

使用Sophos XG防火牆配置安全訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[在安全訪問上配置隧道](#)

[通道資料](#)

[在Sophos上配置隧道](#)

[配置IPSec配置檔案](#)

[配置站點到站點VPN](#)

[配置隧道介面](#)

[配置網關](#)

[配置SD-WAN路由](#)

[設定私人應用程式](#)

[配置訪問策略](#)

[驗證](#)

[RA-VPN](#)

[使用者端基礎ZTNA](#)

[基於瀏覽器的ZTNA](#)

[相關資訊](#)

簡介

本文檔介紹如何使用Sophos XG防火牆配置安全訪問。

必要條件

- [設定使用者啟動設定](#)
- [ZTNA SSO身份驗證配置](#)
- [配置遠端訪問VPN安全訪問](#)

需求

思科建議您瞭解以下主題：

- Sophos XG防火牆
- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA

- 無客戶端ZTNA

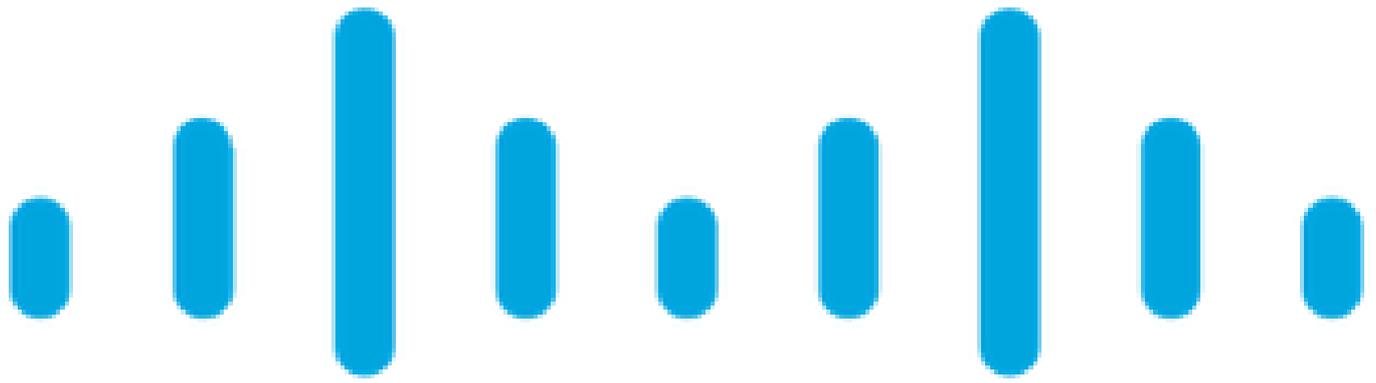
採用元件

本文檔中的資訊基於：

- Sophos XG防火牆
- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊



CISCO

Secure

Access

SOPHOS

安全訪問- Sophos

思科設計了安全訪問，以確保保護和調配對本地和基於雲的私有應用的訪問。它還保護從網路到 Internet 的連線。這透過實施多種安全方法和層來實現，所有這些方法都旨在保護透過雲訪問資訊時所需的資訊。

設定

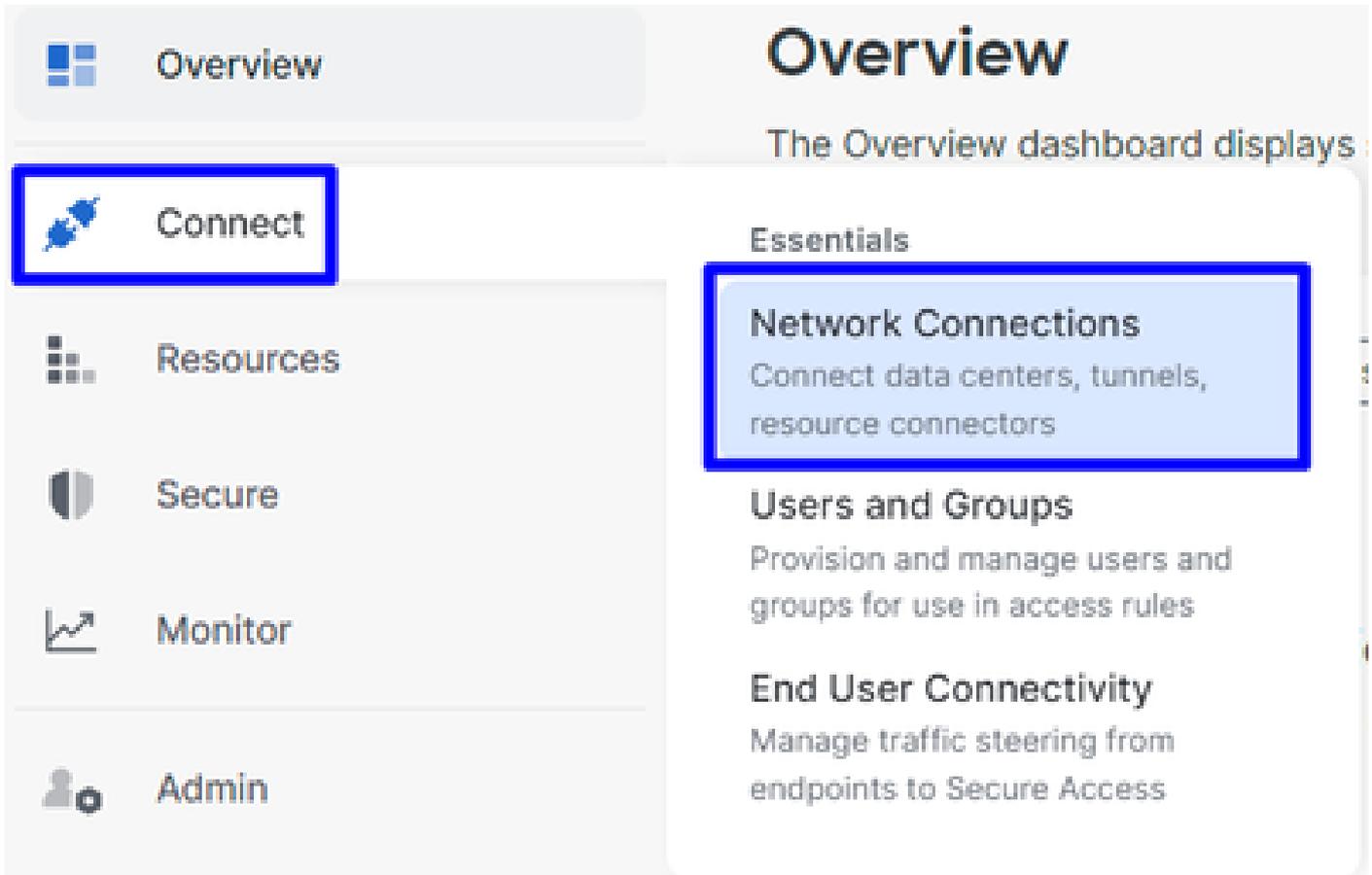
在安全訪問上配置隧道

導航到[安全訪問](#)的管理面板。



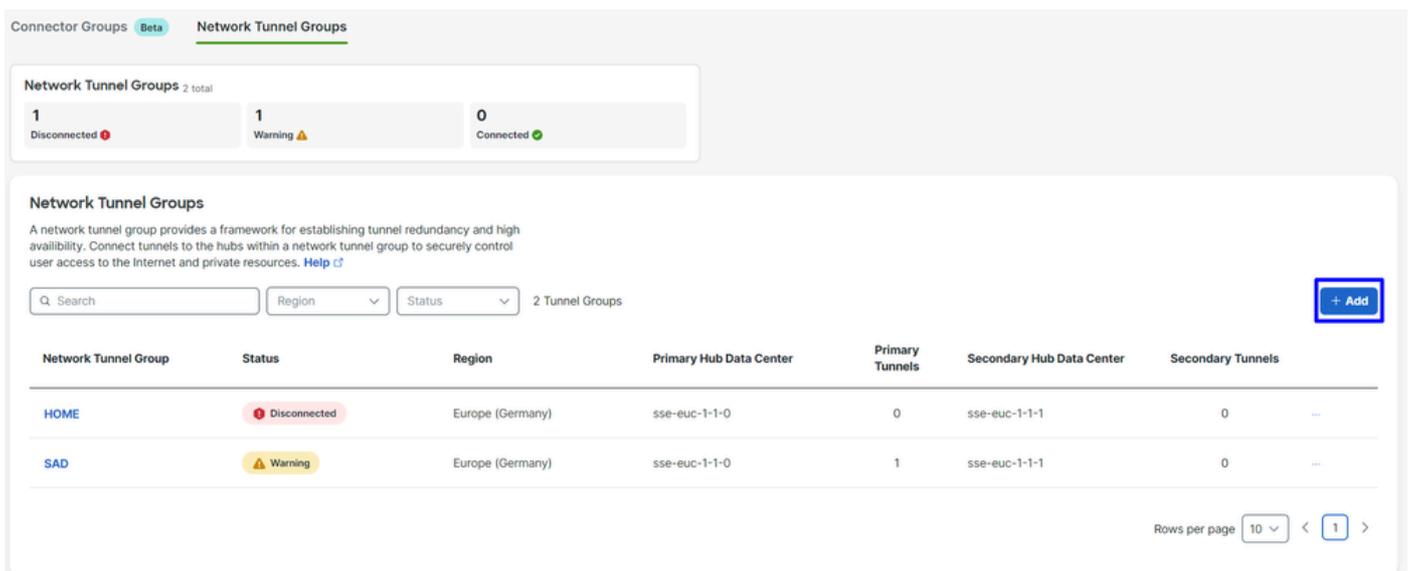
安全存取-首頁

- 按一下 `Connect > Network Connections`.



安全訪問-網路連線

- 在Network Tunnel Groups下，按一下+ Add。



安全訪問-網路隧道組

- 配置Tunnel Group Name、Region和Device Type。
- 按一下 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

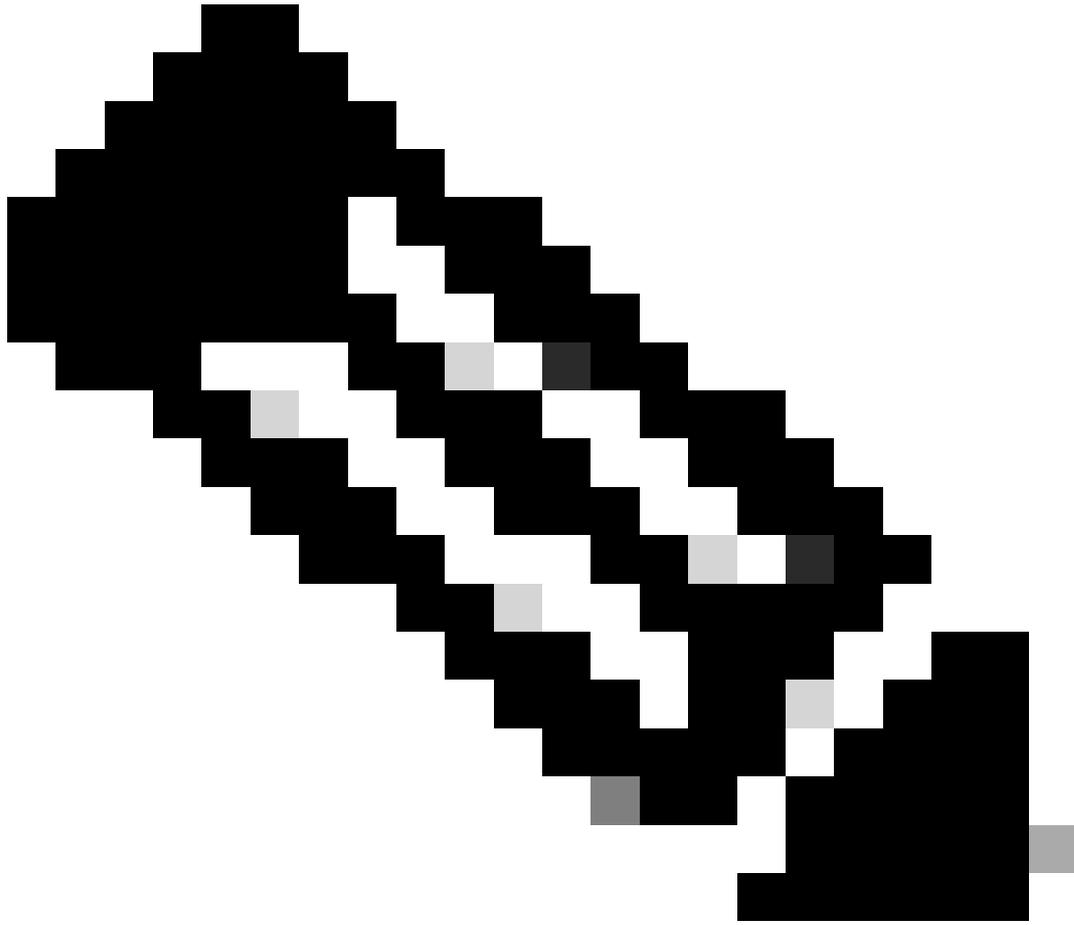
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



附註：選擇最接近防火牆位置的區域。

-
- 配置Tunnel ID Format和Passphrase。
 - 按一下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

安全訪問-隧道組-隧道ID和密碼

- 配置已在網路上配置且希望透過安全訪問傳輸流量的IP地址範圍或主機。
- 點選 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

安全訪問-隧道組-路由選項

按一下顯示Save 的隧道資訊後，請儲存該資訊以用於下一步Configure the tunnel on Sophos。

通道資料

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](#)

安全訪問-隧道組-恢復配置

在Sophos上配置隧道

配置IPSec配置檔案

要配置IPSec配置檔案，請導航到您的Sophos XG防火牆。

您會獲得類似如下所示的內容：

SOPHOS Sophos Firewall PW

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

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

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Advanced protection

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

System

Traffic insight

Web activity 0 max | 0 avg

Cloud applications

0 Apps

0 B In

0 B Out

Security Heartbeat®

0 At risk

Monitor endpoint health and systems at risk

Synchronized Application Control™

0 Apps

Identify unknown apps on your network

Zero-day protection

0 Recent

0 Incidents

0 Scanned

ATP

0 Sources blocked

UTQ

0 Accounts at risk

SSL/TLS connections

0% Of traffic

0% Decrypted

0 Failed

Active firewall rules

0 WAF

1 User

3 Network

4 Scanned

4 Unused

2 Disabled

0 Changed

0 New

Reports

0 Risky apps seen

0 Objectionable websites seen

0 bytes Used by top 10 web users

0 Intrusion attacks

Messages

Alert

Warning

Alert

Click on widgets to open details

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

High availability: [Not configured](#)

12% CPU

61% Memory

61B/s Bandwidth

0 Sessions

0% Decryption capacity

0 Decrypt sessions

0/0 RED

0/0 Wireless APs

0 Connected remote users

0 Live users

Sophos - 管理面板

- 導覽至 Profiles
- 點選 IPsec Profiles 並在點選Add

algorithm

Phase 2

IPsec profiles

Device access

Add

Delete

Manage

在General Settings 配置下：

- **Name**：思科安全訪問策略的參考名稱
- **Key Exchange**：IKEv2
- **Authentication Mode**：主模式
- **Key Negotiation Tries**:0
- **Re-Key connection**：選中該選項

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 配置下：

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

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配置檔案-第1階段

在Phase 2 配置下：

- PFS group (DH group)：與I階段相同
- **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配置檔案-第2階段

在 Dead Peer Detection 配置下：

- **Dead Peer Detection**：選中該選項
- **Check peer after every**:10
- **Wait for response up to**：120（預設）
- **When peer unreachable**：重新啟動（預設）

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配置檔案-失效對等體檢測

然後點選 **Save** and proceed with the next step, Configure Site-to-site VPN。

配置站點到站點VPN

要啟動VPN配置，請按一下**Site-to-site VPN** 並按一下 **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

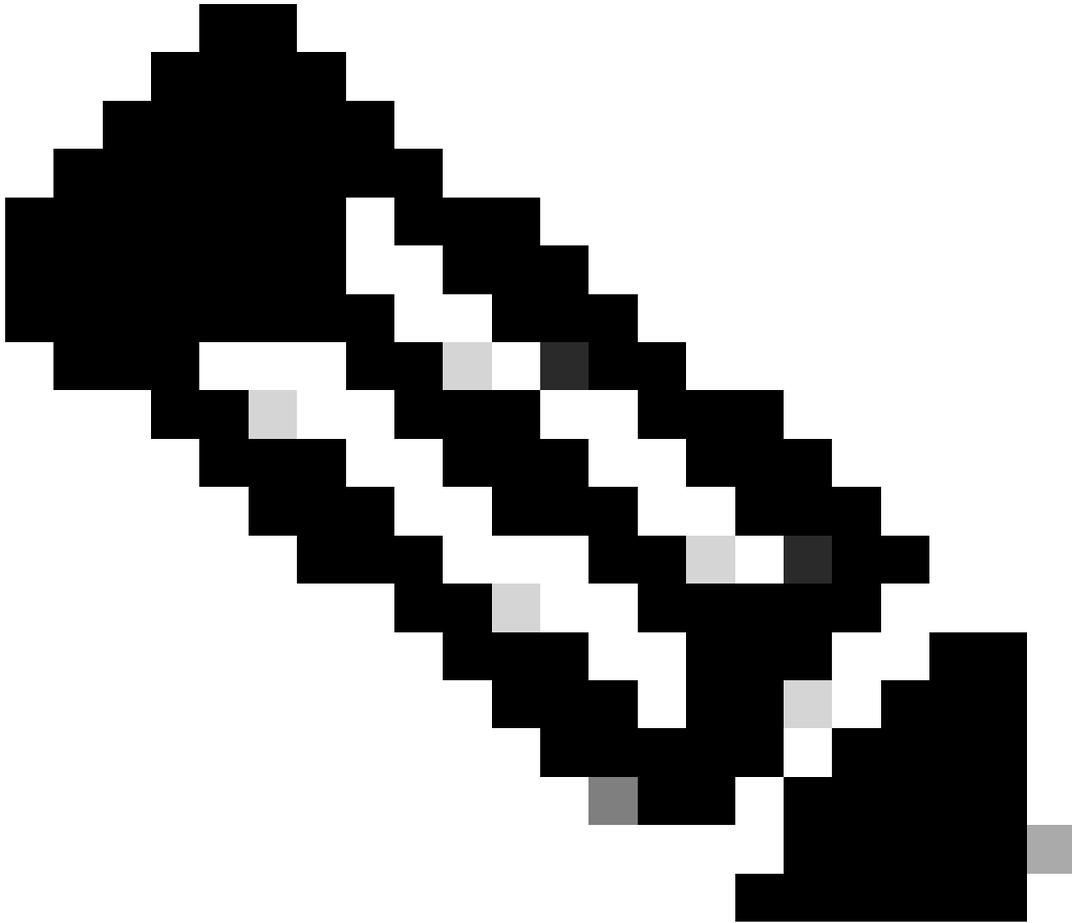
Add Delete

Sophos - 站點到站點VPN

在**General Settings** 配置下：

- **Name**：思科安全訪問IPsec策略的參考名稱
- IP version：IPv4
- Connection type：隧道介面
- Gateway type：啟動連線

- Active on save : 選中該選項
-



注意：在您最終配置站點到站點VPN之後，該選項會Active on save 自動啟用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 - 站點到站點VPN - 常規設定

注意：選項「隧道介面」為Sophos XG防火牆建立一個名為XFRM的虛擬隧道介面。

在Encryption 配置下：

- **Profile**：您在步驟中建立的配置檔案。 **Configure IPsec Profile**
- **Authentication type**：預共用金鑰
- **Preshared key**：您在步驟中配置的金鑰， [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key**：Preshared key

Encryption

Profile CSA	Authentication type Preshared key
	Preshared key
	Repeat preshared key

Sophos - 站點到站點VPN - 加密

在**Gateway Settings** configure Local Gateway和Remote Gateway選項下，請使用此表作為參考。

本地網關	遠端閘道
監聽介面 您的Wan-Internet介面	網關地址 在步驟中生成的公共IP， Tunnel Data
本地ID型別 電子郵件	遠端ID型別 IP 位址

<p>本地ID 在步驟下生成的電子郵件， Tunnel Data</p>	<p>遠端ID 在步驟中生成的公共IP， Tunnel Data</p>
<p>本地子網 任一</p>	<p>遠端子網 任一</p>

Gateway settings

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

Sophos - 站點到站點VPN - 網關設定

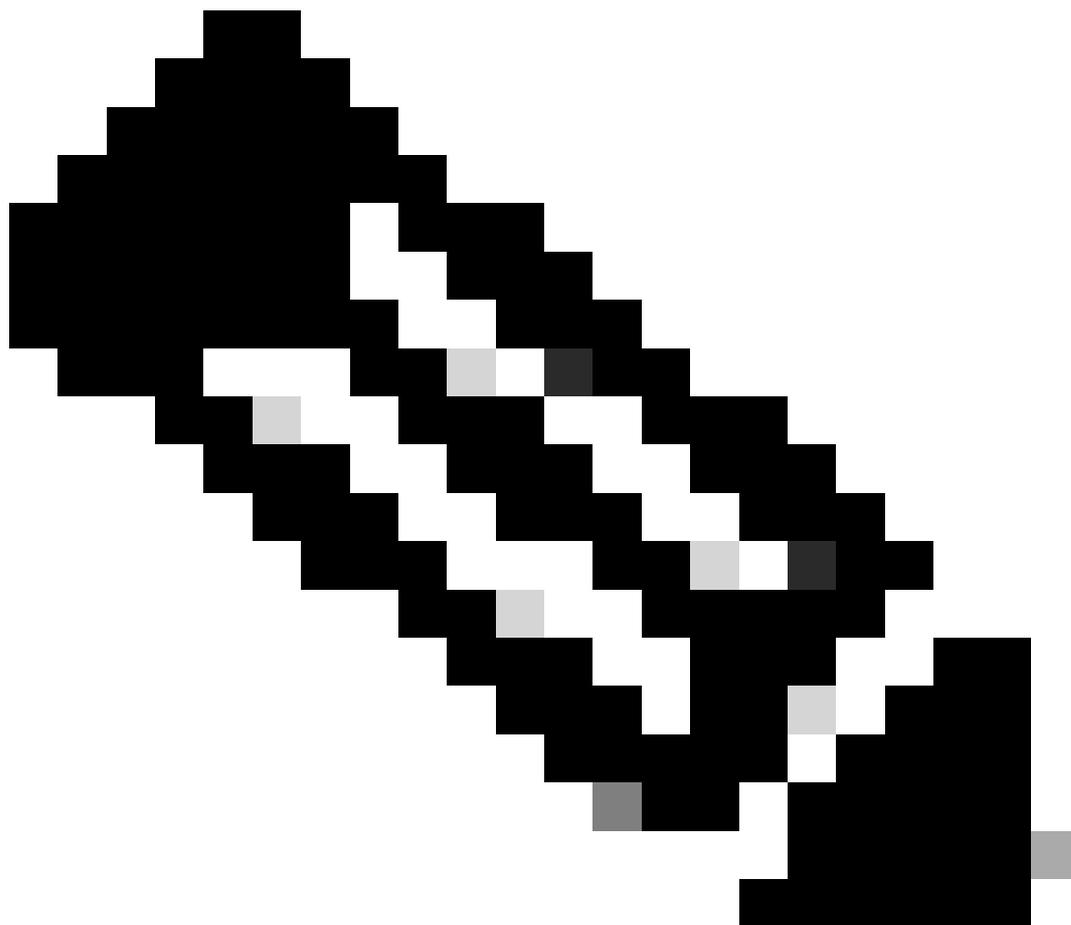
隧道建立完成後，點選Save，您會看到已建立隧道。

IPsec connections

Show additional properties Add Delete Wizard

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

Sophos - 站點到站點VPN - IPsec連線



注意：要檢查隧道在最後一個映像上是否正確啟用，您可以檢查**Connection** 狀態；如果它是綠色的，表示隧道已連線；如果它不是綠色的，表示隧道未連線。

要檢查是否建立了隧道，請導航到 **Current Activities > IPsec Connections**。

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

Sophos - 監控和分析- 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 - 監控和分析- IPsec前後

之後，我們可以繼續執行 **Configure Tunnel Interface Gateway** 步驟。

配置隧道介面

導航到 **Network** 並檢查VPN上配置的介面WAN，以便使用名稱xfrm編輯虛擬隧道介面。

- 按一下接xfrm 口。



Sophos - 網路-隧道介面

- 在網路中配置不可路由的IP介面，例如，可以使用169.254.x.x/30，它通常是不可路由空間中的IP，在我們的示例中，我們使用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 - 網路-隧道介面-配置

配置網關

若要設定虛擬介面的閘道(xfrm)

- 導覽至 Routing > Gateways
- 按一下 Add

Sophos - 路由-網關

在Gateway host 配置下：

- **Name**：引用為VPN建立的虛擬介面的名稱
- **Gateway IP**：在本例169.254.0.2中，即已在步驟中分配的網路169.254.0.1/30下的IP，Configure Tunnel Interface
- **Interface**：VPN虛擬介面
- **Zone**：無（預設）

Sophos - 路由-網關-網關主機

- 在**Health check** 停用檢查下
- 按一下 **Save**

Health check

Health check



Sophos -路由-網關-運行狀況檢查

儲存設定後，您可以觀察閘道的狀態：

IPv4 gateway

<input type="checkbox"/>	Name <small>▼</small>	IP address <small>▼</small>	Interface <small>▼</small>	Health check <small>▼</small>	Status <small>▼</small>	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	●	

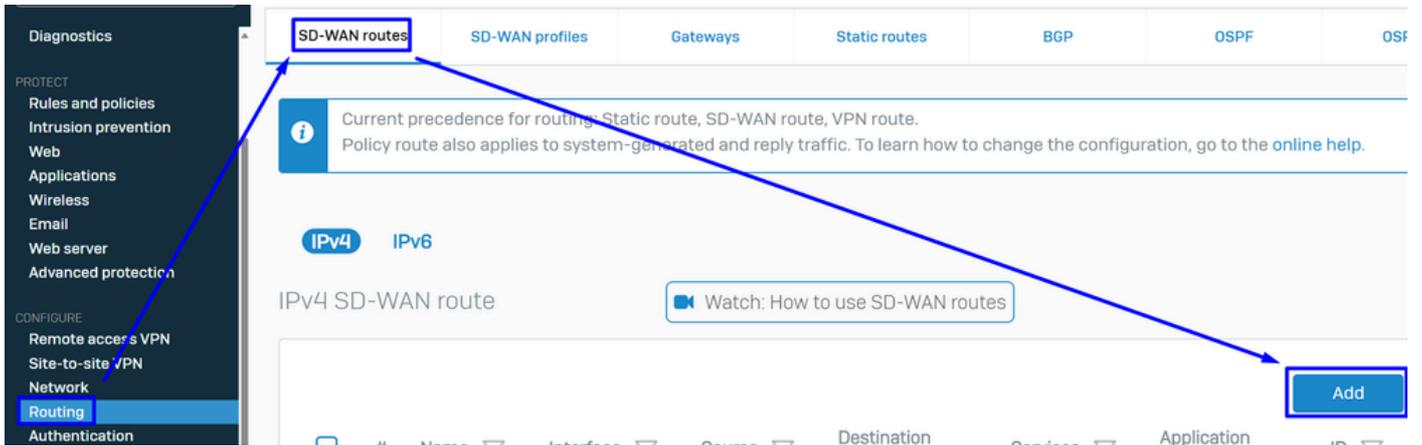
Sophos -路由-網關-狀態

配置SD-WAN路由

要完成配置過程，您需要建立允許將流量轉發到安全訪問的路由。

導覽至 **Routing > SD-WAN routes**.

- 按一下 **Add**



Sophos - SD-Wan路由

在Traffic Selector 配置下：

- Incoming interface：選擇要從中傳送流量的介面，或從RA-VPN、ZTNA或無客戶端ZTNA訪問的使用者
- DSCP marking：此示例沒有任何內容
- **Source networks**：選擇要透過隧道路由的地址
- **Destination networks**：任何或您可以指定目標
- **Services**：任何或您可以指定服務
- **Application object**：如果配置了對象，則為應用程式
- User or groups：如果要增加特定使用者組以將流量路由到安全訪問

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-流量選擇器

在Link selection settings 配置網關下：

- Primary and Backup gateways：選中該選項

- **Primary gateway** : 選擇步驟中配置的網關。 [Configure the Gateways](#)
- 按一下 **Save**

Link selection settings

Select SD-WAN profile ⓘ Primary and Backup gateways

Primary gateway: CSA_GW

Backup gateway: None

Route only through specified gateways ⓘ

Save Cancel

Sophos - SD-Wan路由-流量選擇器-主網關和備份網關

在Sophos XG防火牆上完成配置後，您可以繼續執行步驟。 **Configure Private App.**

設定私人應用程式

要配置專用應用訪問，請登入[管理員門戶](#)。

- 導覽至 **Resources > Private Resources**

Private Resources

Private Resources are applications, r... resource using zero-trust access. Ho...

Private Resources Private F...

Sources and destinations

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

Registered Networks
Point your networks to our servers

Internal Networks
Define internal network segments to use as sources in access rules

Internet and SaaS Resources
Define destinations for internet access rules

Roaming Devices
Mac and Windows

安全存取-私人資源

- 按一下 + Add

Private Resources Private Resource Groups

Private Resources Last 24 Hours

Q 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
------------------	------------------------	-------------------	-------------	-------	----------------

安全存取-私人資源2

- 在General 配置下， Private Resource Name

General

Private Resource Name

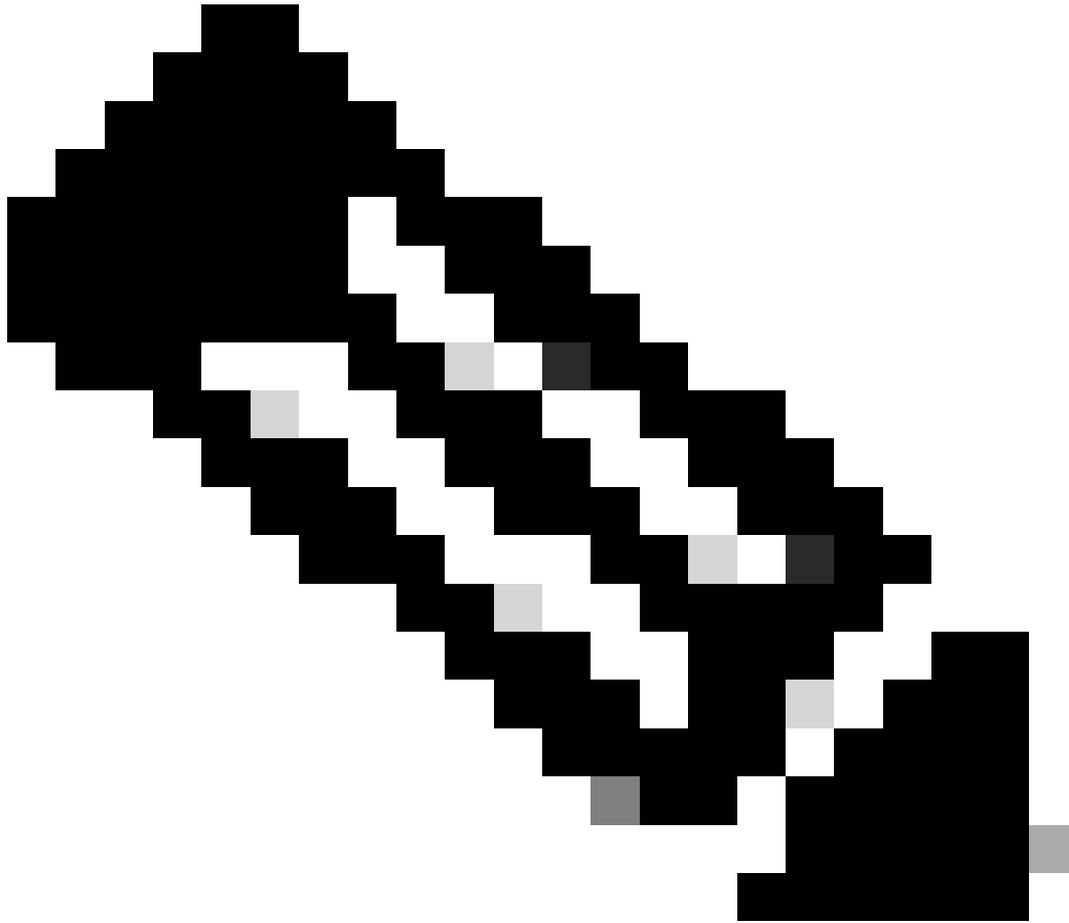
SplunkSophos

Description (optional)

安全存取-私人資源-一般

在Communication with Secure Access Cloud 配置下：

- Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)：選擇要訪問的資源



注意：請記住，內部可到達地址是在步驟 [Configure the Tunnel on Secure Access](#) 中分配的。

-
- **Protocol**：選擇用於訪問該資源的協定
 - **Port / Ranges**：選擇需要啟用的埠以訪問應用

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

安全訪問-私有資源-透過安全訪問雲進行通訊

在中 **Endpoint Connection Methods**，您可以配置透過Secure Access訪問專用資源的所有可能方式，並選擇您要用於您的環境的方法：

- **Zero-trust connections**：選中此框以啟用ZTNA訪問。
 - **Client-based connection**：啟用按鈕以允許客戶端基礎ZTNA
 - **Remotely Reachable Address**：配置專用應用的IP
 - **Browser-based connection**：啟用按鈕以允許基於瀏覽器的ZTNA
 - **Public URL for this resource**：增加與域ztna.sse.cisco.com結合使用的名稱
 - **Protocol**：選擇HTTP或HTTPS作為透過瀏覽器訪問的協定
- **VPN connections**：選中此框以啟用RA-VPN訪問。
- 按一下 **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

安全訪問-私有資源-透過安全訪問雲進行通訊2

組態完成後，會產生以下結果：

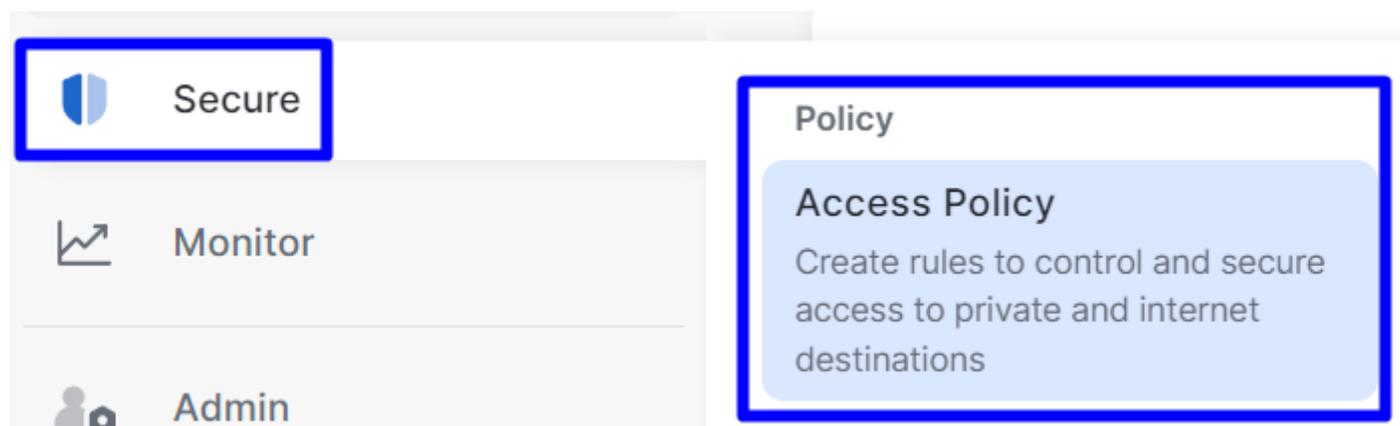
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none">VPNBrowser-based ZTNAClient-based ZTNA	1	2	16

安全訪問-已配置專用資源

現在您可以繼續步驟 **Configure the Access Policy**。

配置訪問策略

要配置訪問策略，請導航到 **Secure > Access Policy**。



安全訪問-訪問策略

- 按一下 **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

安全訪問-訪問策略-專用訪問

設定下一個選項，透過多種驗證方法提供存取：

- 1. Specify Access
 - Action: 允許
 - **Rule name**：指定訪問規則的名稱
 - **From**：您授予訪問許可權的使用者
 - **To**：您要允許訪問的應用程式
 - **Endpoint Requirements**：（預設）
- 按一下 **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**

安全存取-存取原則-指定存取

注意：2. Configure Security 對於所需的步驟，但在本例中，您未啟用 Intrusion Prevention (IPS)或 Tenant Control Profile。

- 按一下Save，您可以：

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

安全訪問-已配置訪問策略

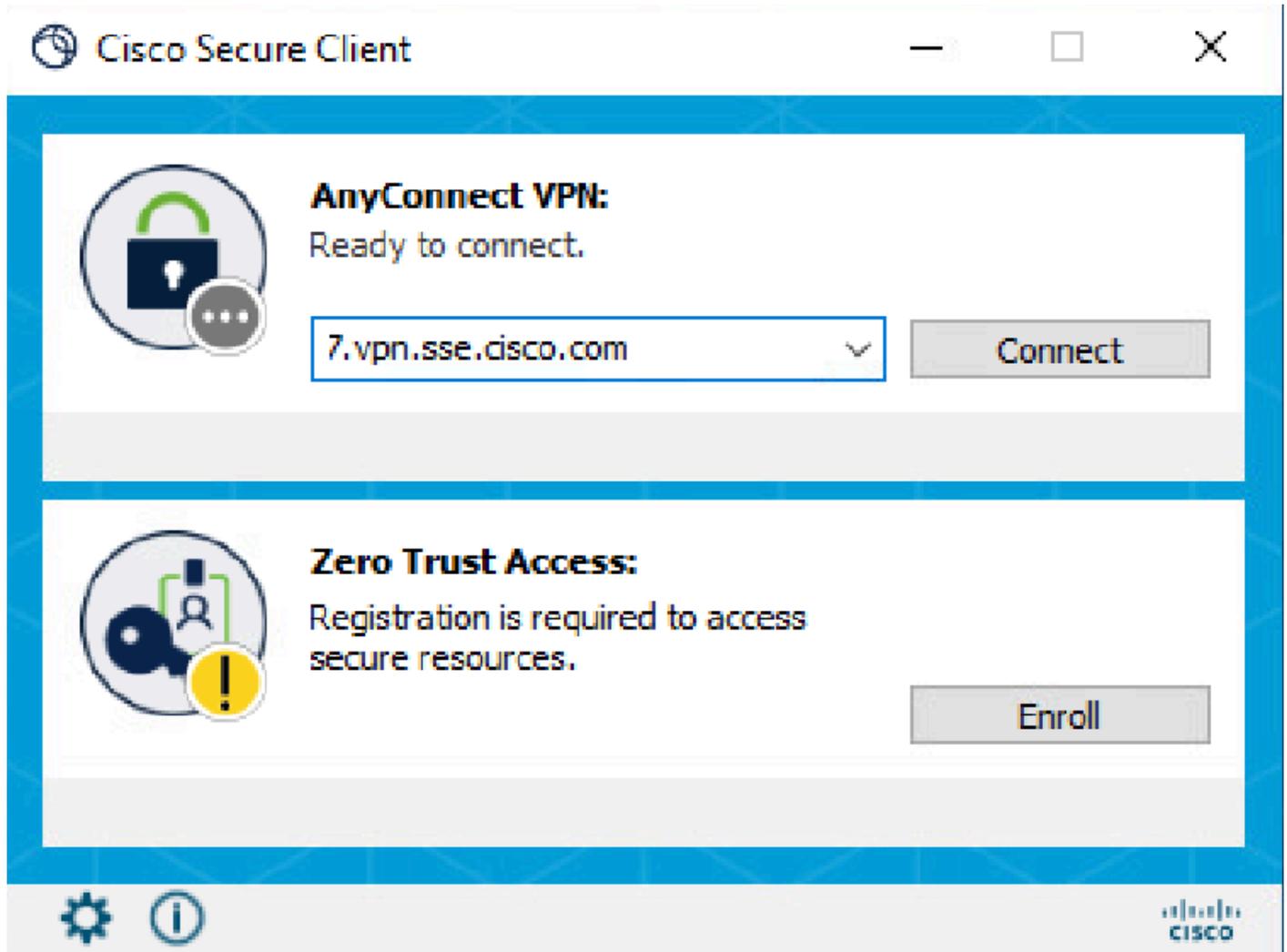
之後，您可以繼續步驟Verify。

驗證

要驗證訪問許可權，必須已安裝可以從[軟體下載- Cisco Secure Client](#)下載的Cisco Secure Client代理。

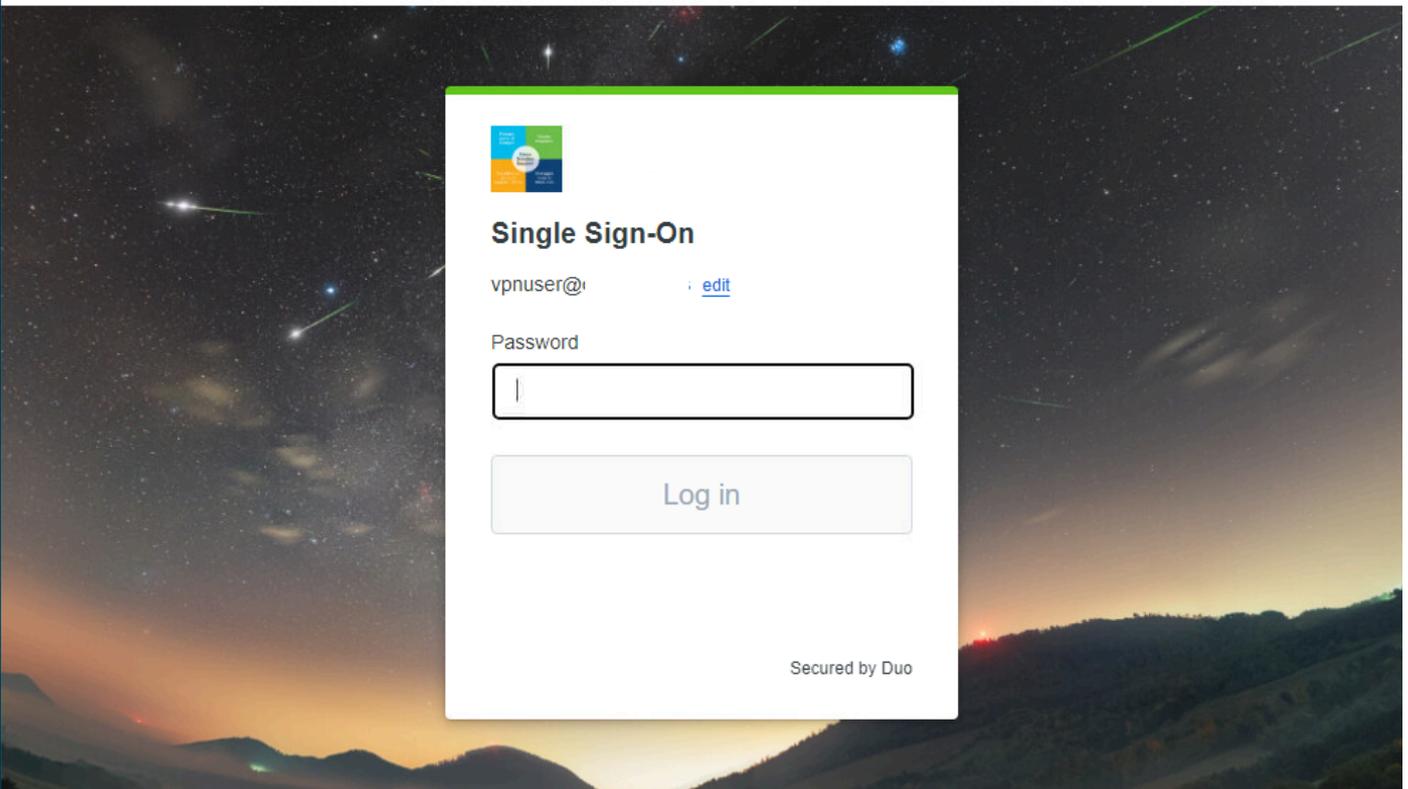
RA-VPN

透過Cisco Secure Client Agent-VPN登入。



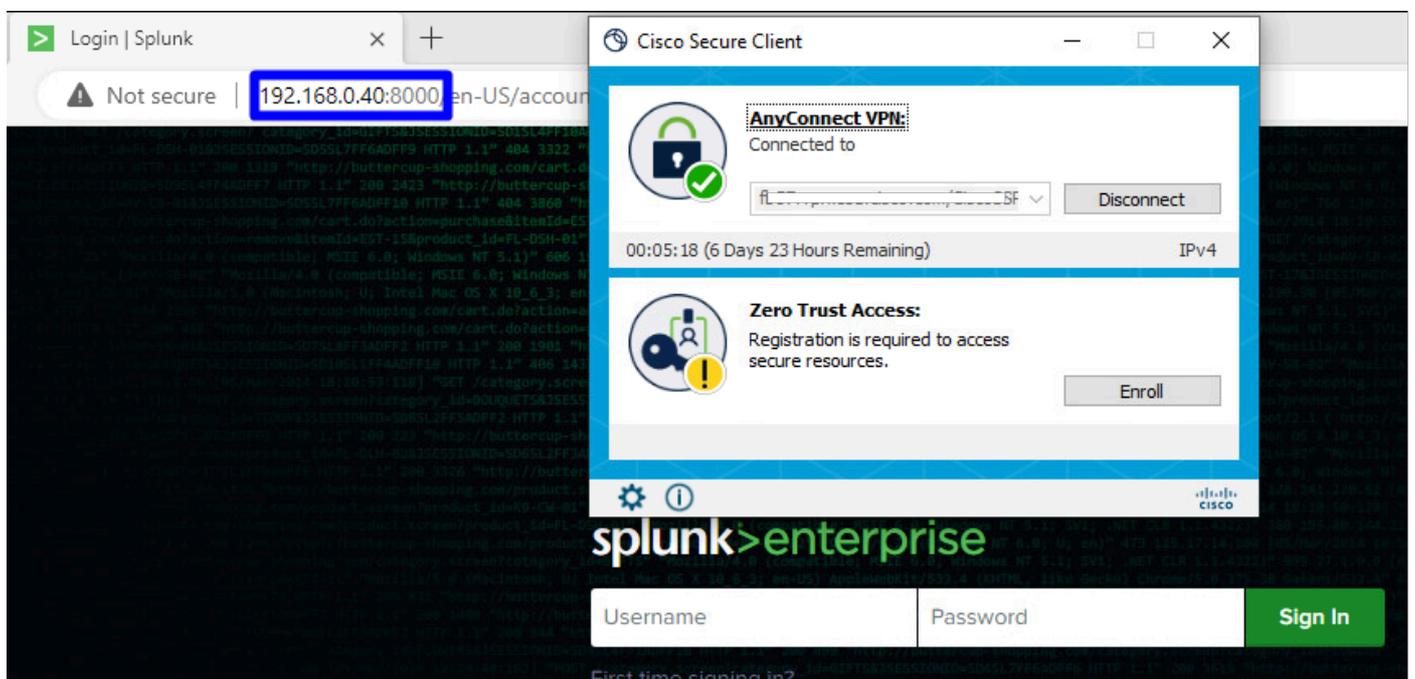
安全客戶端- VPN

- 透過您的SSO提供商進行身份驗證



安全訪問- VPN - SSO

- 透過身份驗證後，請訪問以下資源：



安全訪問- VPN - 已驗證

導覽至：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

安全訪問-活動搜尋- RA-VPN

您可以看到使用者被允許透過RA-VPN進行身份驗證。

使用者端基礎ZTNA

透過Cisco Secure Client Agent - ZTNA登入

```

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

C:\Users\falas>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

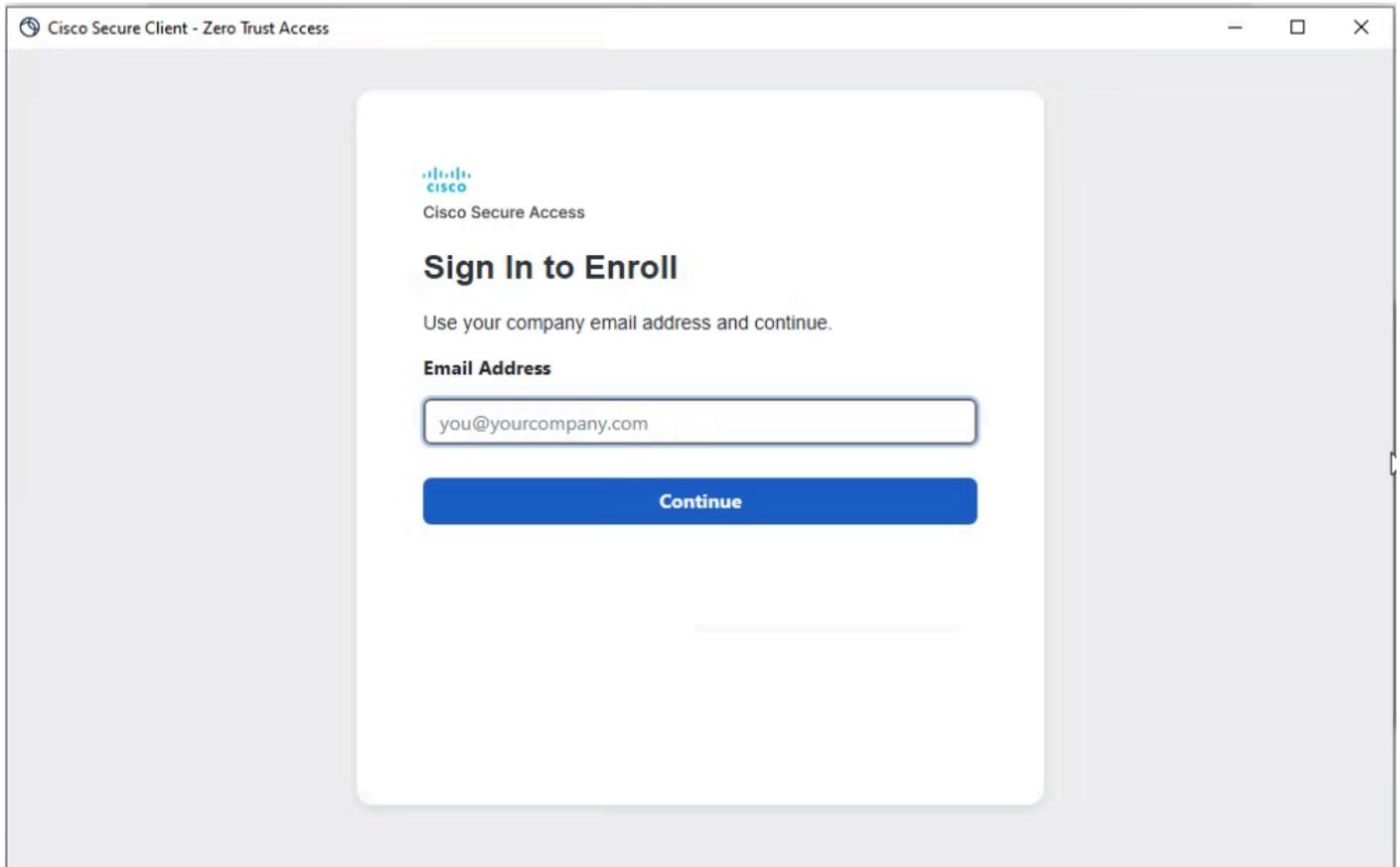
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3c3b:a6aa:6cc9:c1c6%15
    IPv4 Address. . . . . : 10.10.10.120
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1

C:\Users\falas>

```

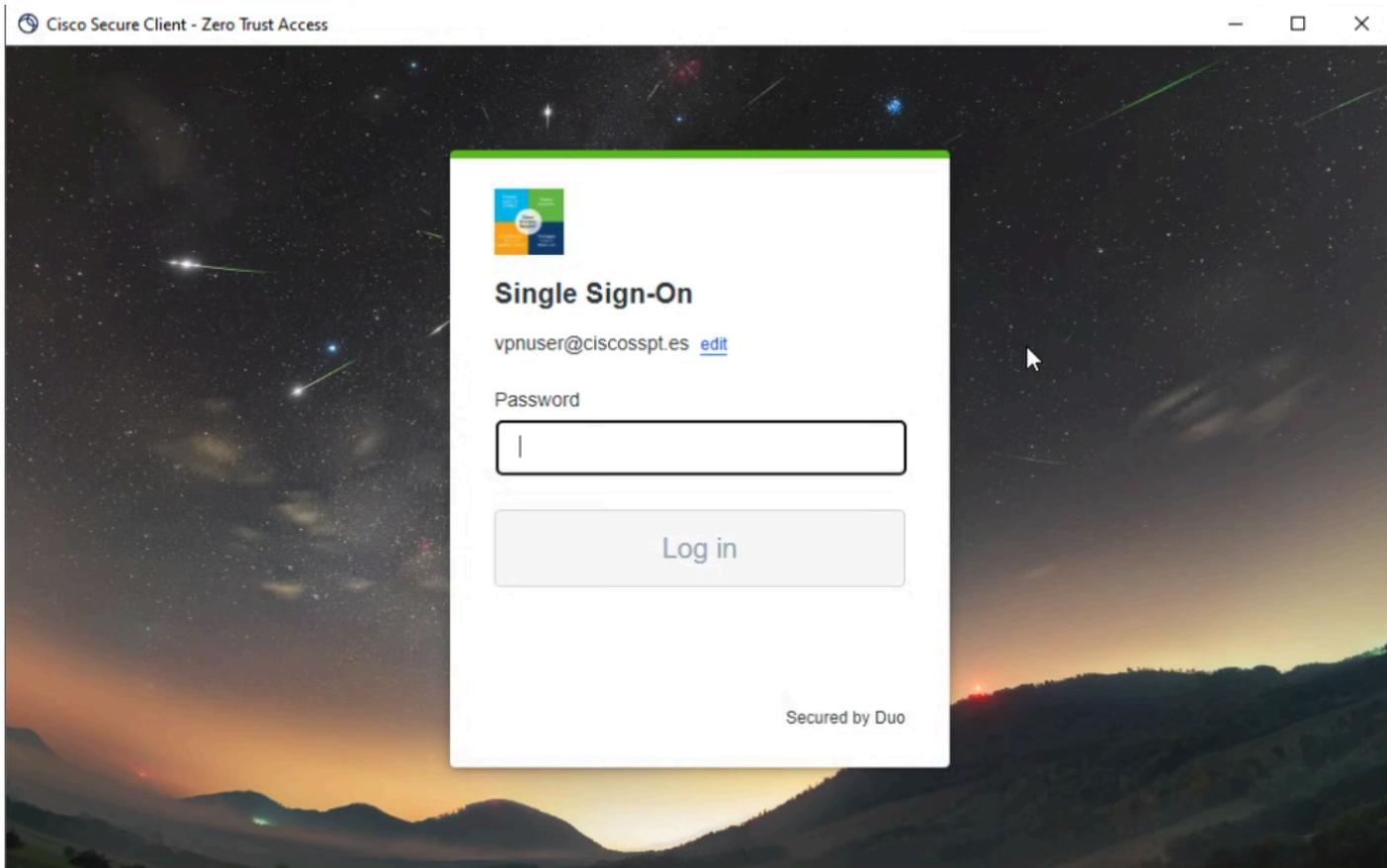
安全使用者端- ZTNA

- 使用您的使用者名稱註冊。



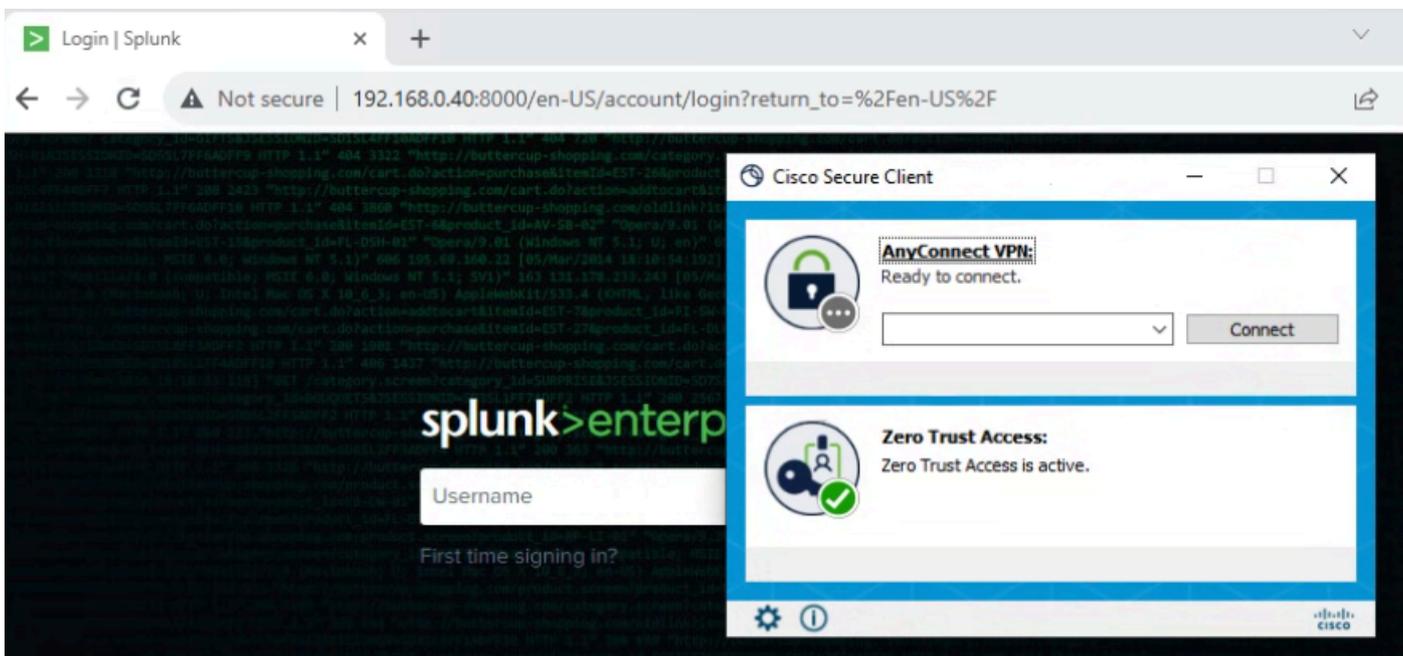
安全客戶端- ZTNA -註冊

- 在您的SSO提供者中進行驗證



安全客戶端- ZTNA - SSO登入

- 透過身份驗證後，請訪問以下資源：



安全訪問- ZTNA -已記錄

導覽至：Monitor > Activity Search

The screenshot shows a navigation sidebar on the left with four main sections: Resources (with a grid icon), Secure (with a shield icon), Monitor (with a line graph icon), and Admin (with a person icon). The main content area is titled "Sources and destinations" and contains two items: "Private Resources" (highlighted with a blue border) and "Registered Networks".

Resources

- Secure
- Monitor
- Admin

Sources and destinations

- Private Resources**
Define internal applications and other resources for use in access rules
- Registered Networks
Point your networks to our servers

安全存取-私人資源

- 按一下您的原則

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" (teal), "Browser-based ZTNA" (purple), and "VPN" (pink). The number "1" is positioned to the right of the buttons.

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

安全訪問-專用資源- *SplunkSophos*

- 向下滾動

SplunkSophos

Client-based ZTNA

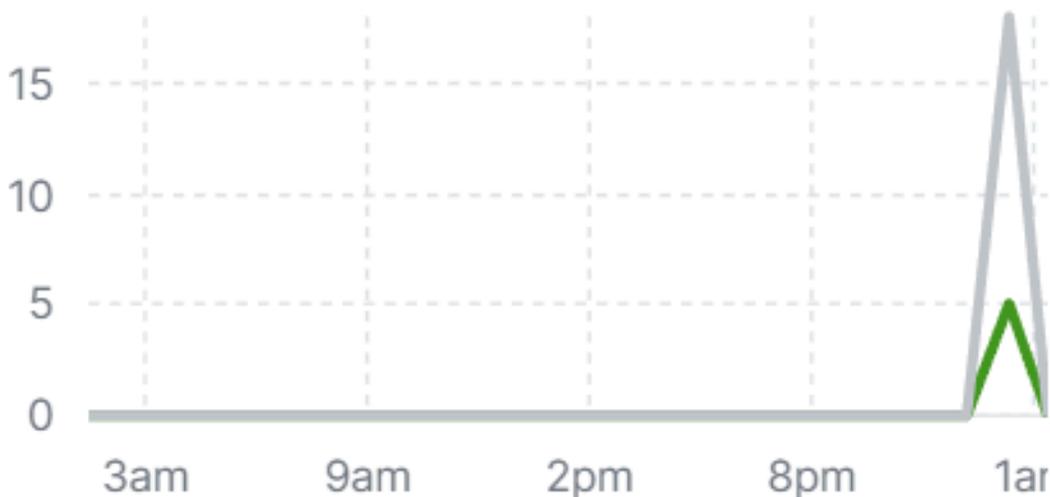
Browser-based ZTNA



VPN

Total Requests

23 ↗ 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status

✓	Success	5
⊘	Blocked	18

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。