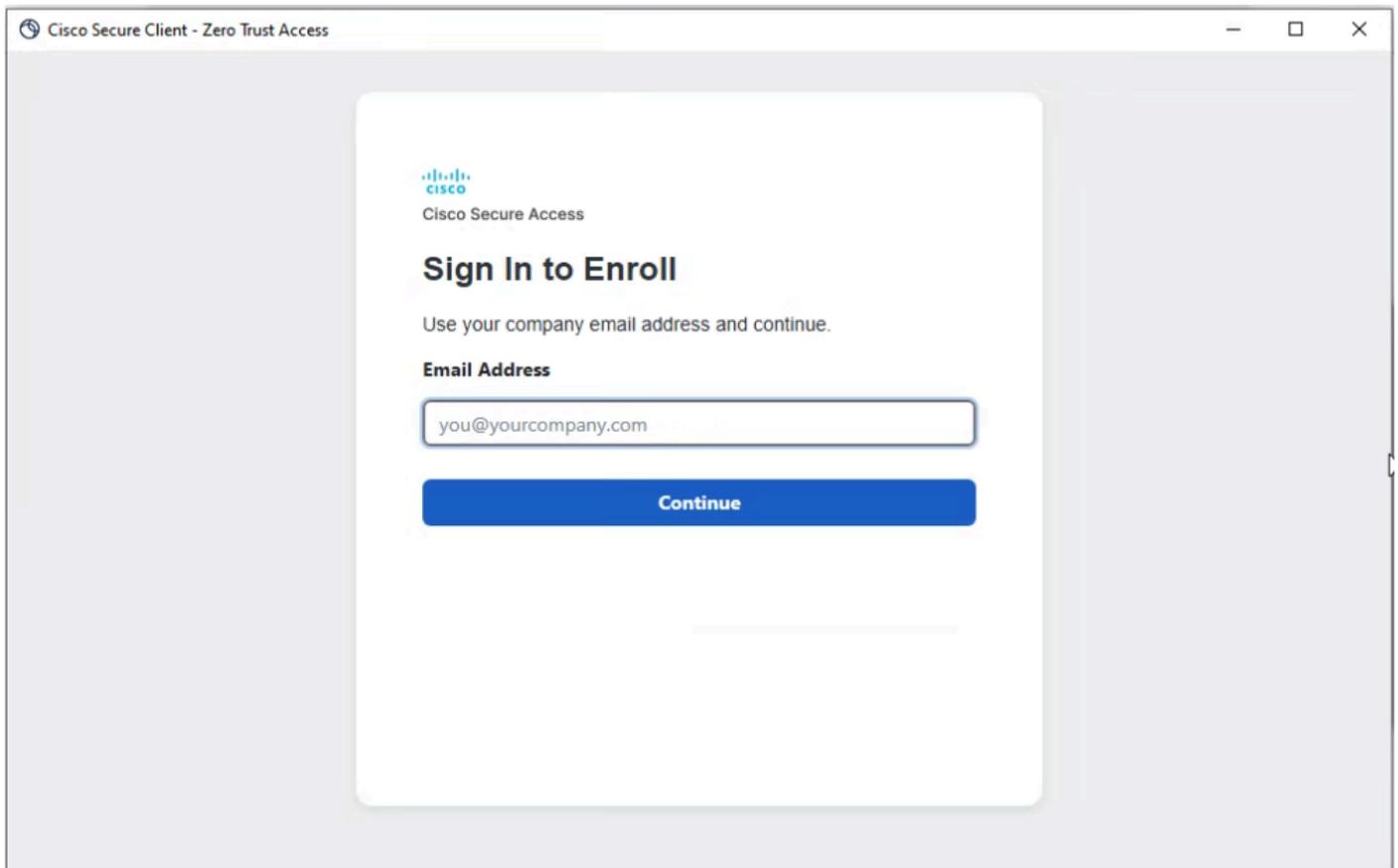
È possibile vedere che all'utente è stata consentita l'autenticazione tramite RA-VPN.

ZTNA basata su client

Accedere tramite Cisco Secure Client Agent - ZTNA.

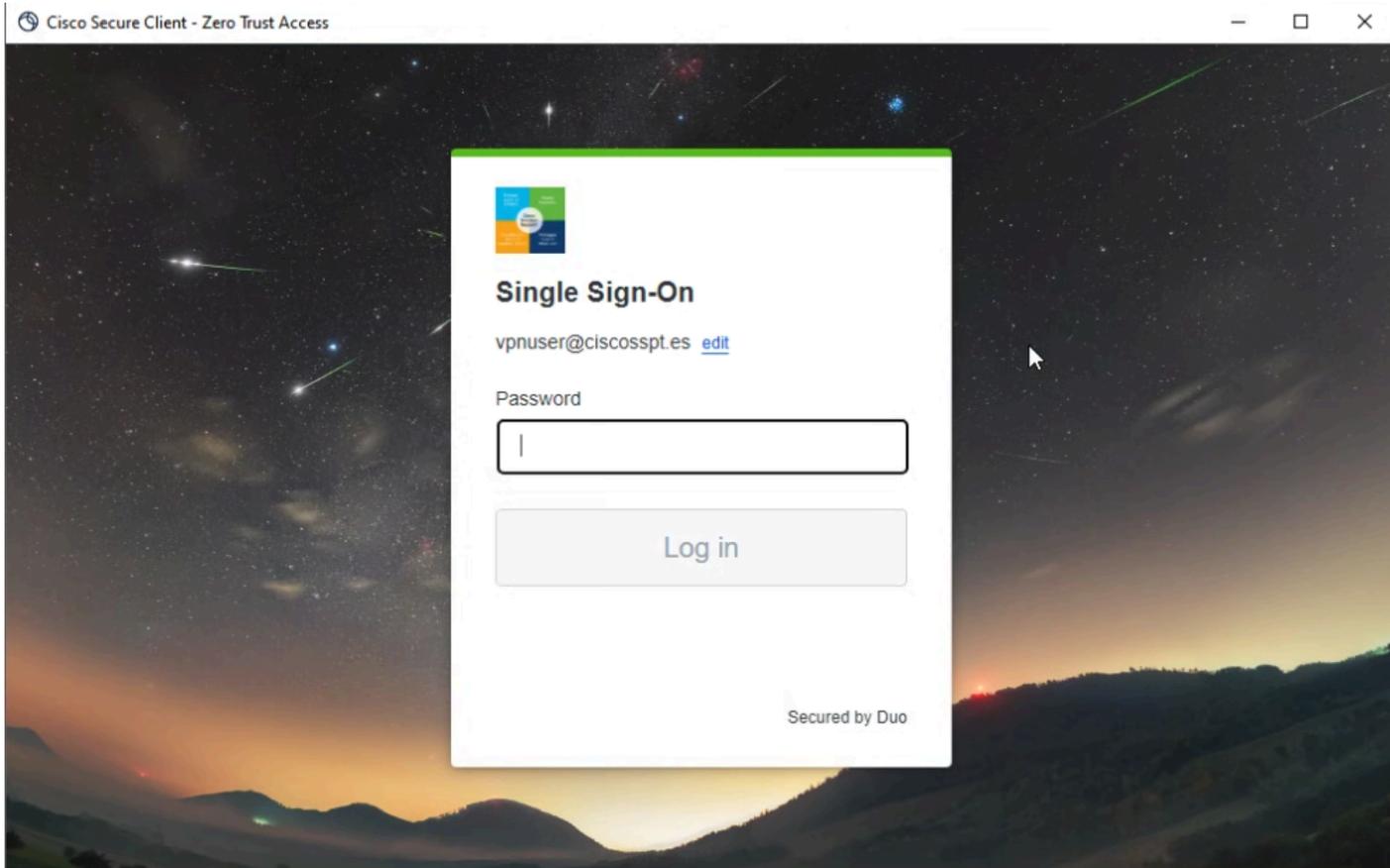
Secure Client - ZTNA

- Registrarsi con il proprio nome utente.



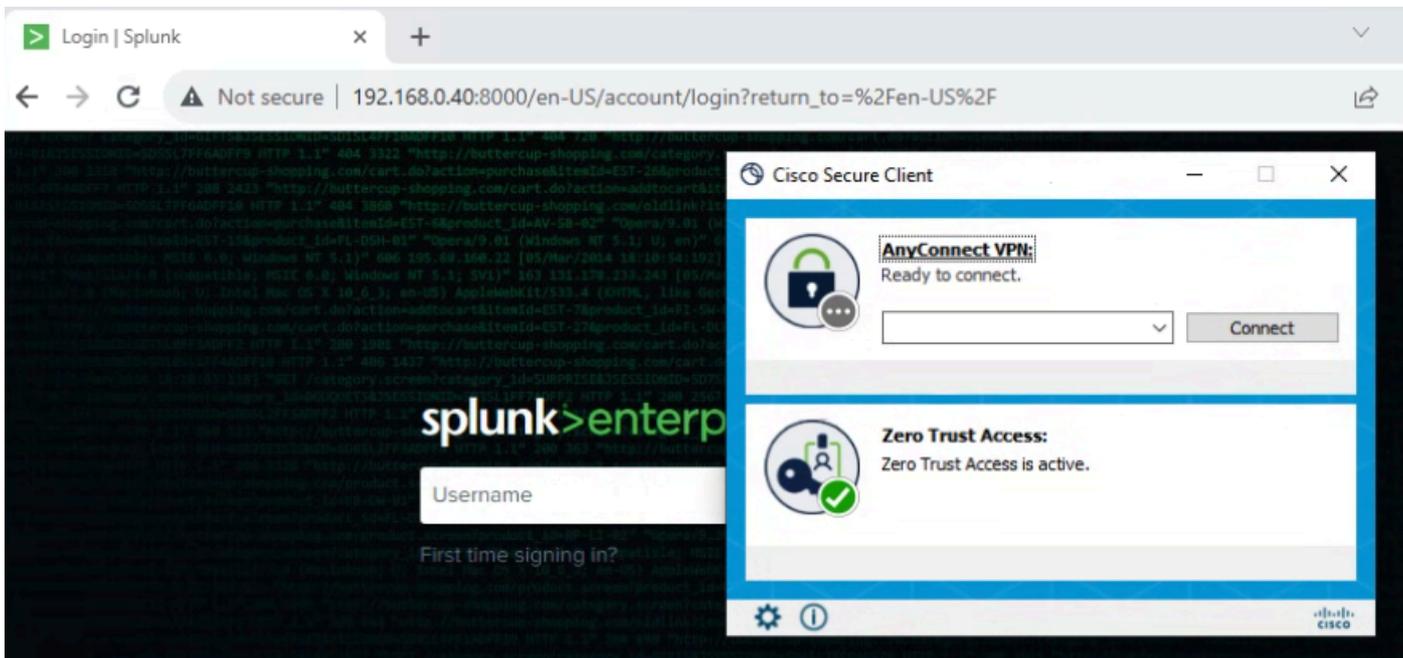
*Secure Client - ZTNA - Registrazione*

- Autenticazione nel provider SSO



Secure Client - ZTNA - Accesso SSO

- Dopo l'autenticazione, accedere alla risorsa:



Accesso sicuro - ZTNA - Accesso registrato

Accedere a: Monitor > Activity Search



The screenshot shows a navigation sidebar on the left with four main categories: Resources (with a grid icon), Secure (with a shield icon), Monitor (with a line graph icon), and Admin (with a person icon). To the right, under the heading "Sources and destinations", there are two sections: "Private Resources" (highlighted with a blue box) which includes the subtext "Define internal applications and other resources for use in access rules", and "Registered Networks" which includes the subtext "Point your networks to our servers".

*Accesso sicuro - Risorsa privata*

- Fare clic sul criterio

The screenshot shows a table with one row. The first column contains the text "SplunkSophos" with a blue arrow pointing to it from the right. The second column contains a hyphen "-". The third column contains three stacked, rounded rectangular buttons: "Client-based ZTNA" (light blue), "Browser-based ZTNA" (light purple), and "VPN" (pink). The number "1" is positioned to the right of these buttons.

*Accesso sicuro - Risorsa privata - SplunkSophos*

- Scorri verso il basso

# SplunkSophos

Client-based ZTNA

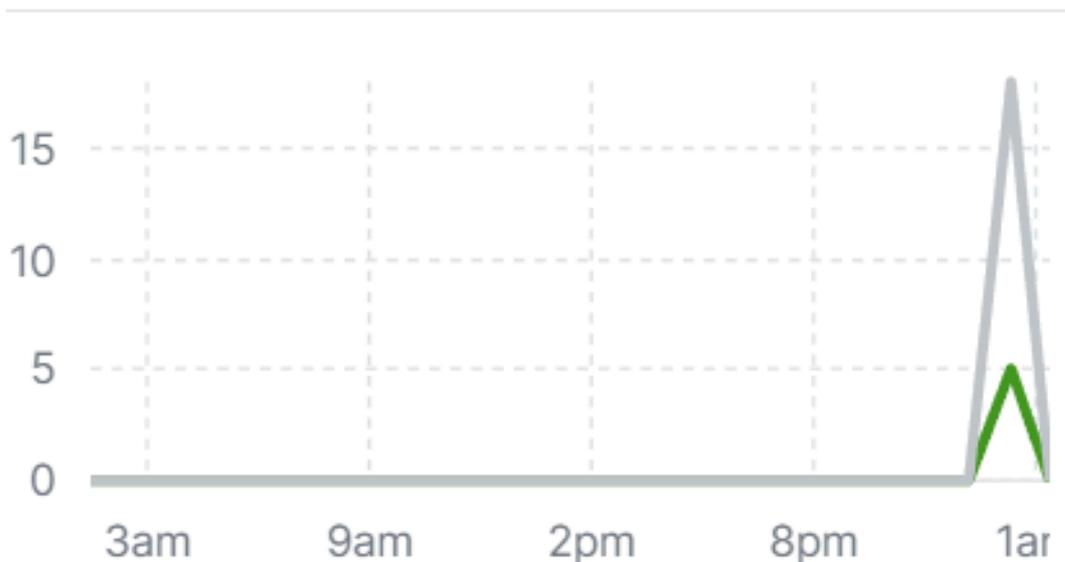
Browser-based ZTNA



VPN

Total Requests

**23** ↗ 44% from previous 24 hours



## TOTAL REQUESTS BY STATUS

### Status

✓	Success	5
⊘	Blocked	18

[Errore Di Risoluzione Dei Problemi Relativi All'Accesso Sicuro: Il Servizio Di Registrazione Non Risponde. Contatta il tuo help desk IT](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).