Configurazione e risoluzione dei problemi di integrazione SSE (Secure Access) su Catalyst SD-WAN

Sommario

Introduzione

Questo documento descrive come configurare l'integrazione SSE attivo-attivo su Catalyst SD-WAN e ne guida la risoluzione dei problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Software Cisco Defined Wide Area Network (SD-WAN)
- Gruppi di configurazione
- Gruppi di criteri

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C800V versione 17.15.02
- vManage versione 20.15.02
- Account Cisco Secure Access

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.

Cisco Secure Access

Cisco Secure Access è una soluzione SSE (Security Service Edge) basata su cloud che converge più servizi di sicurezza di rete, offrendo servizi dal cloud per supportare una forza lavoro ibrida. Cisco SD-WAN Manager sfrutta le API REST per recuperare le informazioni sulle policy da Cisco Secure Access e distribuisce queste informazioni ai dispositivi Cisco IOS XE SD-WAN. Questa integrazione consente l'accesso diretto a Internet (DIA) semplice, trasparente e sicuro per gli utenti, consentendo loro di connettersi da qualsiasi dispositivo, ovunque e in modo sicuro.

Cisco SSE consente ai dispositivi SD-WAN di stabilire connessioni con i provider SSE utilizzando tunnel IPSec. Questo documento è destinato agli utenti di Cisco Secure Access.

Configurazioni preliminari

- Abilita ricerca dominio per il dispositivo: Passare a Gruppi di configurazione > Profilo di sistema > Globale e abilitare Ricerca dominio.

Nota: Per impostazione predefinita, Ricerca dominio è disabilitata.

- Configura DNS: Il router può risolvere il DNS e accedere a Internet sulla VPN 0.
- Configurare NAT DIA: La configurazione DIA deve essere presente sul router in cui viene creato il tunnel SSE.

Creazione di interfacce di loopback

Se entrambi i tunnel in una configurazione attiva/attiva si connettono allo stesso centro dati di destinazione e utilizzano la stessa interfaccia WAN dell'origine, è necessario creare due indirizzi IP di loopback.

Nota: Quando due tunnel sono configurati con la stessa origine e destinazione, IKEv2 forma una coppia di identità costituita da un ID locale e un ID remoto. Per impostazione predefinita,

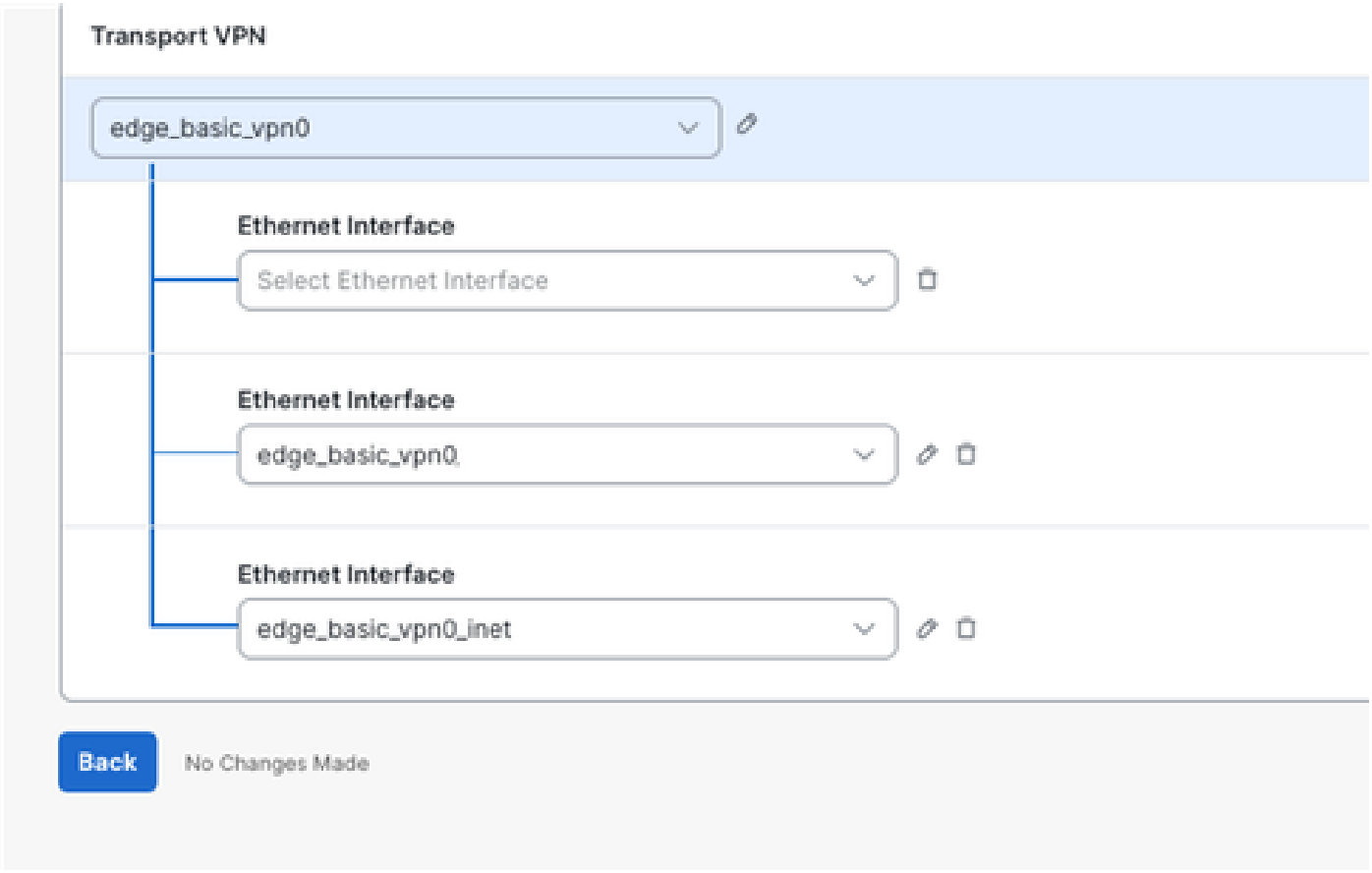
---

l'ID locale è l'indirizzo IP dell'interfaccia di origine del tunnel. Questa coppia di identità deve essere univoca e non può essere condivisa tra due tunnel. Per evitare confusione nello stato IKEv2, ogni tunnel utilizza come origine un'interfaccia di loopback diversa. Anche se i pacchetti IKE vengono convertiti (NAT) sull'interfaccia DIA, l'ID locale rimane invariato e mantiene l'indirizzo IP di loopback originale.

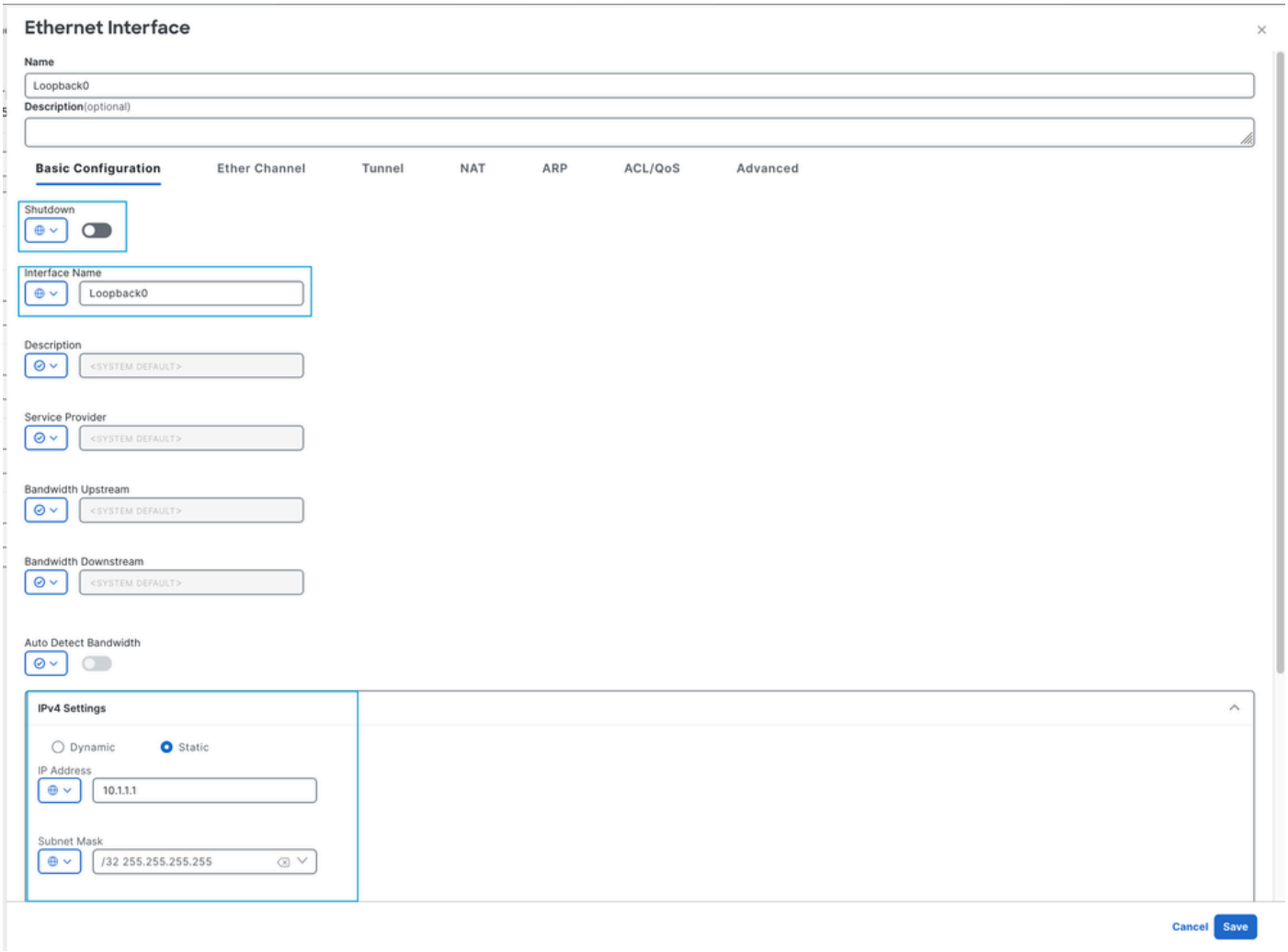
1. Selezionare Configurazione > Gruppi di configurazione > Nome gruppo di configurazione> Profilo di trasporto e gestione > fare clic su Modifica.

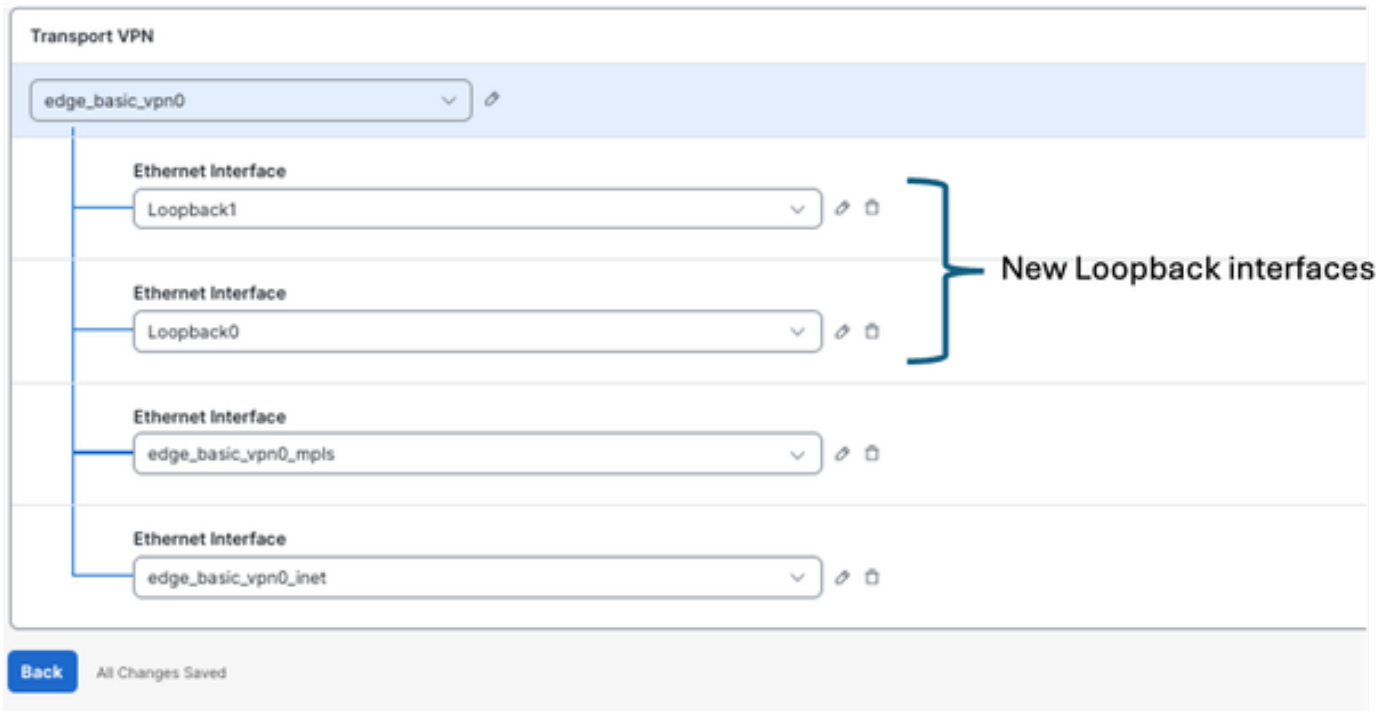
2. Fare clic sul segno più (+) sul lato destro del profilo VPN per il trasporto (profilo principale). Viene visualizzato un menu Aggiungi feature (Add Feature) all'estrema destra.

3. Fare clic su Ethernet Interface (Interfaccia Ethernet). Aggiunge una nuova interfaccia Internet sotto Transport VPN.



4. Creare le due interfacce di loopback utilizzando gli indirizzi IPv4 RFC1918, come esempio Loopback0 nell'immagine.

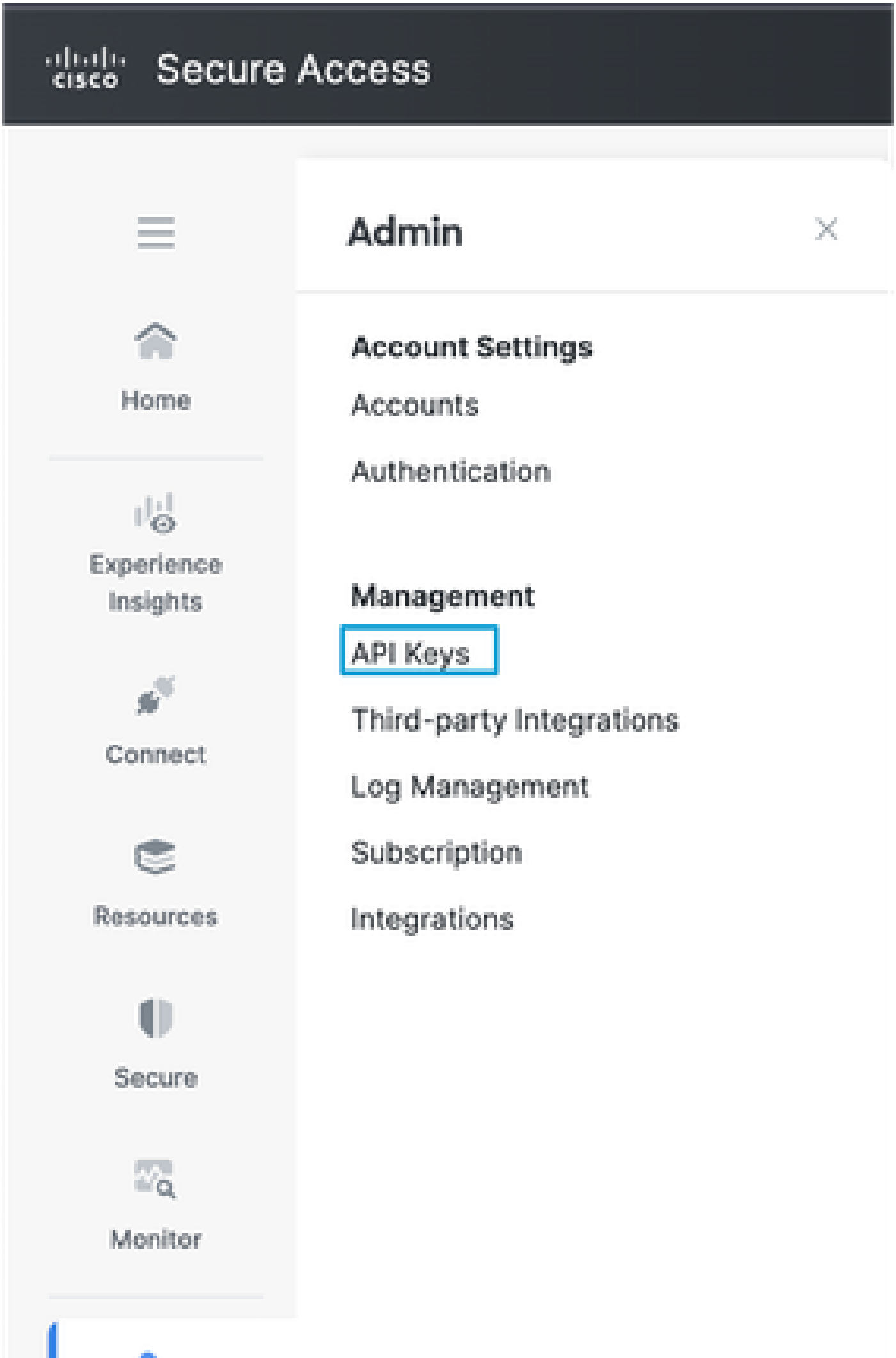




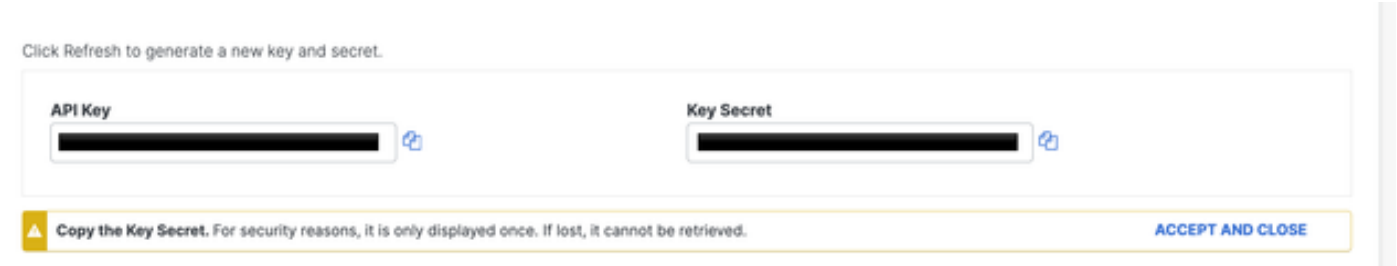
5. Dopo aver applicato la configurazione di loopback, procedere con la distribuzione della modifica di configurazione nel dispositivo. Si noti che lo stato del provisioning passa da1/1a 0/1.

Configura nuove chiavi API sul portale SSE

1. Accesso al portale SSE https://login.sse.cisco.com/
2. Passare a Amministrazione > Chiavi API


Secure Access
Admin
Account Settings
Accounts
Authentication
Management
API Keys
Third-party Integrations
Log Management
Subscription
Integrations
Home
Experience Insights
Connect
Resources
Secure
Monitor

6. Copiare la chiave API e la chiave segreta in un blocco note e selezionare ACCEPT AND CLOSE

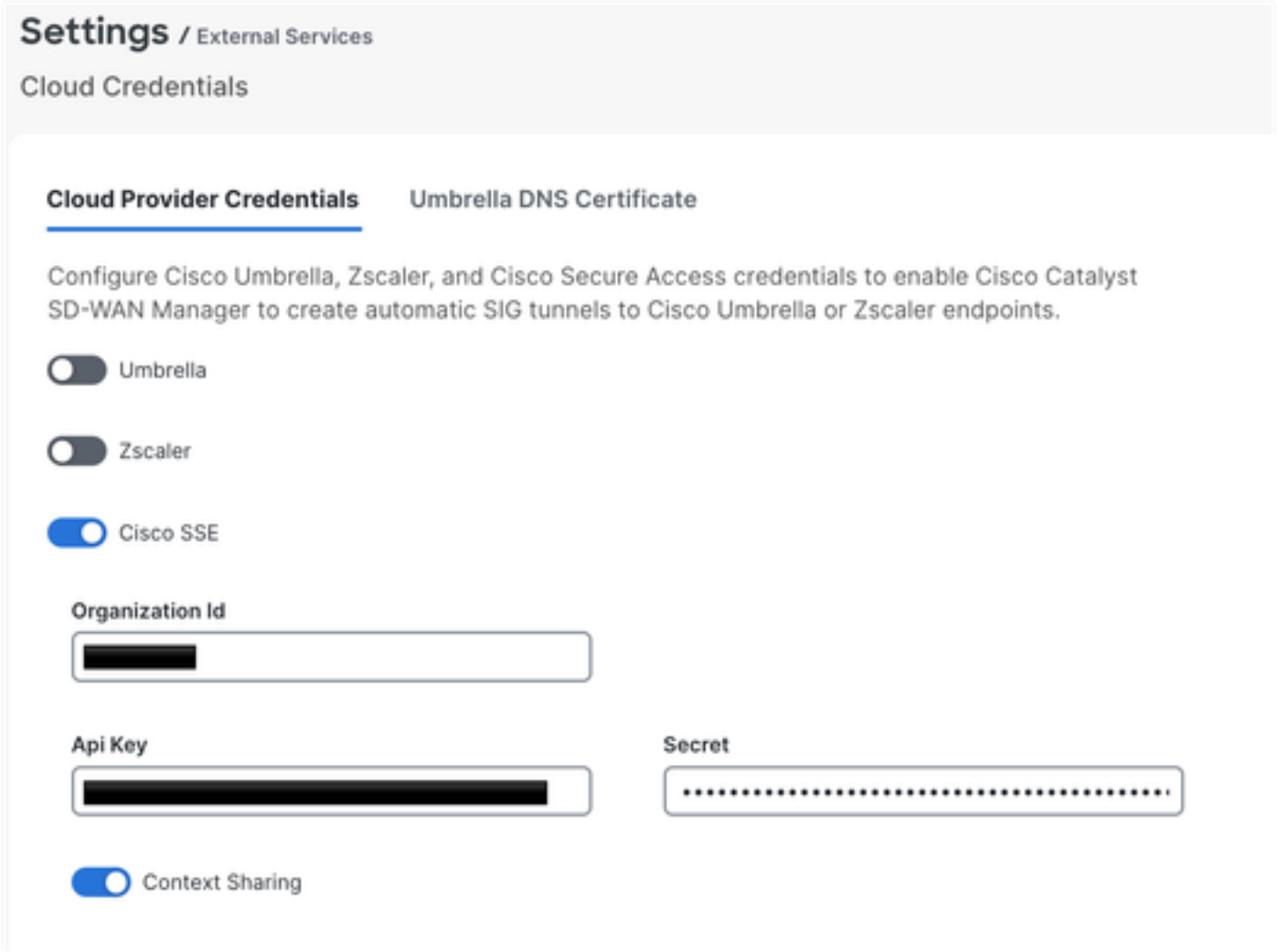


7. Sotto l'URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys il#some-number# è il tuo ID organizzazione. Copiare queste informazioni anche nel blocco note.

Configurare SSE su Catalyst Manager

Imposta credenziali cloud

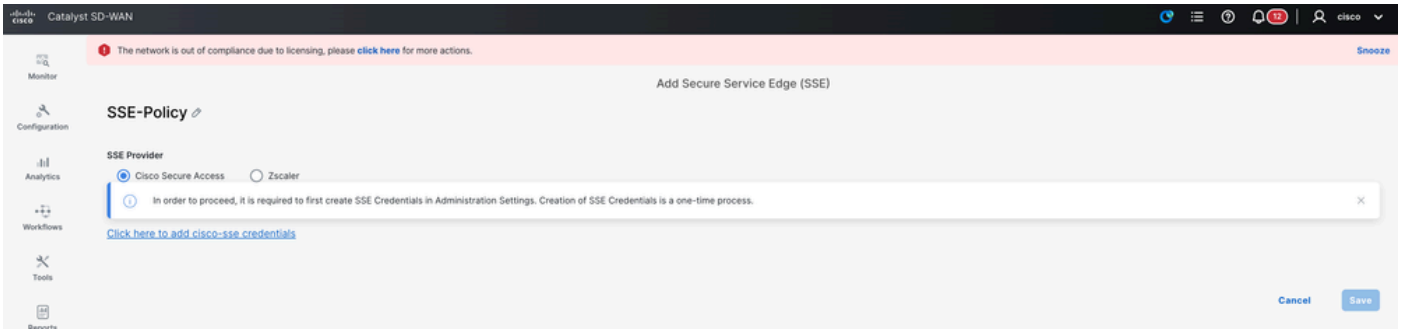
1. Passare a Amministrazione > Impostazioni > Credenziali cloud > Credenziali provider cloud e abilitare Cisco Secure Access
e inserisci i dettagli.



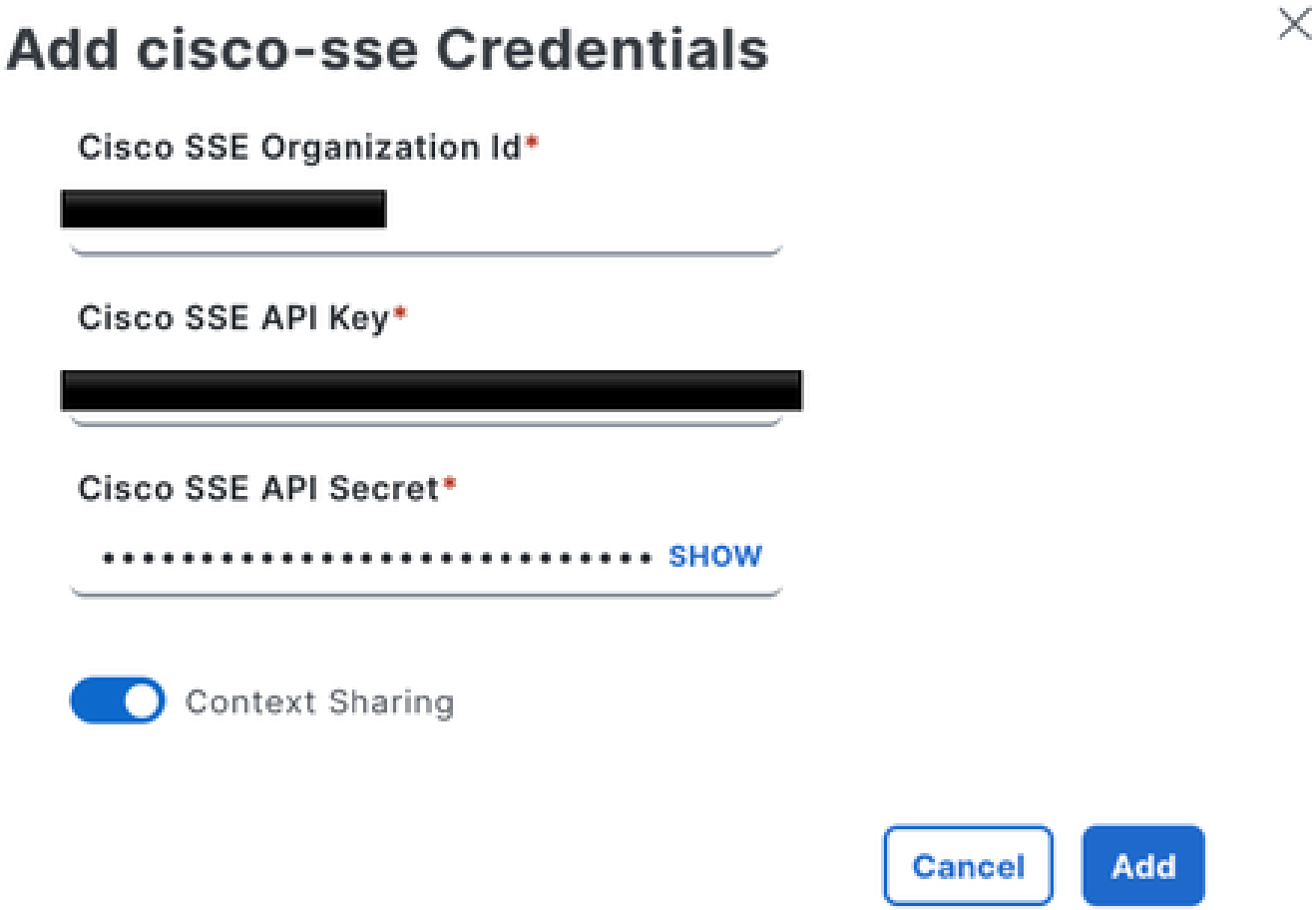
2. Facoltativo: È possibile abilitare la condivisione del contesto per migliorare le funzionalità. Per ulteriori informazioni, consultare la Guida per l'utente di Cisco SSE sulla condivisione del contesto.

Configura tunnel SSE tramite il gruppo di criteri

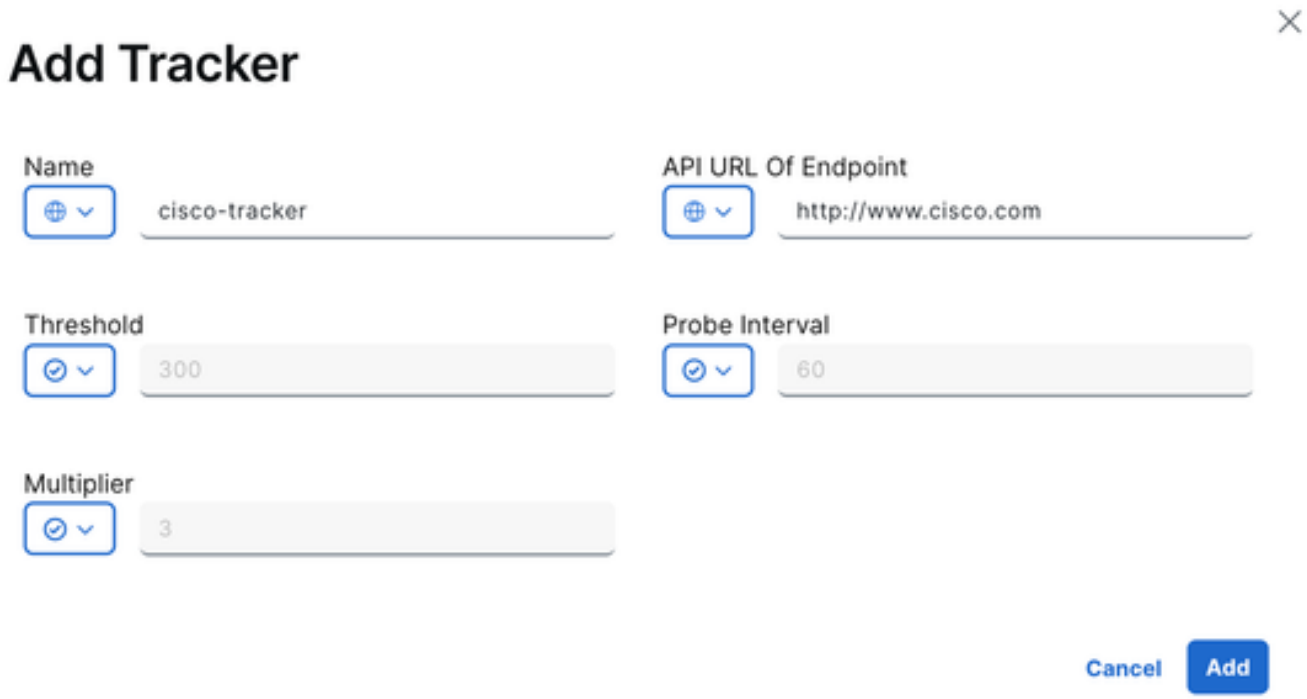
In SD-WAN Manager selezionare Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge (Configurazione > Gruppi di criteri > Secure Internet Gateway/Secure Service Edge), quindi fare clic su Add Secure Service Edge (SSE).

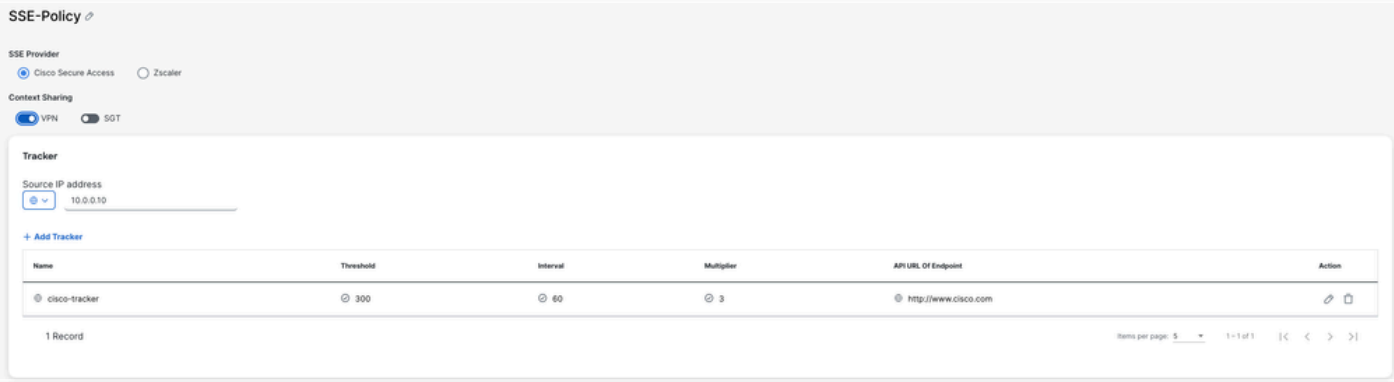


Nota: se le credenziali cloud non sono ancora state configurate, è possibile aggiungerle in questo passaggio. Se le credenziali sono già state configurate, vengono caricate automaticamente.



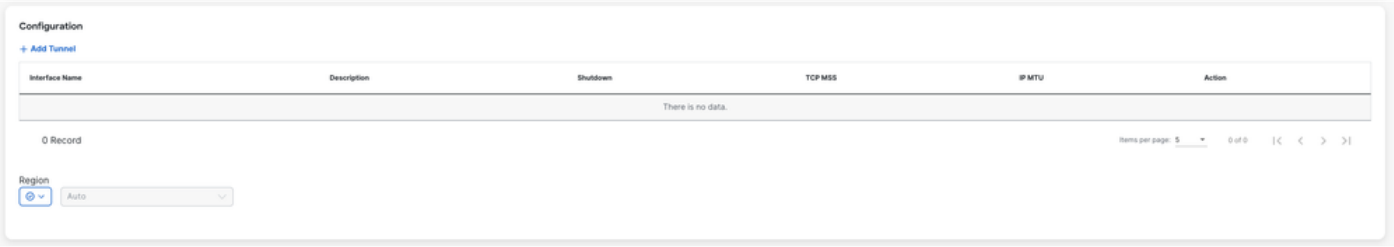
1. Configurare il Tracker SSE. In questo esempio, l'URL del tracker è impostato su http://www.cisco.com, e l'indirizzo IP di origine è assegnato da una delle interfacce di loopback.



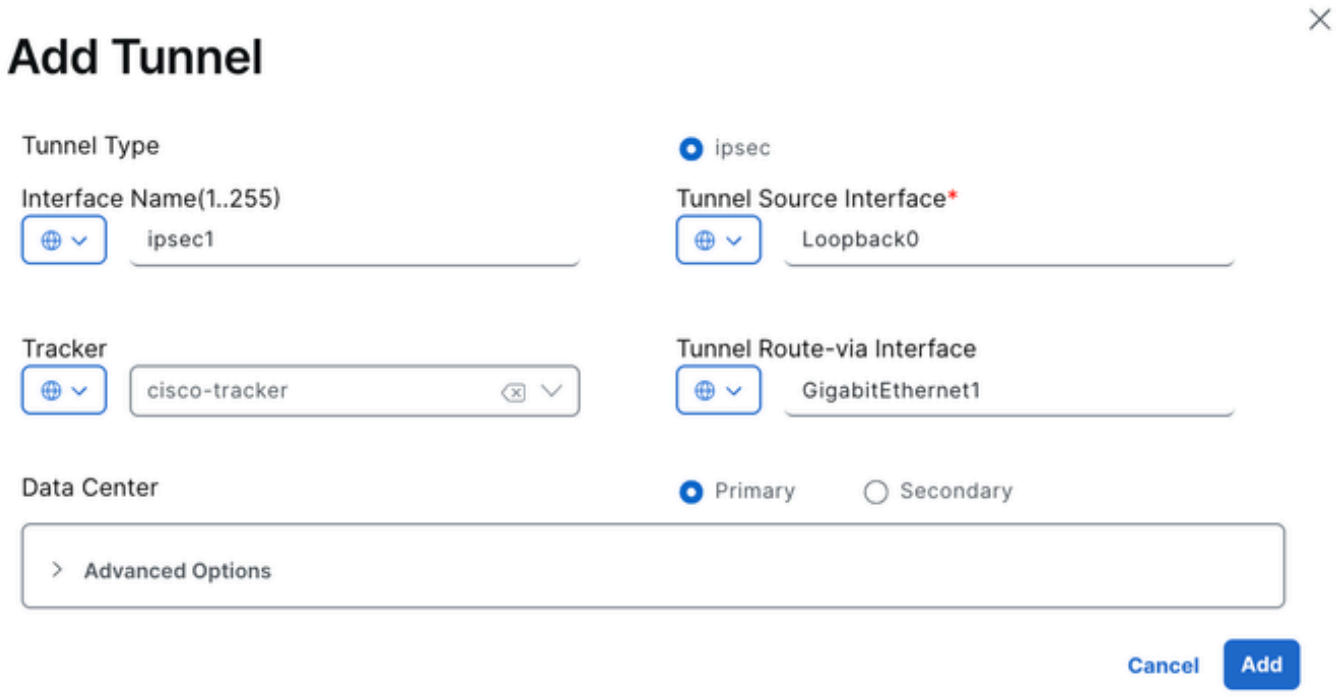


Facoltativamente, poiché la condivisione del contesto è stata abilitata quando sono state configurate le credenziali cloud, l'opzione in questo esempio VPN è selezionata.

2. Fare clic su Add Tunnel

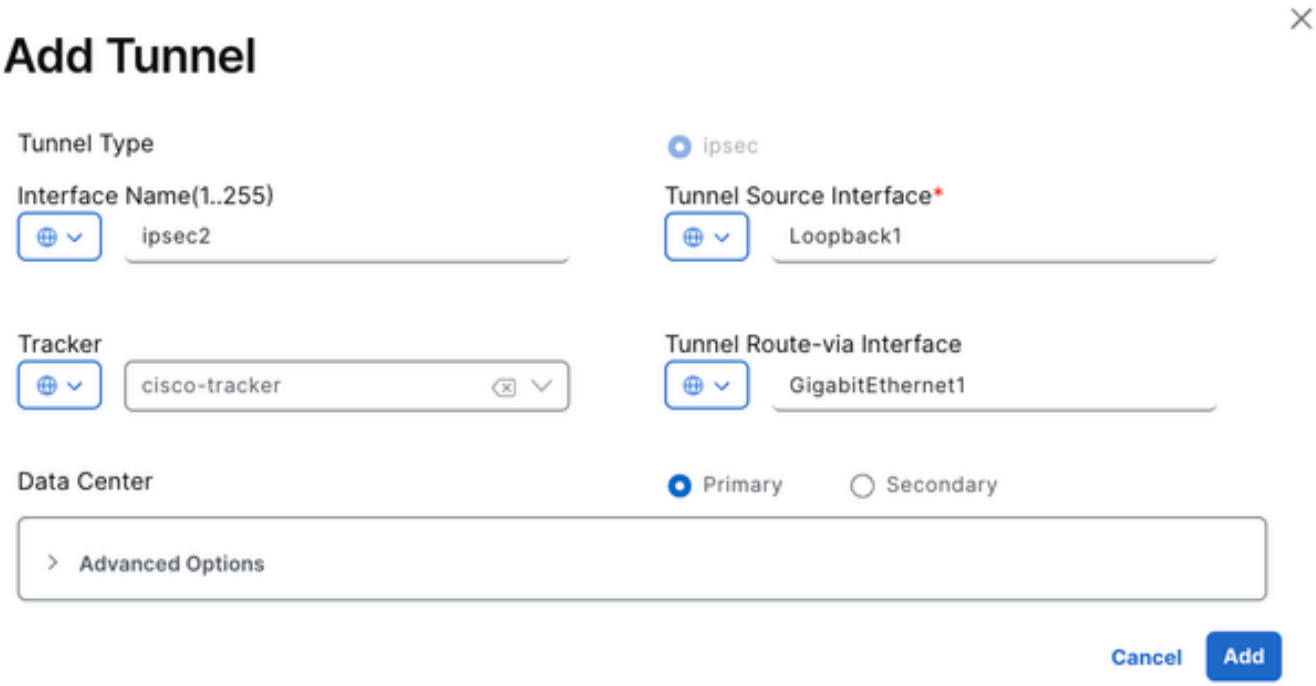


3. Nell'esempio, l'interfaccia Loopback0 viene usata come origine del tunnel, mentre l'interfaccia Gigabit Ethernet1 viene usata come interfaccia WAN per indirizzare il traffico.



Poiché il tracker è stato configurato in questo esempio, l'impostazione viene modificata in Global e cisco-tracker preconfigurato viene selezionato.

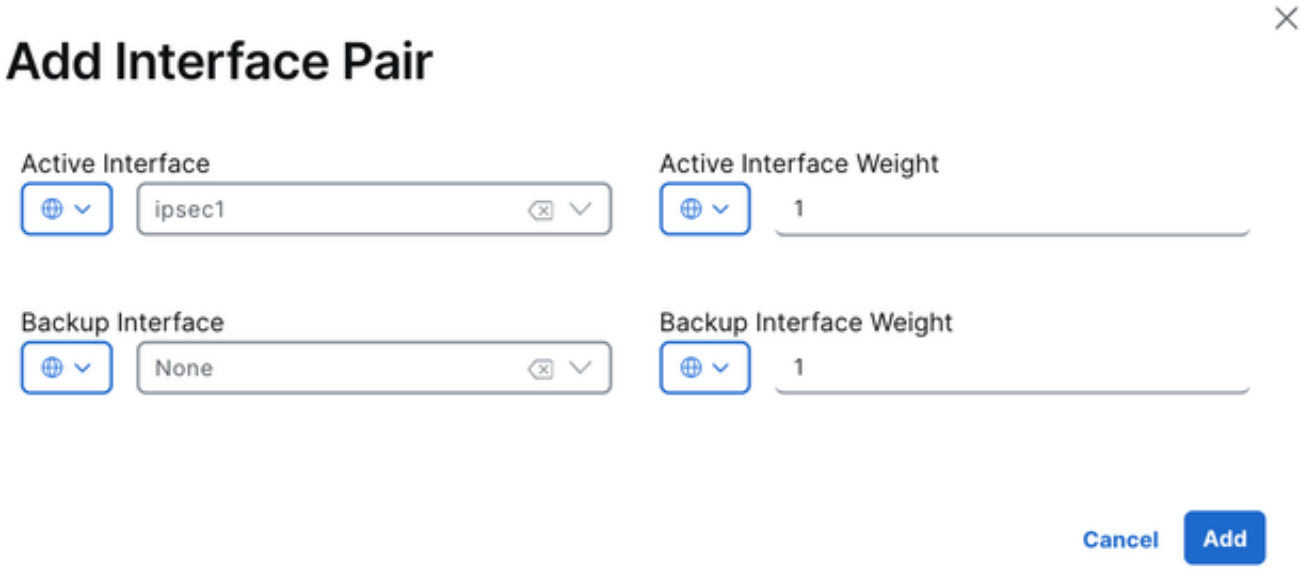
4. Per il secondo tunnel, ripetere gli stessi passaggi utilizzando gli stessi parametri, ma modificare il nome dell'interfaccia da ipsec1 a ipsec2 e il nome dell'interfaccia di origine in Loopback1.



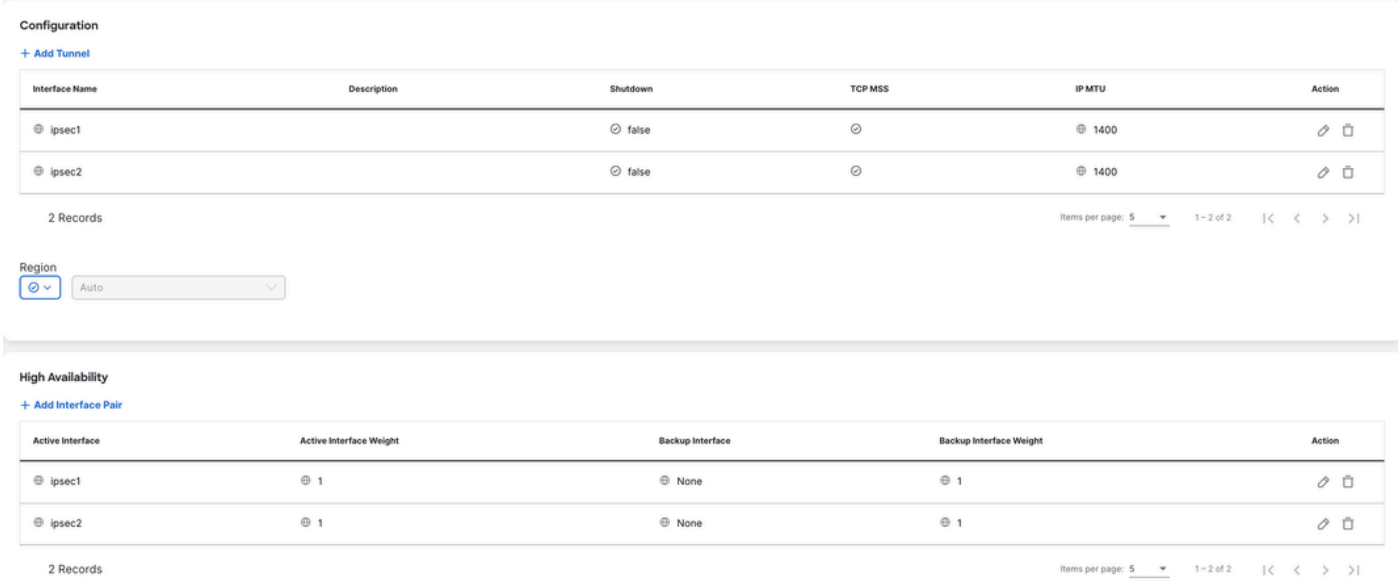
Entrambi i tunnel sono configurati per essere attivi contemporaneamente, senza backup.

5. Fare clic su Add Interface Pair (Aggiungi coppia di interfacce).

6. Fare clic su Add. L'interfaccia attiva è impostata su ipsec1 e non è specificata alcuna interfaccia di backup.



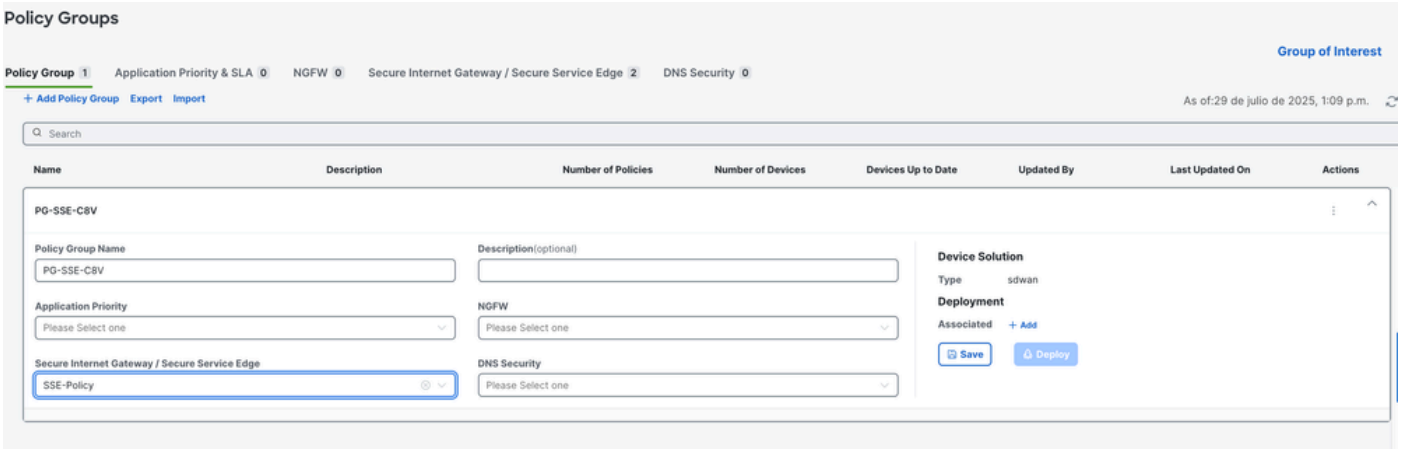
7. La stessa operazione viene ripetuta per il secondo tunnel, ipsec2.



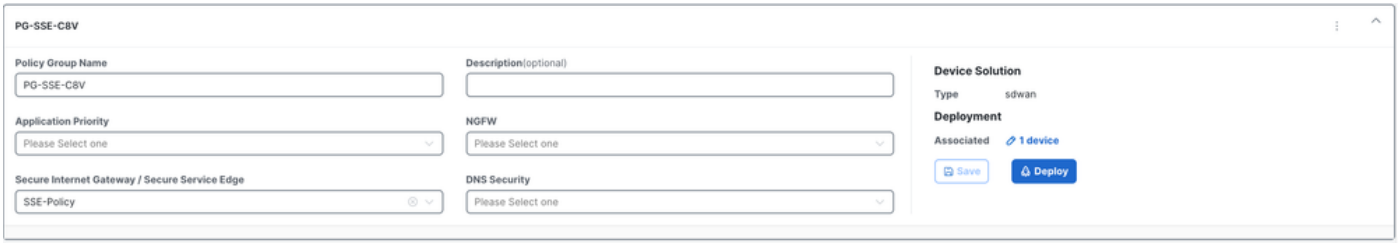
8. Salvare la configurazione.

Configura gruppo di criteri

1. È possibile selezionare il criterio creato in precedenza all'interno del gruppo di criteri e salvarlo.



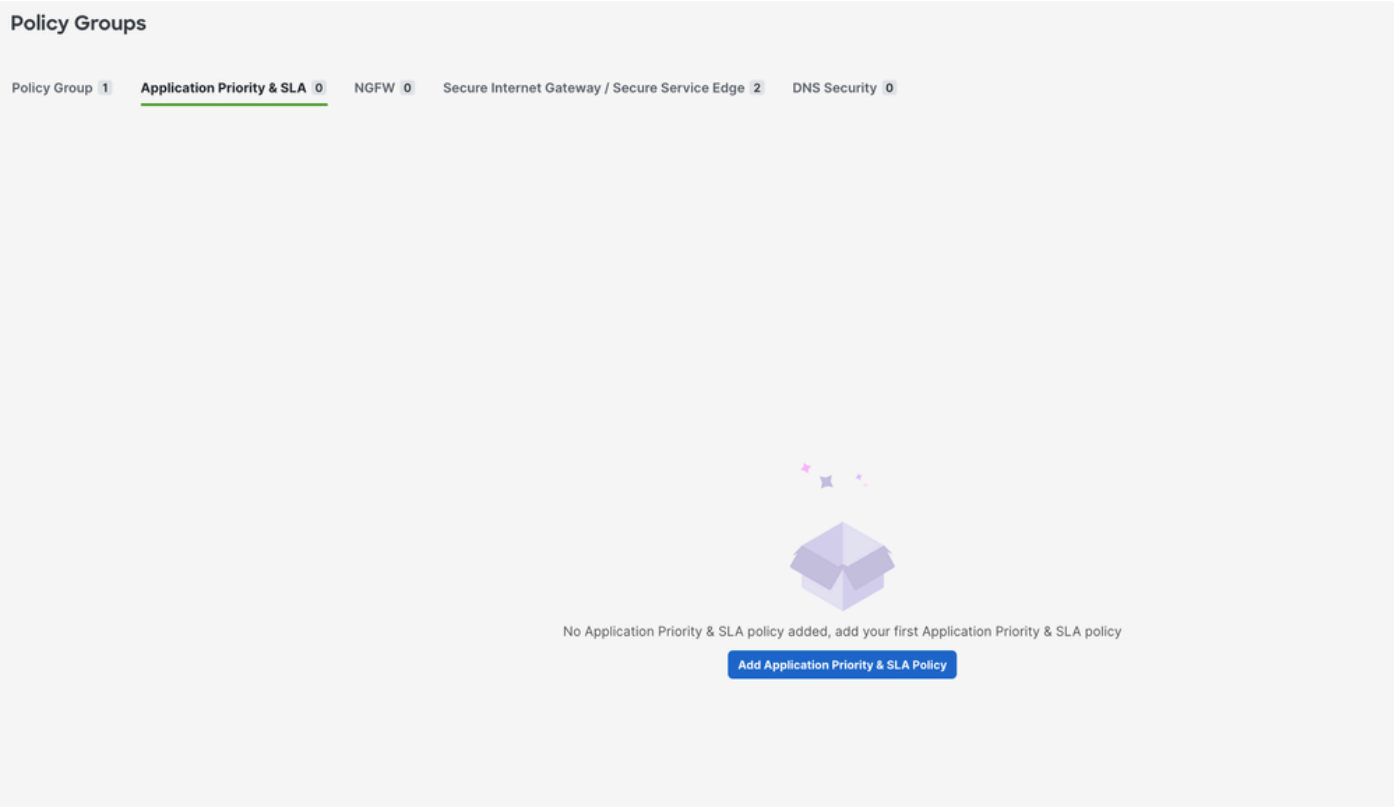
2. Dopo aver associato il dispositivo o i dispositivi al gruppo di criteri, procedere alla distribuzione del gruppo di criteri.



Configura il gruppo di criteri per reindirizzare il traffico a SSE

1. In SD-WAN Manager, selezionare Configuration > Policy Groups > Application Priority & SLA (Configurazione > Gruppi di criteri > Priorità applicazione e SLA).

- Selezionare Aggiungi priorità applicazione e criteri SLA
- Specificare un nome per il criterio.

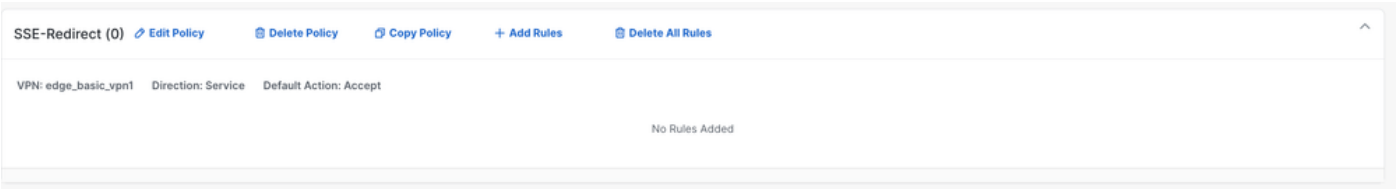


2. Una volta visualizzato il nuovo criterio, selezionare l'interruttore Layout avanzato.

3. Selezionare Add Traffic Policy List.

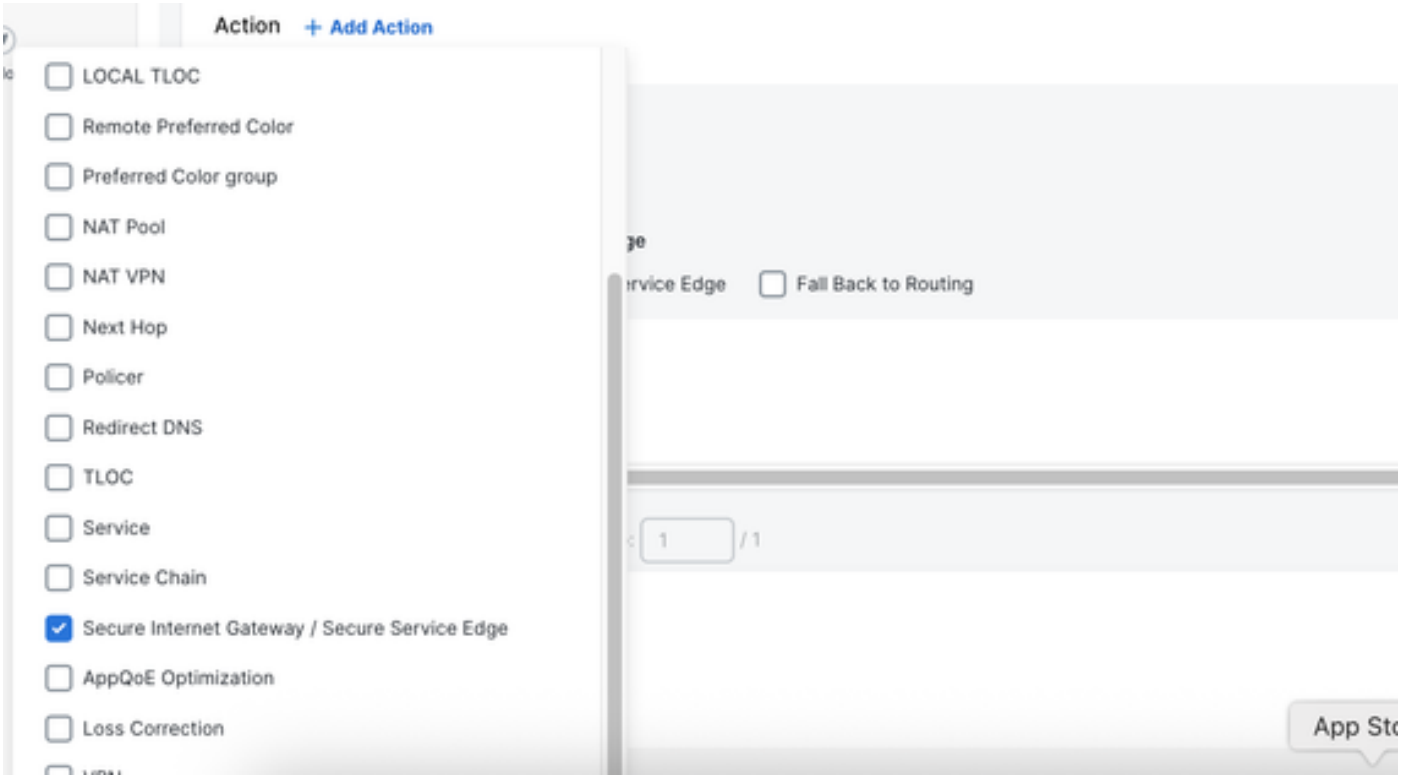
- Configurare le VPN per reindirizzare il traffico al tunnel SSE.
- Impostate le opzioni Direzione (Direction) e Azione di default (Default Action) in base alle esigenze, quindi salvate.

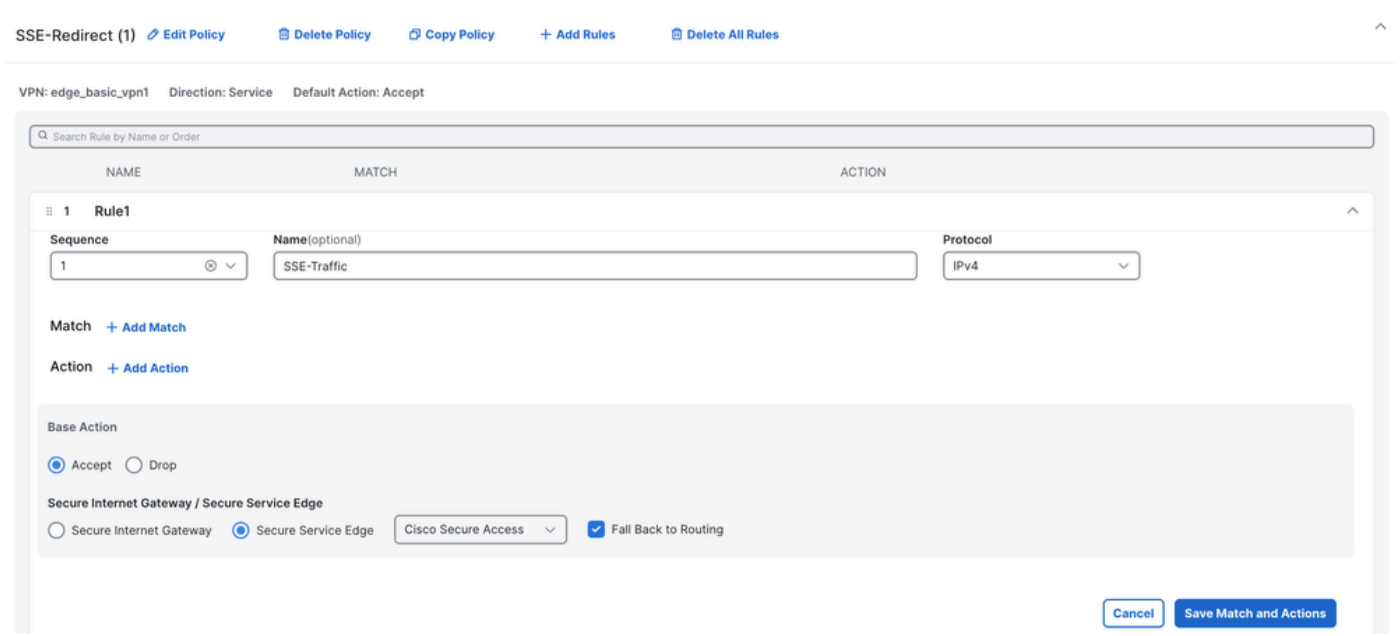
4. Selezionare + Aggiungi regola.



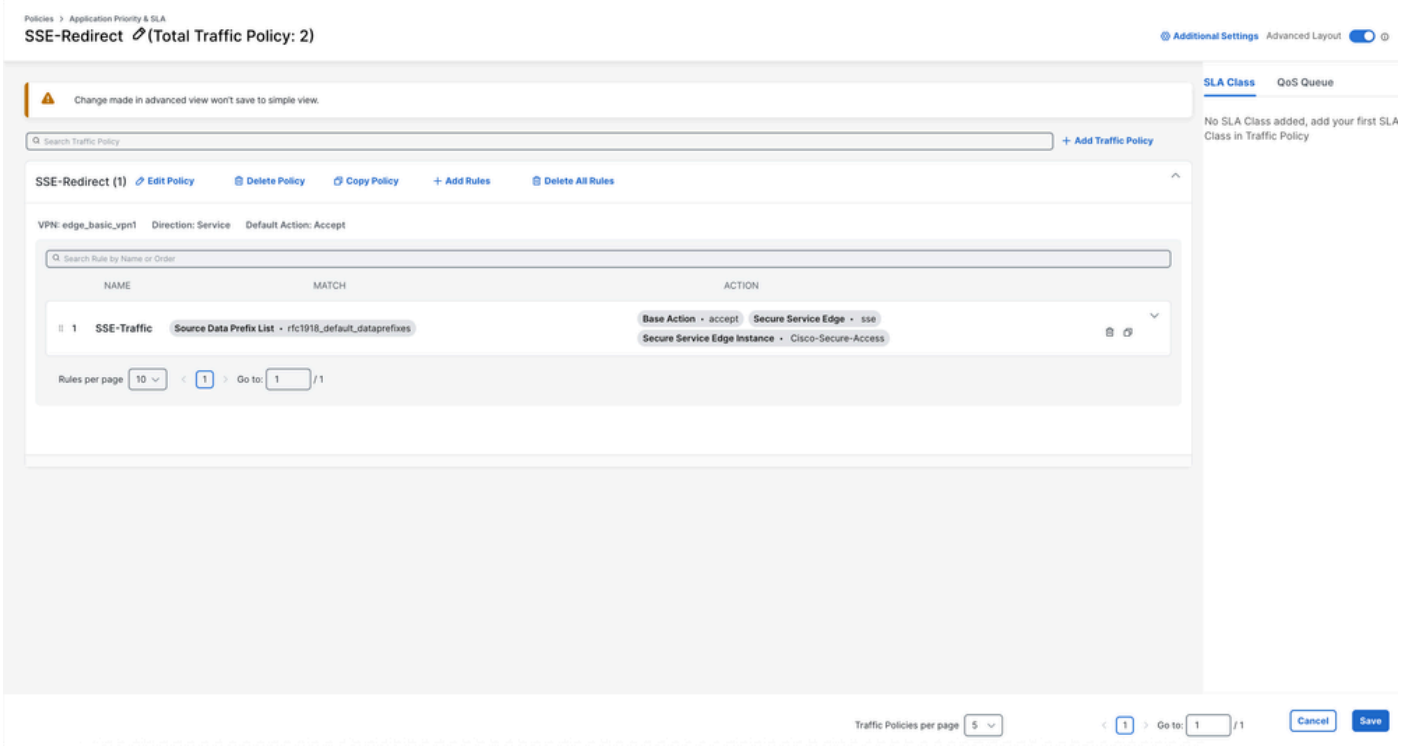
5. Configurare i criteri di corrispondenza del traffico per reindirizzare il traffico all'SSE.
6. Selezionare Accetta come azione di base, quindi fare clic su + Azione.

7. Cercare l'azione Secure Internet Gateway / Secure Service Edge e impostarla su Secure Service Edge.



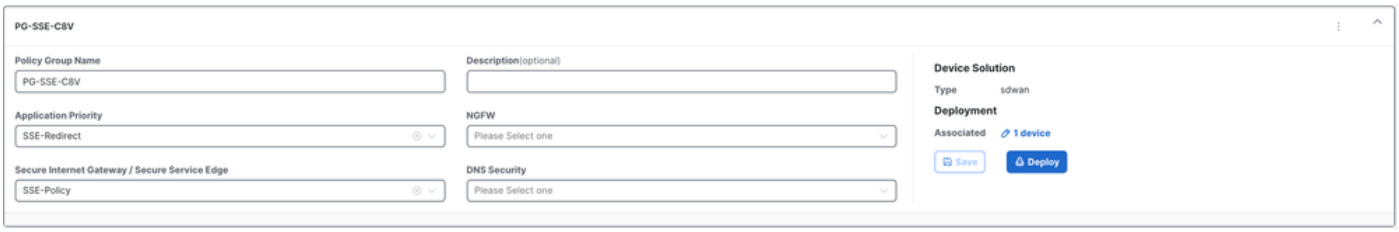


8. Fare clic su Salva corrispondenza e azioni



9. Fare clic su Salva.

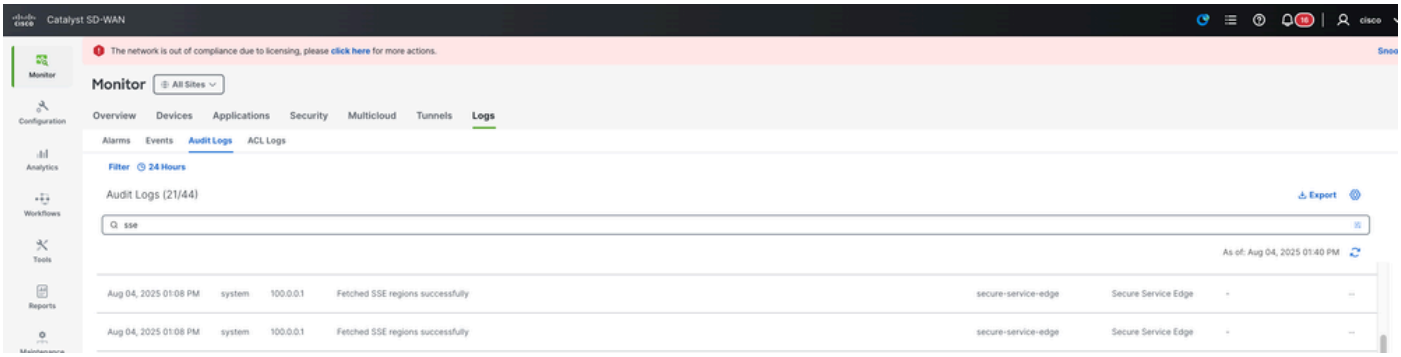
10. Passare a Configurazione > Gruppi di criteri e selezionare il criterio Priorità applicazione appena creato. Salvare e quindi distribuire.



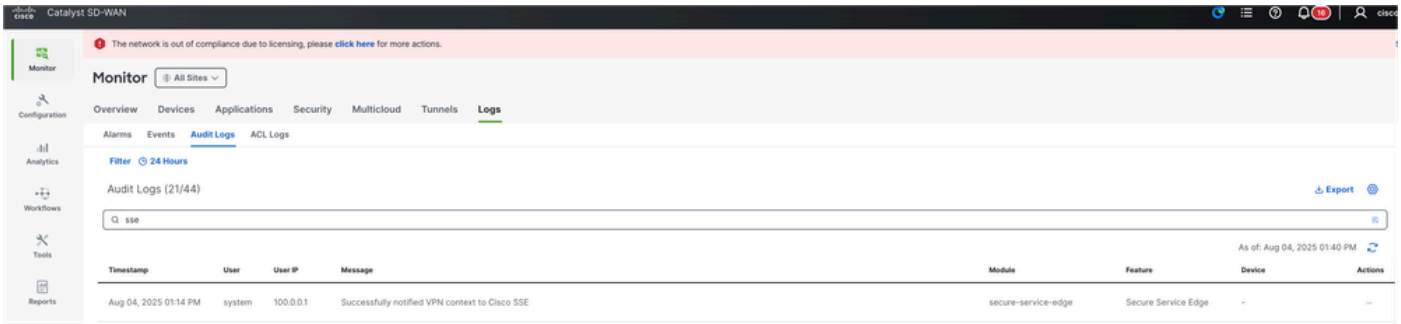
Verifica

Responsabile

1. Monitorare > Registri > Registri di controllo e cercare "sse".



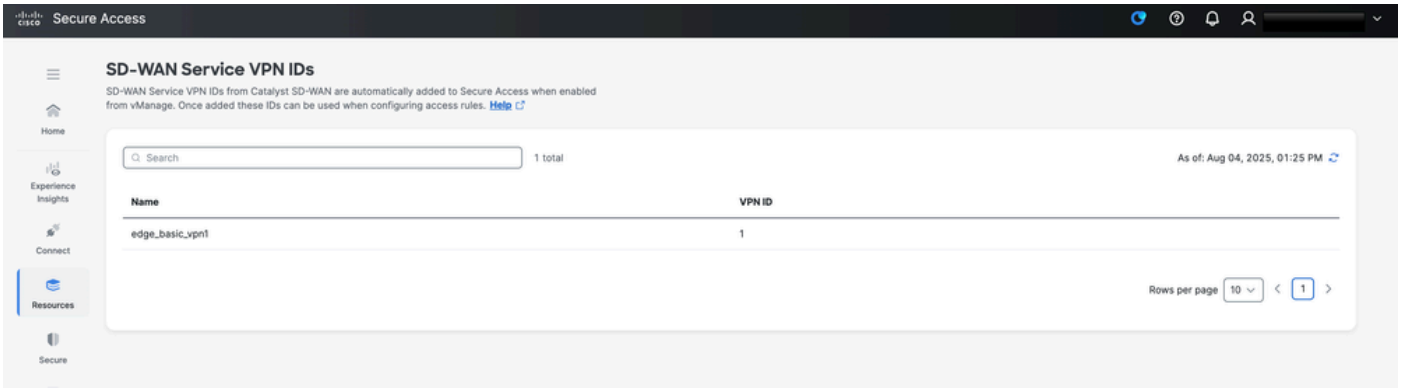
2. È possibile verificare se la VPN di condivisione del contesto è abilitata controllando Manager.



Dashboard di accesso protetto

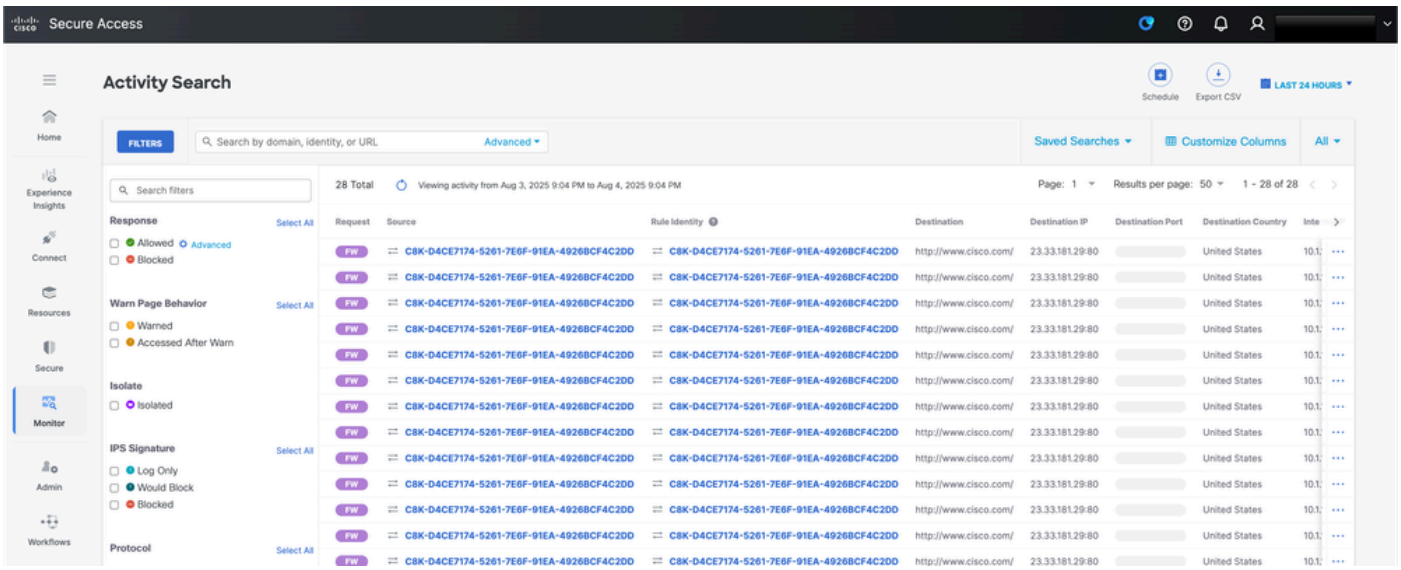
Condivisione contesto

È possibile verificare se la VPN per la condivisione del contesto è stata abilitata controllando il dashboard SSE,Risorse > ID VPN del servizio SD-WAN



Tunnel Up

Quando il tunnel è attivo e il tracciatore è operativo con il traffico che scorre attraverso il tunnel, è possibile convalidarlo passando a Monitor > Ricerca attività. In questa schermata viene visualizzato il traffico che attraversa il tunnel, ad esempio le richieste a www.cisco.com generate dal tracker. Questa visibilità conferma che il tracker è attivo e sta monitorando attivamente il traffico attraverso il tunnel



Comandi CLI (Command Line Interface)

<#root>

```
Hub2-SIG#show sse all
**************************************
SSE Instance Cisco-Secure-Access
**************************************
Tunnel name : Tunnel16000001
Site id: 2
Tunnel id: 655184839
SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD
HA role: Active

Local state: Up


Tracker state: Up


Destination Data Center: 44.217.195.188
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

Informazioni correlate

- Configurazione della condivisione del contesto SD-WAN
- Integrazione di Cisco Secure Access con routing SD
- Documentazione e supporto tecnico – Cisco Systems

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).