

Sophos XGファイアウォールを使用したセキュアアクセスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[セキュアアクセスでのトンネルの設定](#)

[トンネルデータ](#)

[Sophosでのトンネルの設定](#)

[IPSecプロファイルの設定](#)

[サイト間VPNの設定](#)

[トンネルインターフェイスの設定](#)

[ゲートウェイの設定](#)

[SD-WANルートの設定](#)

[プライベートアプリの構成](#)

[アクセスポリシーの設定](#)

[確認](#)

[RA-VPN \(オプション \)](#)

[クライアントベースのZTNA](#)

[ブラウザベースのZTNA](#)

[関連情報](#)

はじめに

このドキュメントでは、Sophos XGファイアウォールでセキュアアクセスを設定する方法について説明します。

前提条件

- [ユーザプロビジョニングの設定](#)
- [ZTNA SSO認証設定](#)
- [リモートアクセスVPNセキュアアクセスの設定](#)

要件

次の項目に関する知識があることが推奨されます。

- Sophos XGファイアウォール

- セキュアなアクセス
- Cisco Secure Client - VPN (トンネルモード)
- Cisco Secureクライアント – ZTNA
- クライアントレスZTNA

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Sophos XGファイアウォール
- セキュアなアクセス
- Cisco Secure Client - VPN (トンネルモード)
- Cisco Secureクライアント – ZTNA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明



CISCO

Secure

Access

SOPHOS

セキュアなアクセス – Sophos

シスコは、プライベートアプリケーション（オンプレミスとクラウドベースの両方）へのアクセスの保護とプロビジョニングを確実に行えるように、セキュアなアクセスを設計しました。また、ネットワークからインターネットへの接続も保護します。これは、複数のセキュリティ方式とレイヤの実装によって実現されます。すべての目的は、クラウド経由でアクセスする情報を保持

することです。

設定

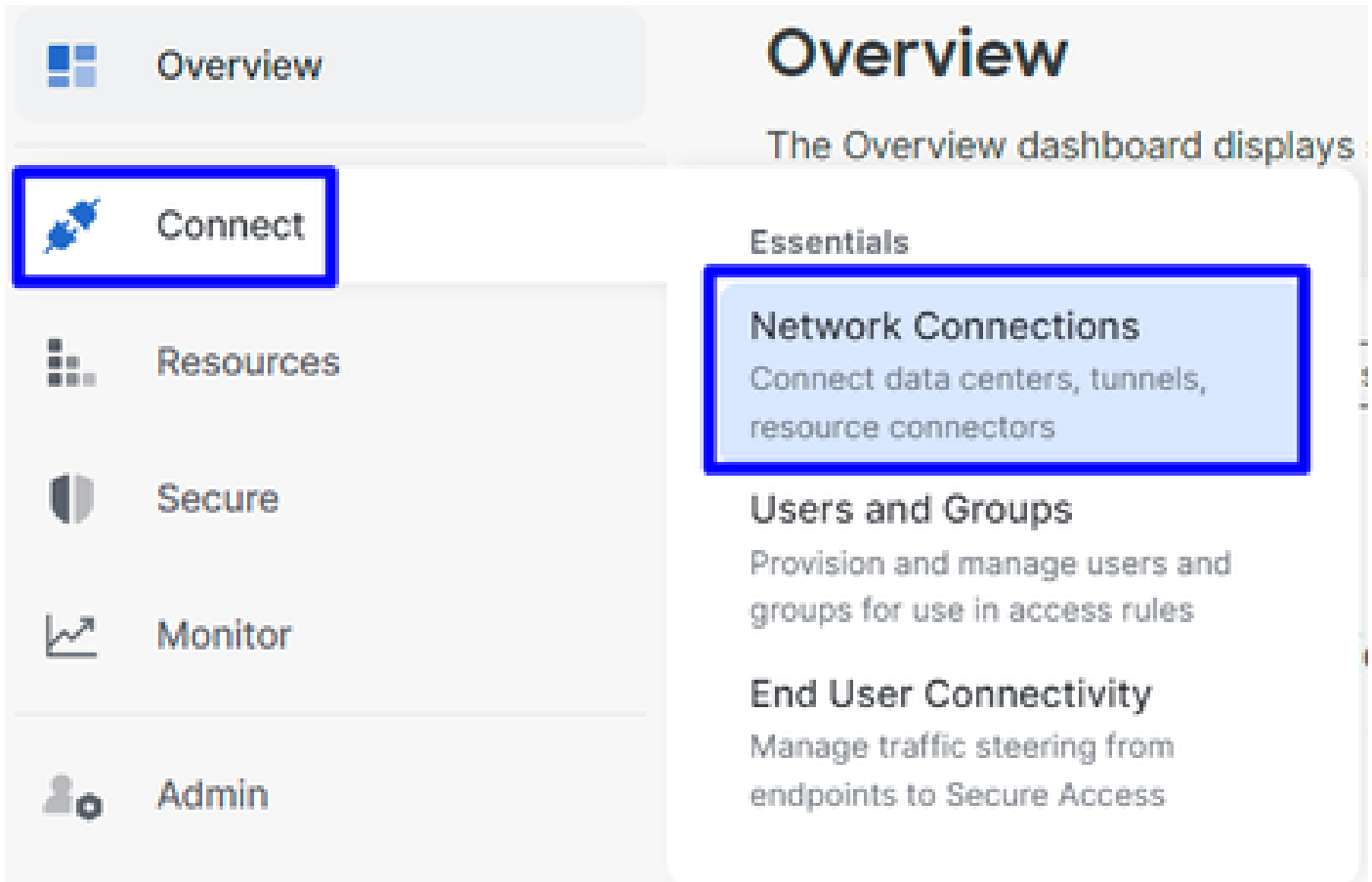
セキュアアクセスでのトンネルの設定

[Secure Access](#)の管理パネルに移動します。



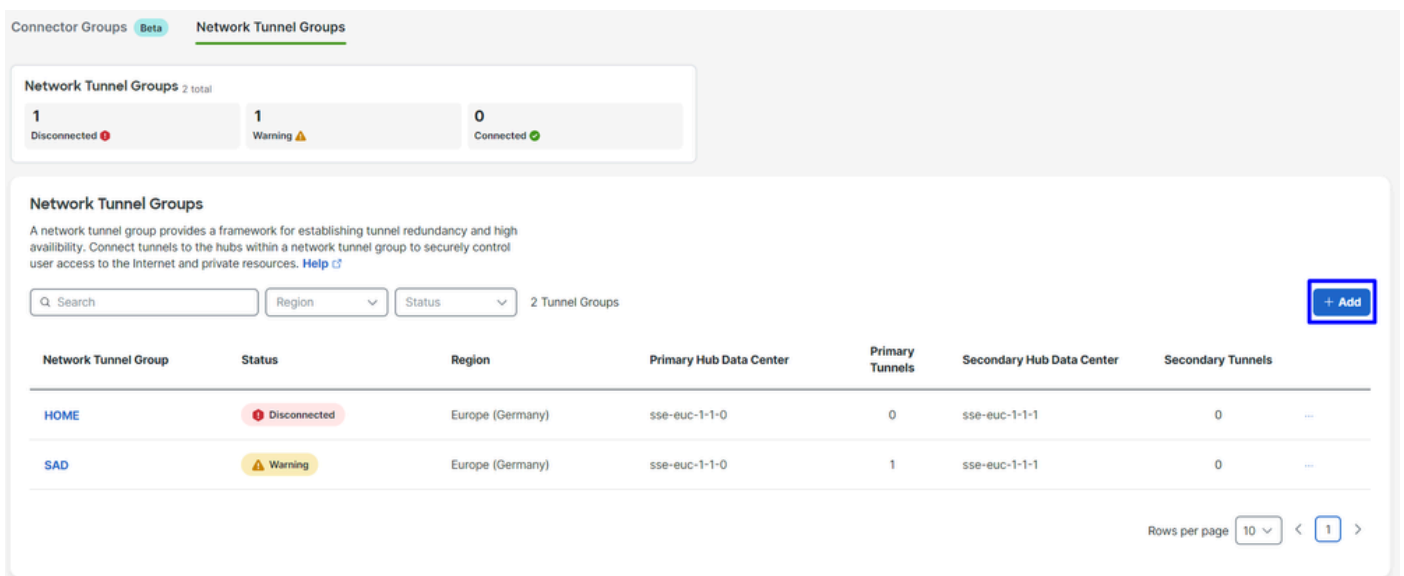
セキュアアクセス – メインページ

- クリック [Connect > Network Connections](#).



セキュアアクセス – ネットワーク接続

- Network Tunnel Groupsの下で、+ Addをクリックします。



セキュアアクセス – ネットワークトンネルグループ

- Tunnel Group Name、Region、およびDevice Typeを設定します。
- をクリックします。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

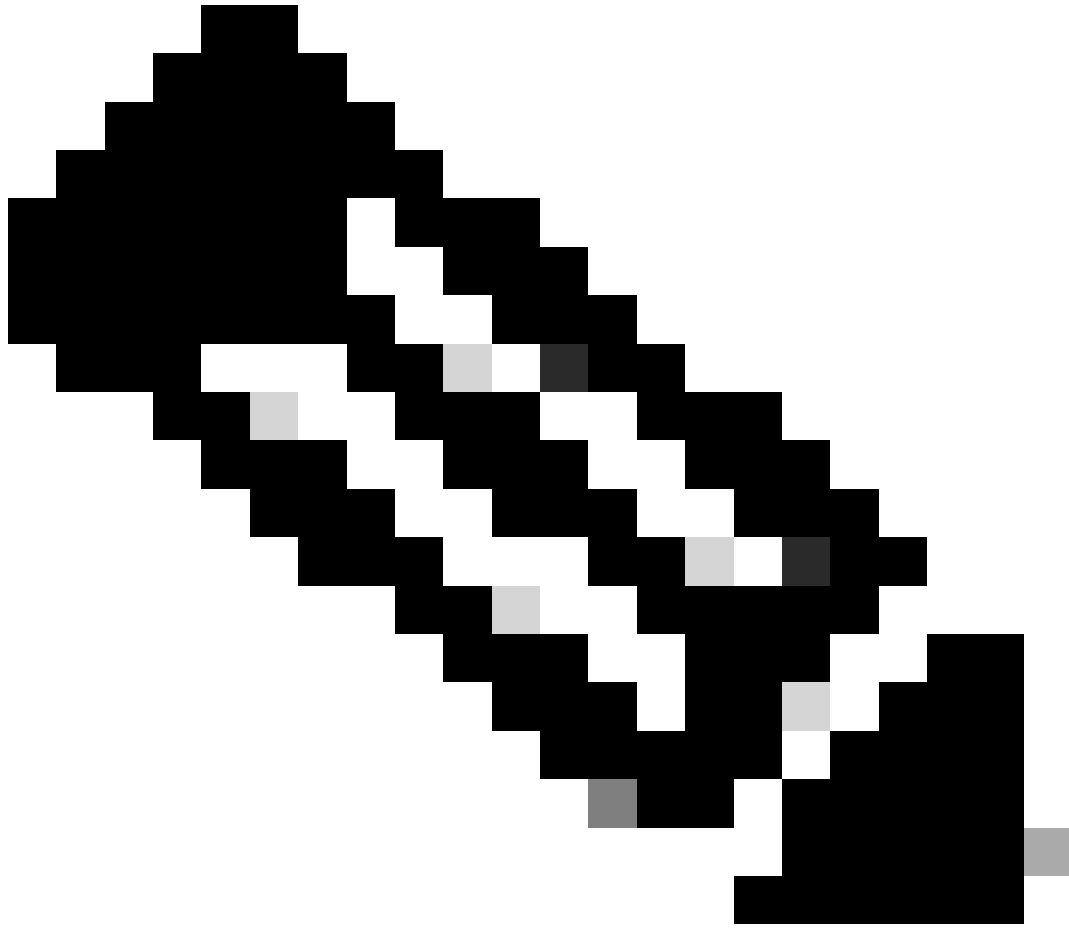
 ▼

Device Type

 ▼

[Cancel](#)

[Next](#)



注：ファイアウォールの場所に最も近い地域を選択します。

Tunnel ID Format

-
- およびPassphraseを設定します。
 - をクリックします。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

セキュアアクセス – トンネルグループ – トンネルIDおよびパスフレーズ

- ネットワークで設定したIPアドレス範囲またはホストを設定し、トラフィックをセキュアアクセス経由で通過させる。
- をクリックします。 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

セキュアアクセス – トンネルグループ – ルーティングオプション

トンネルに関するSave する情報をクリックして表示した後、次の手順Configure the tunnel on Sophosでその情報を保存してください。

トンネルデータ

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](#)

[セキュアアクセス – トンネルグループ – 設定の再開](#)

[Sophosでのトンネルの設定](#)

[IPSecプロファイルの設定](#)

IPSecプロファイルを設定するには、Sophos XGファイアウォールに移動します。

次のような結果が得られます。

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

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

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

Performance

Interfaces

Services

VPN

0/0 RED

0 Connected remote users

12% CPU

61B/s Bandwidth

0% Decryption capacity

0/0 Wireless APs

0 Live users

61% Memory

0 Sessions

0 Decrypt sessions

High availability: Not configured

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

Traffic insight

Web activity: 0 max | 0 avg

Cloud applications: 0 Apps, 0 B In, 0 B Out

Allowed app categories: N/A

Network attacks: N/A

Allowed web categories: N/A

Blocked app categories: N/A

User & device insights

Security Heartbeat®: 0 At risk

Synchronized Application Control™: 0 Apps

Zero-day protection: 0 Recent, 0 Incidents, 0 Scanned

ATP: 0 Sources blocked

UTQ: 0 Accounts at risk

SSL/TLS connections: 0% Of traffic, 0% Decrypted, 0 Failed

Active firewall rules

WAF	User	Network	Scanned
4	2	0	0

Unused: 4, Disabled: 2, Changed: 0, New: 0

Reports

- 0 Risky apps seen (Yesterday)
- 0 Objectionable websites seen (Yesterday)
- 0 bytes Used by top 10 web users (Yesterday)
- 0 Intrusion attacks (Yesterday)

Messages

- Alert** (7:56): Create a secure storage master key to improve protect...
- Warning** (7:56): IPS protection is turned off. To enforce the intrusion pr...
- Alert** (11:47): New system firmware is available for download. [Click h...](#)

Click on widgets to open details

Sophos – 管理パネル

- 移動先 Profiles
- **IPsec Profiles**
- をクリックし、その後でAdd

IPsec profiles

Device access

Add

Delete

algorithm
Manage

Phase 2

設General Settings 定の下 :

- **Name:**Cisco Secure Access Policyへの参照名
- **Key Exchange:**IKEv2
- **Authentication Mode:**Main Mode
- **Key Negotiation Tries:**0
- **Re-Key connection** : オプションをオンにします。

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

設Phase 1 定の下 :

- **Key Life:**28800
- **DH group(key group):** 19と20を選択
- **Encryption:** AES256
- **Authentication:** SHA2 256
- Re-key margin:360 (デフォルト)
- **Randomize re-keying margin by:**50 (デフォルト)

Phase 1

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

Sophos - IPsecプロファイル - フェーズ1

設Phase 2 定の下 :

- PFS group (DH group): phase-Iと同じ
- **Key life:**3600
- **Encryption:** AES 256
- Authentication: SHA2 256

Phase 2

PFS group (DH group) Same as phase-1 <input checked="" type="checkbox"/>	Key life 3600 <input checked="" type="checkbox"/>
Seconds	
Encryption AES256 <input checked="" type="checkbox"/>	Authentication SHA2 256 <input checked="" type="checkbox"/>
+ You can add up to 3 different algorithm combinations	

Sophos - IPsecプロファイル - フェーズ2

設 Dead Peer Detection 定の下 :

- **Dead Peer Detection** : オプションをオンにします。
- **Check peer after every:**10
- **Wait for response up to:**120 (デフォルト)
- **When peer unreachable** : 再初期化 (デフォルト)

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

Sophos - IPsecプロファイル - デッドピア検出

その後、**Save and proceed with the next step, Configure Site-to-site VPN**をクリックします。

サイト間VPNの設定

VPNの設定を開始するには、**Site-to-site VPN** をクリックし、**Add**をクリックします。

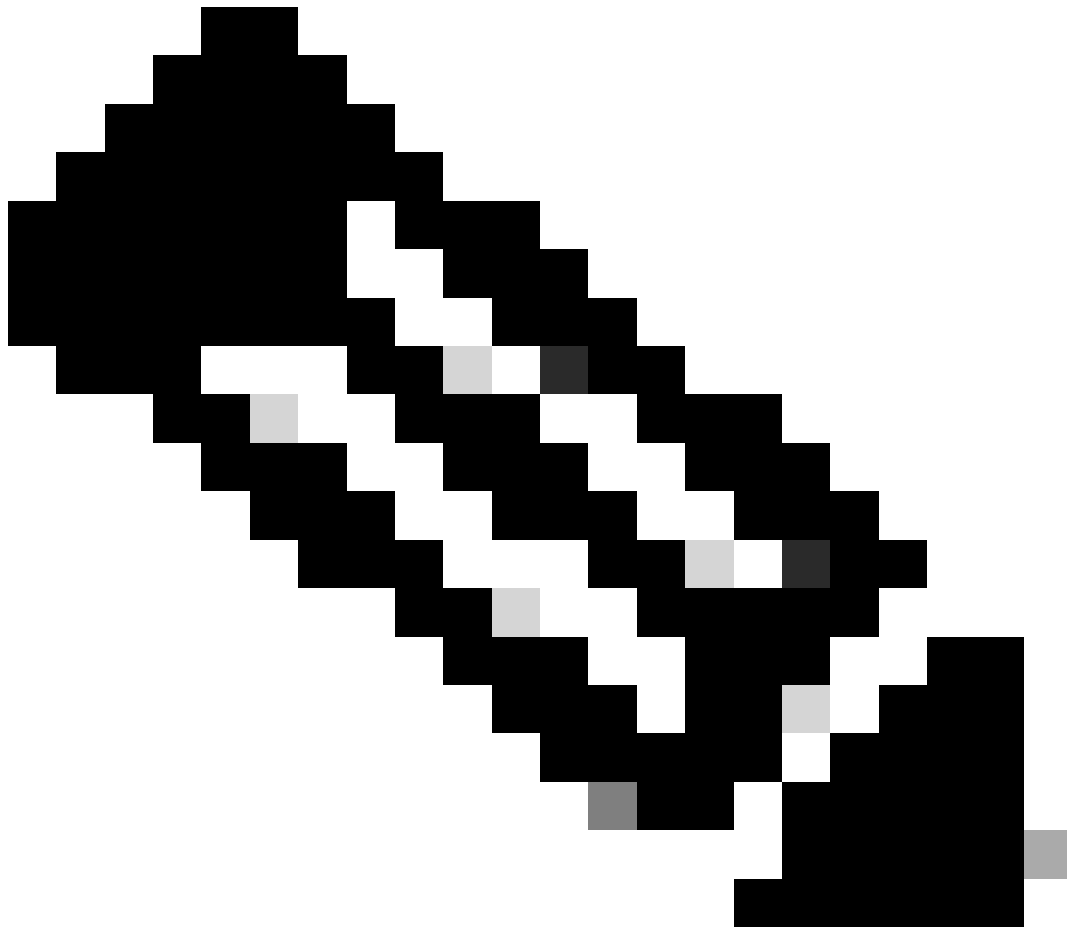
The screenshot shows the Sophos management console interface. On the left is a navigation menu with categories like 'PROTECT' and 'CONFIGURE'. Under 'CONFIGURE', 'Site-to-site VPN' is selected. The main area shows a table with columns for Name, Group name, Profile, Connection type, Status, and Manage. The table is currently empty, displaying 'No records found'. Above the table are buttons for 'Add', 'Delete', and 'Wizard'. A blue arrow points from the 'Add' button in the table header area to the 'Add' button in the top right corner of the main content area.

Sophos:Site-to-site VPN (サイト間VPN)

設General Settings 定の下 :

- **Name:**Cisco Secure Access IPsecポリシーへの参照名
- IP version: IPv4
- Connection type : トンネルインターフェイス
- Gateway type : 接続を開始します

- Active on save : オプションをオンにします。
-



注：サイト間VPNを設定した後、このオプションによってVPNが自動的に有Active on save 効になります。

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 - サイト間VPN - 全般設定

注：オプションのトンネルインターフェイスでは、Sophos XGファイアウォール用の仮想トンネルインターフェイスがXFRMという名前で作成されます。

設Encryption 定の下：

- **Profile** : ステップで作成したプロファイル、 **Configure IPsec Profile**
- **Authentication type**:事前共有鍵
- **Preshared key** : ステップで設定するキー、 [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key**: Preshared key

Encryption

Profile	Authentication type
CSA	Preshared key
	Preshared key
	Repeat preshared key

Sophos – サイト間VPN – 暗号化

設Gateway Settings 定Local GatewayおよびRemote Gatewayオプションで、次の表を参照用に使用します。

ローカル ゲートウェイ	リモートゲートウェイ
リスニングインターフェイス Wanインターネットインターフェイス	ゲートウェイ アドレス ステップの下で生成されたパブリックIPアドレス、 Tunnel Data
ローカルIDタイプ Email	リモートIDの種類

	IP アドレス
ローカルID 手順の下で生成された電子メール Tunnel Data	リモート ID ステップの下で生成されたパブリックIPアドレス、 Tunnel Data
ローカルサブネット [Any]	リモートサブネット [Any]

Gateway settings

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

Sophos - サイト間VPN - ゲートウェイ設定

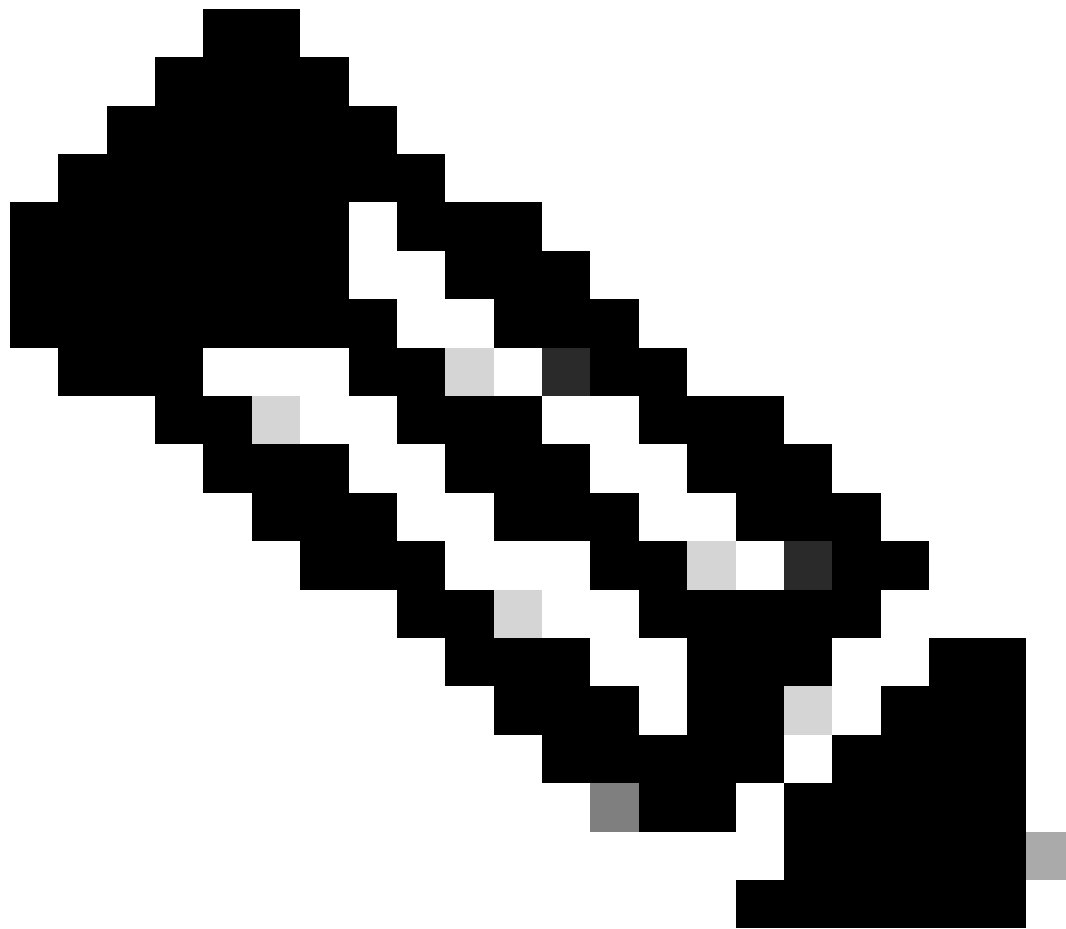
その後、Saveをクリックすると、トンネルが作成されたことが分かります。

IPsec connections

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

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

Sophos - サイト間VPN - IPsec接続



注：最後のイメージでトンネルが正しく有効化されているかどうかを確認するには、**Connection** ステータスを確認します。ステータスが緑の場合、トンネルは接続されています（緑ではない場合）。トンネルは接続されていません。

トンネルが確立されているかどうかを確認するには、**Current Activities > IPsec Connections**に移動します。

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

Sophos – 監視と分析 – 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	

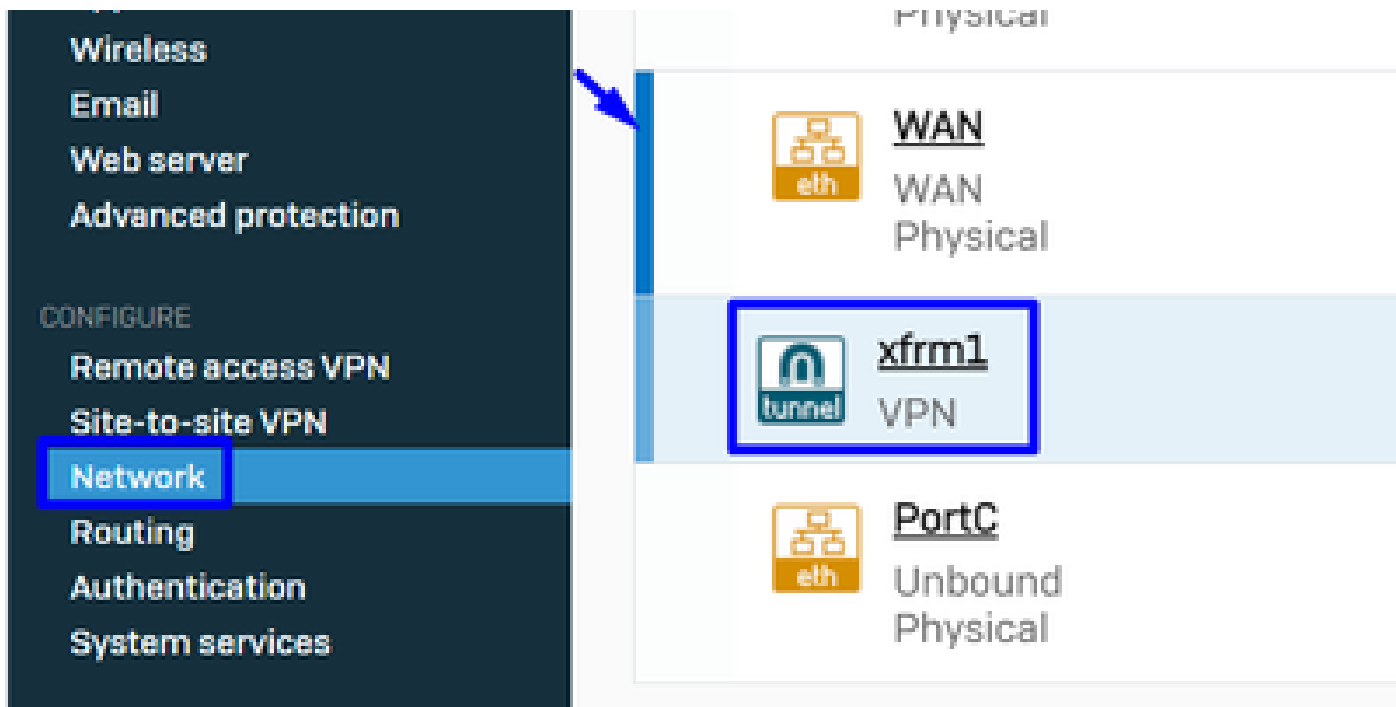
Sophos – 監視と分析 – 前後のIPSec

その後、手順 **Configure Tunnel Interface Gateway**に進みます。

トンネルインターフェイスの設定

Network に移動し、VPN上で設定されているWANインターフェイスを確認して、仮想トンネルインターフェイスを名前xfrmで編集します。

- インターフェイスxfrm をクリックします。



Sophos – ネットワーク – トンネルインターフェイス

- ネットワーク内でルーティング不可能なIPを使用してインターフェイスを設定します。たとえば、ルーティング不可能な空間のIPである169.254.x.x/30を使用できます。この例では、169.254.0.1/30を使用します

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 – ネットワーク – トンネルインターフェイス – 設定

ゲートウェイの設定

仮想インターフェイス(xfrm)のゲートウェイを設定するには、

- 移動先 Routing > Gateways
- クリック Add

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

IPv4 gateway

Add Delete

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

IPv6 gateway

Sophos – ルーティング – ゲートウェイ

設Gateway host 定の下：

- **Name:**VPN用に作成された仮想インターフェイスを参照する名前
- **Gateway IP :** この例では169.254.0.2が、このステップですでに割り当てたネットワーク169.254.0.1/30のIPです。
Configure Tunnel Interface
- **Interface:**VPN仮想インターフェイス
- **Zone :** なし (デフォルト)

Gateway host

Name *

Gateway IP

Interface

Zone

Sophos – ルーティング – ゲートウェイ – ゲートウェイホスト

- チェックを無Health check 効にする
- クリック Save

Health check

Health check



Sophos - ルーティング - ゲートウェイ - ヘルスチェック

設定を保存すると、ゲートウェイのステータスを確認できます。

IPv4 gateway

<input type="checkbox"/>	Name ▾	IP address ▾	Interface ▾	Health check ▾	Status ▾	Manage
<input type="checkbox"/>	<u>CSA_GW</u>	169.254.0.2	xfrm1	Off		
<input type="checkbox"/>	<u>DHCP_PortB_GW</u>	192.168.0.1	WAN	On		

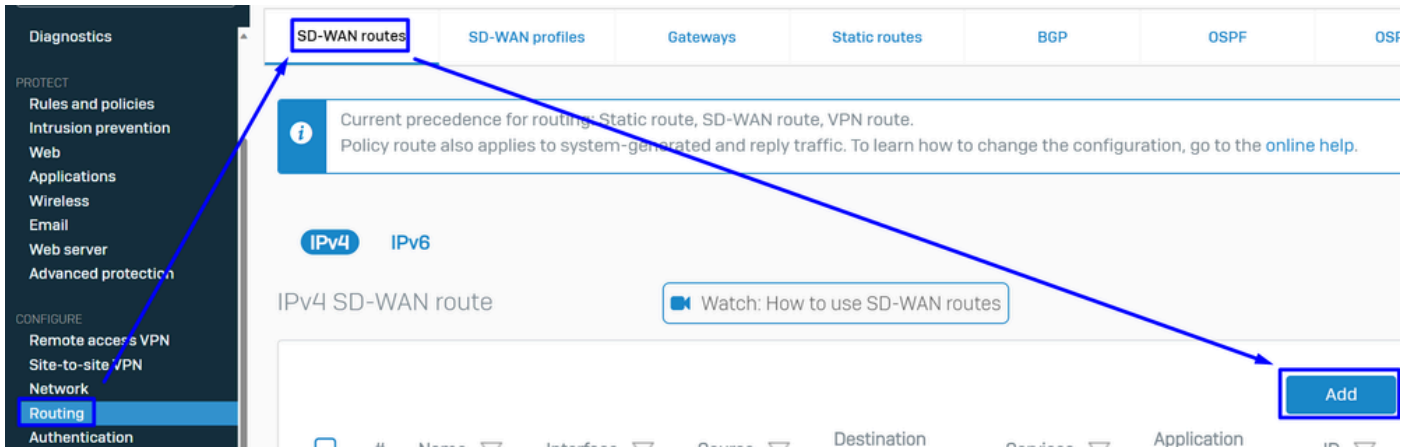
Sophos - ルーティング - ゲートウェイ - ステータス

SD-WANルートの設定

設定プロセスを完了するには、トラフィックをセキュアアクセスに転送できるルートを作成する必要があります。

移動先 **Routing > SD-WAN routes.**

- クリック **Add**



Sophos:SD-Wanルート

設Traffic Selector 定の下：

- Incoming interface：トラフィックを送信するインターフェイス、またはRA-VPN、ZTNA、またはクライアントレスZTNAからアクセスするユーザを選択します。
- DSCP marking：この例では何も行いません
- Source networks：トンネル経由でルーティングするアドレスを選択します
- Destination networks：任意の宛先、または宛先を指定できます。
- Services：サービスを指定できます。
- Application object：オブジェクトが構成されている場合のアプリケーション
- User or groups：特定のユーザグループを追加して、トラフィックをセキュアアクセスにルーティングする場合

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ルート - トラフィックセレクタ

ゲートウェイの設Link selection settings 定：

- Primary and Backup gateways : オプションをオンにします。
- **Primary gateway** : 手順で設定したゲートウェイを選択します。 [Configure the Gateways](#)
- クリック **Save**

Link selection settings

Select SD-WAN profile ⓘ Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

Sophos - SD-Wan ルート - トラフィックセレクター - プライマリおよびバックアップゲートウェイ

Sophos XGファイアウォールの設定を完了したら、次の手順に進みます。 **Configure Private App.**

プライベートアプリの構成

プライベートアプリケーションアクセスを設定するには、[管理ポータル](#)にログインします。

- 移動先 **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

セキュアアクセス – プライベートリソース

- クリック + 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
------------------	------------------------	-------------------	-------------	-------	----------------

セキュアアクセス – プライベートリソース2

- 「設定」の **Private Resource Name**

General

Private Resource Name

SplunkSophos

Description (optional)

セキュアアクセス - プライベートリソース - 全般

設定 **Communication with Secure Access Cloud** 定の下 :

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)** : アクセスするリソースを選択します



注：内部で到達可能なアドレスはステップ [Configure the Tunnel on Secure Access](#) で割り当てられていることに注意してください。

-
- **Protocol** : そのリソースにアクセスするために使用するプロトコルを選択します
 - **Port / Ranges** : アプリにアクセスするために有効にする必要があるポートを選択します

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

セキュアアクセス – プライベートリソース – セキュアアクセスクラウドを使用した通信

では **Endpoint Connection Methods**、セキュアアクセスを介してプライベートリソースにアクセスするために可能なすべての方法を設定し、環境で使用する方法を選択します。

- **Zero-trust connections:**ZTNAアクセスを有効にするには、このチェックボックスをオンにします。
 - **Client-based connection** : ボタンを有効にしてクライアントベースZTNAを許可します。
 - **Remotely Reachable Address** : プライベートアプリのIPを設定します
 - **Browser-based connection** : ボタンを有効にしてブラウザベースのZTNAを許可します。
 - **Public URL for this resource** : ドメインztna.sse.cisco.comとともに使用する名前を追加します。
 - **Protocol** : ブラウザ経由でアクセスするプロトコルとしてHTTPまたはHTTPSを選択します。
- **VPN connections:**RA-VPNアクセスを有効にするには、このチェックボックスをオンにします。
- **クリック 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

セキュアアクセス – プライベートリソース – セキュアアクセスクラウドを使用した通信2

設定が完了すると、次のような結果になります。

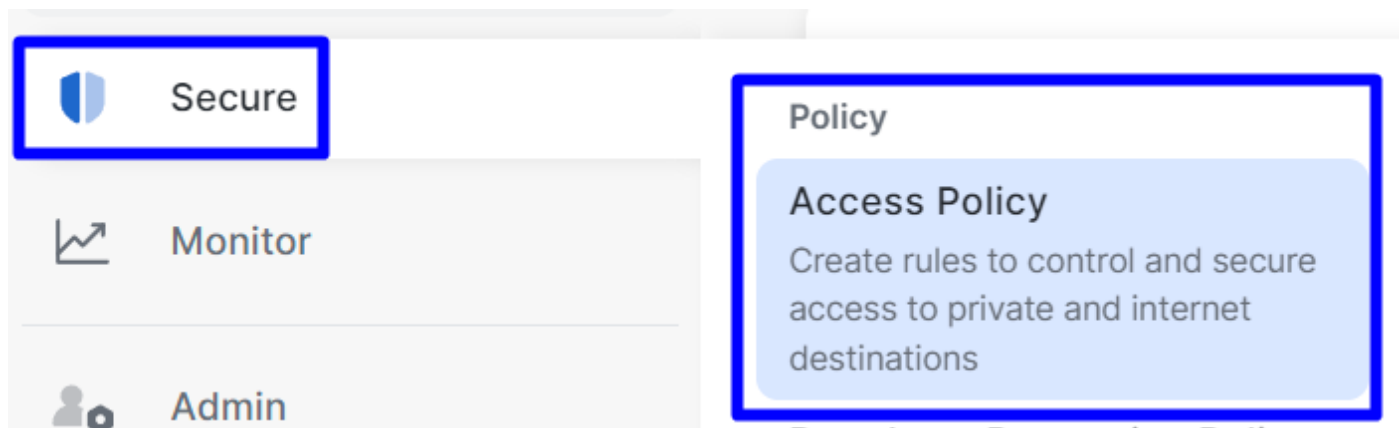
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<ul style="list-style-type: none">VPNBrowser-based ZTNAClient-based ZTNA	1	2	16

セキュアアクセス – プライベートリソースの設定

ここで、ステップ **Configure the Access Policy**に進むことができます。

アクセスポリシーの設定

アクセスポリシーを設定するには、Secure > Access Policyに移動します。



セキュアアクセス：アクセスポリシー

- クリック **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

セキュアアクセス - アクセスポリシー - プライベートアクセス

次のオプションを設定して、複数の認証方式によるアクセスを提供します。

- 1. Specify Access
 - Action:プライベート ネットワーク間で
 - **Rule name** : アクセスルールの名前を指定します
 - **From** : アクセス権を付与するユーザ
 - **To** : アクセスを許可したいアプリケーション
 - **Endpoint Requirements**: (デフォルト)
- クリック 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**

セキュアアクセス – アクセスポリシー – アクセスの指定

注：必要に応じて手順 2. **Configure Security** を実行しますが、この場合、**Intrusion Prevention (IPS)**も **Tenant Control Profile**も有効にしていません。

Save

- をクリックすると、次の情報が表示されます。

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

セキュアアクセス：アクセスポリシーの設定

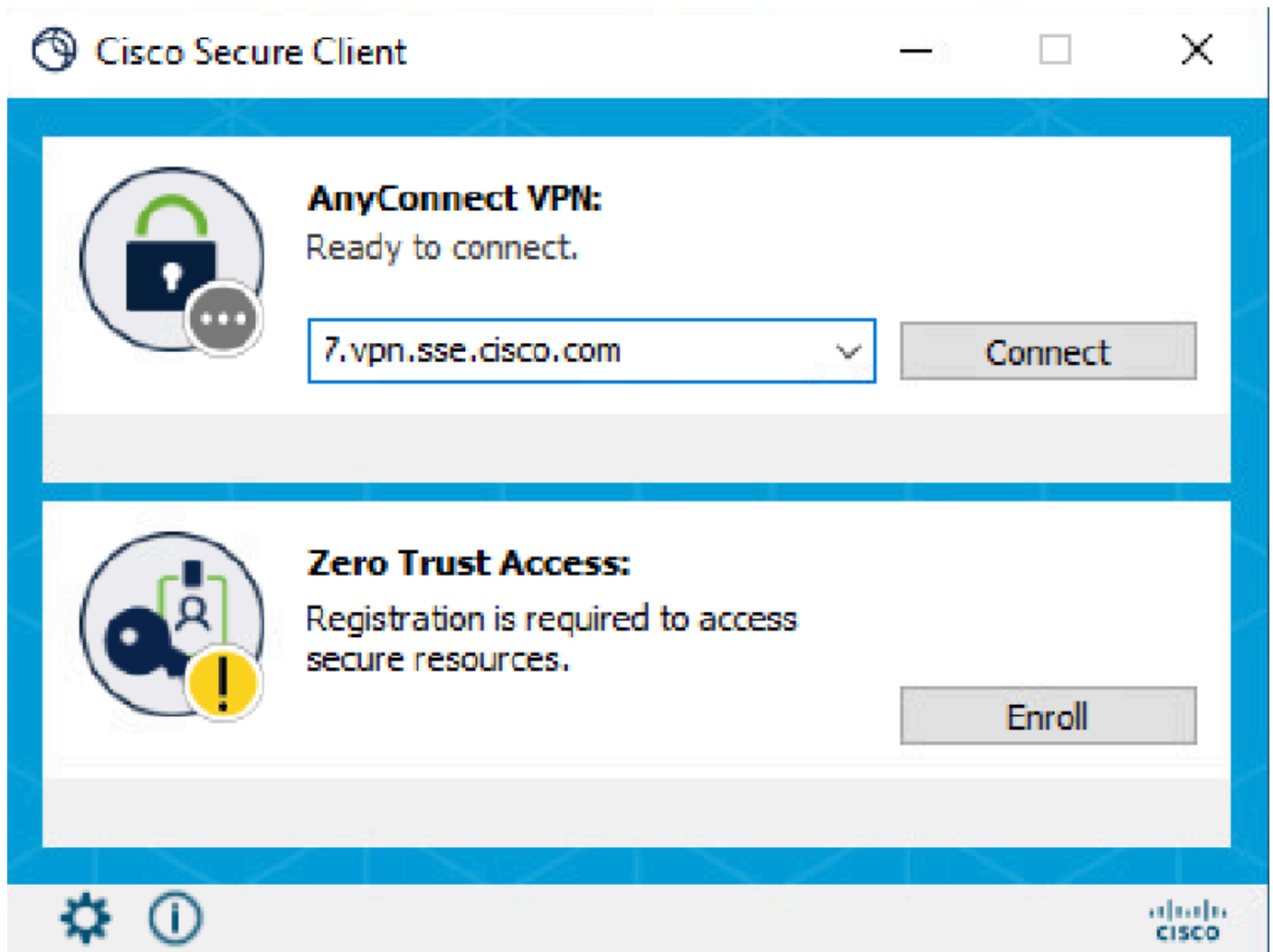
その後、Verifyステップに進むことができます。

確認

アクセスを確認するには、[ソフトウェアダウンロード - Cisco Secure Client](#)からダウンロードできるCisco Secure Clientのエージェントをインストールしている必要があります。

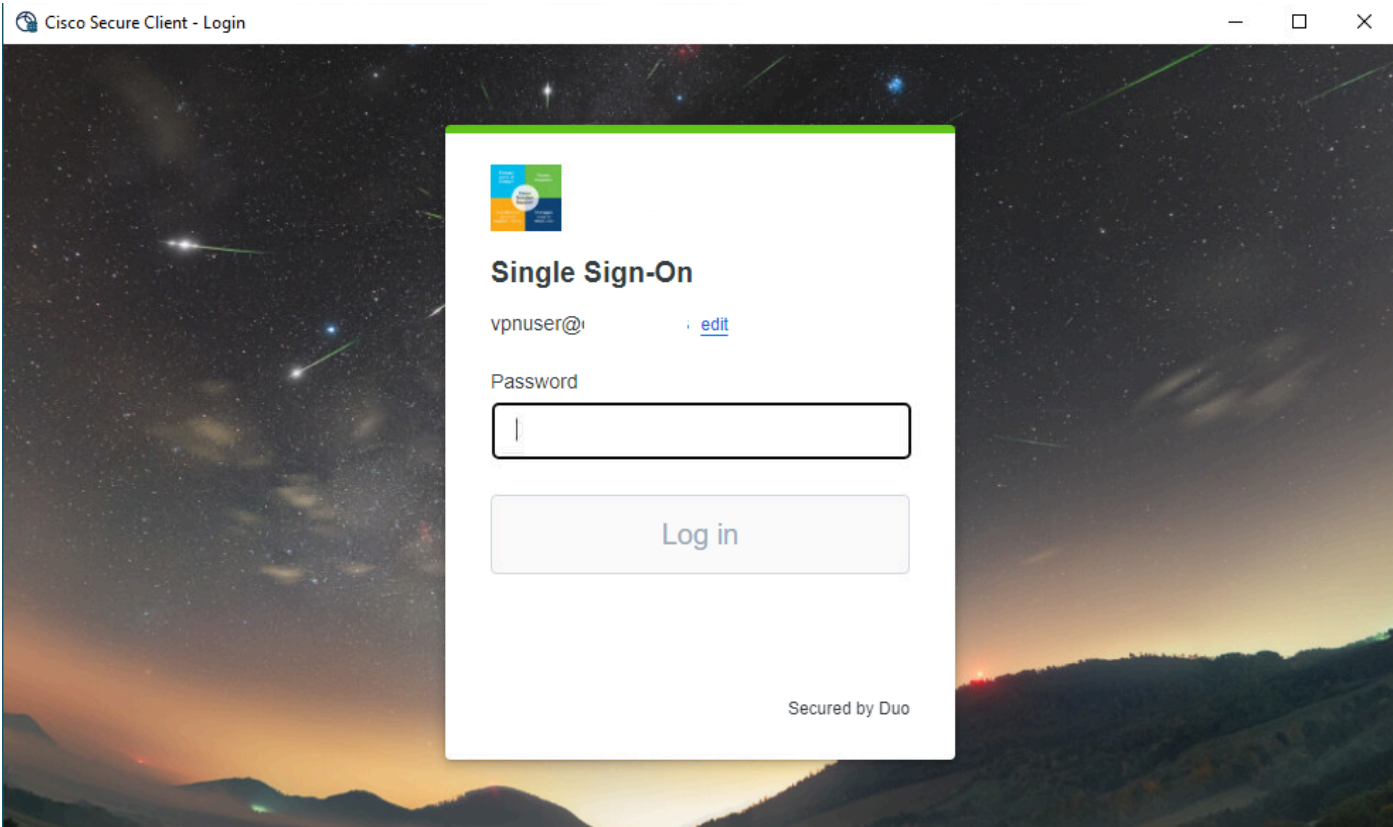
RA-VPN (オプション)

Cisco Secure Client Agent-VPNからログインします。



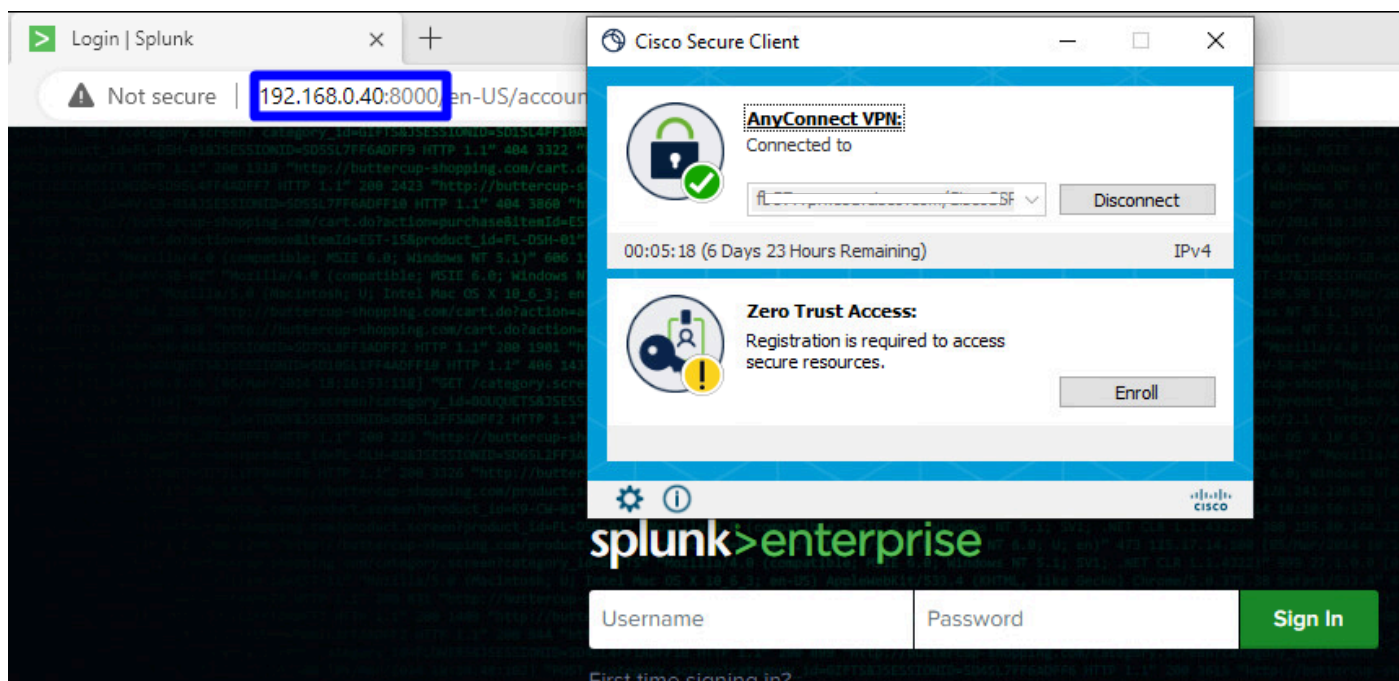
セキュアクライアント - VPN

- SSOプロバイダーを介した認証



セキュアアクセス - VPN - SSO

- 認証を受けた後、リソースにアクセスします。



セキュアアクセス - VPN - 認証

次のとおりに移動します。Monitor > Activity Search

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

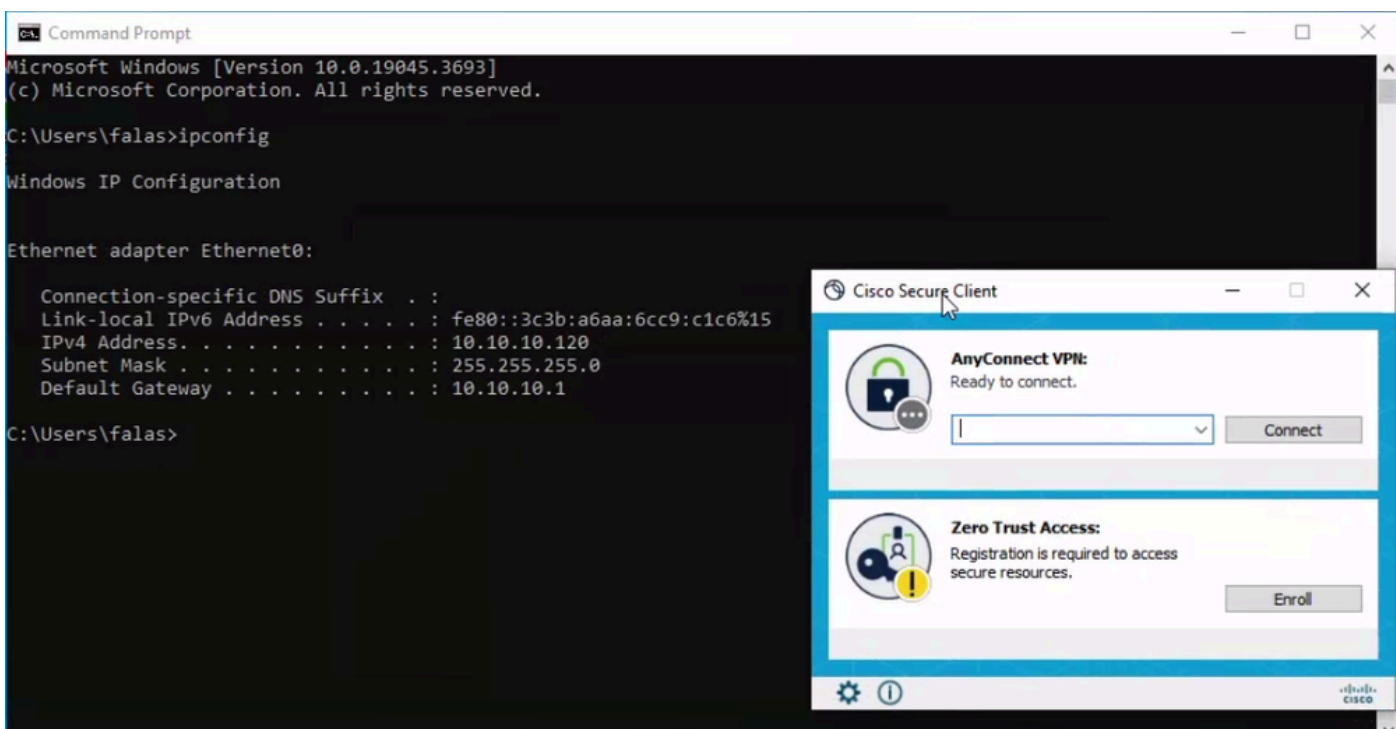
Categories: Uncategorized, Dispute Categorization

セキュアアクセス - アクティビティ検索 - RA-VPN

ユーザがRA-VPNを介して認証を受けたことを確認できます。

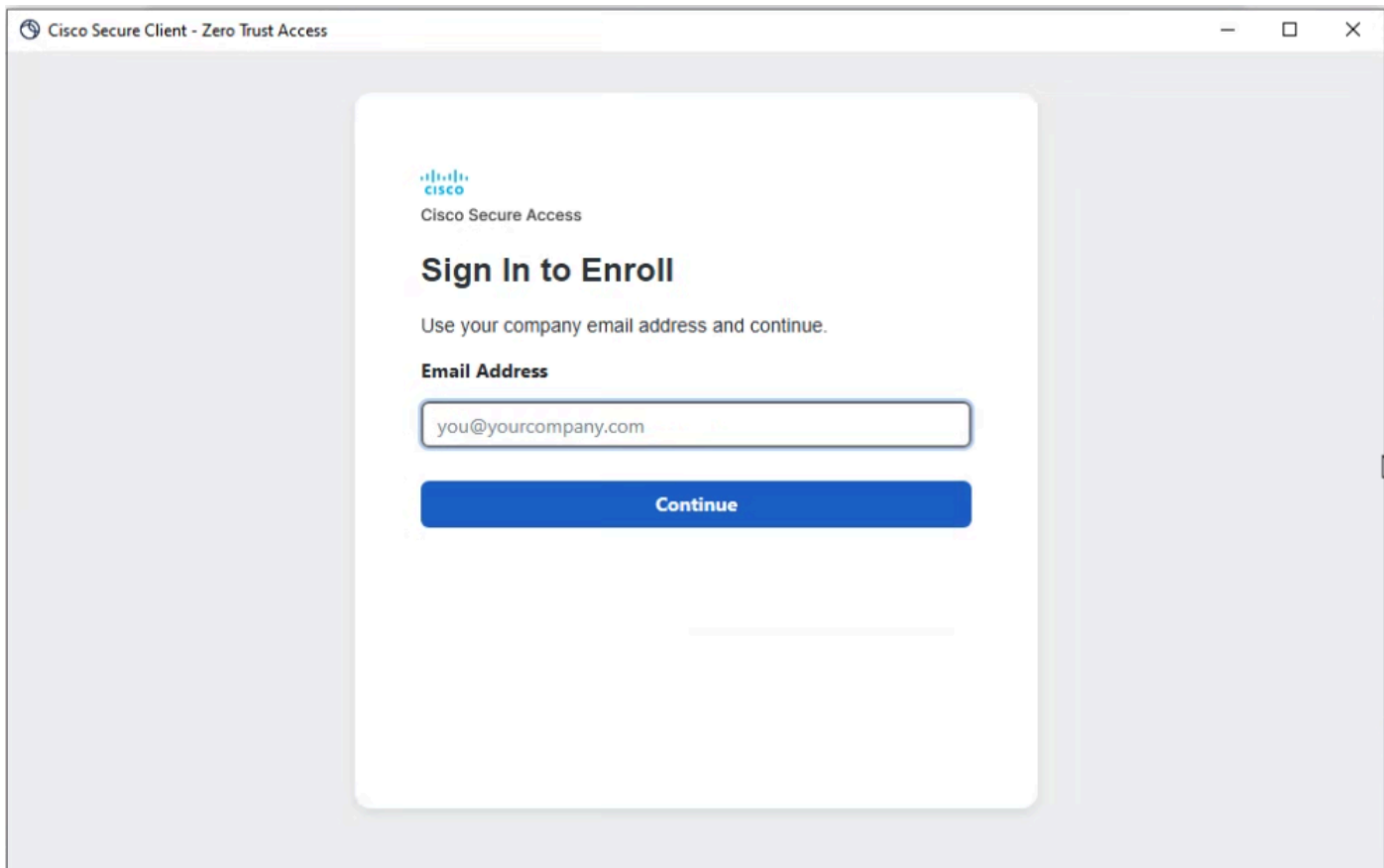
クライアントベースのZTNA

Cisco Secure Client Agent(ZTNA)からログインします。



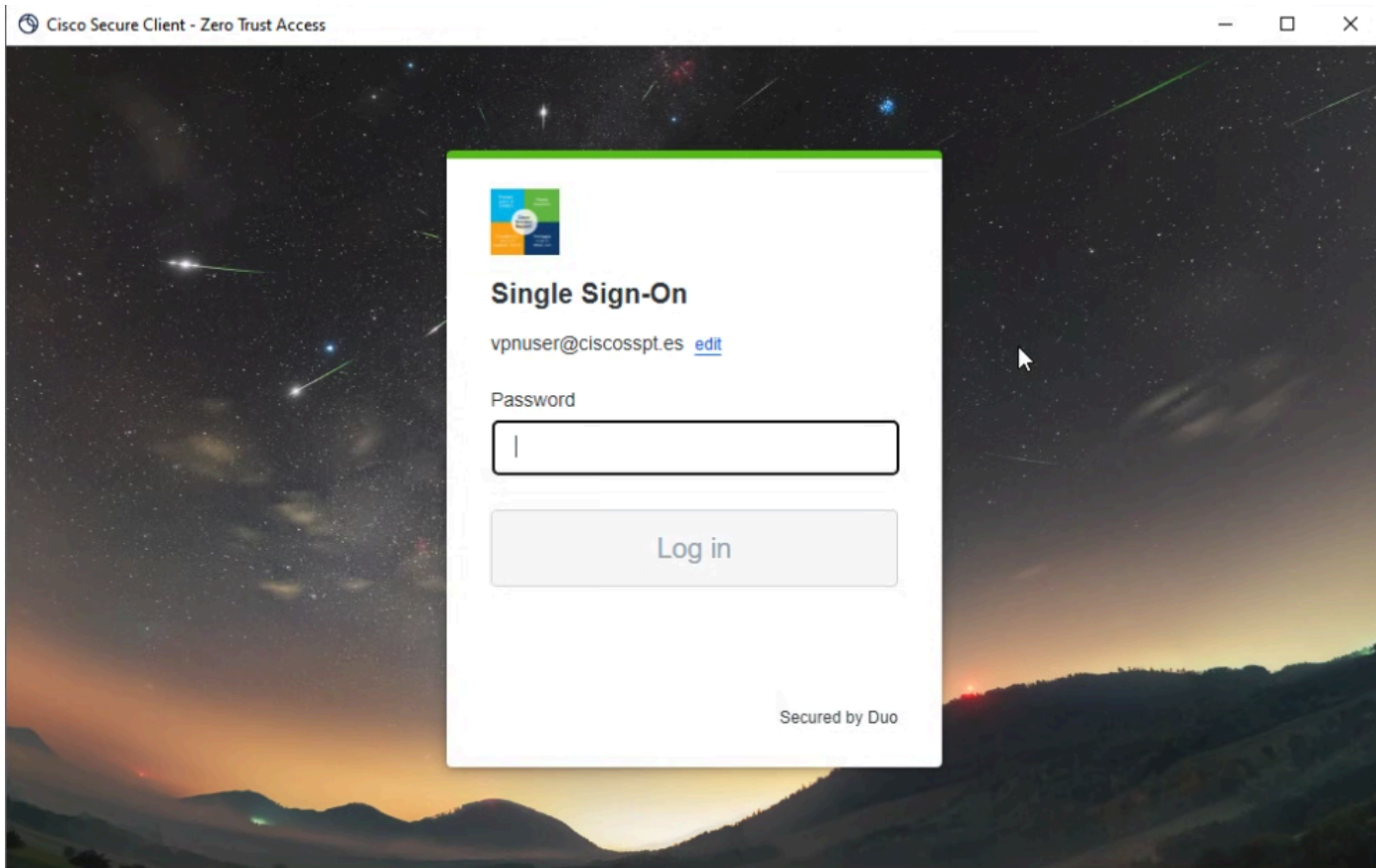
セキュアクライアント - ZTNA

- ユーザ名で登録します。



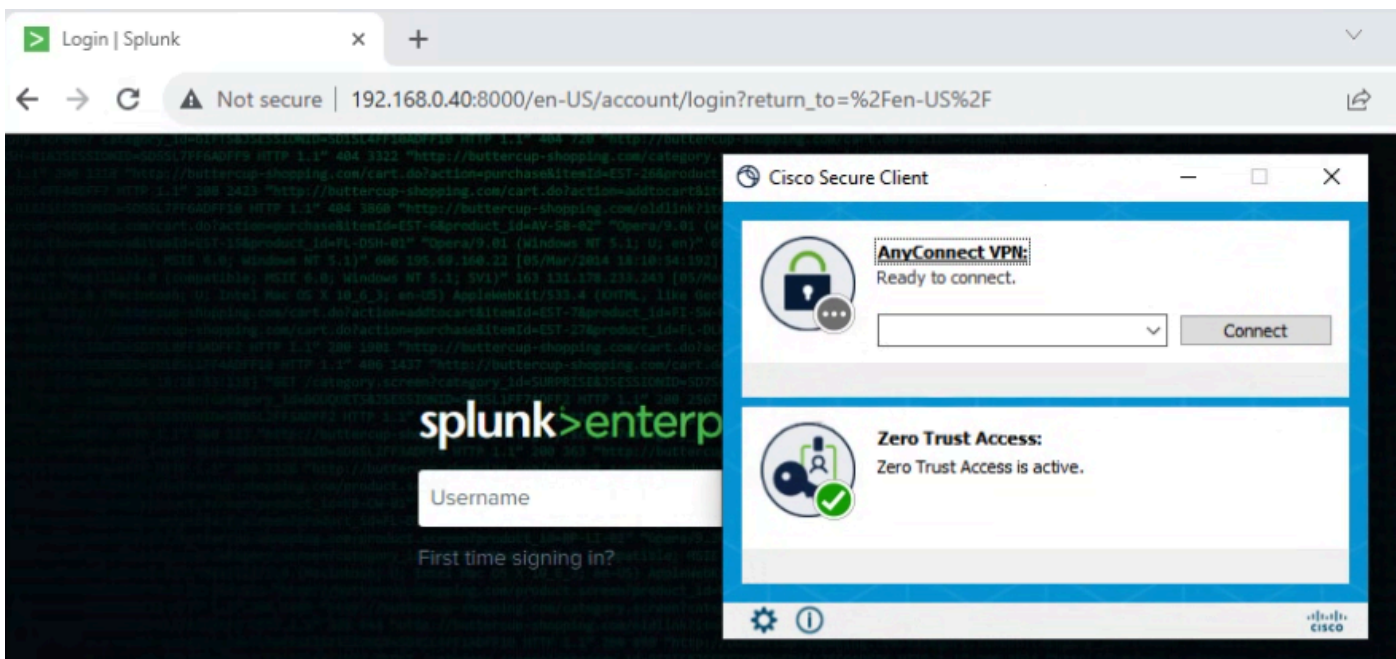
セキュアクライアント - ZTNA - 登録

- SSOプロバイダーでの認証



セキュアクライアント - ZTNA - SSOログイン

- 認証を受けた後、リソースにアクセスします。



セキュアアクセス - ZTNA - ログ

次のとおりに移動します。Monitor > Activity Search

FW	vpn user (vpnuser@ciscospt.es)	Action	Allowed
FW	vpn user (vpnuser@ciscospt.es)	Time	Nov 23, 2023 1:27 AM
FW	vpn user (vpnuser@ciscospt.es)	Rule Name	Splunksophos
FW	vpn user (vpnuser@ciscospt.es)	Identity	vpn user (vpnuser@ciscospt.es)
FW	vpn user (vpnuser@ciscospt.es)	Policy or Ruleset Identity	vpn user (vpnuser@ciscospt.es)
FW	vpn user (vpnuser@ciscospt.es)	Resource/Application	SplunkSophos
FW	vpn user (vpnuser@ciscospt.es)	OS	win 10.0.19045.3693
FW	vpn user (vpnuser@ciscospt.es)	Location	US
FW	vpn user (vpnuser@ciscospt.es)	Location IP	47.185.249.220
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscospt.es)	Endpoint Security Agent	windows-defender[]
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscospt.es)	Firewall	System
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscospt.es)	System Password	enabled[]
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscospt.es)	Disk Encryption	None
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
WEB	vpn user (vpnuser@ciscospt.es)		
WEB	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
FW	vpn user (vpnuser@ciscospt.es)		
WEB	vpn user (vpnuser@ciscospt.es)		

セキュアアクセス - アクティビティ検索 - ZTNAクライアントベース

ユーザがクライアントベースのZTNAを介して認証を許可されたことを確認できます。

ブラウザベースのZTNA

URLを取得するには、Resources > Private Resourcesに移動する必要があります。

The screenshot shows a navigation sidebar on the left with four items: 'Resources' (with a grid icon), 'Secure' (with a shield icon), 'Monitor' (with a line graph icon), and 'Admin' (with a person icon). To the right, the 'Sources and destinations' section is visible, containing two items: 'Private Resources' (highlighted with a blue box) and 'Registered Networks'. The 'Private Resources' item includes the text 'Define internal applications and other resources for use in access rules'.

セキュアアクセス – プライベートリソース

- ポリシーをクリックします。

The screenshot shows a table with one entry: 'SplunkSophos'. A blue arrow points to this entry. To the right of the table is a filter menu with three options: 'Client-based ZTNA' (teal), 'Browser-based ZTNA' (purple), and 'VPN' (pink). The number '1' is displayed to the right of the filter menu.

セキュアアクセス – プライベートリソース – *SplunkSophos*

- 下にスクロール

SplunkSophos

Client-based ZTNA

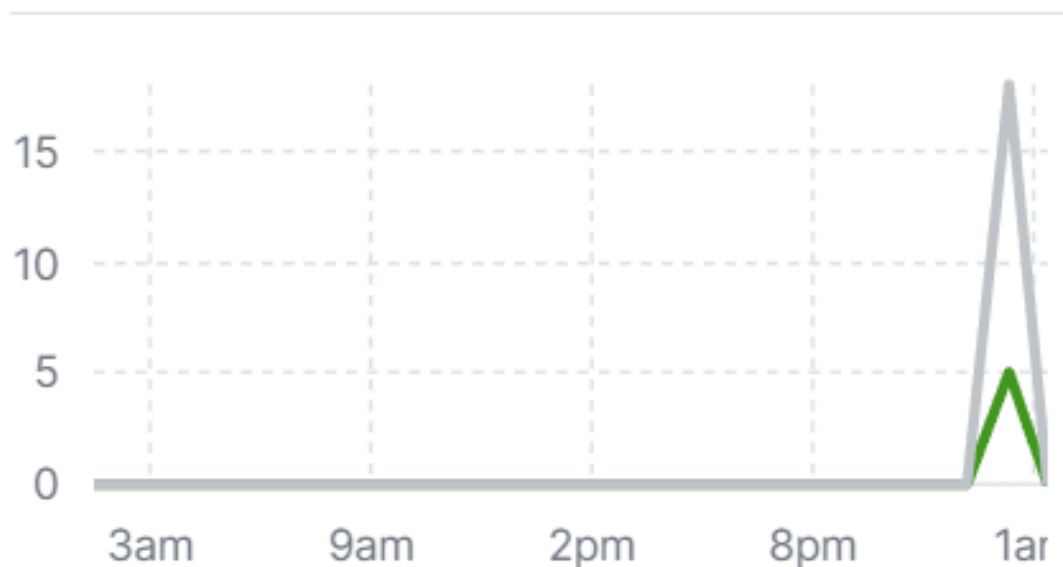
Browser-based ZTNA



VPN

Total Requests

23 ↗ 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status

✓	Success	5
⊘	Blocked	18

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。