使用Sophos XG防火牆配置安全訪問

目錄

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

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。

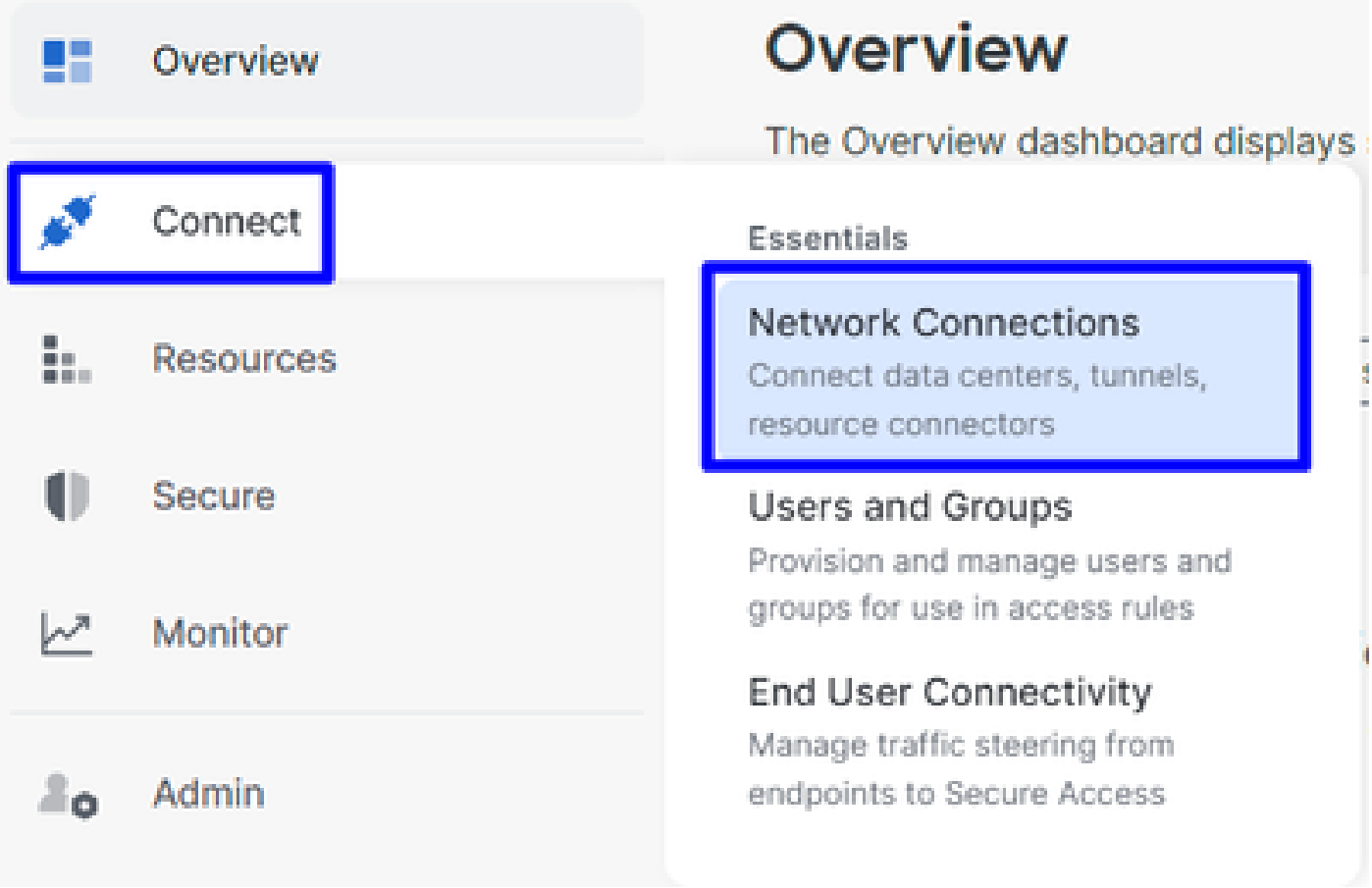
設定

在安全訪問上配置隧道

導航到安全訪問的管理面板。

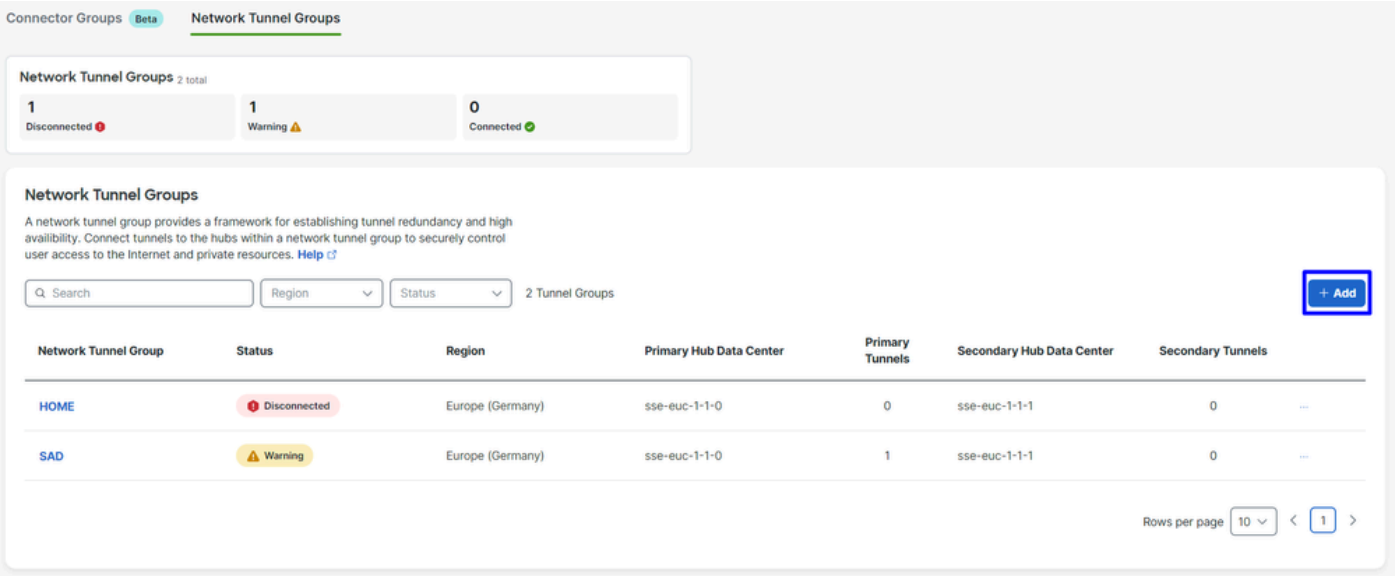
安全存取-首頁

- 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

SophosFirewall

Region

Europe (Germany)

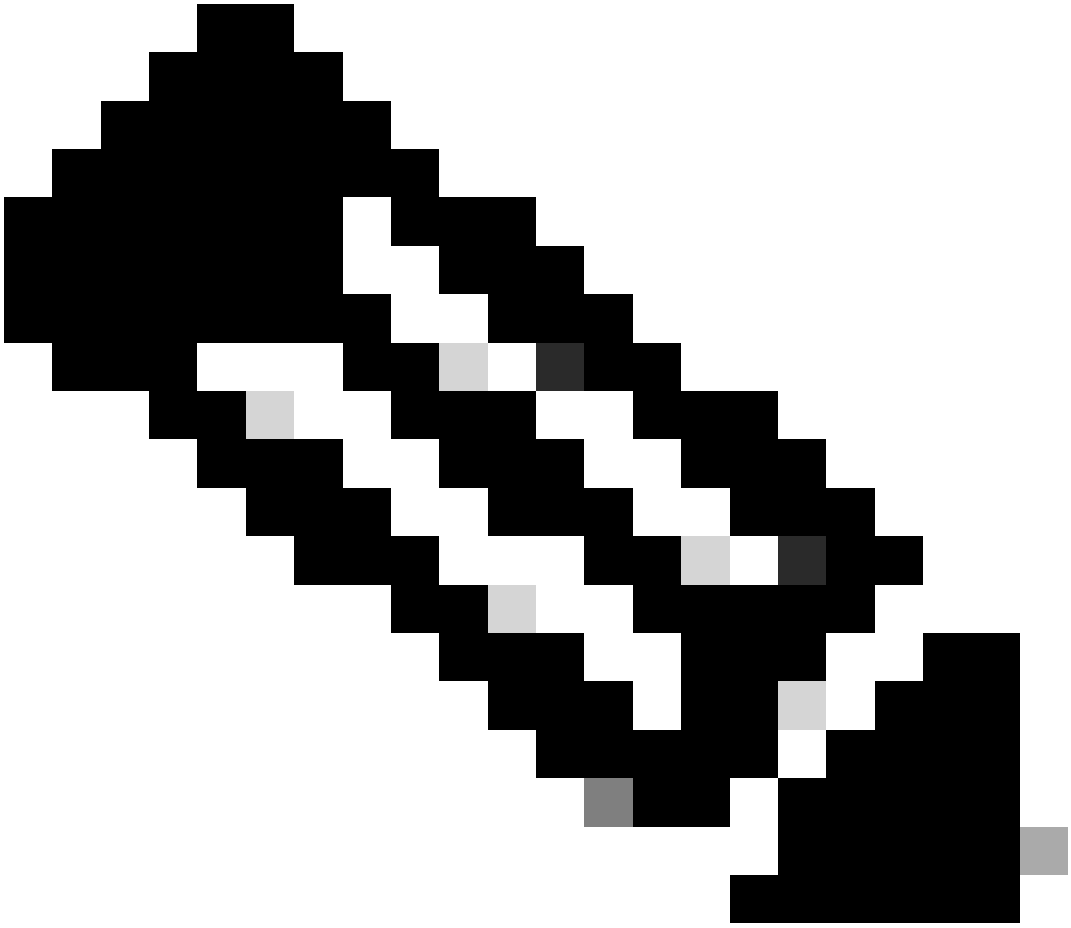
Device Type

Other

Cancel

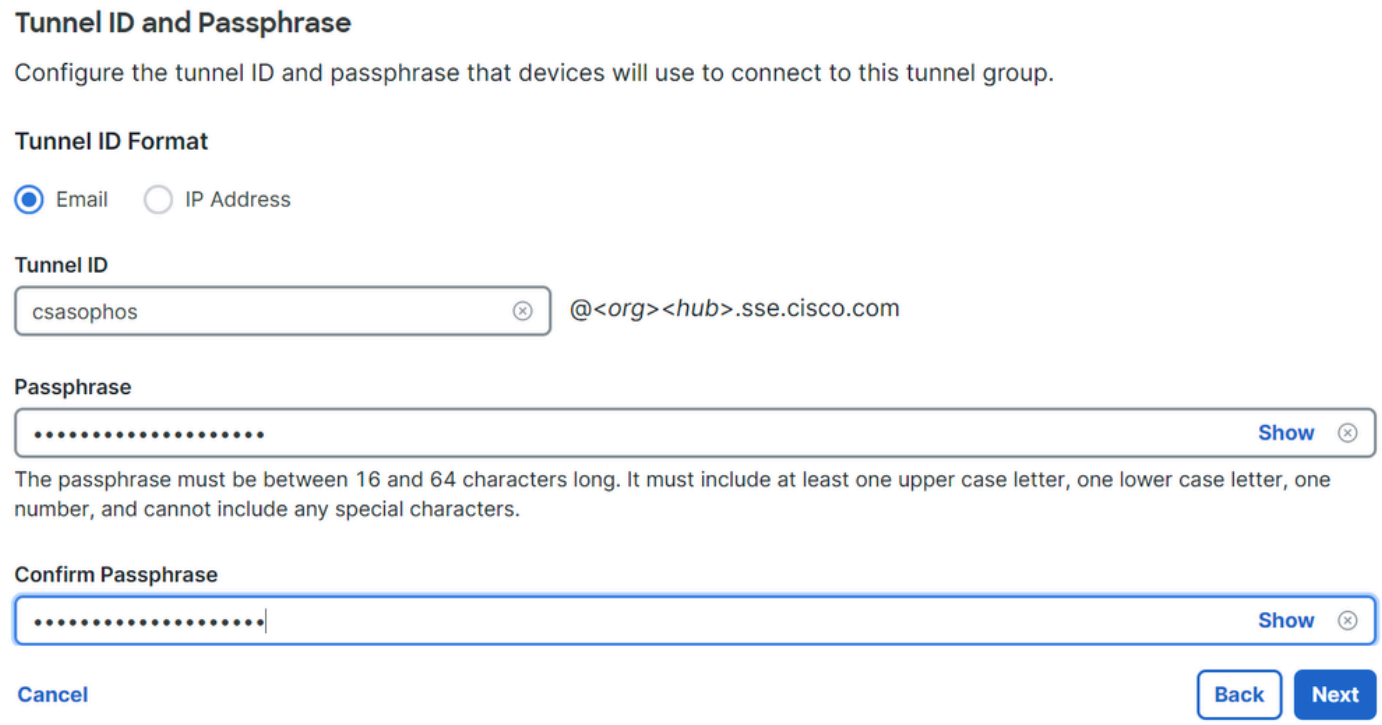
Next

安全訪問-隧道組-常規設定



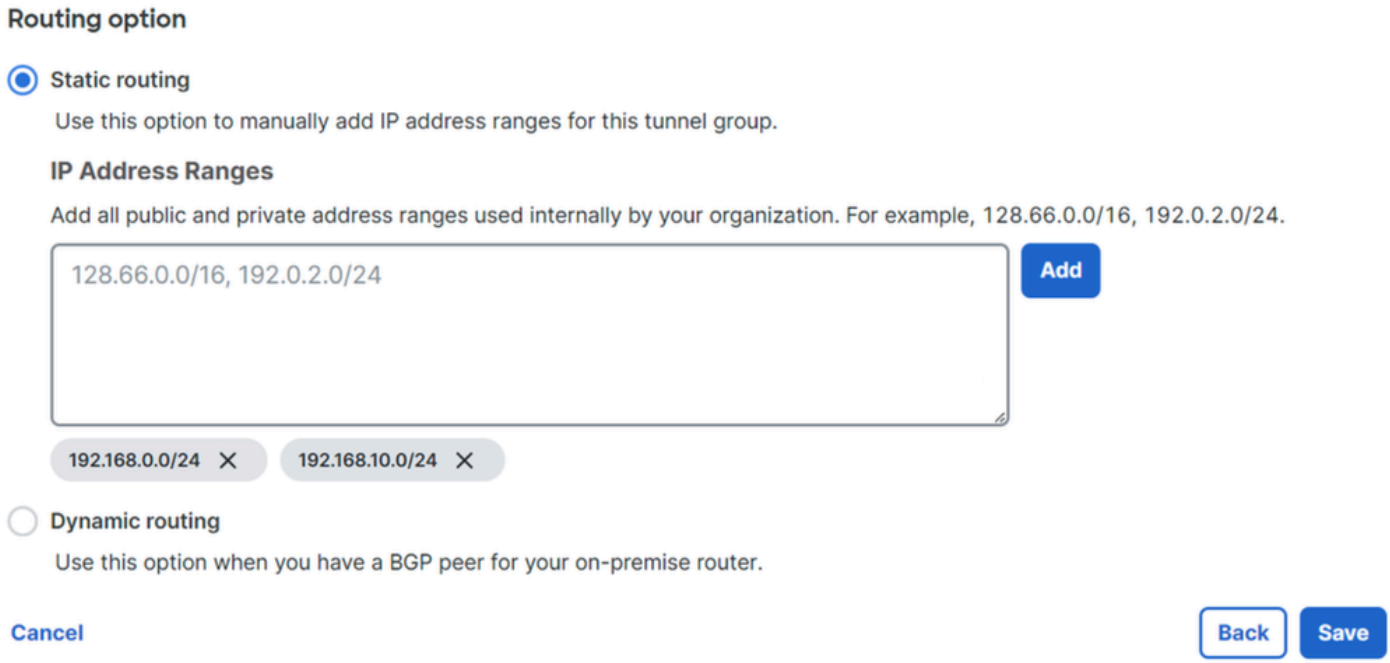
附註：選擇最接近防火牆位置的區域。

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



安全訪問-隧道組-隧道*ID*和密碼

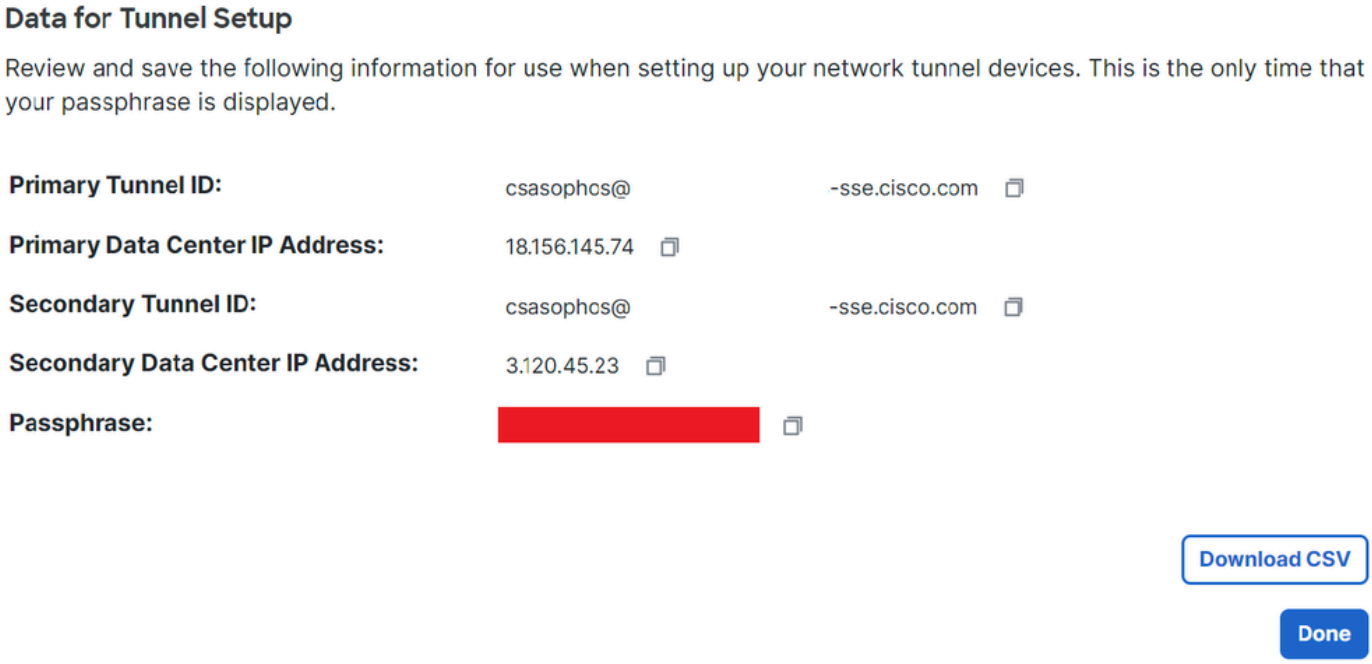
- 配置已在網路上配置且希望透過安全訪問傳輸流量的IP地址範圍或主機。
- 點選 **Save**。



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



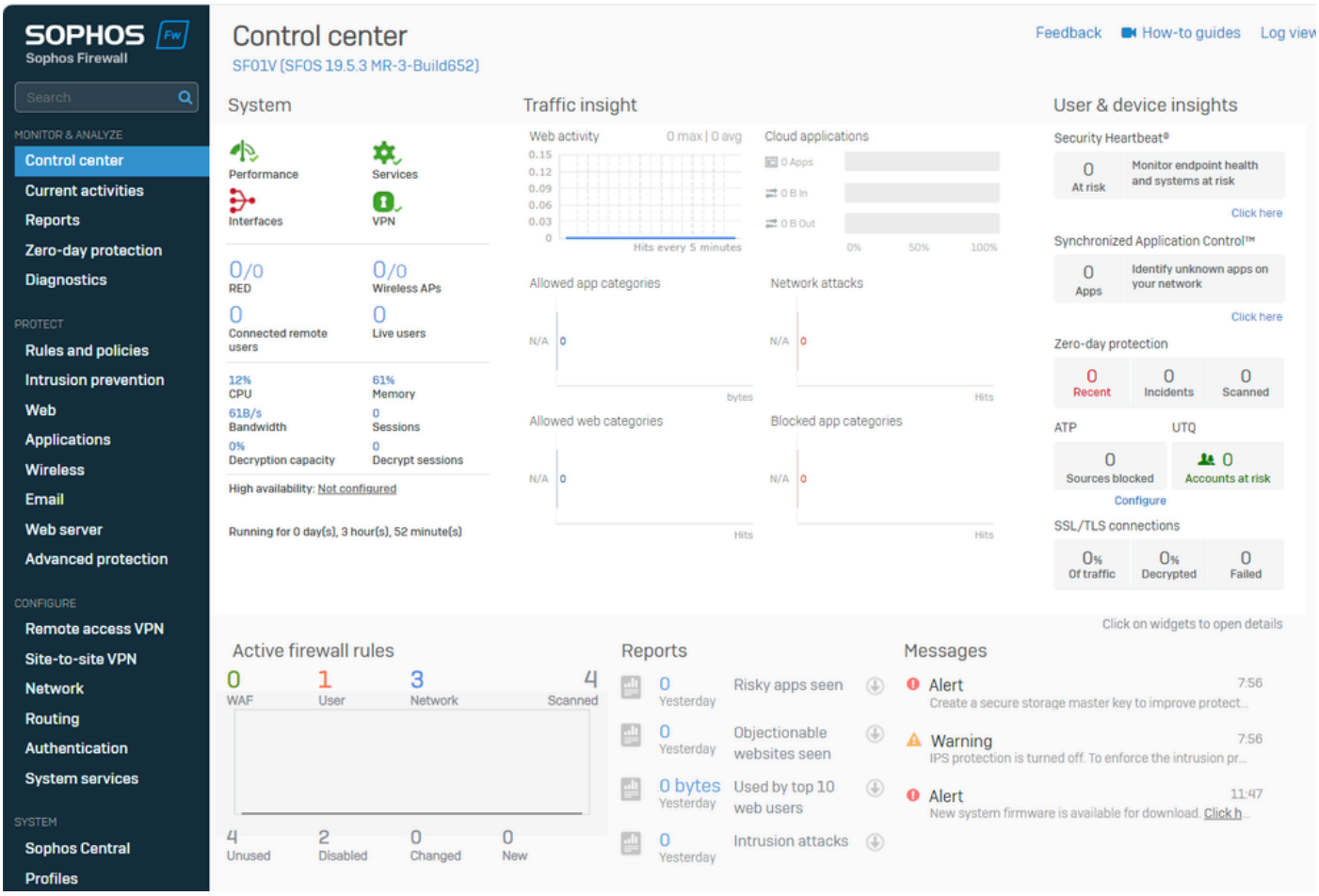
安全訪問-隧道組-恢復配置

在Sophos上配置隧道

配置IPSec配置檔案

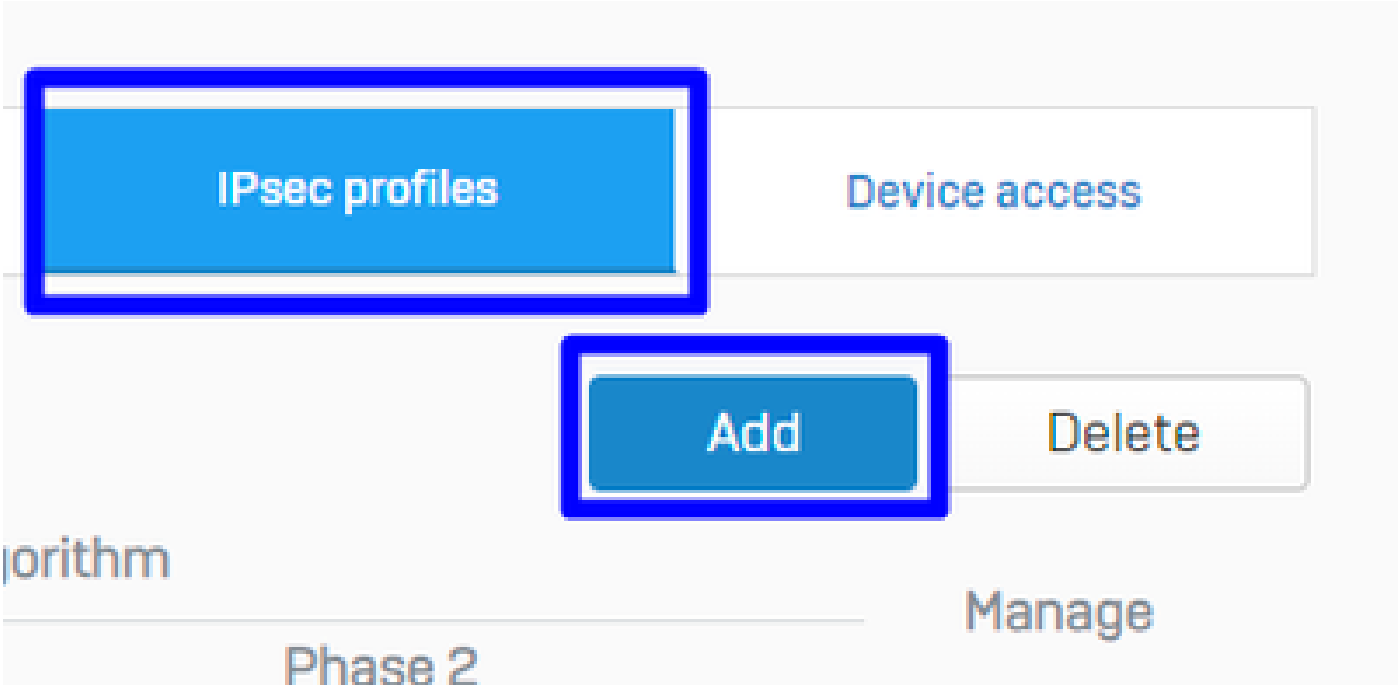
要配置IPSec配置檔案，請導航到您的Sophos XG防火牆。

您會獲得類似如下所示的內容：



Sophos -管理面板

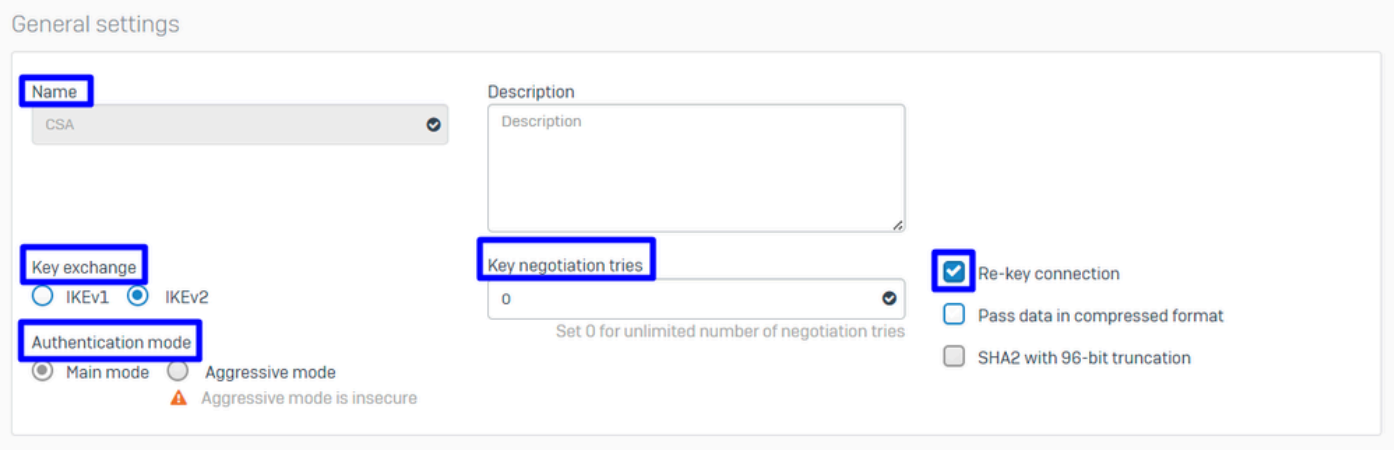
- 導覽至 Profiles
- 點選 **IPsec Profiles** 並在點選Add



Sophos - IPsec配置檔案

在General Settings 配置下：

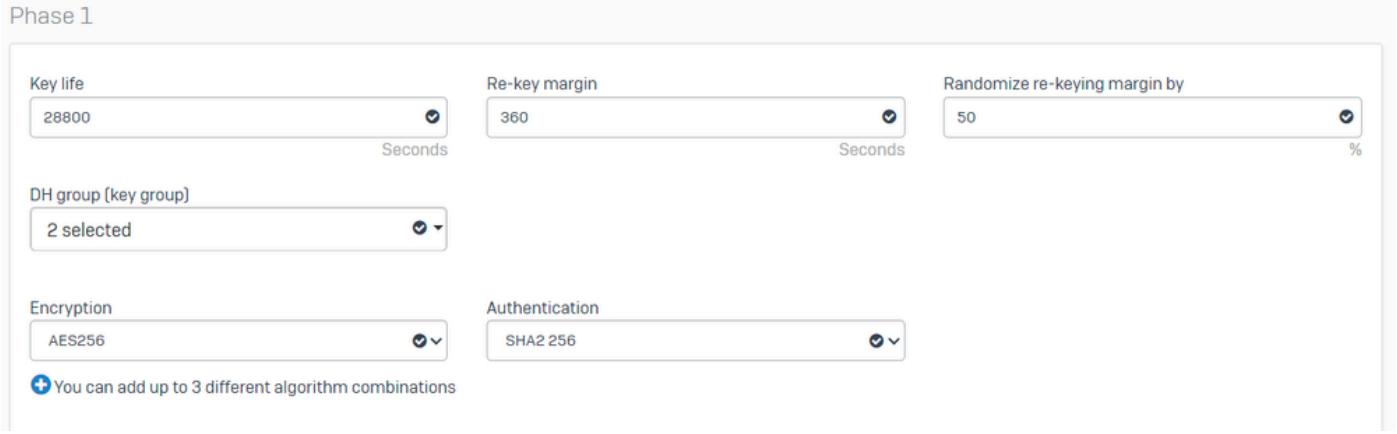
- **Name**：思科安全訪問策略的參考名稱
- **Key Exchange**： IKEv2
- **Authentication Mode**：主模式
- **Key Negotiation Tries**:0
- **Re-Key connection**：選中該選項



Sophos - IPsec配置檔案-常規設定

在Phase 1 配置下：

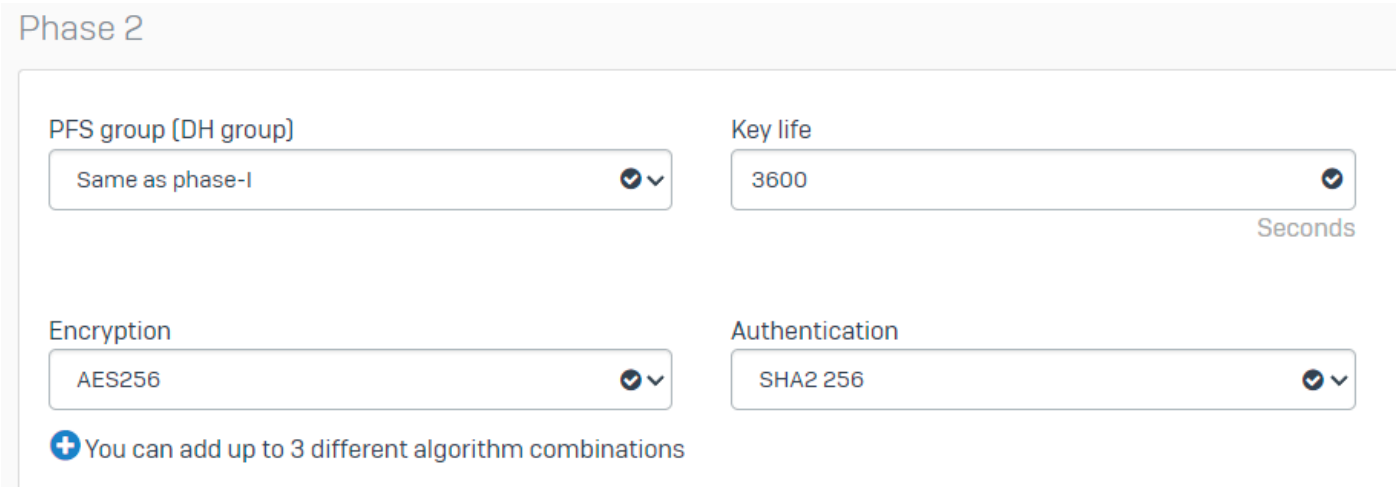
- **Key Life**:28800
- **DH group(key group)**：選擇19和20
- **Encryption**： AES256
- **Authentication**： SHA2 256
- Re-key margin： 360（預設）
- **Randomize re-keying margin by**： 50（預設）



*Sophos - IPsec*配置檔案-第1階段

在Phase 2 配置下：

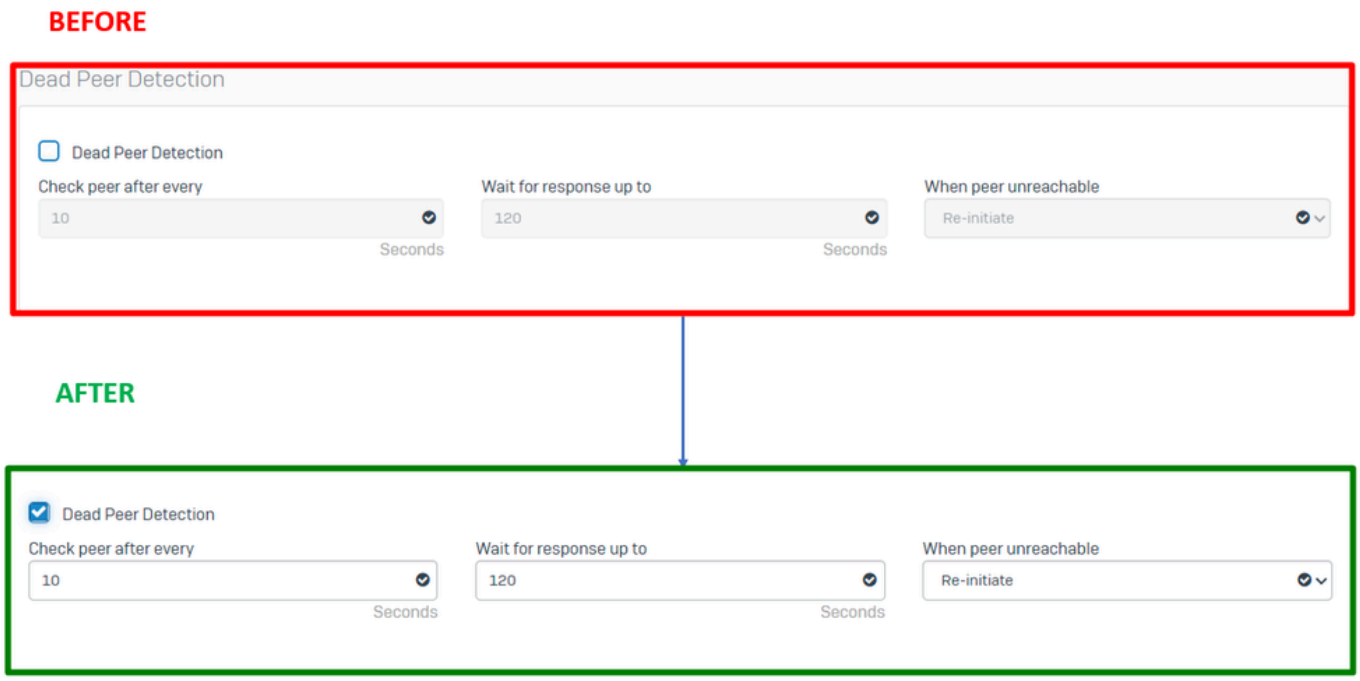
- PFS group (DH group)：**與I階段相同**
- **Key life**:3600
- **Encryption**：AES 256
- Authentication： SHA2 256



*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 ）

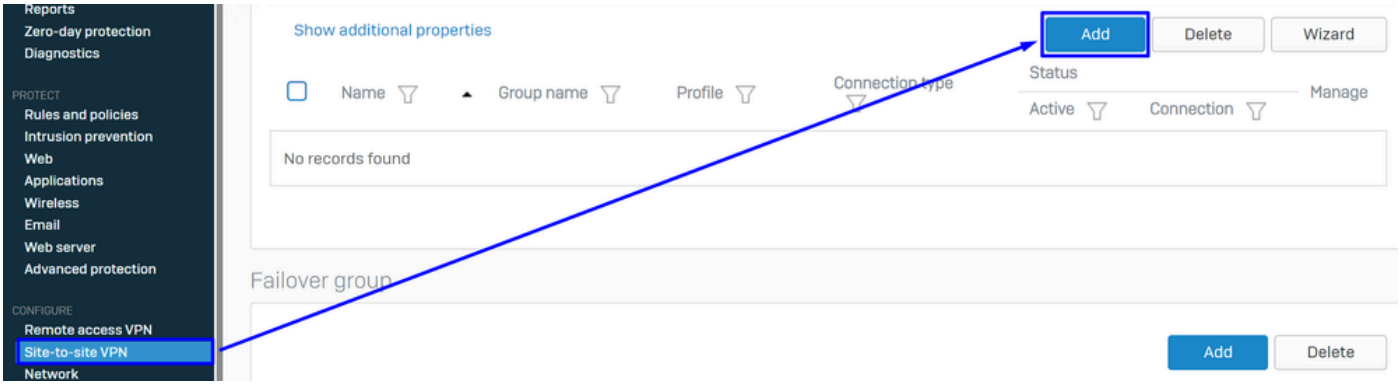


*Sophos - IPsec*配置檔案-失效對等體檢測

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**。

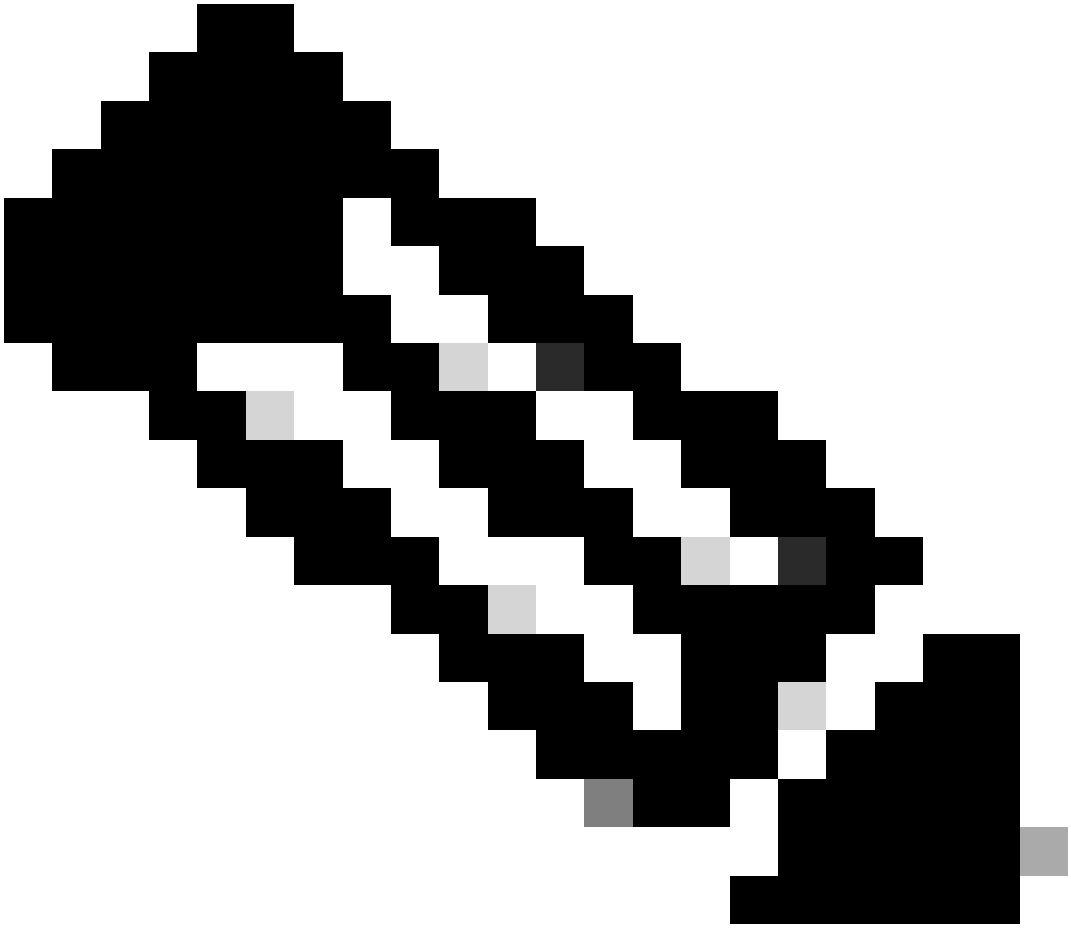


*Sophos -*站點到站點*VPN*

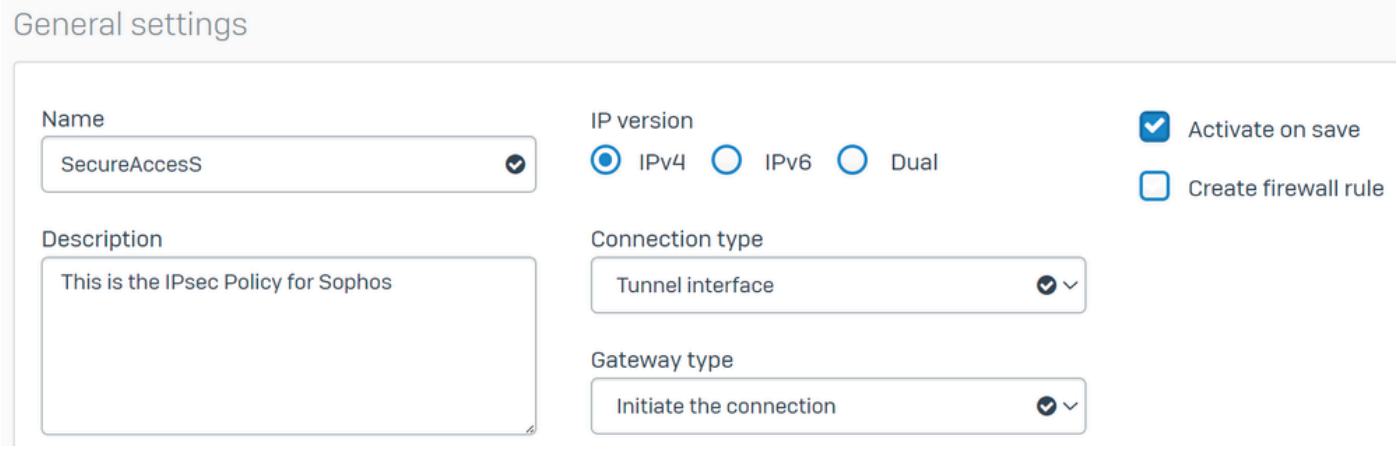
在**General Settings** 配置下：

- **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

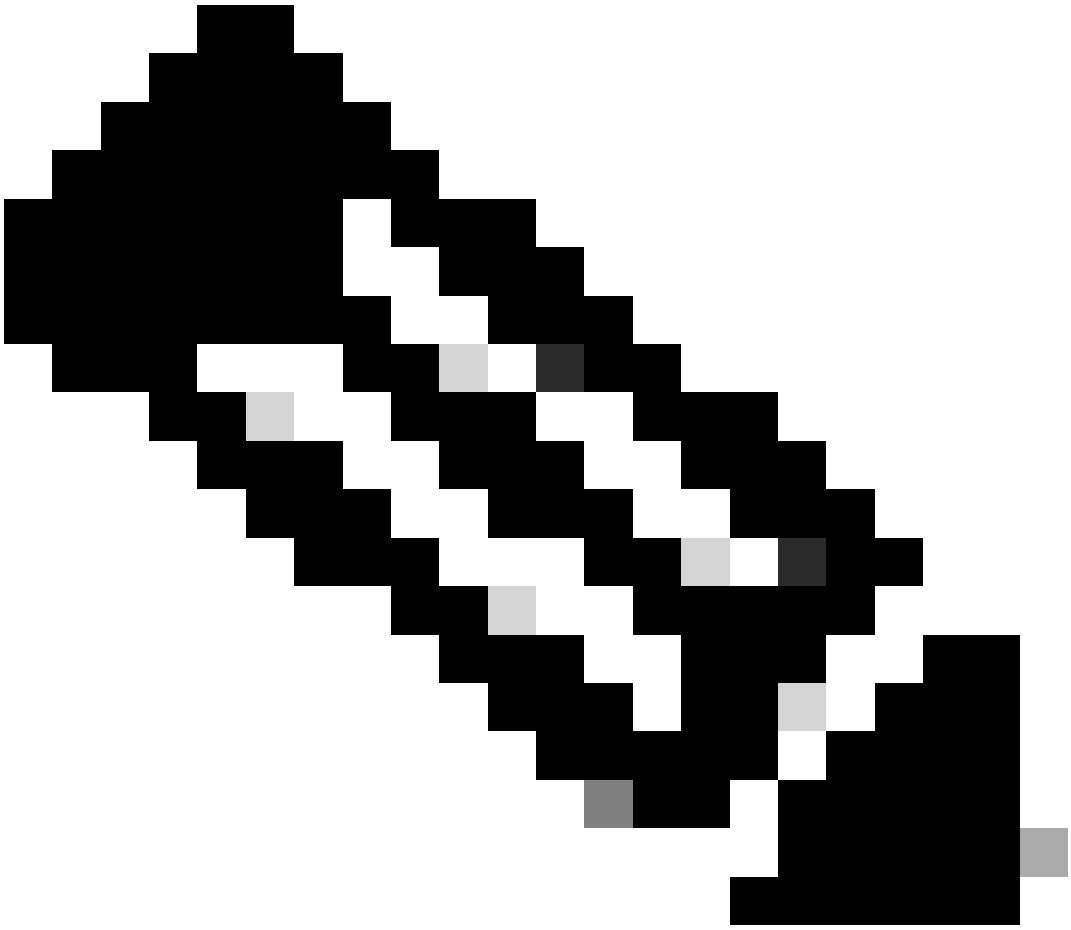
- Active on save：**選中該選項**



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。



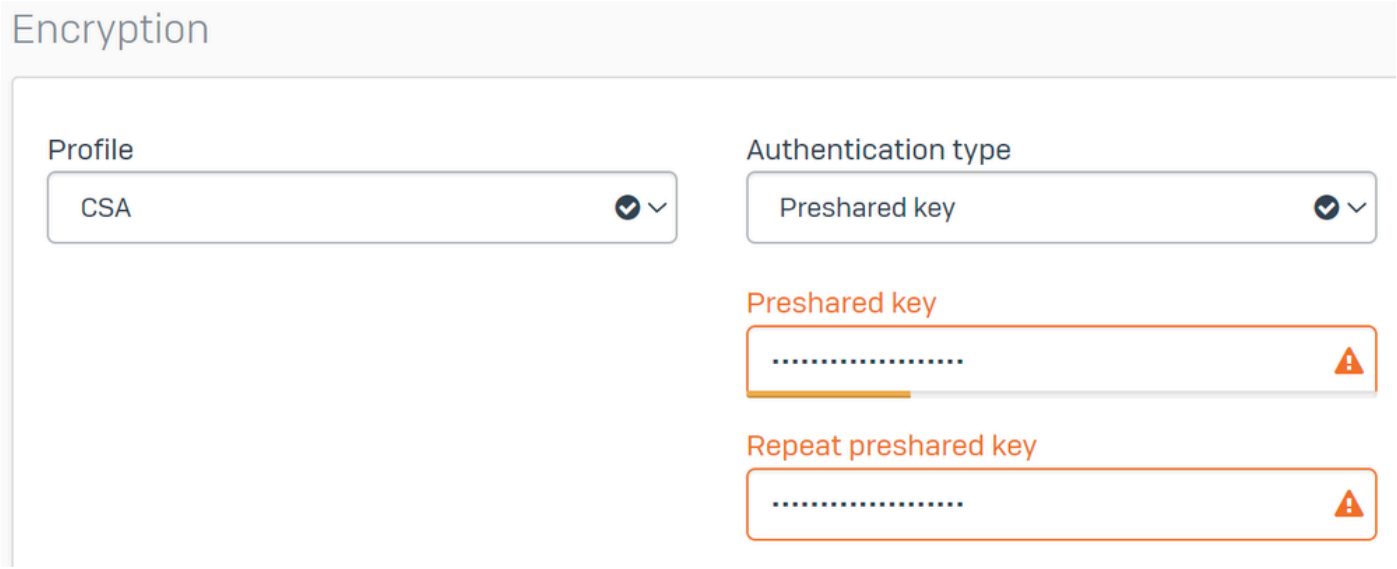
Sophos -站點到站點*VPN* -常規設定



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**

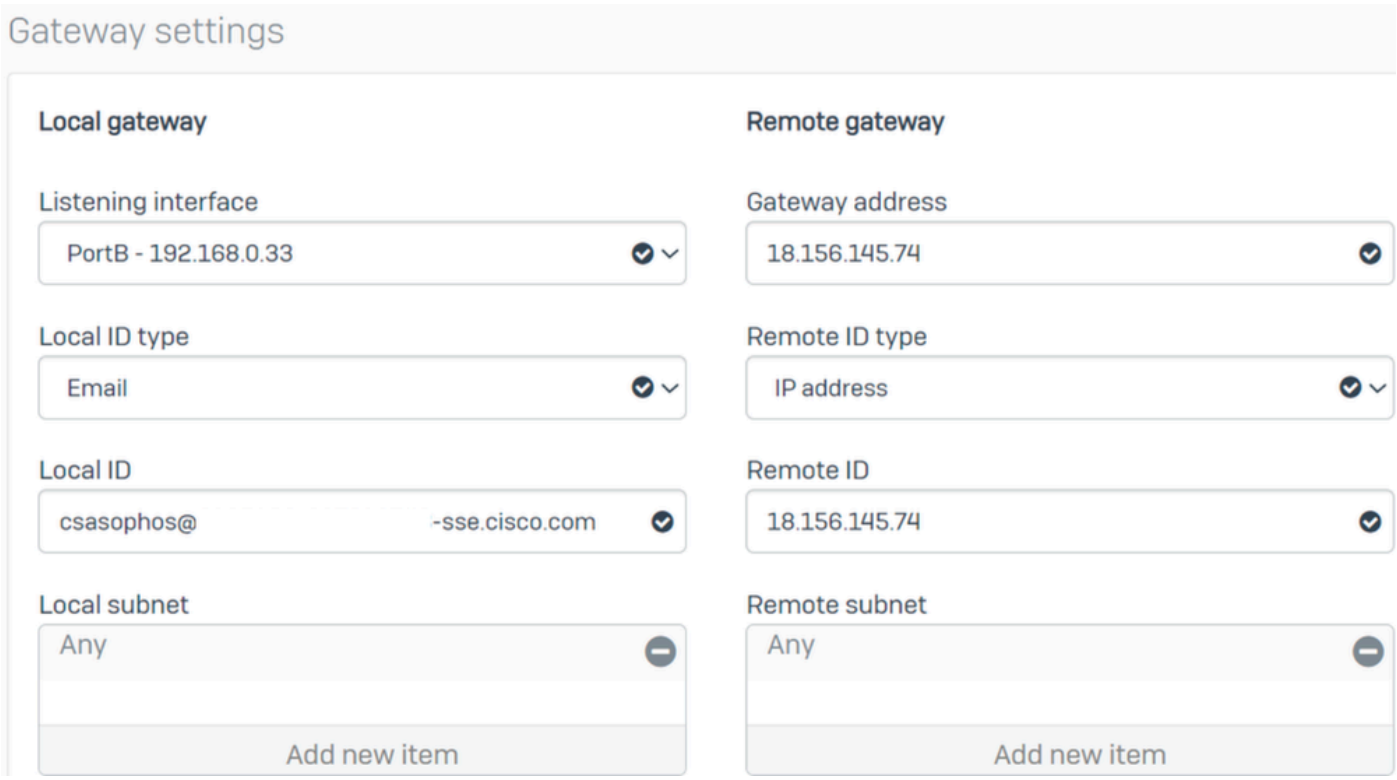


Sophos -站點到站點*VPN* -加密

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

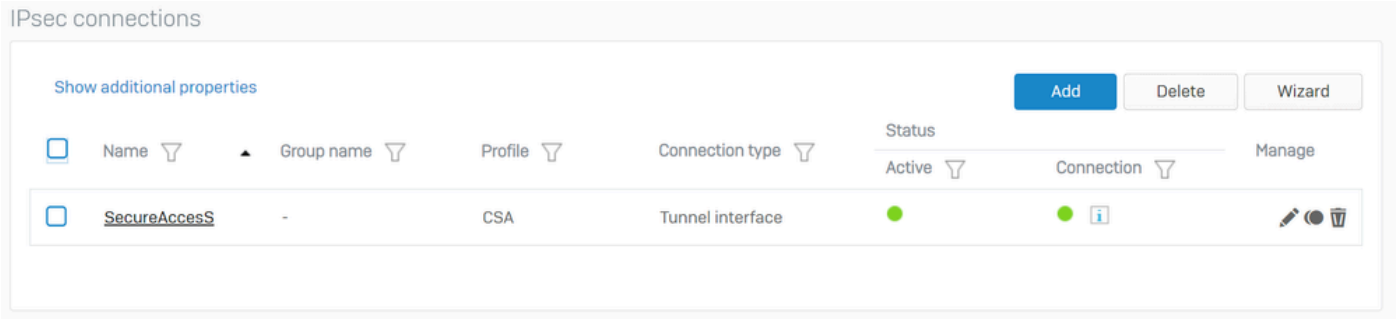
本地網關	遠端閘道
監聽介面 您的Wan-Internet介面	網關地址 在步驟中生成的公共IP， **Tunnel Data**
本地ID型別 電子郵件	遠端ID型別 IP 位址

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

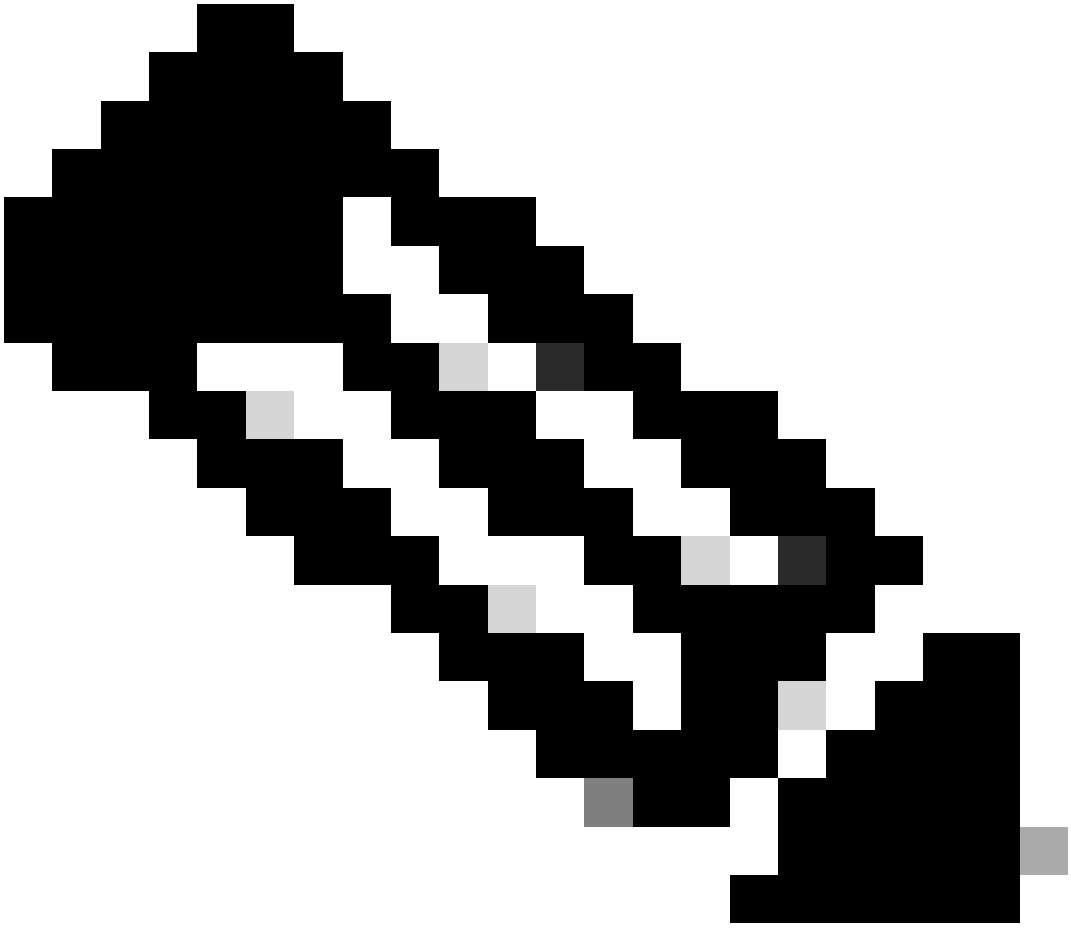


Sophos -站點到站點*VPN* -網關設定

隧道建立完成後，點選Save，您會看到已建立隧道。

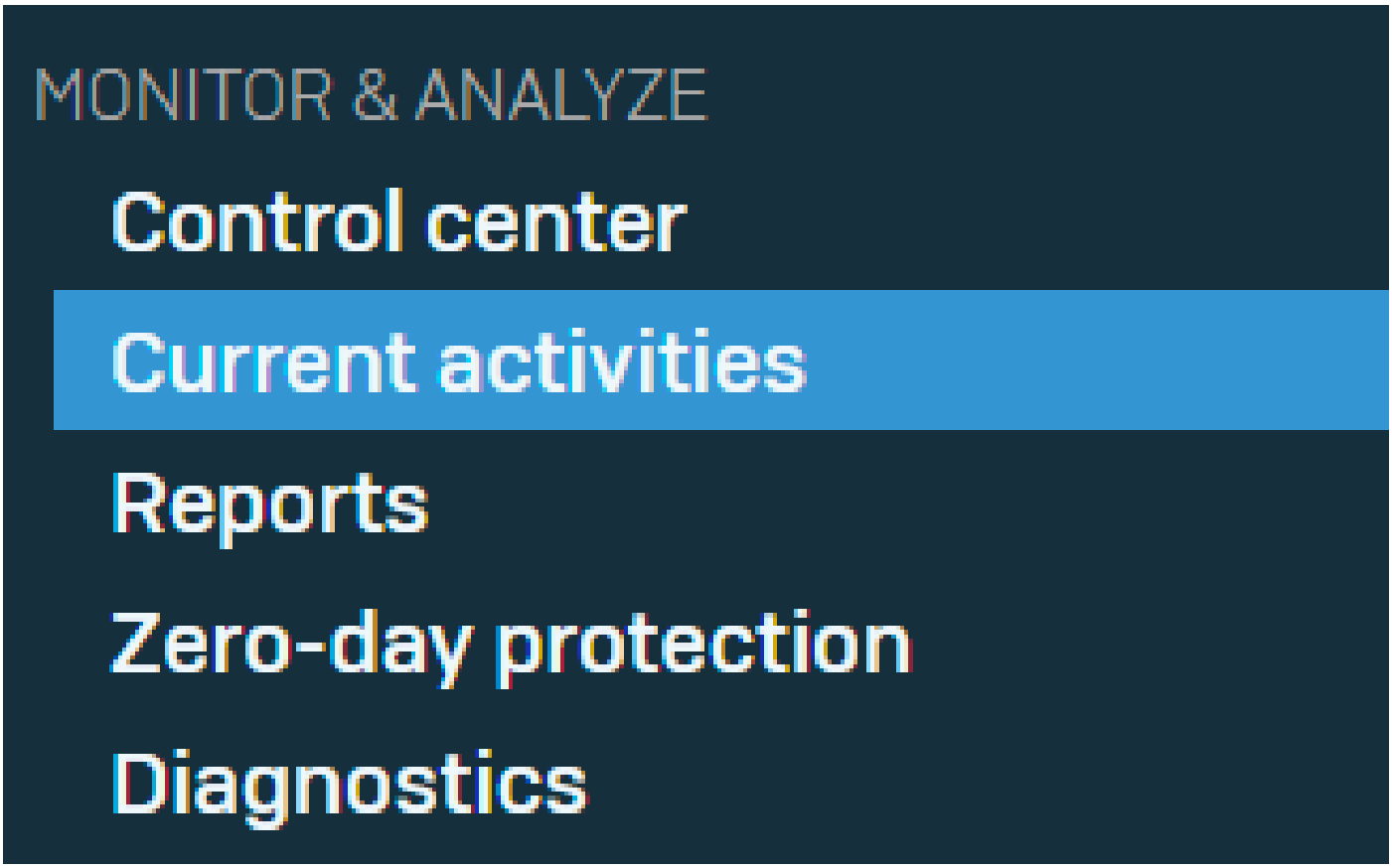


Sophos -站點到站點*VPN - IPsec*連線

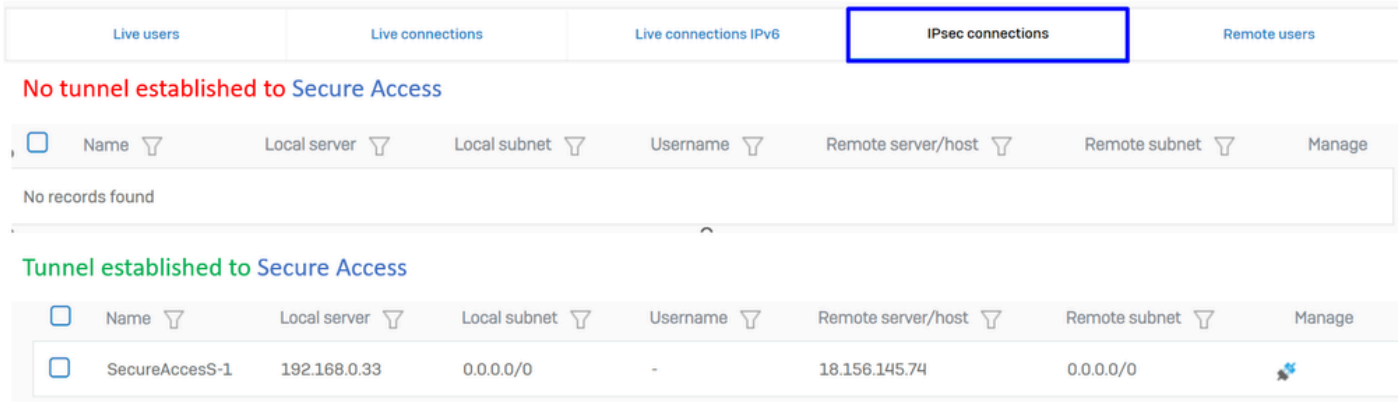


注意：要檢查隧道在最後一個映像上是否正確啟用，您可以檢查**Connection** 狀態；如果它是綠色的，表示隧道已連線；如果它不是綠色的，表示隧道未連線。

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



Sophos -監控和分析- *IPsec*



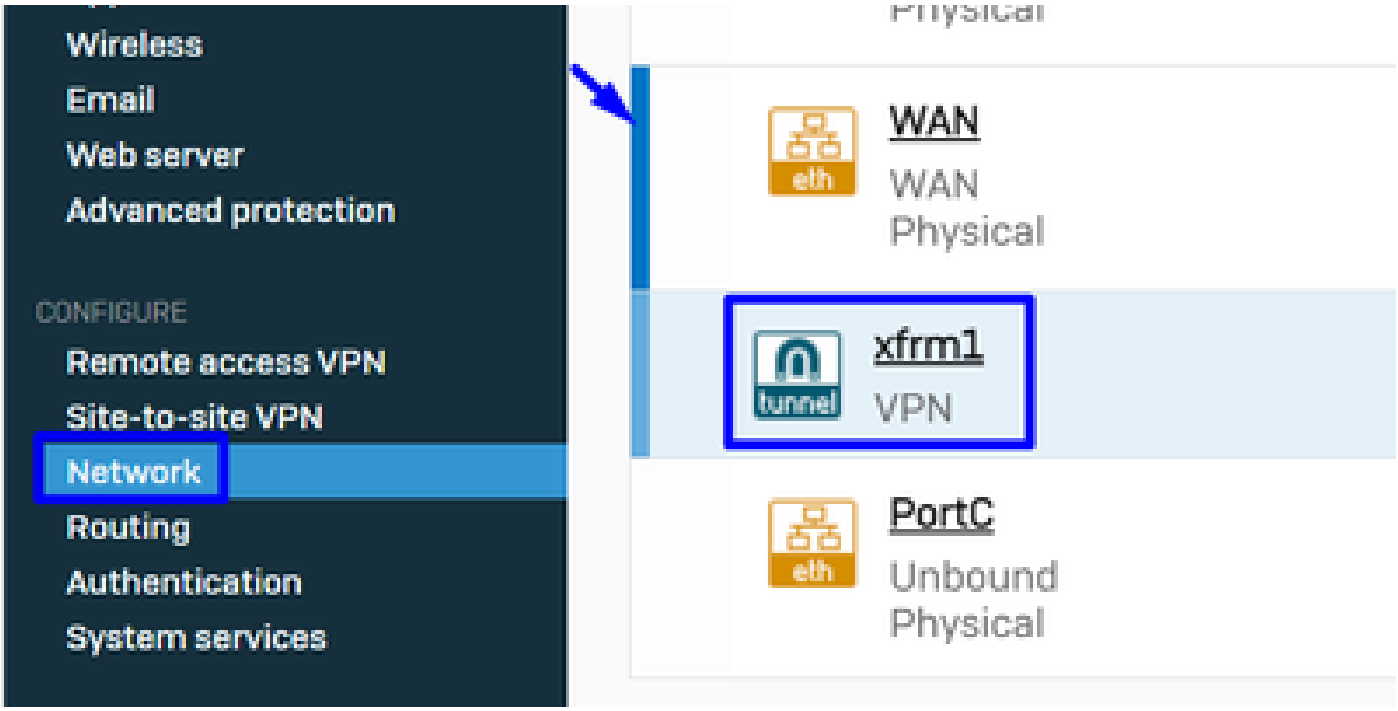
Sophos -監控和分析- *IPsec*前後

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

Sophos -網路-隧道介面-配置

配置網關

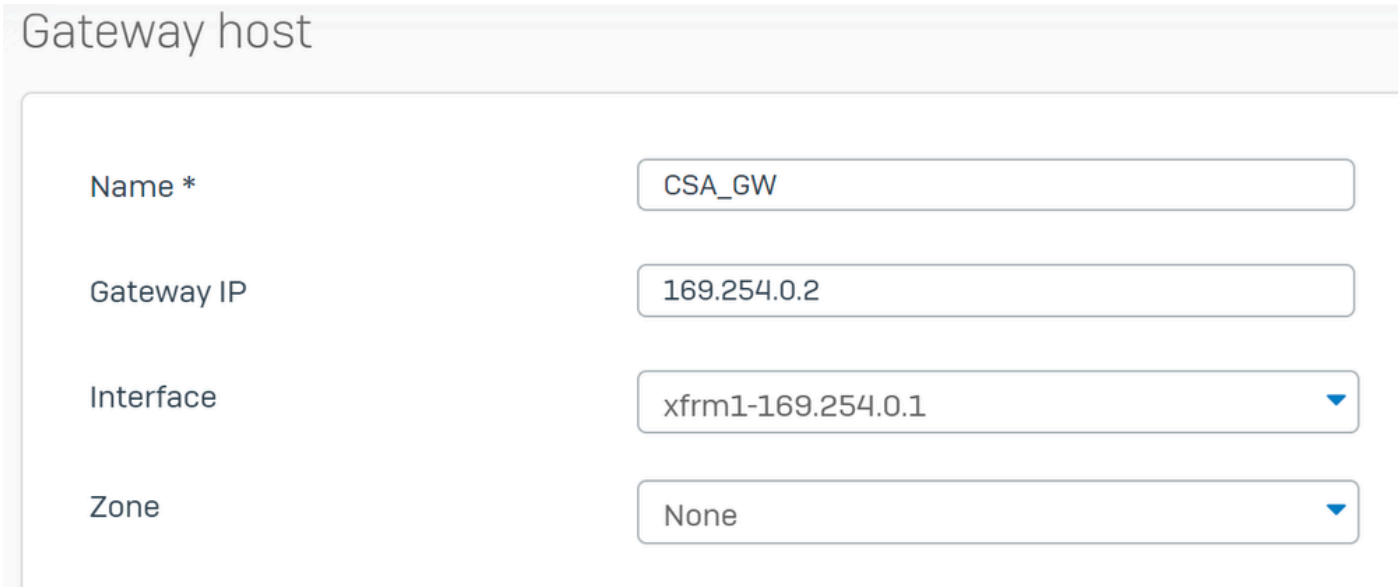
若要設定虛擬介面的閘道(xfrm)

- **導覽至** Routing > Gateways
- **按一下** Add

Sophos -路由-網關

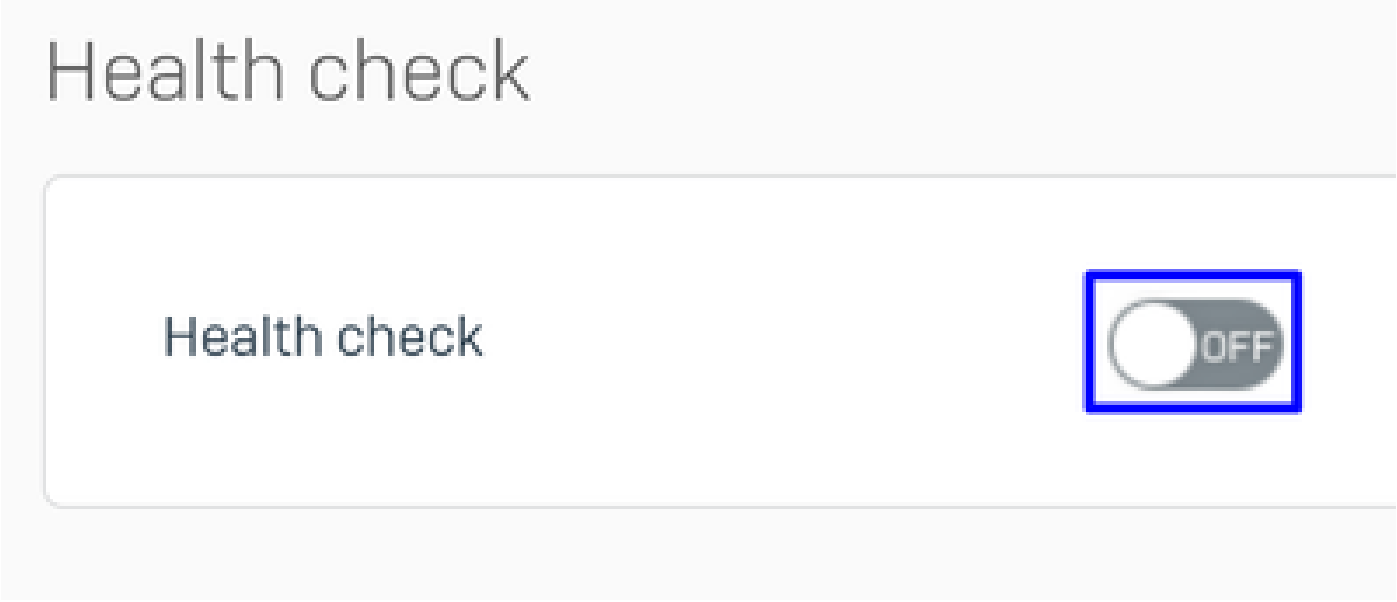
在Gateway host 配置下：

- **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）



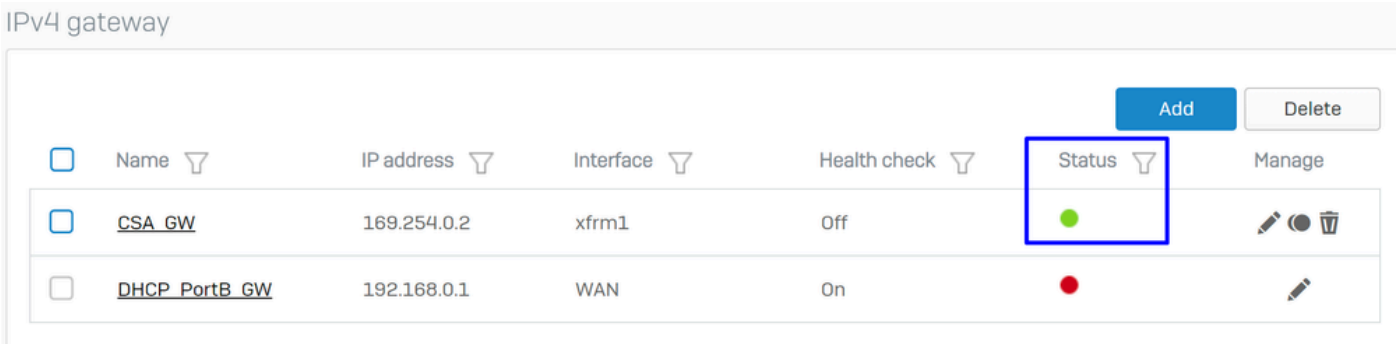
Sophos -路由-網關-網關主機

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



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：



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。

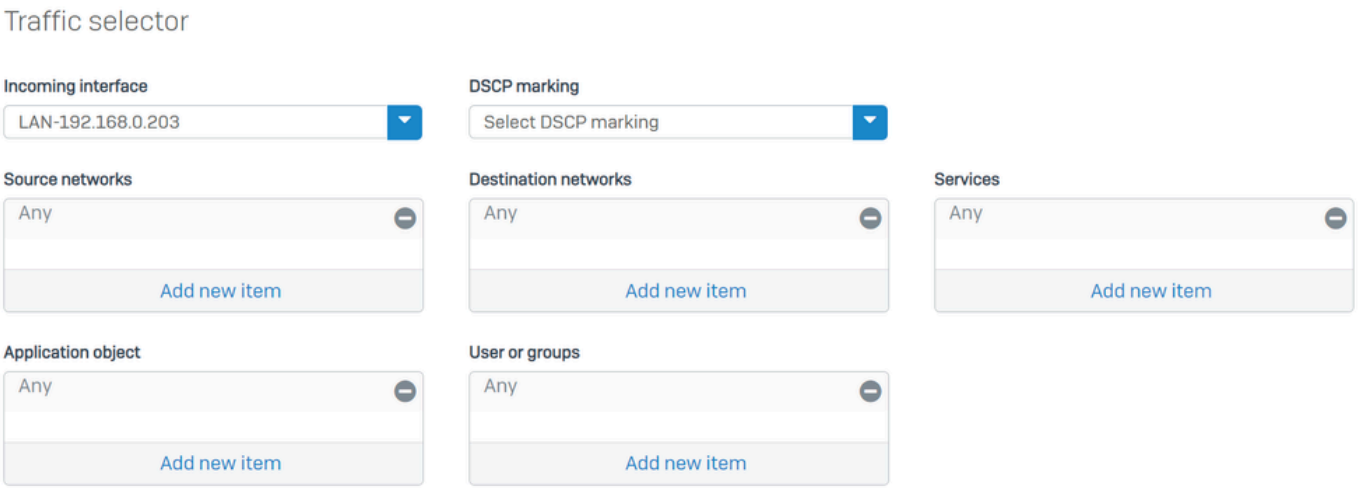
導覽至 Routing > SD-WAN routes.

- 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

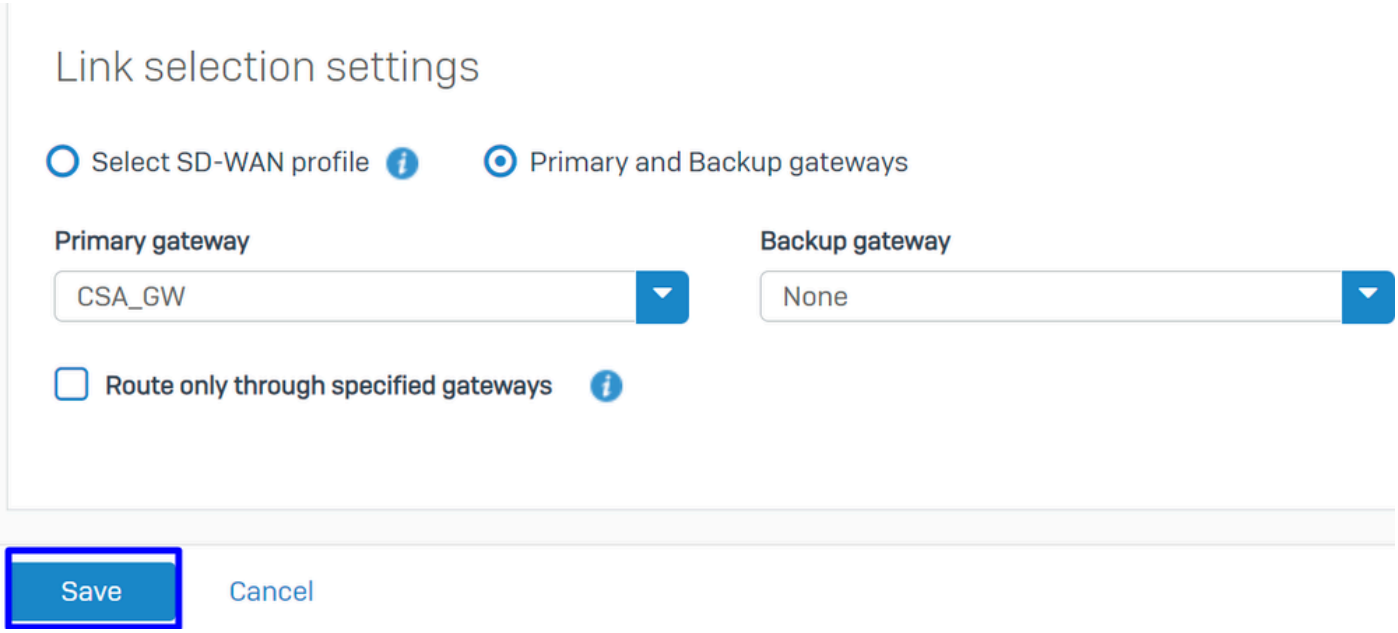


Sophos - SD-Wan路由-流量選擇器

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**



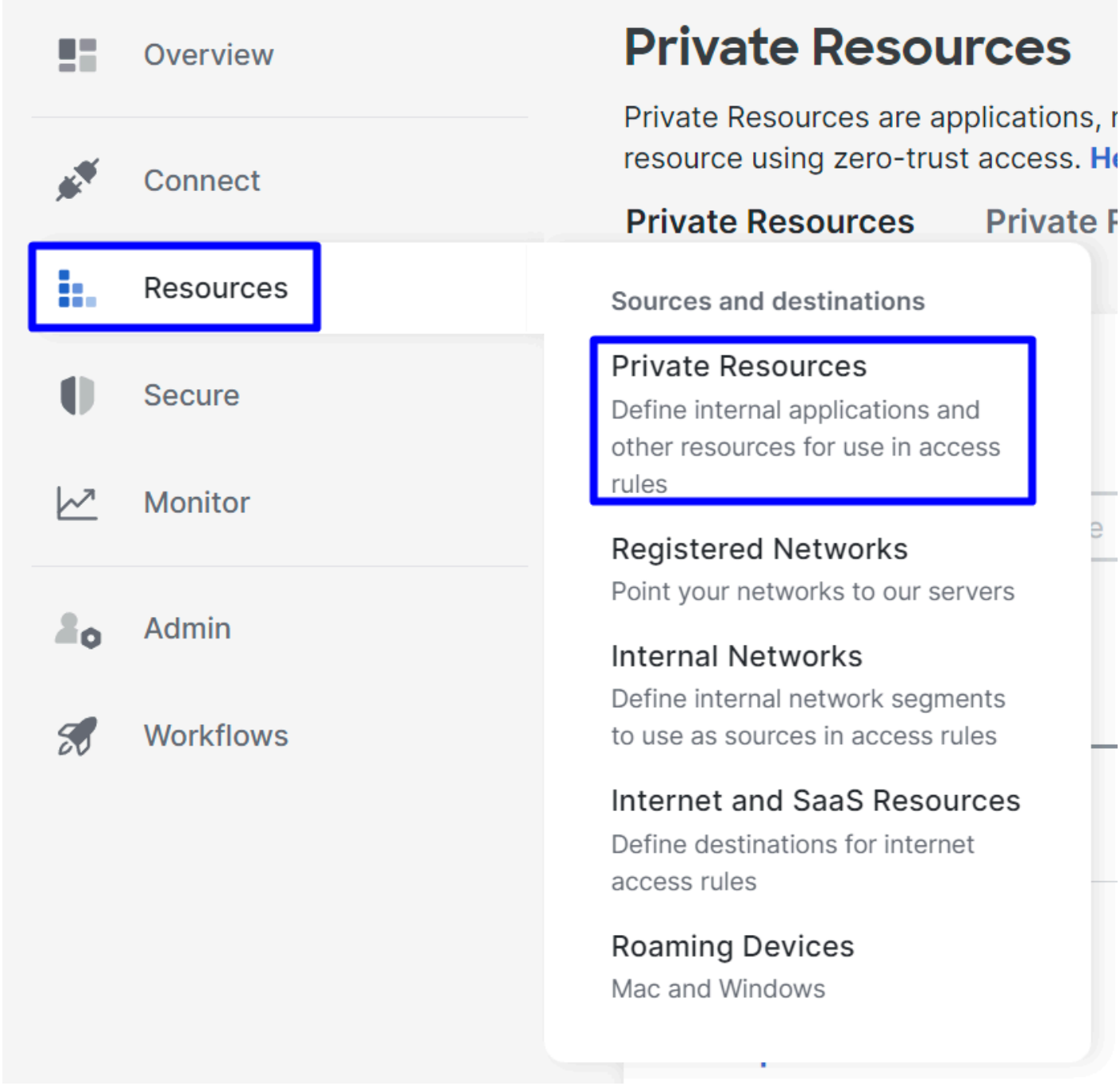
*Sophos - SD-Wan*路由-流量選擇器-主網關和備份網關

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

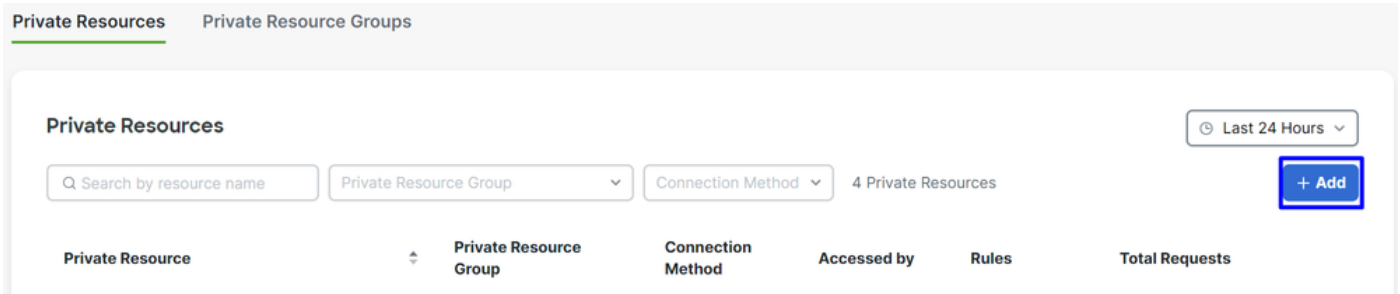
要配置專用應用訪問，請登入管理員門戶。

- 導覽至 **Resources** > **Private Resources**



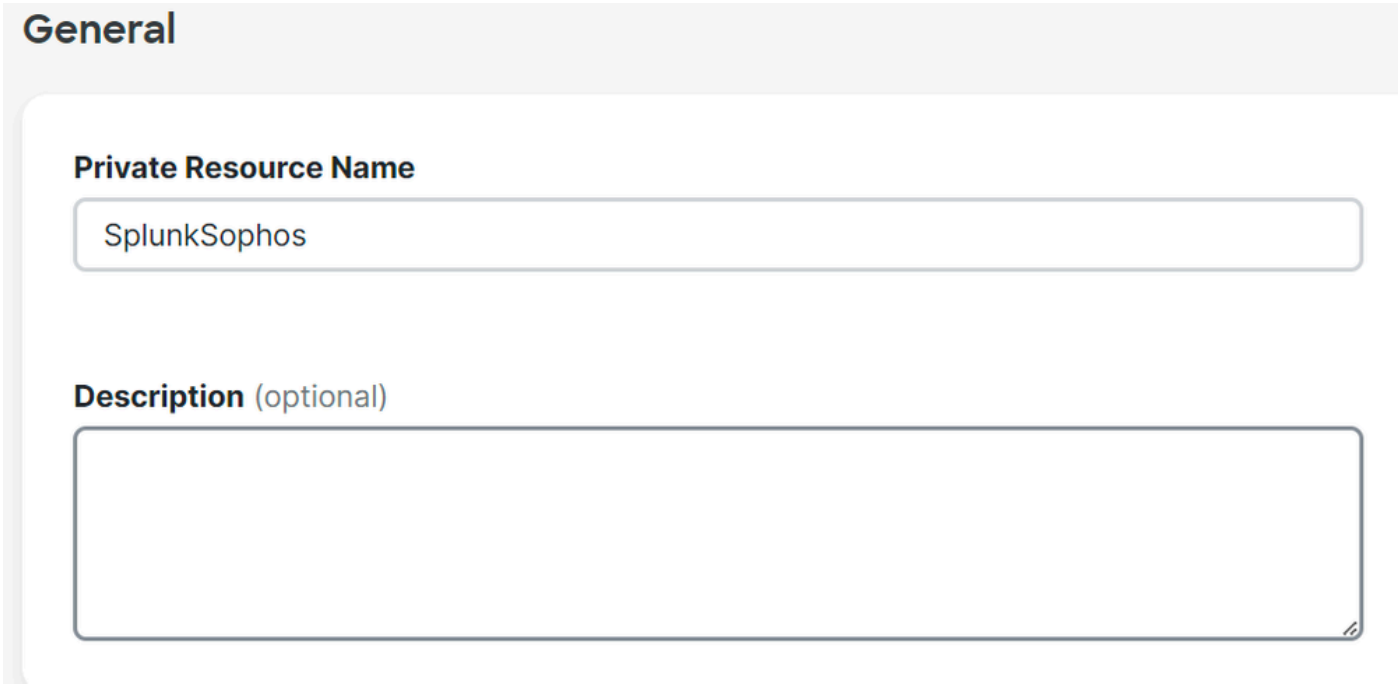
安全存取-私人資源

- 按一下 + Add



安全存取-私人資源2

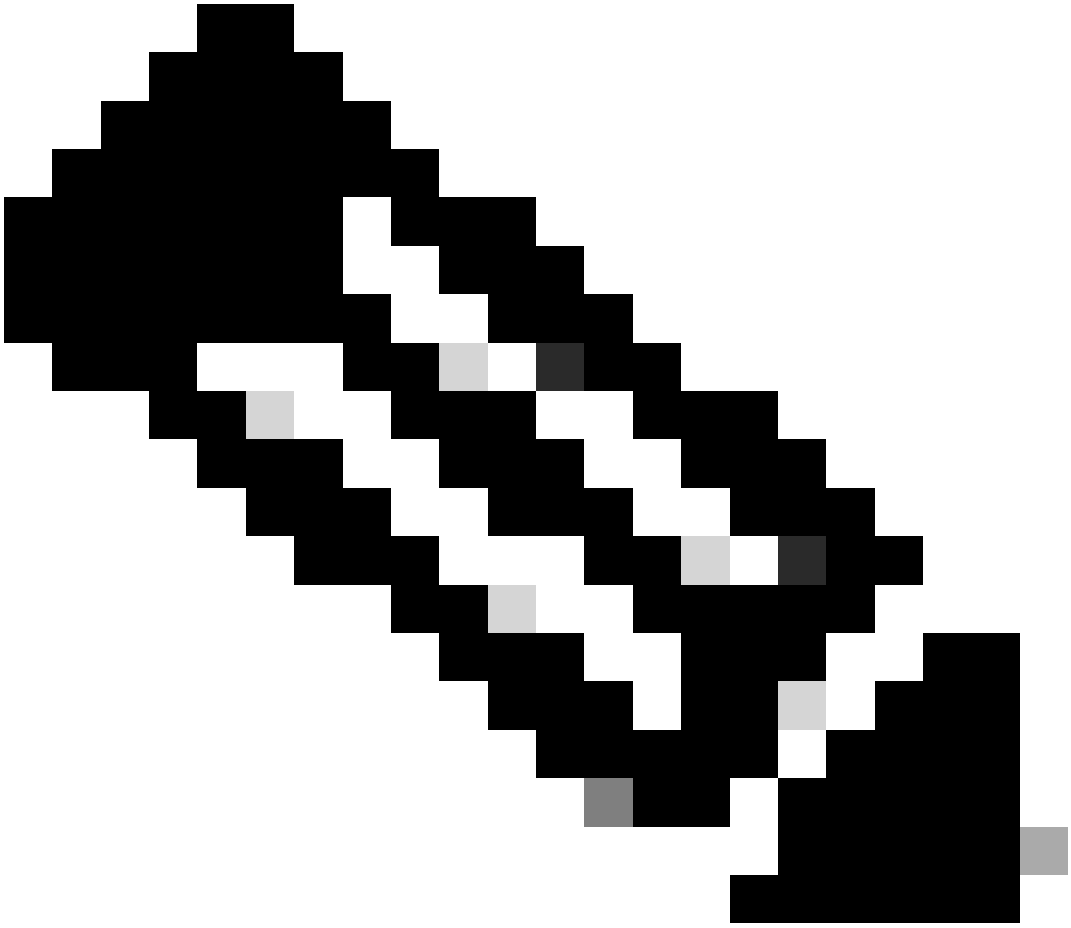
- 在**General 配置下， Private Resource Name**



安全存取-私人資源-一般

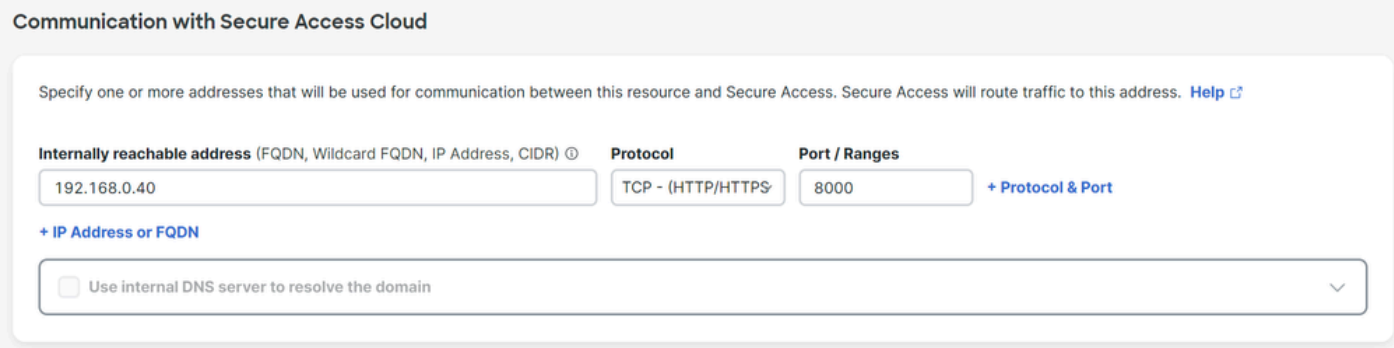
在Communication with Secure Access Cloud 配置下：

- **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。

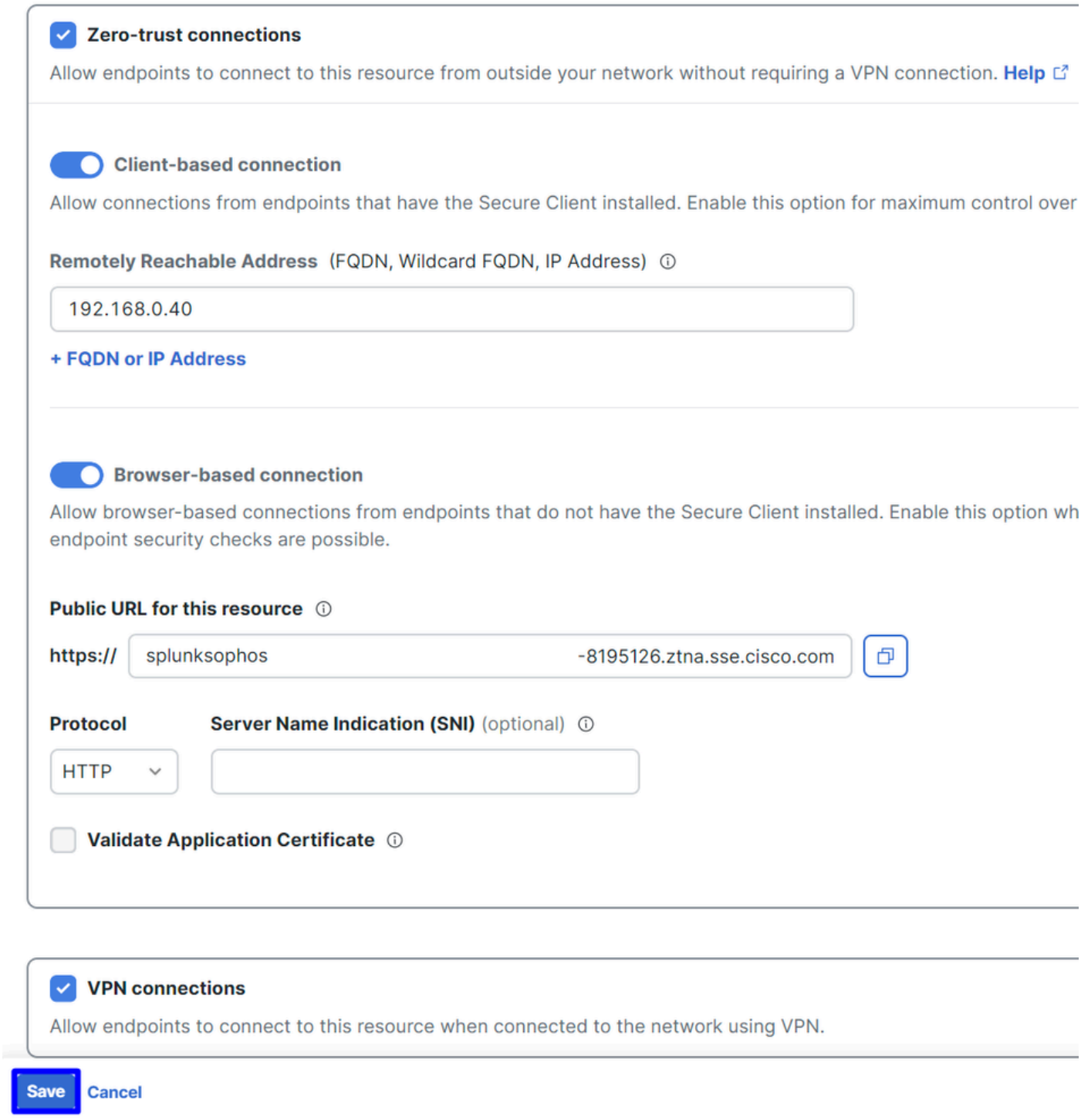
- **Protocol**：選擇用於訪問該資源的協定
- Port / Ranges ：選擇需要啟用的埠以訪問應用



安全訪問-私有資源-透過安全訪問雲進行通訊

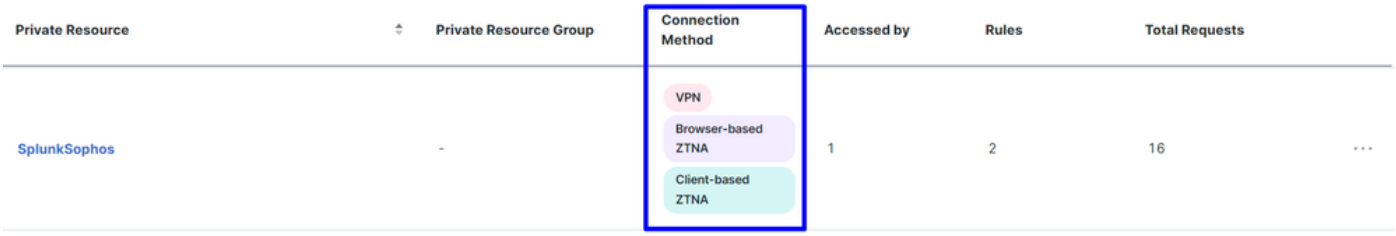
在中 **Endpoint Connection Methods**，您可以配置透過Secure Access訪問專用資源的所有可能方式，並選擇您要用於您的環境的方法：

- **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**



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：

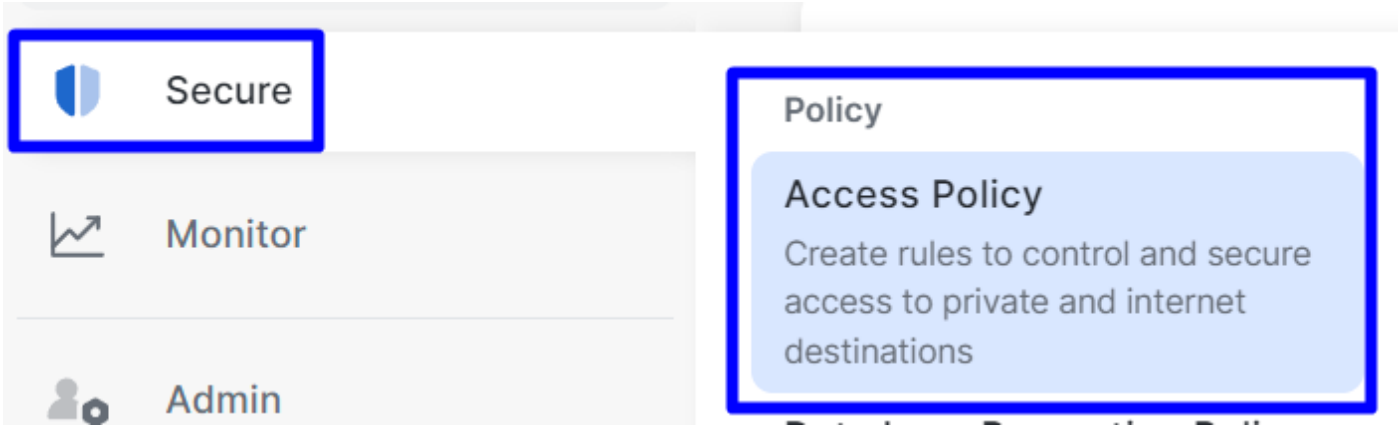


安全訪問-已配置專用資源

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

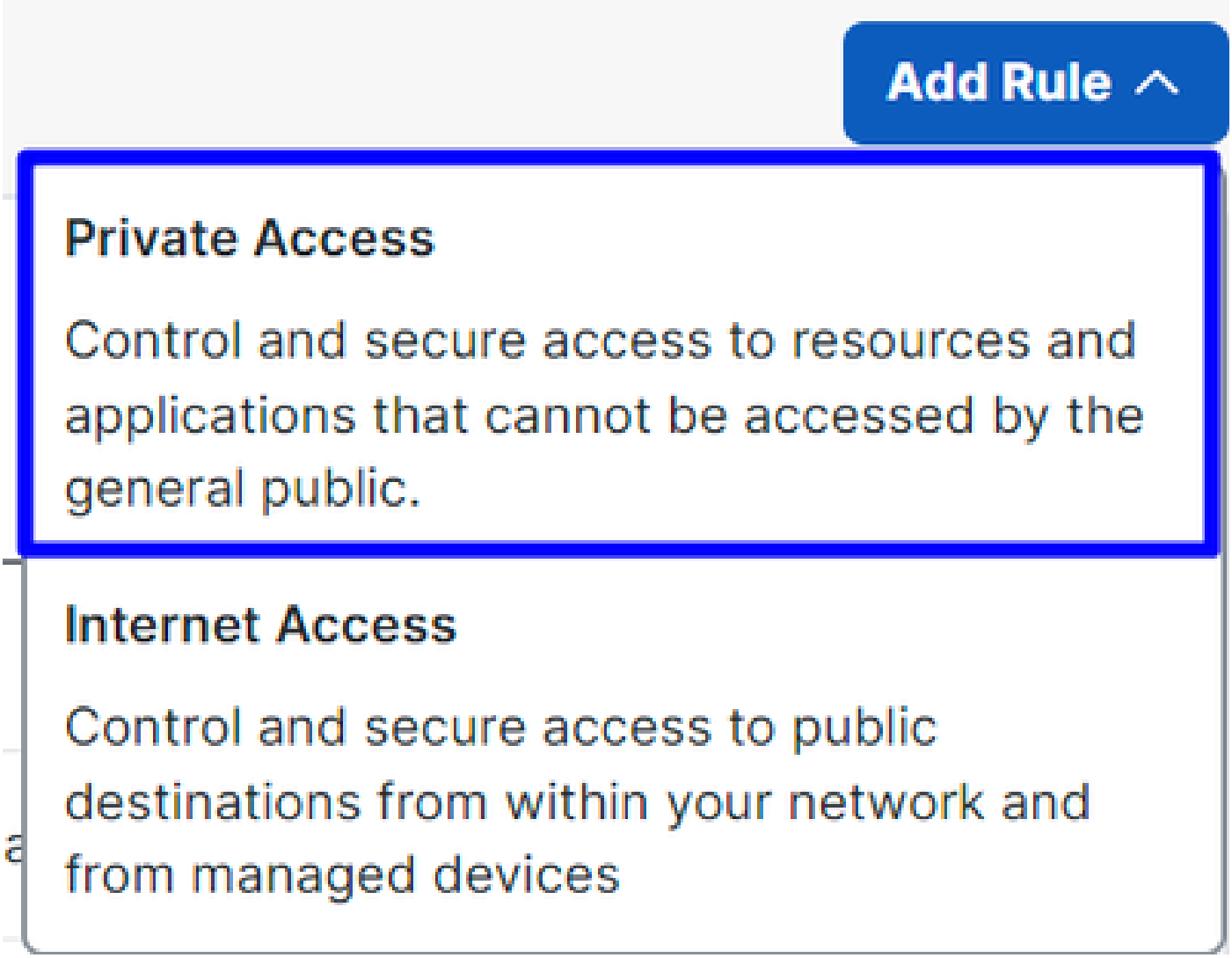
配置訪問策略

要配置訪問策略，請導航到Secure > Access Policy。



安全訪問-訪問策略

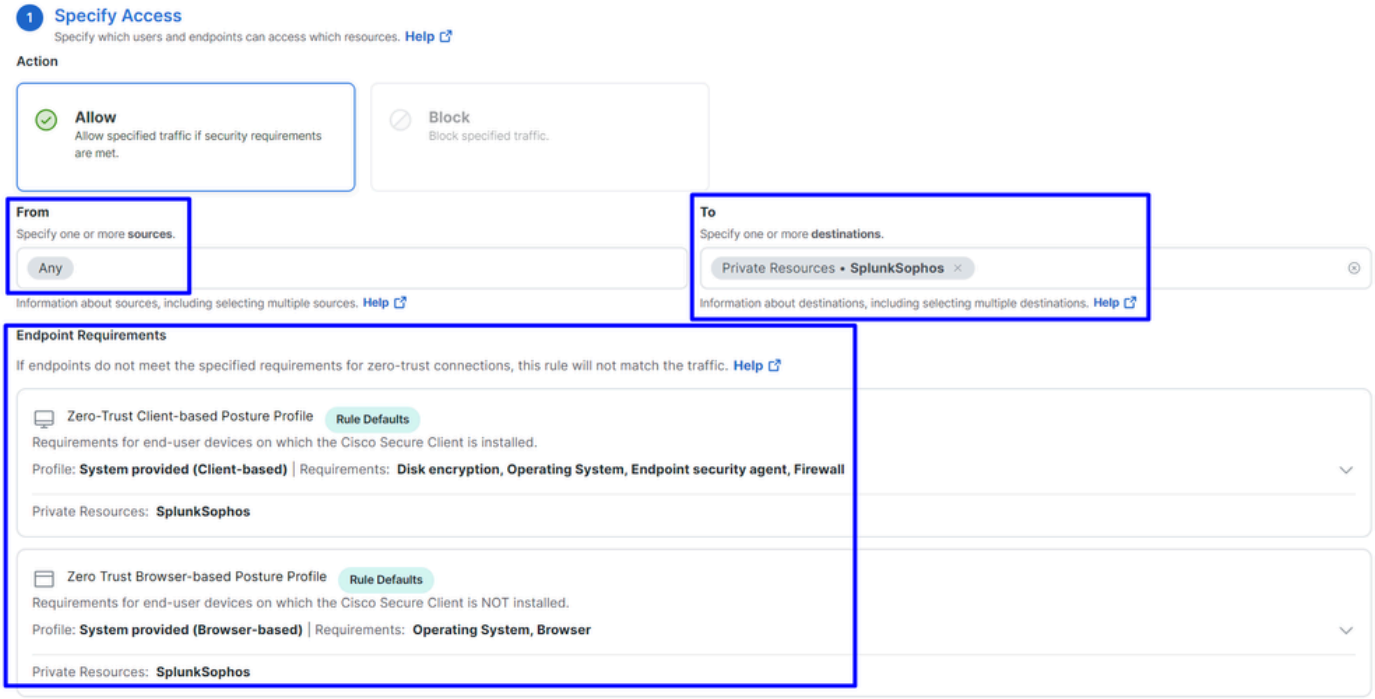
- 按一下 **Add Rule** > **Private Access**



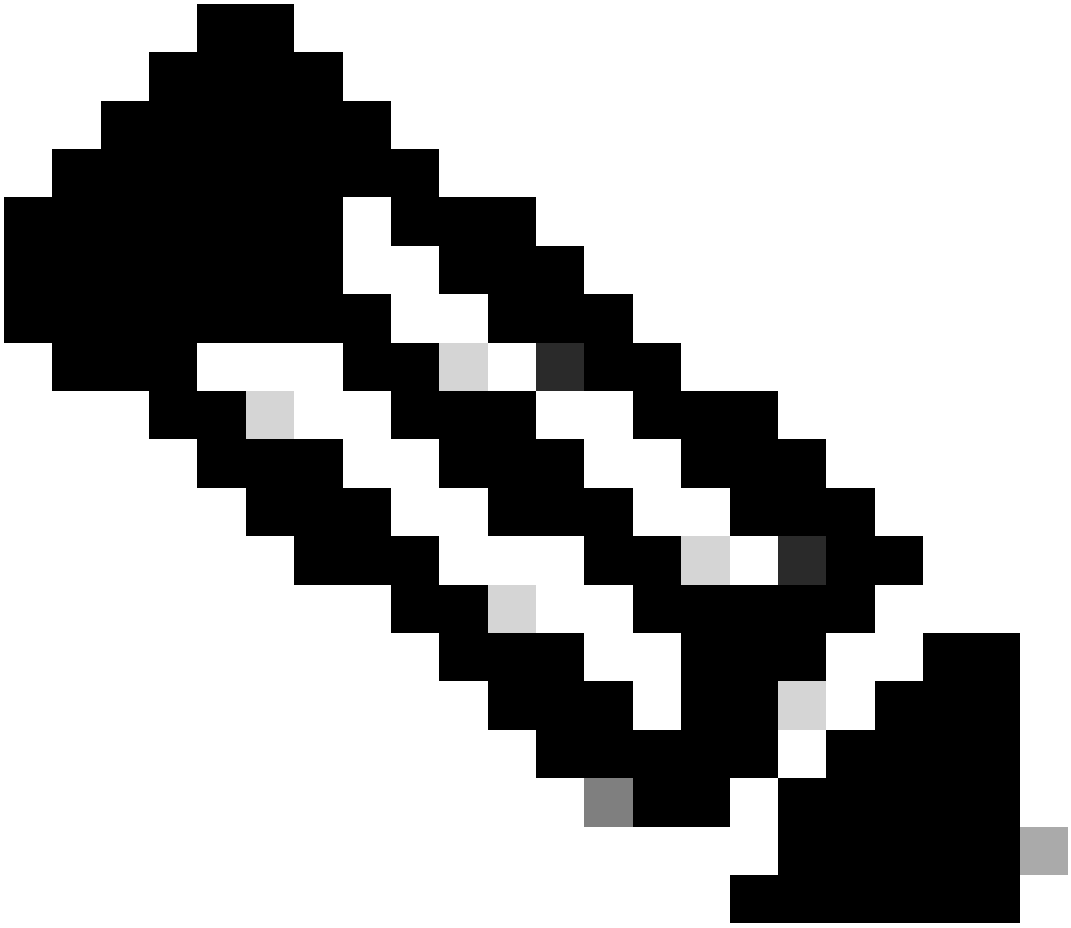
安全訪問-訪問策略-專用訪問

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**

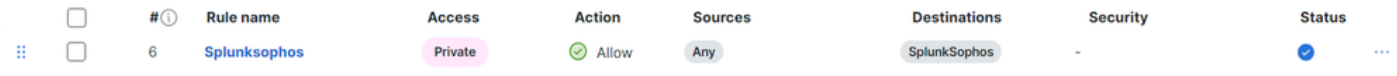


安全存取-存取原則-指定存取



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：



安全訪問-已配置訪問策略

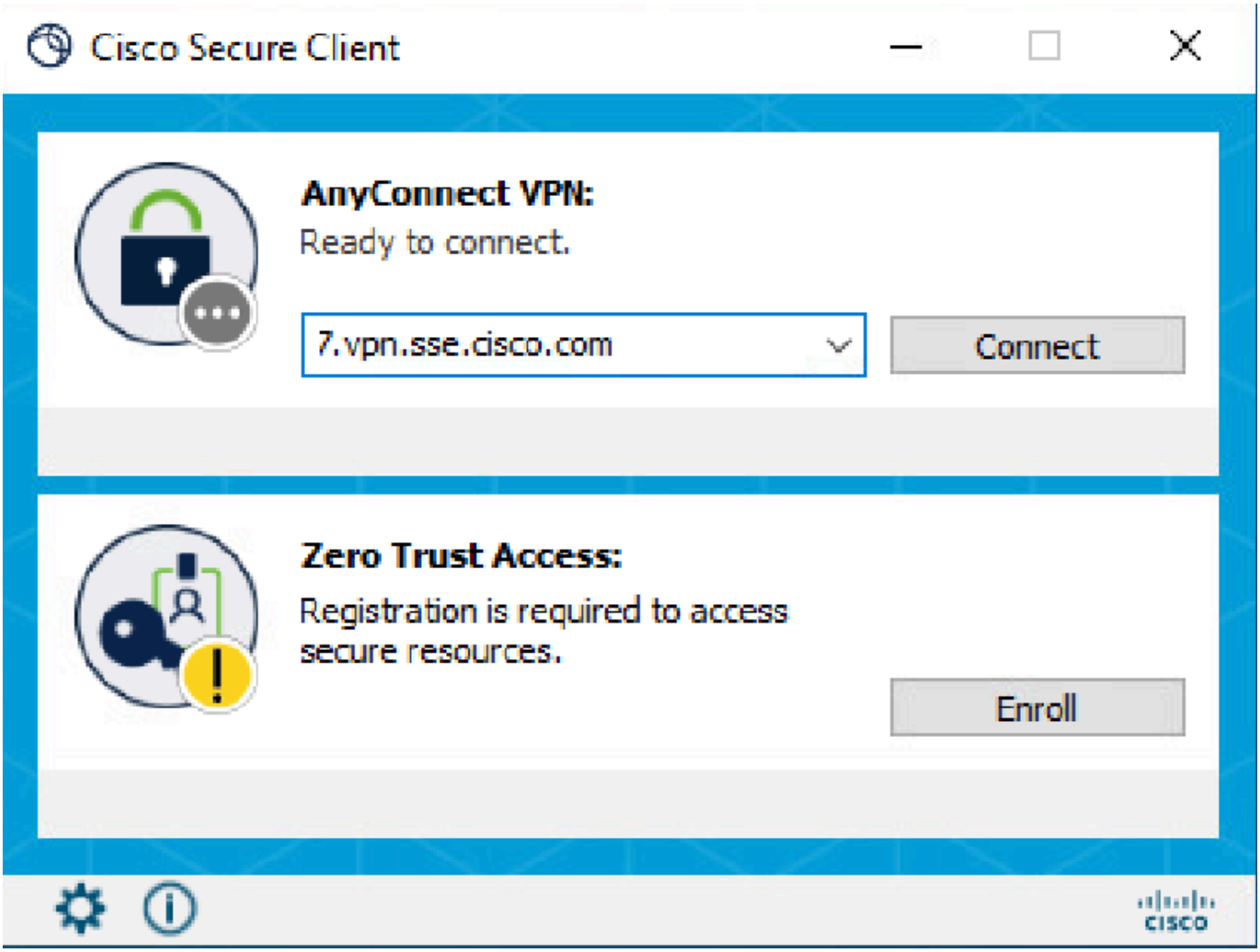
之後，您可以繼續步驟Verify。

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。

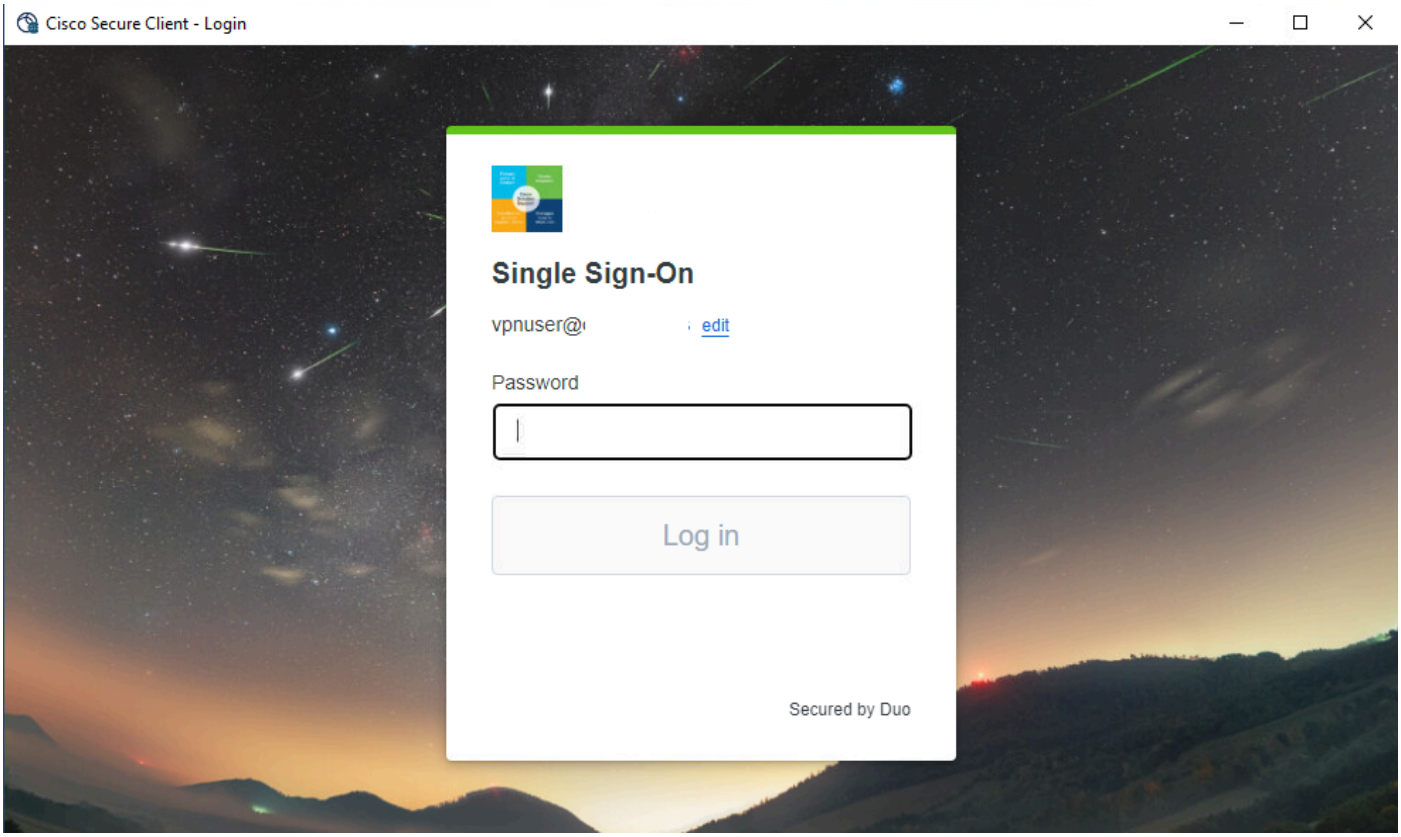
RA-VPN

透過Cisco Secure Client Agent-VPN登入。



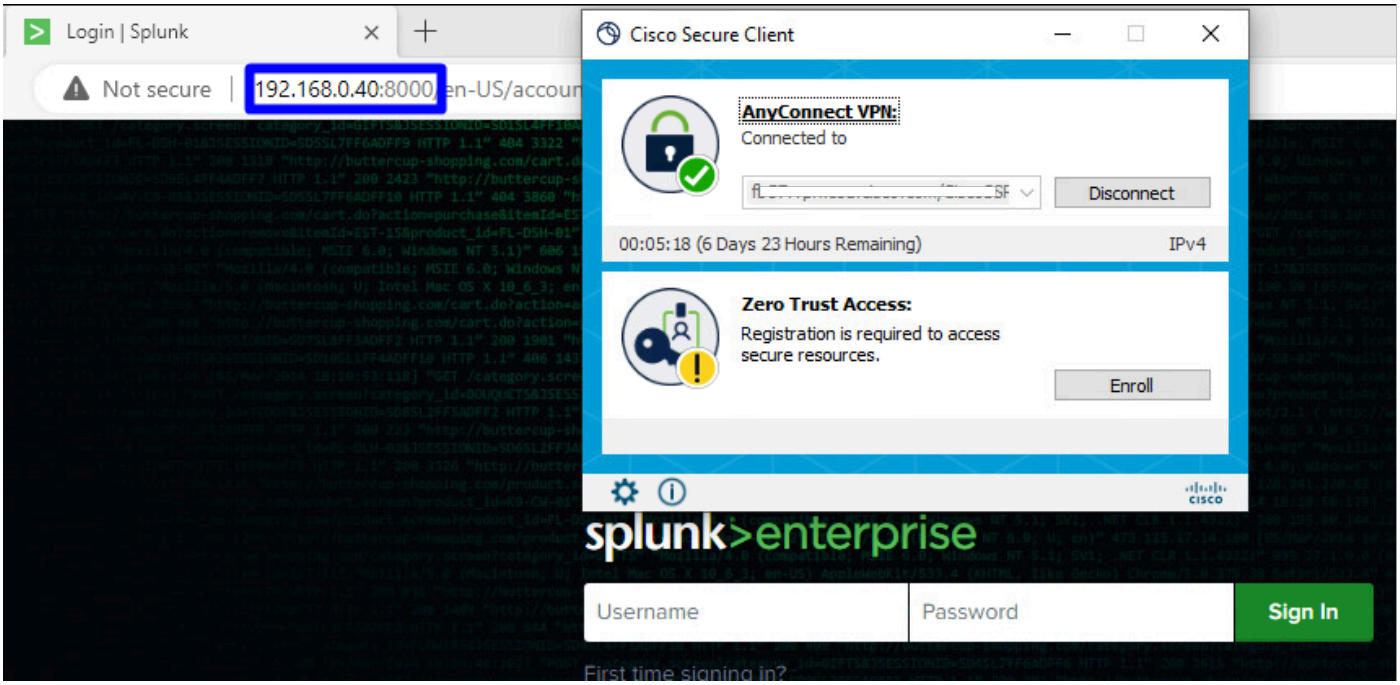
安全客戶端- *VPN*

- 透過您的SSO提供商進行身份驗證



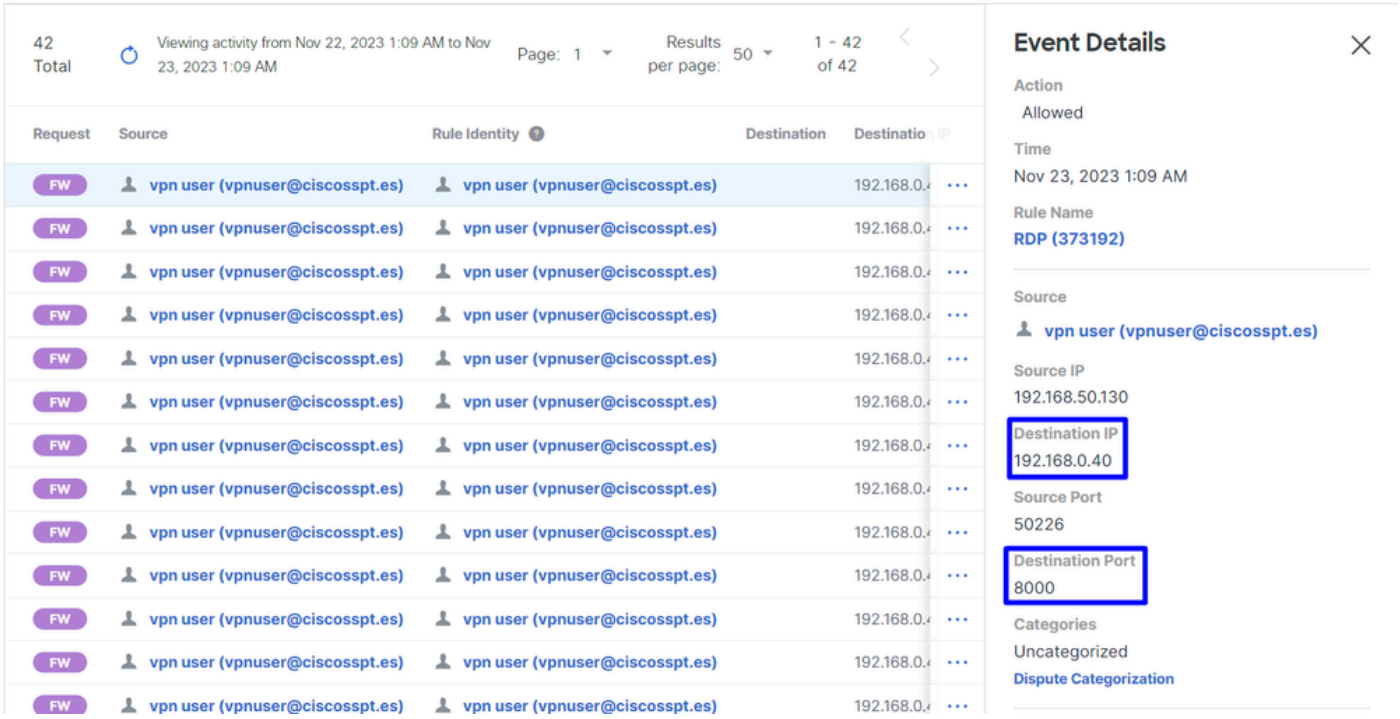
安全訪問- *VPN - SSO*

- **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

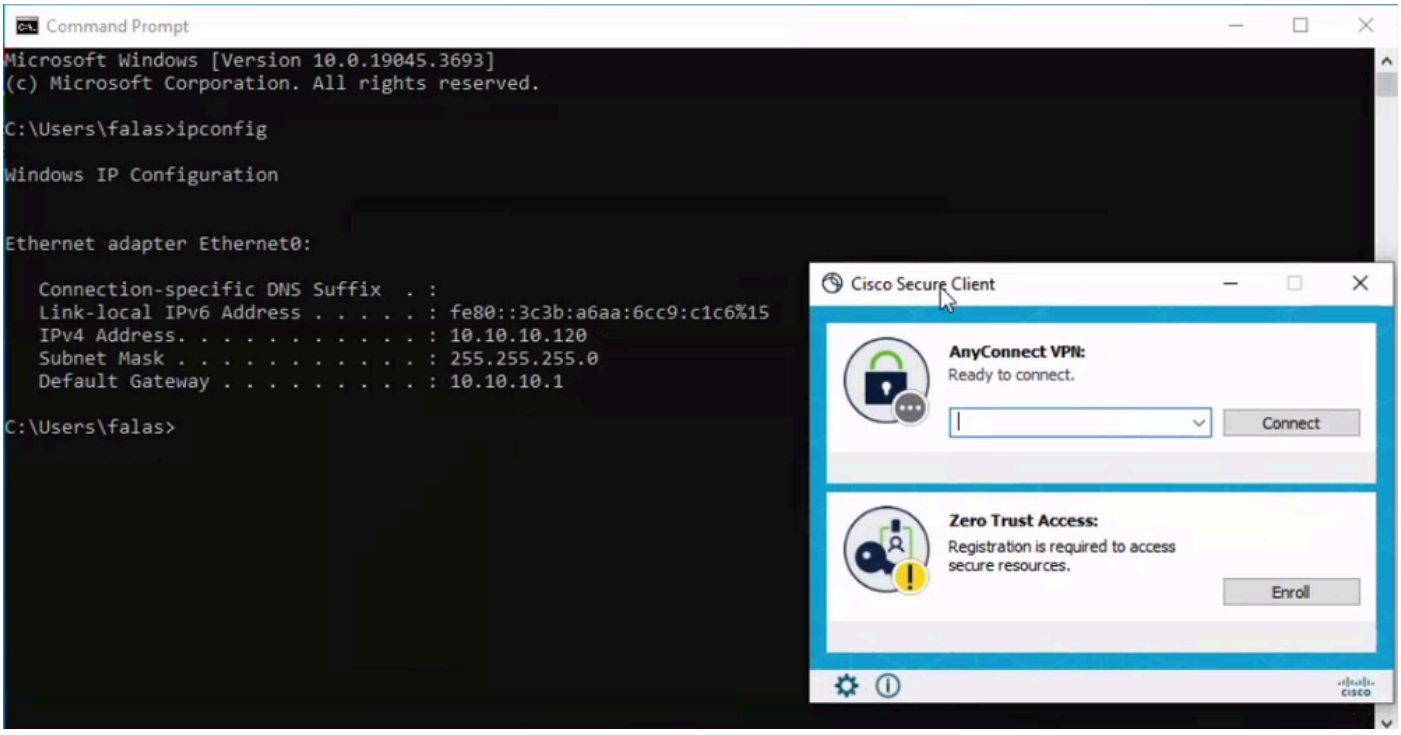


安全訪問-活動搜尋- *RA-VPN*

您可以看到使用者被允許透過RA-VPN進行身份驗證。

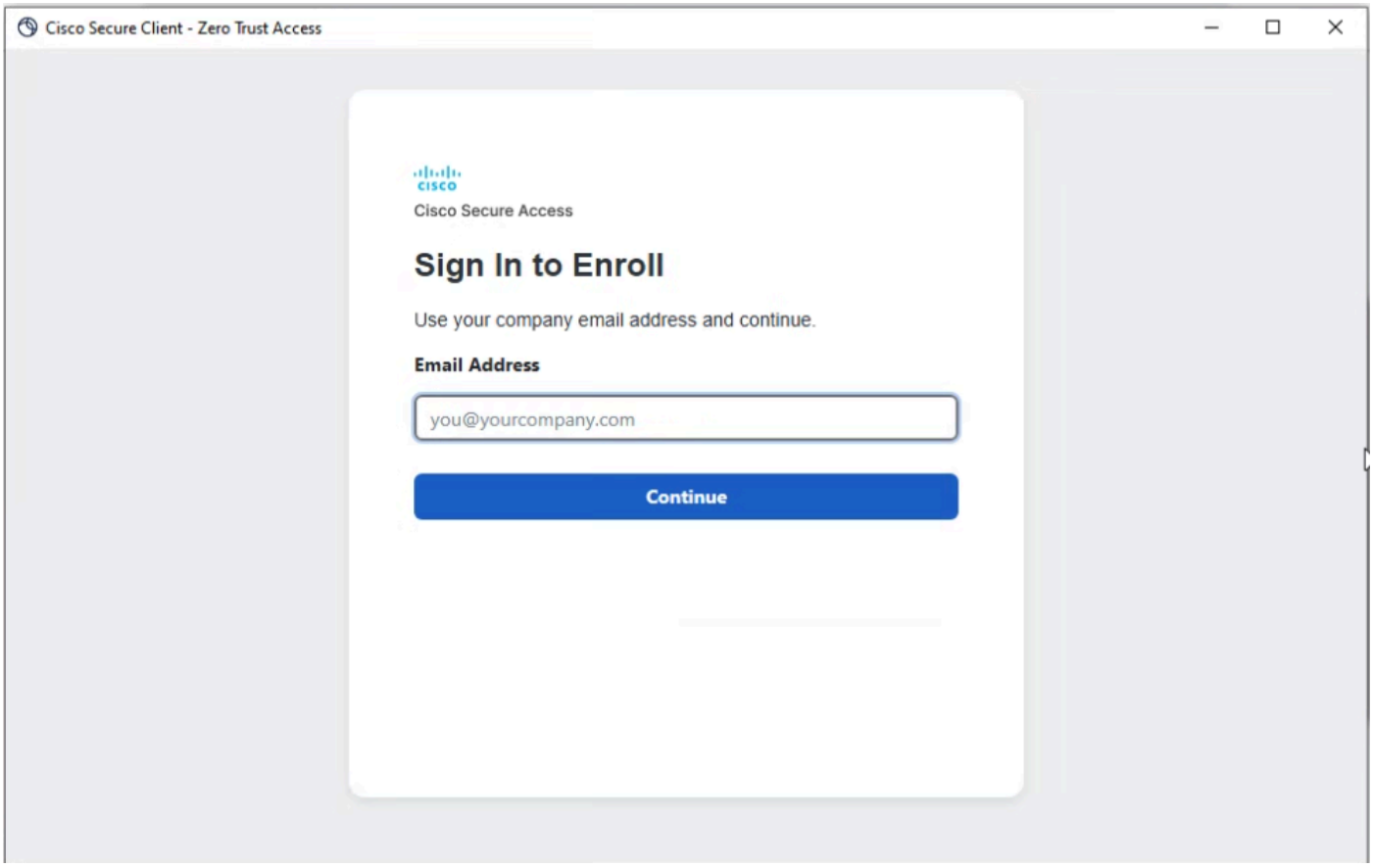
使用者端基礎ZTNA

透過Cisco Secure Client Agent - ZTNA登入



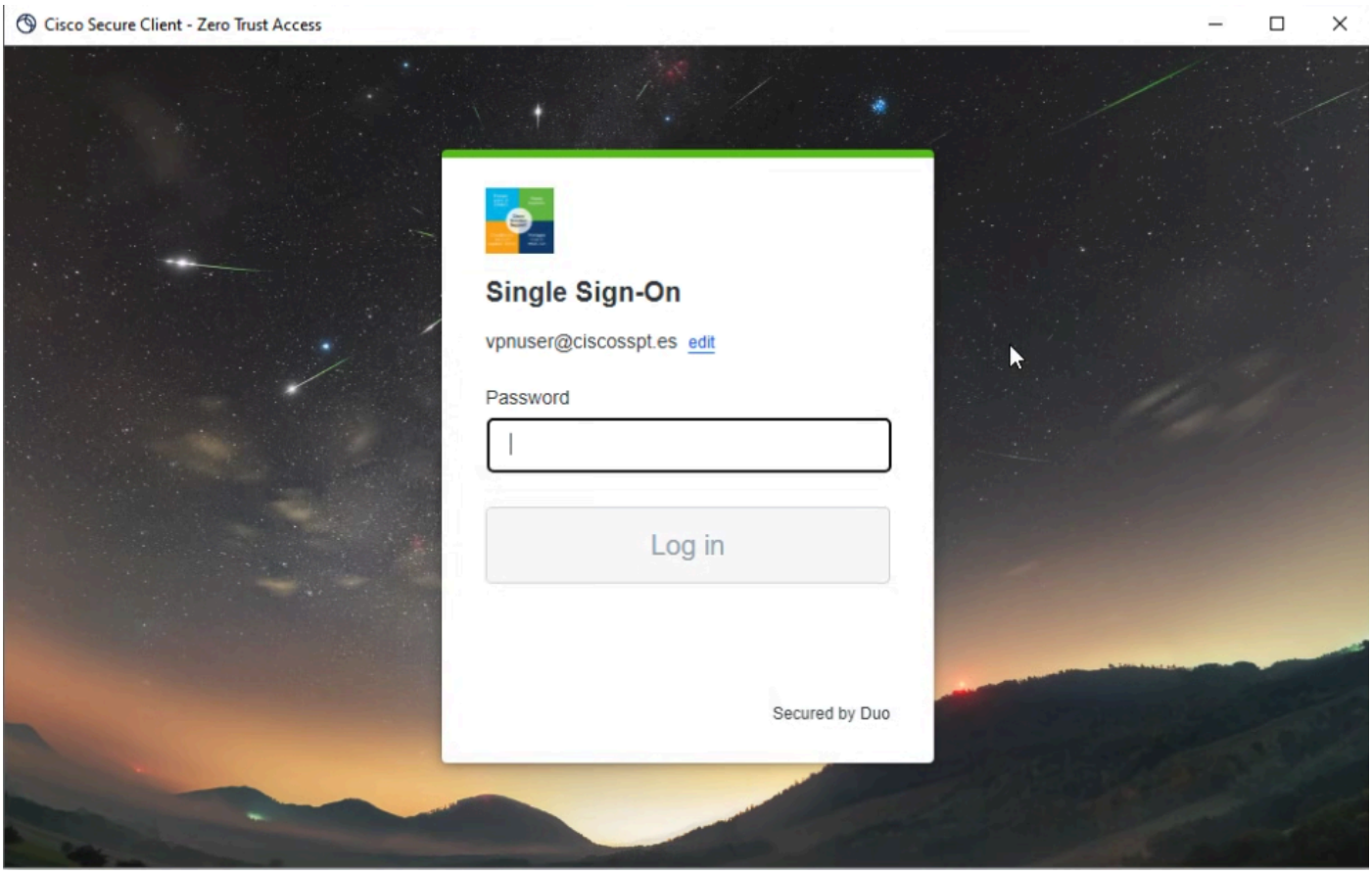
安全使用者端- *ZTNA*

- 使用您的使用者名稱註冊。



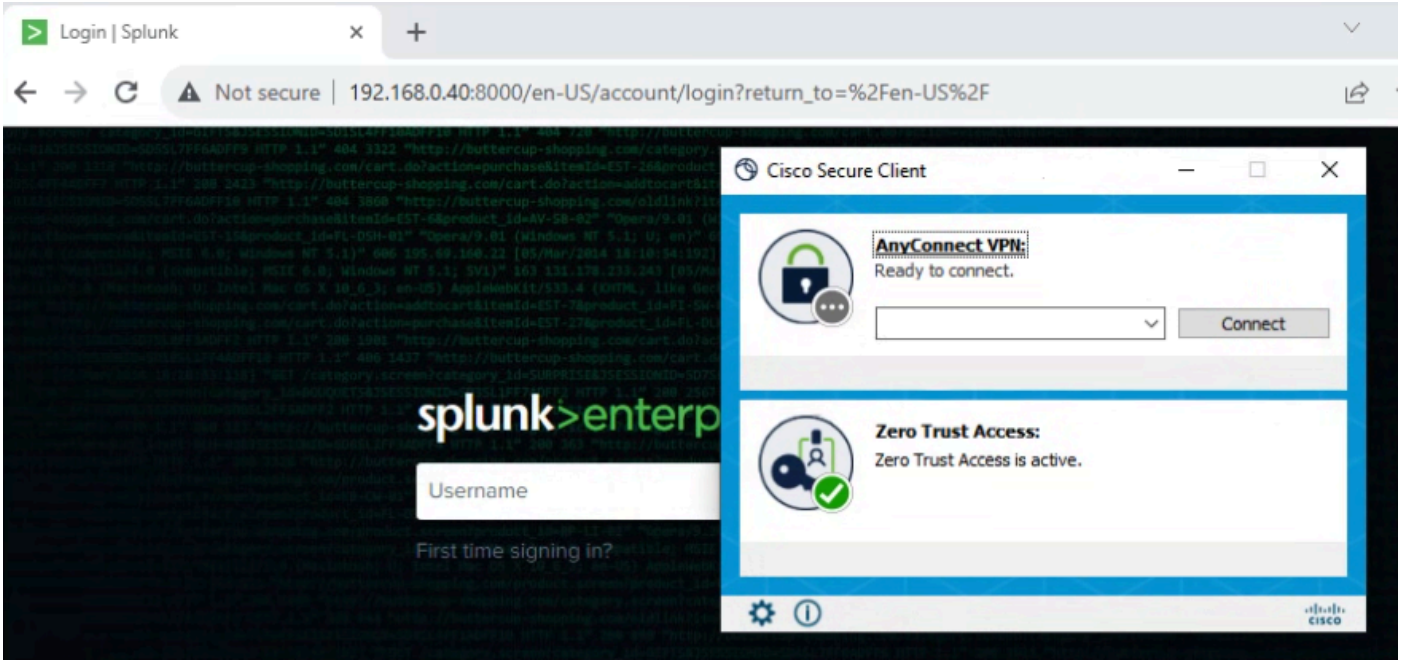
安全客戶端- *ZTNA* -註冊

- 在您的SSO提供者中進行驗證



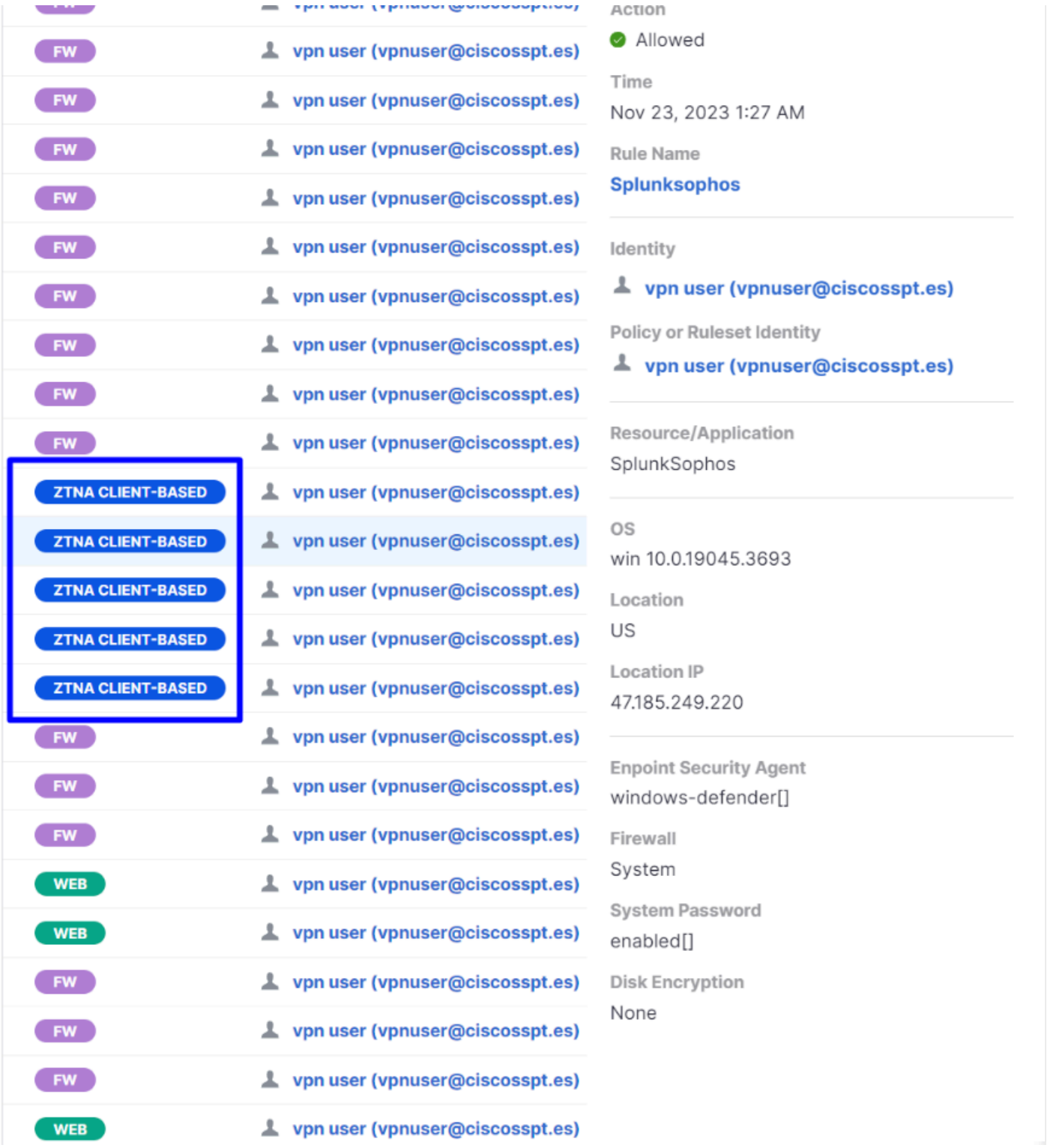
安全客戶端- *ZTNA - SSO*登入

- **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

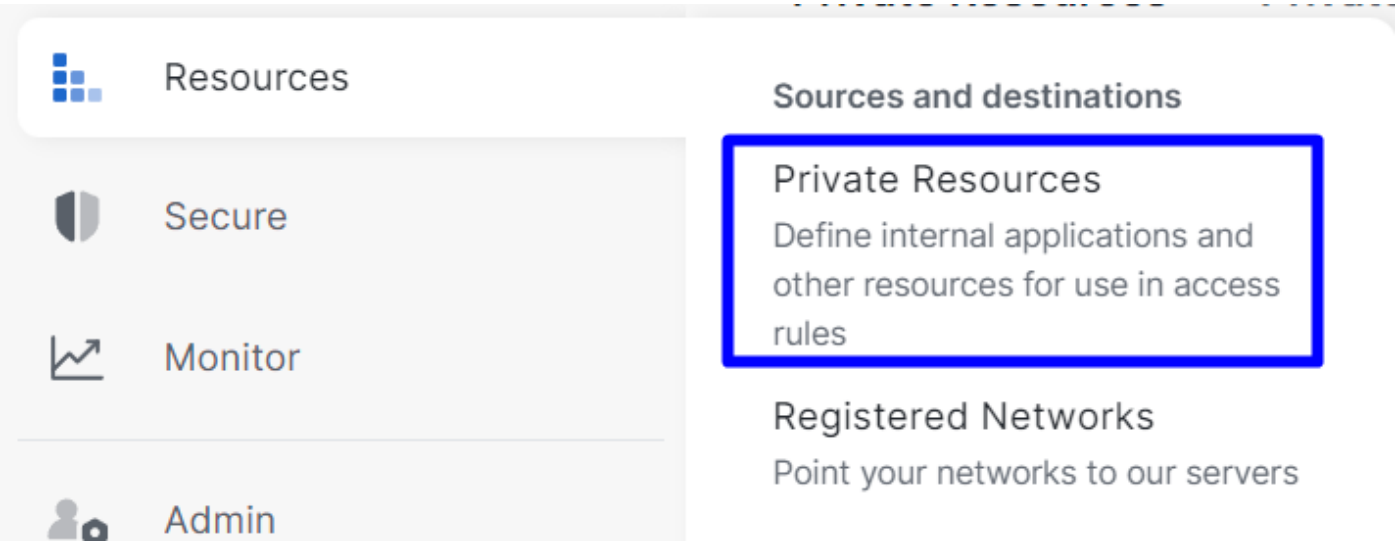


安全存取-活動搜尋- *ZTNA*使用者端

您可以看到使用者被允許透過基於客戶端的ZTNA進行身份驗證。

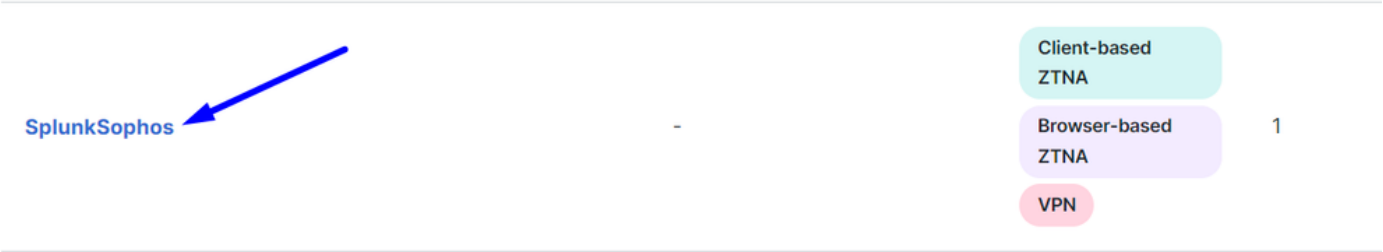
基於瀏覽器的ZTNA

要獲取URL，您需要轉到**Resources > Private Resources**。



安全存取-私人資源

- 按一下您的原則



安全訪問-專用資源- *SplunkSophos*

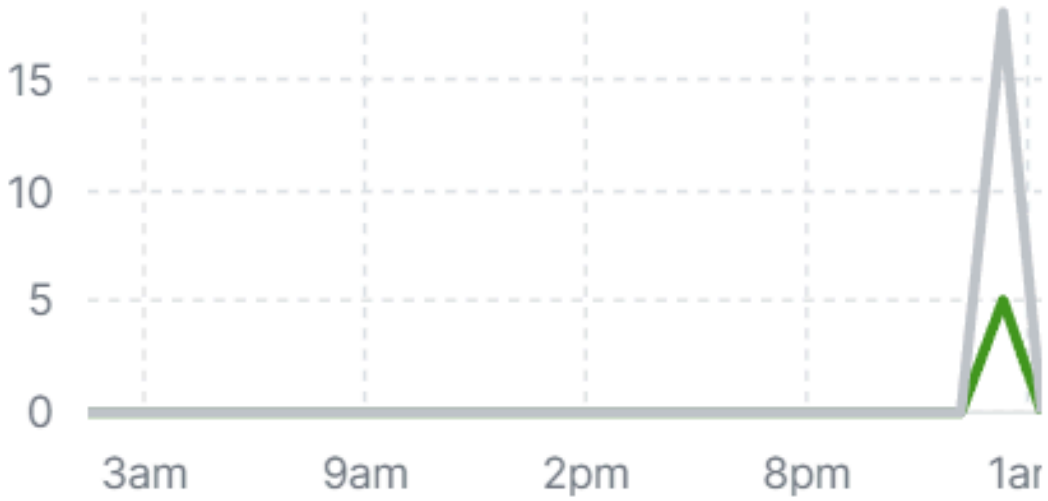
- 向下滾動

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）。