

# ةيامح رادج مادختساب نمآلا لوصولا نيوكت Sophos XG

## تايوتحمل

---

[ةمدقمل](#)

[ةيساسآلا تابلطتمل](#)

[تابلطتمل](#)

[ةمدختسمل تانوكمل](#)

[ةيساسآا تامولعم](#)

[نيوكتل](#)

[نمآلا لوصولا ىلع قفئل نيوكت](#)

[قفئل تاناي](#)

[Sophos ىلع قفئل نيوكت](#)

[IPsec فيرعت فلم نيوكت](#)

[عقوم ىلا عقوم نم VPN ةكبش نيوكت](#)

[قفئل ةوچاو نيوكت](#)

[تابلويل نيوكت](#)

[SD-WAN راسم نيوكت](#)

[صاڭلا قيبطتل نيوكت](#)

[لوصولا جهن نيوكت](#)

[ةحصلل نم ققحتل](#)

[ار-VPN](#)

[يساسآلا لي معمل ZTNA](#)

[ضرعتسمل ىلا دننتسمل ZTNA](#)

[قلص تاذا تامولعم](#)

---

## ةمدقمل

Sophos XG ةيامح رادج مادختساب نمآلا لوصولا نيوكت ةيفي ك دننتسمل اذه حضوي

## ةيساسآلا تابلطتمل

- [مدختسمل ري فوت نيوكت](#)
- [ZTNA SSO ةقداصم نيوكت](#)
- [دعب نع لوصولل VPN ىلا نمآلا لوصولا نيوكت](#)

## تابلطتمل

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- Sophos XG ةيامح رادج
- نمآلا لوصولا

- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- اياوز نودب انتز

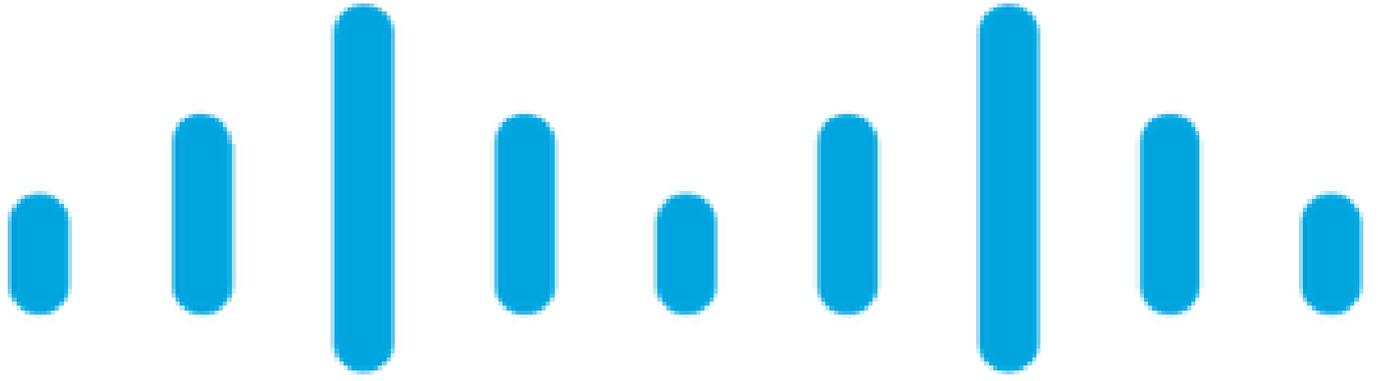
## ةمدختسمل تانوكملا

ىل دن تسمل اذه يف ةدراول تامولعمل دن تس

- ةيامح راج Sophos XG
- نمل لوصول
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دن تسمل اذه يف ةدراول تامولعمل ءاشنإ مت  
تناك اذإ. (يضا رتفا) حوسمم نيوكتب دن تسمل اذه يف ةمدختسمل ةزهجال عيمج تادب  
رما يال لم تحمل ريثاتلل كمهف نم دكأتف ، ليغشتلا ديقتك تبش

## ةيساسأ تامولعمل



# CISCO

## Secure

## Access

# SOPHOS

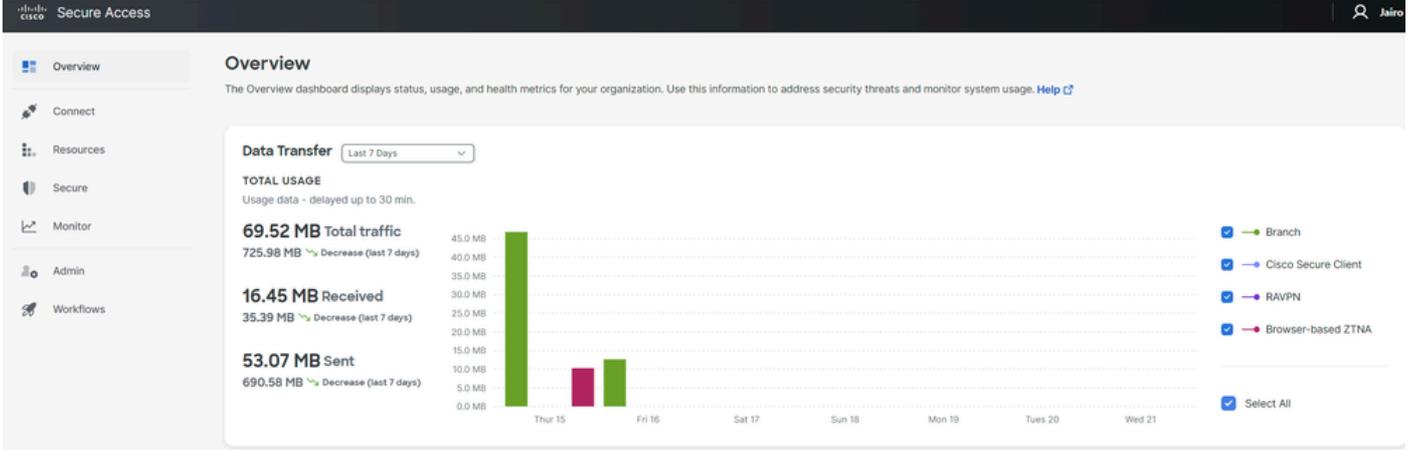
نمآل لوصول - Sophos

هري فوتو ةصاخلا تاقي ببطتلا ىلإ لوصول ةيامح نامضل Secure Access ةزيم Cisco تتم مص ةكبشلا نم لاصتالا نمضي هنا امك. ءاوس دح ىلع ةكبشلا ىلع مئاقو يلحم اساسا ىلع اهعيمج فدهت، ةددعتم ةينما تاقتو بيل اساسا قي ببطت لالخنم كلذ ققحتي و. تنرتنإلا ىلإ ةباحسلا ربع اهلا لوصول دنع تامولعمل ىلع ظافحل ىلإ

# نيوكتلا

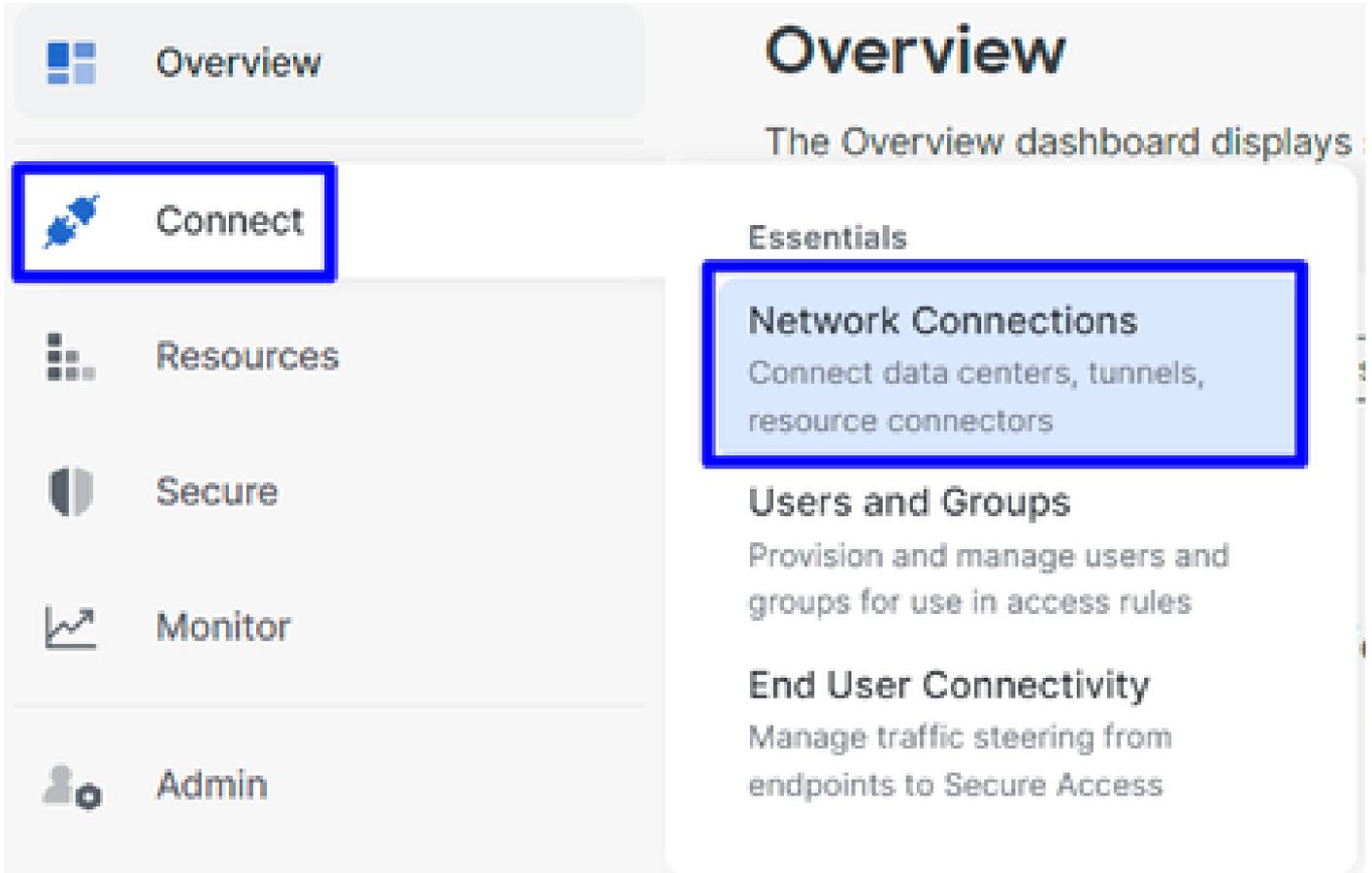
نمآلا لوصولا ىلع قفنلا نيوكت

ب ةصاخلا ةرادإلا ةحول ىلا لقتنا [Secure Access](#).



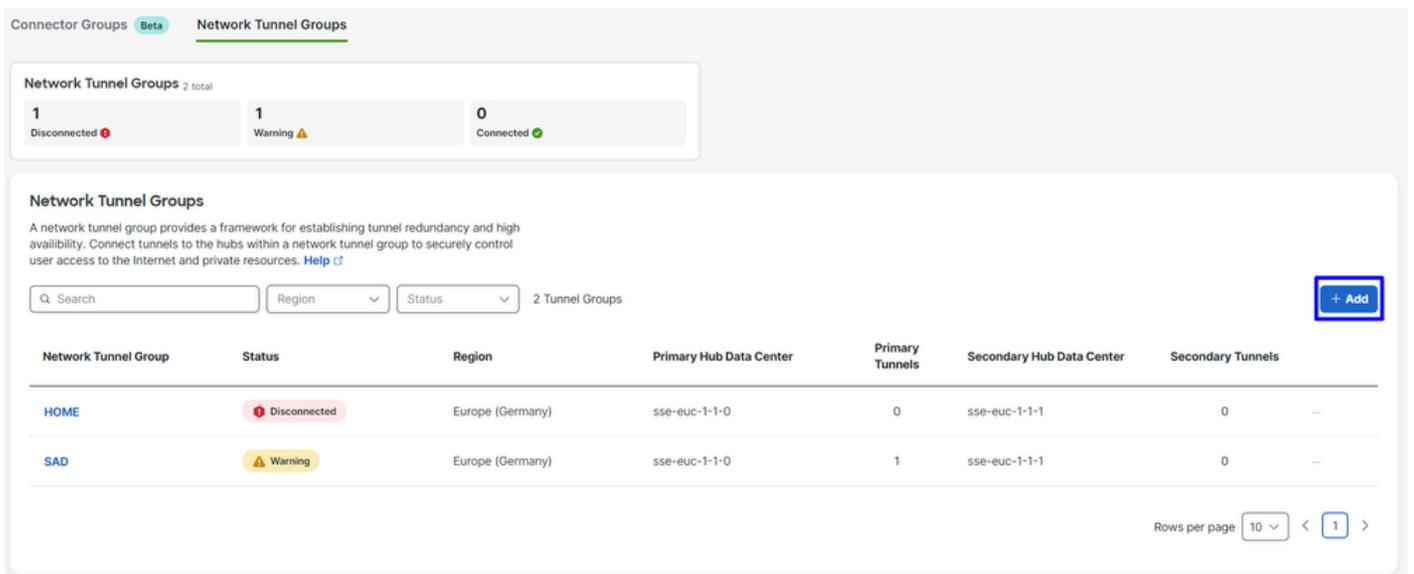
ةيسيئرلا ةحفصلا - نمآلا لوصولا

- قوف رقنا Connect > Network Connections.



ةكبشلا تالاصتا - نمالا لوصولا

- + Add. ىلع طغضلا Network Tunnel Groups تحت



ةكبشلا قف ناعومجم - نمالا لوصولا

- Tunnel Group Name، Region وDevice Type. نيوكتلا
- Next. رقنا

## 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

 ∨

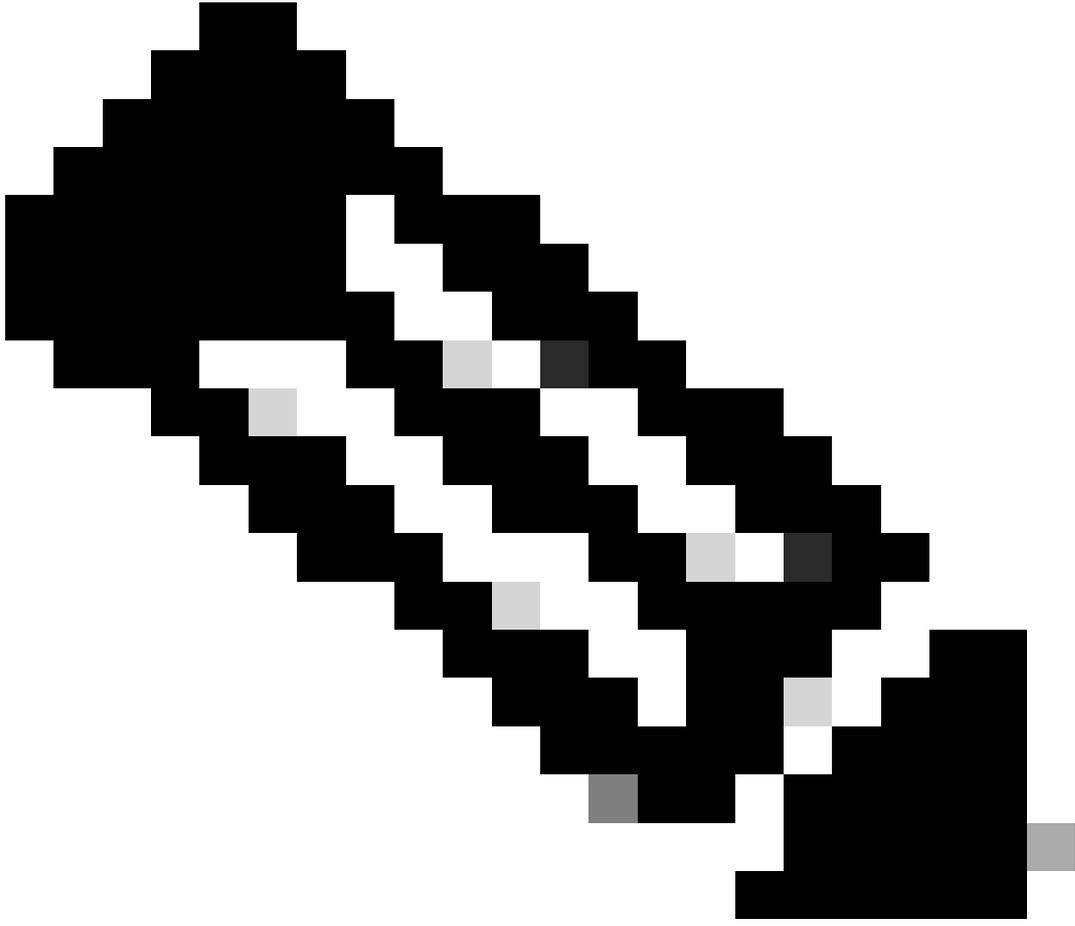
### Device Type

 ∨

[Cancel](#)

[Next](#)

ةماعةل تادادعإلإ - قافنألأ تاعومجم - نمألأ لوصولأ



ة.امحل رادج ع قوم ىل اة قطنم برقأ رتخأ :ةظحالم

- 
- Tunnel ID Format و Passphrase نى و ك ت ب مق
  - ر ق ن ا .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

رورم الة رابع و ق فنل الفرع - قافنأل تا ع و م جم - نمأل لوصول

- كرح ريرمت ديرتو ة كبشال لعل اهنويك تب تمق يتل ة فيضم ال تا ئيبل وأ IP نيوانع تا قاطن نيوك تب مق نمأل لوصول لال خ نم رورم الة .
- رقا . 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

ه ج و تل تارا ي خ - قافنأل تا ع و م جم - نمأل لوصول

Configure the tunnel on Sophos. ة لال ة و ط خ لل تامول عمل كلت ظفح ءا ج رل ، ق فنل ضرع لوح Save تامول عمل قوف رقا دع ب

## قفلنل تانايب

### 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>	csasophos@	-sse.cisco.com	📄
<b>Primary Data Center IP Address:</b>	18.156.145.74		📄
<b>Secondary Tunnel ID:</b>	csasophos@	-sse.cisco.com	📄
<b>Secondary Data Center IP Address:</b>	3.120.45.23		📄
<b>Passphrase:</b>	[REDACTED] 📄		

[Download CSV](#)

[Done](#)

نڤيوكتل فانئئس | قافنأل تاومجم - نمأل لوصول

Sophos لى قفلنل نڤيوكتل

IPsec فيرعت فلم نڤيوكتل

كب صألل Sophos XG ةيامح رادج لى لقتنا ، IPsec فيرعت فلم نڤيوكتل

اذهل هباشم ءيش لى لصحت

**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

Security Heartbeat®

Synchronized Application Control™

Zero-day protection

ATP

UTQ

SSL/TLS connections

Active firewall rules

Reports

Messages

قراة الة حول - Sophos

- Profiles الة لقتنا
- Add قوف رقتنا كلذ دعبو IPsec Profiles قوف رقتنا

IPsec profiles

Device access

Add

Delete

algorithm

Phase 2

Manage

تحت **General Settings** التوكات:

- **Name:** Cisco نم نم آل لوصولا جه نل عجرم مس
- **Key Exchange:** IKEv2
- **Authentication Mode:** سيسئزللا عضولا
- **Key Negotiation Tries:**0
- **Re-Key connection:** راخال ددح

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

تحت **Phase 1** التوكات:

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

## 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

1 حل مرحل - IPsec في رعت تافل م - Sophos

ن يوك الت ال Phase 2 تحت

- PFS group (DH group): لوالأ حل مرحل س فن
- **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

2 حل مرحل - IPsec في رعت تافل م - Sophos

ن يوك الت ال Dead Peer Detection تحت

- **Dead Peer Detection:** راخ ل ددح
- **Check peer after every:** 10
- **Wait for response up to:** 120 (يضا رت فالال)
- **When peer unreachable:** ادب ل اداع (يضا رت فالال)

## BEFORE

Dead Peer Detection

Dead Peer Detection

Check peer after every  Seconds

Wait for response up to  Seconds

When peer unreachable

## AFTER

Dead Peer Detection

Check peer after every  Seconds

Wait for response up to  Seconds

When peer unreachable

تيمم ال ريظننل فاشتك - IPsec فيرعت تافل - Sophos

طغضا كلذ دعب Save and proceed with the next step, Configure Site-to-site VPN.

عقوم لىل عقوم نم VPN ةكبش نيوكت

Add قوف رقنا مث Site-to-site VPN قوف رقنا (VPN)، ةرهاظلا ةصاخلا ةكبشلا نيوكت ادبل

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

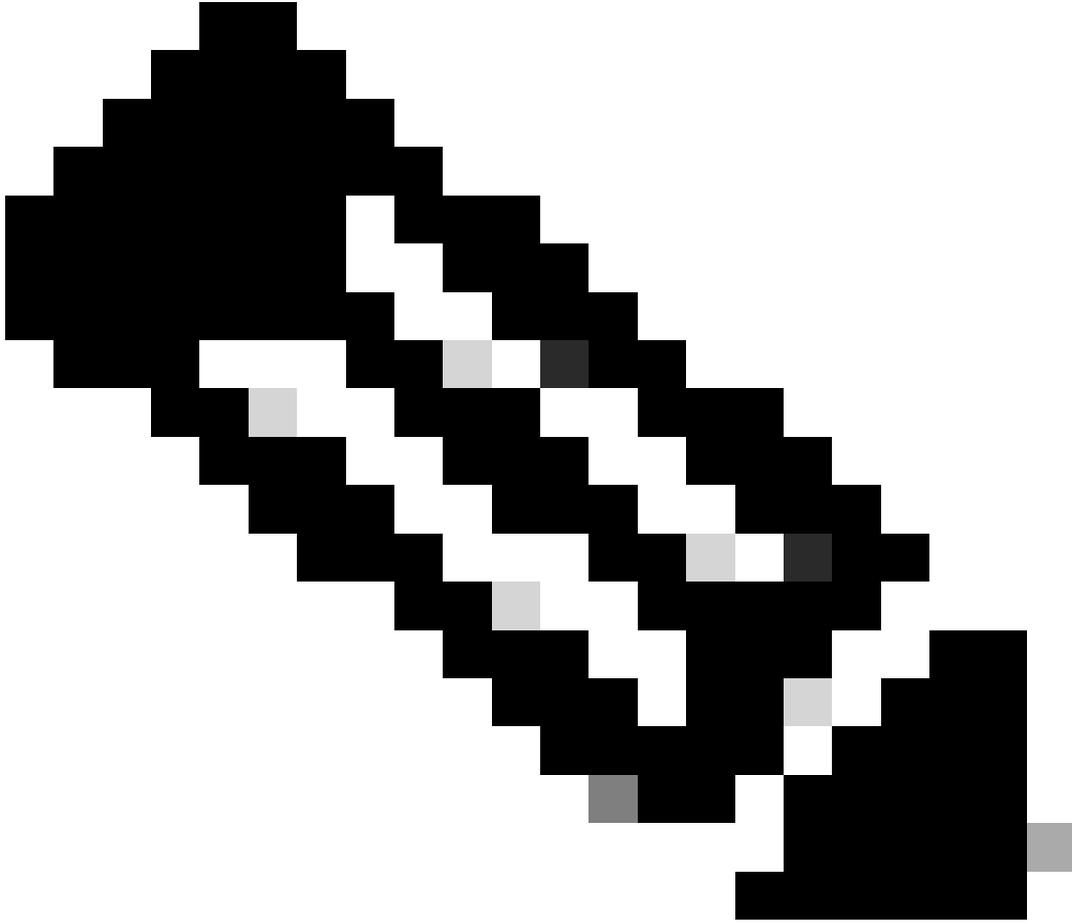
Add Delete

عقوم لىل عقوم نم VPN ةكبش - Sophos

نيوكتلا ال General Settings تحت:

- Name: Cisco نم نمال لوصولل IPsec جهنل عجرم مسا
- IP version: IPv4
- Connection type: قفنل ةهجاو
- Gateway type: لاصتالا ادب

- رايخلا ددح: Active on save
- 



عقوم ىل عقوم نم VPN ةكبش نيوكت ىل يهتنت نأ دعب ايئاقلت VPN ةكبش رايخلا نكمي Active on save : ةظحالم

---

## General settings

Name

SecureAccessS

IP version



IPv4



IPv6



Dual



Activate on save



Create firewall rule

Description

This is the IPsec Policy for Sophos

Connection type

Tunnel interface

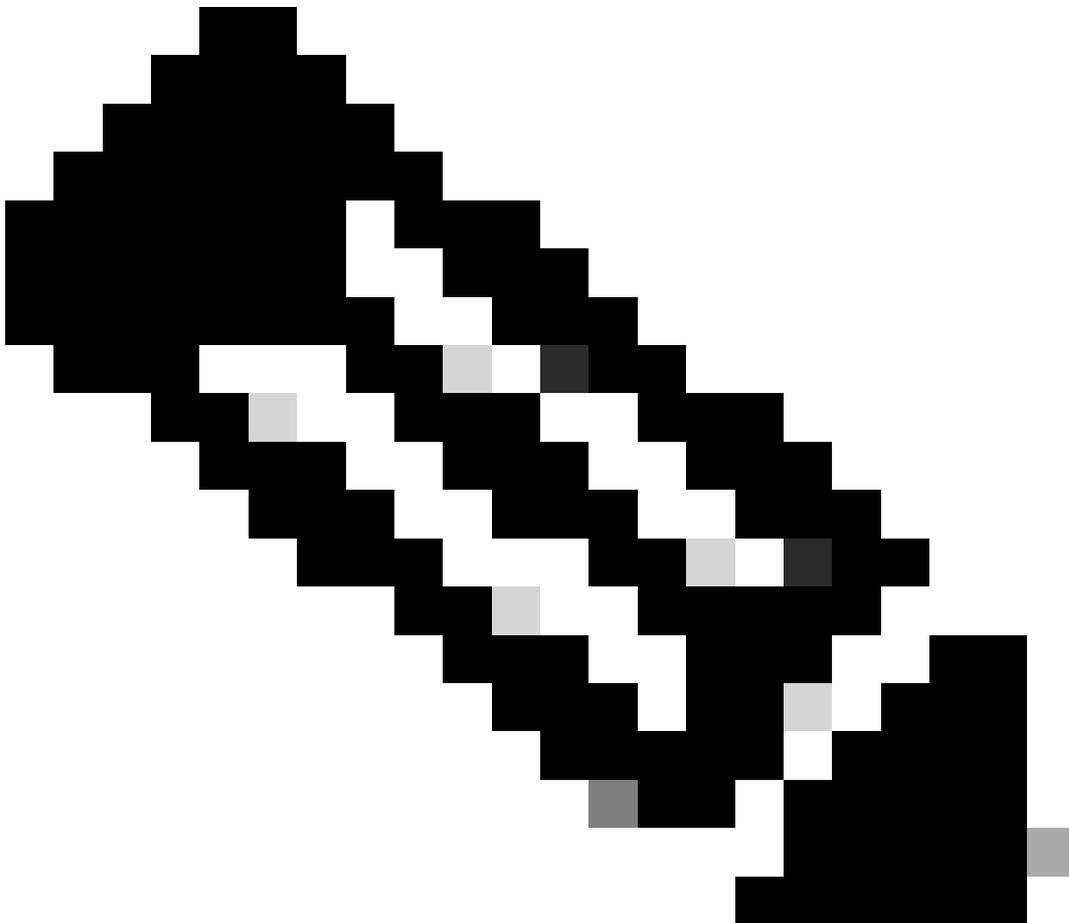


Gateway type

Initiate the connection



قواع تادادع | عقوم ىل عقوم نم VPN ةكبش - Sophos



XFRM مساب Sophos XG ةي امح رادج ل ةي ضار ت فا ق فن ةه جا و عاش ناب ةي راي ت خالا ق فن لا ةه جا و موقت :تظالم

ن.يوكتل Encryption تحت

- **Profile:** موطخلال ىلع هئاشناب موقت يذلا فيرعتال فلم **Configure IPsec Profile**
- **Authentication type:** اقبس م كرتشملا حاتفملا
- **Preshared key:** موطخلال ىلع هنيوكتب موقت يذلا حاتفملا [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key:** Preshared key

## Encryption

Profile	Authentication type
CSA	Preshared key
	Preshared key
	Repeat preshared key

ريفشتل - عقوم ىل عقوم نم (VPN) ةيره اظلال ةصاخلا ةكبشلا - Sophos

تحت Gateway Settings تاراخي Local Gateway Remote Gateway، عجرمك لودجال اذه مدختسا.

ةيولحملا ةباوبلا	ةديعبلا ةباوبلا
عامتساللة ةهجاو كيذل تنرتنلال-WAN ةكبش ةهجاو	ةباوبلا ناوع وطخلال بجومب هؤاشنإ مت يذلا ماعلا IP <a href="#">Tunnel Data</a>
يولحملا فرعمال عون ينورتكللال ديربلا	ديعبلا فرعمال عون

	IP ناوع
ي لجم فرعم تحت هؤاشنإ مت يذلا ينورتكلإلا ديربلا ، ؤوطخال <a href="#">Tunnel Data</a>	ديعب فرعم ، ؤوطخال بجومب هؤاشنإ مت يذلا ماعلا IP <a href="#">Tunnel Data</a>
ةي لجملا ؤي عرفلا ؤكبشلا أ	ةديعبلا ؤي عرفلا ؤكبشلا أ

## Gateway settings

Local gateway	Remote gateway
Listening interface PortB - 192.168.0.33	Gateway address 18.156.145.74
Local ID type Email	Remote ID type IP address
Local ID csasophos@ -sse.cisco.com	Remote ID 18.156.145.74
Local subnet Any	Remote subnet Any
Add new item	Add new item

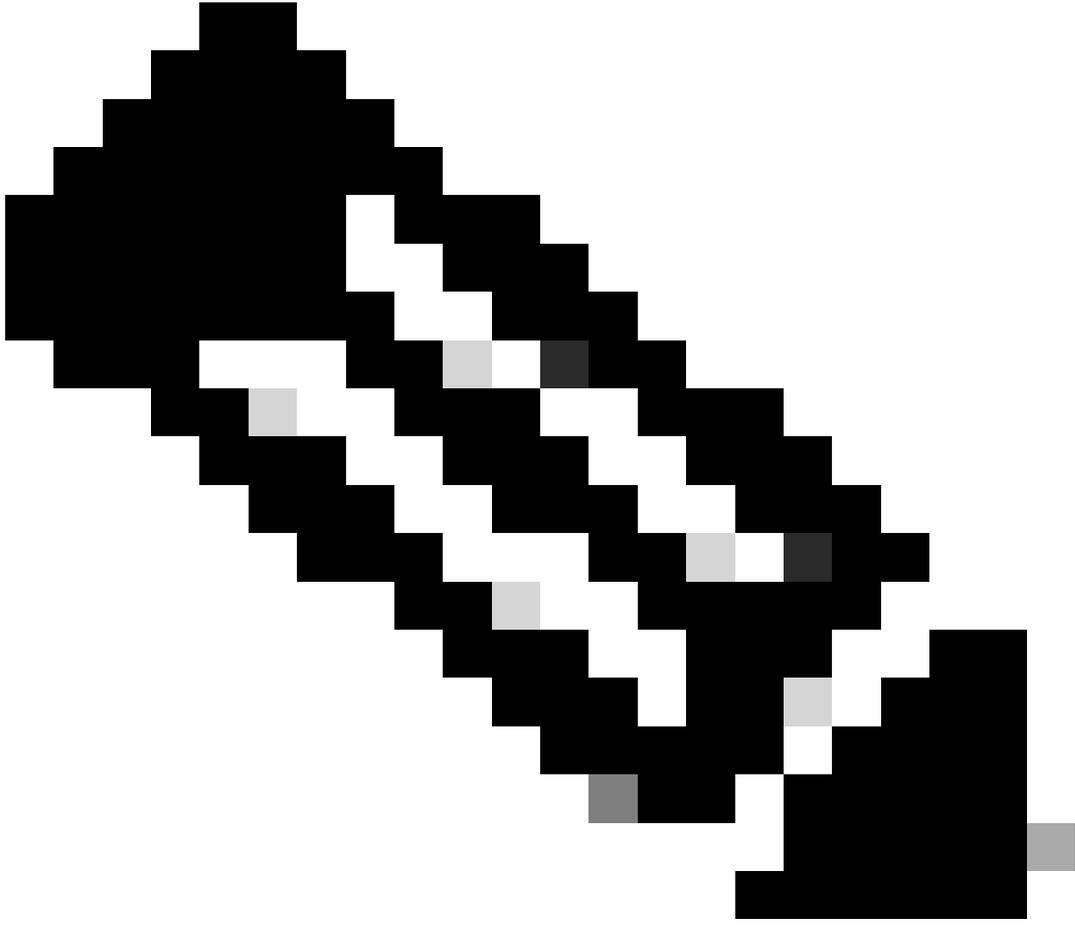
ةباوبلا - عقوم يلا عقوم نم (VPN) ؤيرهاظلا ؤصاخلا ؤكبشلا تاداع | Sophos

هؤاشنإ مت قفنلا نأ ىرت نأ كنكمي **Save**، رقنا كلذ دعب

## IPsec connections

Show additional properties						Add	Delete	Wizard
Name	Group name	Profile	Connection type	Status	Connection	Manage		
SecureAccessS	-	CSA	Tunnel interface	Active				

IPsec - عقوم يلا عقوم نم VPN تالاصت | Sophos



إذا، لإحلال Connection نم ققحتللا كنكمي، ةرئخألا ةروصللا ىلع عئحص لكشب قفنللا نئكمت نم ققحتللل: ةظحالم  
لصتم رءق قفنللا ارضأ نكئ مل إذا لصتم قفنللا نإف، ارضأ ناك.

---

Current Activities > IPsec Connections ىلإ لوقتنا، قفنلا ءاشنإ مت إذا امم ققحتللل

MONITOR & ANALYZE

# Control center

Current activities

Reports

Zero-day protection

Diagnostics

Sophos - IPsec - ليلحتالو ةبقارملا - Sophos

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 - IPsec - ليلحتالو ةبقارملا - Sophos

دعبو لببق IPsec - ليلحتالو ةبقارملا - Sophos. **Configure Tunnel Interface Gateway.** ةوطخلال لصاون نأ نكمي، كلذ دعبو

قفنلال ةهجاو نيوكت

مادختساب ةيره اظلالا قفنلال ةهجاو ريرحتل WAN اهصحفو VPN ةكبش ىلع اهن نيوكت مت يتل Network ةهجاو اولى لىلقتنا ماسالا xfrm.

- ةهجاو ال xfrm ىلع رقتنا.



قفلنلا ةهجاو - ةكبشال - Sophos

- مادختسا كنكمي ، لاثلما ليلبس ىلع ، كتكبش يه هيچوتلل لباقلا ريهغ IP مادختساب ةهجاوالا نيوكتب مق 169.254.0.1/30 مدختسن هلثمن يذلا لاثملا يهو ، ةداع هيچوتلل ةلباق ريهغ ةحاسم يه IP وهو 169.254.x.x/30

#### General settings

Name *	<input type="text" value="xfrm1"/>
Hardware	xfrm1
IPsec connection	SecureAccess
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)"/>

نيوكتلا - قفلنلا ةهجاو - ةكبشال - Sophos

#### تاپاوبال نيوكت

ةرهاطلا ةهجاوالا ةرابع نيوكتل (xfrm)

- Routing > Gateways ىلى لقتنا
- Add رقتنا

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

تأبواب الـ - هجوت الـ - Sophos

تحت Gateway host الـ وكالت:

- **Name:** VPN كةبشل اهؤاشن مت يت الـ هره اطلال هه ااولا الـ ريشي مس
- **Gateway IP:** انمق يذلا 169.254.0.1/30 كةبشلال تحت (IP) تنرتن الـ لوكوتورب وه اذه، 169.254.0.2 انتالاح في، ةوطخل تحت لع الفاب هني عتت ب، Configure Tunnel Interface
- **Interface:** VPN كةبشلال هره اطلال هه ااولا
- **Zone:** الـ ب (يضارت فالال)

Gateway host

Name \*

Gateway IP

Interface

Zone

ةبواب الـ فيضم - تأبواب الـ - هجوت الـ - Sophos

- ققحت الـ ليطعت **Health check** تحت
- **Save** رقنا

# Health check

Health check



ةحصلا نم ققحتلا - تاباوبلا - هيوتلا - Sophos

نيوتلا ظفح دعب ةباوبلا ةلاحة طحالم كنكمي

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	<span style="color: green;">●</span>	
<input type="checkbox"/>	<u>DHCP_PortB_GW</u>	192.168.0.1	WAN	On	<span style="color: red;">●</span>	

ةلاحة - تاباوبلا - هيوتلا - Sophos

SD-WAN راسم نيوتلا

نم آلا لوصوللا ىلا رورملا ةكره هيوت ةداعاب كل حمسي يذلا راسملا عاشنا كمزلي، نيوتلا ةلمع عاهنا

ىلا لقتنا **Routing > SD-WAN routes**.

- **Add** قوف رقنا



- Primary and Backup gateways: راڤخال ددح
- **Primary gateway:** ةوطخلال نمض ةنوكملا ةبوابلا ددحت [Configure the Gateways](#)
- Save قوف رقتنا

### 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

يطايتحال افسنل او ةسسائل تابوابلا - رورملا ةكرح ددحم - SD-WAN تاراسم - SOPHOS

ءوطخلال ةبوابلا كنكمي Sophos XG ةيامح رادج ىلع نيوكتلل اهان دعب **Configure Private App.**

صاخال قيبطتلل نيوكتل

لءؤسملل لءدم ىلا لءوخلال لءجستب مق ، صاخال قيبطتلل ىلا لءوصلال نيوكتلل

- Resources > Private Resources ىلا لقتنا

- Overview
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

# 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

ةصاخلا دراوملا - نمآلا لوصولا

- Add + قوف رقنا

Private Resources
Private Resource Groups

**Private Resources**

Private Resource Group

Connection Method

4 Private Resources

+ Add

Last 24 Hours

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

2 ةصاخلا دراوملا - نمآلا لوصولا

- **Private Resource Name** نيوكت General تحت

## General

### Private Resource Name

SplunkSophos

### Description (optional)

ماع - ةصاخلا دراوملا - نمآلا لوصولا

نيوكت ال **Communication with Secure Access Cloud** تحت

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR):** ده لوصولا ديرت يذلا دروملا دح





**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

Secure Access Cloud 2 مداخلتساب تالاصتالال - ةصاخلا دراوملا - Secure Access

ةجيتنللا يه هذه نوكت ، نيوكتلا لامتكادع ب

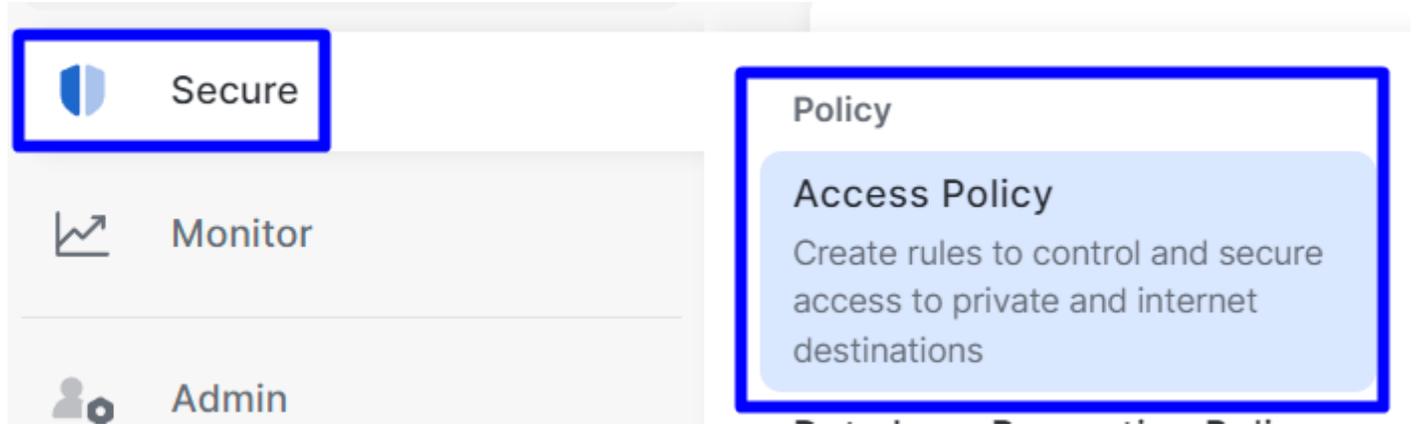
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none"><li>VPN</li><li>Browser-based ZTNA</li><li>Client-based ZTNA</li></ul>	1	2	16

ةصاخلا دراوملا نيوكت - نملآلا لوصولا

لوطخلال ةعباتم كنكمي نآلا **Configure the Access Policy**.

لوصولا جهن نيوكت

لوصولا جهن نيوكتل **Secure > Access Policy**.



لوصولا ةسايس - نآالا لوصولا

- **Add Rule > Private Access** رقنا

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

صاخال لوصولوا - لوصولوا ةسايس - نمالا لوصولوا

ةقداصم لل ةددعتم قرط ربع لوصولوا ريفوتل ةيلاتال تاراخيال نيوكتب مق:

- 1. Specify Access
  - Action: خامس
    - **Rule name:** كب ةصاخال لوصولوا ةدعاقول مسا ديحت
    - **From:** لال لوصولوا قح مهل حنمت نيذال نومدختسمال
    - **To:** هيلال لوصولوا ب خامسالا تدرأ يذال قيبتال
    - **Endpoint Requirements:** (يضا رتفالال)
- **Next** رقنا

## 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**

لوصول دي دحت - لوصول اة سايس - ن مآل لوصول

وإن Intrusion Prevention (IPS) نيكتمت بمقت مل. ةلأجل هذه يف نكل، ةلأجل بسح Configure Security 2. ةوطخلل: ةظالم Tenant Control Profile.

- كدل و، Save رقنا:

	# ⓘ	Rule name	Access	Action	Sources	Destinations	Security	Status
☰	6	SplunkSophos	Private	✔ Allow	Any	SplunkSophos	-	✔ ...

لوصول ةسايس نيوكت مت - نأل لوصول

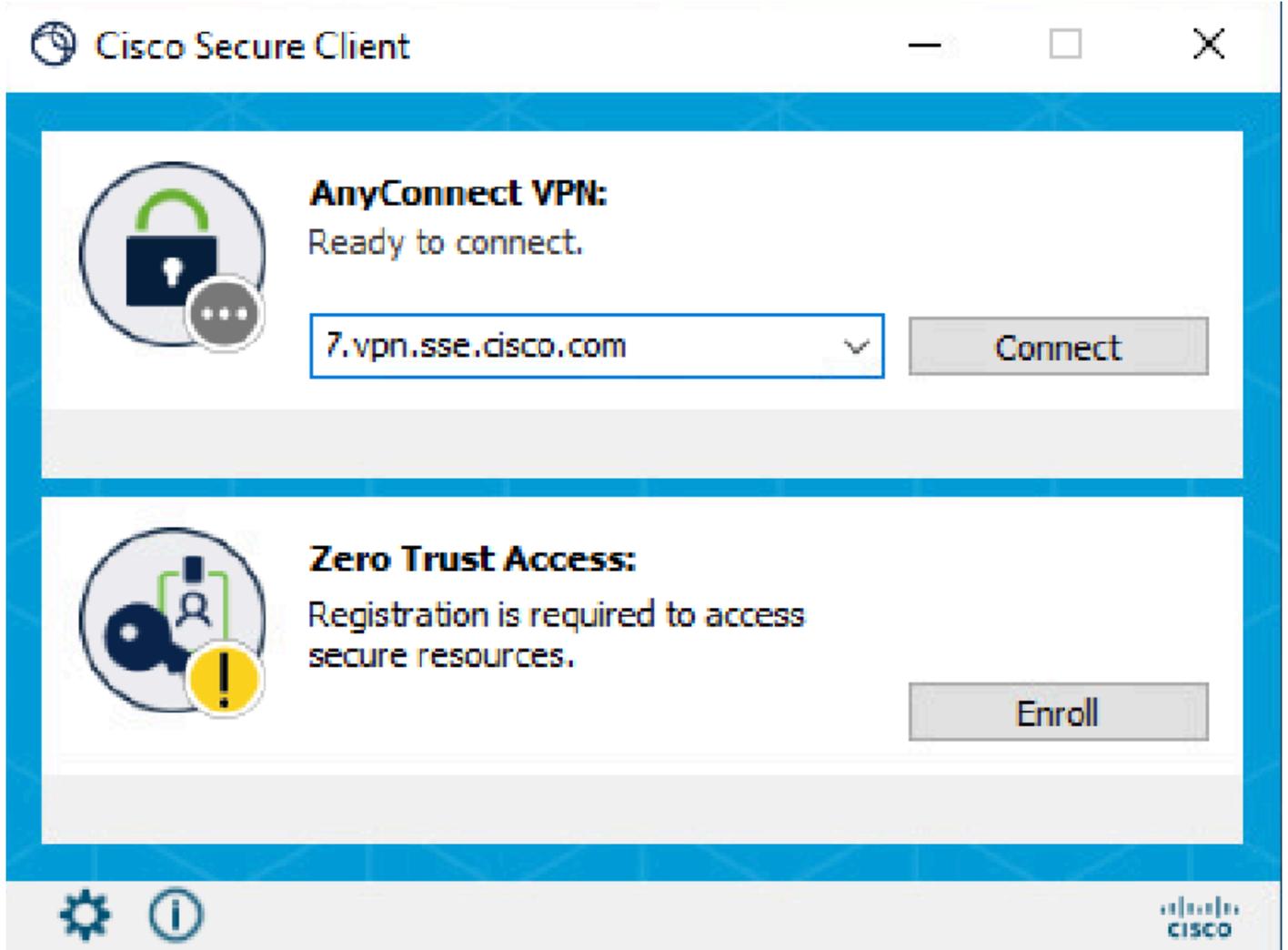
Verify ةوطخلل ةعباتم كنكمي، كلذ دعب

ةحصلال نم ققحتال

-[جماربالا ليزنت](#) نم هليزنت كنكمي يذال Cisco Secure Client ليمع تيبتبتم قق دق نوكت نا بجي ،لوصولا نم ققحتلال [Cisco Secure Client](#).

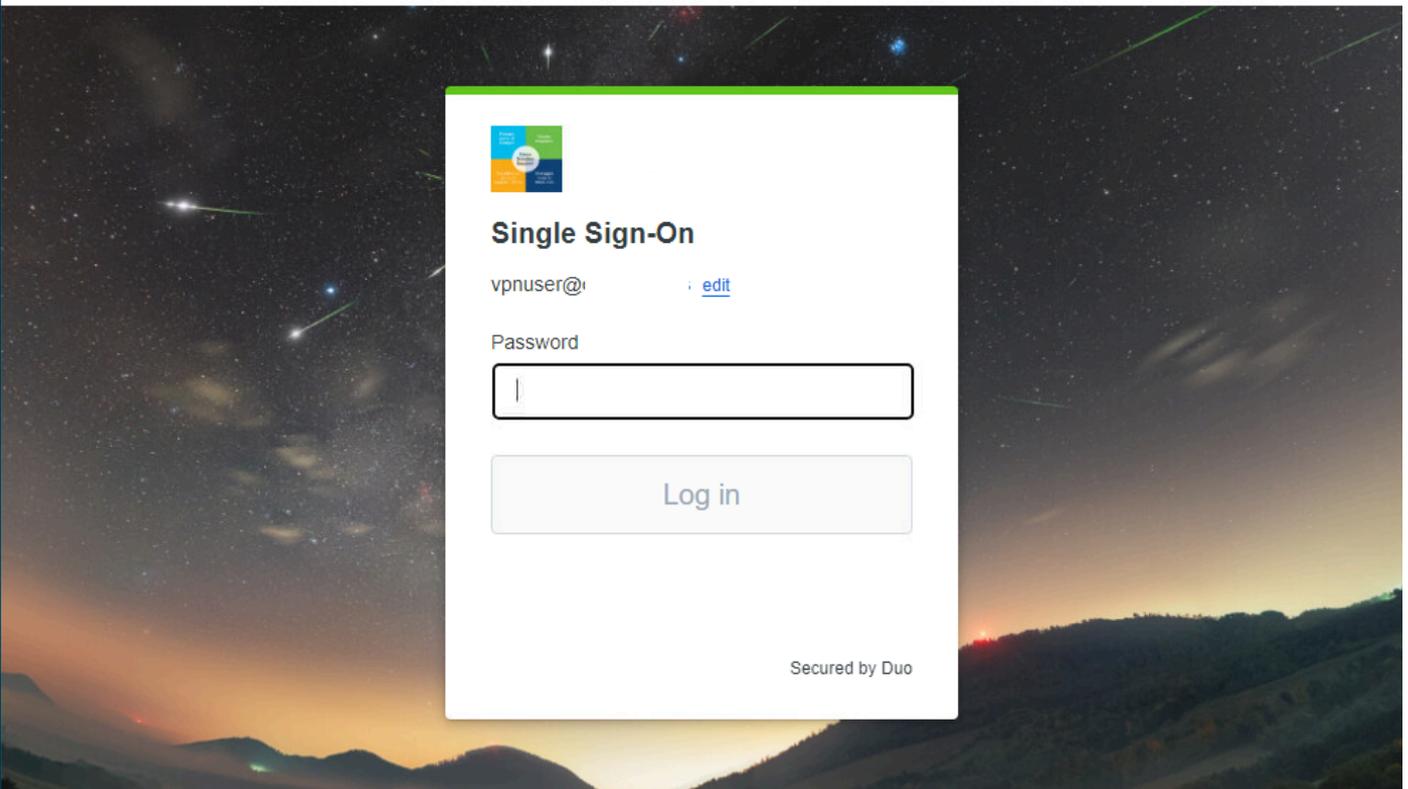
ار-VPN

ت Cisco Secure Client Agent-VPN لالخنم لوخذلا ليجست



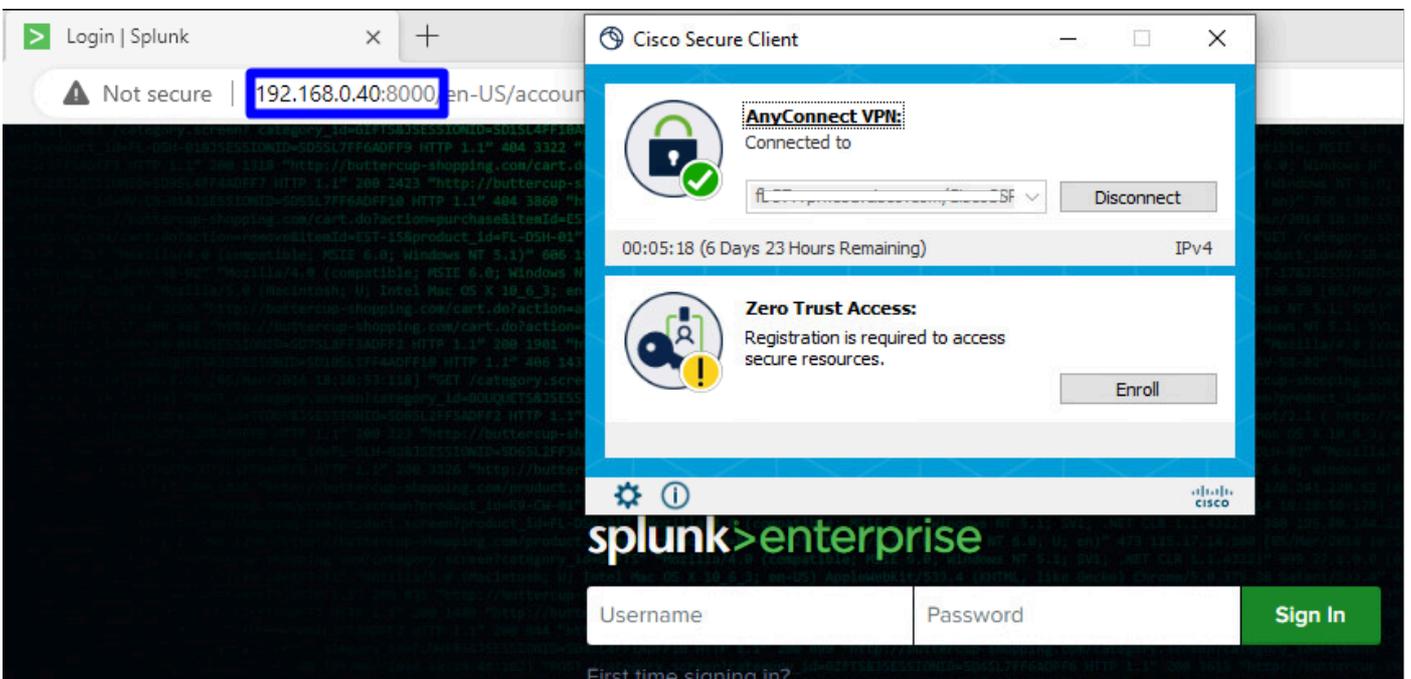
Secure Client - VPN

- SSO رفوم لالخنم ةقداصلال



VPN - SSO - نمآلا لوصول

- دروملا لوصول كنكمي، كتقداصم مت نأ دعب



قداصم - VPN - نمآلا لوصول

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@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	...

### Event Details

Action: Allowed

Time: Nov 23, 2023 1:09 AM

Rule Name: RDP (373192)

Source: vpn user (vpnuser@ciscosspt.es)

Source IP: 192.168.50.130

Destination IP: 192.168.0.40

Source Port: 50226

Destination Port: 8000

Categories: Uncategorized, Dispute Categorization

طاشنل ن ع ثحبل - نمآلا لوصول

RA-VPN لال خ نم ق دصي نأ حمسي ناك لمعتسملا ىري نأ عي طتسي تنأ

يساسال-ليمال ZTNA

Cisco - ZTNA نم نمأ ليمع ليك و لال خ نم لوخدلا ليجست

The screenshot shows a Windows Command Prompt window with the following text:

```

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

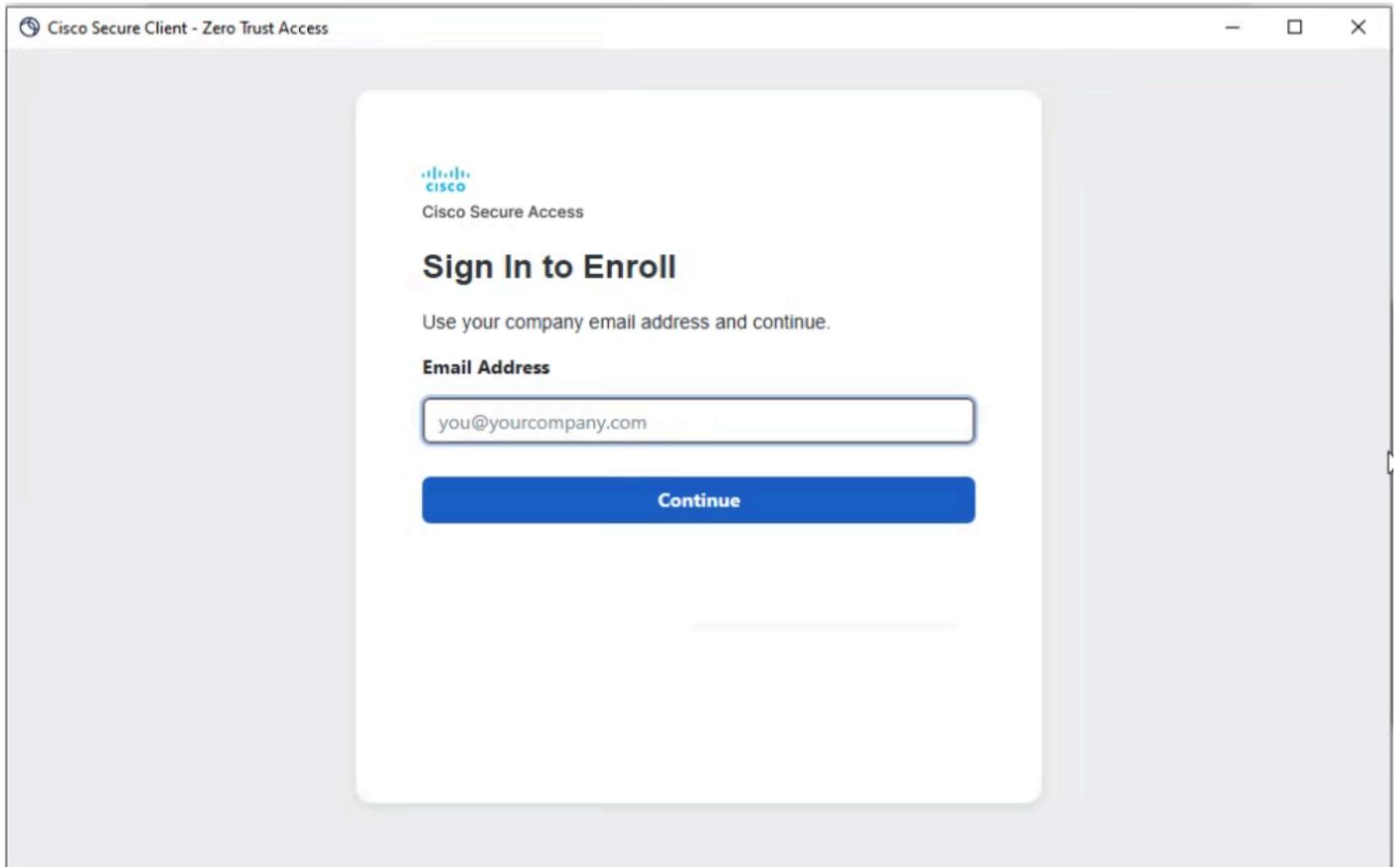
C:\Users\falas>
  
```

Overlaid on the bottom right is the Cisco Secure Client window, which displays:

- AnyConnect VPN:** Ready to connect. Includes a dropdown menu and a "Connect" button.
- Zero Trust Access:** Registration is required to access secure resources. Includes an "Enroll" button.

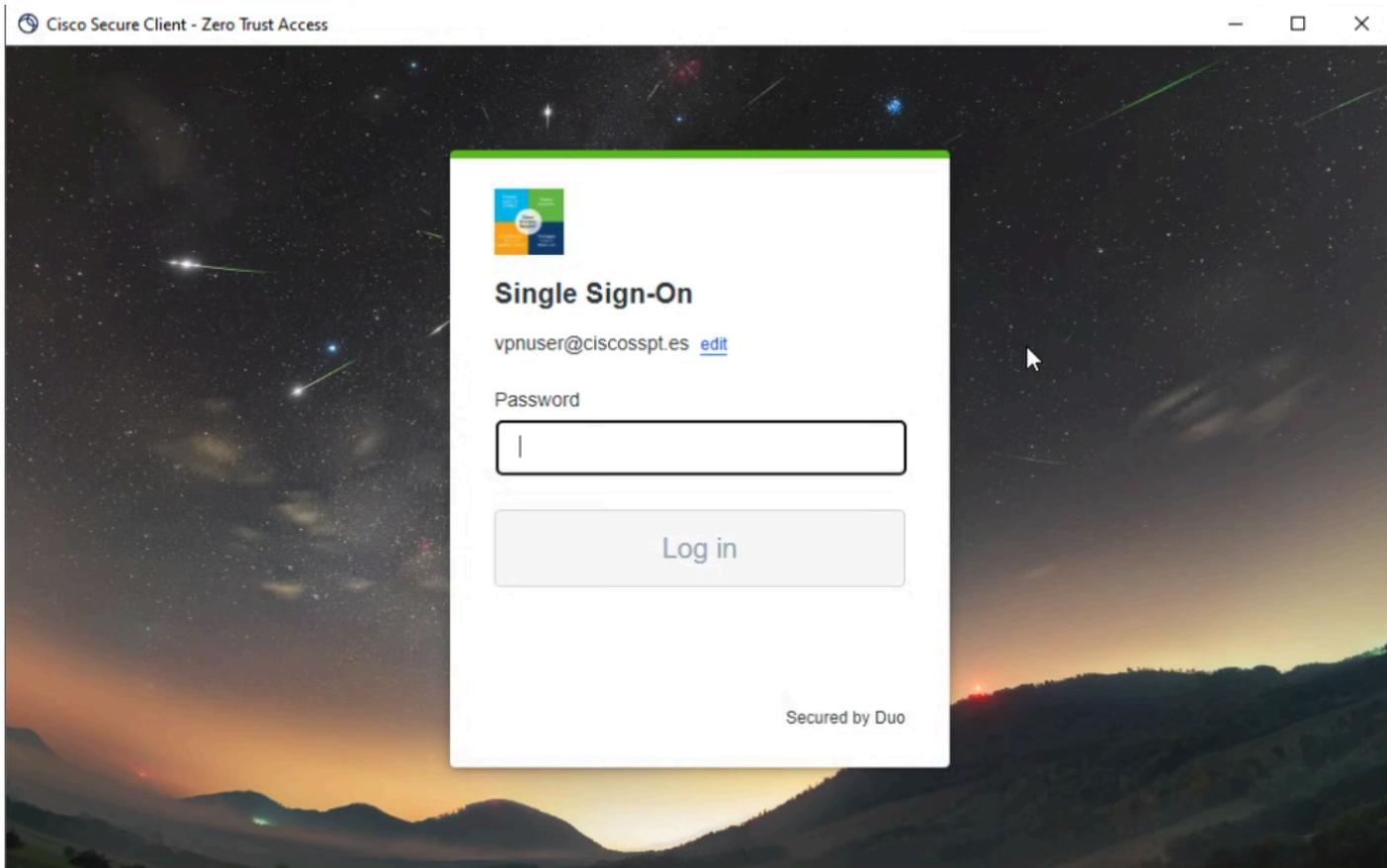
Secure Client - ZTNA

- ك صاخلا مدختسملا مساب ليجستلا



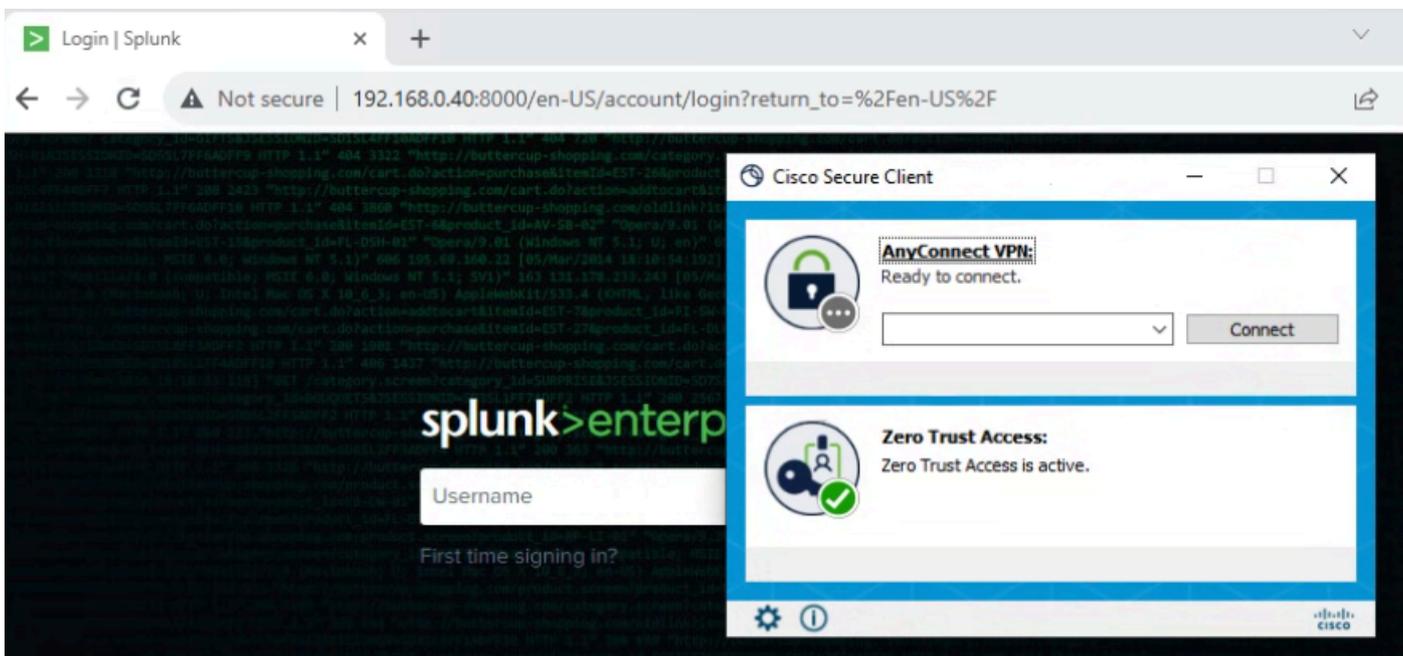
لجستال - ZTNA - نمآال ليمعلا

- SSO رفوم يف ةقداصملا



Secure Client - ZTNA - ل وخذ ليجست - SSO

- دروملا لى ل وصولا كنكمي ،كتقد اصم مت نأ دعب :



لجسم - ZTNA - نم آلا ل وصولا

Monitor > Activity Search لى ل لقتنا



**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

صاڅ دروم - نم آلا لوصولا

- جهنلا يلع رقننا

SplunkSophos

Client-based ZTNA

Browser-based ZTNA

VPN

1

SplunkSophos - صاڅ دروم - نم آلا لوصولا

- لفسأل ريرمت

# SplunkSophos

Client-based ZTNA

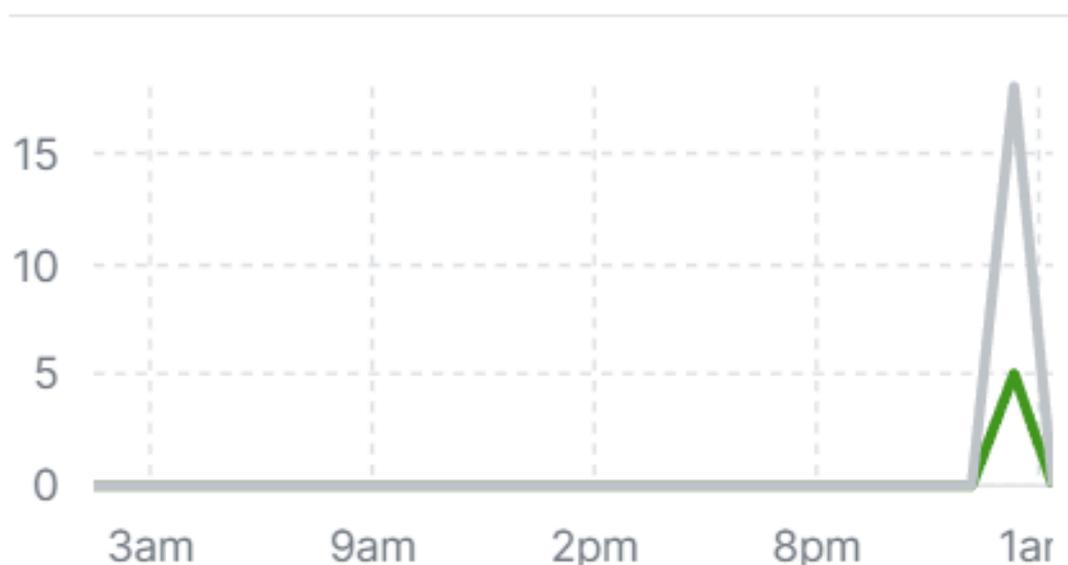
Browser-based ZTNA



VPN

Total Requests

**23** ↗ 44% from previous 24 hours



## TOTAL REQUESTS BY STATUS

### Status

✓	Success	5
⊘	Blocked	18



ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إامئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل