# تكوين الوصول الآمن باستخدام جدار حماية Sophos XG

## المحتويات



## المقدمة

يوضح هذا المستند كيفية تكوين الوصول الآمن باستخدام جدار حماية Sophos XG.

## المتطلبات الأساسية

- تكوين توفير المستخدم
- تكوين مصادقة ZTNA SSO
- تكوين الوصول الآمن إلى VPN للوصول عن بعد

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جدار حماية Sophos XG
- الوصول الآمن

- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- زتنا بدون زواي

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى:

- جدار حماية Sophos XG
- الوصول الآمن
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# معلومات أساسية


الوصول الآمن - Sophos

صممت Cisco ميزة Secure Access لضمان حماية الوصول إلى التطبيقات الخاصة وتوفيره، على أساس محلي وقائم على الشبكة على حد سواء. كما أنه يضمن الاتصال من الشبكة إلى الإنترنت. ويتحقق ذلك من خلال تطبيق أساليب وطبقات أمنية متعددة، تهدف جميعها إلى الحفاظ على المعلومات عند الوصول إليها عبر السحابة.

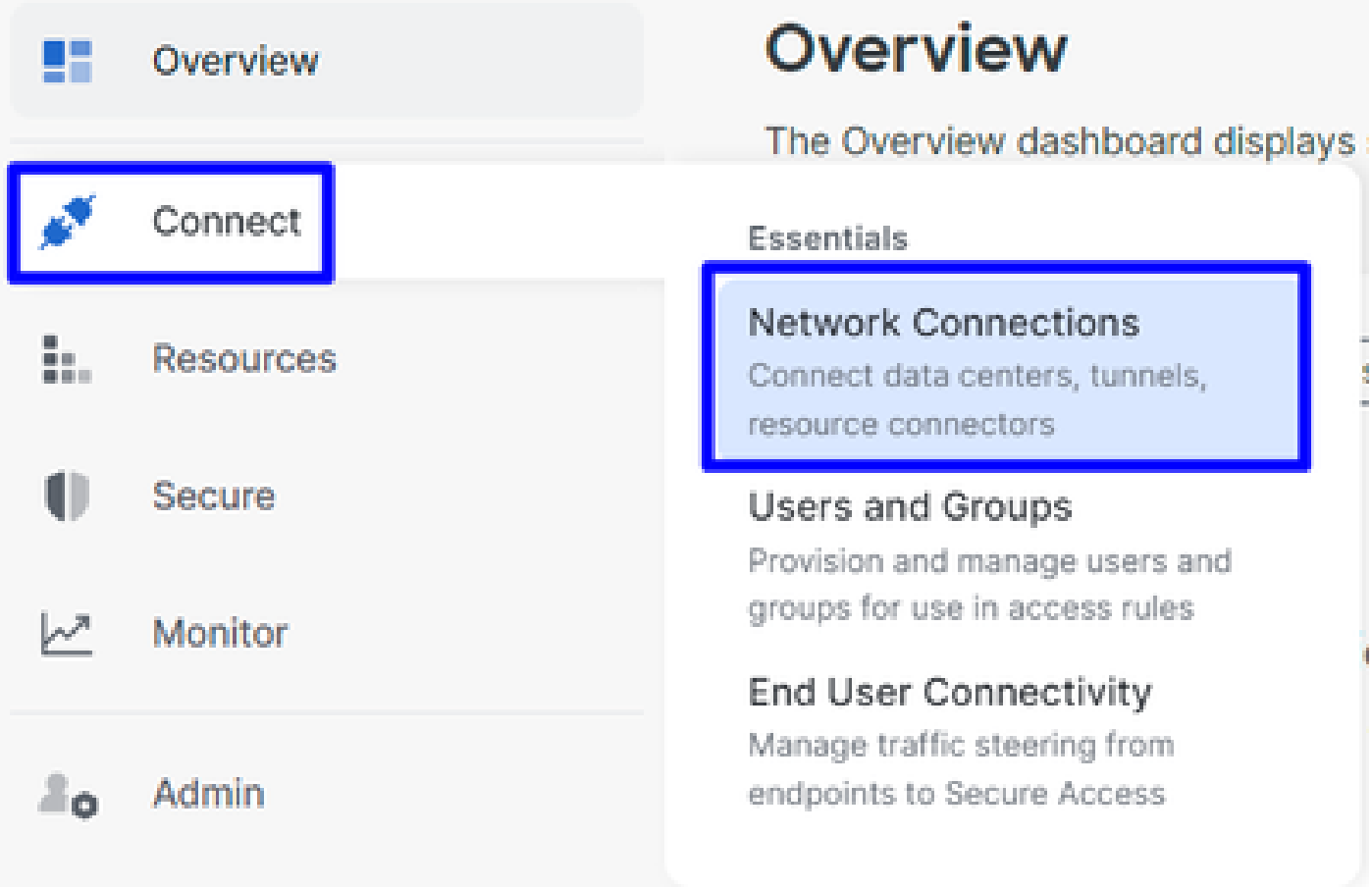
# التكوين

## تكوين النفق على الوصول الآمن

انتقل إلى لوحة الإدارة الخاصة ب Secure Access.

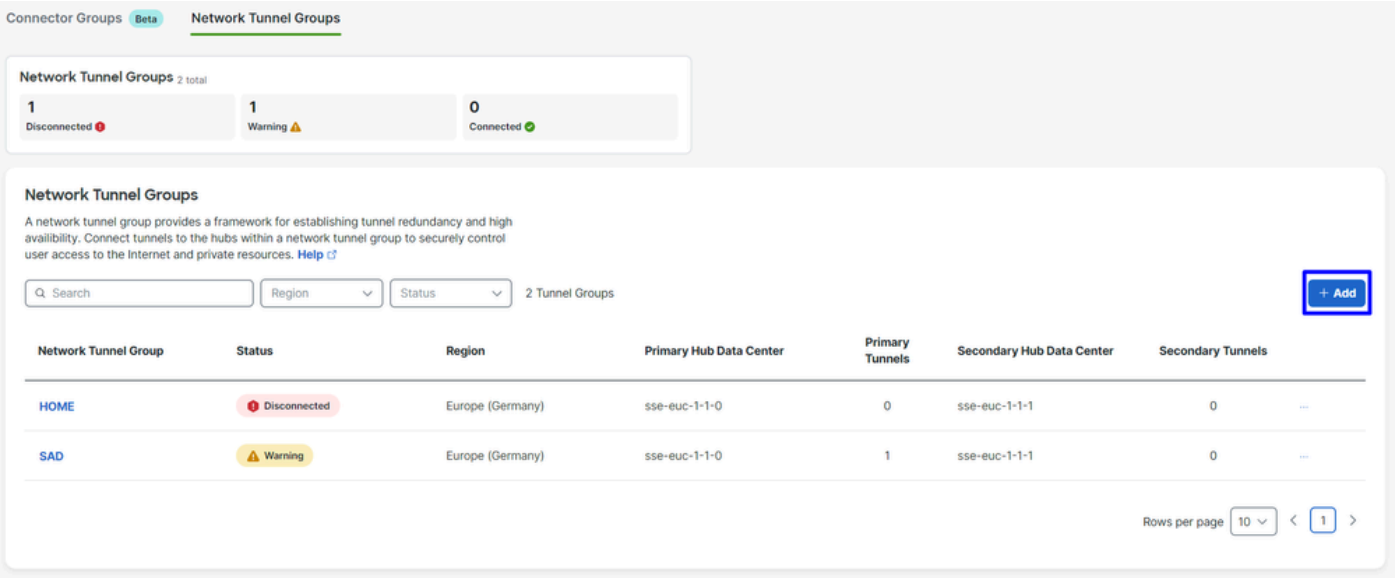

الوصول الآمن - الصفحة الرئيسية

- انقر فوق Connect > Network Connections.




الوصول الآمن - إتصالات الشبكة

- تحت Network Tunnel Groups الضغط على + Add.




الوصول الآمن - مجموعات نفق الشبكة

- التكوين Tunnel Group Name، Region وDevice Type.
- انقر. **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**

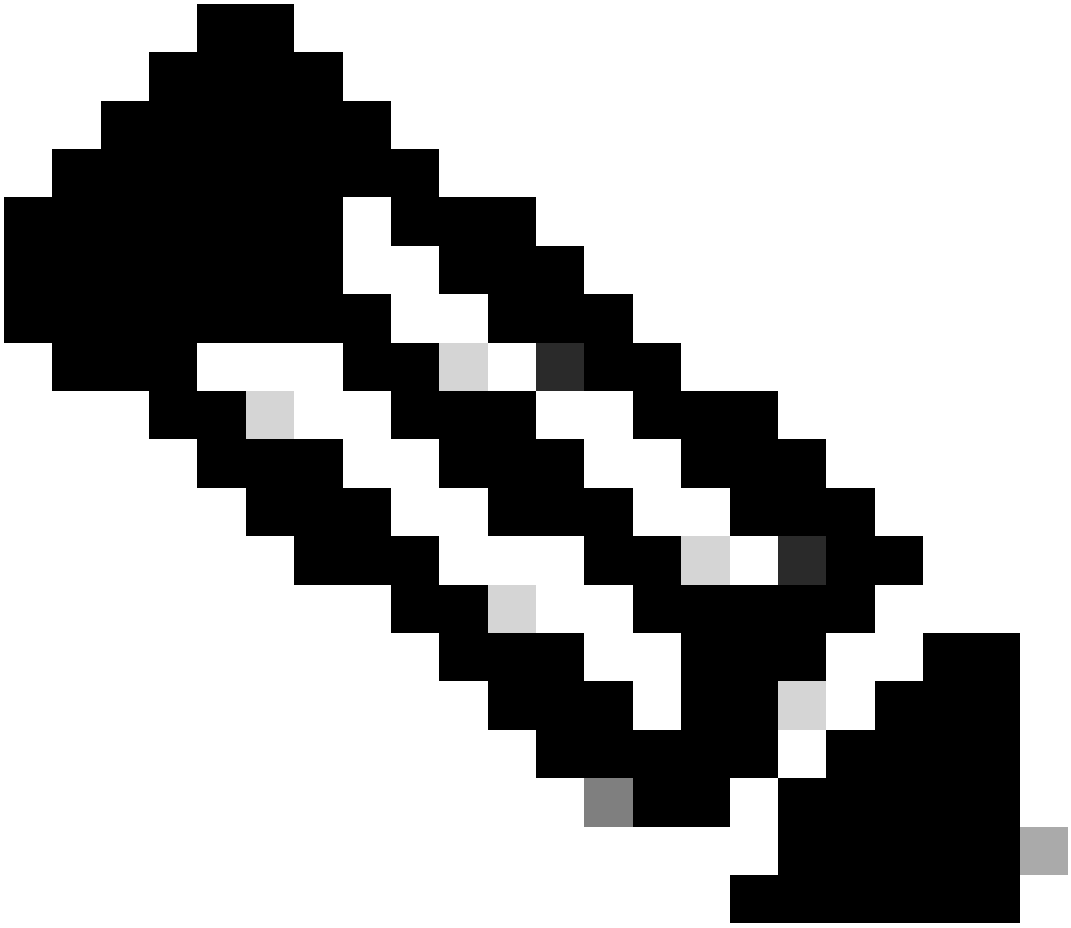
Europe (Germany)

**Device Type**

Other

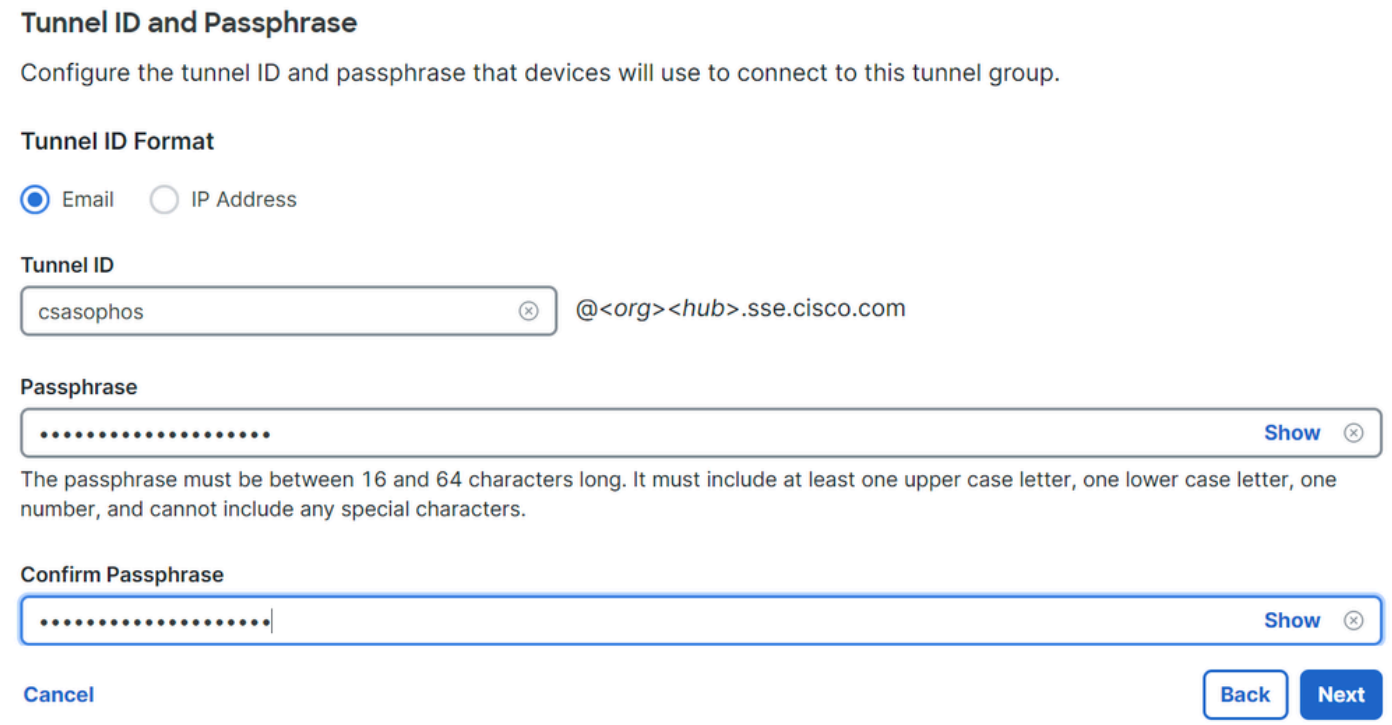
Cancel

Next



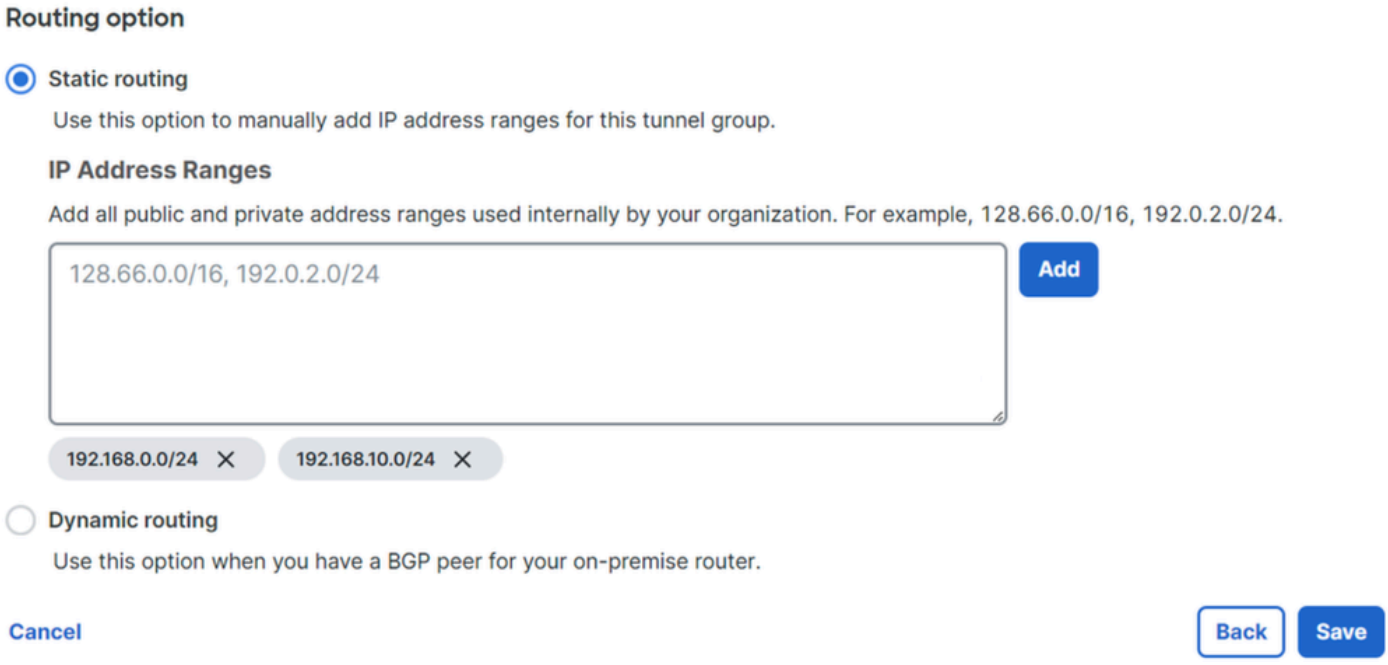
**ملاحظة:** أختر أقرب منطقة إلى موقع جدار الحماية.

- قم بتكوين Tunnel ID Formatو Passphrase.
- انقر Next.




الوصول الآمن - مجموعات الأنفاق - معرف النفق وعبارة المرور

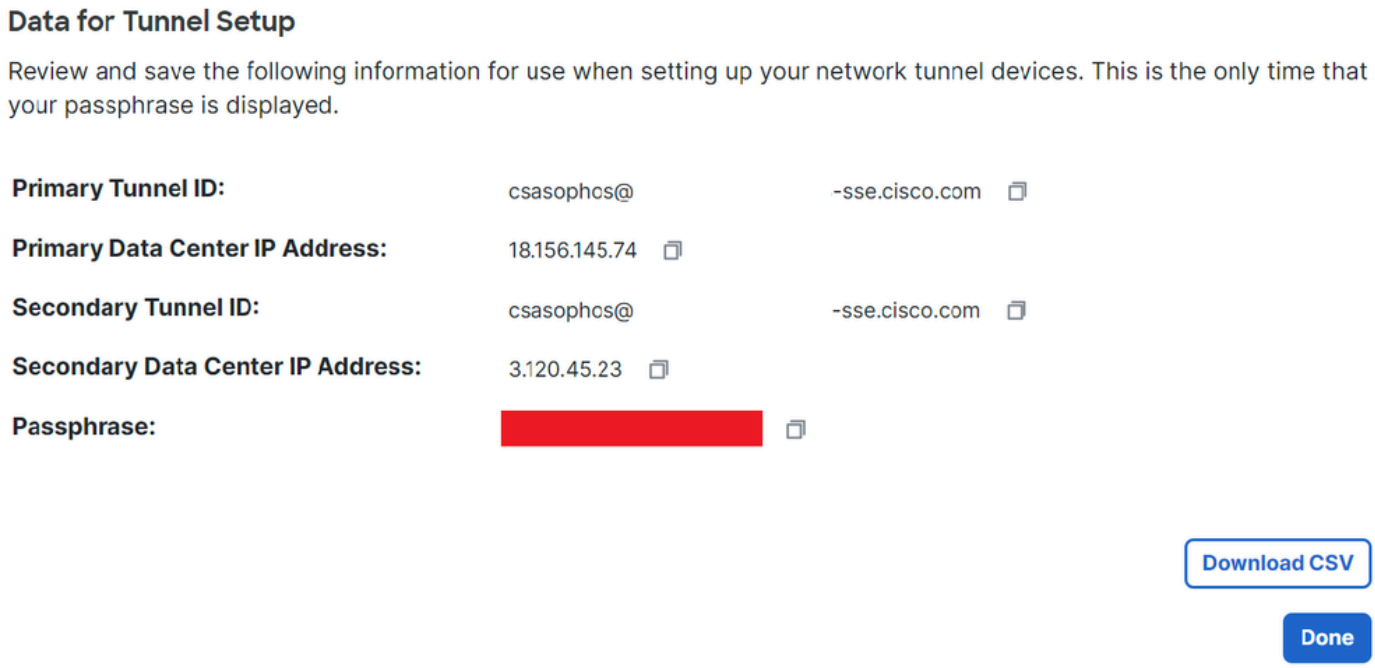
- قم بتكوين نطاقات عناوين IP أو البيئات المضيفة التي قمت بتكوينها على الشبكة وتريد تمرير حركة المرور من خلال الوصول الآمن.
- انقر. **Save**




الوصول الآمن - مجموعات الأنفاق - خيارات التوجيه

بعد النقر فوق المعلومات **Save** حول عرض النفق، الرجاء حفظ تلك المعلومات للخطوة التالية، **Configure the tunnel on Sophos**.

بيانات النفق



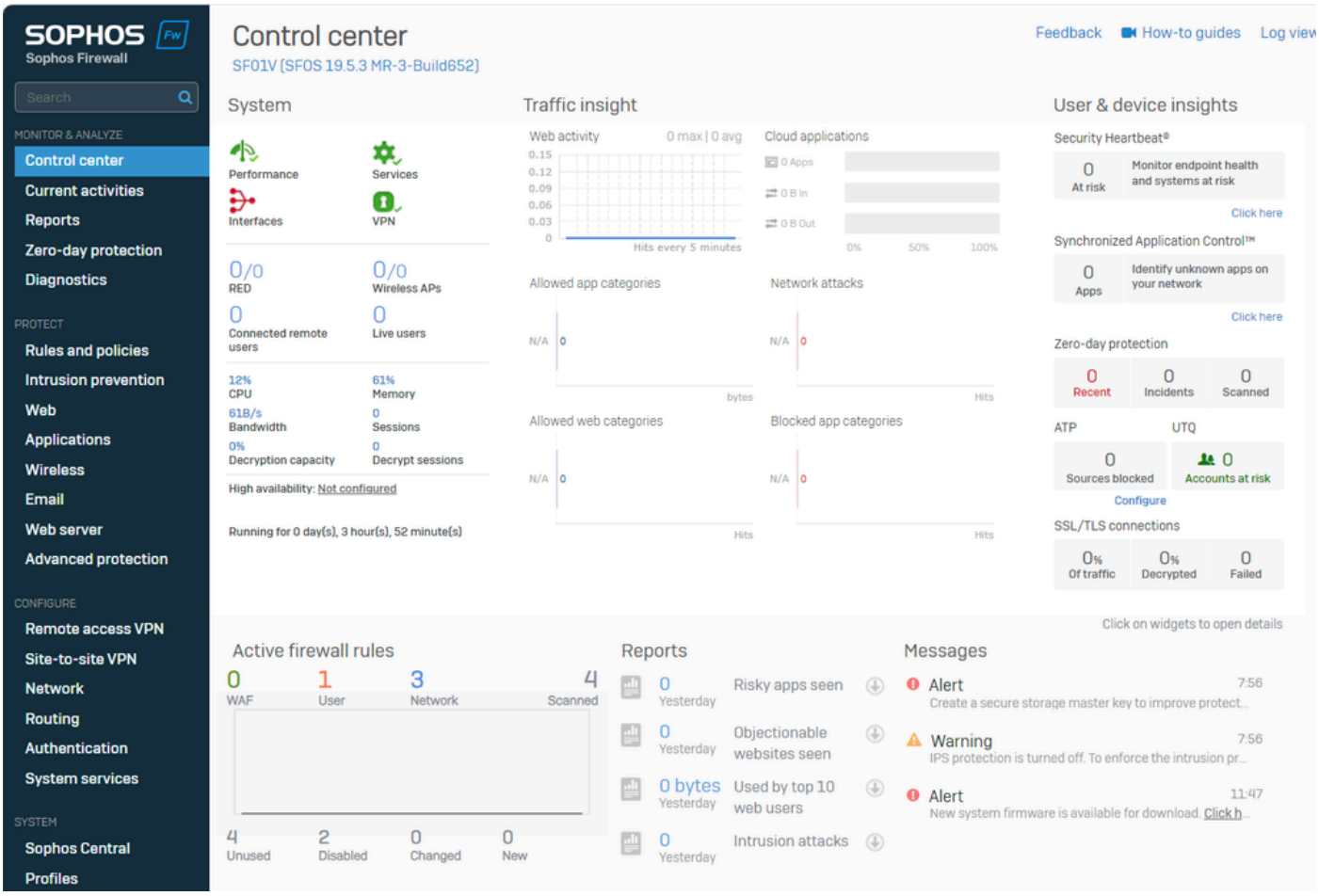

الوصول الآمن - مجموعات الأنفاق - إستئناف التكوين

تكوين النفق على Sophos

تكوين ملف تعريف IPsec

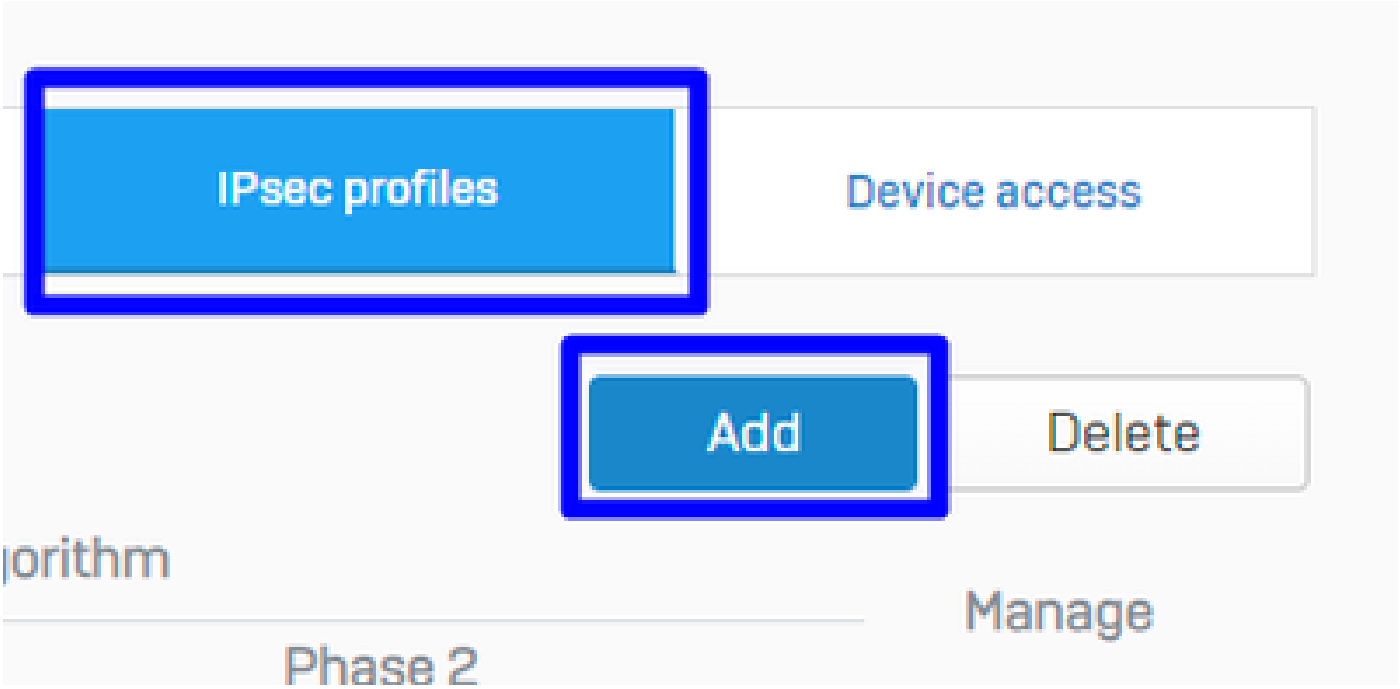
لتكوين ملف تعريف IPsec، انتقل إلى جدار حماية Sophos XG الخاص بك.

تحصل على شيء مشابه لهذا:




*Sophos* - لوحة الإدارة

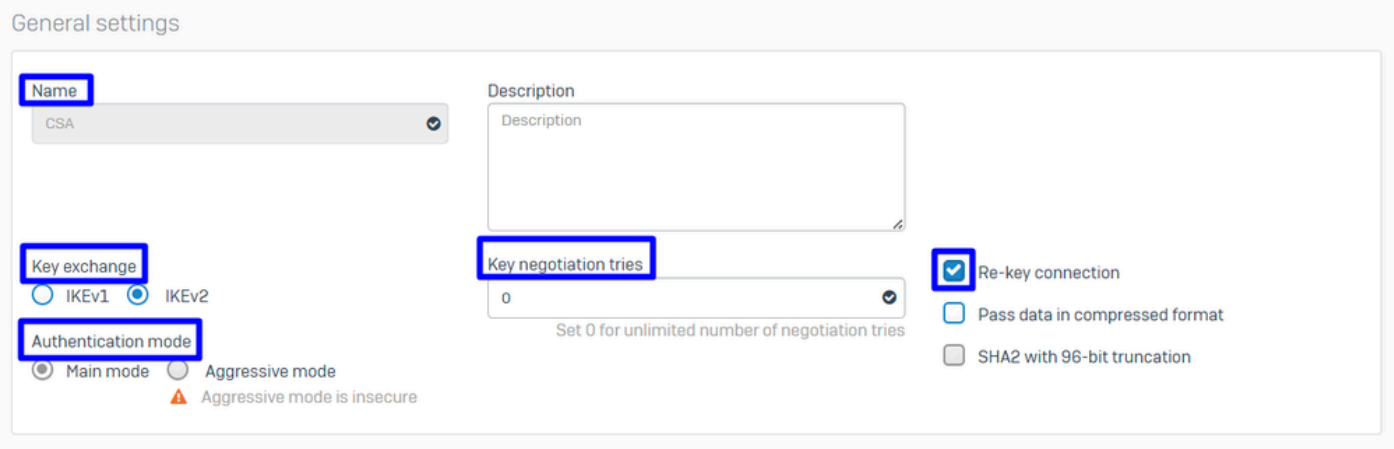
- انتقل إلى Profiles
- انقر فوق **IPsec Profiles** وبعد ذلك انقر فوقAdd



*Sophos - ملفات تعريف IPsec*

تحت **General Settings** التكوين:

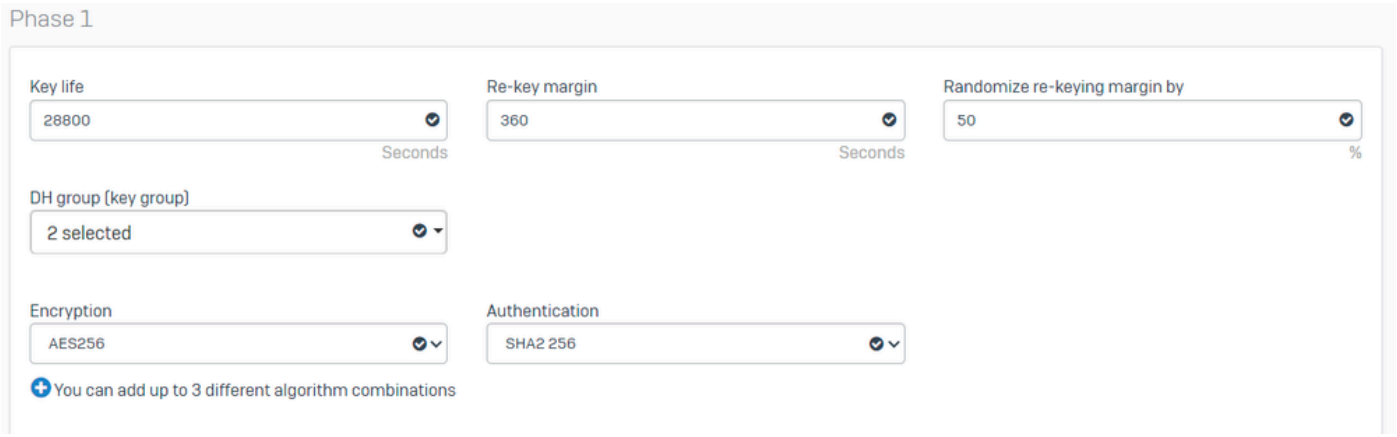
- **Name**: اسم مرجع لنهج الوصول الآمن من Cisco
- **Key Exchange**: IKEv2
- **Authentication Mode**: الوضع الرئيسي
- **Key Negotiation Tries**:0
- **Re-Key connection**: حدد الخيار




*Sophos - توصيفات IPsec - إعدادات عامة*

تحت **Phase 1** التكوين:

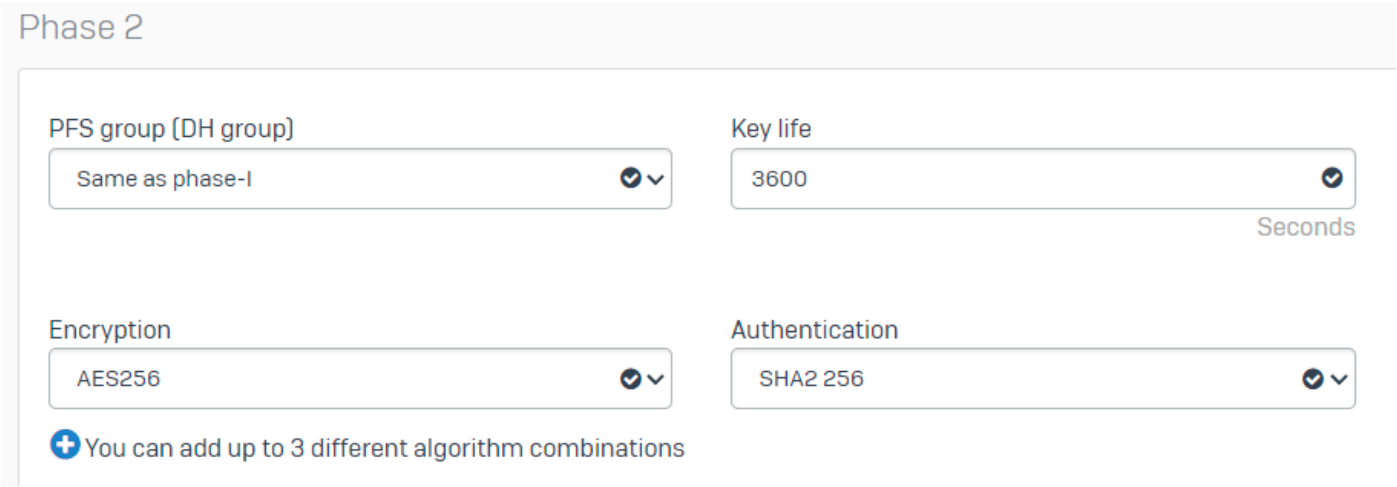
- **Key Life**:28800
- **DH group(key group)**: تحديد 19 و 20
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin: 360 (الافتراضي)
- **Randomize re-keying margin by**: 50 (افتراضي)




*Sophos - ملفات تعريف IPsec - المرحلة 1*

تحت **Phase 2** التكوين:

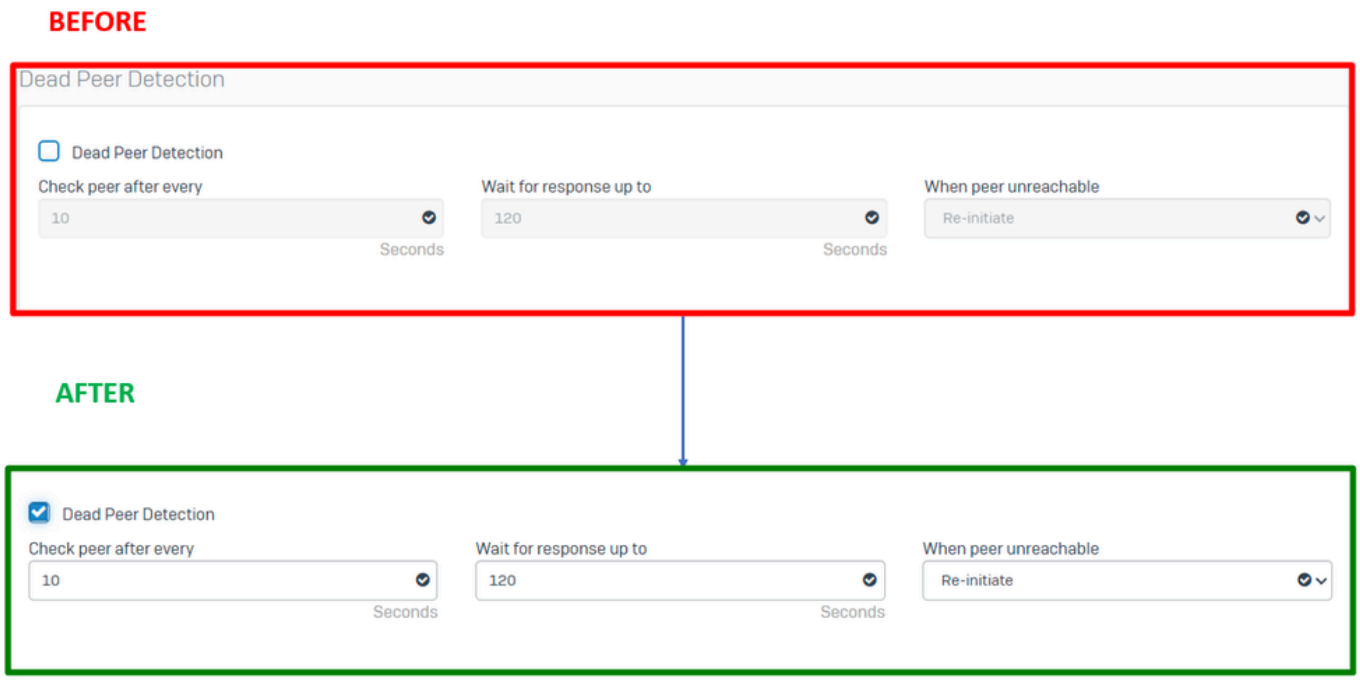
- PFS group (DH group): نفس المرحلة الأولى
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256




*Sophos - ملفات تعريف IPsec - المرحلة 2*

تحت **Dead Peer Detection** التكوين:

- **Dead Peer Detection**: حدد الخيار
- **Check peer after every**:10
- **Wait for response up to**: 120 (الافتراضي)
- **When peer unreachable**: إعادة البدء (الافتراضي)

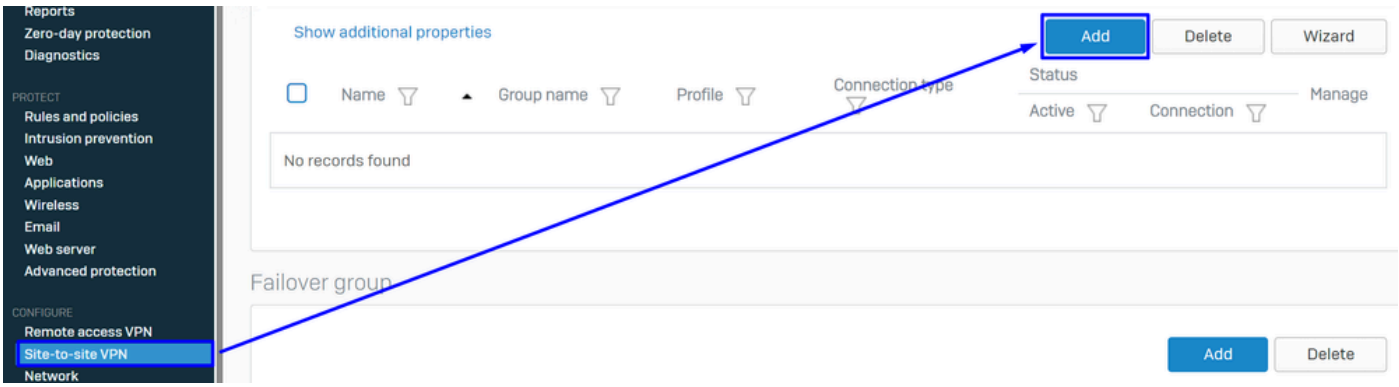



*Sophos - ملفات تعريف IPsec - اكتشاف النظير الميت*

بعد ذلك اضغط **Save** and proceed with the next step, Configure Site-to-site VPN.

تكوين شبكة VPN من موقع إلى موقع

لبدء تكوين الشبكة الخاصة الظاهرية (VPN)، انقر فوق **Site-to-site VPN** ثم انقر فوق **Add**.



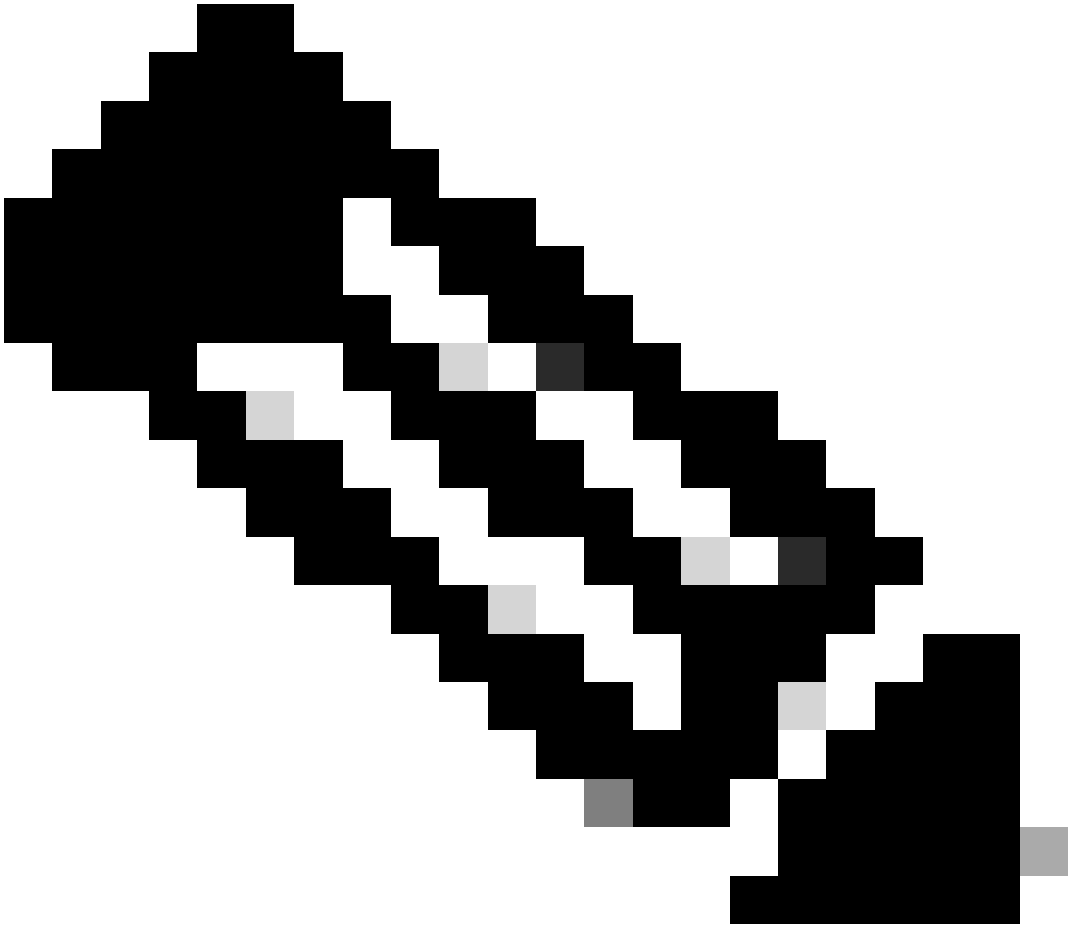

*Sophos - شبكة VPN من موقع إلى موقع*

تحت **General Settings** التكوين:

- **Name**: اسم مرجع لنهج IPsec للوصول الآمن من Cisco
- IP version: IPv4
- Connection type: واجهة النفق
- Gateway type: بدء الاتصال

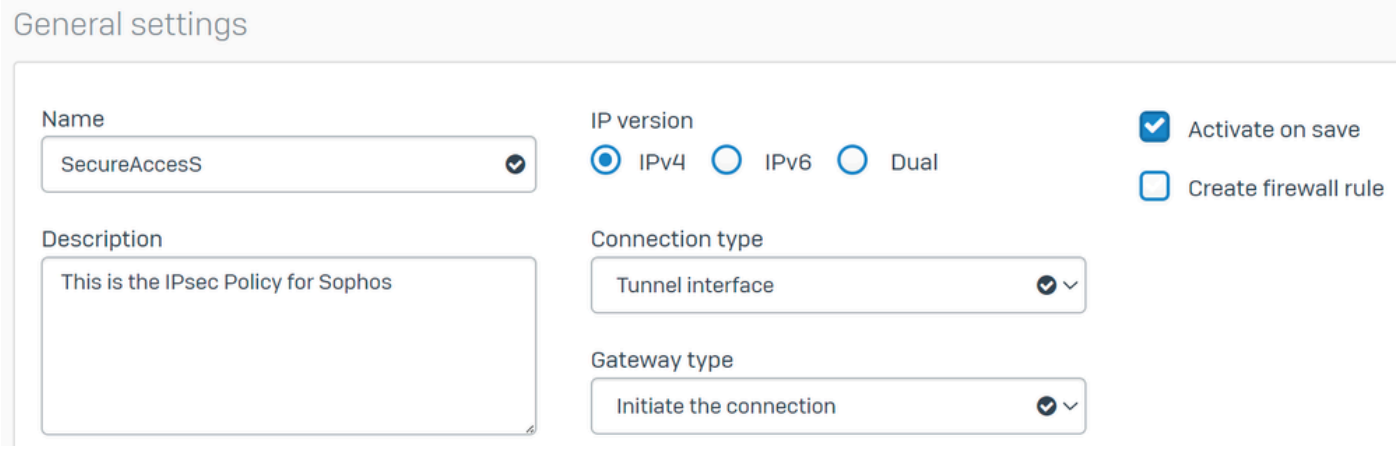
- Active on save: حدد الخيار

---



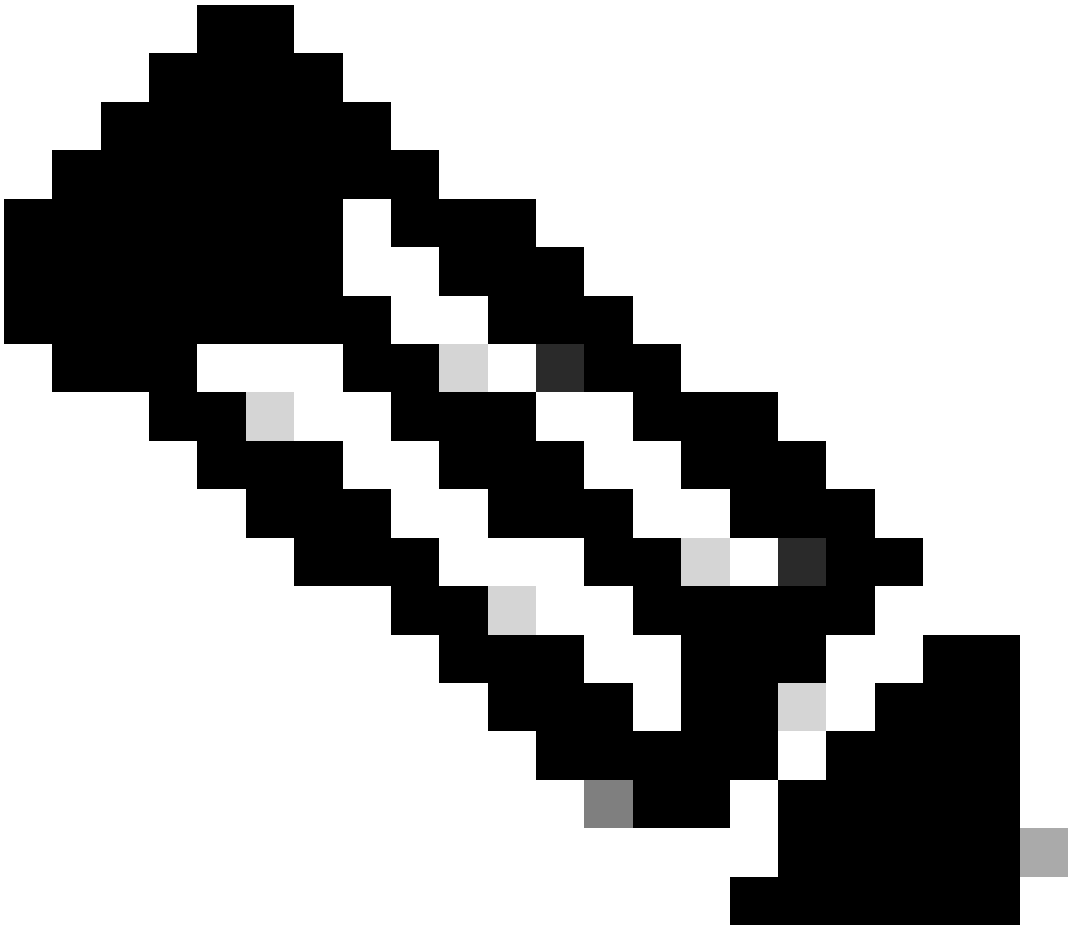
**ملاحظة**: **Active on save** يمكن الخيار شبكة VPN تلقائيا بعد أن تنتهي إلى تكوين شبكة VPN من موقع إلى موقع.

---




*Sophos - شبكة VPN من موقع إلى موقع - إعدادات عامة*

---

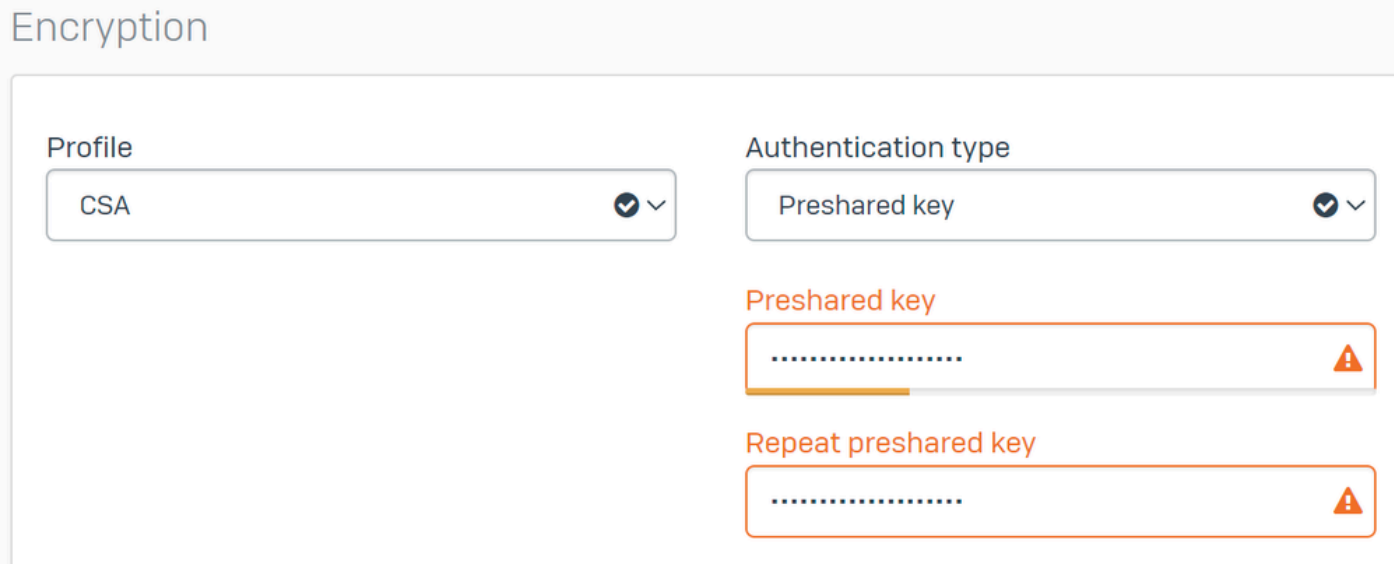


**ملاحظة:** تقوم واجهة النفق الاختيارية بإنشاء واجهة نفق افتراضية لجدار حماية Sophos XG باسم XFRM.

---

تحت **Encryption** التكوين:

- **Profile**: ملف التعريف الذي تقوم بإنشائه على الخطوة، **Configure IPsec Profile**
- **Authentication type**: المفتاح المشترك مسبقا
- **Preshared key**: المفتاح الذي تقوم بتكوينه على الخطوة، Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**

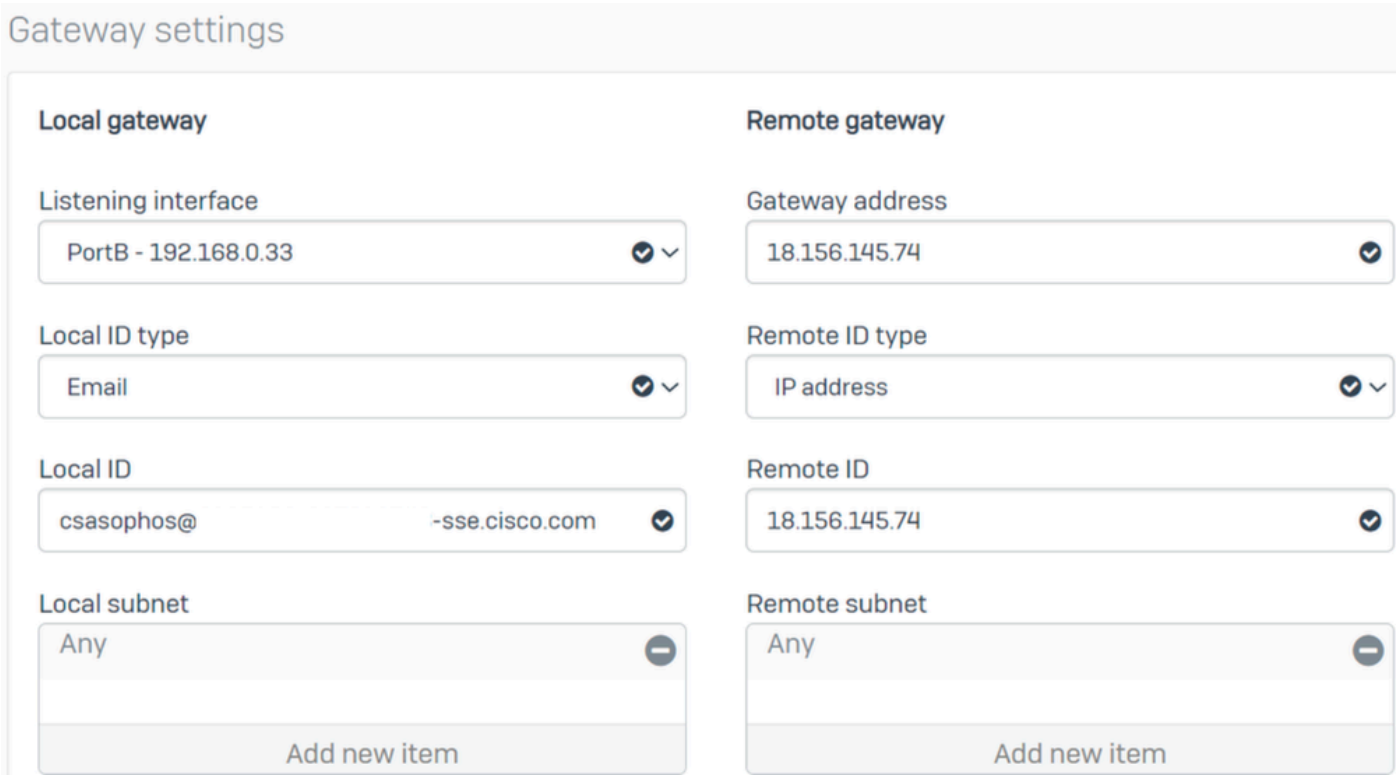



*Sophos* - الشبكة الخاصة الظاهرية (*VPN*) من موقع إلى موقع - التشفير

تحت **Gateway Settings** خيارات التكوين Local Gateway Remote Gateway، أستخدم هذا الجدول كمرجع.

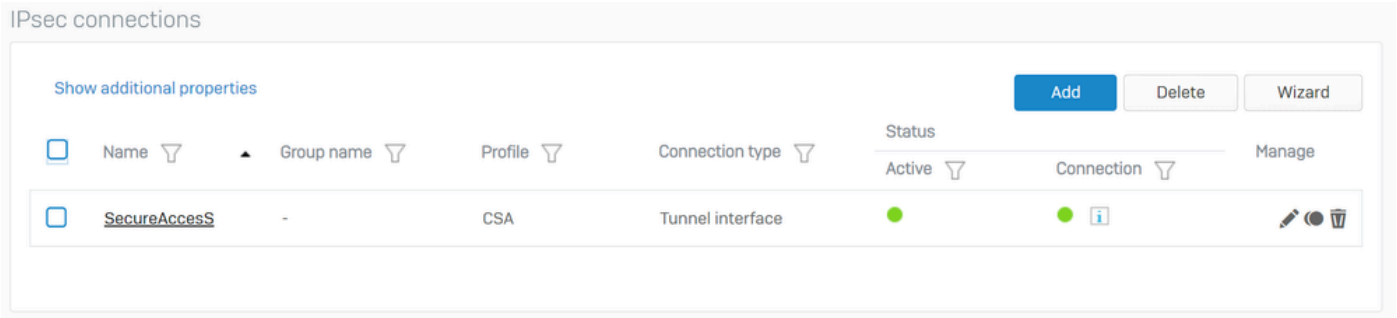
| البوابة المحلية | البوابة البعيدة |
|---|---|
| واجهة الاستماع<br>واجهة شبكة WAN-الإنترنت لديك | عنوان البوابة<br>IP العام الذي تم إنشاؤه بموجب الخطوة، **Tunnel Data** |
| نوع المعرف المحلي<br>البريد الإلكتروني | نوع المعرف البعيد |

| | |
|---|---|
| عنوان IP | |
| معرف بعيد<br>IP العام الذي تم إنشاؤه بموجب الخطوة، Tunnel Data | معرف محلي<br>البريد الإلكتروني الذي تم إنشاؤه تحت الخطوة، Tunnel Data |
| الشبكة الفرعية البعيدة<br>أي | الشبكة الفرعية المحلية<br>أي |

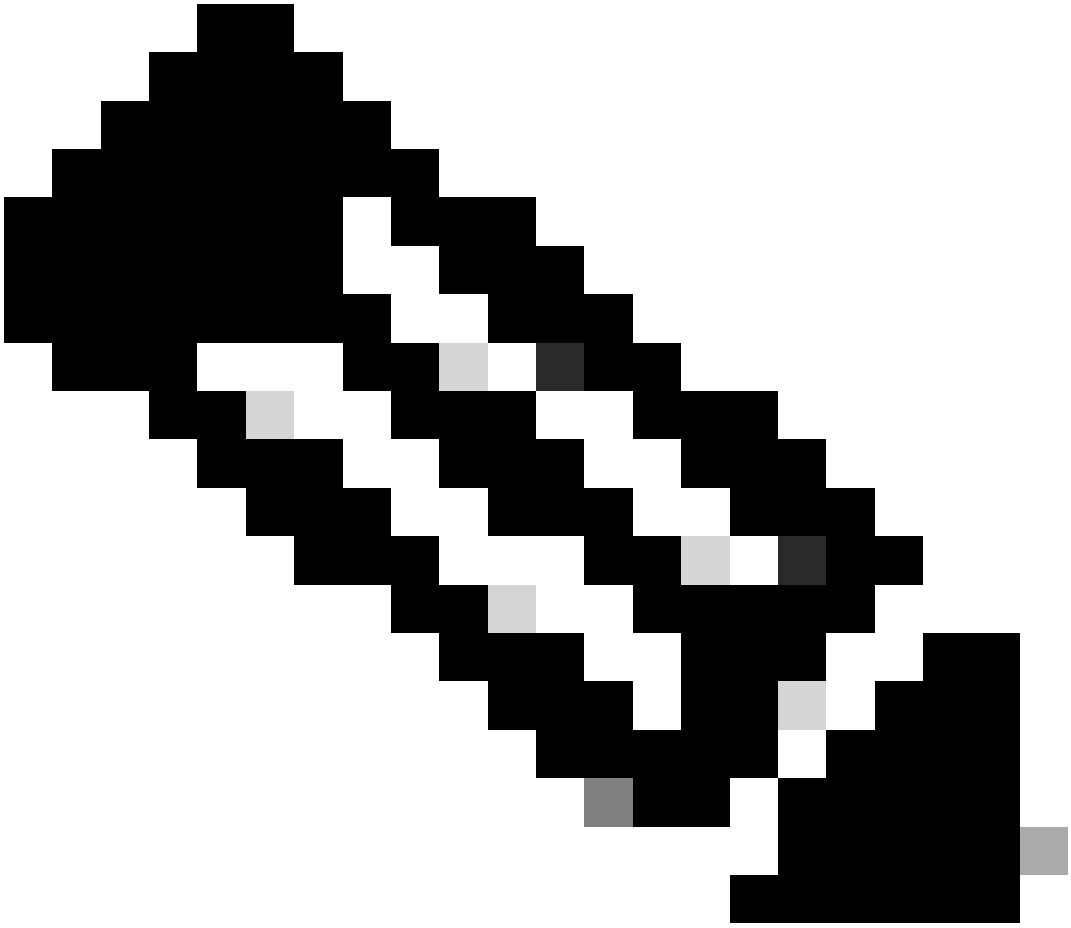



*Sophos* - إعدادات الشبكة الخاصة الظاهرية (*VPN*) من موقع إلى موقع - البوابة

بعد ذلك انقر، **Save**ويمكنك أن ترى أن النفق تم إنشاؤه.

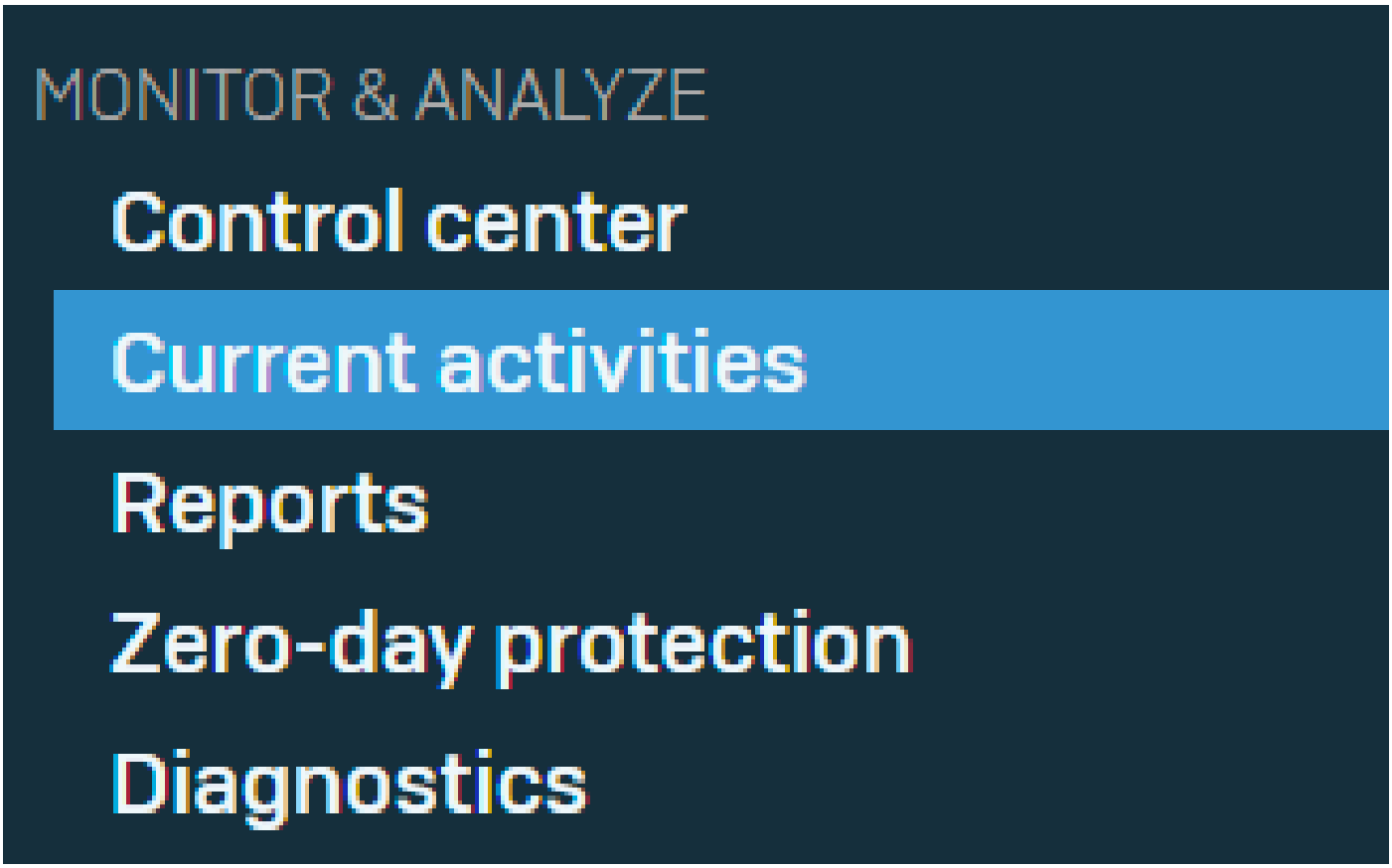



*Sophos* - إتصالات *VPN* من موقع إلى موقع - *IPsec*

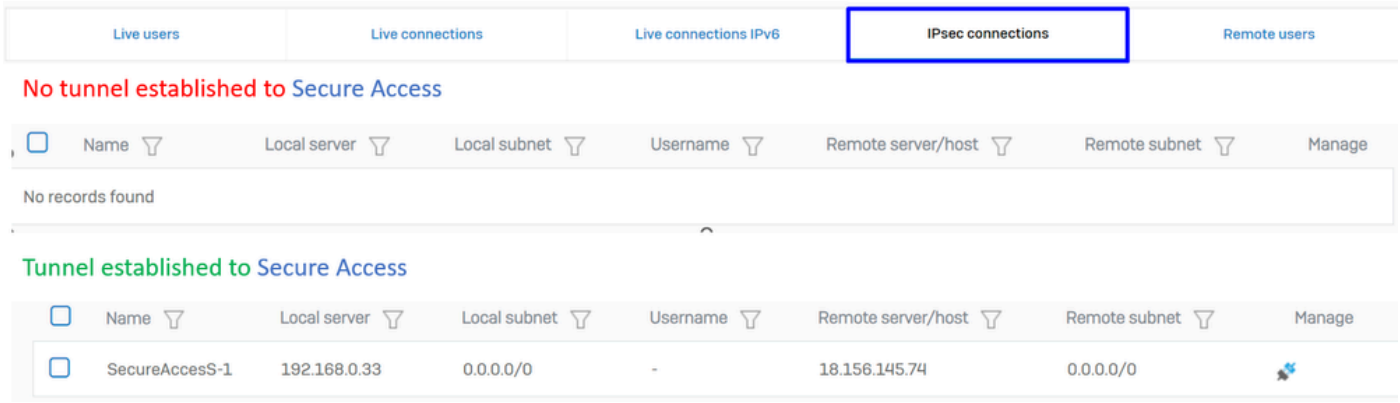


**ةظحلام:** للتحقق من تمكين النفق بشكل صحيح على الصورة الأخيرة، يمكنك التحقق من **Connection** الحالة، إذا كان أخضر، فإن النفق متصل إذا لم يكن أخضر النفق غير متصل.

للتحقق مما إذا تم إنشاء نفق، انتقل إلى **Current Activities** > **IPsec Connections**.




*Sophos* - المراقبة والتحليل - *IPsec*



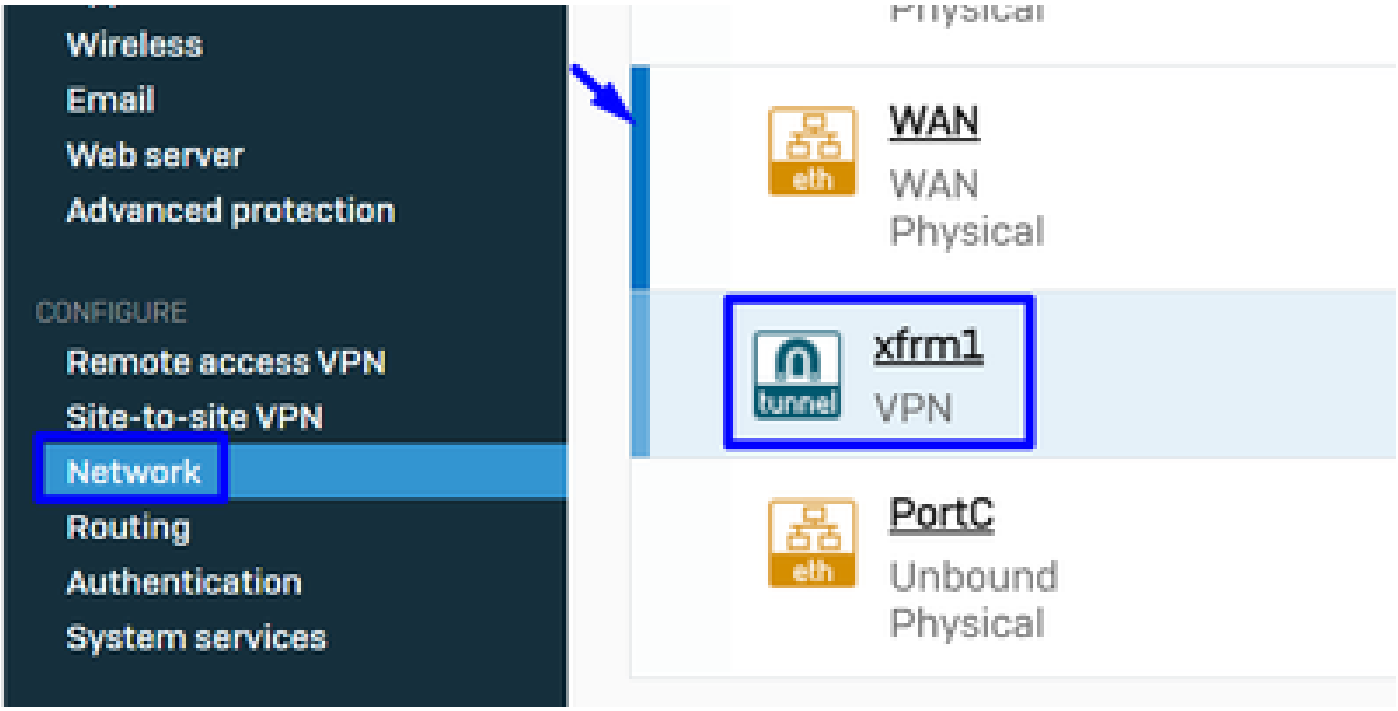

*Sophos* - المراقبة والتحليل - *IPsec* قبل وبعد

وبعد ذلك، يمكن أن نواصل الخطوة، **Configure Tunnel Interface Gateway**.

تكوين واجهة النفق

انتقل إلى الواجهة **Network** التي تم تكوينها على شبكة VPN وفحصهاWAN لتحرير واجهة النفق الظاهرية باستخدام الاسم xfrm.

- انقر على **xfrm** الواجهة.




*Sophos - الشبكة - واجهة النفق*

- قم بتكوين الواجهة باستخدام IP غير القابل للتوجيه في شبكتك، على سبيل المثال، يمكنك استخدام 169.254.0.1/30 وهو IP في مساحة غير قابلة للتوجيه عادة، وفي المثال الذي نمثله نستخدم 169.254.x.x/30


*Sophos - الشبكة - واجهة النفق - التكوين*

تكوين البوابات

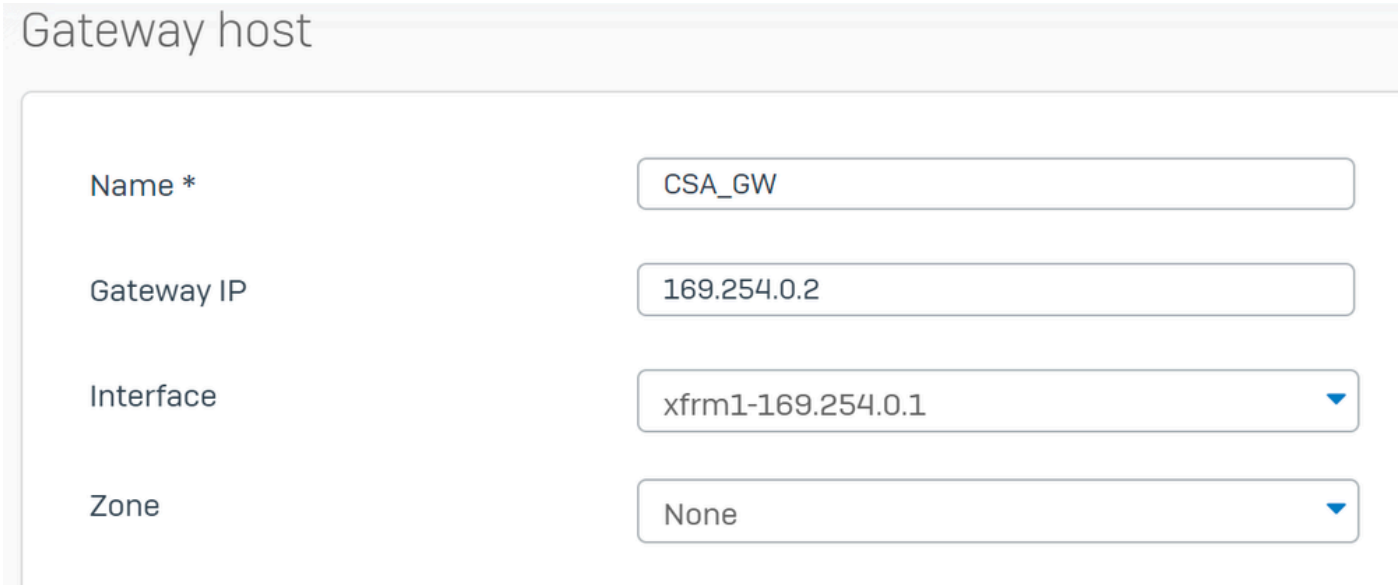
لتكوين عبارة الواجهة الظاهرية (xfrm)

- انتقل إلى Routing > Gateways
- انقر Add


*Sophos* - التوجيه - البوابات

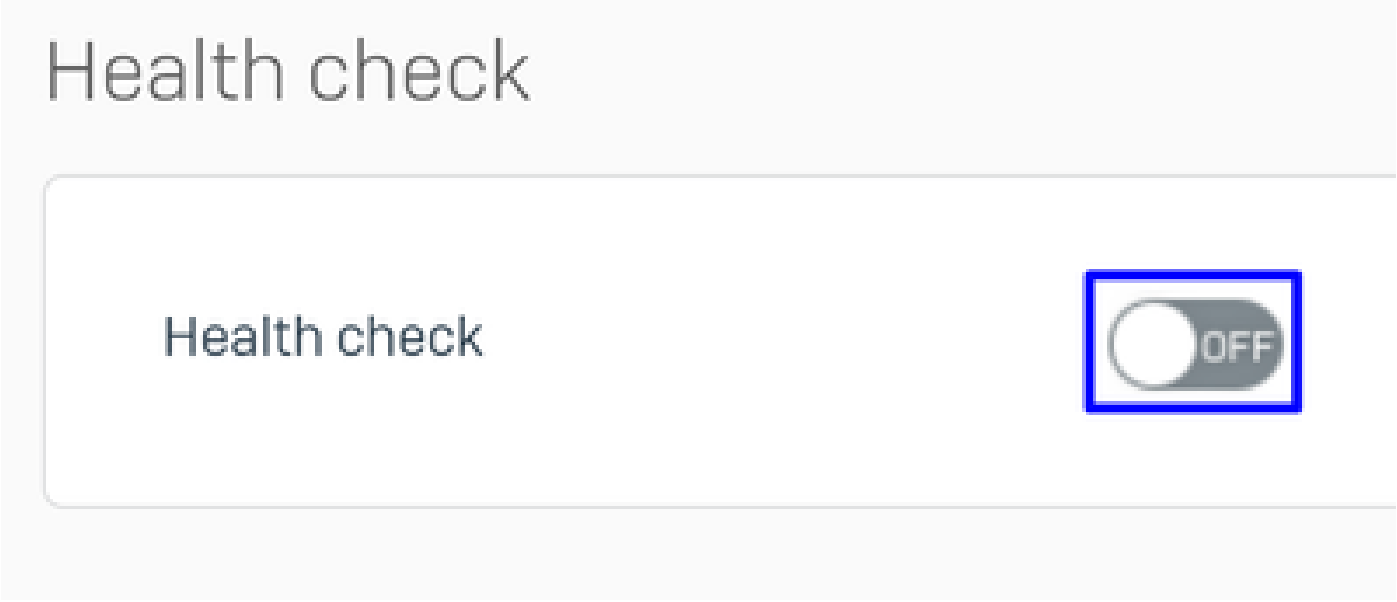
تحت **Gateway host** التكوين:

- **Name**: اسم يشير إلى الواجهة الظاهرية التي تم إنشاؤها لشبكة VPN
- **Gateway IP**: في حالتنا 169.254.0.2، وهذا هو بروتوكول الإنترنت (IP) تحت الشبكة 169.254.0.1/30 الذي قمنا بتعيينه بالفعل تحت الخطوة، Configure Tunnel Interface
- Interface: الواجهة الظاهرية لشبكة VPN
- **Zone**: بلا (الافتراضي)



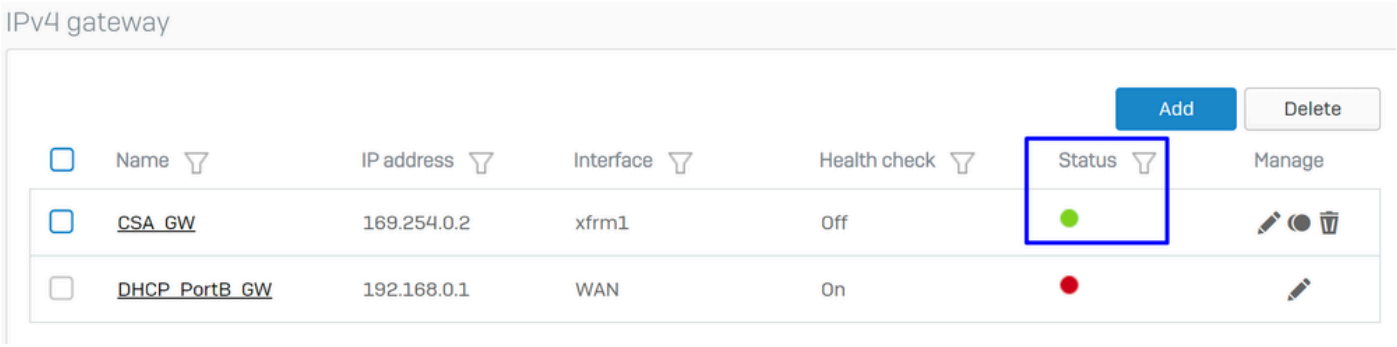

*Sophos* - التوجيه - البوابات - مضيف البوابة

- تحت **Health check** تعطيل التحقق
- انقر **Save**




*Sophos* - التوجيه - البوابات - التحقق من الصحة

يمكنك ملاحظة حالة البوابة بعد حفظ التكوين:




*Sophos* - التوجيه - البوابات - الحالة

تكوين مسار SD-WAN

لإنهاء عملية التكوين، يلزمك إنشاء المسار الذي يسمح لك بإعادة توجيه حركة المرور إلى الوصول الآمن.

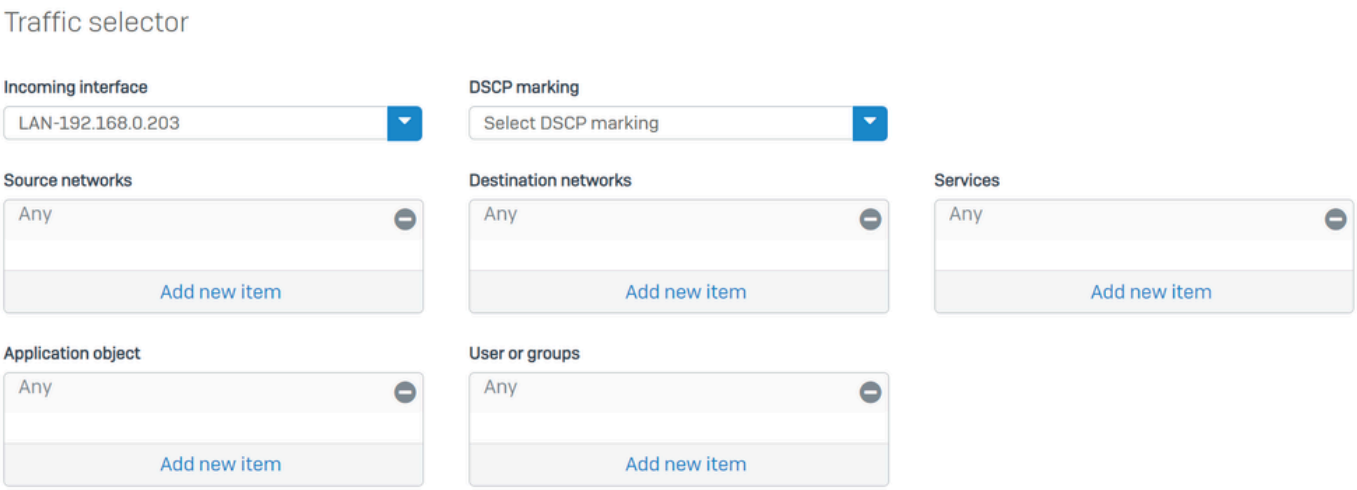
انتقل إلى **Routing** > **SD-WAN routes.**

- انقر فوق **Add**


طرق *Sophos* - شبكة *WAN* المعرفة عن طريق البرامج

تحت **Traffic Selector** التكوين:

- Incoming interface: حدد الواجهة من حيث تريد إرسال حركة المرور أو المستخدمين الذين يصلون من RA-VPN أو ZTNA أو ClientLess-ZTNA
- DSCP marking: ال شيء على هذا المثال
- **Source networks**: حدد العنوان الذي تريد توجيهه عبر النفق
- **Destination networks**: أي أو يمكنك تحديد وجهة
- **Services**: أي أو يمكنك تحديد الخدمات
- **Application object**: تطبيق إذا تم تكوين الكائن
- User or groups: إذا كنت ترغب في إضافة مجموعة معينة من المستخدمين لتوجيه حركة المرور إلى الوصول الآمن



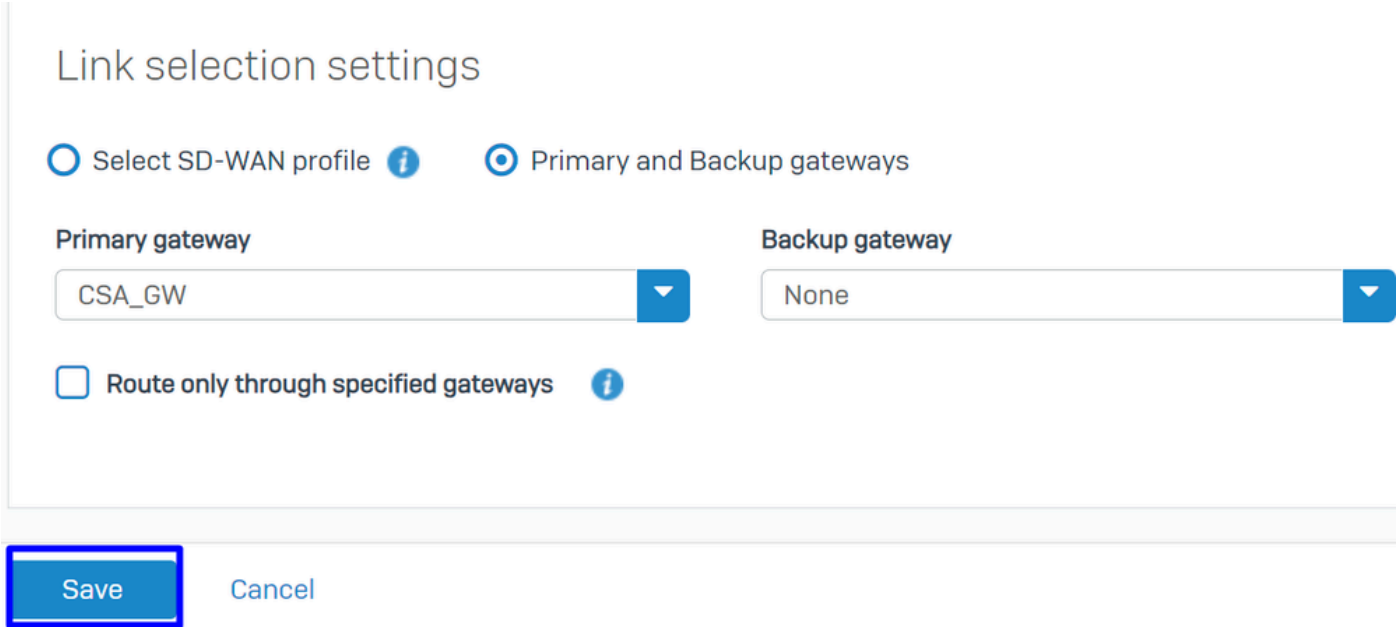

*SOPHOS* - مسارات *SD-WAN* - محدد حركة المرور

تحت **Link selection settings** تكوين البوابة:

- Primary and Backup gateways: حدد الخيار

- **Primary gateway**: تحديد البوابة المكونة ضمن الخطوة، Configure the Gateways

- انقر فوق **Save**



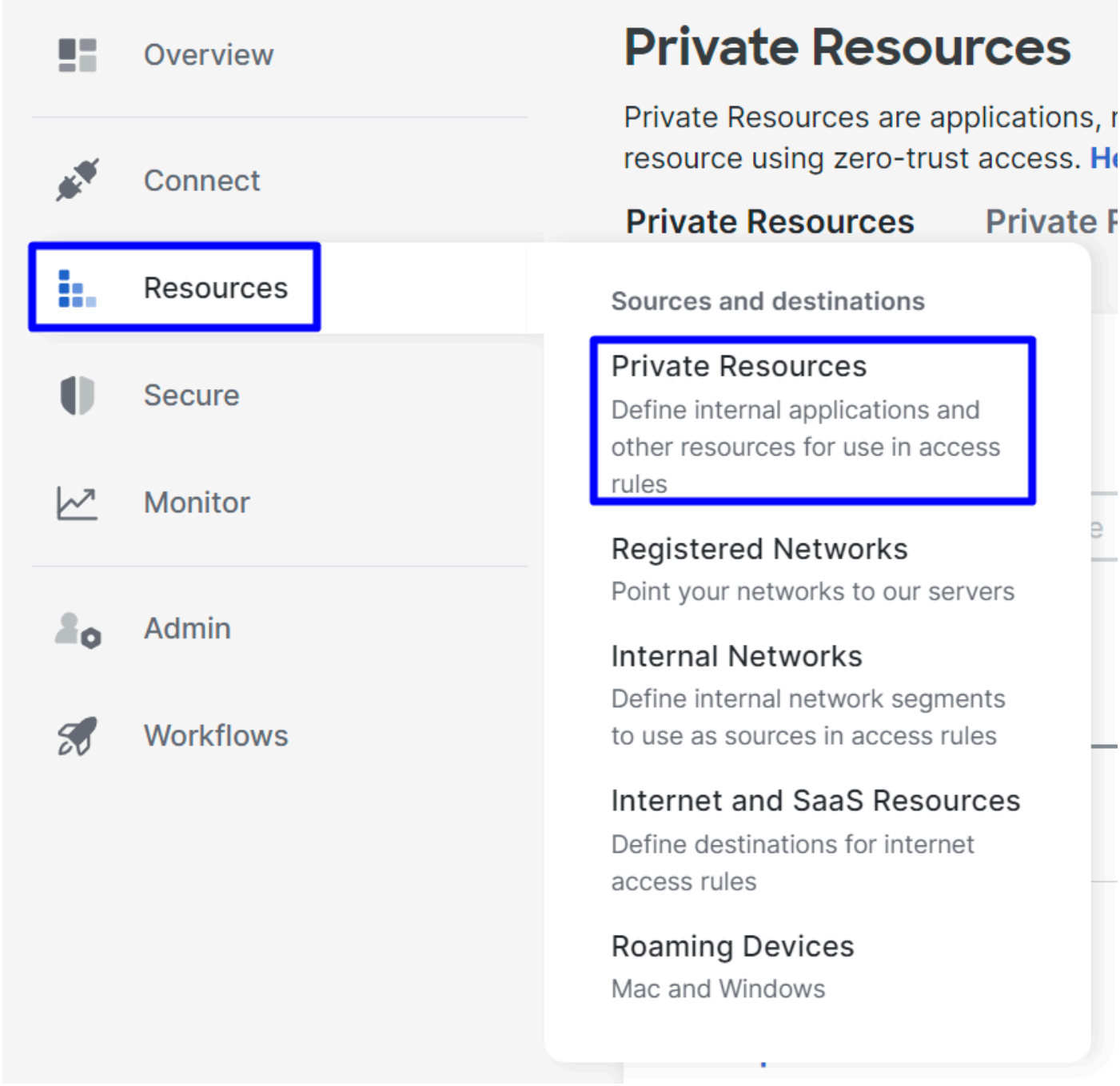

*SOPHOS - مسارات SD-WAN - محدد حركة المرور - البوابات الأساسية والنسخ الاحتياطي*

بعد إنهاء التكوين على جدار حماية Sophos XG، يمكنك المتابعة بالخطوة، **Configure Private App.**

تكوين التطبيق الخاص

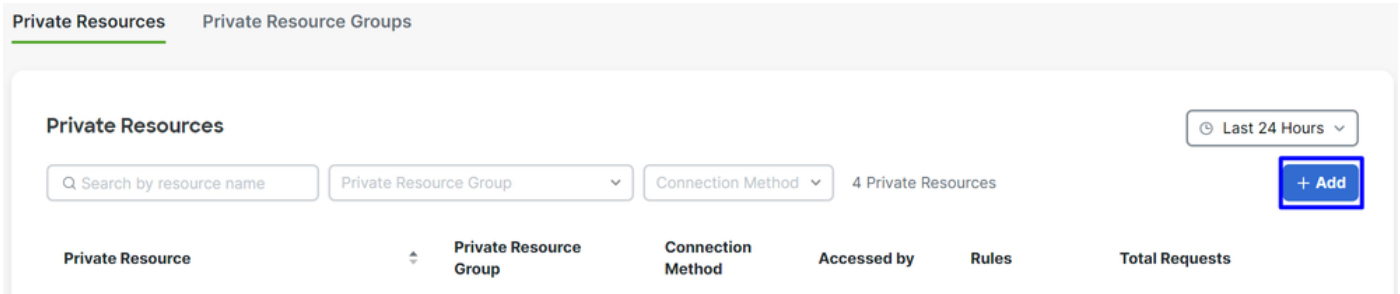
لتكوين الوصول إلى التطبيق الخاص، قم بتسجيل الدخول إلى مدخل المسؤول.

- انتقل إلى **Resources** > **Private Resources**



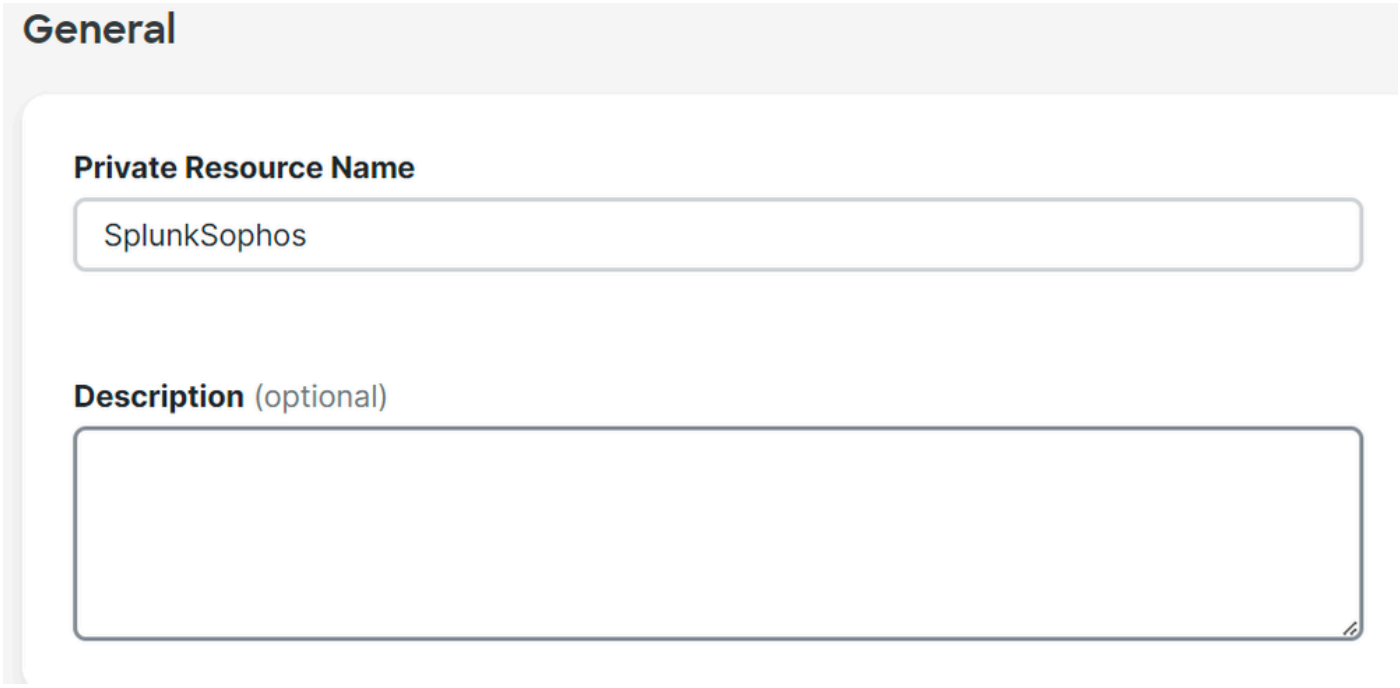

الوصول الآمن - الموارد الخاصة

- انقر فوق + Add




الوصول الآمن - الموارد الخاصة 2

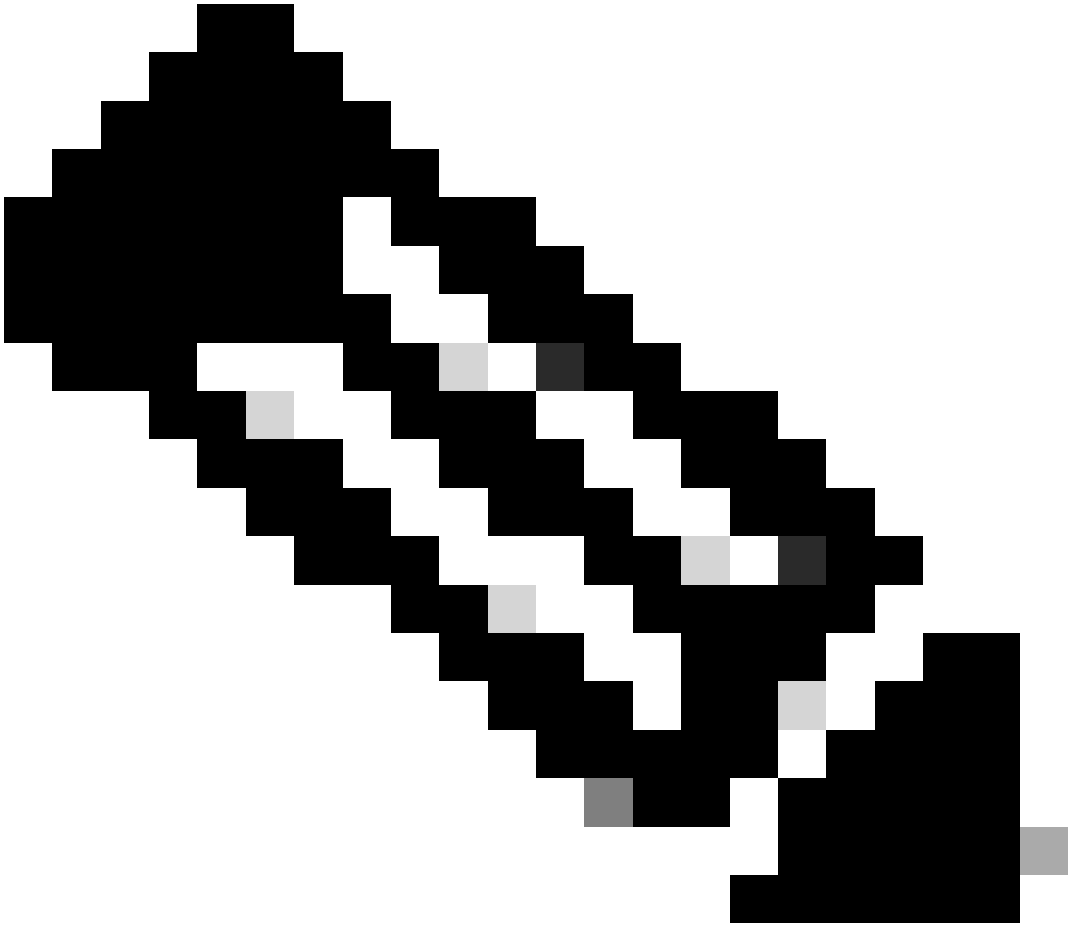
- تحت **General** تكوين **Private Resource Name**




الوصول الآمن - الموارد الخاصة - عام

تحت **Communication with Secure Access Cloud** التكوين:

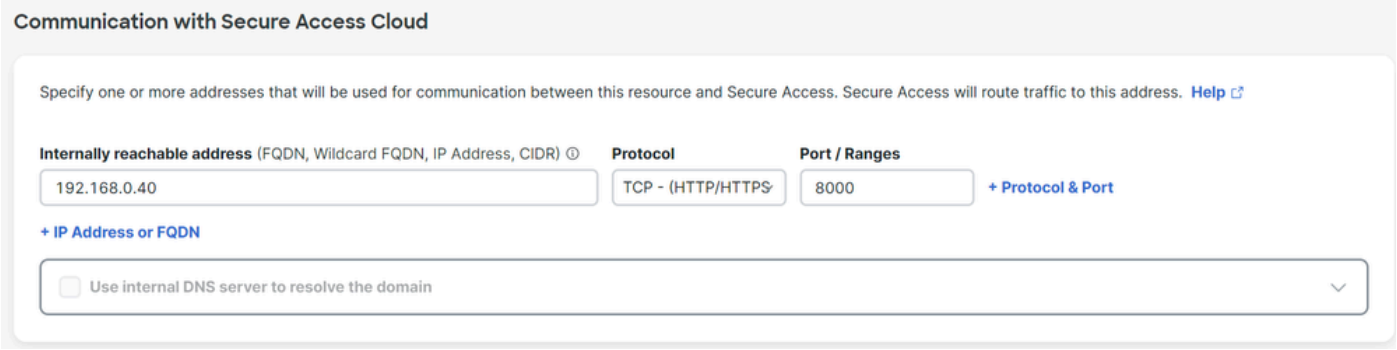
- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: حدد المورد الذي تريد الوصول إليه



**ملاحظة**: تذكر أنه قد تم تعيين العنوان القابل للوصول إليه داخليا في الخطوة، **Configure the Tunnel on Secure Access**.

---

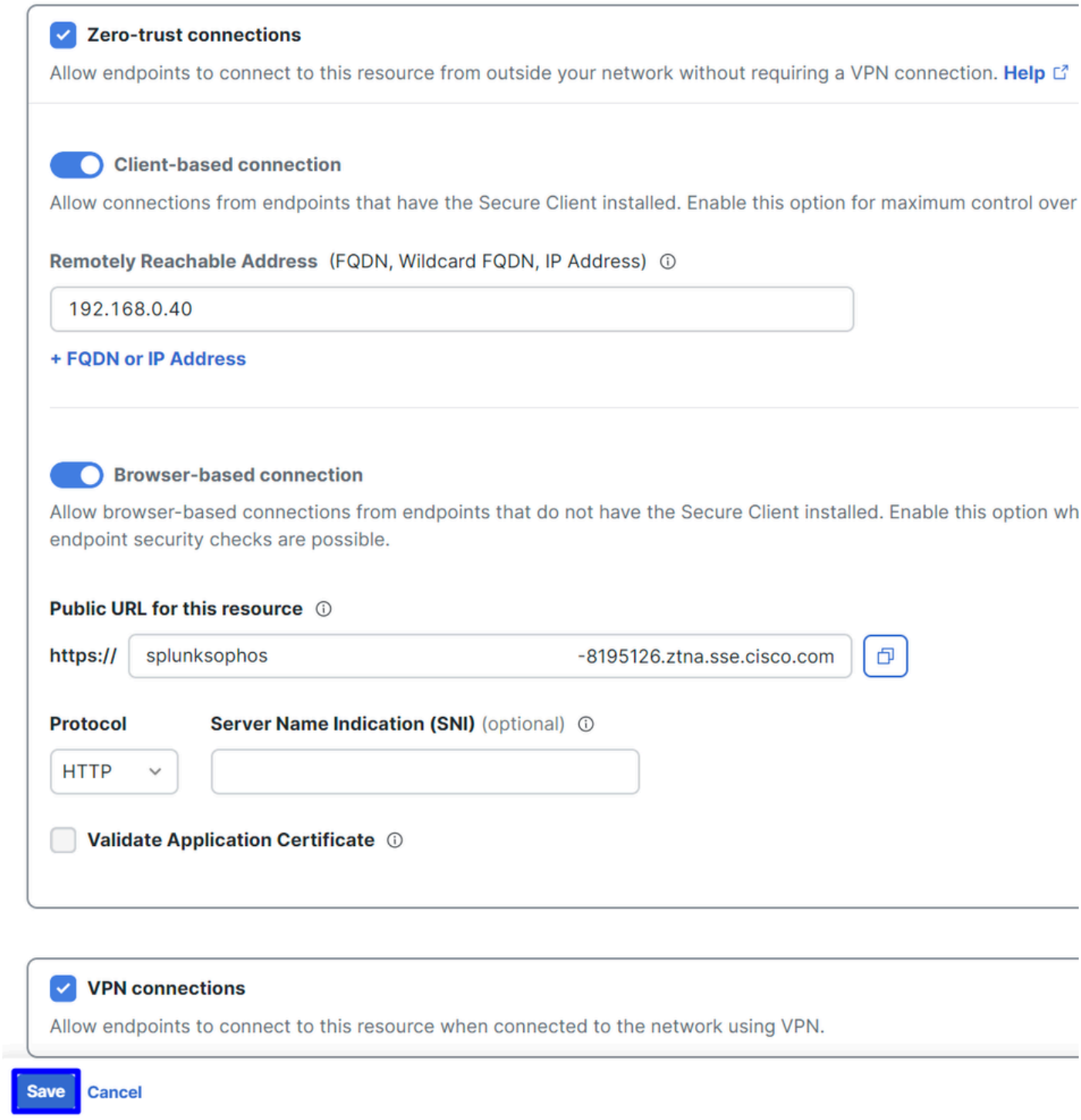
- **Protocol**: تحديد البروتوكول الذي تستخدمه للوصول إلى هذا المورد
- Port / Ranges : تحديد المنافذ التي تحتاج إلى تمكينها للوصول إلى التطبيق




*Secure Access - الموارد الخاصة - الاتصالات باستخدام Secure Access Cloud*

وضمن **Endpoint Connection Methods** هذه الوحدة، يمكنك تكوين جميع الطرق الممكنة للوصول إلى الموارد الخاصة عبر "الوصول الآمن"، واختر الطرق التي تريد إستخدامها لبيئتك:

- **Zero-trust connections**: حدد المربع لتمكين وصول ZTNA.
    - **Client-based connection**:: تمكين الزر للسماح بقاعدة زتنا الخاصة بالعميل
        - **Remotely Reachable Address**: تكوين IP الخاص بتطبيقك الخاص
    - **Browser-based connection**:: تمكين الزر للسماح ل ZTNA المستندة إلى المستعرض
        - Public URL for this resource: إضافة اسم لاستخدامه بالاقتران مع المجال ztna.sse.cisco.com
            - Protocol: أختر HTTP أو HTTPS كبروتوكول للوصول إليه من خلال المستعرض
    - **VPN connections**: حدد المربع لتمكين وصول RA-VPN.
- انقر **Save**




*Secure Access* - الموارد الخاصة - الاتصالات باستخدام *Secure Access Cloud 2*

بعد اكتمال التكوين، تكون هذه هي النتيجة:

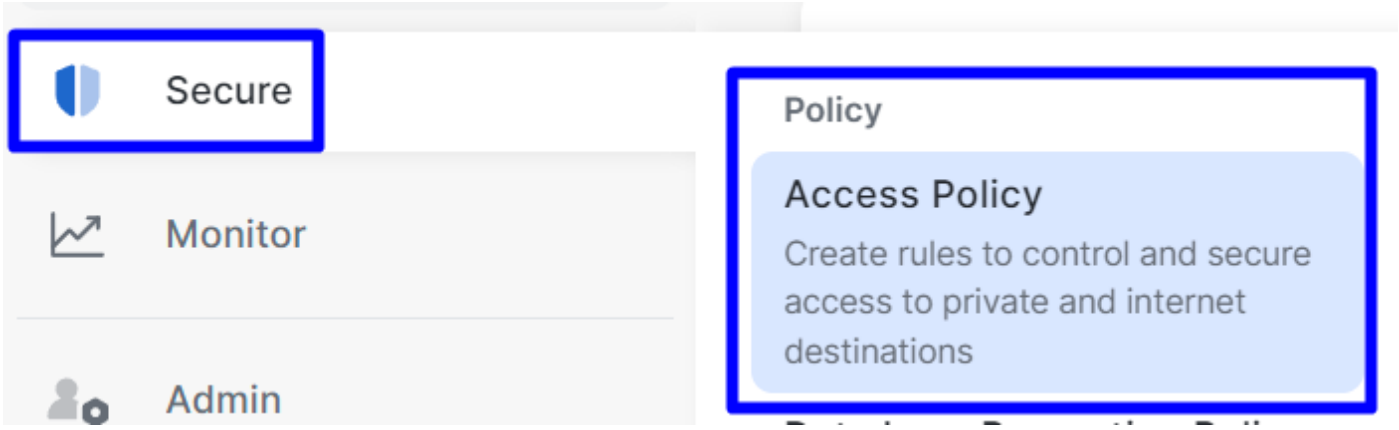
| Private Resource | Private Resource Group | Connection Method | Accessed by | Rules | Total Requests |
|---|---|---|---|---|---|
| SplunkSophos | - | VPN<br>Browser-based ZTNA<br>Client-based ZTNA | 1 | 2 | 16 |

الوصول الآمن - تكوين الموارد الخاصة

الآن يمكنك متابعة الخطوة، **Configure the Access Policy**.

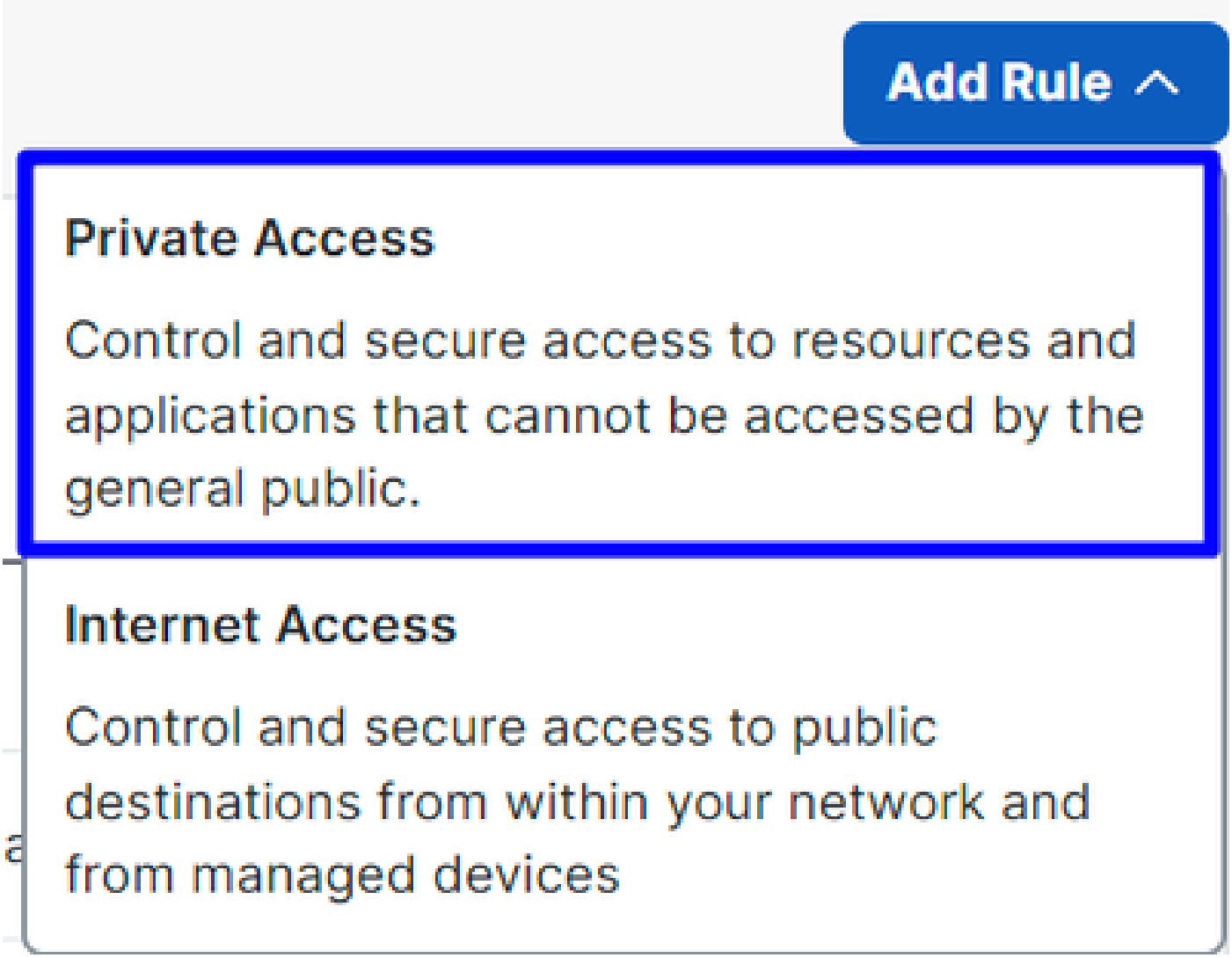
تكوين نهج الوصول

لتكوين نهج الوصول إلى Secure > Access Policy.




الوصول الآمن - سياسة الوصول

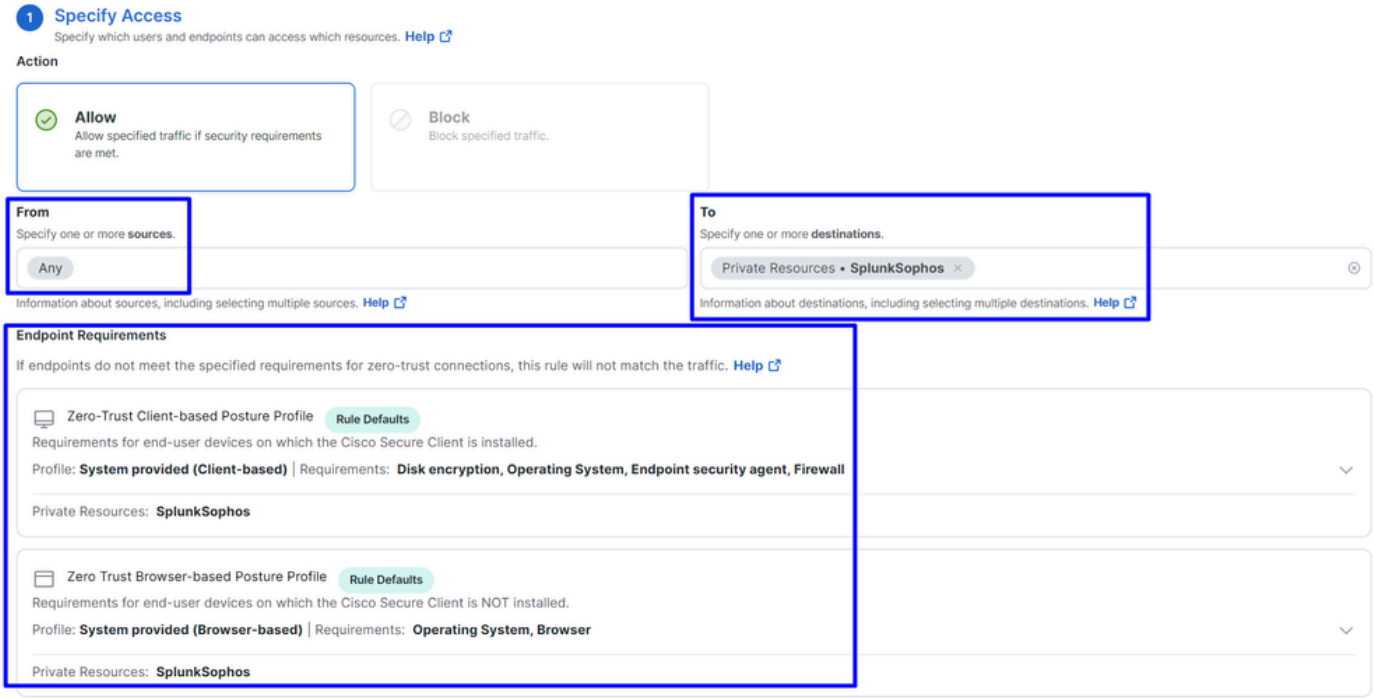
- انقر **Add Rule** > **Private Access**



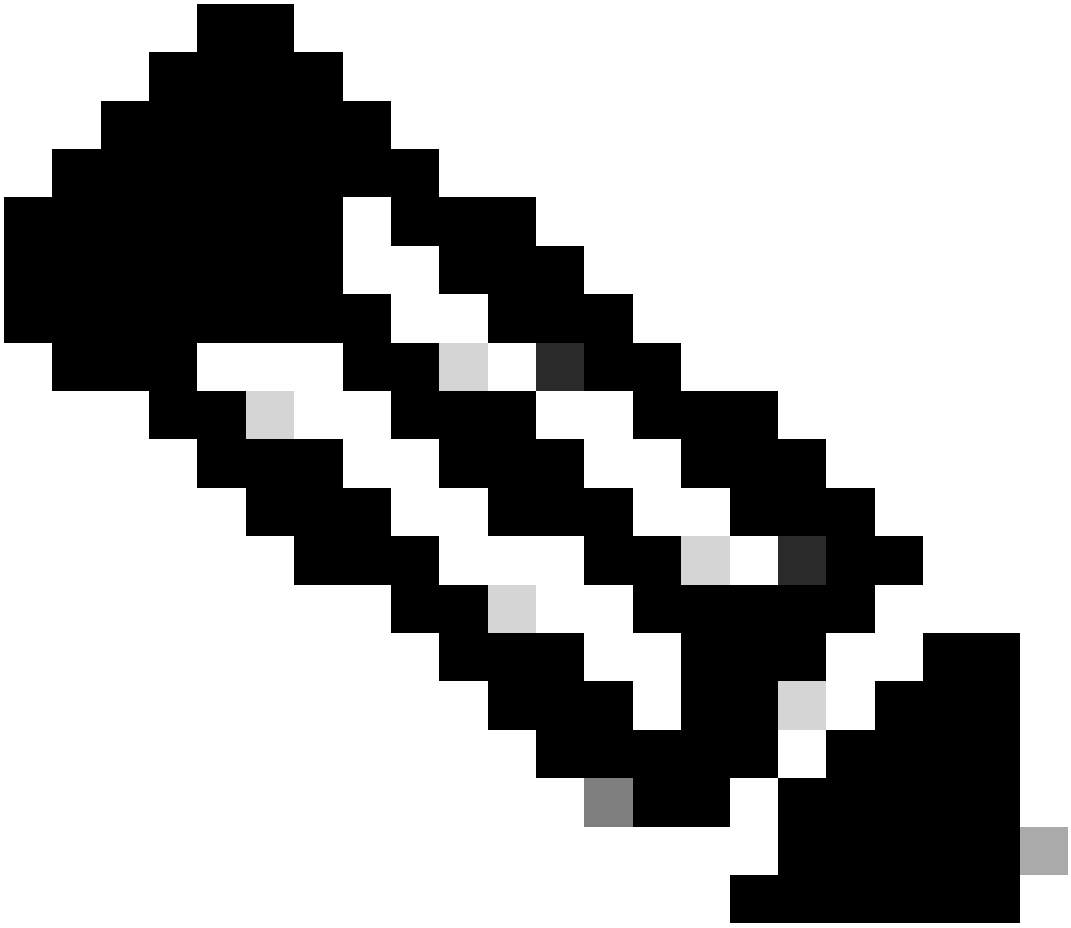

الوصول الآمن - سياسة الوصول - الوصول الخاص

قم بتكوين الخيارات التالية لتوفير الوصول عبر طرق متعددة للمصادقة:

- 1. Specify Access
    - Action:سماح
        - **Rule name**: تحديد اسم لقاعدة الوصول الخاصة بك
        - **From**: المستخدمون الذين تمنح لهم حق الوصول إلى
        - **To**: التطبيق الذي أردت السماح بالوصول إليه
        - Endpoint Requirements: (الافتراضي)
- انقر **Next**




الوصول الآمن - سياسة الوصول - تحديد الوصول



**ملاحظة**: للخطوة **2. Configure Security** حسب الحاجة، لكن في هذه الحالة، لم تقم بتمكين **Intrusion Prevention (IPS)**، أو **Tenant Control Profile**.

- انقر Save، ولديك:

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

الوصول الآمن - تم تكوين سياسة الوصول

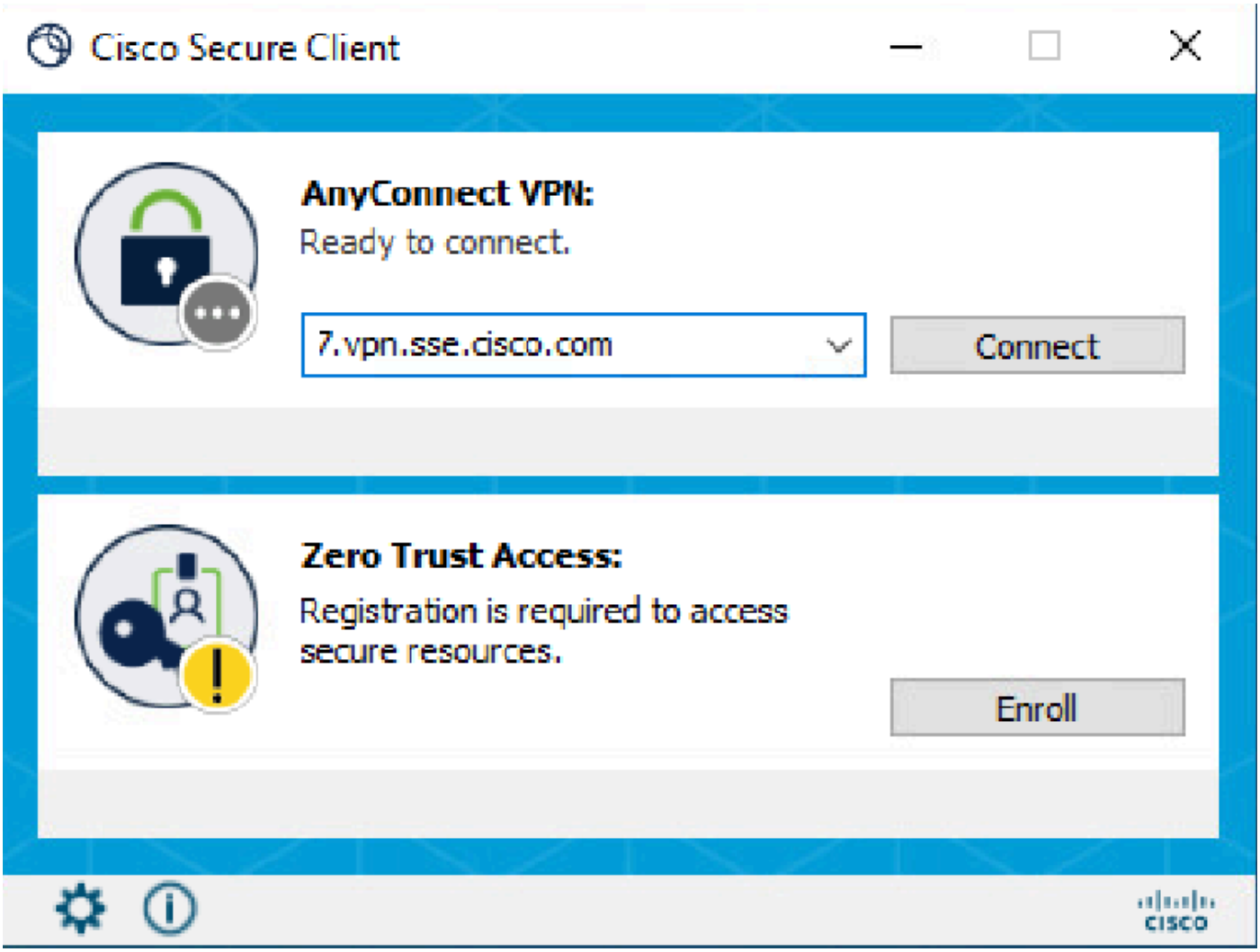
بعد ذلك، يمكنك متابعة الخطوة Verify.

التحقق من الصحة

للتحقق من الوصول، يجب أن تكون قد قمت بتثبيت عميل Cisco Secure Client الذي يمكنك تنزيله من تنزيل البرامج - Cisco Secure Client.

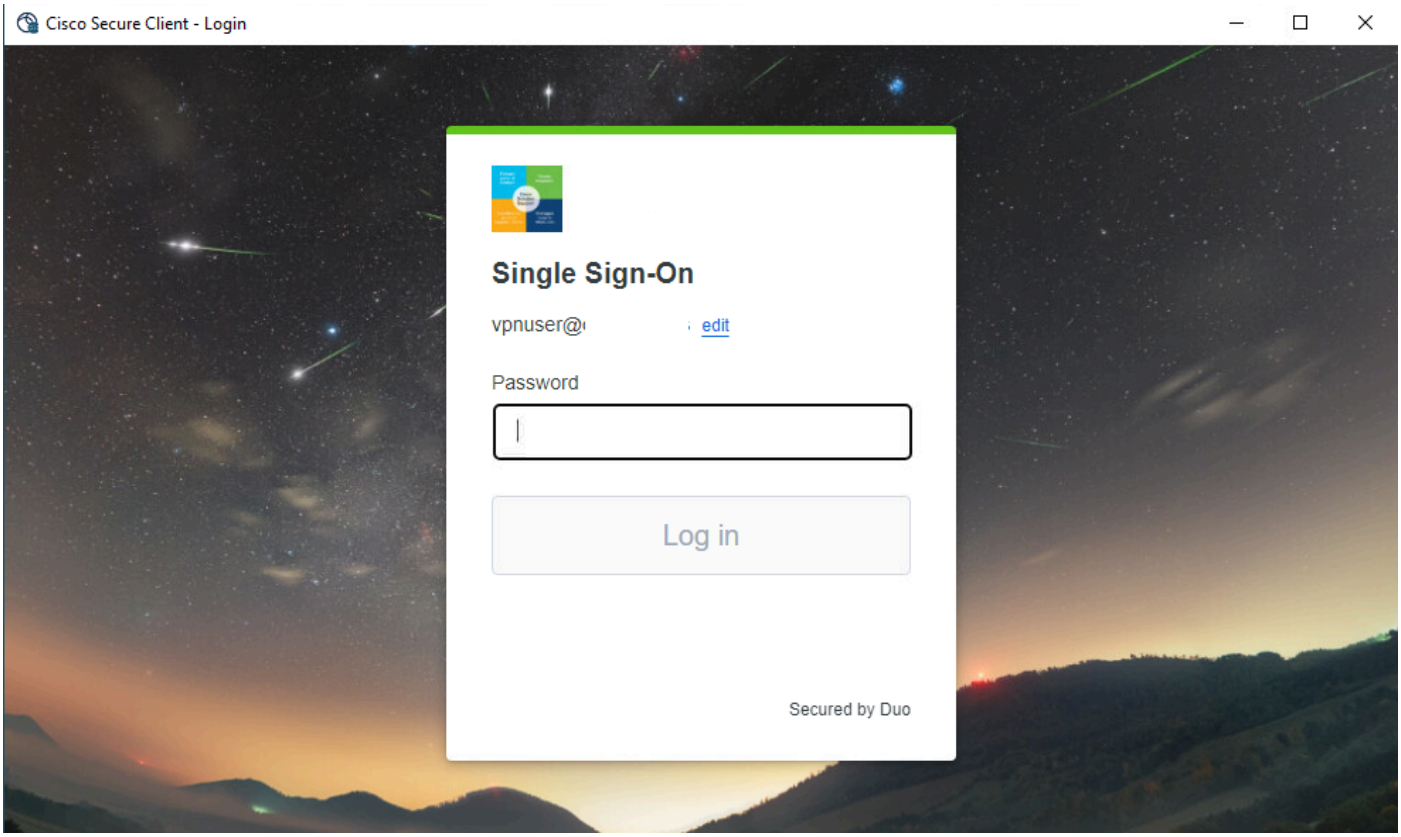
ار-VPN

تسجيل الدخول من خلال Cisco Secure Client Agent-VPN.



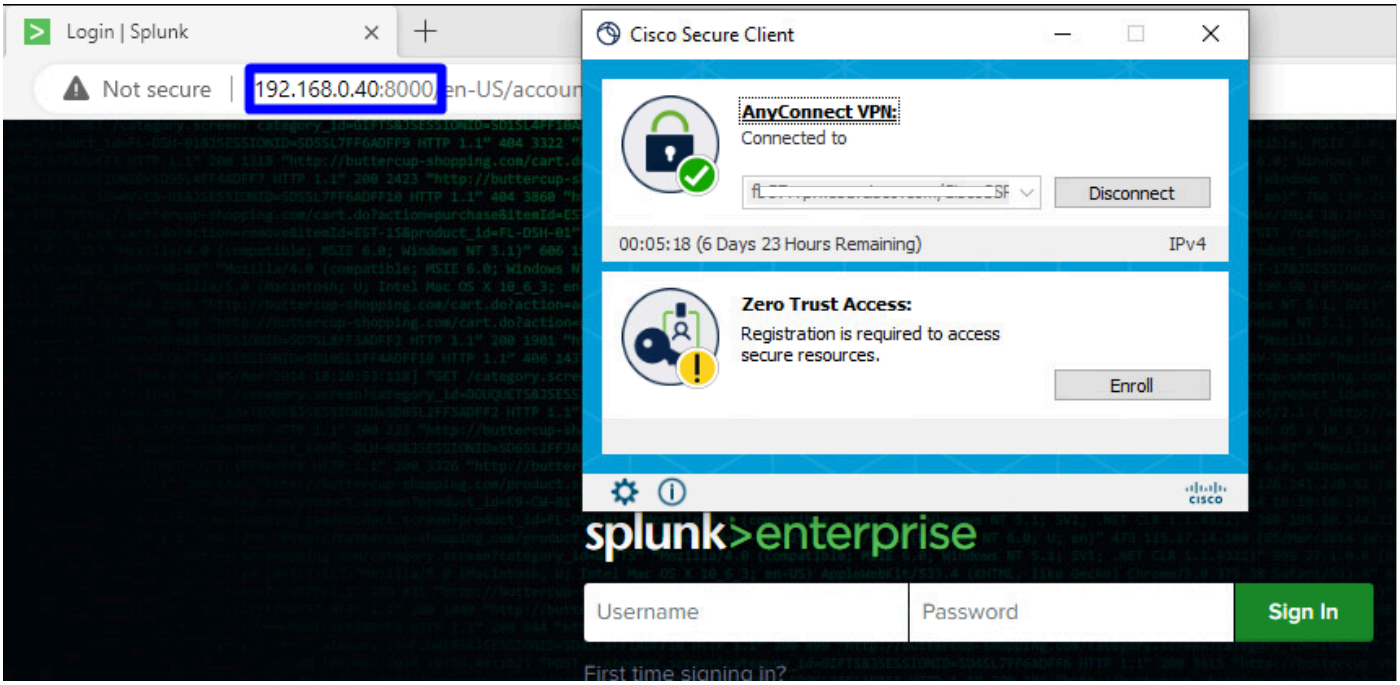

*Secure Client - VPN*

- المصادقة من خلال موفر SSO



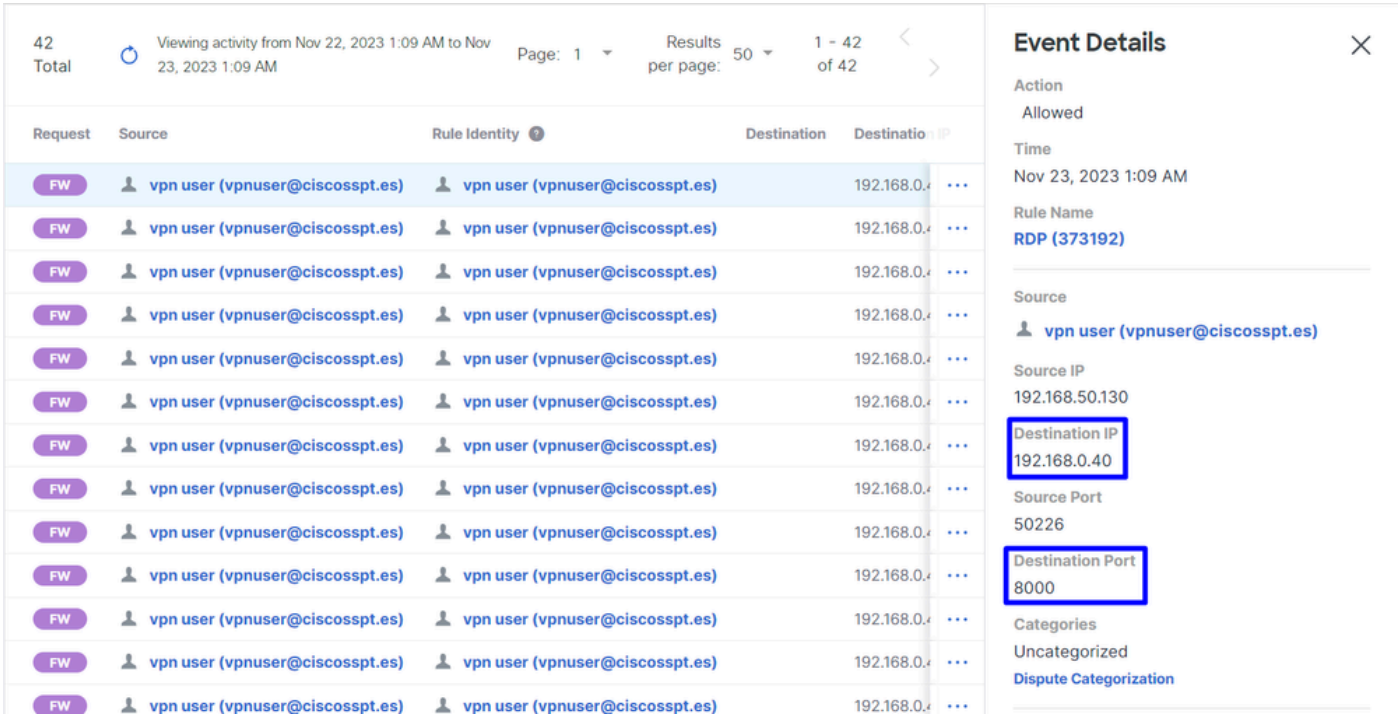

الوصول الآمن - *VPN - SSO*

- بعد أن تتم مصادقتك، يمكنك الوصول إلى الموارد:




الوصول الآمن - *VPN* - مصدق

انتقل إلى:Monitor > Activity Search

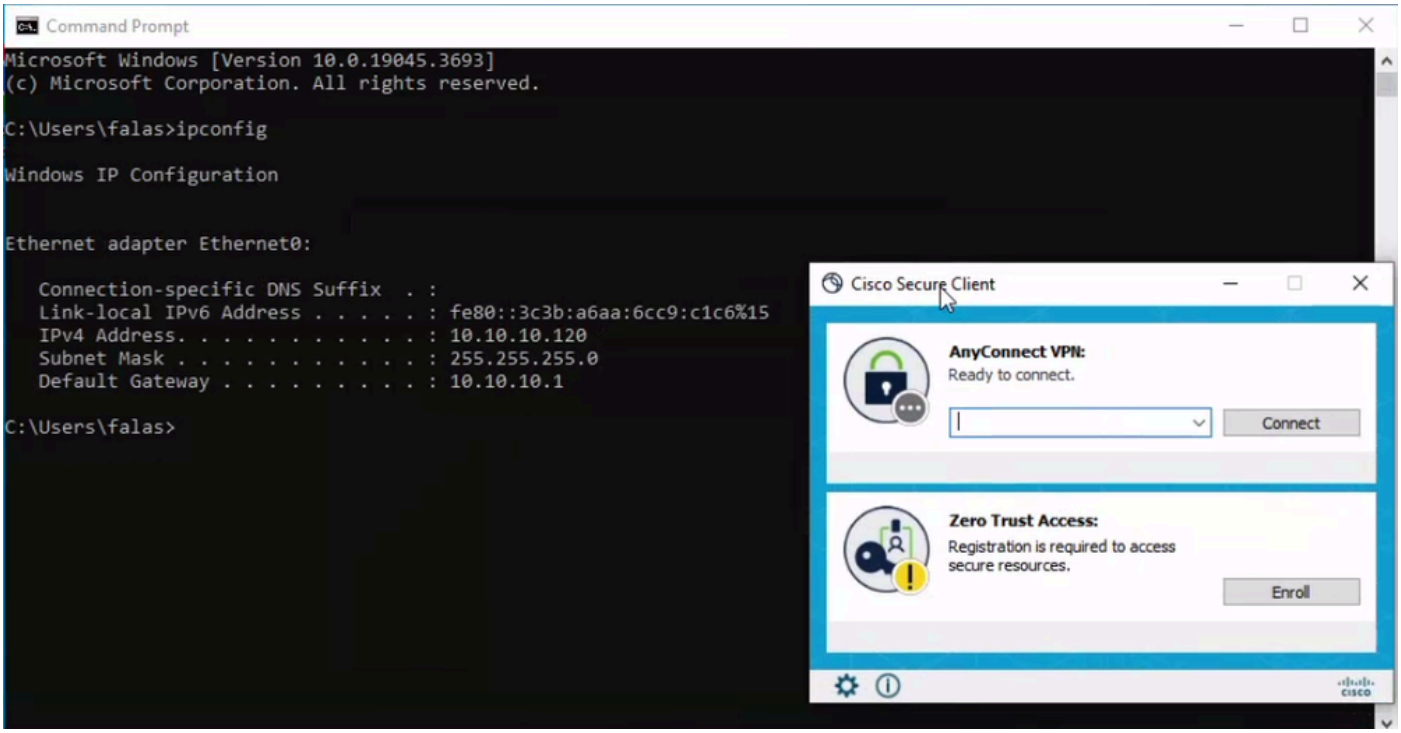



الوصول الآمن - البحث عن النشاط - *RA-VPN*

أنت يستطيع أن يرى المستعمل كان يسمح أن يصدق من خلال RA-VPN.

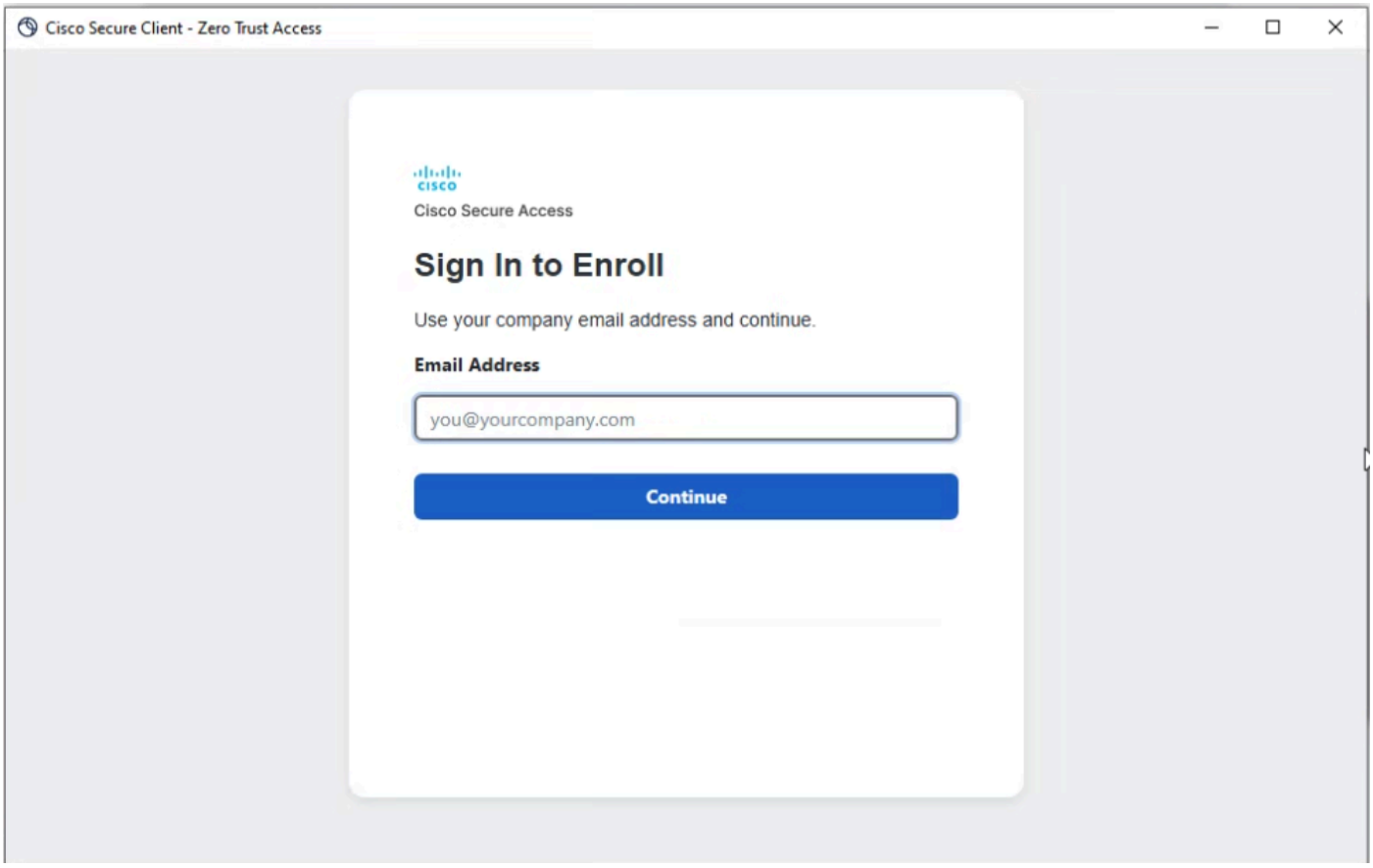
ZTNA العميل-الأساسي

تسجيل الدخول من خلال وكيل عميل آمن من Cisco - ZTNA.



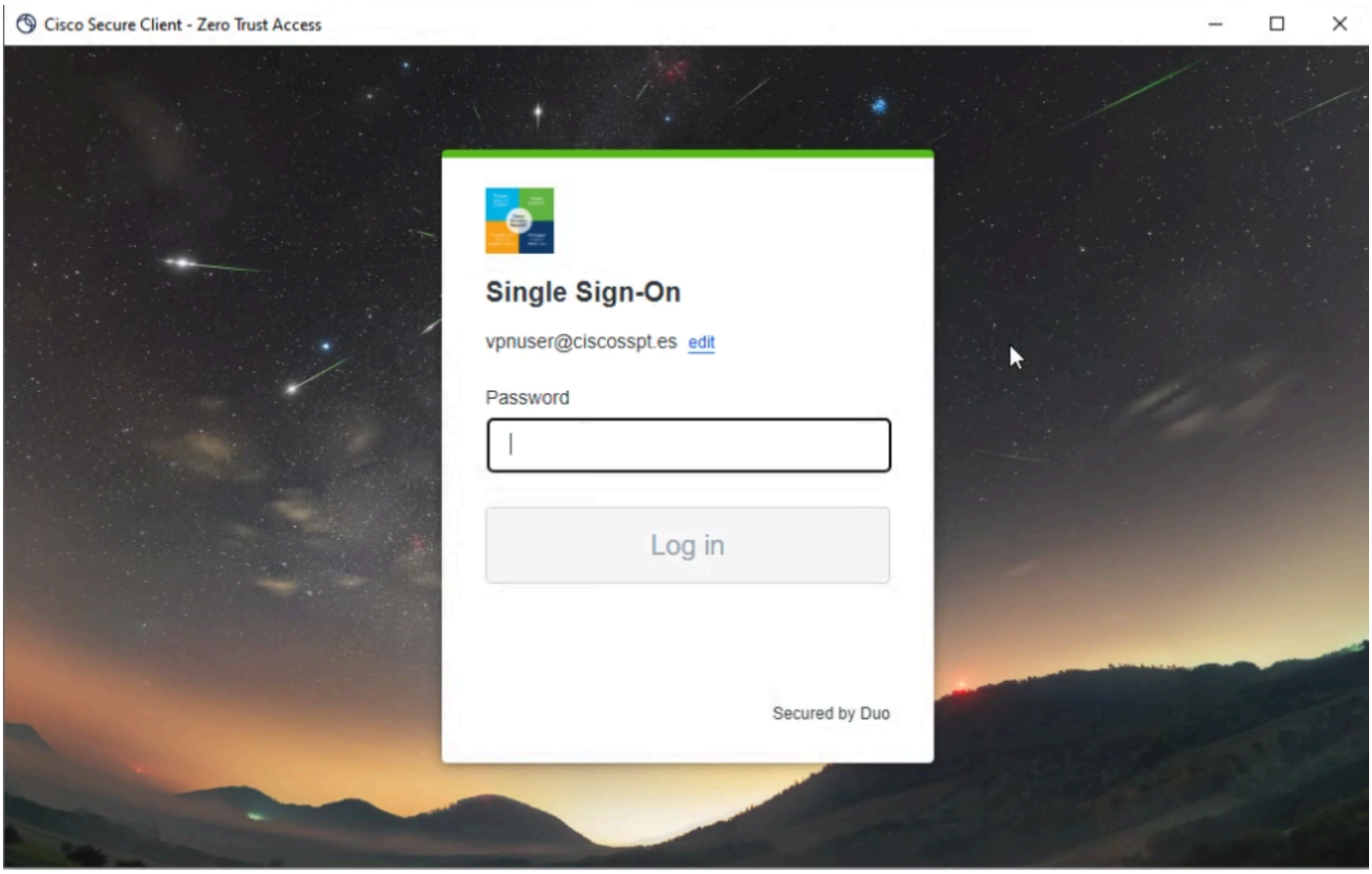

*Secure Client - ZTNA*

- التسجيل باسم المستخدم الخاص بك.



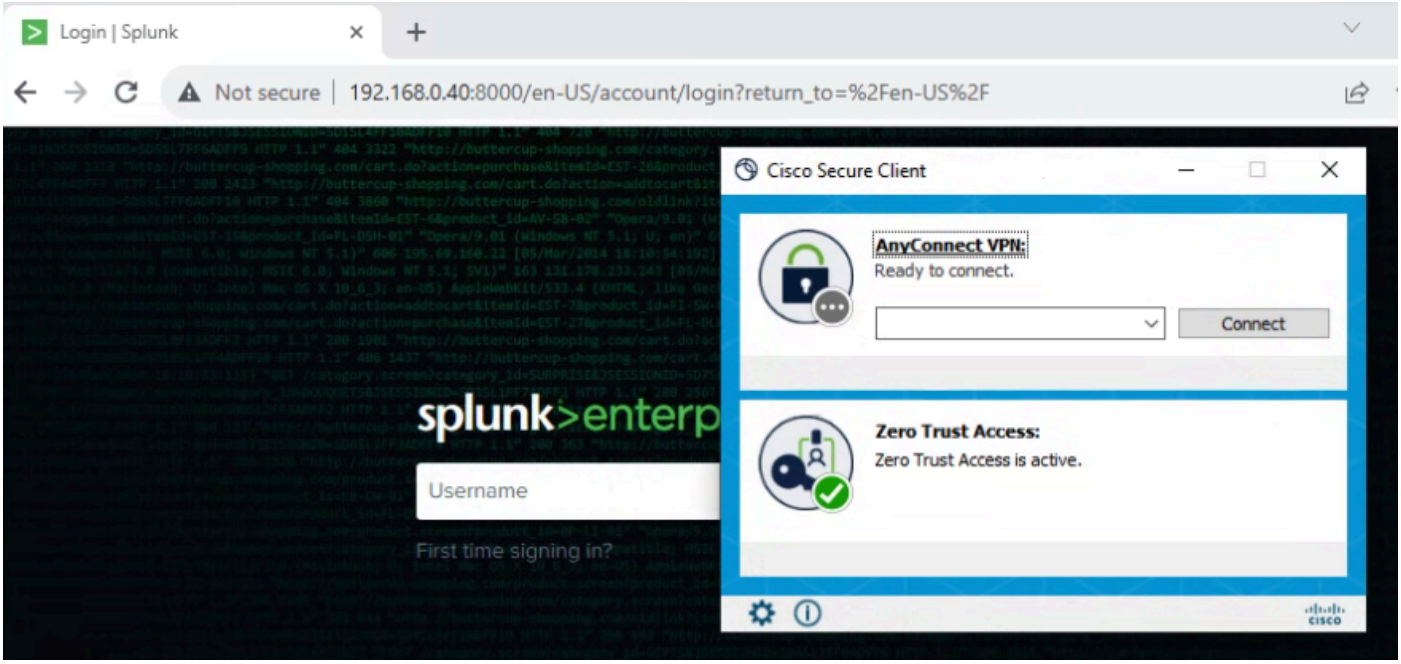

العميل الآمن - *ZTNA* - التسجيل

- المصادقة في موفر SSO



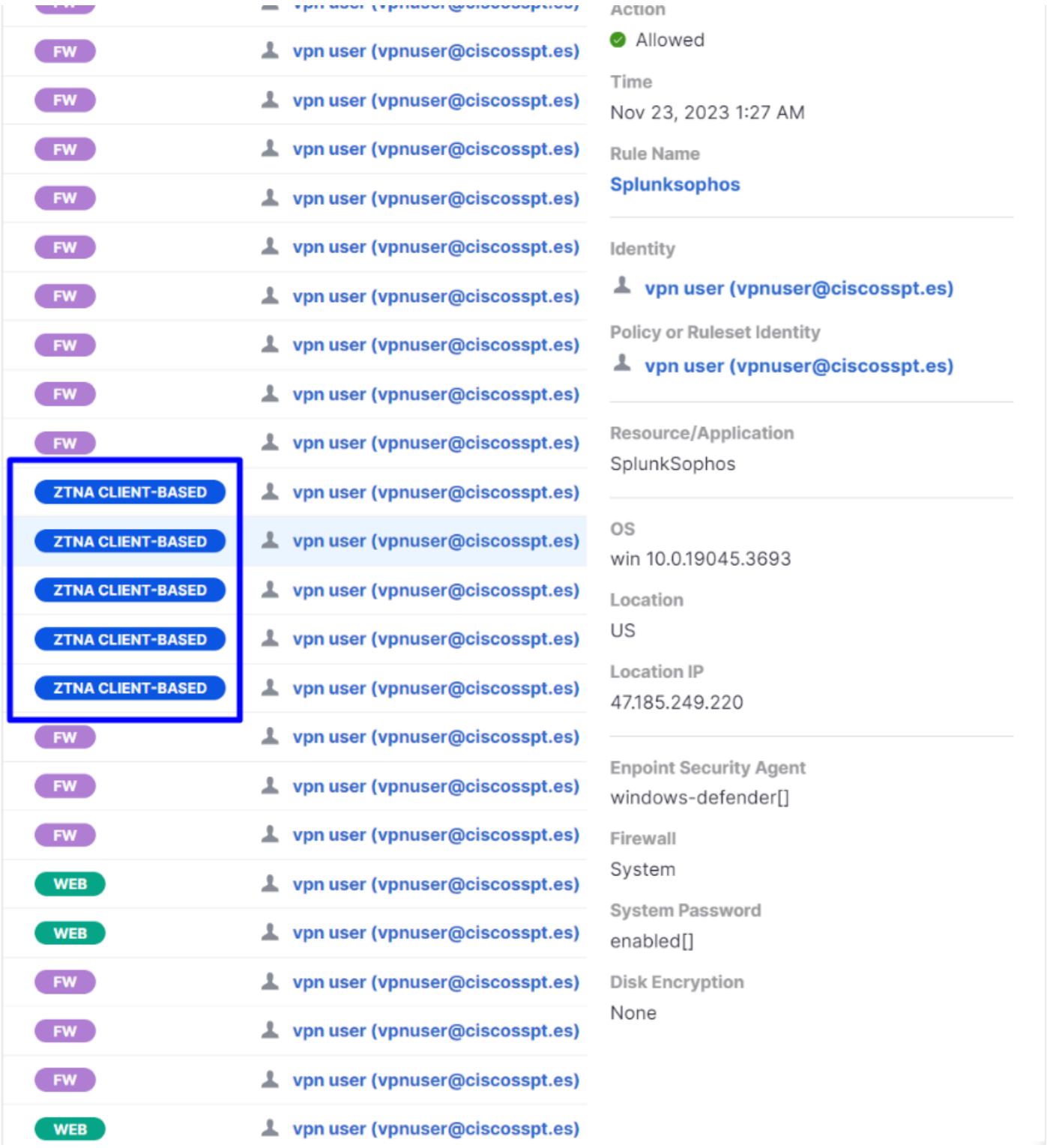

*Secure Client - ZTNA - تسجيل دخول SSO*

- بعد أن تتم مصادقتك، يمكنك الوصول إلى المورد:




*الوصول الآمن - ZTNA - مسجل*

انتقل إلى:Monitor > Activity Search

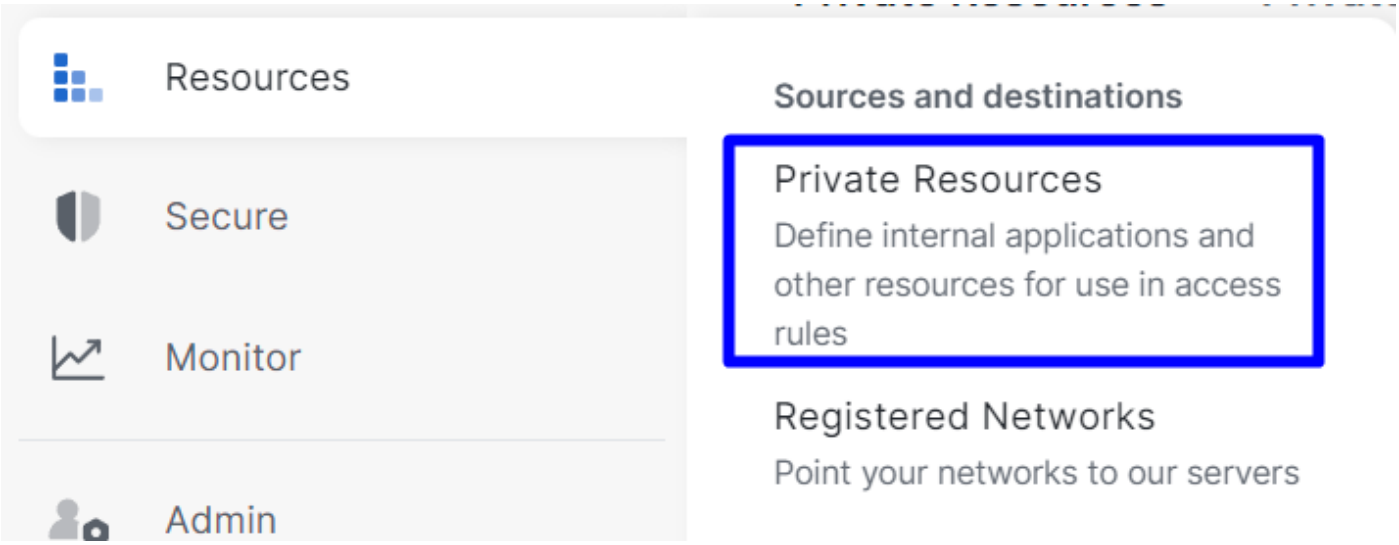



الوصول الآمن - البحث عن النشاط - المستند إلى عميل *ZTNA*

أنت يستطيع رأيت أن المستعمل كان يسمح أن يصدق من خلال ZTNA baser.

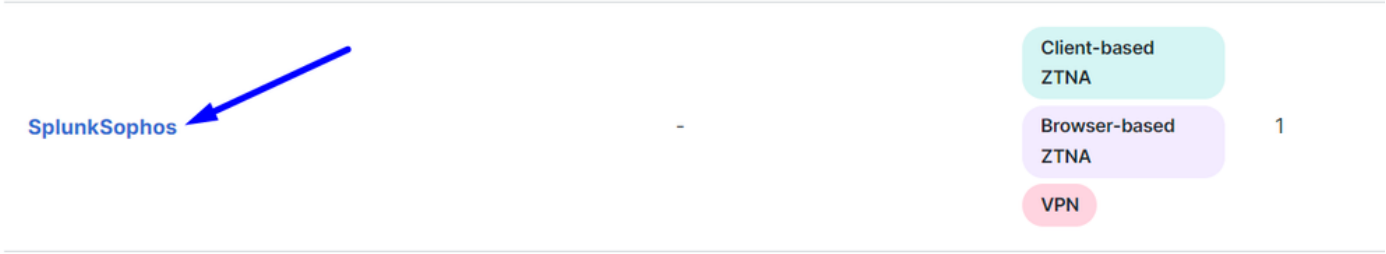
ZTNA المستند إلى المستعرض

للحصول على عنوان URL، يجب الانتقال إلى **Resources** > **Private Resources**.




الوصول الآمن - مورد خاص

- انقر على النهج




الوصول الآمن - مورد خاص - *SplunkSophos*

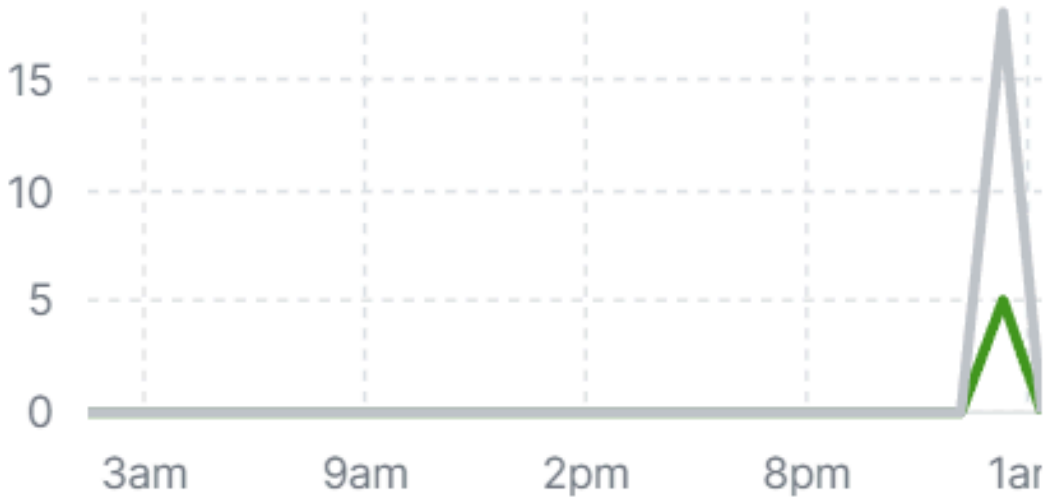
- تمرير لأسفل

# 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 |

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).