

Konfigurieren von sicherem Zugriff mit der Sophos XG-Firewall

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren des Tunnels für sicheren Zugriff](#)

[Tunneldaten](#)

[Konfigurieren des Tunnels auf Sophos](#)

[IPsec-Profil konfigurieren](#)

[Site-to-Site-VPN konfigurieren](#)

[Konfigurieren der Tunnelschnittstelle](#)

[Konfigurieren der Gateways](#)

[Konfigurieren der SD-WAN-Route](#)

[Private App konfigurieren](#)

[Konfigurieren der Zugriffsrichtlinie](#)

[Überprüfung](#)

[RA-VPN](#)

[Client-Basis-ZTNA](#)

[Browserbasiertes ZTNA](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit der Sophos XG-Firewall konfigurieren.

Voraussetzungen

- [Konfiguration der Benutzerbereitstellung](#)
- [Konfiguration der ZTNA SSO-Authentifizierung](#)
- [Konfigurieren des sicheren Remotezugriff-VPN](#)

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sophos XG-Firewall

- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Sophos XG-Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen



CISCO

Secure

Access

SOPHOS

Sicherer Zugriff - Sophos

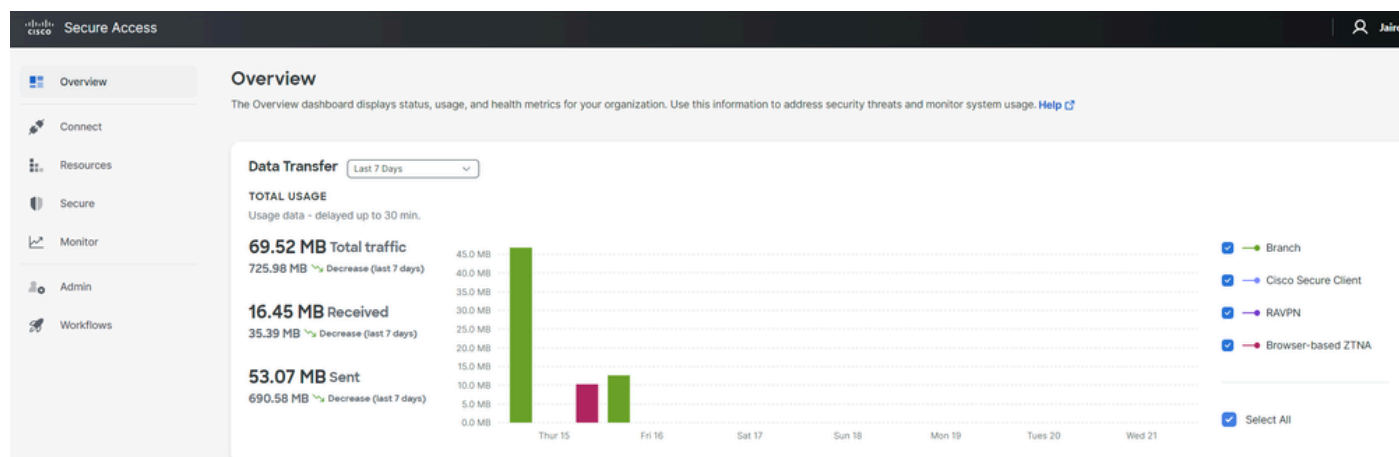
Cisco hat Secure Access entwickelt, um den Schutz und die Bereitstellung des Zugriffs auf private Anwendungen vor Ort und Cloud-basiert zu gewährleisten. Außerdem wird die Verbindung vom Netzwerk zum Internet gesichert. Dies wird durch die Implementierung mehrerer Sicherheitsmethoden und -ebenen erreicht, die alle darauf abzielen, die Informationen beim Zugriff

über die Cloud zu erhalten.

Konfigurieren

Konfigurieren des Tunnels für sicheren Zugriff

Navigieren Sie zum Admin-Bereich von [Secure Access](#).



Sicherer Zugriff - Hauptseite

- **Klicken Sie** Connect > Network Connections.

Overview

The Overview dashboard displays

Connect

Resources

Secure

Monitor

Admin

Essentials

Network Connections
Connect data centers, tunnels, resource connectors

Users and Groups
Provision and manage users and groups for use in access rules

End User Connectivity
Manage traffic steering from endpoints to Secure Access

Sicherer Zugriff - Netzwerkverbindungen

- Klicken Sie unter Network Tunnel Groups auf + Add.

Connector Groups **Beta** Network Tunnel Groups

Network Tunnel Groups 2 total

1 Disconnected ● 1 Warning ▲ 0 Connected ●

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Q Search Region Status 2 Tunnel Groups **+ Add**

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
HOME	● Disconnected	Europe (Germany)	sse-euc-1-1-0	0	sse-euc-1-1-1	0
SAD	▲ Warning	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1	0

Rows per page 10 < 1 >

Sicherer Zugriff - Netzwerk-Tunnelgruppen

- Konfigurieren Tunnel Group Name, Region und Device Type.
- Klicken Sie auf . 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](#)



Hinweis: Wählen Sie die Region aus, die dem Standort Ihrer Firewall am nächsten ist.

-
- Konfigurieren Sie die Tunnel ID Format und Passphrase.
 - Klicken Sie auf .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

Sicherer Zugriff - Tunnelgruppen - Tunnel-ID und Passphrase

- Konfigurieren Sie die IP-Adressbereiche oder Hosts, die Sie in Ihrem Netzwerk konfiguriert haben, und leiten Sie den Datenverkehr über Secure Access weiter.
- Klicken Sie auf **. 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

Sicherer Zugriff - Tunnelgruppen - Routing-Optionen

Nachdem Sie auf **Save** die Informationen über den Tunnel wird angezeigt, speichern Sie diese Informationen für den nächsten Schritt, **Configure the tunnel on Sophos**.

Tunneldaten

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](#)

Sicherer Zugriff - Tunnelgruppen - Fortsetzen der Konfiguration

Konfigurieren des Tunnels auf Sophos

IPsec-Profil konfigurieren

Um das IPsec-Profil zu konfigurieren, navigieren Sie zu Ihrer Sophos XG Firewall.

Sie erhalten etwas Ähnliches:

SOPHOS Firewall
Sophos Firewall

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

Feedback | How-to guides | Log view

System

Traffic insight

User & device insights

Active firewall rules

Reports

Messages

Sophos - Administratorkonsole

- Navigieren Sie zu Profiles
- Klicken Sie auf **IPsec Profiles** und anschließend auf Add

IPsec profiles

Device access

Add

Delete

Manage

Phase 2

Unter **General Settings** Konfigurieren:

- **Name:** Ein Referenzname für die Cisco Secure Access Policy
- **Key Exchange:** IKEv2
- **Authentication Mode:** Main-Modus
- **Key Negotiation Tries:** 0
- **Re-Key connection:** Aktivieren Sie die Option

The screenshot displays the 'General settings' configuration interface. The 'Name' field is set to 'CSA'. The 'Key exchange' is set to 'IKEv2'. The 'Authentication mode' is set to 'Main mode'. The 'Key negotiation tries' field is set to '0'. The 'Re-key connection' checkbox is checked. The 'Pass data in compressed format' and 'SHA2 with 96-bit truncation' checkboxes are unchecked. A warning message states 'Aggressive mode is insecure'.

Unter **Phase 1** Konfigurieren:

- **Key Life:** 28800
- **DH group(key group):** Wählen Sie 19 und 20
- **Encryption:** AES256
- **Authentication:** SHA2 256
- Re-key margin: 360 (Standard)
- **Randomize re-keying margin by:** 50 (Standard)

Phase 1

Key life 28800 Seconds	Re-key margin 360 Seconds	Randomize re-keying margin by 50 %
DH group (key group) 2 selected		
Encryption AES256	Authentication SHA2 256	

+ You can add up to 3 different algorithm combinations

Sophos - IPsec-Profile - Phase 1

Unter **Phase 2** Konfigurieren:

- PFS group (DH group): Wie Phase I
- **Key life:**3600
- **Encryption:** AES 256
- Authentication: SHA2 256

Phase 2

PFS group (DH group) Same as phase-I	Key life 3600 Seconds
Encryption AES256	Authentication SHA2 256

+ You can add up to 3 different algorithm combinations

Sophos - IPsec-Profile - Phase 2

Unter **Dead Peer Detection** Konfigurieren:

- **Dead Peer Detection:** Aktivieren Sie die Option
- **Check peer after every:**10
- **Wait for response up to:** 120 (Standard)
- **When peer unreachable:** Re-initiate (Standard)

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-Profile - Dead Peer Detection

Danach klicke auf **Save** and proceed with the next step, Configure Site-to-site VPN.

Site-to-Site-VPN konfigurieren

Um die Konfiguration des VPNs zu starten, klicken Sie auf **Site-to-site VPN** und dann auf **Add**.

Reports
Zero-day protection
Diagnostics

PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced protection

CONFIGURE
Remote access VPN
Site-to-site VPN
Network

Show additional properties

Name ▾ ▲ Group name ▾ Profile ▾ Connection type ▾ Status ▾ Manage

Active ▾ Connection ▾

No records found

Failover group

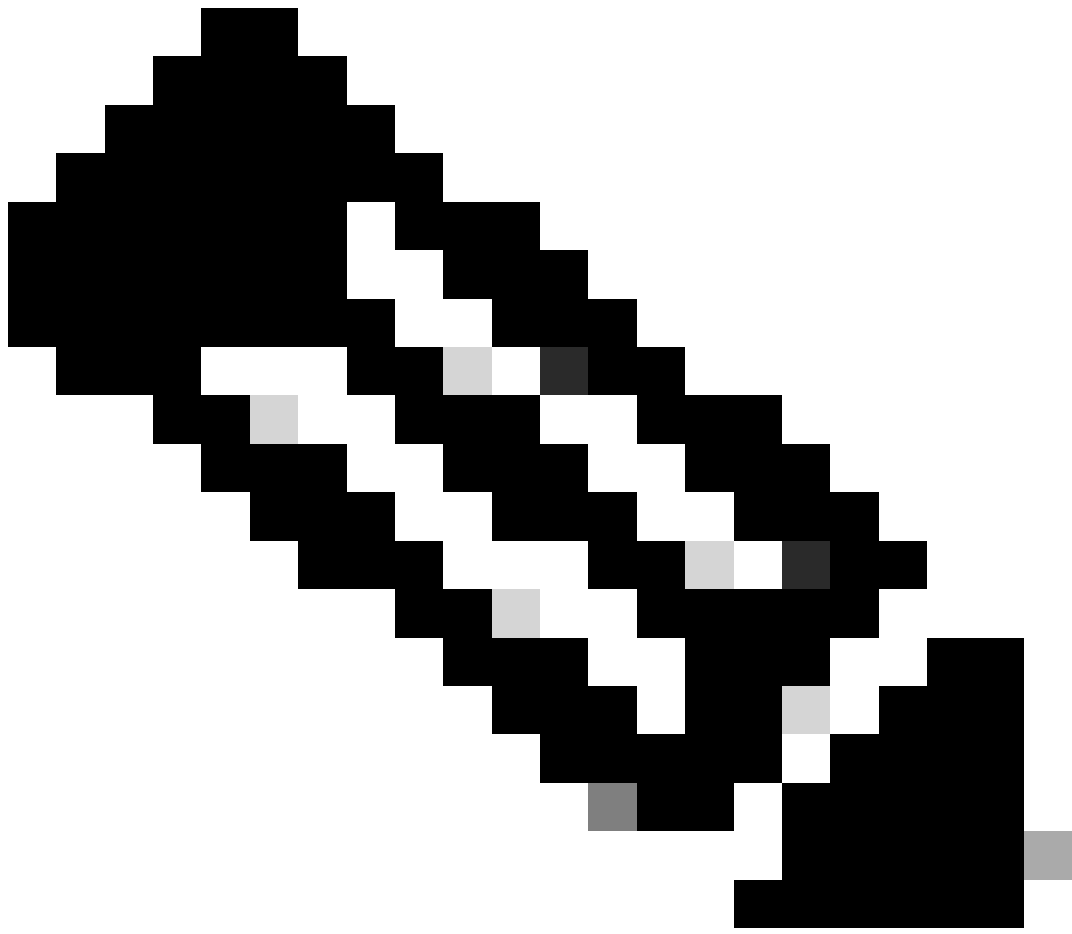
Add Delete Wizard

Add Delete

Sophos - Site-to-Site-VPN

Unter **General Settings** Konfigurieren:

- **Name:** Ein Referenzname für die Cisco Secure Access IPsec-Richtlinie
- IP version: IPv4
- Connection type: Tunnelschnittstelle
- Gateway type: Verbindung herstellen
- Active on save: Aktivieren Sie die Option



Hinweis: Die Option **Active on save** aktiviert das VPN automatisch, nachdem Sie das Site-to-Site-VPN konfiguriert haben.

General settings

Name

SecureAccessS

IP version

IPv4 IPv6 Dual

Activate on save

Create firewall rule

Description

This is the IPsec Policy for Sophos

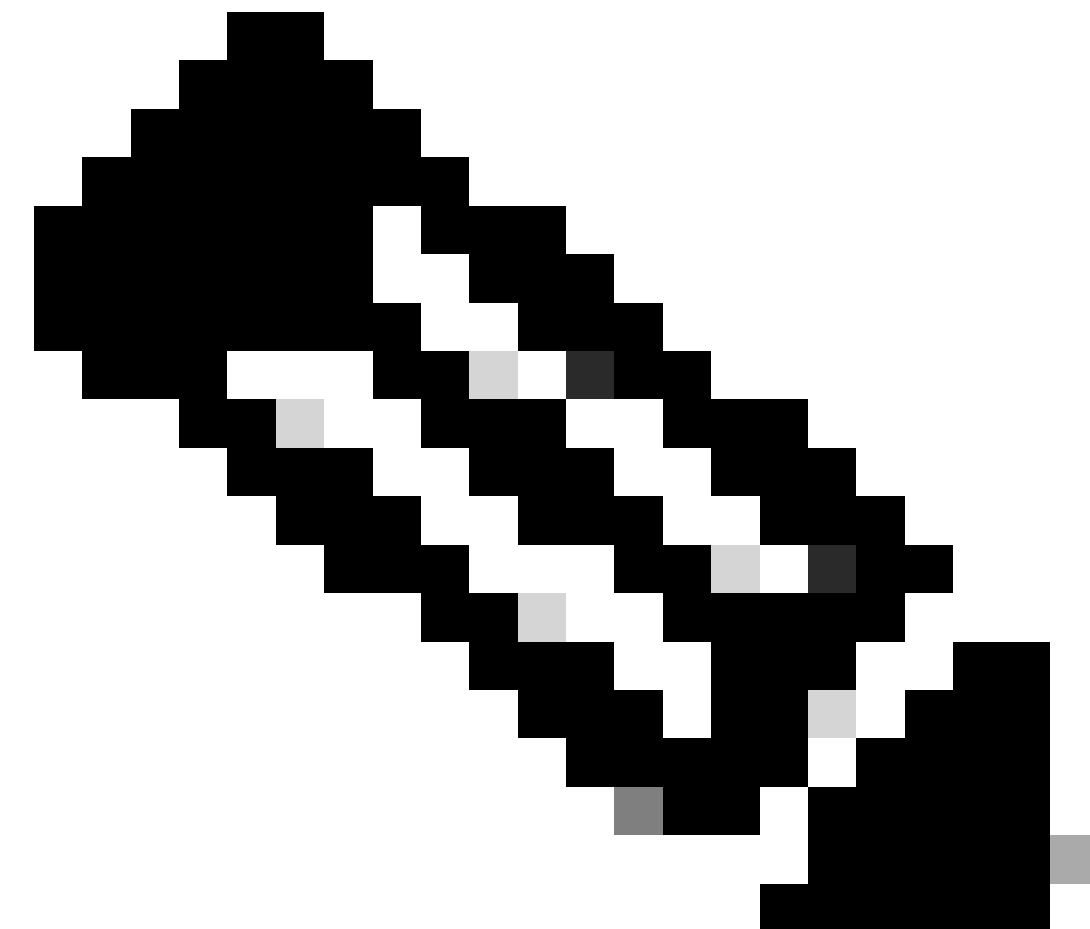
Connection type

Tunnel interface

Gateway type

Initiate the connection

Sophos - Site-to-Site-VPN - Allgemeine Einstellungen



Hinweis: Mit der Option "Tunnel interface" wird eine virtuelle Tunnelschnittstelle für die Sophos XG Firewall mit dem Namen XFRM erstellt.

Unter **Encryption** Konfigurieren:

- **Profile:** Das Profil, das Sie auf dem Schritt erstellen, **Configure IPsec Profile**
- **Authentication type:** Vorinstallierter Schlüssel
- **Preshared key:** Der Schlüssel, den Sie auf dem Schritt konfigurieren, [Configure the Tunnel on Secure Access](#)
- **Repeat preshared key:** Preshared key

Encryption

Profile: CSA

Authentication type: Preshared key

Preshared key:

Repeat preshared key:

Sophos - Site-to-Site-VPN - Verschlüsselung

Verwenden Sie diese Tabelle unter **Gateway Settings** configure Local Gateway and Remote Gateway options (Konfigurieren und Optionen) als Referenz.

Lokales Gateway	Remote-Gateway
Listening-Schnittstelle Ihre WAN-Internetschnittstelle	Gateway-Adresse Die unter dem Schritt generierte öffentliche IP, Tunnel Data
Lokaler ID-Typ	Remote-ID-Typ

E-Mail	IP-Adresse
Lokale ID Die unter Schritt generierte E-Mail, Tunnel Data	Remote-ID Die unter dem Schritt generierte öffentliche IP, Tunnel Data
Lokales Subnetz Beliebig	Remote-Subnetz Beliebig

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 - Site-to-Site-VPN - Gateway-Einstellungen

Danach klicken Sie auf **Save**, und Sie können sehen, dass der Tunnel erstellt wurde.

IPsec connections

Show additional properties							Add	Delete	Wizard
Name	Group name	Profile	Connection type	Status	Connection	Manage			
<input type="checkbox"/> <u>SecureAccesS</u>	-	CSA	Tunnel interface	●	● ⓘ	✎ ⏻ 🗑			

Sophos - Site-to-Site-VPN - IPsec-Verbindungen



Hinweis: Um zu überprüfen, ob der Tunnel auf dem letzten Bild korrekt aktiviert ist, können Sie den **Connection** Status überprüfen. Wenn er grün ist, ist der Tunnel verbunden, wenn er nicht grün ist, und der Tunnel ist nicht verbunden.

Um zu überprüfen, ob ein Tunnel eingerichtet ist, navigieren Sie zu **Current Activities > IPsec Connections**.

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

Sophos - Überwachen und Analysieren - 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	

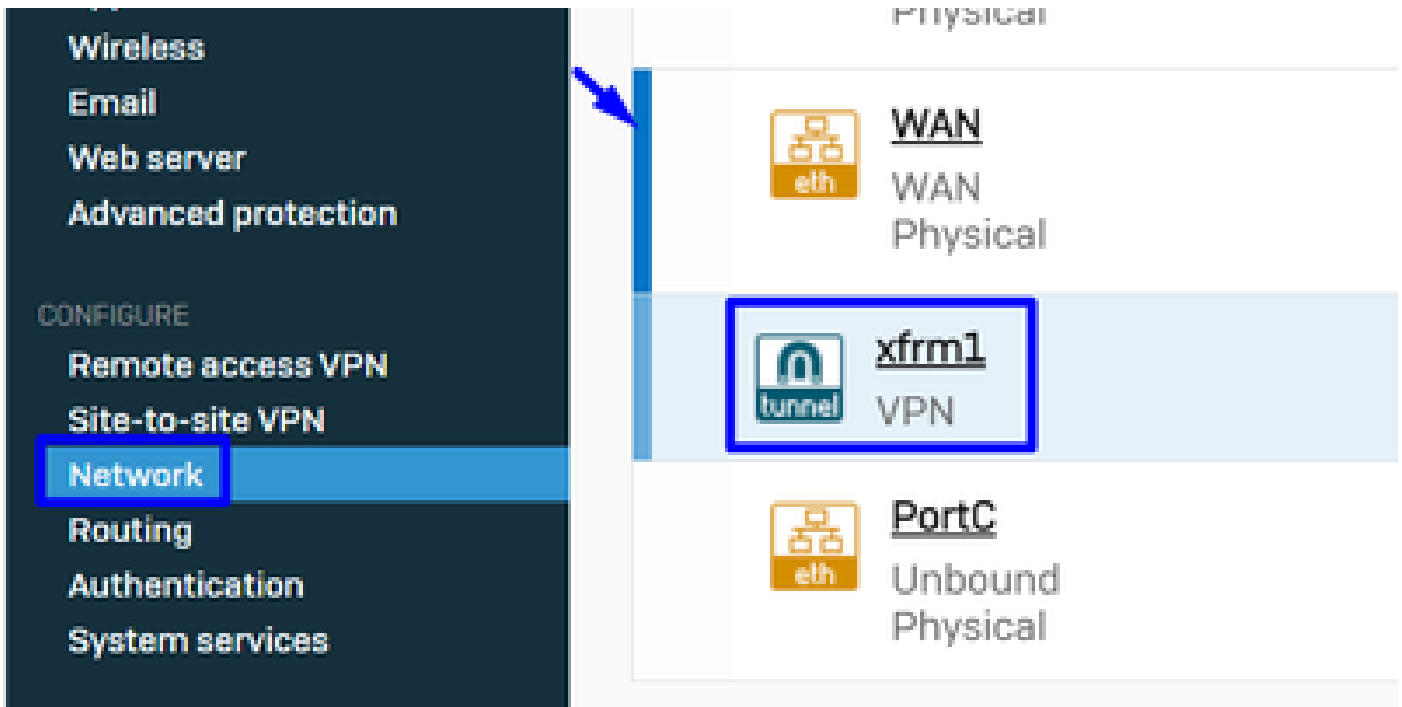
Sophos - Überwachen und Analysieren - IPsec vor und nach

Danach können wir mit dem Schritt fortfahren, **Configure Tunnel Interface Gateway**.

Konfigurieren der Tunnelschnittstelle

Navigieren Sie zu Ihrer WAN im VPN konfigurierten Schnittstelle, **Network** und überprüfen Sie sie, um die virtuelle Tunnelschnittstelle mit dem Namen xfrm zu bearbeiten.

- Klicken Sie auf **xfrm** die Schnittstelle.



Sophos - Netzwerk - Tunnelschnittstelle

- Konfigurieren Sie die Schnittstelle mit einer IP, die in Ihrem Netzwerk nicht geroutet werden kann. Sie können beispielsweise 169.254.x.x/30 verwenden. Dies ist normalerweise eine IP in einem nicht routbaren Bereich. In unserem Beispiel verwenden wir 169.254.0.1/30.

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)"/>

Sophos - Netzwerk - Tunnelschnittstelle - Konfiguration

Konfigurieren der Gateways

Um das Gateway für die virtuelle Schnittstelle zu konfigurieren (xfrm)

- Navigieren Sie zu Routing > Gateways
- Klicken Sie auf Add

Sophos - Routing - Gateways

Unter **Gateway host** Konfigurieren:

- **Name:** Ein Name, der auf die für das VPN erstellte virtuelle Schnittstelle verweist.
- **Gateway IP:** In unserem Fall 169.254.0.2 ist das die IP unter dem Netzwerk 169.254.0.1/30, die wir bereits unter dem Schritt zugewiesen haben, Configure Tunnel Interface
- **Interface:** Virtuelle VPN-Schnittstelle
- **Zone:** Keine (Standard)

Sophos - Routing - Gateways - Gateway-Host

- Aktivieren **Health check** Sie unter Deaktivieren die Option
- Klicken Sie auf **Save**

Health check



Health check



Sophos - Routing - Gateways - Statusprüfung

Sie können den Status des Kabelmodems beobachten, nachdem Sie die Konfiguration gespeichert haben:

IPv4 gateway

<input type="checkbox"/>	Name <input type="text"/>	IP address <input type="text"/>	Interface <input type="text"/>	Health check <input type="text"/>	Status <input type="text"/>	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		

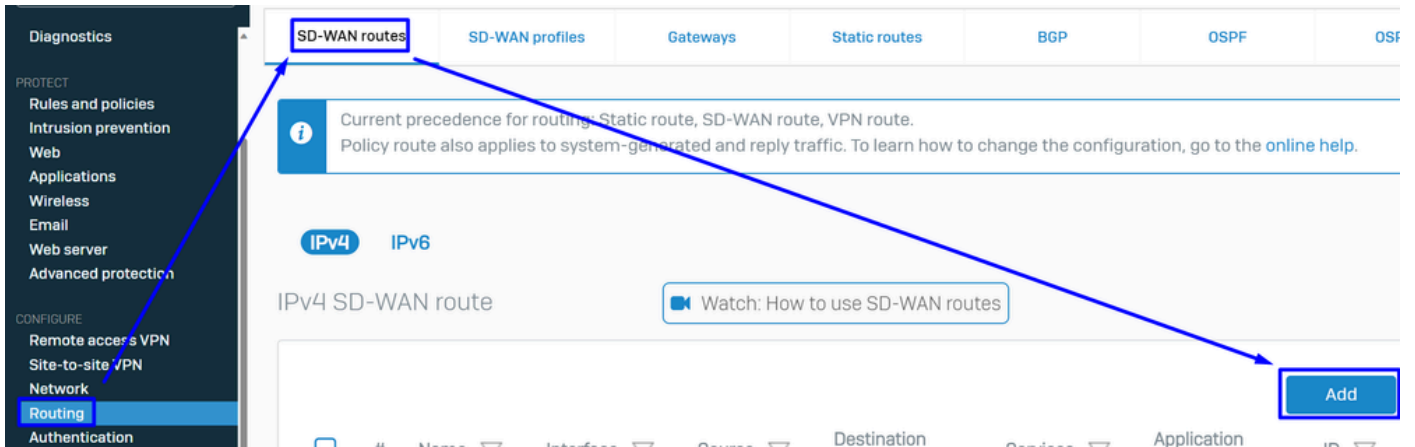
Sophos - Routing - Gateways - Status

Konfigurieren der SD-WAN-Route

Um den Konfigurationsprozess abzuschließen, müssen Sie die Route erstellen, die die Weiterleitung des Datenverkehrs an Secure Access ermöglicht.

Navigieren Sie zu **Routing > SD-WAN routes**.

- Klicken Sie **Add**



Sophos - SD-WAN-Routen

Unter **Traffic Selector** Konfigurieren:

- **Incoming interface:** Wählen Sie die Schnittstelle aus, von der aus der Datenverkehr gesendet werden soll, oder die Benutzer, die über RA-VPN, ZTNA oder Clientless-ZTNA darauf zugreifen
- **DSCP marking:** Nichts für dieses Beispiel
- **Source networks:** Wählen Sie die Adresse aus, die Sie durch den Tunnel routen möchten.
- **Destination networks:** Beliebige Ziel oder Sie können ein Ziel angeben
- **Services:** Beliebige oder Sie können die Dienste angeben
- **Application object:** Eine Anwendung, wenn Sie das Objekt konfiguriert haben
- **User or groups:** Wenn Sie eine bestimmte Benutzergruppe hinzufügen möchten, um den Datenverkehr an Secure Access weiterzuleiten

Traffic selector

<p>Incoming interface</p> <input type="text" value="LAN-192.168.0.203"/>	<p>DSCP marking</p> <input type="text" value="Select DSCP marking"/>	
<p>Source networks</p> <input type="text" value="Any"/> <p style="text-align: right;">-</p> <p style="text-align: center;">Add new item</p>	<p>Destination networks</p> <input type="text" value="Any"/> <p style="text-align: right;">-</p> <p style="text-align: center;">Add new item</p>	<p>Services</p> <input type="text" value="Any"/> <p style="text-align: right;">-</p> <p style="text-align: center;">Add new item</p>
<p>Application object</p> <input type="text" value="Any"/> <p style="text-align: right;">-</p> <p style="text-align: center;">Add new item</p>	<p>User or groups</p> <input type="text" value="Any"/> <p style="text-align: right;">-</p> <p style="text-align: center;">Add new item</p>	

Sophos - SD-WAN-Routen - Datenverkehrsauswahl

Konfigurieren **Link selection settings** Sie das Kabelmodem wie folgt:

- Primary and Backup gateways: Aktivieren Sie die Option
- **Primary gateway:** Wählen Sie das Gateway aus, das im Schritt konfiguriert wurde. [Configure the Gateways](#)
- Klicken Sie **Save**

Link selection settings

Select SD-WAN profile ⓘ Primary and Backup gateways

Primary gateway

Backup gateway

Route only through specified gateways ⓘ

Sophos - SD-WAN-Routen - Traffic Selector - Primäre und Backup-Gateways

Nachdem Sie die Konfiguration auf der Sophos XG-Firewall abgeschlossen haben, können Sie mit dem Schritt fortfahren: **Configure Private App.**

Private App konfigurieren

Um den Zugriff auf die private App zu konfigurieren, melden Sie sich beim [Admin-Portal an](#).

- Navigieren Sie zu **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

Sicherer Zugriff - Private Ressourcen

- Klicken Sie + Add

Private Resources Private Resource Groups

Private Resources

Q Search by resource name Private Resource Group Connection Method 4 Private Resources Last 24 Hours + Add

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

Sicherer Zugriff - Private Ressourcen 2

- Unter **General** Konfigurieren **Private Resource Name**

General

Private Resource Name

SplunkSophos

Description (optional)

Sicherer Zugriff - Private Ressourcen - Allgemein

Unter **Communication with Secure Access Cloud** Konfigurieren:

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR):** Wählen Sie die Ressource aus, auf die Sie zugreifen möchten



Hinweis: Denken Sie daran, dass die intern erreichbare Adresse auf dem Schritt zugewiesen wurde [Configure the Tunnel on Secure Access](#).

-
- **Protocol:** Wählen Sie das Protokoll aus, mit dem Sie auf diese Ressource zugreifen
 - **Port / Ranges :** Wählen Sie die Ports aus, die Sie für den Zugriff auf die App aktivieren müssen.

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

Sicherer Zugriff - Private Ressourcen - Kommunikation mit sicherer Zugriffs-Cloud

In **Endpoint Connection Methods** konfigurieren Sie alle Möglichkeiten für den Zugriff auf private Ressourcen über sicheren Zugriff und wählen die Methoden aus, die Sie für Ihre Umgebung verwenden möchten:

- **Zero-trust connections:** Aktivieren Sie das Kontrollkästchen, um den ZTNA-Zugriff zu aktivieren.
 - **Client-based connection:** Schaltfläche aktivieren, um Client-Basis-ZTNA zuzulassen
 - **Remotely Reachable Address:** Konfigurieren Sie die IP-Adresse Ihrer privaten App.
 - **Browser-based connection:** Aktivieren Sie die Schaltfläche, um browserbasiertes ZTNA zuzulassen.
 - **Public URL for this resource:** Fügen Sie einen Namen hinzu, der zusammen mit der Domäne `ztna.sse.cisco.com` verwendet werden soll.
 - **Protocol:** Wählen Sie HTTP oder HTTPS als Protokoll für den Zugriff über den Browser.
- **VPN connections:** Aktivieren Sie das Kontrollkästchen, um den RA-VPN-Zugriff zu aktivieren.
- Klicken Sie auf **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) ⓘ

[+ 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:// -8195126.ztna.sse.cisco.com

Protocol **Server Name Indication (SNI)** (optional) ⓘ

Validate Application Certificate ⓘ

VPN connections
 Allow endpoints to connect to this resource when connected to the network using VPN.

Save Cancel

Sicherer Zugriff - Private Ressourcen - Kommunikation mit sicherem Zugriff Cloud 2

Nach Abschluss der Konfiguration ist dies das Ergebnis:

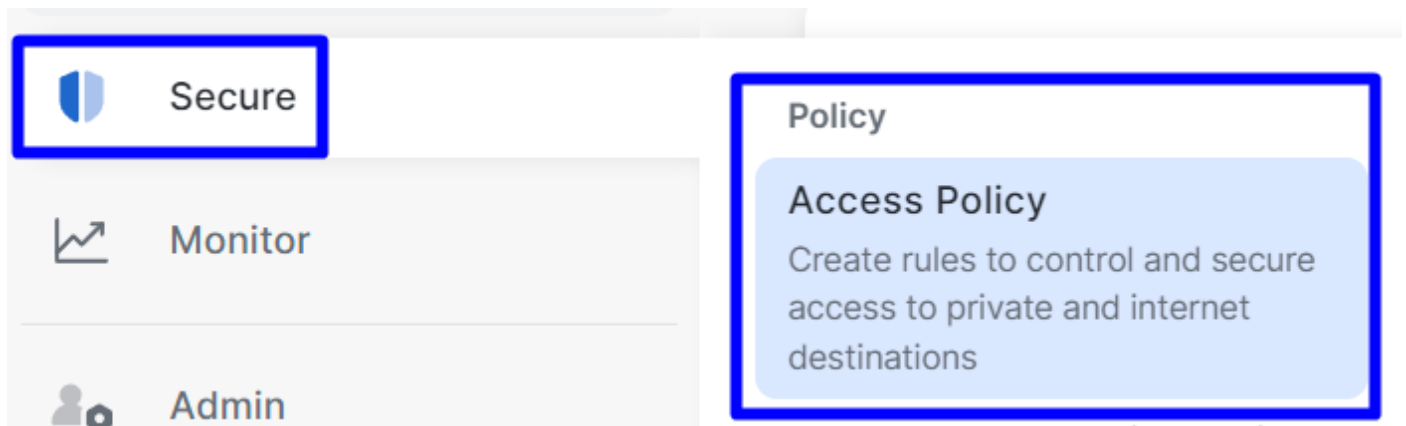
Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
SplunkSophos	-	<input checked="" type="checkbox"/> VPN <input checked="" type="checkbox"/> Browser-based ZTNA <input checked="" type="checkbox"/> Client-based ZTNA	1	2	16

Sicherer Zugriff - Konfigurierte private Ressourcen

Jetzt können Sie mit dem Schritt fortfahren, **Configure the Access Policy**.

Konfigurieren der Zugriffsrichtlinie

Um die Zugriffsrichtlinie zu konfigurieren, navigieren Sie zu Secure > Access Policy.



Sicherer Zugriff - Zugriffsrichtlinie

- Klicken Sie auf **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

Sicherer Zugriff - Zugriffsrichtlinie - Privater Zugriff

Konfigurieren Sie die nächsten Optionen, um den Zugriff über mehrere Authentifizierungsmethoden bereitzustellen:

- 1. Specify Access
 - Action: Zulassen
 - **Rule name:** Geben Sie einen Namen für Ihre Zugriffsregel an.
 - **From:** Die Benutzer, denen Sie den Zugriff gewähren
 - **To:** Die Anwendung, für die Sie den Zugriff zulassen möchten
 - Endpoint Requirements: (Standard)
- Klicken Sie auf **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**

Sicherer Zugriff - Zugriffsrichtlinie - Zugriff festlegen



Hinweis: Schritt 2. **Configure Security** nach Bedarf, aber in diesem Fall haben Sie nicht aktiviert, **Intrusion Prevention (IPS)**, oder **Tenant Control Profile**.

- Klicken Sie auf Save, um Folgendes anzuzeigen:

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

Sicherer Zugriff - Zugriffsrichtlinie konfiguriert

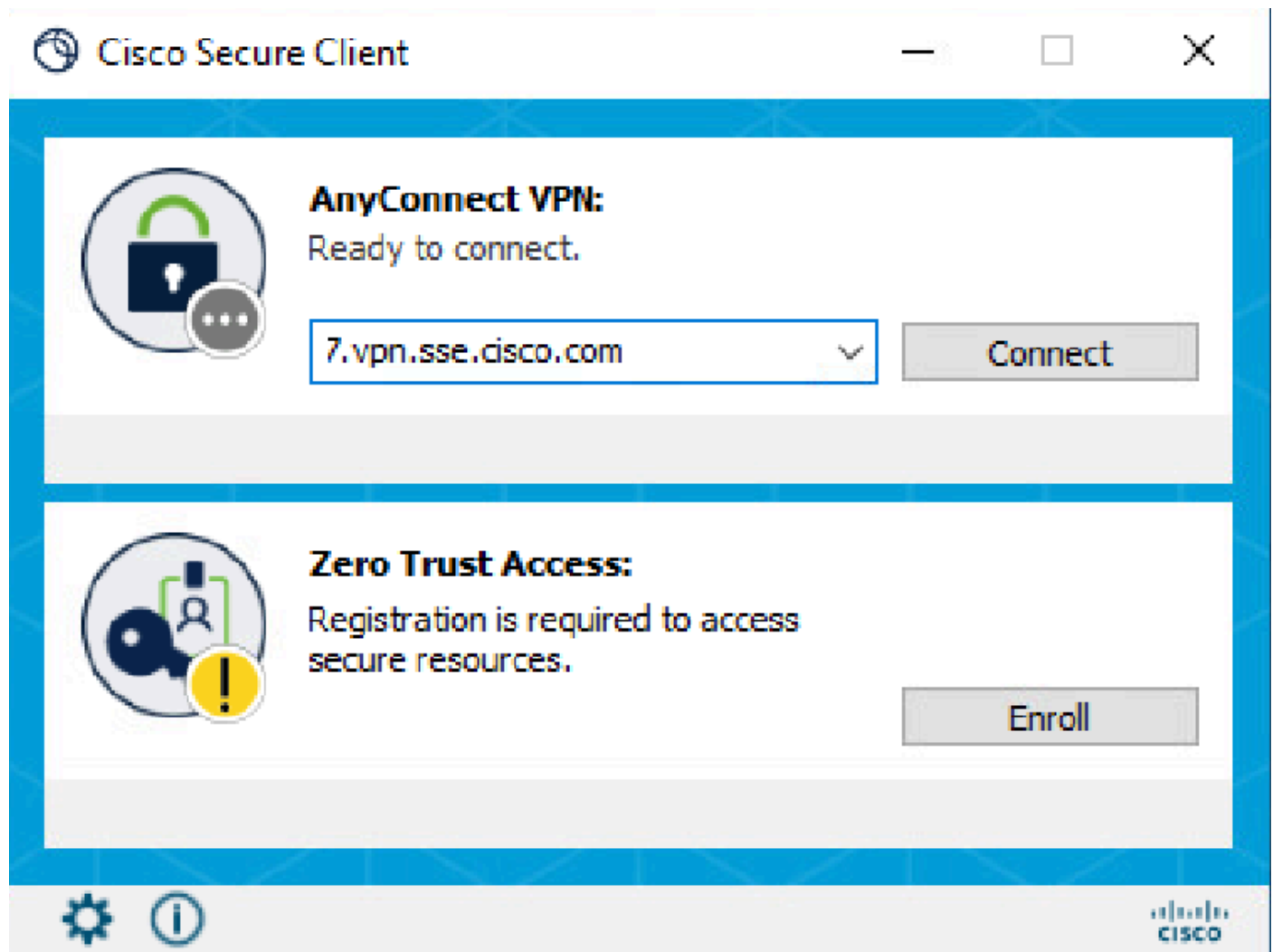
Danach können Sie mit dem Schritt fortfahren Verify.

Überprüfung

Um den Zugriff zu überprüfen, müssen Sie den Agenten von Cisco Secure Client installiert haben, den Sie von [Software Download - Cisco Secure Client](#) herunterladen können.

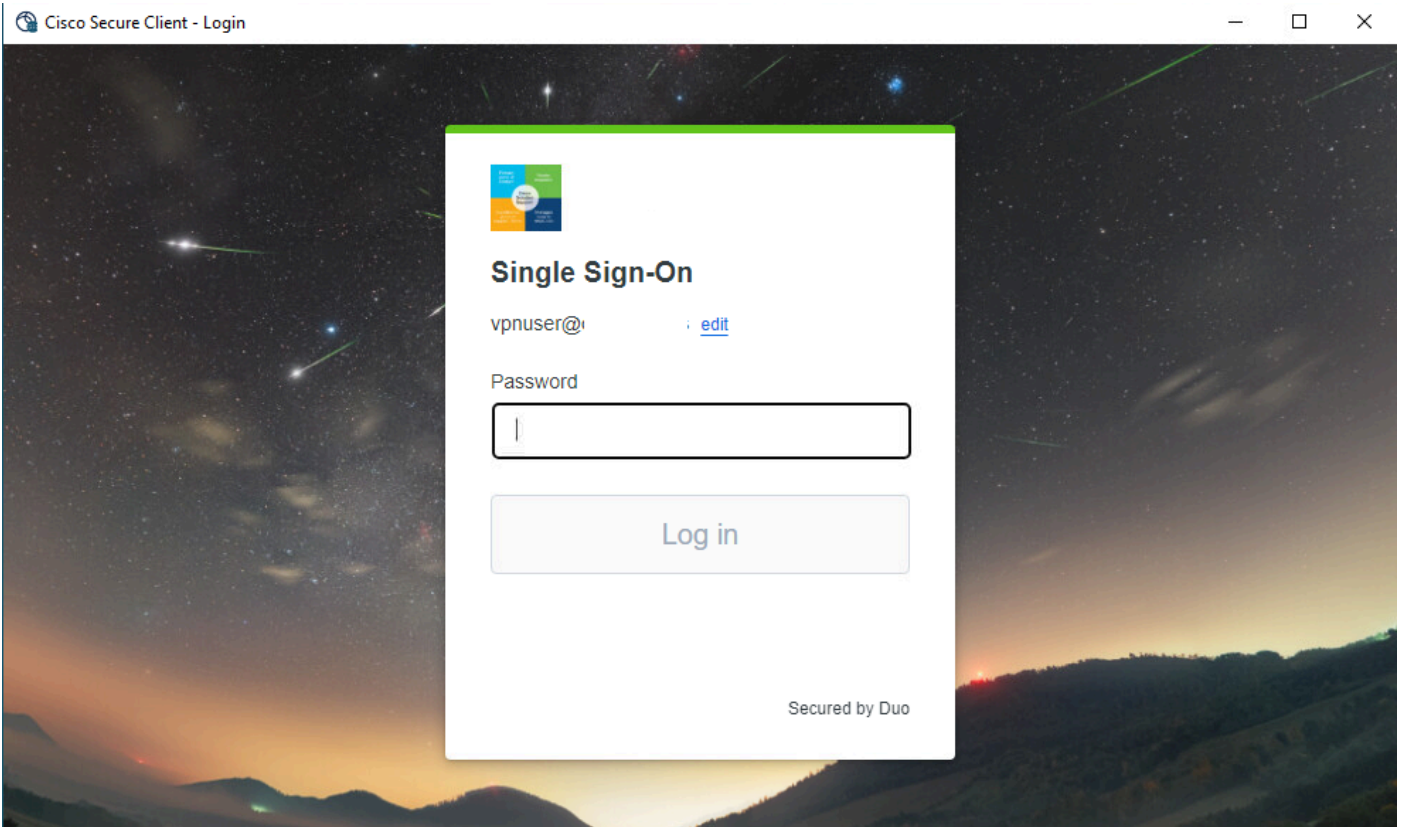
RA-VPN

Anmeldung über Cisco Secure Client Agent - VPN.



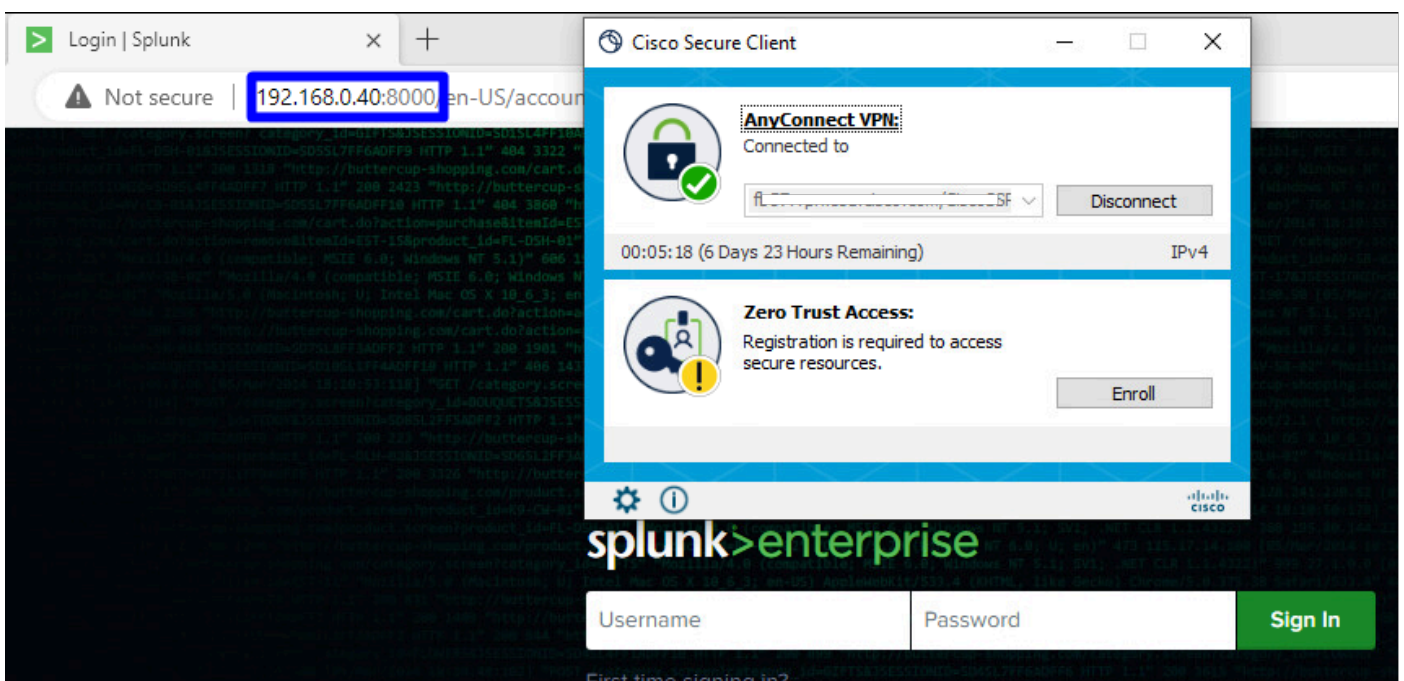
Sicherer Client - VPN

- Authentifizierung über Ihren SSO-Anbieter



Sicherer Zugriff - VPN - SSO

- Nachdem Sie authentifiziert wurden, können Sie auf die Ressource zugreifen:



Sicherer Zugriff - VPN - Authentifizierung

Navigieren Sie zu: Monitor > Activity Search

42 Total Viewing activity from Nov 22, 2023 1:09 AM to Nov 23, 2023 1:09 AM Page: 1 Results per page: 50 1 - 42 of 42

Request	Source	Rule Identity	Destination	Destination IP
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...
FW	vpn user (vpnuser@ciscospt.es)	vpn user (vpnuser@ciscospt.es)	192.168.0.4	...

Event Details

Action: Allowed

Time: Nov 23, 2023 1:09 AM

Rule Name: RDP (373192)

Source: vpn user (vpnuser@ciscospt.es)

Source IP: 192.168.50.130

Destination IP: 192.168.0.40

Source Port: 50226

Destination Port: 8000

Categories: Uncategorized, Dispute Categorization

Sicherer Zugriff - Aktivitätssuche - RA-VPN

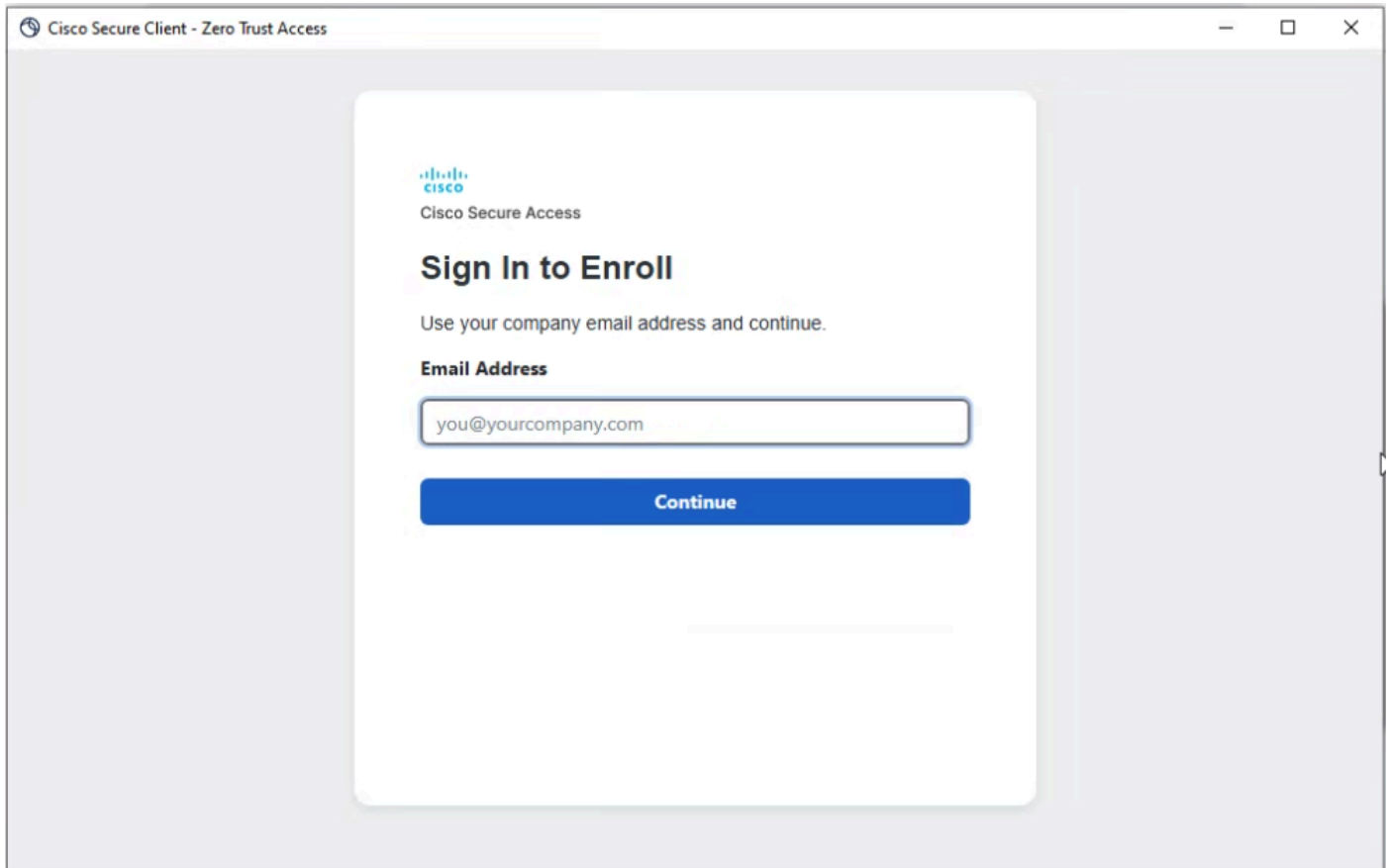
Sie können sehen, dass sich der Benutzer über RA-VPN authentifizieren durfte.

Client-Basis-ZTNA

Anmeldung über Cisco Secure Client Agent - ZTNA.

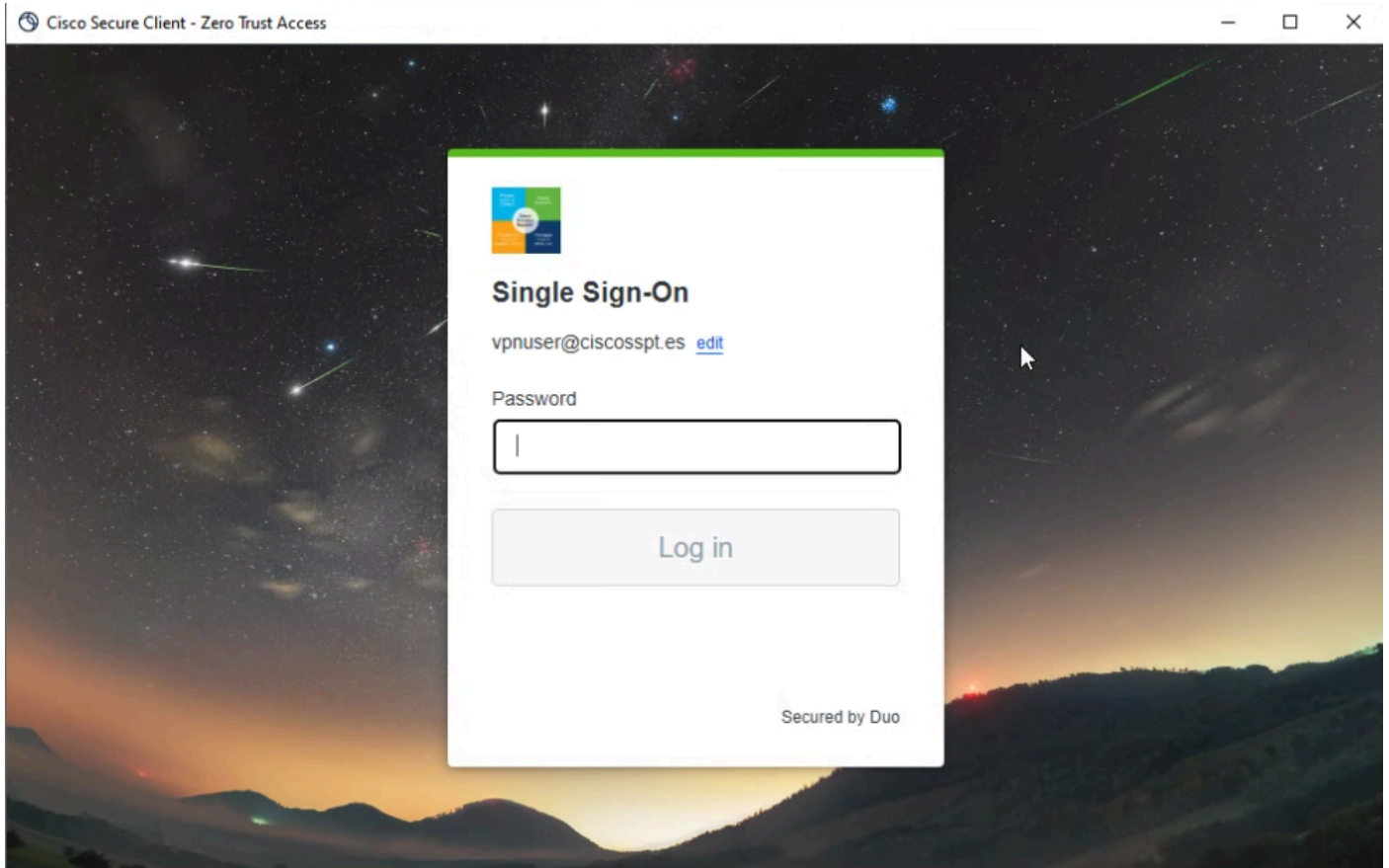
Sicherer Client - ZTNA

- Melden Sie sich mit Ihrem Benutzernamen an.



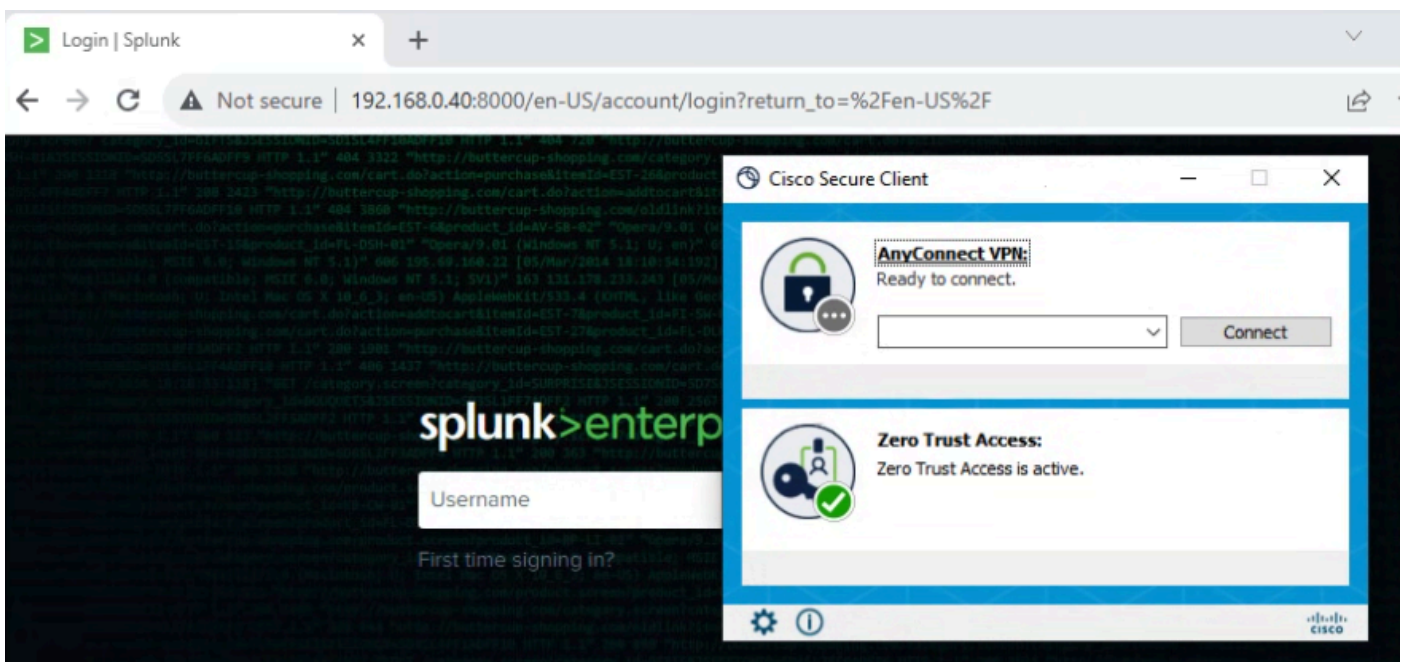
Secure Client - ZTNA - Anmeldung

- Authentifizierung bei Ihrem SSO-Anbieter



Secure Client - ZTNA - SSO-Anmeldung

- Nachdem Sie authentifiziert wurden, können Sie auf die Ressource zugreifen:



Sicherer Zugriff - ZTNA - Protokolliert

Navigieren Sie zu: Monitor > Activity Search

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

Sicherer Zugriff - Aktivitätssuche - Client-basiert mit ZTNA

Sie können sehen, dass sich der Benutzer über eine clientbasierte ZTNA authentifizieren durfte.

Browserbasiertes ZTNA

Um die URL abzurufen, müssen Sie zu gehen **Resources > Private Resources**.

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

Sicherer Zugriff - Private Ressource

- Klicken Sie auf Ihre Richtlinie.

SplunkSophos

Client-based ZTNA

Browser-based ZTNA

VPN

1

Sicherer Zugriff - Private Ressource - SplunkSophos

- Nach unten

SplunkSophos

Client-based ZTNA

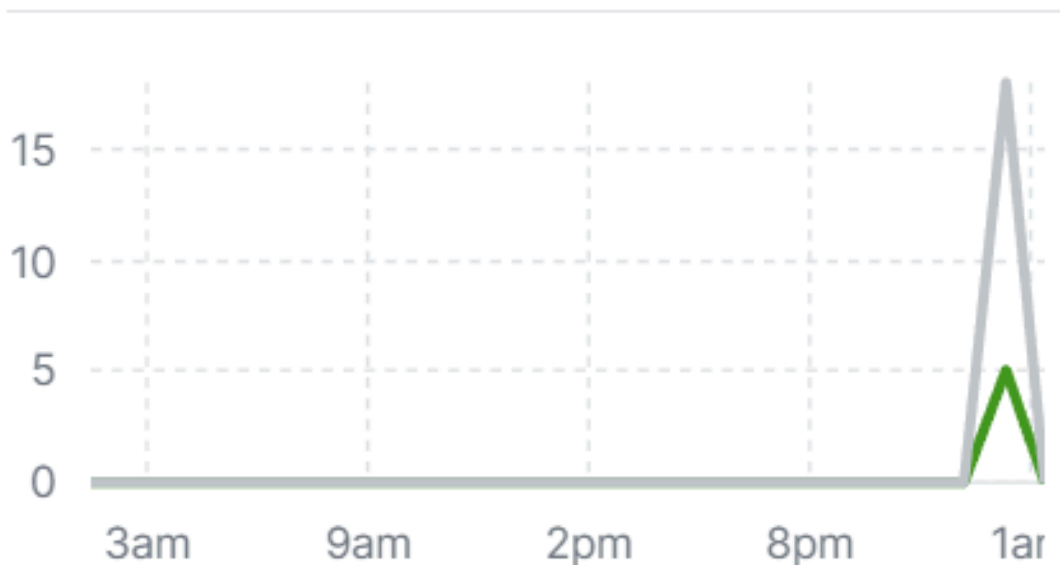
Browser-based ZTNA



VPN

Total Requests

23 ↗ 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status

✓	Success	5
⊘	Blocked	18

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.