Configurazione di Secure Access con Sophos XG Firewall

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Access con Sophos XG Firewall.

Prerequisiti

- Configura assegnazione ruoli utente
- Configurazione autenticazione SSO ZTNA
- Configura accesso sicuro VPN di accesso remoto

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Sophos XG Firewall
- Accesso sicuro

- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Sophos XG Firewall
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Secure Access - Sophos

Cisco ha progettato Secure Access per garantire la protezione e la fornitura dell'accesso alle applicazioni private, sia in sede che basate su cloud. Inoltre, garantisce il collegamento dalla rete a Internet. Questo risultato è ottenuto attraverso l'implementazione di più metodi e livelli di sicurezza, il tutto finalizzato a preservare le informazioni mentre vi accedono tramite il cloud.

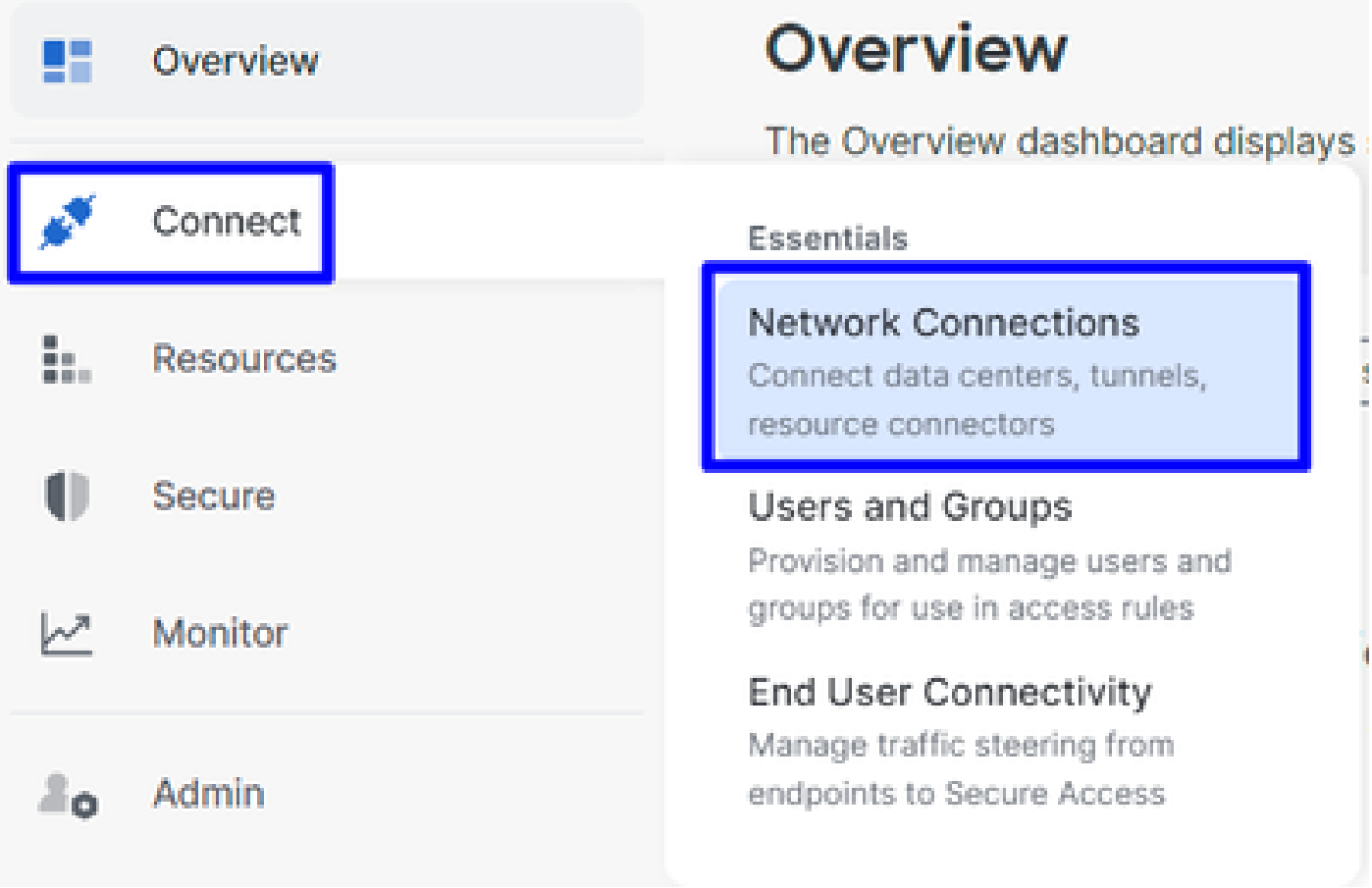
Configurazione

Configurazione del tunnel su accesso sicuro

Passare al pannello di amministrazione di Accesso sicuro.

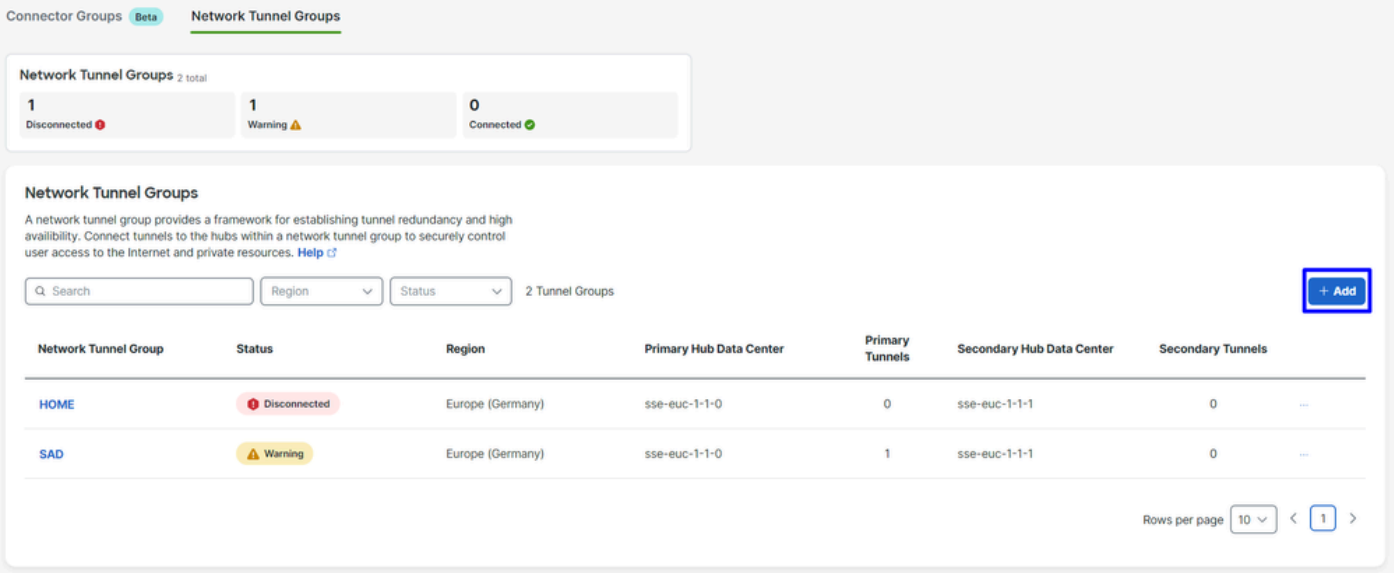
Secure Access - Pagina principale

- Fare clic su Connect > Network Connections.



Accesso sicuro - Connessioni di rete

- In fareNetwork Tunnel Groups clic su + Add.



Accesso sicuro - Gruppi di tunnel di rete

- Configurare Tunnel Group Name, Region e Device Type.
- Fare clic su . **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)

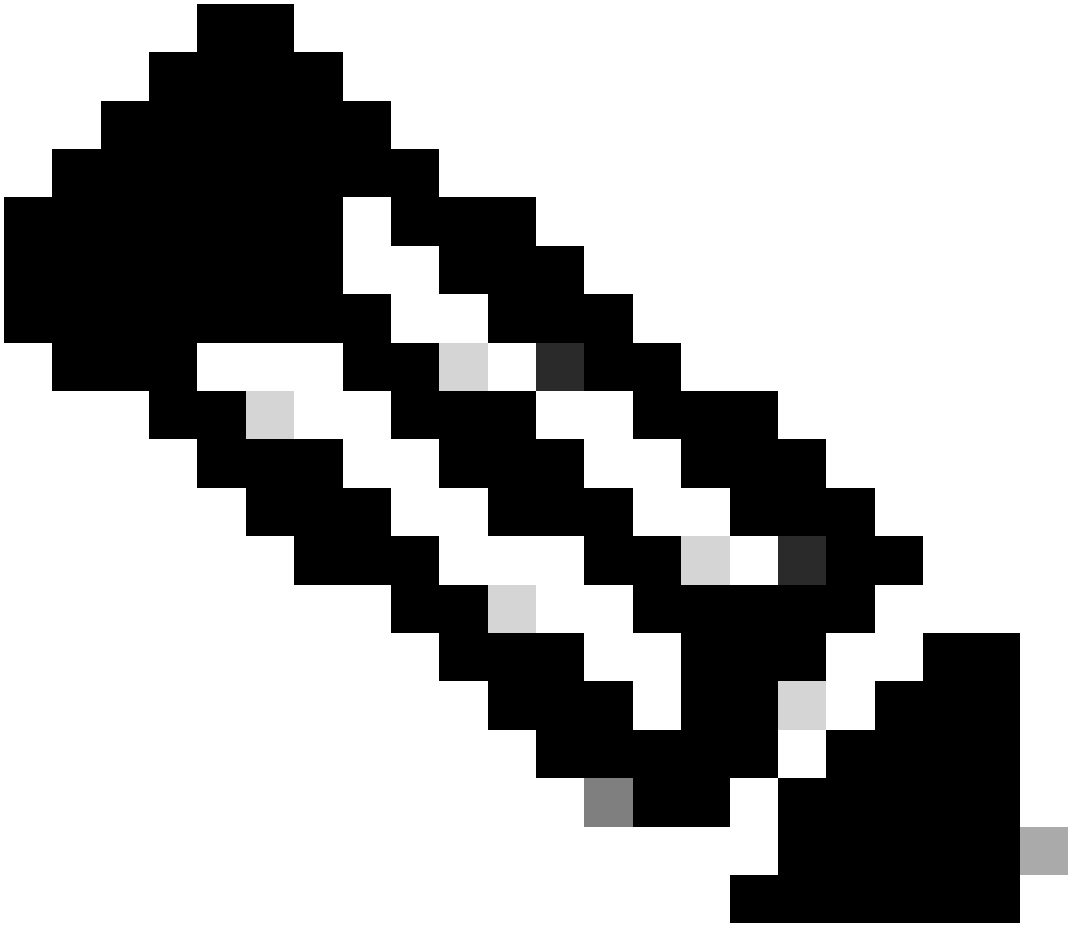
Device Type

Other

Cancel

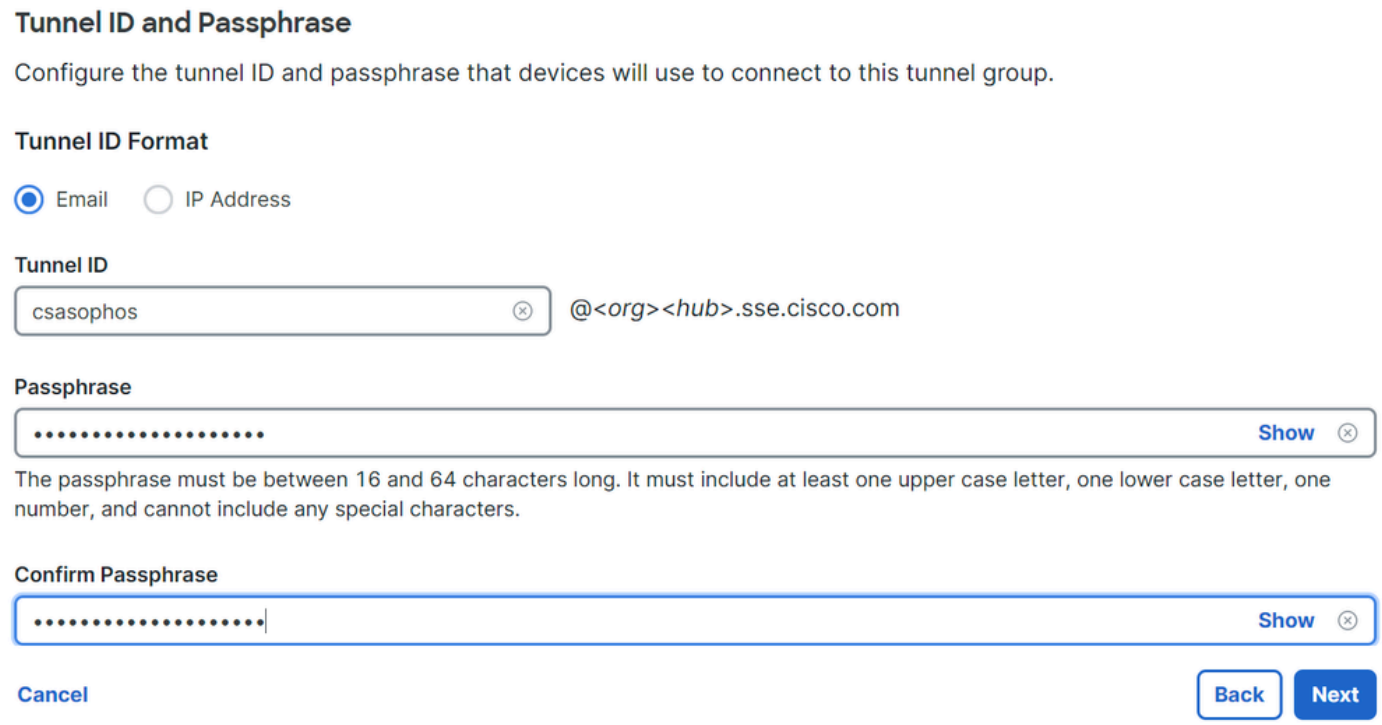
Next

Accesso sicuro - Gruppi di tunnel - Impostazioni generali



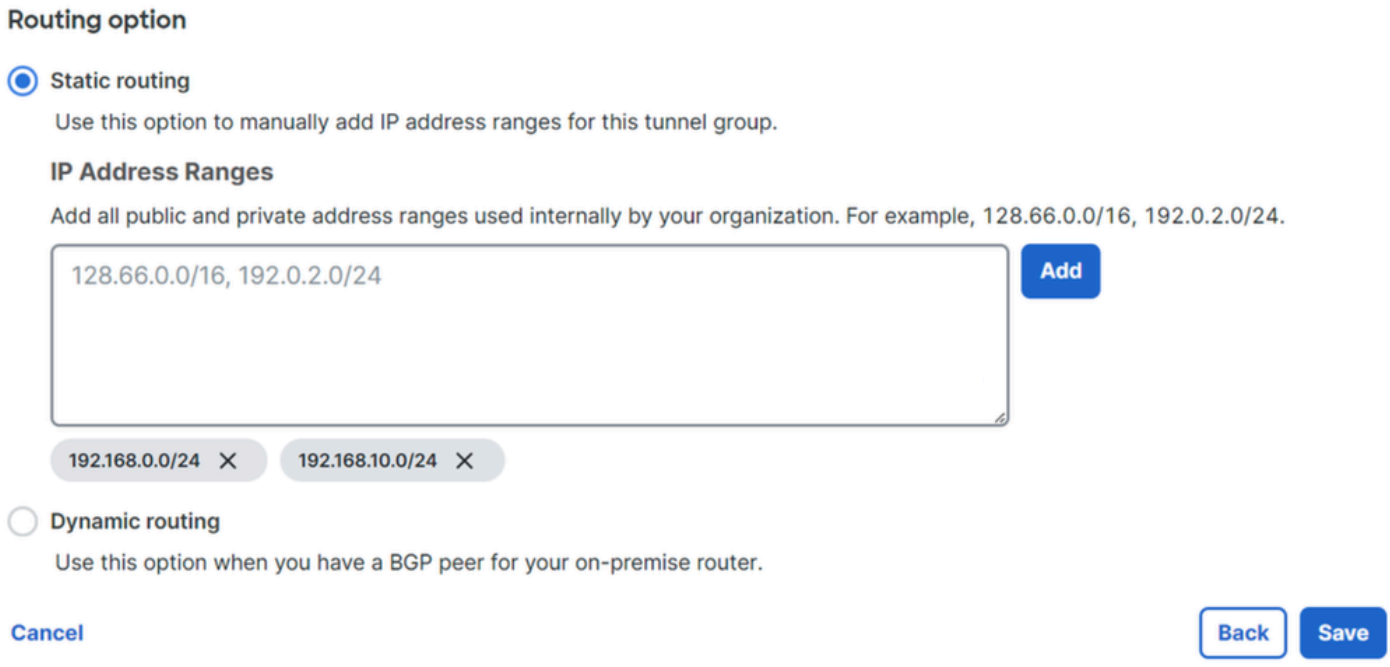
Nota: scegliere la regione più vicina alla posizione del firewall.

- Configurare Tunnel ID Format e Passphrase.
- Fare clic su .Next



Accesso sicuro - Gruppi di tunnel - ID tunnel e passphrase

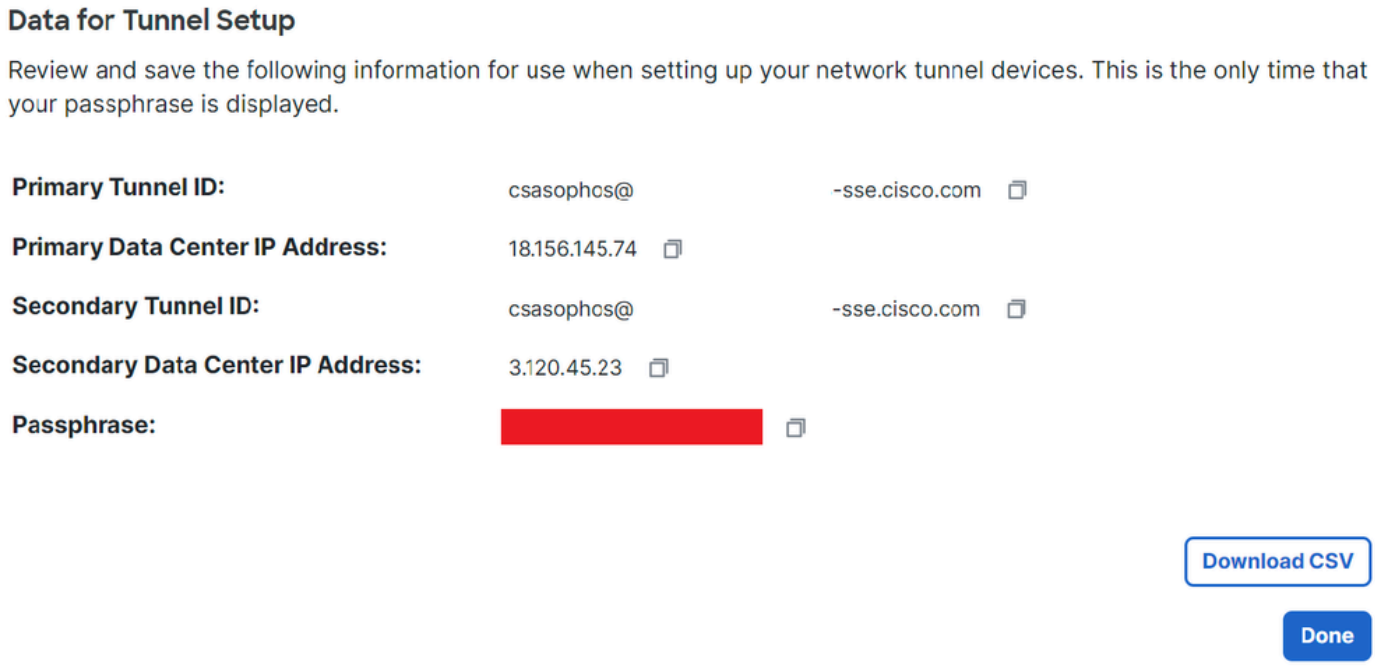
- Configurare gli intervalli di indirizzi IP o gli host configurati nella rete e che si desidera passare il traffico attraverso l'accesso sicuro.
- Fare clic su . **Save**



Accesso sicuro - Gruppi di tunnel - Opzioni di routing

Dopo aver fatto clic sulle informazioni **Save** del tunnel che vengono visualizzate, salvare le informazioni per il passaggio successivo, **Configure the tunnel on Sophos**.

Dati tunnel



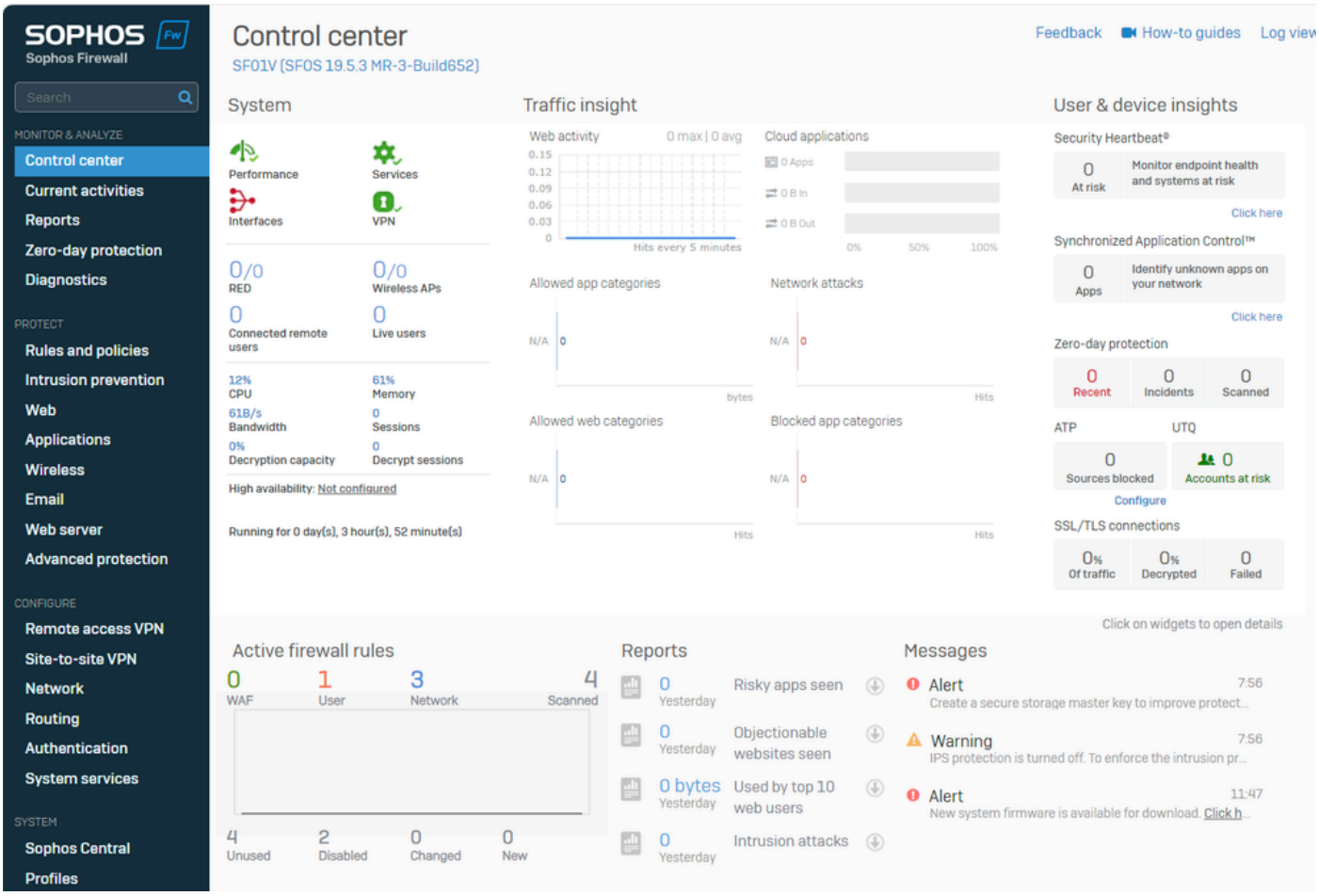
Accesso sicuro - Gruppi di tunnel - Ripresa della configurazione

Configurazione del tunnel su Sophos

Configura profilo IPsec

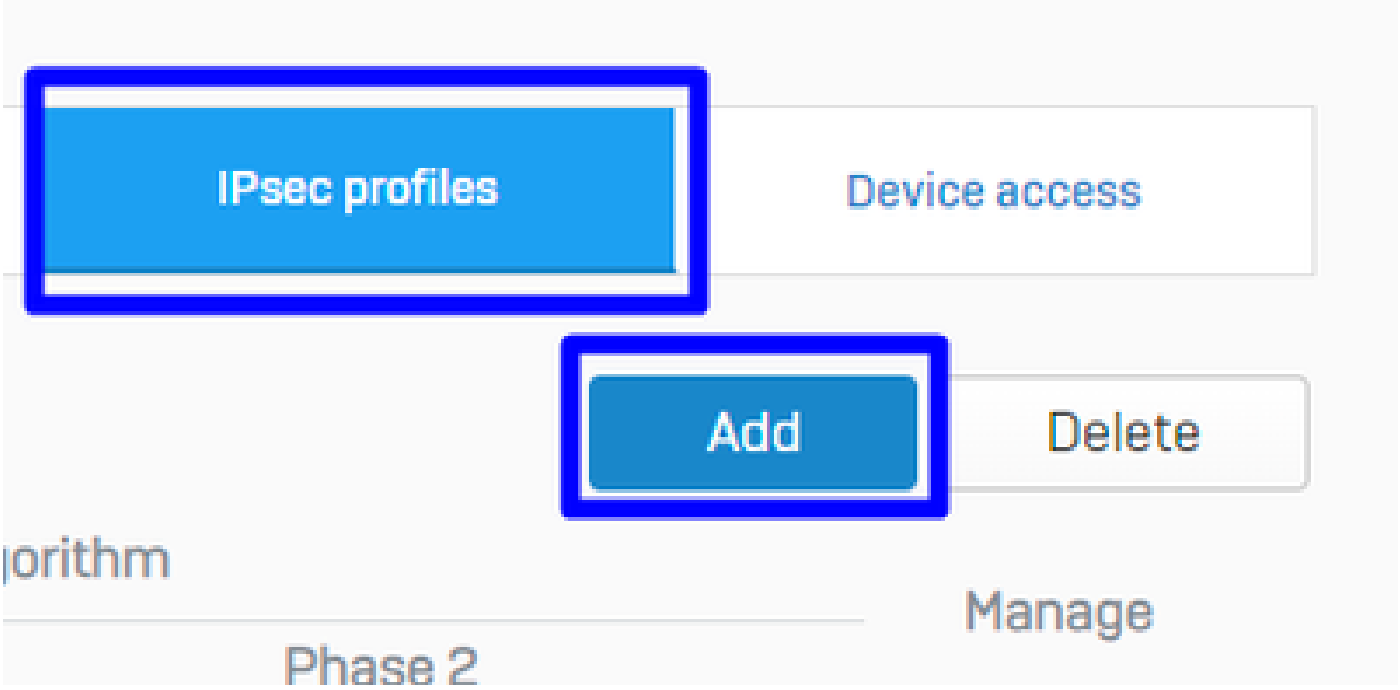
Per configurare il profilo IPsec, passare al firewall Sophos XG.

Si ottiene qualcosa di simile al seguente:



Sophos - Pannello di amministrazione

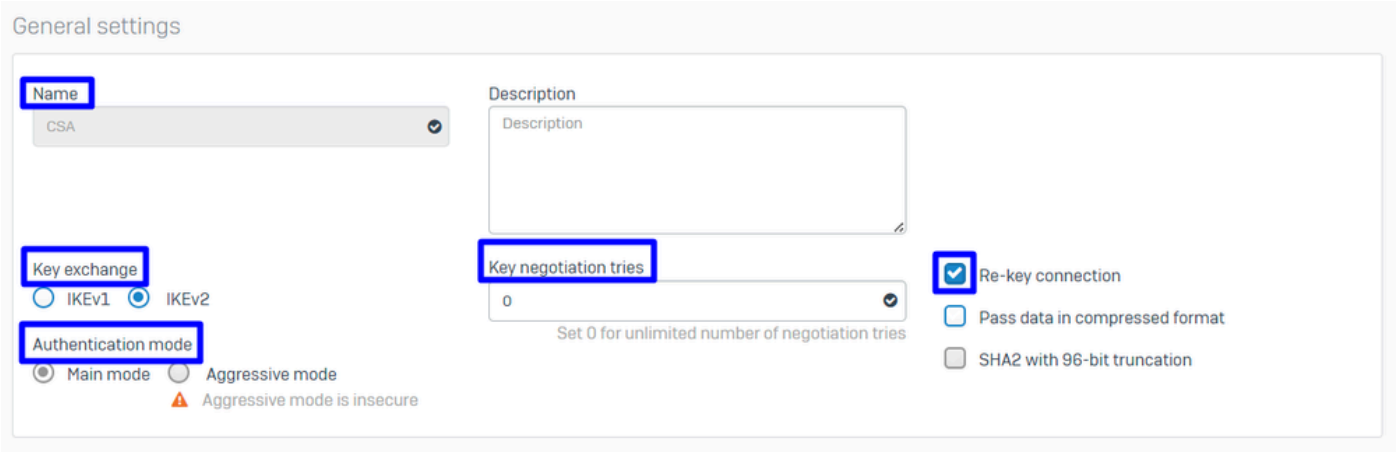
- Passa a Profiles
- Fare clic su **IPsec Profiles** e quindi suAdd



Sophos - Profili IPsec

In **General Settings** Configura:

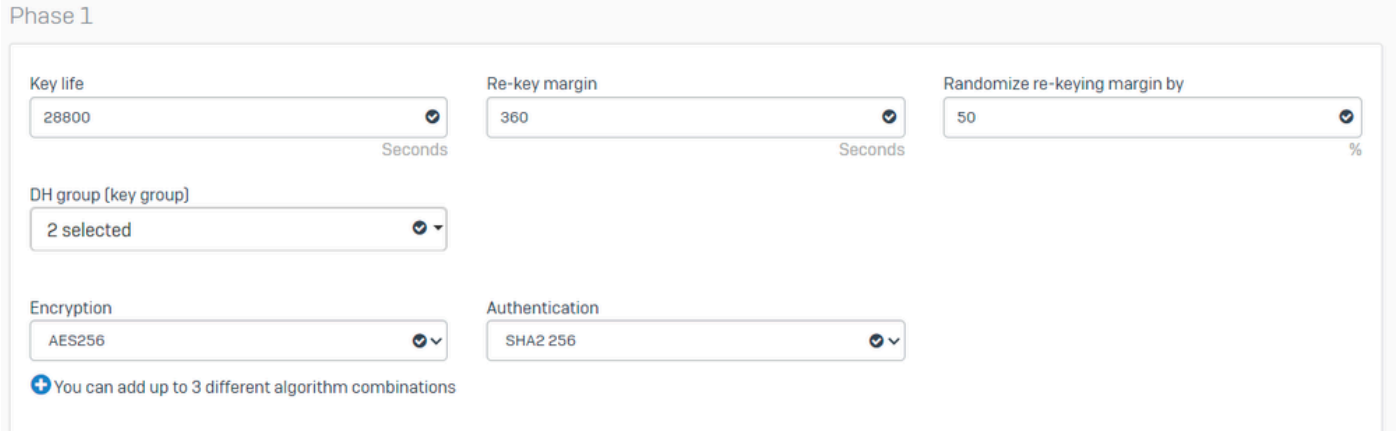
- **Name**: nome di riferimento ai criteri di accesso sicuro Cisco
- **Key Exchange**: IKEv2
- **Authentication Mode**: Modalità principale
- **Key Negotiation Tries**:0
- **Re-Key connection**: selezionare l'opzione



Sophos - Profili IPSec - Impostazioni generali

In **Phase 1** Configura:

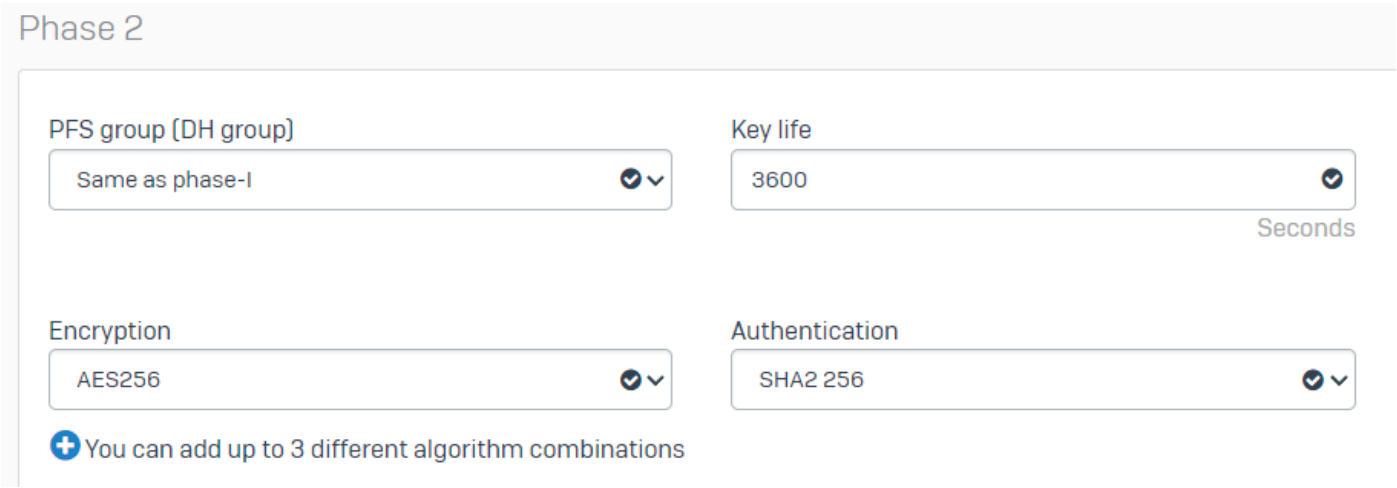
- **Key Life**:28800
- **DH group(key group)**: selezionare 19 e 20
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin: 360 (predefinito)
- **Randomize re-keying margin by**: 50 (predefinito)



Sophos - Profili IPsec - Fase 1

In **Phase 2** Configura:

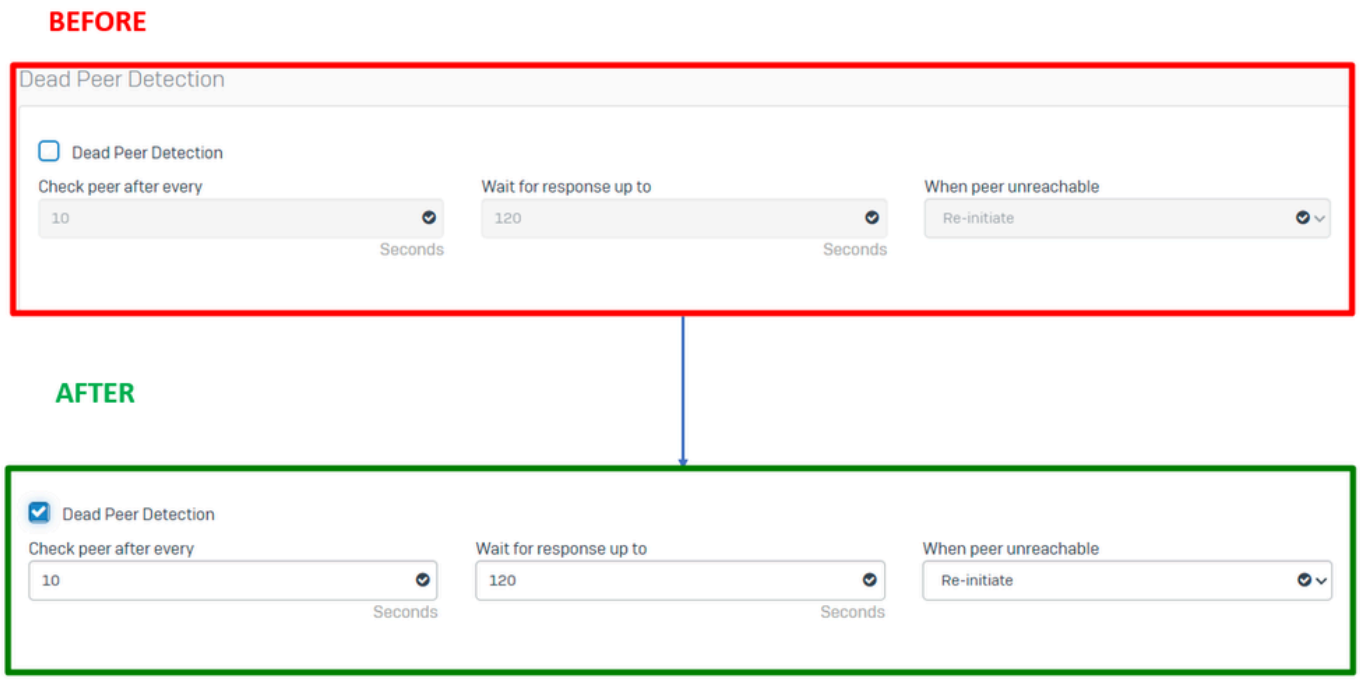
- PFS group (DH group): uguale alla fase I
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256



Sophos - Profili IPsec - Fase 2

In **Dead Peer Detection** Configura:

- **Dead Peer Detection**: selezionare l'opzione
- **Check peer after every**:10
- **Wait for response up to**: 120 (predefinito)
- **When peer unreachable**: riavvio (predefinito)

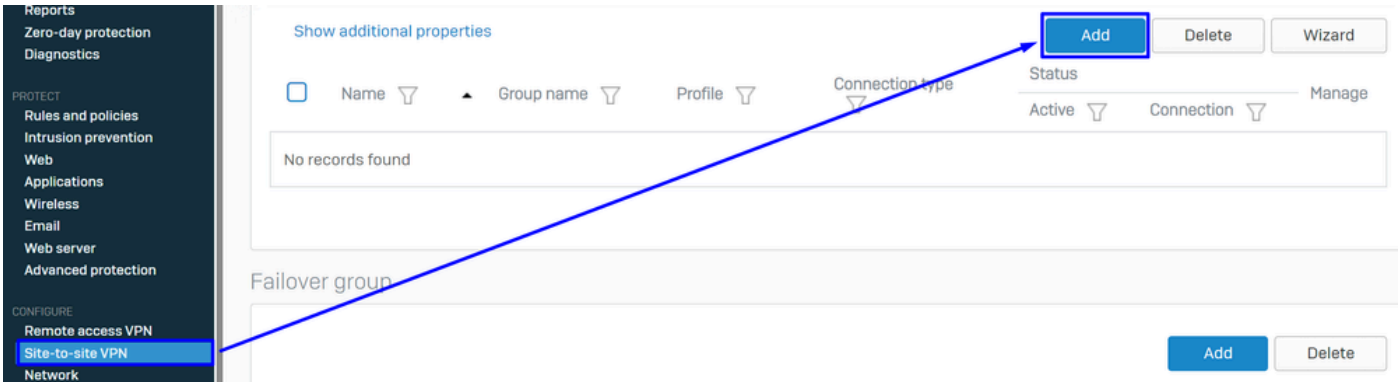


Sophos - Profili IPsec - Rilevamento peer inattivi

Dopodiché, fate clic su **Save** and proceed with the next step, Configure Site-to-site VPN.

Configura VPN da sito a sito

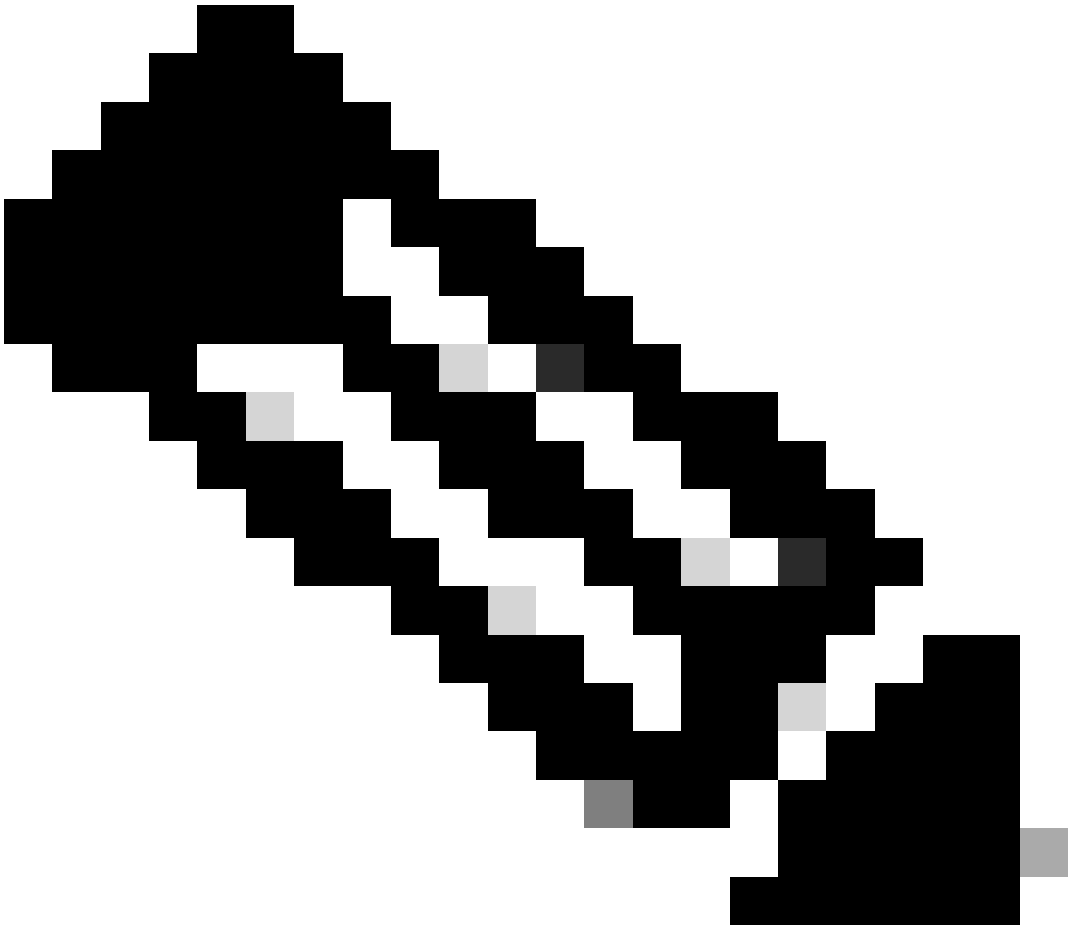
Per avviare la configurazione della VPN, fare clic su **Site-to-site VPN** e su **Add**.



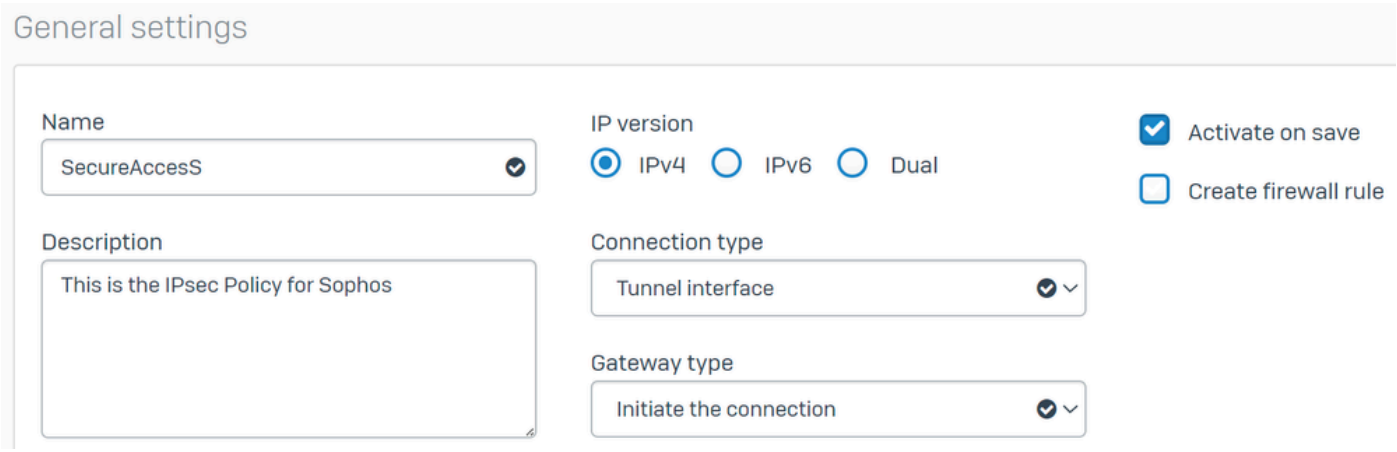
Sophos - VPN da sito a sito

In **General Settings** Configura:

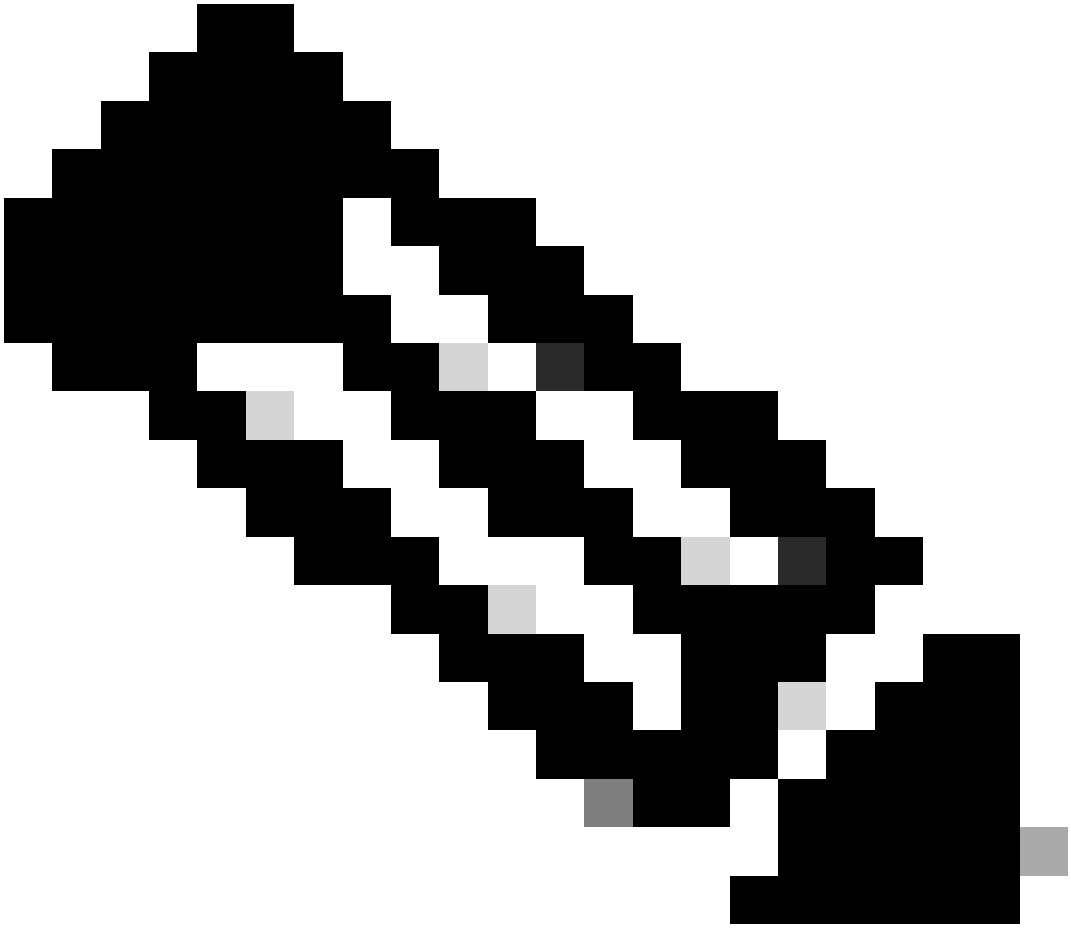
- **Name**: nome di riferimento al criterio IPsec di Cisco Secure Access
- IP version:IPv4
- Connection type: Interfaccia tunnel
- Gateway type: avvia la connessione
- Active on save: selezionare l'opzione



Nota: l'opzione **Active on save** abilita la VPN automaticamente dopo la configurazione della VPN da sito a sito.



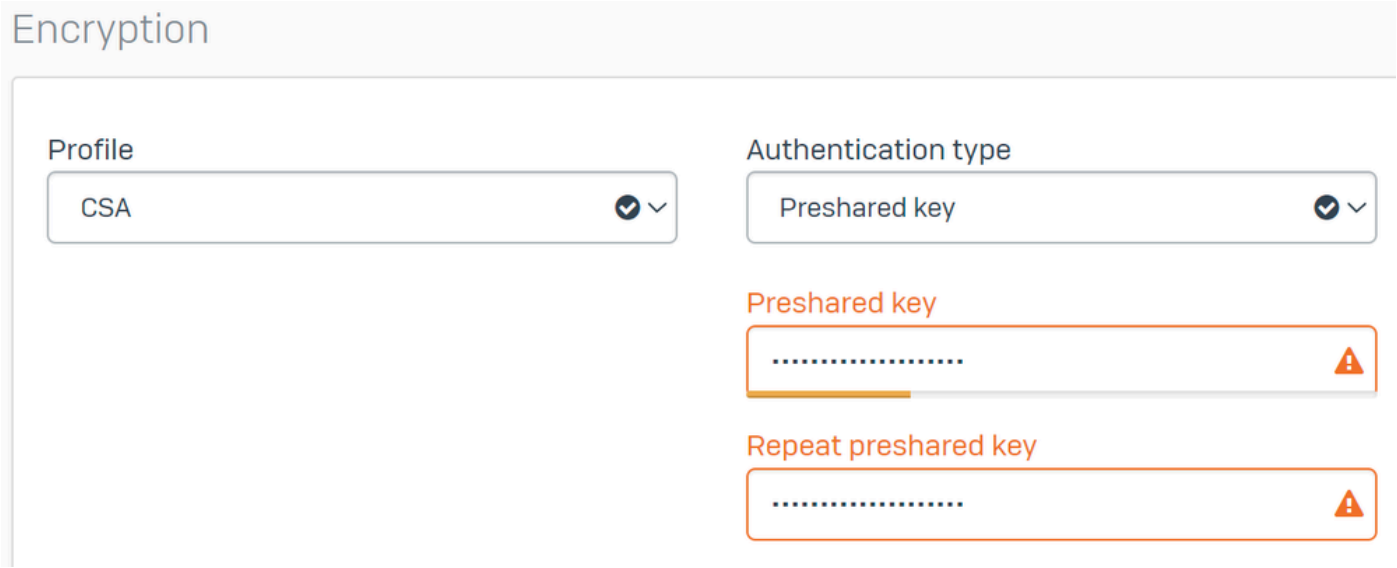
Sophos - VPN da sito a sito - Impostazioni generali



Nota: l'opzione Tunnel interface (interfaccia tunnel) crea un'interfaccia tunnel virtuale per il firewall Sophos XG con il nome XFRM.

In **Encryption** Configura:

- **Profile**: il profilo creato sulla fase, **Configure IPsec Profile**
- **Authentication type**: chiave già condivisa
- **Preshared key**: il tasto che si configura nella fase, Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**

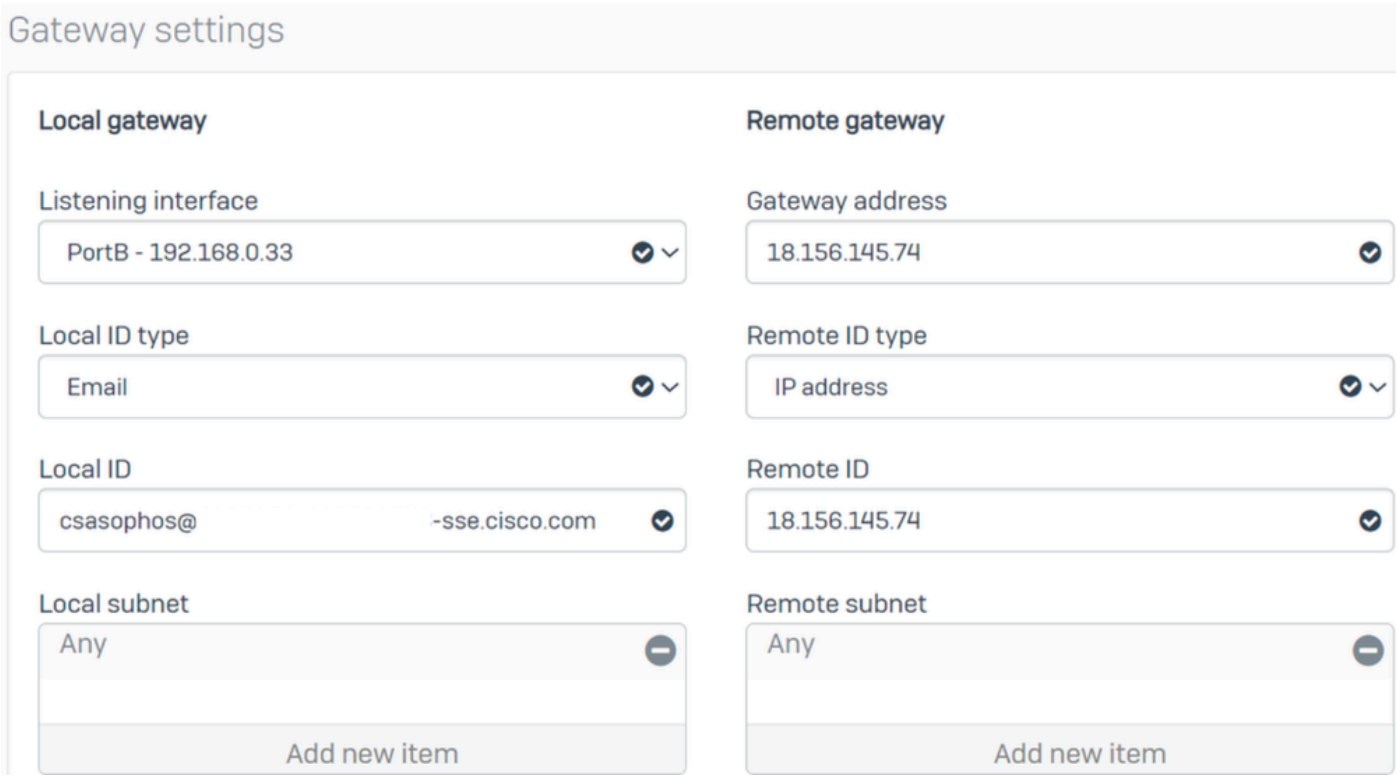


Sophos - VPN da sito a sito - Crittografia

In **Gateway Settings** Configura opzioni Local Gatewaye Remote Gateway utilizzare questa tabella come riferimento.

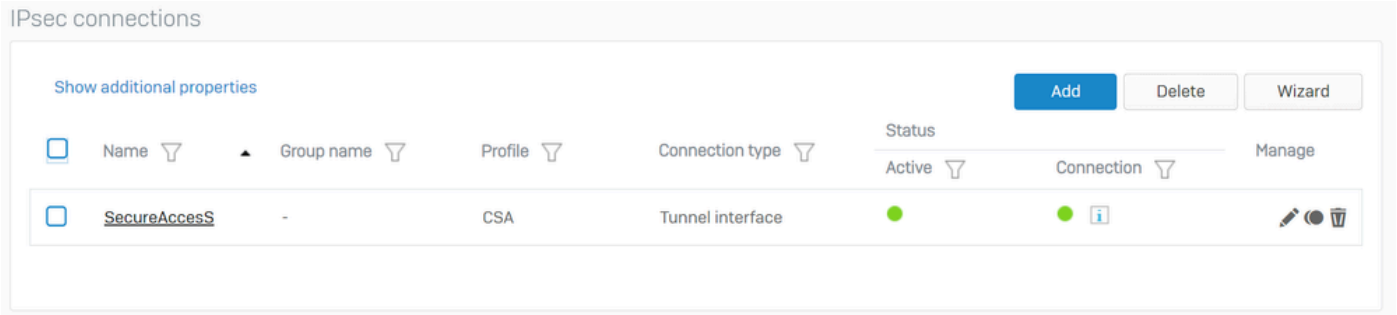
Gateway locale	Gateway remoto
Interfaccia di ascolto Interfaccia Wan-Internet	Indirizzo gateway L'indirizzo IP pubblico generato nella fase, **Tunnel Data**
Tipo ID locale Email	Tipo ID remoto

	Indirizzo IP
ID locale L'e-mail generata nella fase, Tunnel Data	ID remoto L'indirizzo IP pubblico generato nella fase, Tunnel Data
Subnet locale Qualsiasi	Subnet remota Qualsiasi

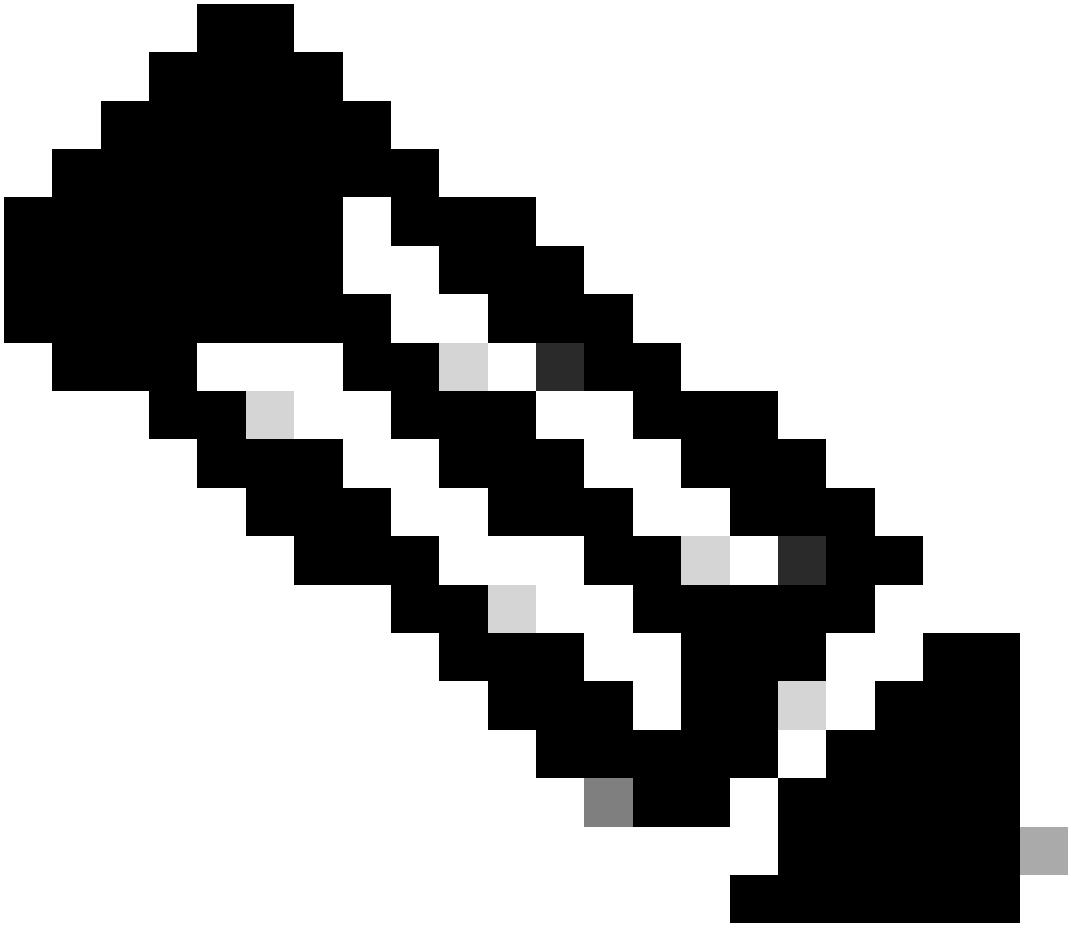


Sophos - VPN da sito a sito - Impostazioni gateway

Dopodiché, fare clic su **Save**, e si può vedere che il tunnel è stato creato.

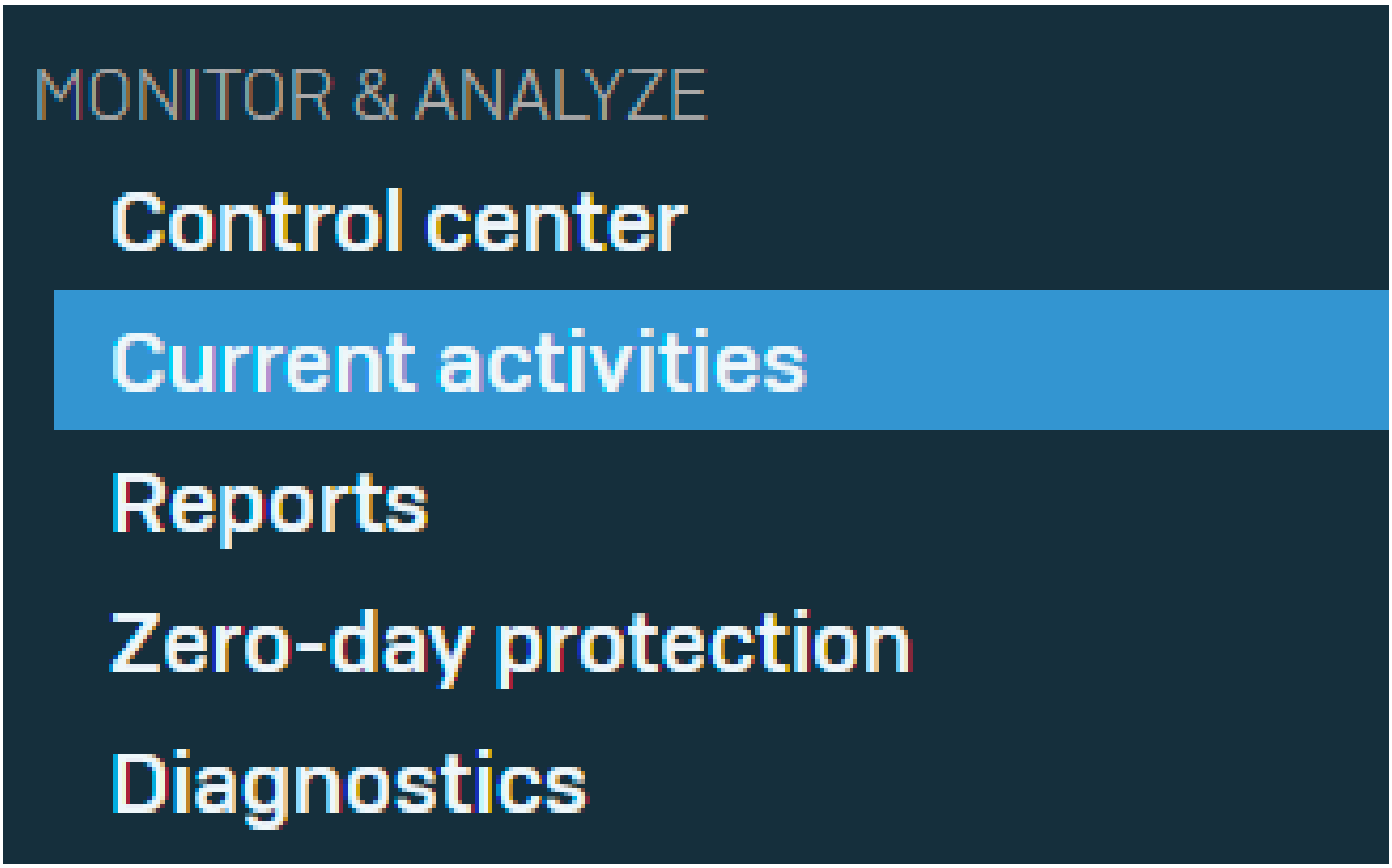


Sophos - VPN da sito a sito - Connessioni IPsec

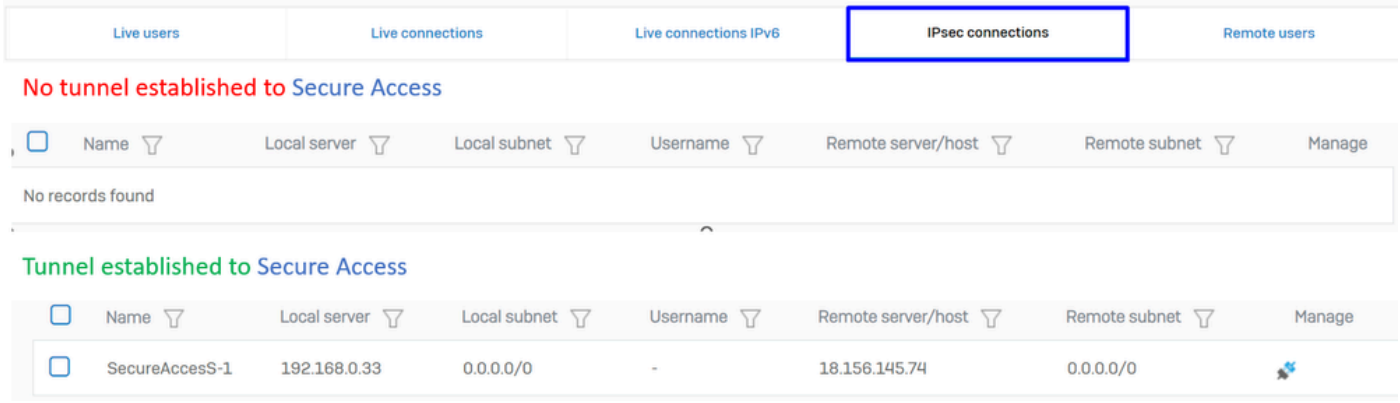


Nota: per verificare se il tunnel è stato abilitato correttamente sull'ultima immagine, è possibile controllare **Connection** lo stato. Se il colore è verde, il tunnel è connesso se non è verde e il tunnel non è connesso.

Per verificare se è stato stabilito un tunnel, passare a **Current Activities > IPsec Connections**.



Sophos - Monitoraggio e analisi - IPsec



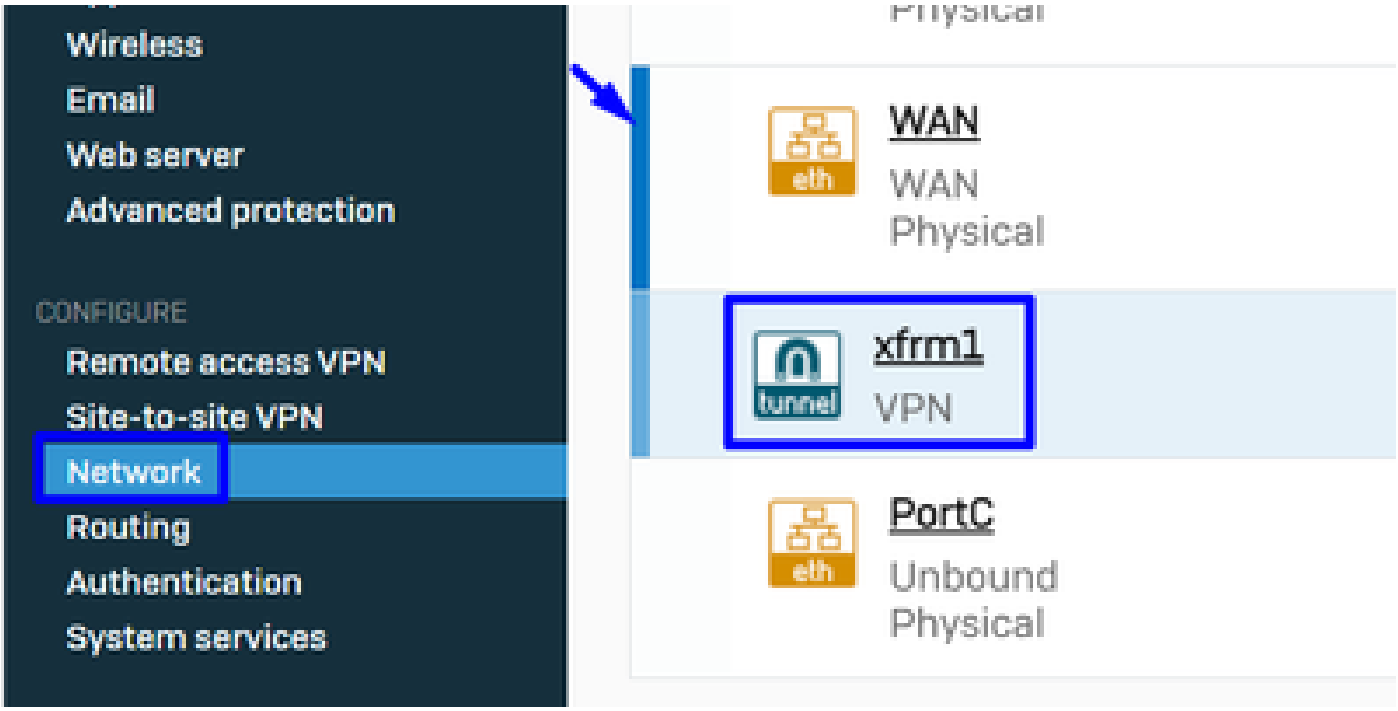
Sophos - Monitoraggio e analisi - IPSec prima e dopo

Dopo di che, possiamo continuare con il passo, **Configure Tunnel Interface Gateway**.

Configura interfaccia tunnel

Individuare l'interfaccia configurata sulla VPN **Network** e controllarla perWAN modificare l'interfaccia del tunnel virtuale con il nome xfrm.

- Fare clic su nell'**xfrm** interfaccia.



Sophos - Rete - Interfaccia tunnel

- Configurare l'interfaccia con un IP non instradabile nella rete. Ad esempio, è possibile usare 169.254.x.x/30 che è un IP in uno spazio non instradabile. In genere, nell'esempio riportato viene usato 169.254.0.1/30

Sophos - Rete - Interfaccia tunnel - Configurazione

Configurazione dei gateway

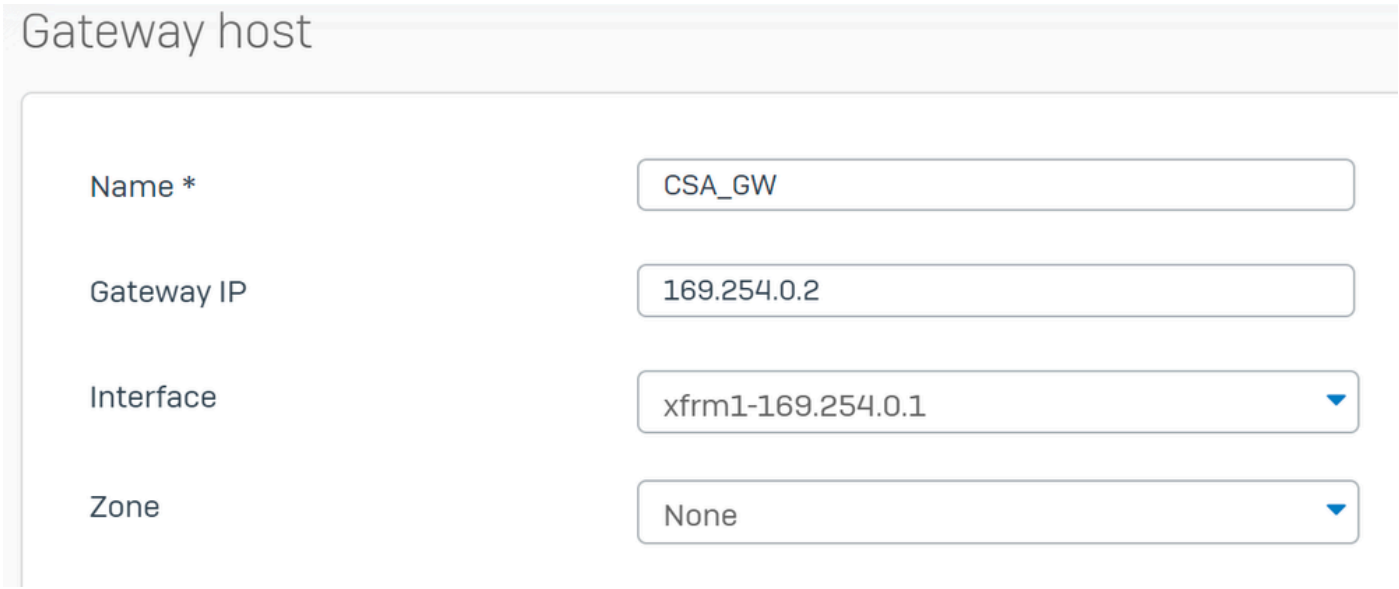
Per configurare il gateway per l'interfaccia virtuale (xfrm)

- Passa a Routing > Gateways
- Fare clic su Add

Sophos - Routing - Gateway

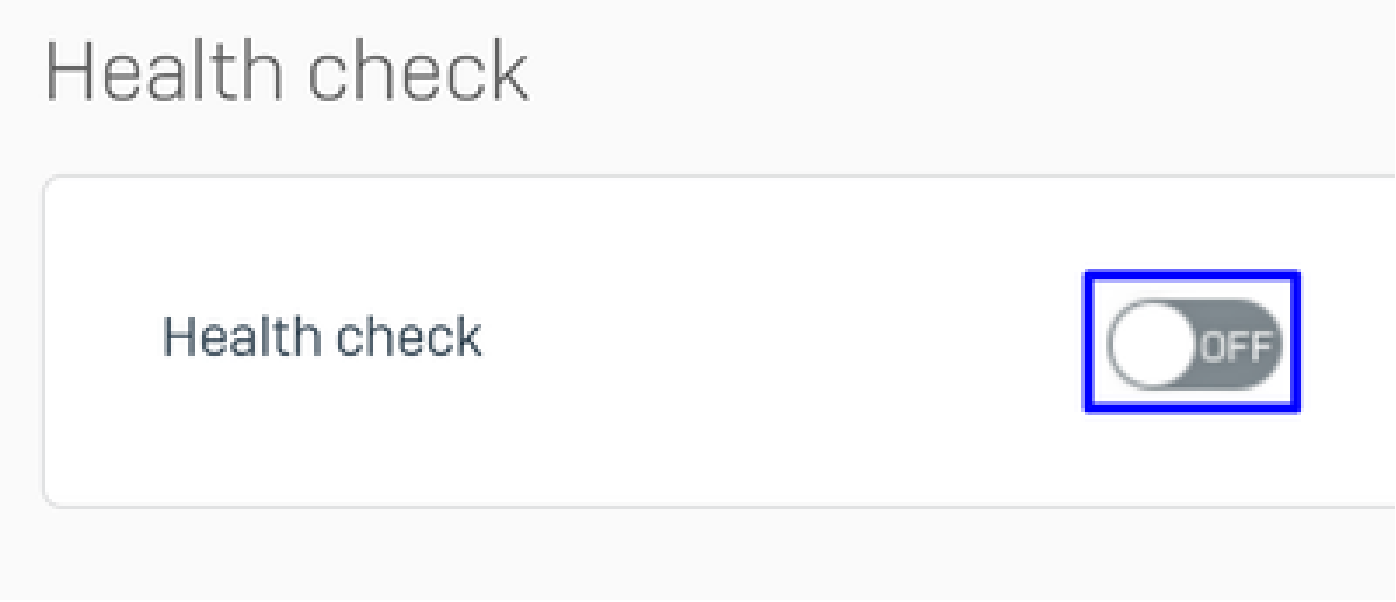
In **Gateway host** Configura:

- **Name**: nome che fa riferimento all'interfaccia virtuale creata per la VPN
- **Gateway IP**: nel nostro caso 169.254.0.2, ossia l'IP sotto la rete 169.254.0.1/30 che già abbiamo assegnato sotto la fase, Configure Tunnel Interface
- Interface: Interfaccia virtuale VPN
- **Zone**: Nessuno (predefinito)



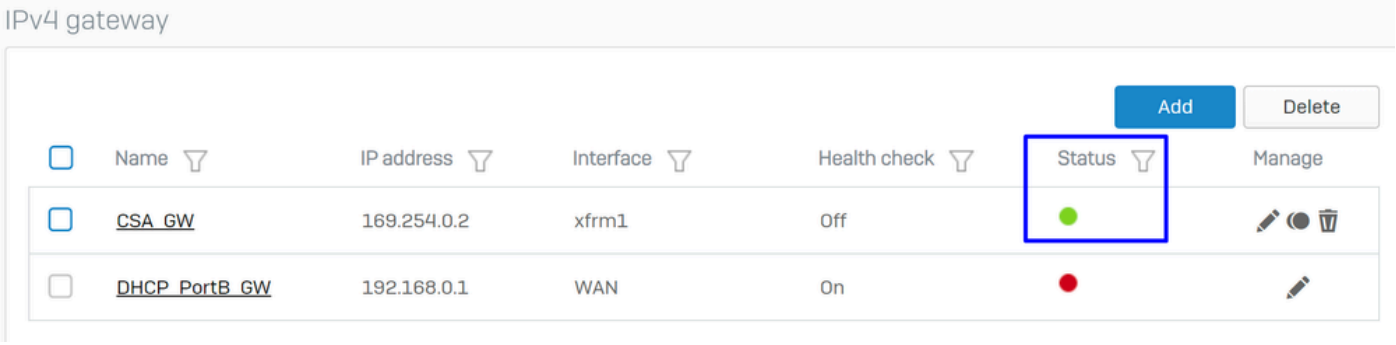
Sophos - Routing - Gateway - Host gateway

- Sotto **Health check** disattiva controllo
- Fare clic su **Save**



Sophos - Routing - Gateway - Controllo dello stato

Dopo aver salvato la configurazione, è possibile osservare lo stato del gateway:



Sophos - Routing - Gateway - Stato

Configurazione del router SD-WAN

Per finalizzare il processo di configurazione, è necessario creare il percorso che consente di inoltrare il traffico a Secure Access.

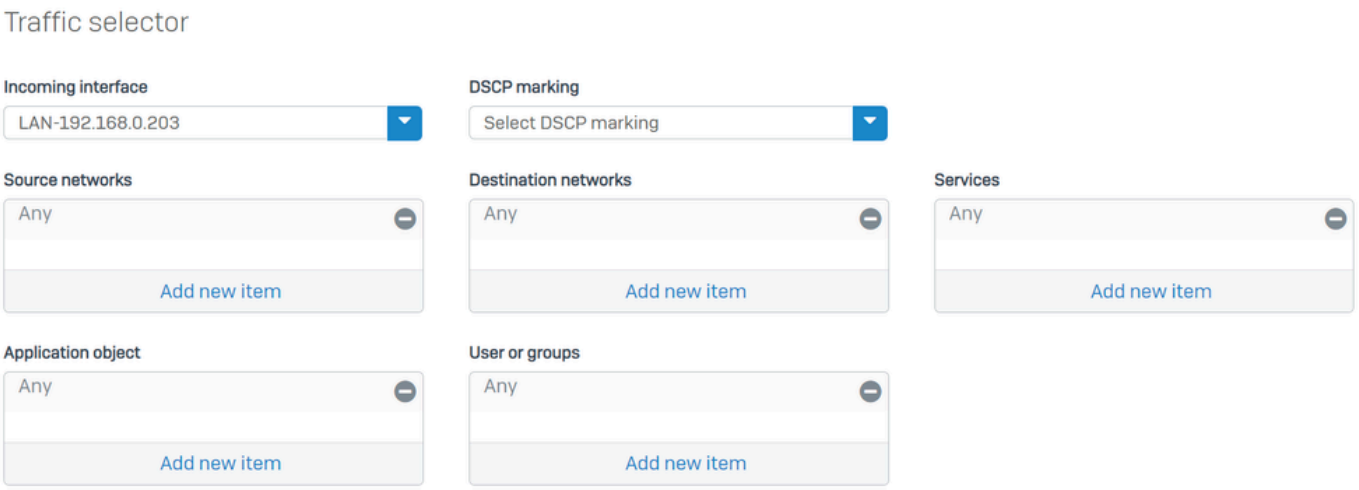
Passa a **Routing > SD-WAN routes.**

- Fare clic su **Add**

Sophos - Router SD-Wan

In **Traffic Selector** Configura:

- Incoming interface: selezionare l'interfaccia da cui inviare il traffico o gli utenti che accedono da RA-VPN, ZTNA o Clientless-ZTNA
- DSCP marking: nessuna informazione per questo esempio
- **Source networks**: selezionare l'indirizzo che si desidera indirizzare attraverso il tunnel
- **Destination networks**: qualsiasi o è possibile specificare una destinazione
- **Services**: qualsiasi o è possibile specificare i servizi
- **Application object**: applicazione se l'oggetto è stato configurato
- User or groups: se si desidera aggiungere un gruppo specifico di utenti per indirizzare il traffico ad Accesso sicuro

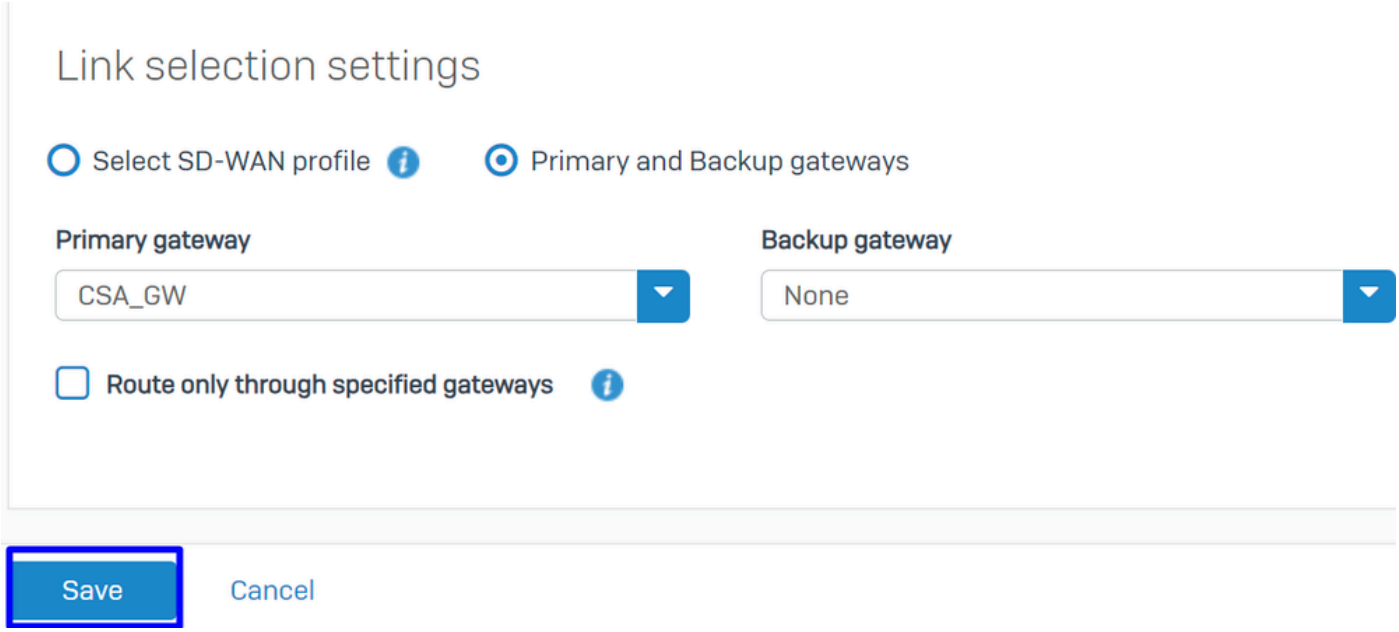


Sophos - Route SD-Wan - Selettore traffico

In **Link selection settings** Configurazione gateway:

- Primary and Backup gateways: selezionare l'opzione

- **Primary gateway**: selezionare il gateway configurato nella fase, Configure the Gateways
- Fare clic su **Save**



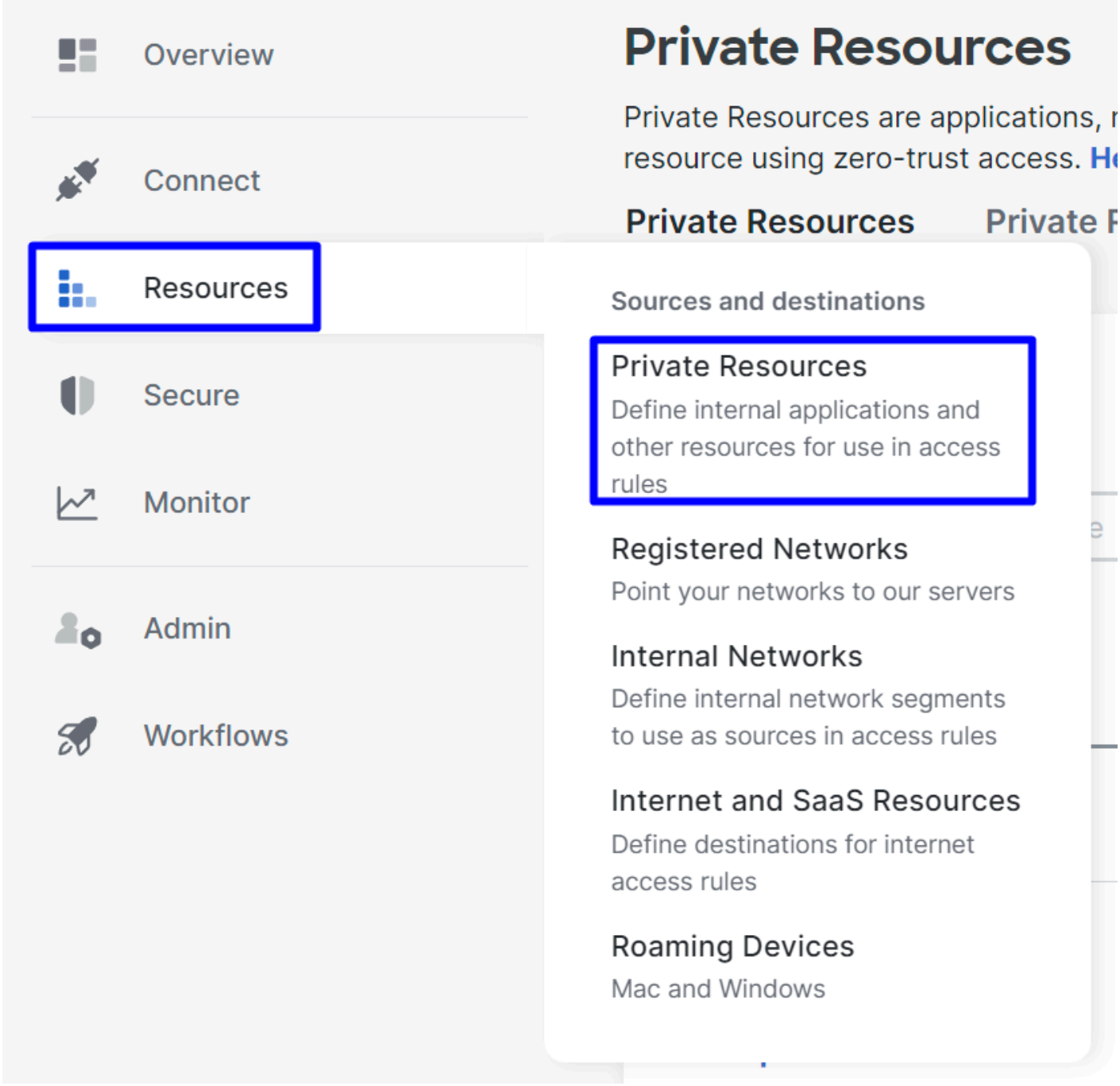
Sophos - Route SD-Wan - Selettore traffico - Gateway principali e di backup

Dopo aver finalizzato la configurazione sul Sophos XG Firewall, è possibile procedere con la procedura, **Configure Private App.**

Configura app privata

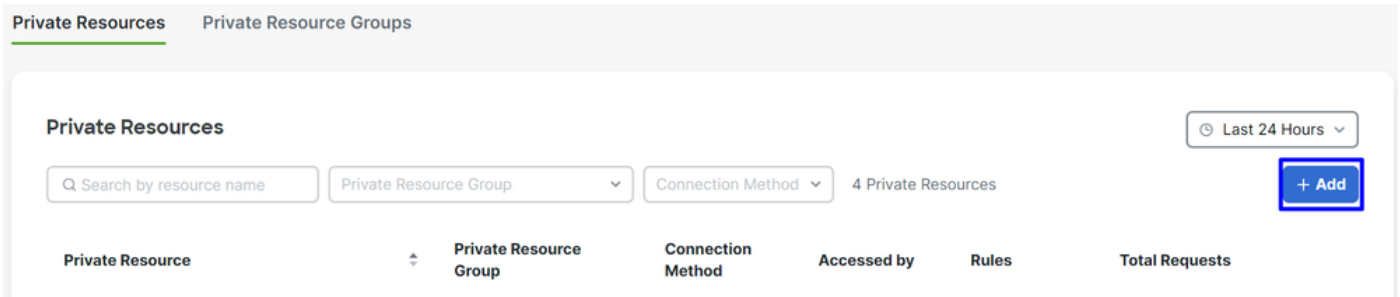
Per configurare l'accesso all'app privata, accedere al portale di amministrazione.

- Passa a **Resources > Private Resources**



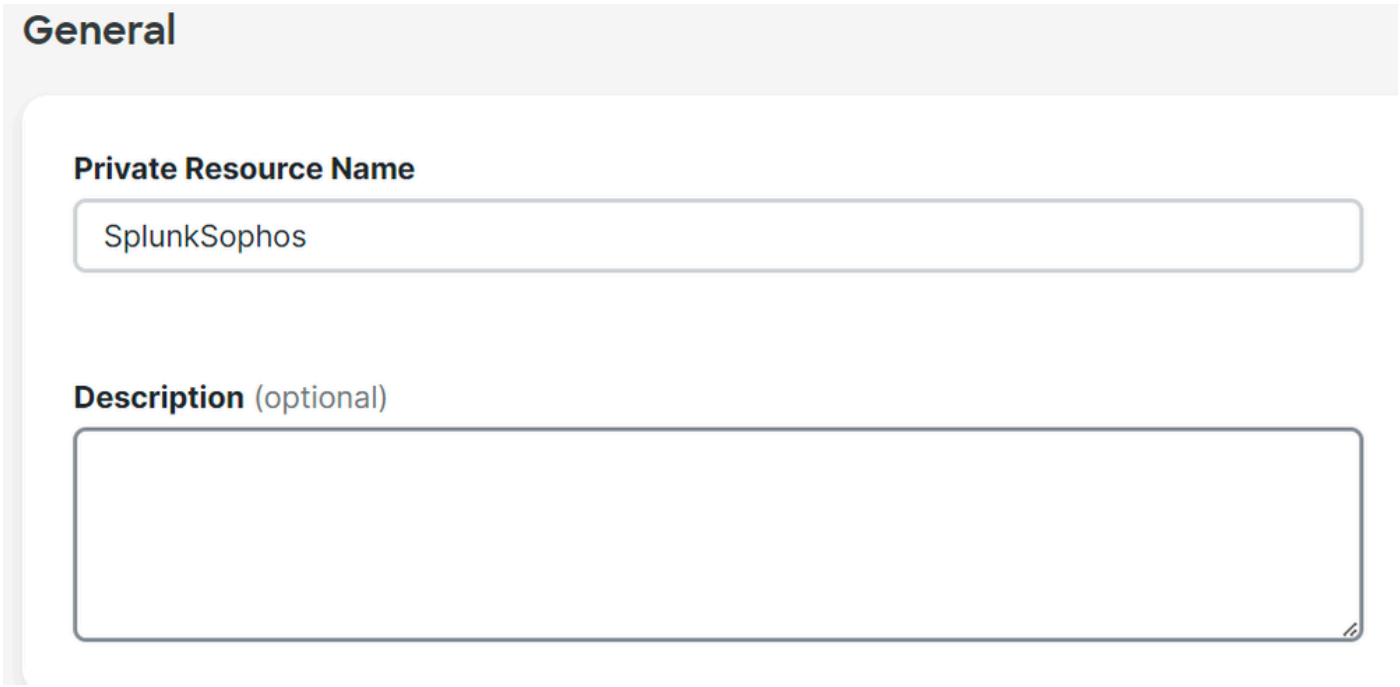
Accesso sicuro - Risorse private

- Fare clic su + Add



Accesso sicuro - Risorse private 2

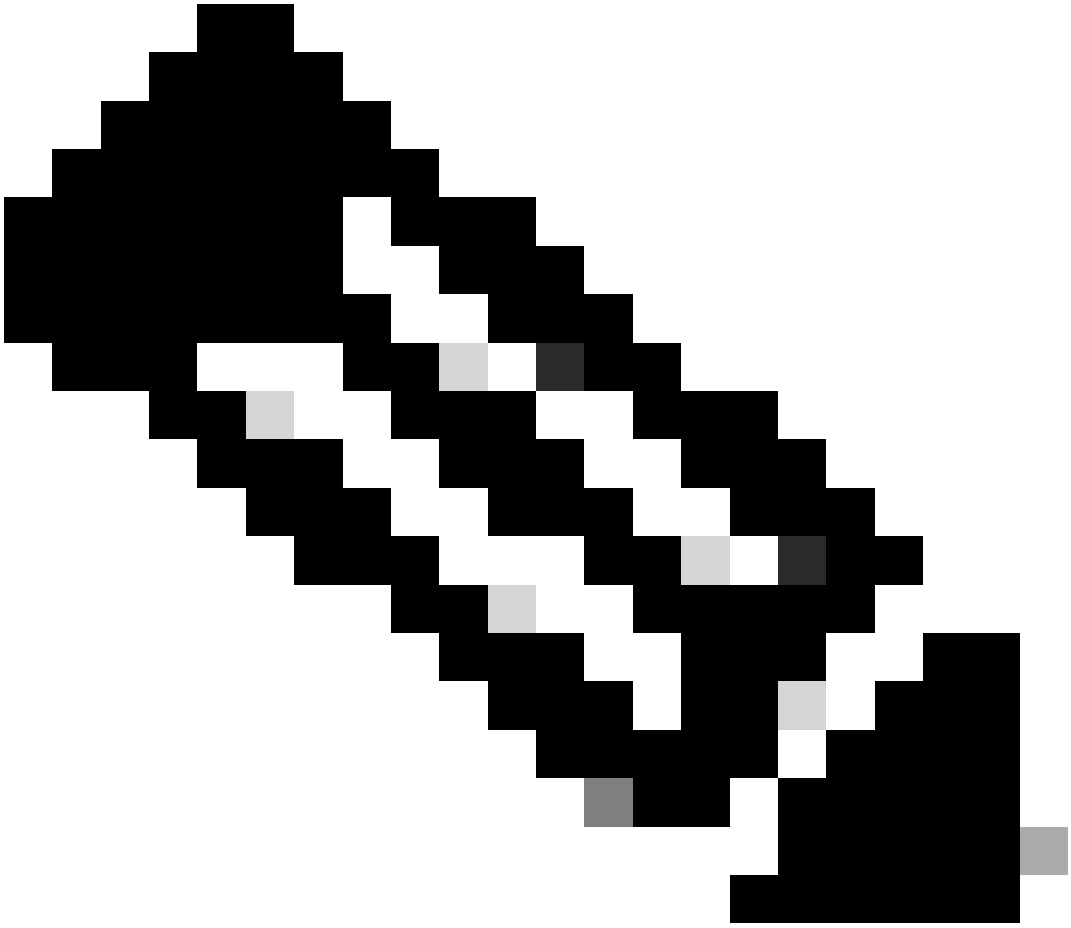
- In **General** Configurazione **Private Resource Name**



Accesso sicuro - Risorse private - Generale

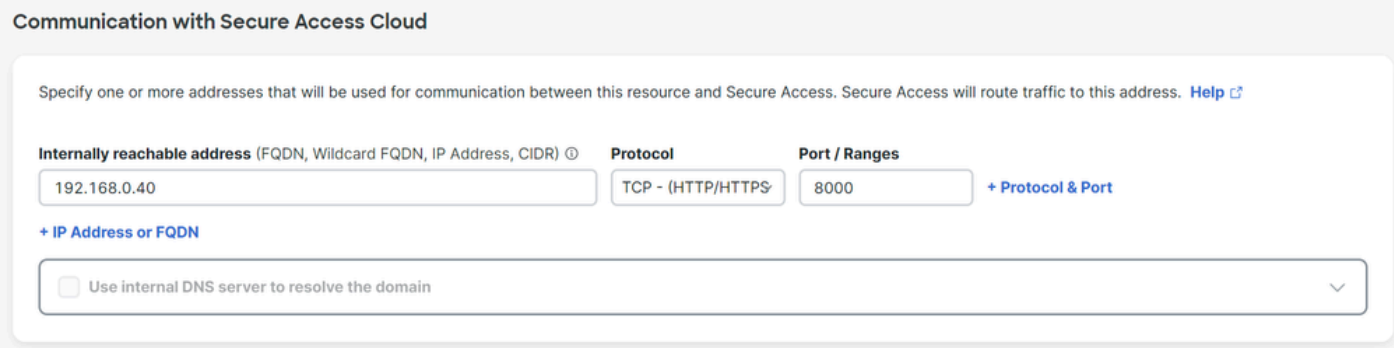
In **Communication with Secure Access Cloud** Configura:

- I**nternally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: selezionare la risorsa a cui si desidera accedere



Nota: ricordare che l'indirizzo raggiungibile internamente è stato assegnato nella fase, **Configure the Tunnel on Secure Access**.

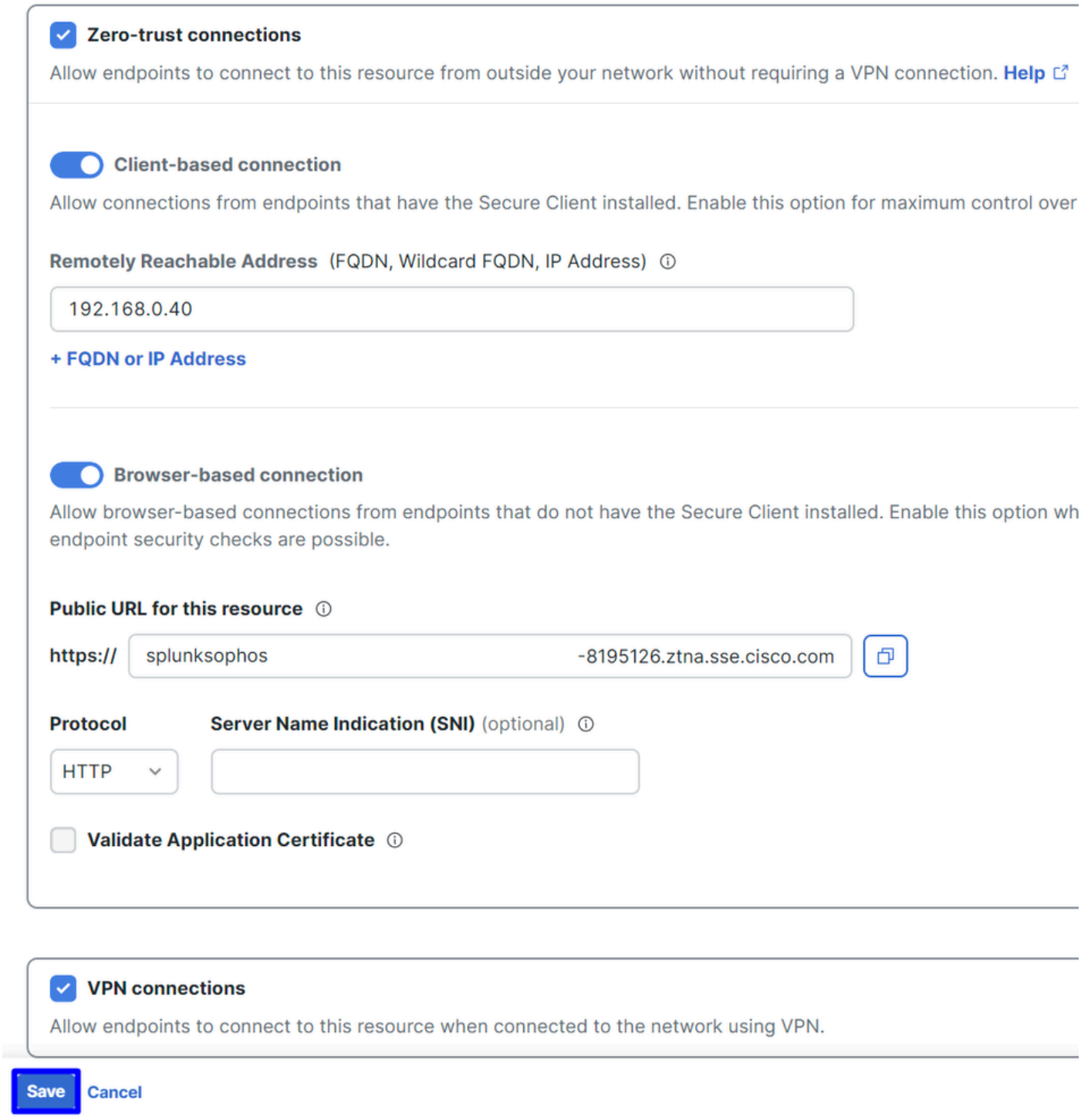
- **Protocol**: selezionare il protocollo da utilizzare per accedere alla risorsa
- Port / Ranges : selezionare le porte da abilitare per accedere all'app



Accesso sicuro - Risorse private - Comunicazioni con Secure Access Cloud

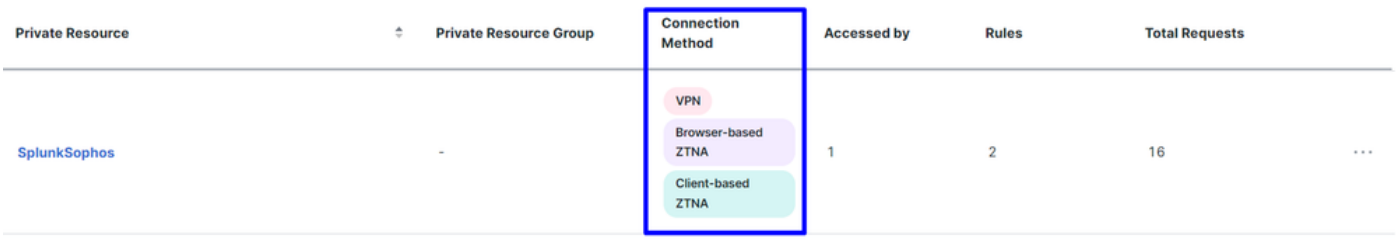
All'interno **Endpoint Connection Methods** di è possibile configurare tutte le modalità di accesso alle risorse private tramite Secure Access e scegliere i metodi che si desidera utilizzare per l'ambiente:

- **Zero-trust connections**: selezionare la casella per abilitare l'accesso ZTNA.
    - **Client-based connection**: Abilita il pulsante per consentire l'utilizzo di ZTNA di base client
        - **Remotely Reachable Address**: configurare l'indirizzo IP dell'app privata
    - **Browser-based connection**: Abilita il pulsante per consentire l'utilizzo di ZTNA basato su browser
        - Public URL for this resource: aggiungere un nome da utilizzare insieme al dominio ztna.sse.cisco.com
            - Protocol: scegliere HTTP o HTTPS come protocollo a cui accedere tramite il browser
    - **VPN connections**: selezionare la casella per abilitare l'accesso RSA-VPN.
- Fare clic su **Save**



Accesso sicuro - Risorse private - Comunicazioni con Secure Access Cloud 2

Al termine della configurazione, si ottiene quanto segue:

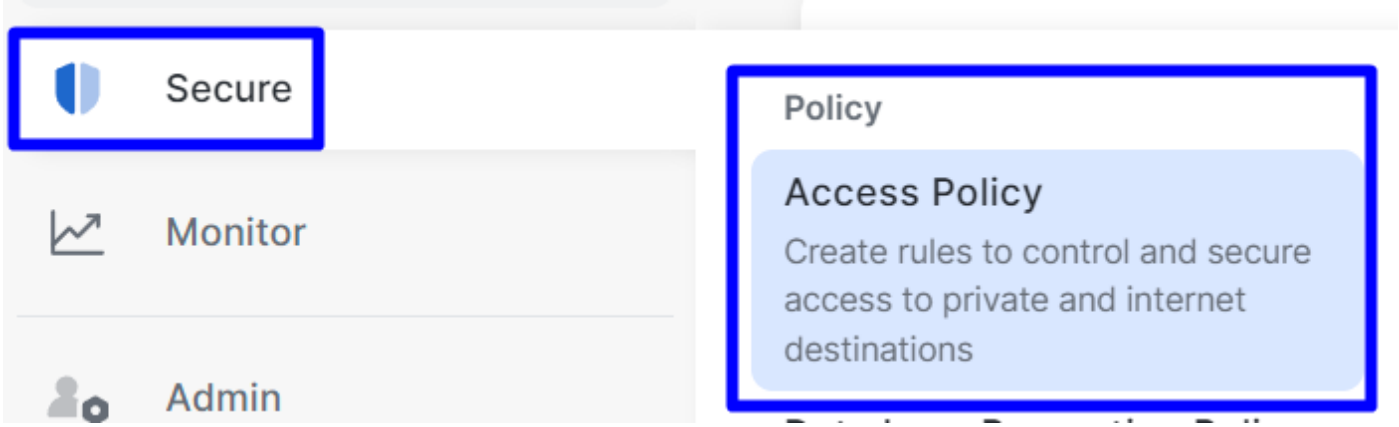


Accesso sicuro - Risorse private configurate

A questo punto è possibile procedere con il passaggio, **Configure the Access Policy**.

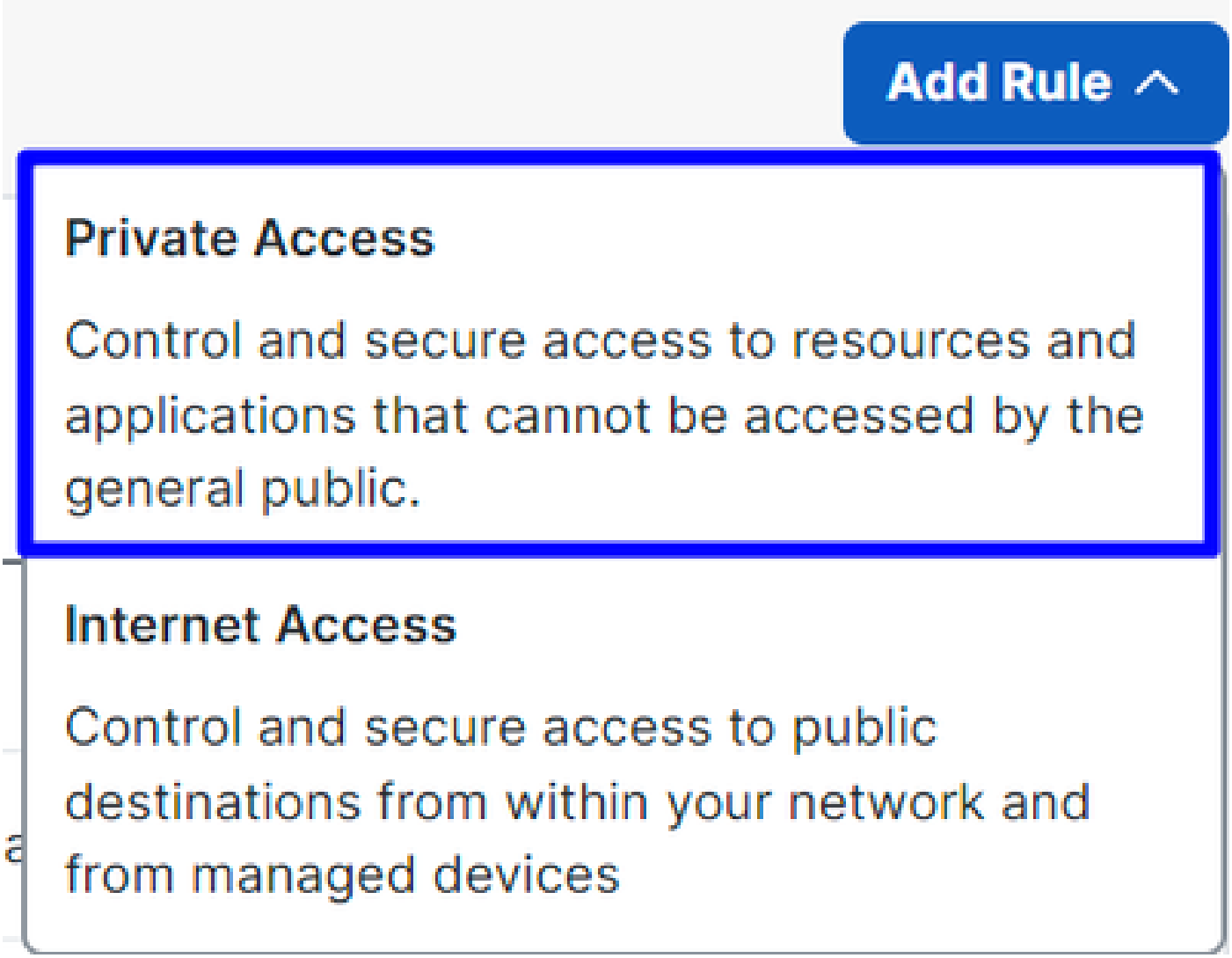
Configurare i criteri di accesso

Per configurare i criteri di accesso, passare a Secure > Access Policy.



Accesso sicuro - Criteri di accesso

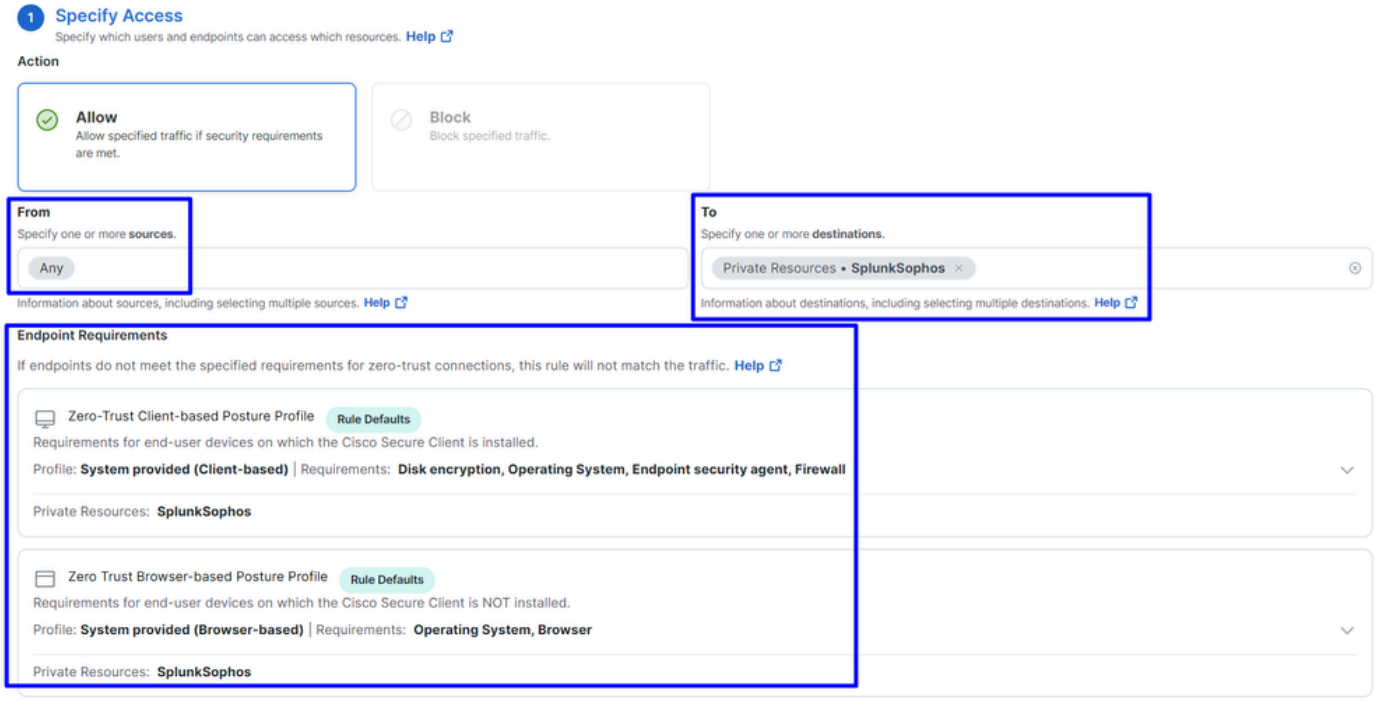
- Fare clic su **Add Rule > Private Access**



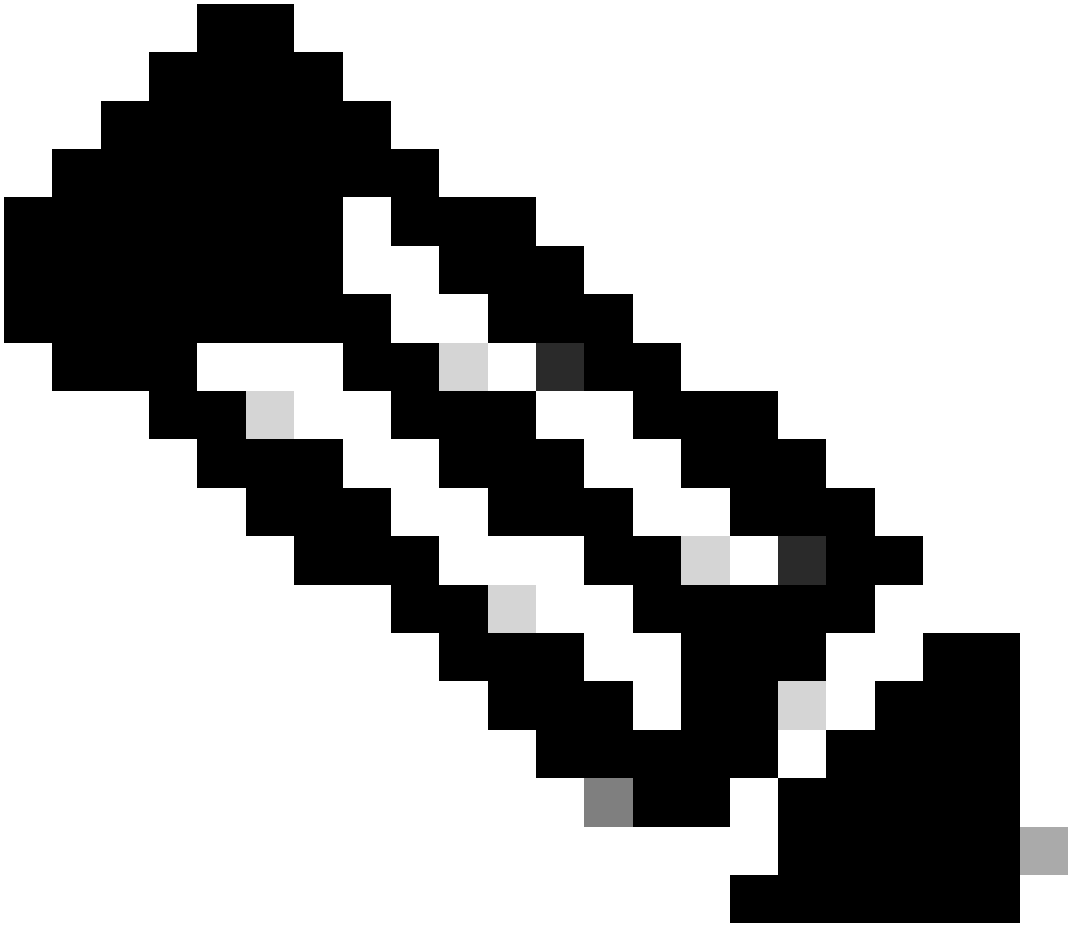
Accesso sicuro - Criteri di accesso - Accesso privato

Configurare le opzioni successive per consentire l'accesso tramite più metodi di autenticazione:

- 1. Specify Access
    - Action:Allow (Autorizza)
        - **Rule name**: specificare un nome per la regola di accesso
        - **From**: gli utenti a cui si concede l'accesso
        - **To**: applicazione alla quale si desidera consentire l'accesso
        - Endpoint Requirements: (predefinito)
- Fare clic su **Next**



Accesso sicuro - Criteri di accesso - Specifica accesso



Nota: per il passaggio **2. Configure Security** in base alle esigenze, ma in questo caso non è stato abilitato il **Intrusion Prevention (IPS)**, o **Tenant Control Profile**.

- Fare clic su Save per:

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

Accesso protetto - Criteri di accesso configurati

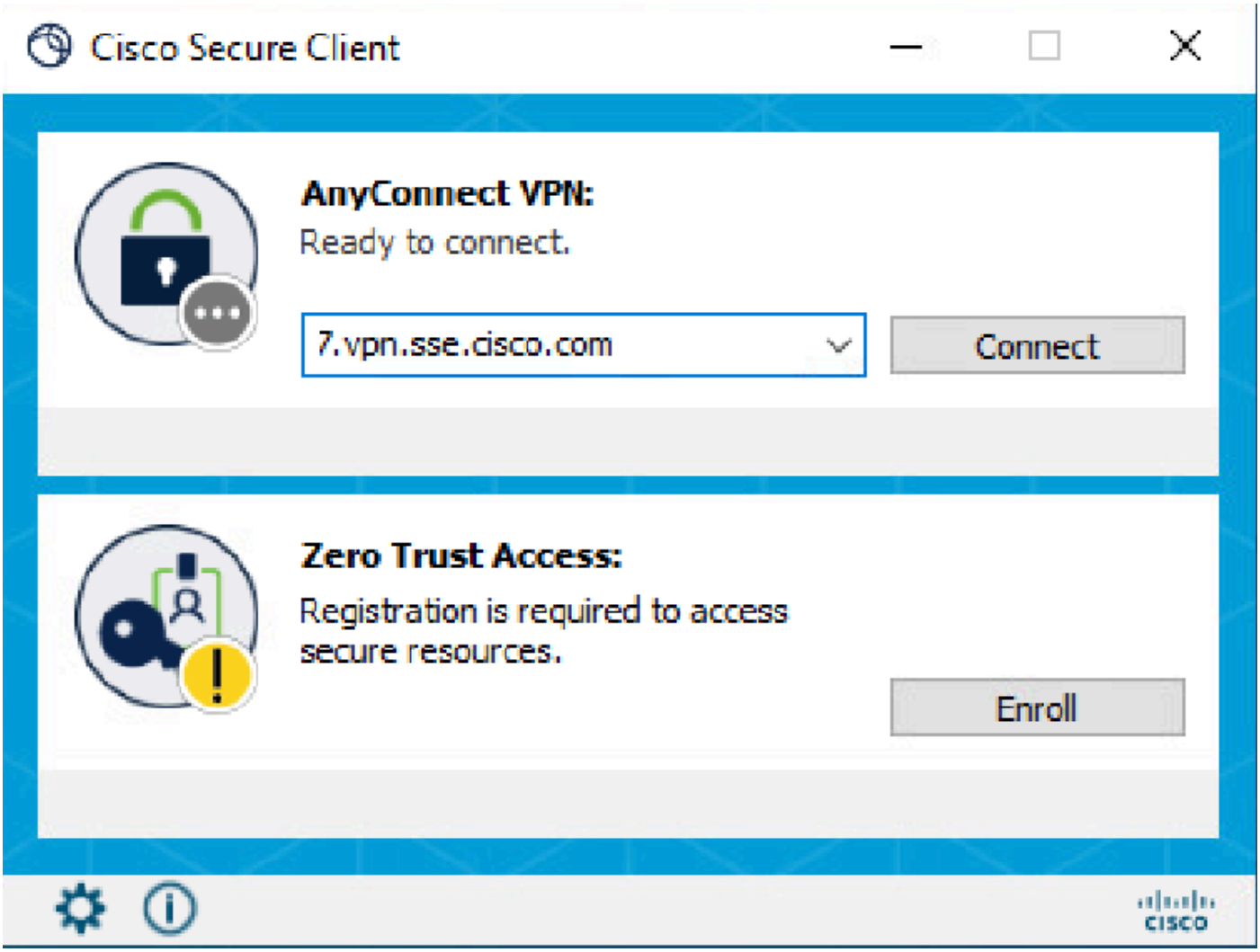
In seguito, è possibile procedere con il passaggio Verify.

Verifica

Per verificare l'accesso, è necessario aver installato l'agente di Cisco Secure Client che è possibile scaricare da Software Download - Cisco Secure Client.

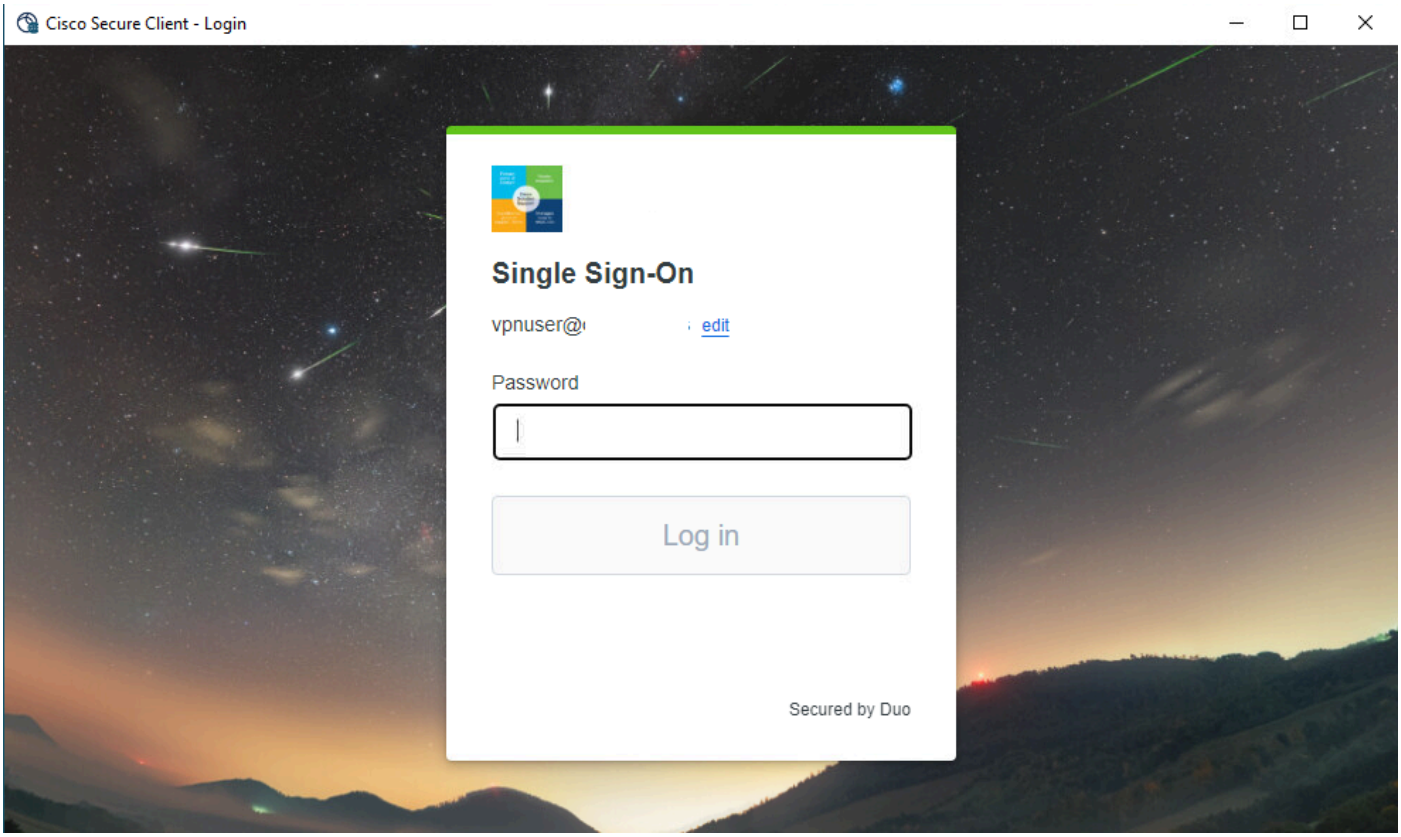
RA-VPN

Accedere tramite Cisco Secure Client Agent-VPN.



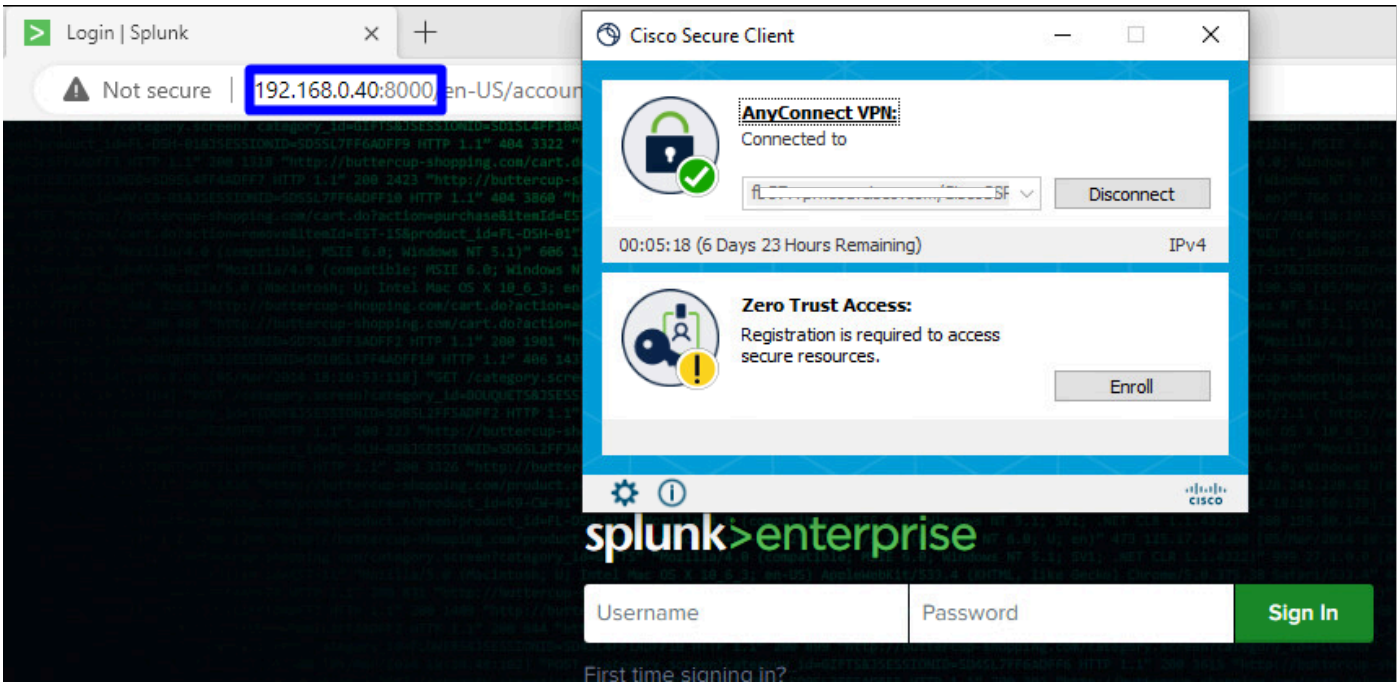
Secure Client - VPN

- Autenticazione tramite il provider SSO



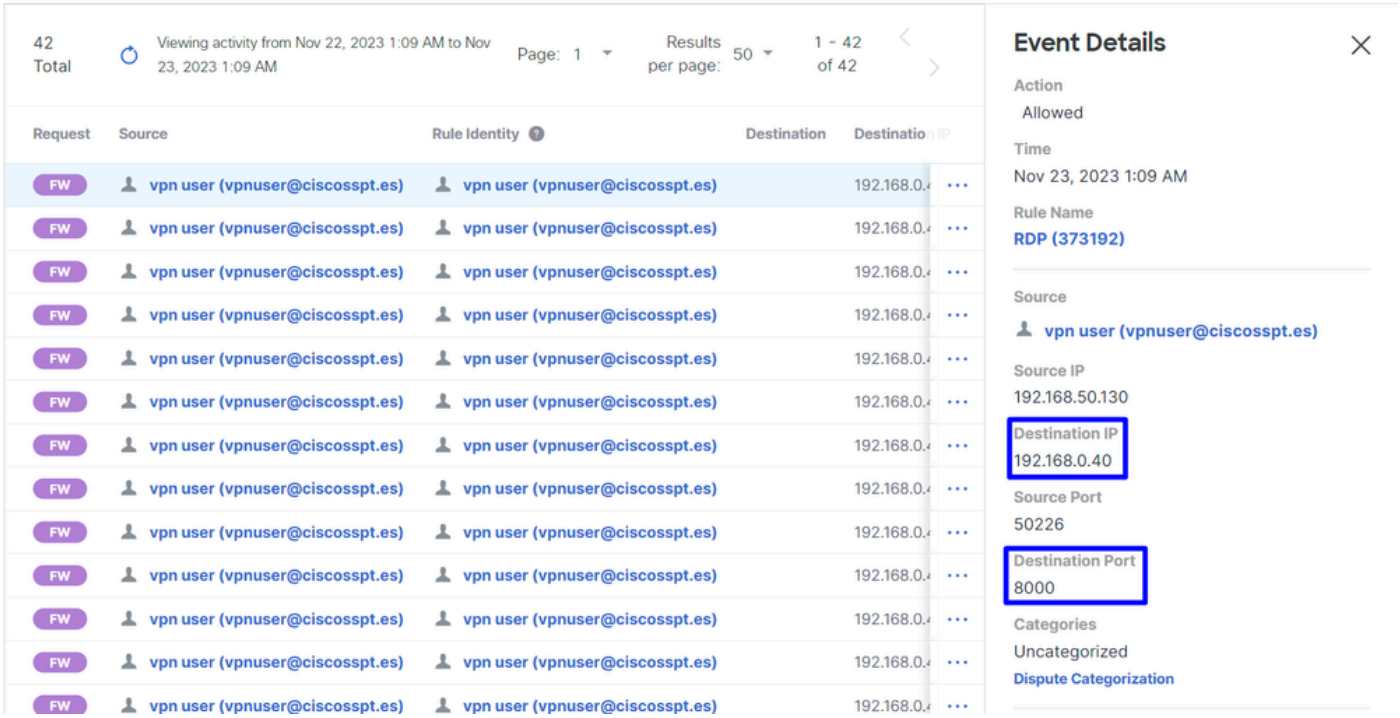
Accesso sicuro - VPN - SSO

- Dopo l'autenticazione, accedere alla risorsa:



Accesso sicuro - VPN - Autenticato

Accedere a:Monitor > Activity Search

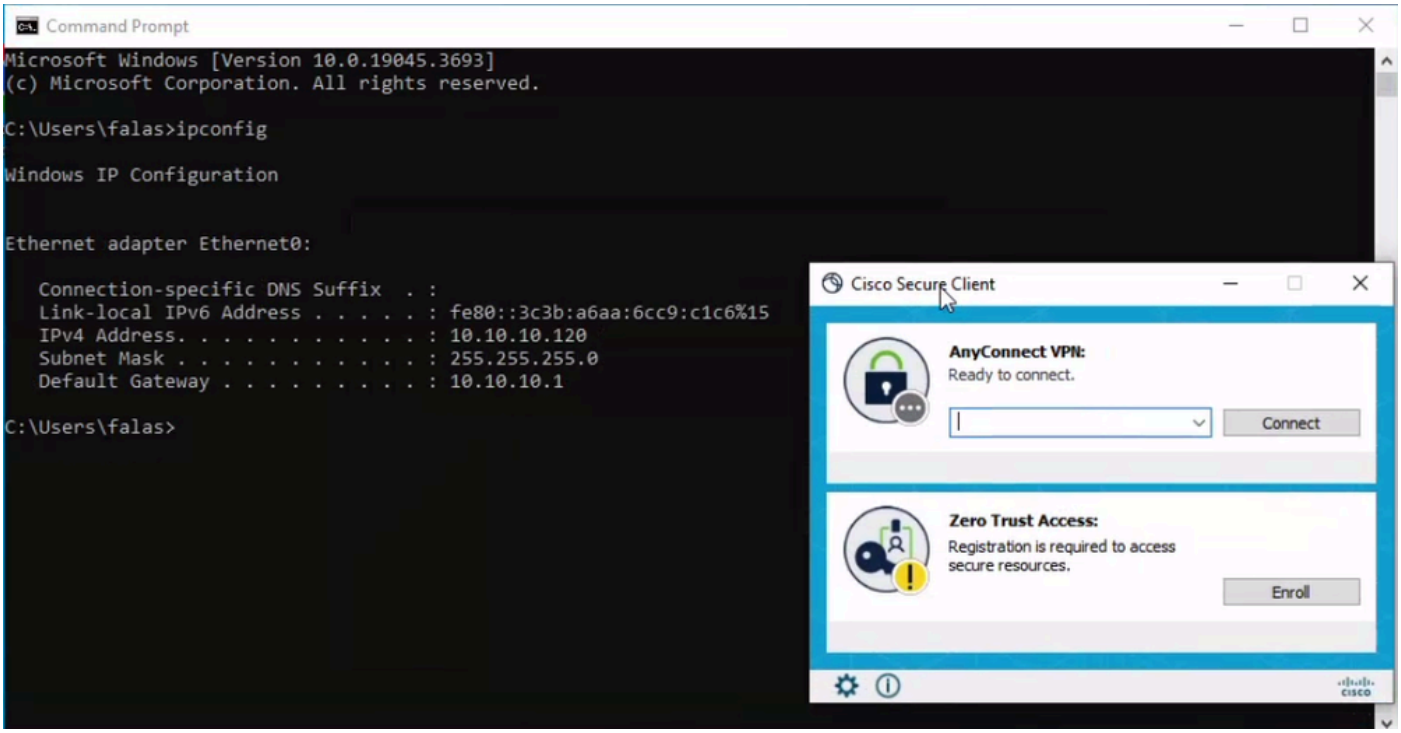


Accesso sicuro - Ricerca attività - RA-VPN

È possibile vedere che all'utente è stata consentita l'autenticazione tramite RA-VPN.

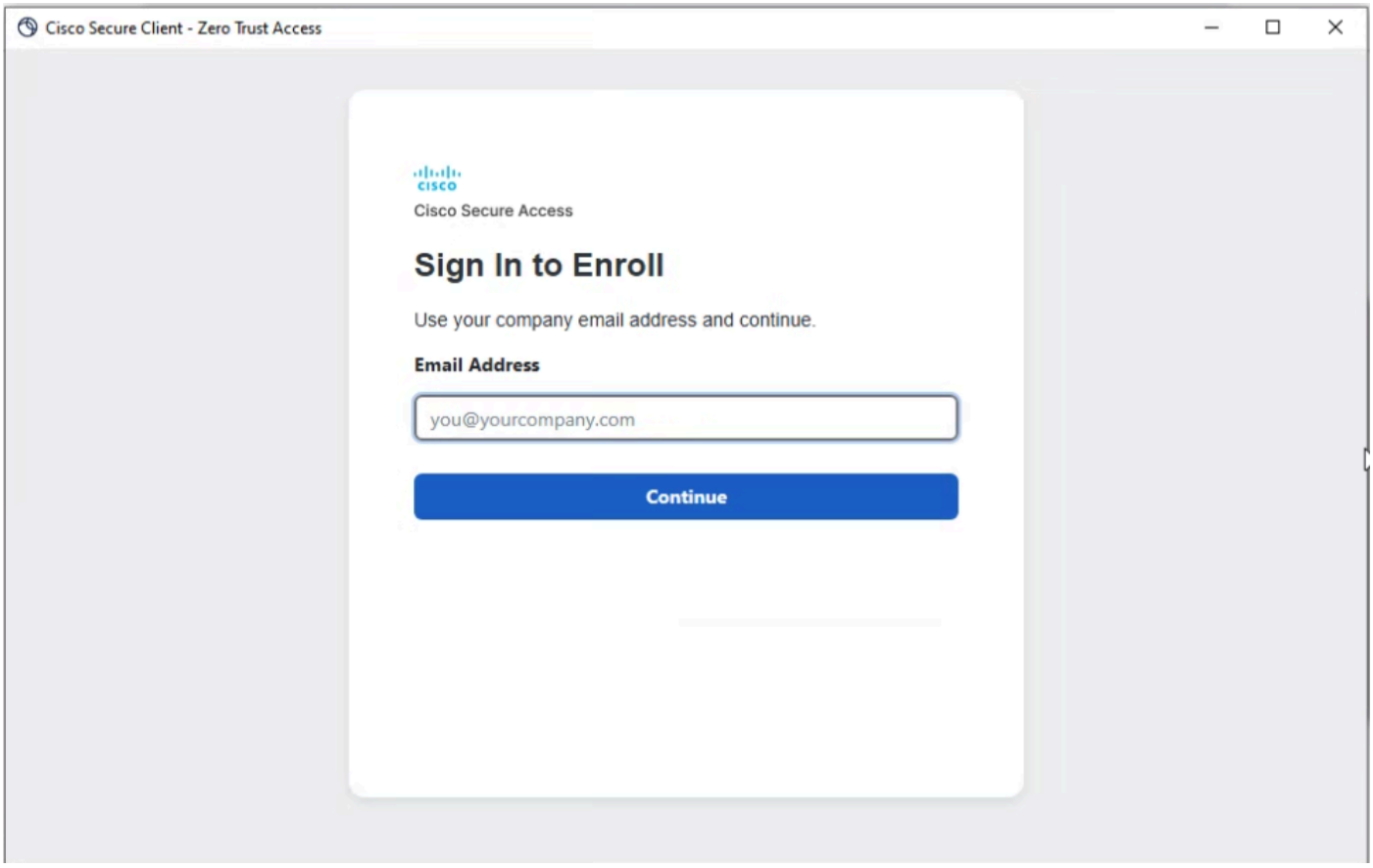
ZTNA basata su client

Accedere tramite Cisco Secure Client Agent - ZTNA.



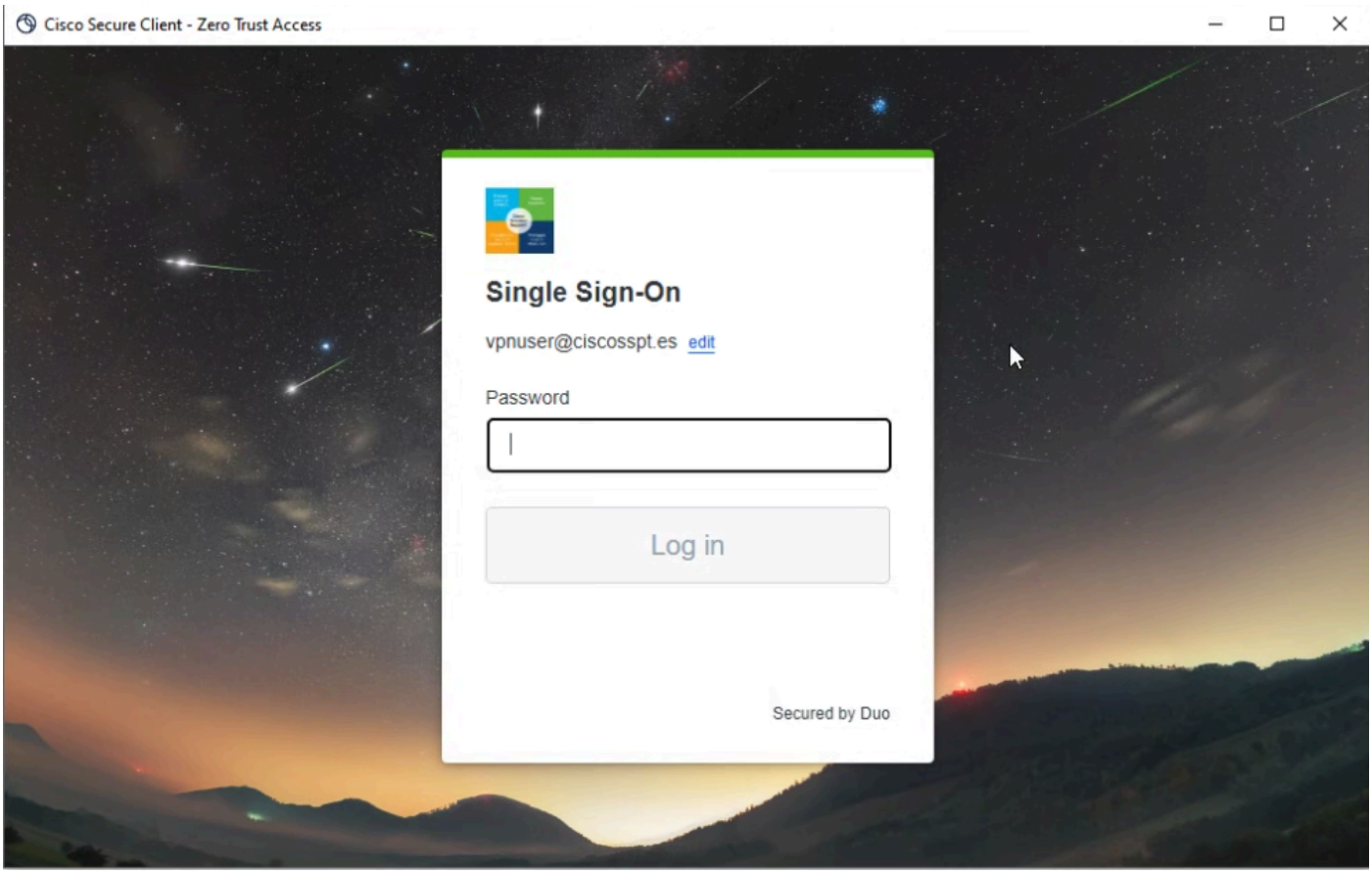
Secure Client - ZTNA

- Registrarsi con il proprio nome utente.



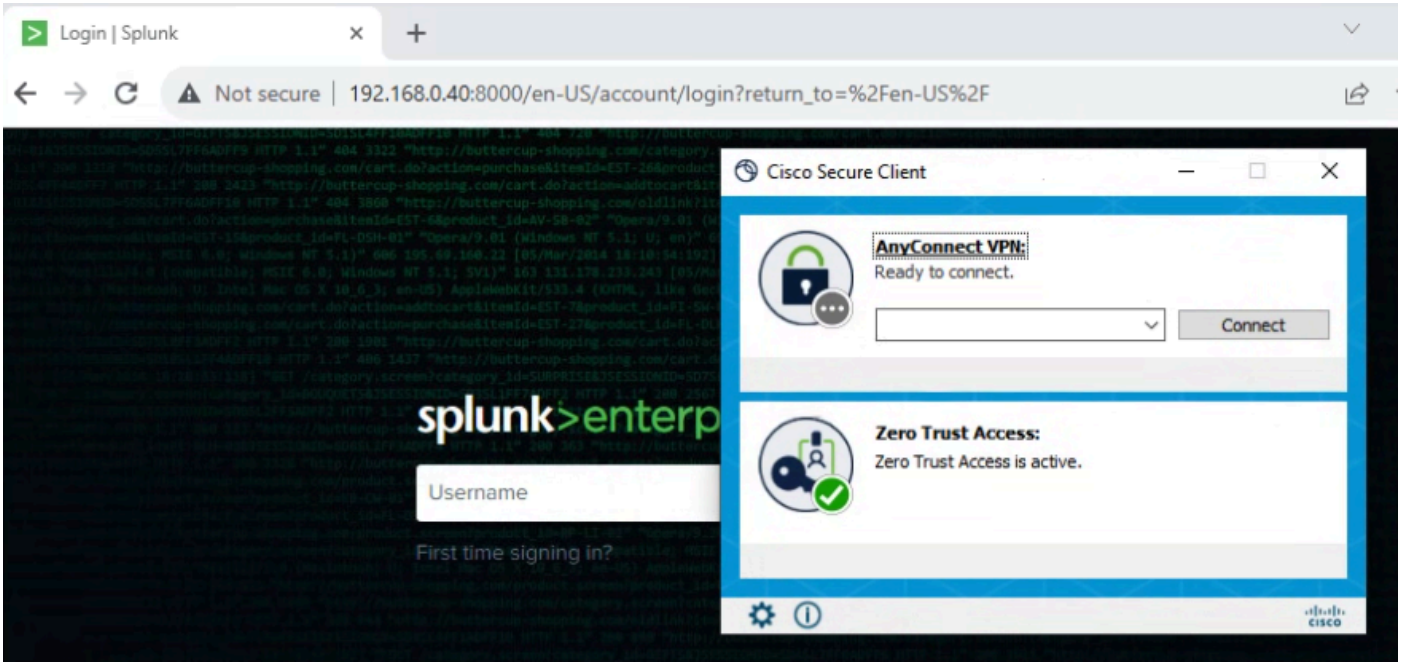
Secure Client - ZTNA - Registrazione

- Autenticazione nel provider SSO



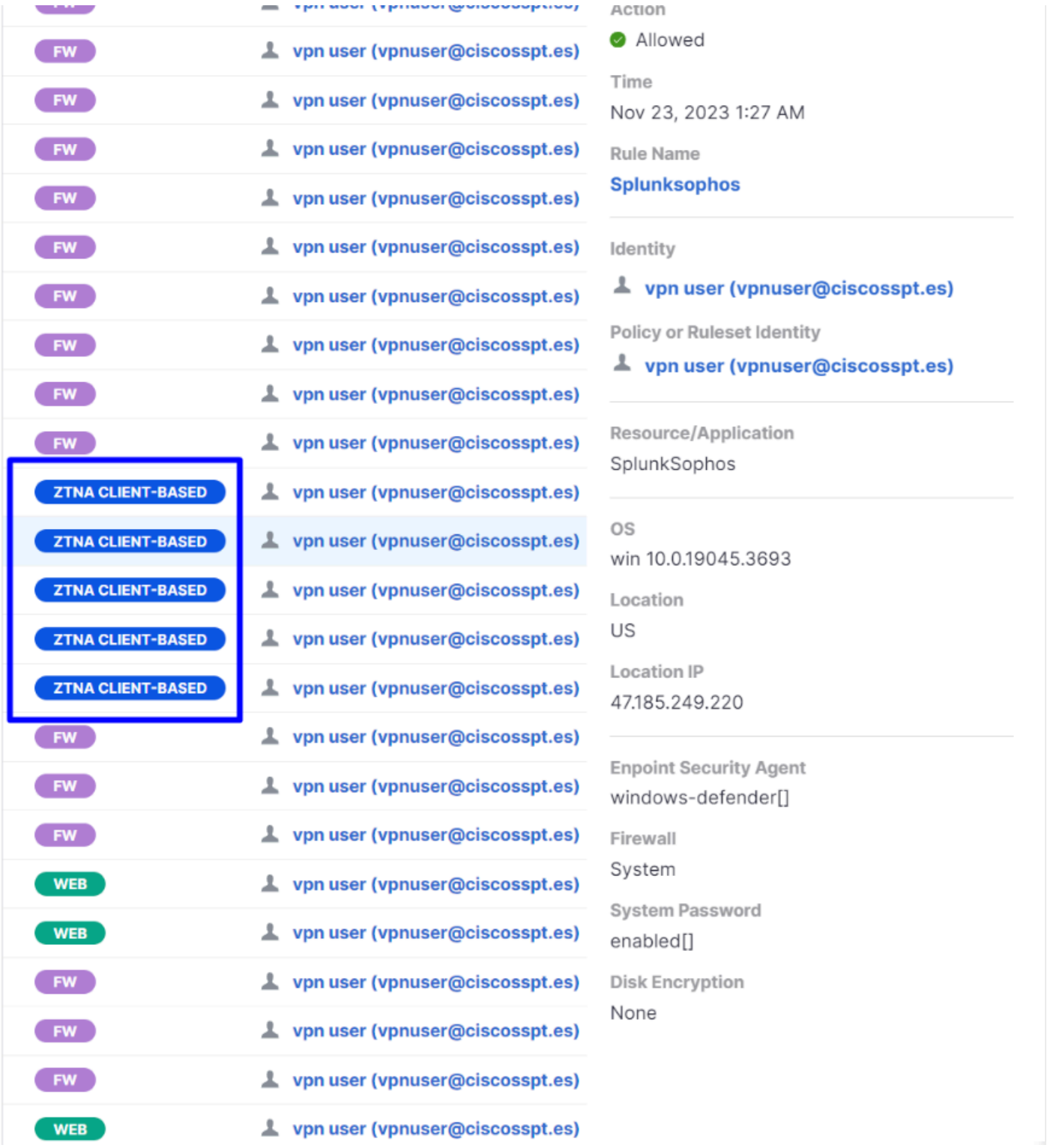
Secure Client - ZTNA - Accesso SSO

- Dopo l'autenticazione, accedere alla risorsa:



Accesso sicuro - ZTNA - Accesso registrato

Accedere a:Monitor > Activity Search

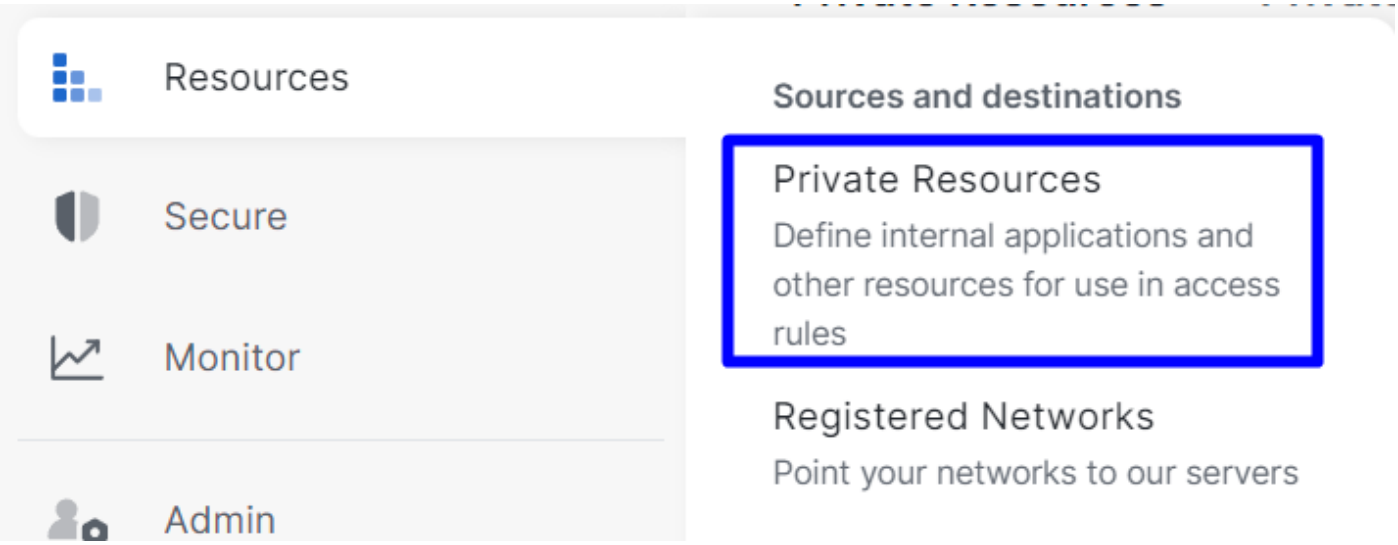


Accesso sicuro - Ricerca attività - Basato su client ZTNA

È possibile vedere che all'utente è stata consentita l'autenticazione tramite ZTNA basata su client.

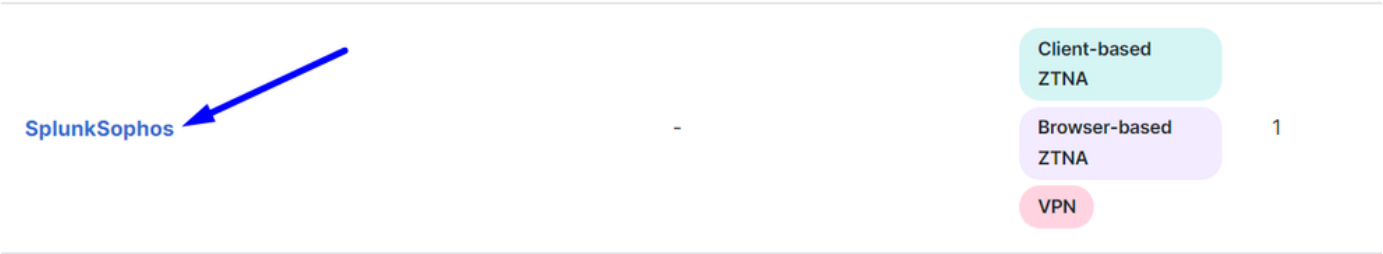
ZTNA basata su browser

Per ottenere l'URL, occorre andare alla **Resources > Private Resources**pagina.



Accesso sicuro - Risorsa privata

- Fare clic sul criterio



Accesso sicuro - Risorsa privata - SplunkSophos

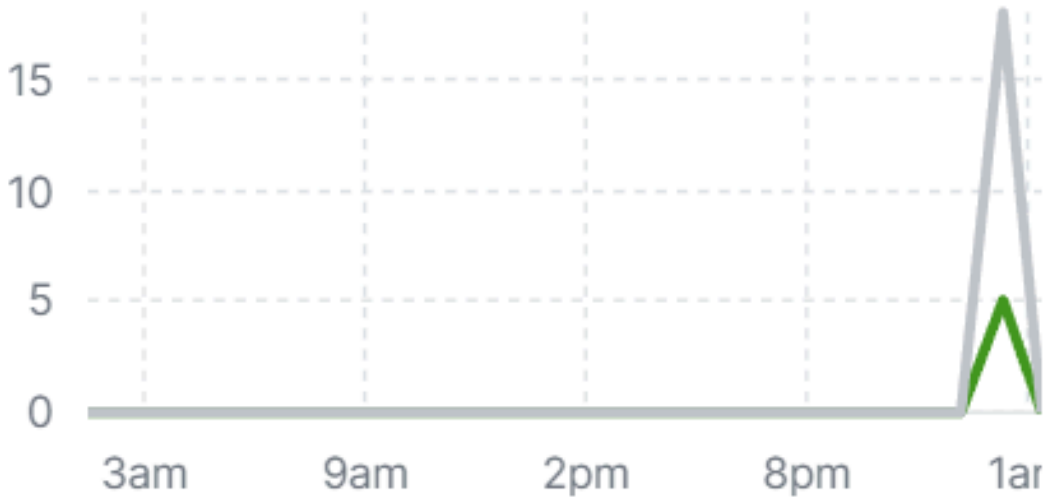
- Scorri verso il basso

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

Errore Di Risoluzione Dei Problemi Relativi All'Accesso Sicuro: Il Servizio Di Registrazione Non Risponde. Contatta il tuo help desk IT"

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).