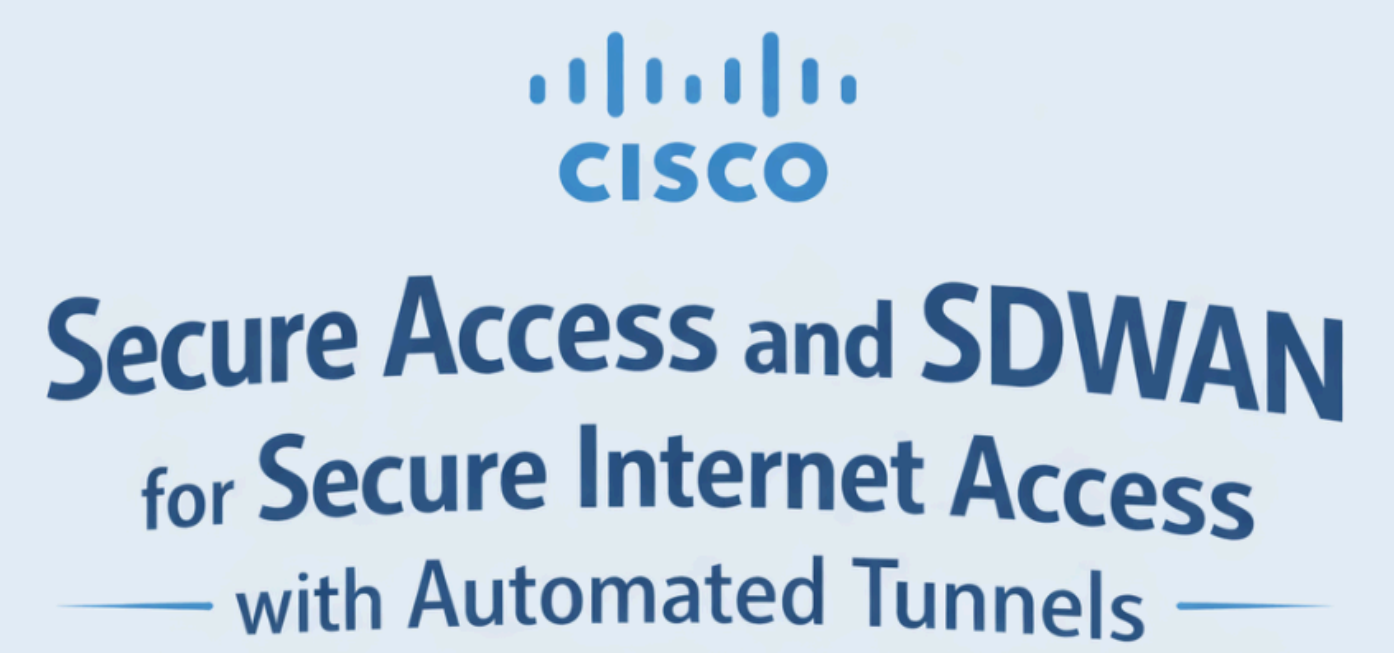
Configurazione dell'accesso sicuro con i tunnel automatizzati SD-WAN per l'accesso sicuro a Internet

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Access con SD-WAN Automated Tunnels per Secure Internet Access.



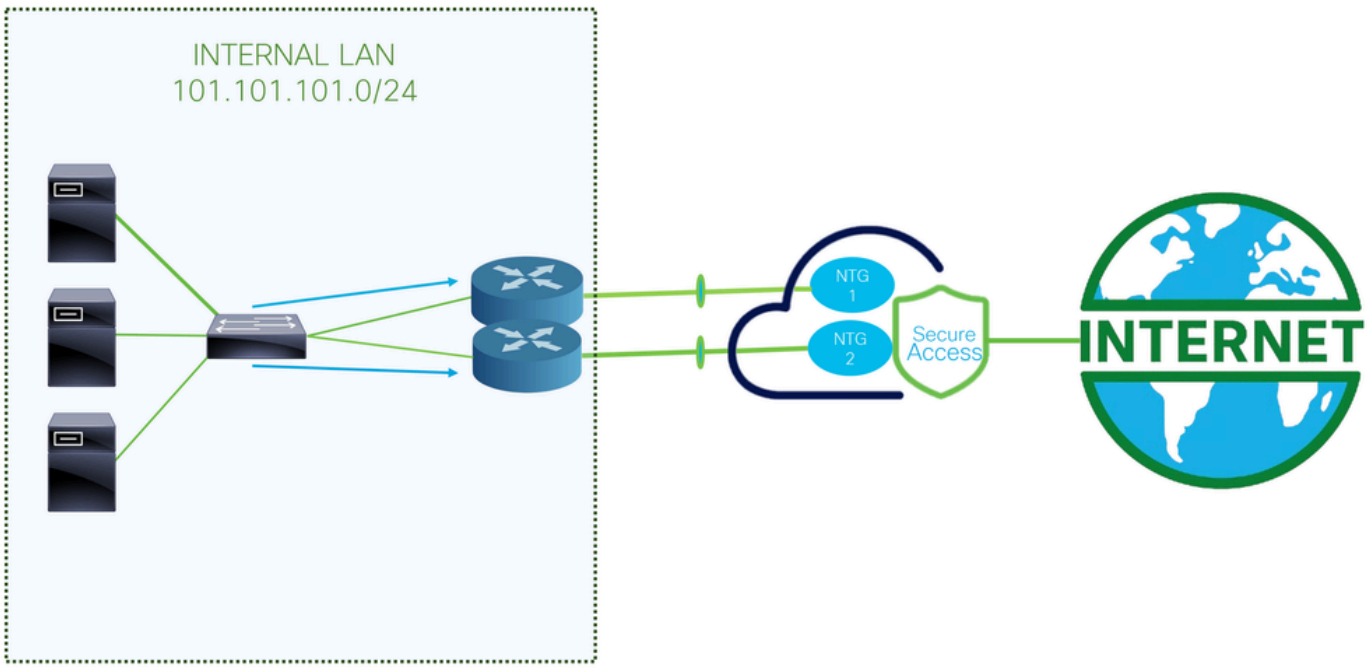
Premesse

Poiché le organizzazioni adottano sempre più applicazioni basate su cloud e supportano forze di lavoro distribuite, le architetture di rete devono evolversi per fornire un accesso sicuro, affidabile e scalabile alle risorse. Secure Access Service Edge (SASE) è un framework che converge la rete e la sicurezza in un unico servizio fornito dal cloud, combinando le funzionalità SD-WAN con funzioni di sicurezza avanzate come Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), sicurezza a livello DNS, Zero Trust Network Access (ZTNA) o VPN integrata per un accesso remoto sicuro.

L'integrazione di Cisco Secure Access con SD-WAN attraverso tunnel automatizzati consente alle organizzazioni di indirizzare il traffico Internet in modo sicuro ed efficiente. SD-WAN offre una selezione intelligente dei percorsi e una connettività ottimizzata tra sedi distribuite, mentre Cisco Secure Access assicura che tutto il traffico venga ispezionato e protetto in base alle policy di sicurezza aziendali prima di raggiungere Internet.

Automatizzando la configurazione del tunnel tra dispositivi SD-WAN e Secure Access, le organizzazioni possono semplificare l'installazione, migliorare la scalabilità e garantire l'applicazione coerente della sicurezza per gli utenti, indipendentemente dalla loro posizione. Questa integrazione è un componente chiave di una moderna architettura SASE, che consente l'accesso sicuro a Internet per filiali, siti remoti e utenti mobili.

Esempio di rete



Architettura utilizzata per questo esempio di configurazione. Come si può vedere, vi sono due router perimetrali:

Se si sceglie di distribuire i criteri a due dispositivi diversi, per ogni router viene configurato un NTG e NAT viene abilitato sul lato Secure Access. In questo modo, entrambi i router possono inviare il traffico dalla stessa origine attraverso i tunnel. Normalmente ciò non è consentito; tuttavia, l'abilitazione dell'opzione NAT per questi tunnel consente a due router perimetrali di inviare il traffico proveniente dallo stesso indirizzo di origine.

Prerequisiti

Requisiti

- Secure Access Knowledge
- Cisco Catalyst SD-WAN Manager release 20.15.1 e Cisco IOS XE Catalyst SD-WAN release 17.15.1 o successive
- Conoscenze intermedie di routing e switching
- Knowledge Base ECMP
- Conoscenza VPN

Componenti usati

- Tenant accesso sicuro
- Catalyst SD-WAN Manager release 20.18.1 e Cisco IOS XE Catalyst SD-WAN release 17.18.1
- Catalyst SD-WAN Manager

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.

Configurazione

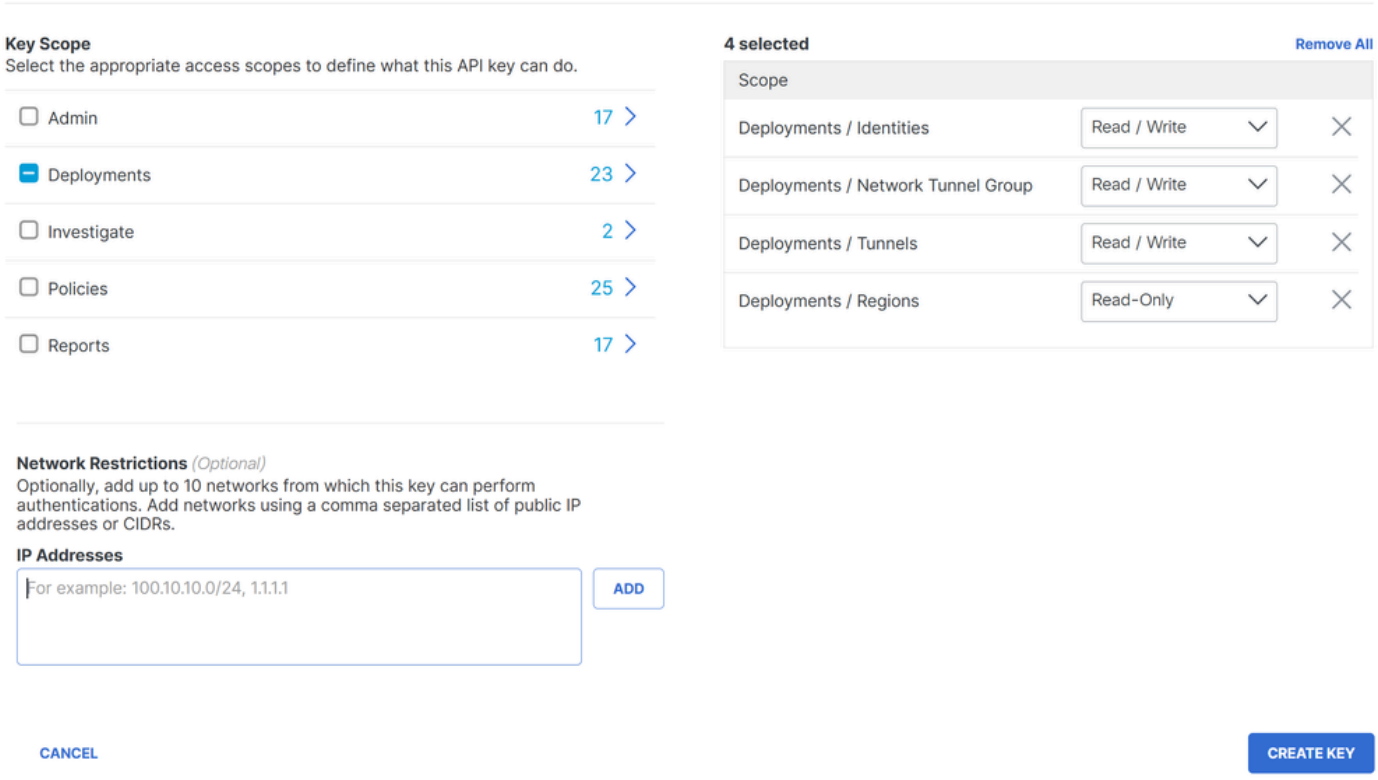
Configurazione accesso sicuro

Creazione API

Per creare i tunnel automatizzati con Secure Access, verificare i passaggi successivi:

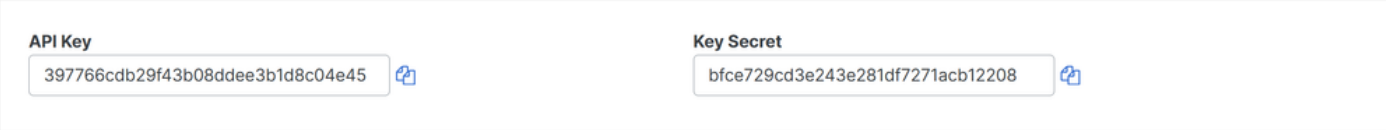
Passare a [Dashboard di accesso protetto](#).

- Fare clic su Admin > API Keys
- Fare clic su Add
- Scegliere le opzioni successive:
  - Deployments / Network Tunnel Group: Lettura/scrittura
  - Deployments / Tunnels: Lettura/scrittura
  - Deployments / Regions: Read-Only
  - Deployments / Identities: Read-Write
  - Expiry Date: Nessuna scadenza



Nota: Facoltativamente, aggiungere fino a 10 reti da cui questa chiave può eseguire autenticazioni. Aggiungere reti utilizzando un elenco separato da virgole di indirizzi IP pubblici o CIDR.

- Fate clic su CREATE KEY per completare la creazione della API Key e della Key Secret.



⚠ Attenzione: Copiarli prima di fare clic su ACCEPT AND CLOSE; in caso contrario, è necessario crearli di nuovo ed eliminare quelli che non sono stati copiati.

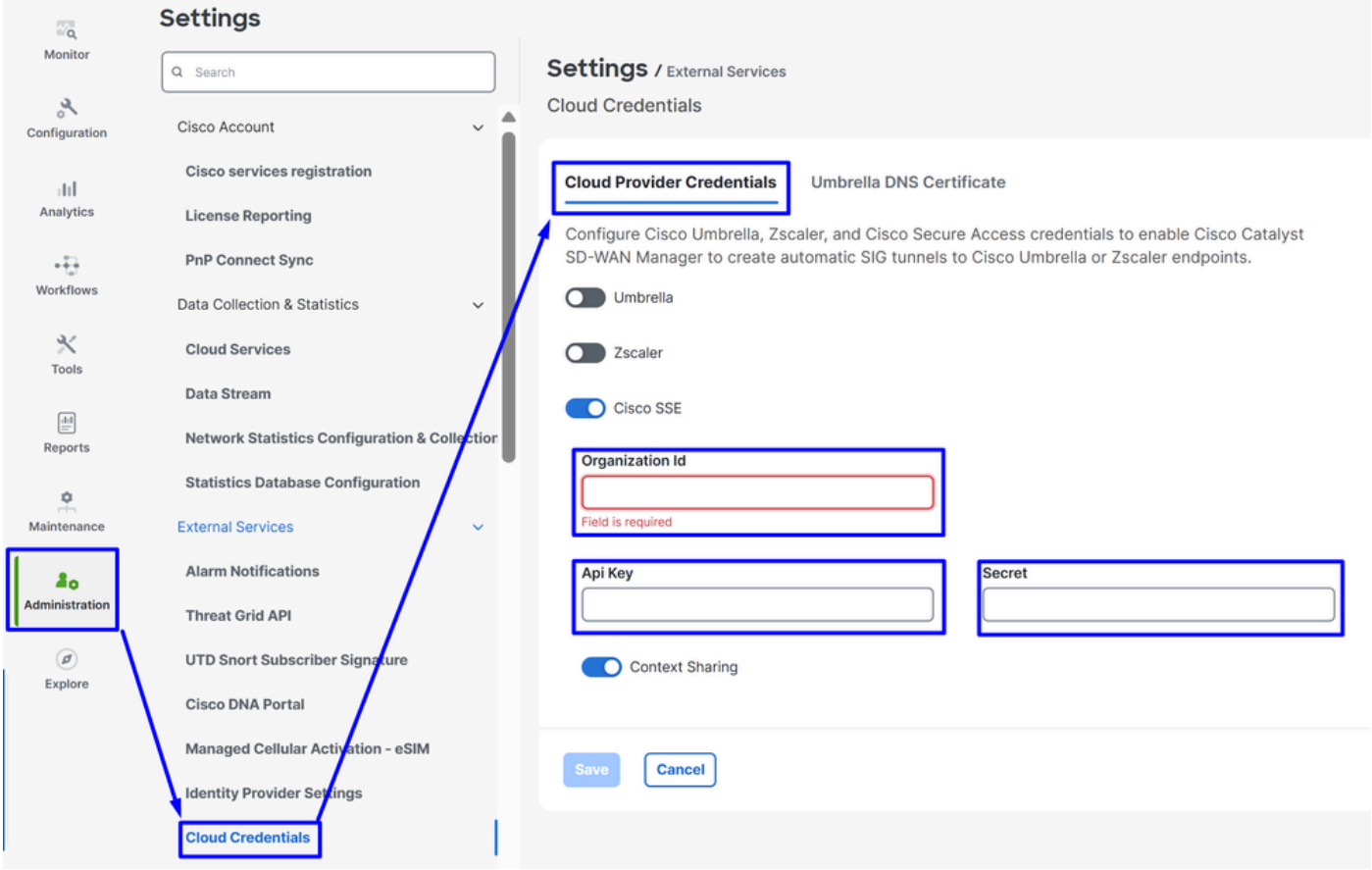
Quindi, per finalizzare, fare clic su ACCEPT AND CLOSE.

Configurazione SD-WAN

Integrazione API

Passare a Catalyst SD-WAN Manager:

- Fare clic su **Administration** >Settings> Cloud Credentials
- Quindi fare clic su Cloud Provider Credentials e abilitare Cisco SSEe compilare API e Impostazioni di organizzazione



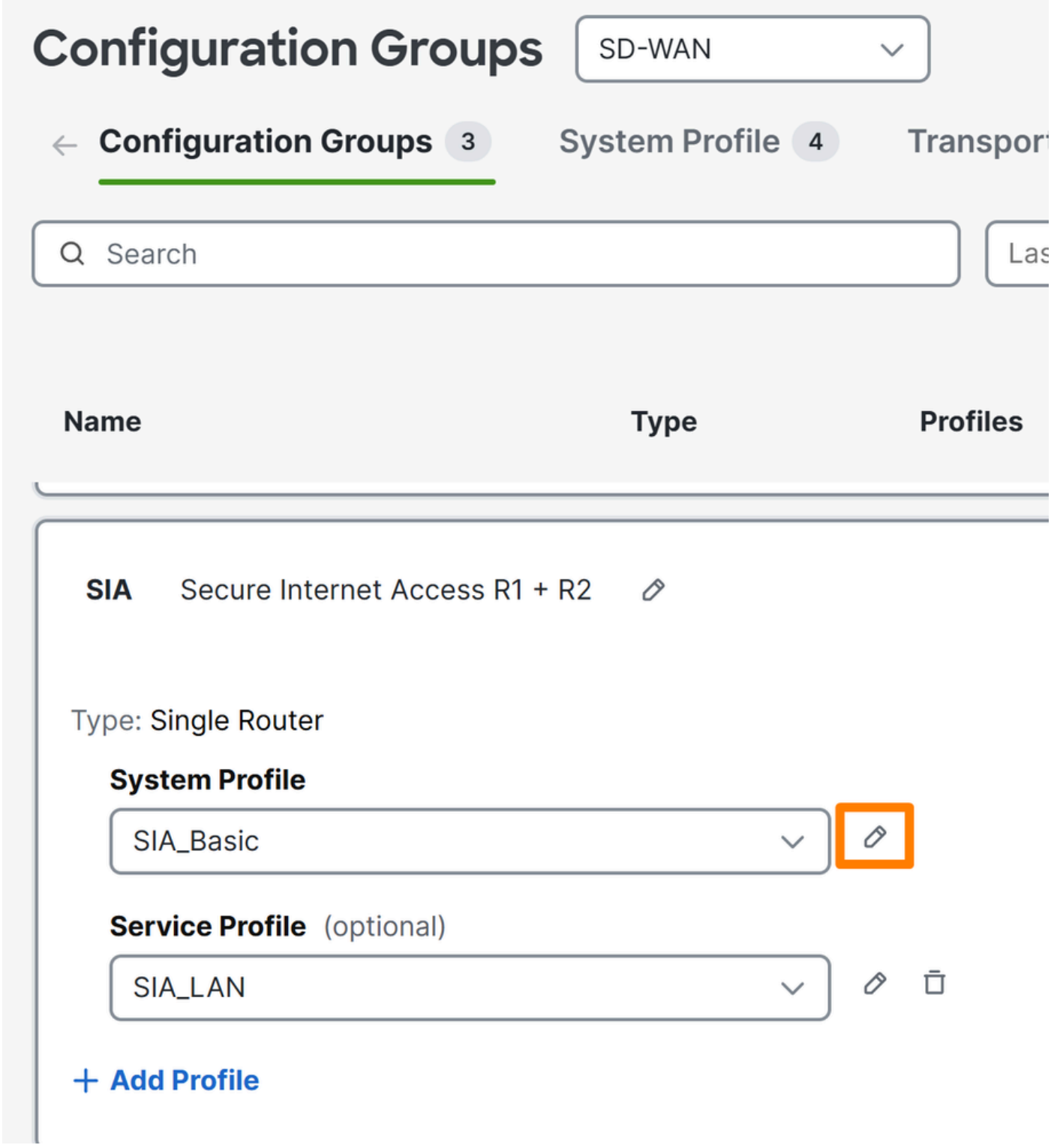
- Organization ID: È possibile ottenere questo dall'URL del dashboard SSE https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Copiarlo dalla fase Configurazione accesso sicuro
- Secret: copiarlo dalla fase Configurazione accesso sicuro

Quindi clicca sul Save pulsante.

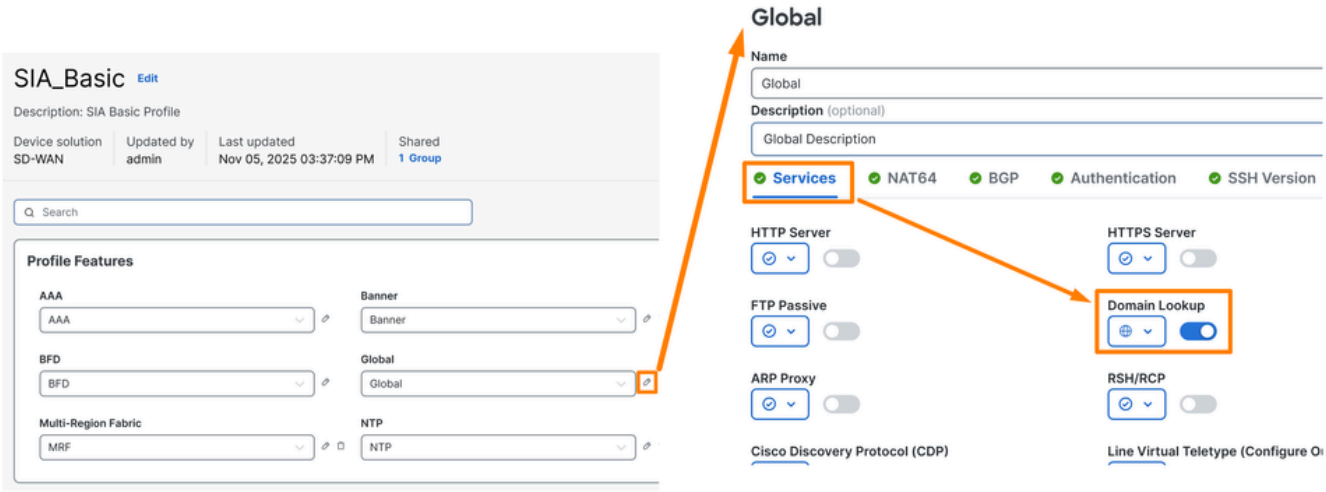
Nota: Prima di procedere con i passaggi successivi, è necessario verificare che SD-WAN Manager e Catalyst SD-WAN Edge dispongano della risoluzione DNS e dell'accesso a Internet.

Per verificare se la ricerca DNS è abilitata, passare a:

- Fare clic su Configurazione > Gruppi di configurazione
- Fare clic sul profilo dei dispositivi Edge e modificare il profilo di sistema



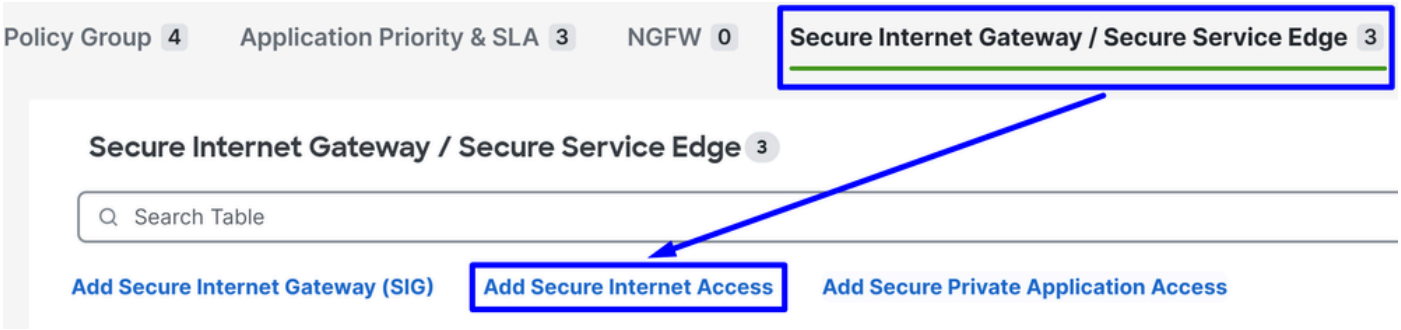
- Modificare quindi l'opzione Global e assicurarsi che l'opzione Domain Resolution sia abilitata



Configura gruppo di criteri

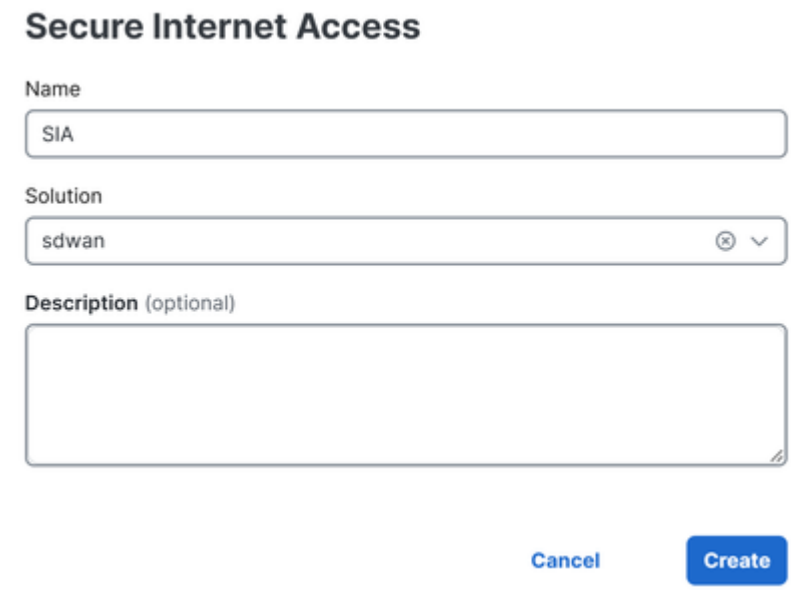
Passare a Configurazione > Gruppi di criteri:

- Fare clic su Secure Internet Gateway / Secure Service Edge> *Add Secure Internet Access*

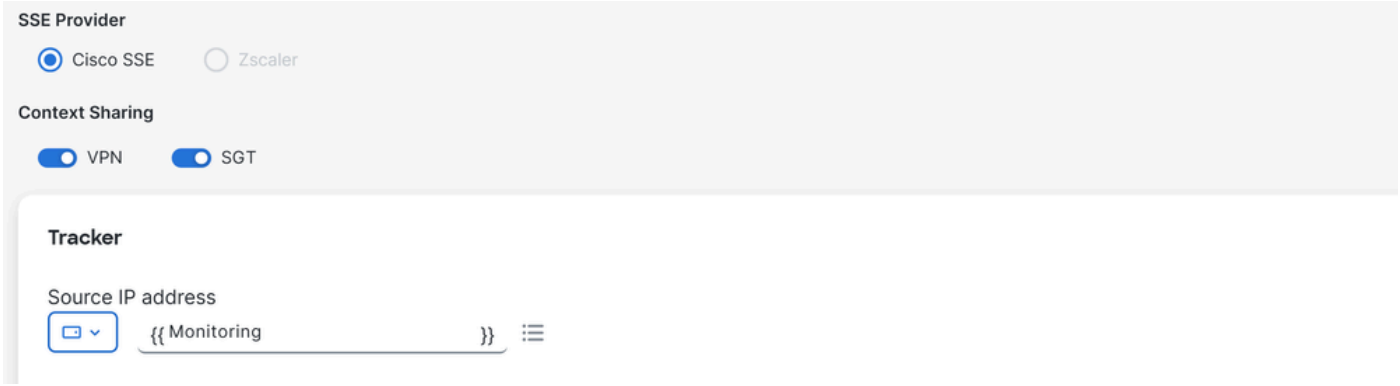


Nota: Nelle versioni precedenti alla 20.18, questa opzione è denominata Add Secure Service Edge (SSE)

- Configurare un nome, una soluzione e fare clic su Create

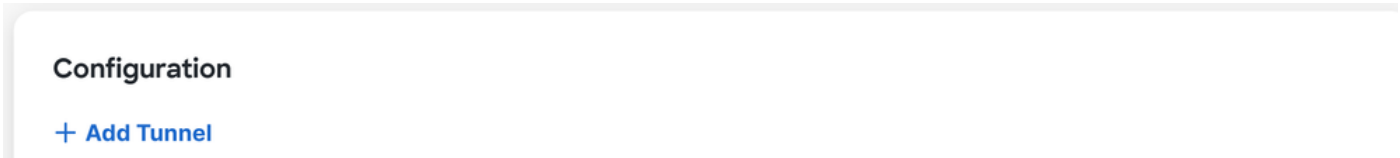


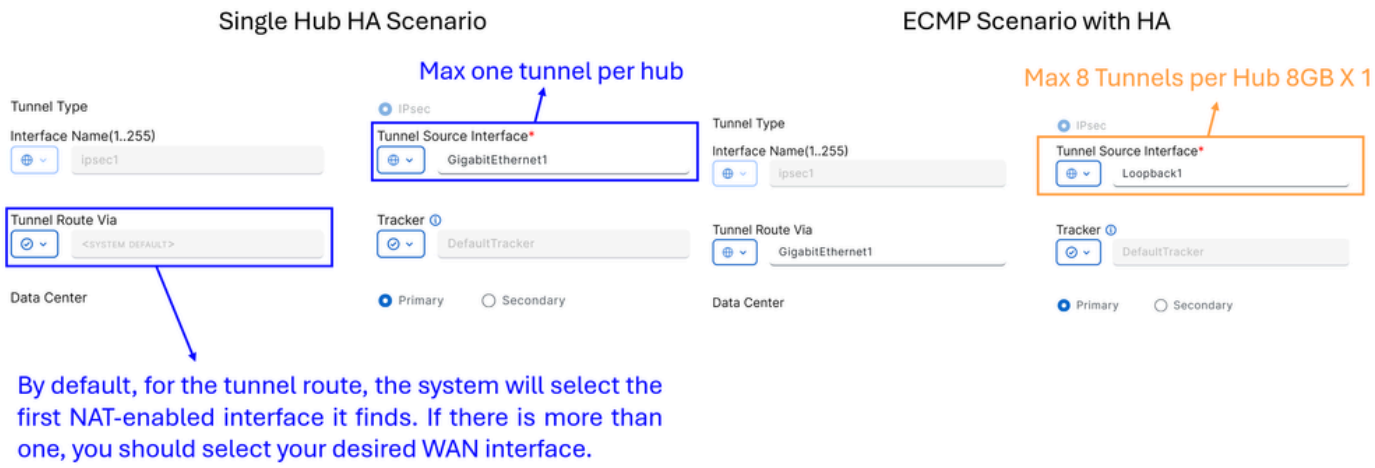
Le configurazioni successive consentono di creare i tunnel dopo aver distribuito la configurazione nei bordi Catalyst SD-WAN:



- SSE Provider: SSE
- Context Sharing: Scegli VPN o/e SGT a seconda delle tue esigenze
- Tracker
  - **Source IP Address**: Scegliere Specifico per dispositivo (ciò consente di modificarlo per dispositivo e di identificare il relativo caso di utilizzo nella fase di distribuzione)

Nella fase di Configuration configurazione dei tunnel:





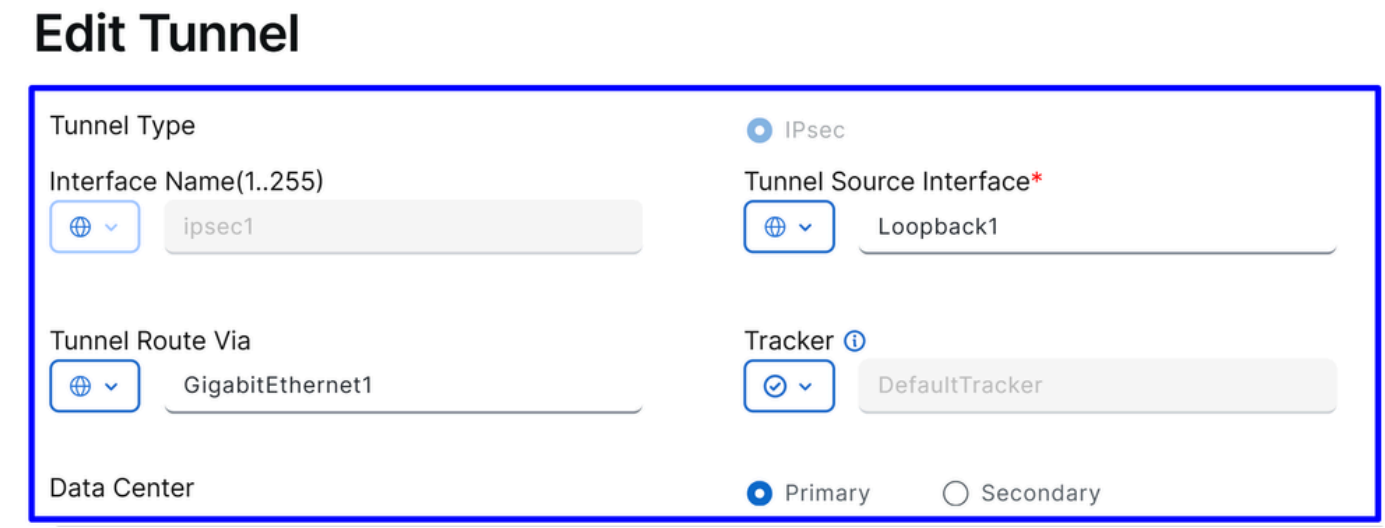
- **Single Hub HA Scenario**: In questo scenario, è possibile configurare l'elevata disponibilità utilizzando un NTG come attivo e un altro come passivo, con un throughput massimo di 1 Gbps per NTG
- ECMP Scenario with HA: In questo scenario, è possibile configurare fino a 8 tunnel per hub, supportando un totale di fino a 16 tunnel per NTG. Questa configurazione consente un throughput più elevato attraverso i tunnel

---

Nota: Se le interfacce di rete hanno un throughput superiore a 1 Gbps e si richiede la scalabilità, è necessario utilizzare le interfacce di loopback. In caso contrario, è possibile utilizzare le interfacce standard sul dispositivo. per abilitare ECMP dal lato accesso sicuro.

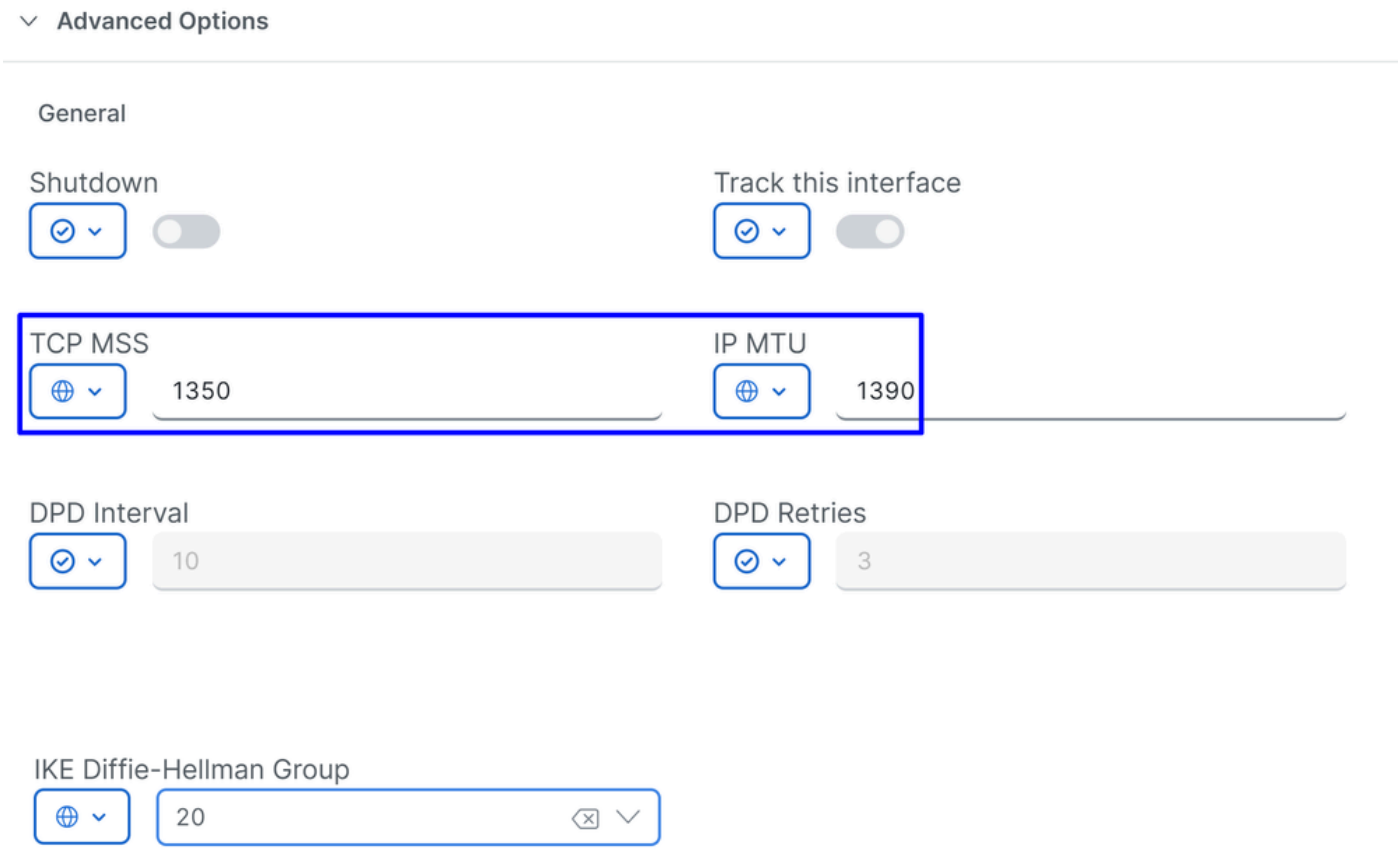
Avviso: Per configurare le interfacce di loopback per uno scenario ECMP, è necessario innanzitutto configurare le interfacce di loopback in Configuration Groups >Transport & Management Profile, in base alla policy utilizzata nel router.

- Fare clic suAdd Tunnel



- Interface Name: ipsec1, ipsec2, ipsec3 e così via
- Tunnel Source Interface: Scegliere le interfacce di loopback o una specifica da cui stabilire il tunnel
- **Tunnel Route Via**: Se si sceglie Loopback, è necessario selezionare l'interfaccia fisica da cui si desidera instradare il traffico. Se non si seleziona Loopback, questa opzione è visualizzata in grigio e il sistema trova la prima interfaccia abilitata NAT. Se sono presenti più interfacce, è necessario selezionare quella desiderata
- **Data Center**: Ciò significa a quale hub in accesso sicuro viene stabilita la connessione

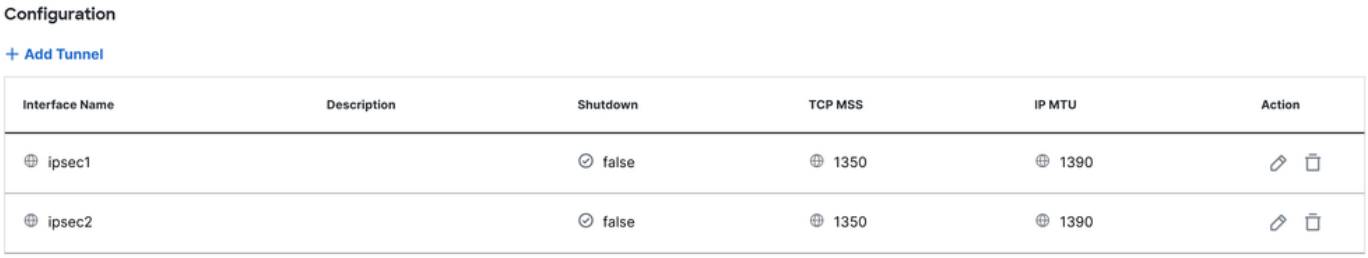
Nella parte successiva della configurazione del tunnel, è possibile configurare i tunnel con le best practice fornite da Cisco.



- TCP MSS: 1350
- IP MTU: 1390
- IKE Diffie-Hellman Group: 20

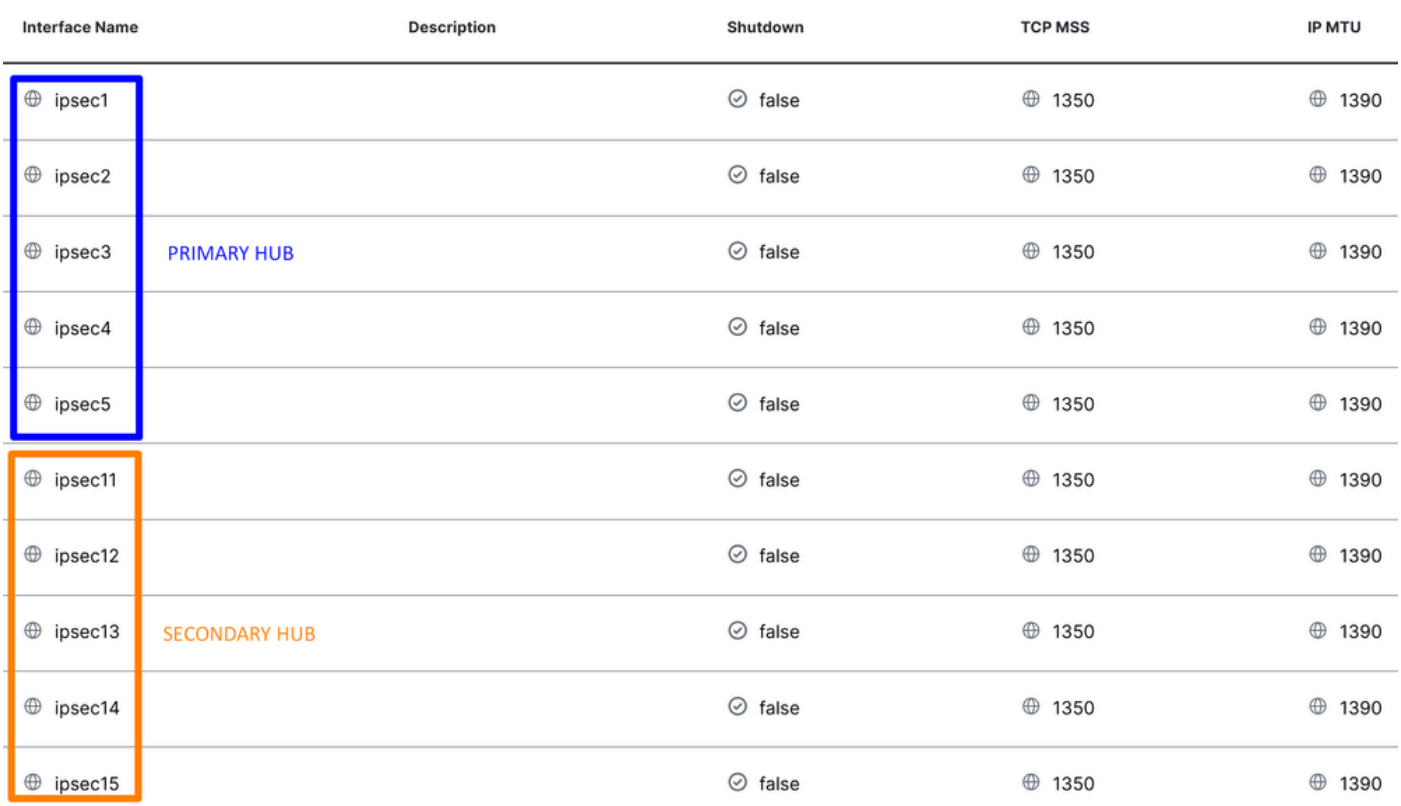
Sarà quindi necessario configurare il tunnel secondario che punta al data center secondario.

SCENARIO HUB SINGOLO HA

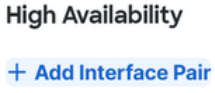


Questo è il risultato finale quando si utilizza la distribuzione dello scenario normale.

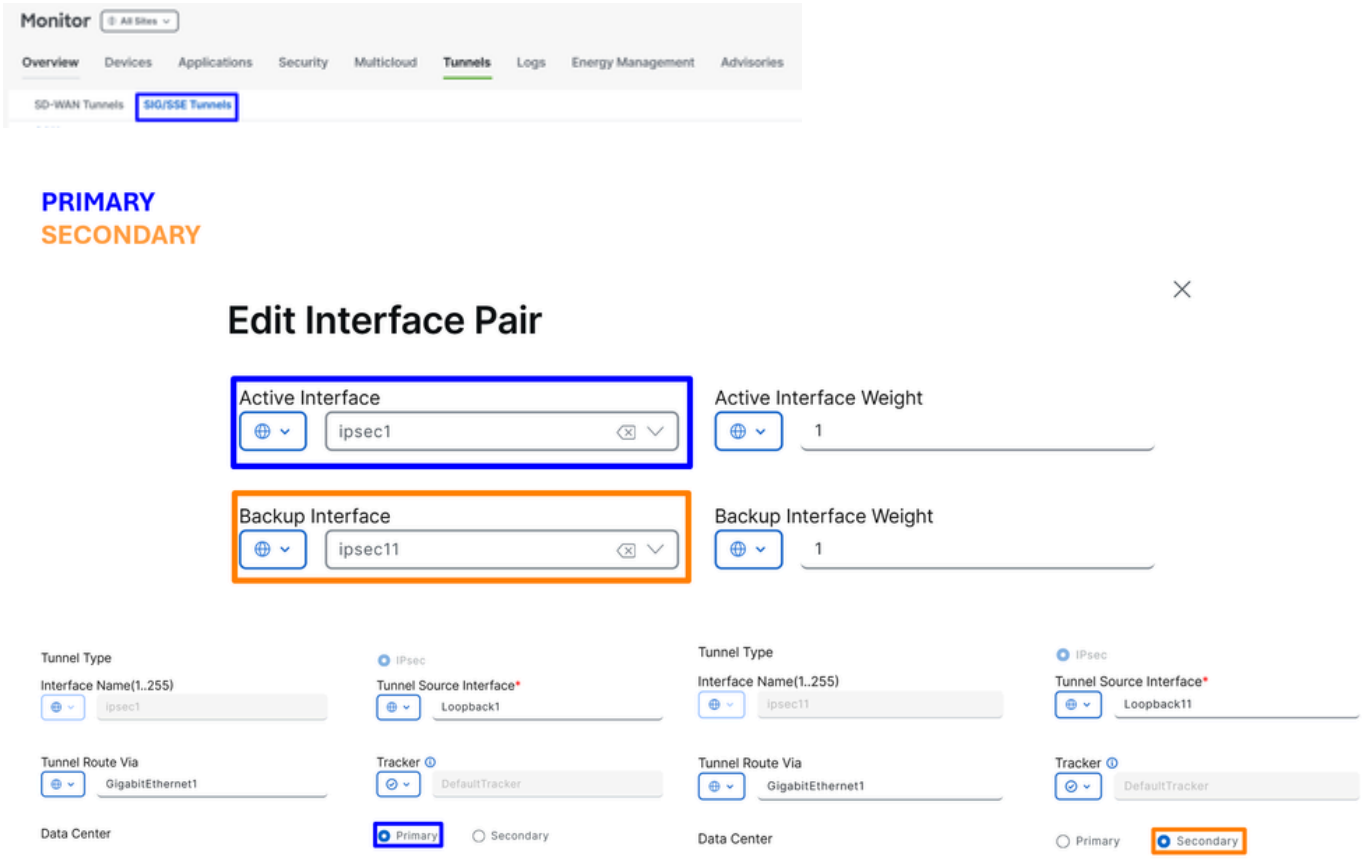
ECMP SCENARIO WITH HA



È quindi necessario configurare la disponibilità elevata nel criterio Secure Internet.



Fare clic su Add Interface Pair:

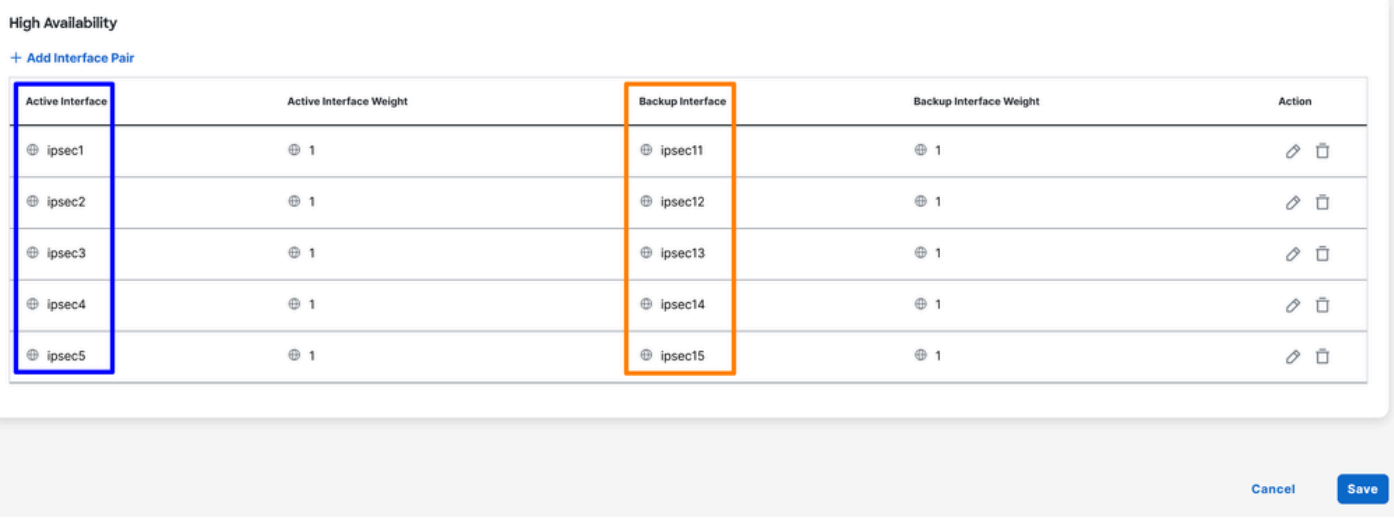


In questo passaggio sarà necessario configurare il tunnel primario e secondario per ciascuna coppia di tunnel che si sta configurando. Ciò significa che ogni tunnel ha il proprio backup. Ricordate, questi tunnel sono stati creati come primari e secondari per questo scopo esatto. "Active interface" si riferisce al tunnel primario, mentre "Backup interface" si riferisce al tunnel secondario:

- Active Interface: Primario
- Backup Interface: Secondaria

Avviso: Se questo passaggio viene ignorato, i tunnel non verranno visualizzati e non verrà stabilita alcuna connessione dai router ad Accesso protetto.

Dopo aver configurato High Availability per i tunnel, l'impostazione viene visualizzata come mostrato nell'immagine seguente. Nell'esempio di laboratorio utilizzato per questa guida, cinque tunnel sono mostrati in HA. Il numero di tunnel può essere regolato in base alle esigenze.



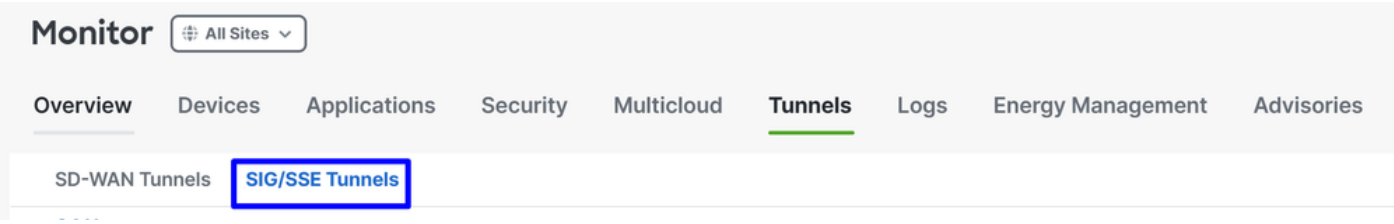
Nota: Un massimo di 8 coppie di tunnel (16 tunnel: 8 primario e 8 secondario) può essere configurato in SD-WAN Catalyst vManage. Cisco Secure Access supporta fino a 10 coppie di tunnel.

- Fare clic su Save

Dopo questo punto, se tutto è configurato correttamente, i tunnel appaiono come UP in SD-WAN Manager and Secure Access.

Per la verifica in SD-WAN, vedere i passaggi successivi:

- Fare clic su Monitor > Tunnels
- Quindi fai clic suSIG/SSE Tunnels

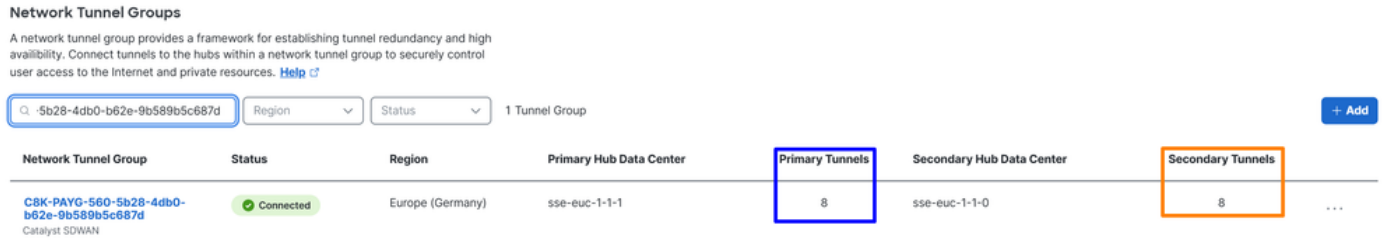


Inoltre, è possibile vedere i tunnel impostati per Cisco Secure Access UP o meno.

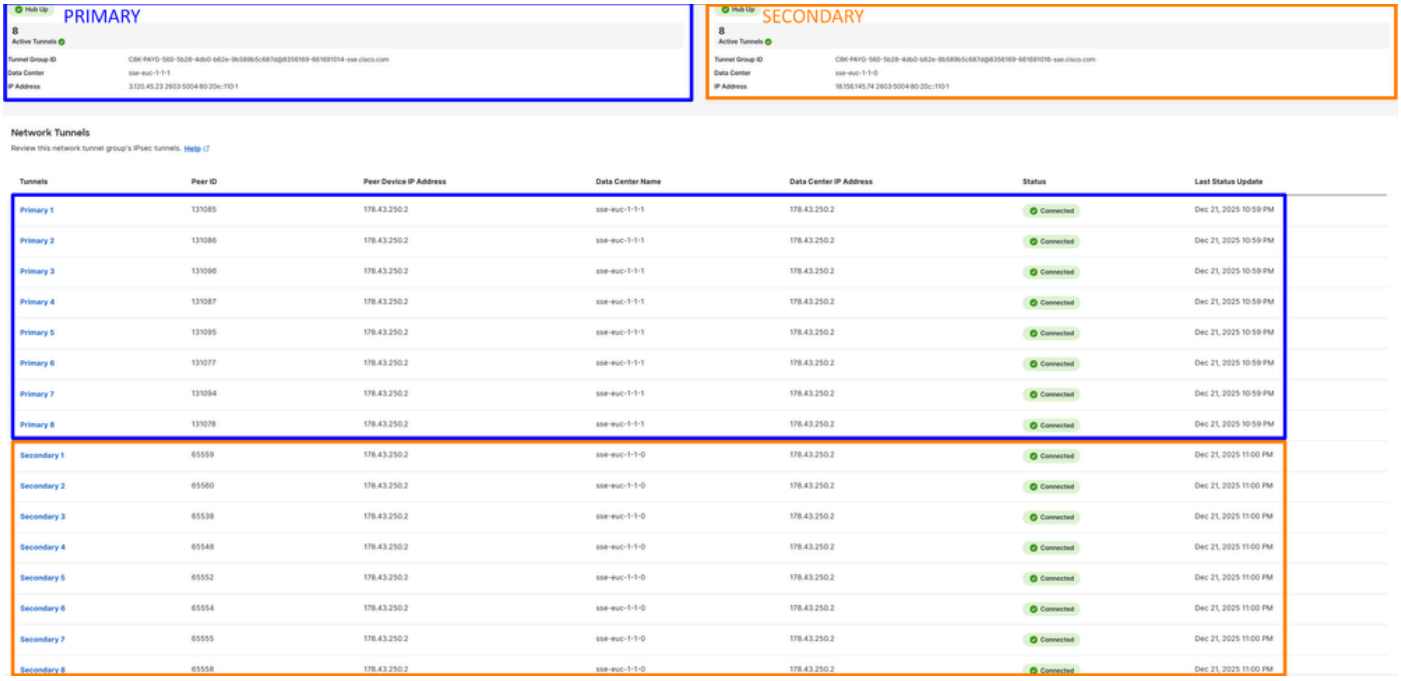
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000002	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000003	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000004	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000005	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000006	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000007	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000008	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000011	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000012	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000013	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000014	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000015	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000016	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000017	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000018	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

Per eseguire la verifica inSecure Access, verificare i passaggi seguenti:

- Fare clic su Connect > Network Connections



In una visualizzazione dettagliata, fare clic sul nome del tunnel:



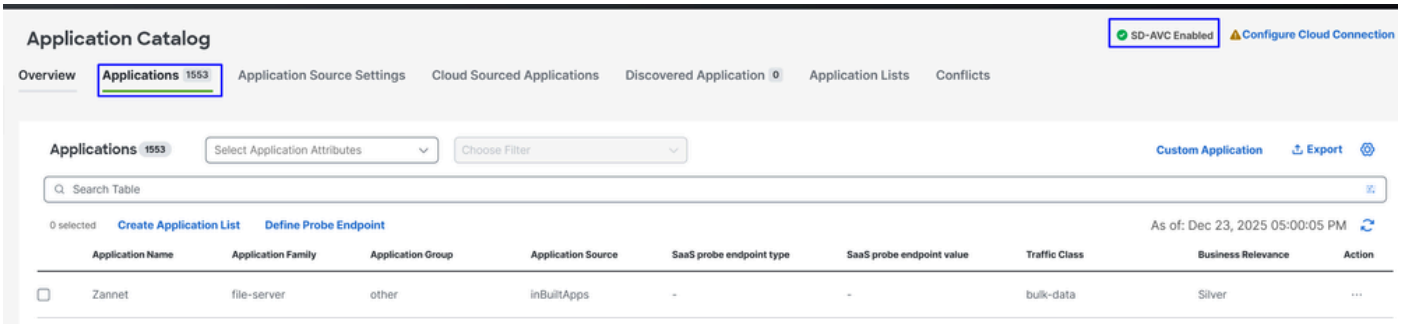
In seguito, è possibile passare alla fase, Create your Custom Bypass FQDN or APP in SD-WAN

Crea il tuo FQDN o APP di bypass personalizzato in SD-WAN (OPZIONALE)

Esistono casi di utilizzo speciali in cui è necessario creare il bypass dell'applicazione e l'FQDN o l'IP che è possibile applicare ai criteri di routing:

Passare al portale SD-WAN Manager:

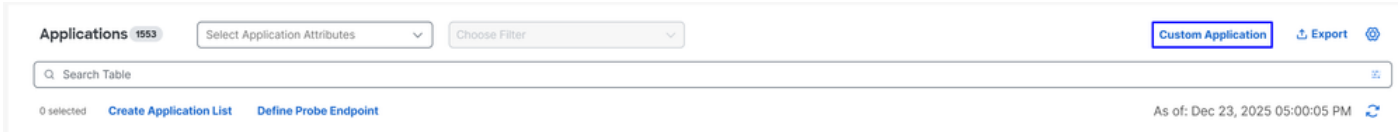
- Fare clic su Configuration > Application Catalog > Applications



Suggerimento: Se si esegue una versione precedente alla 20.15, è possibile creare applicazioni personalizzate in Elenchi criteri

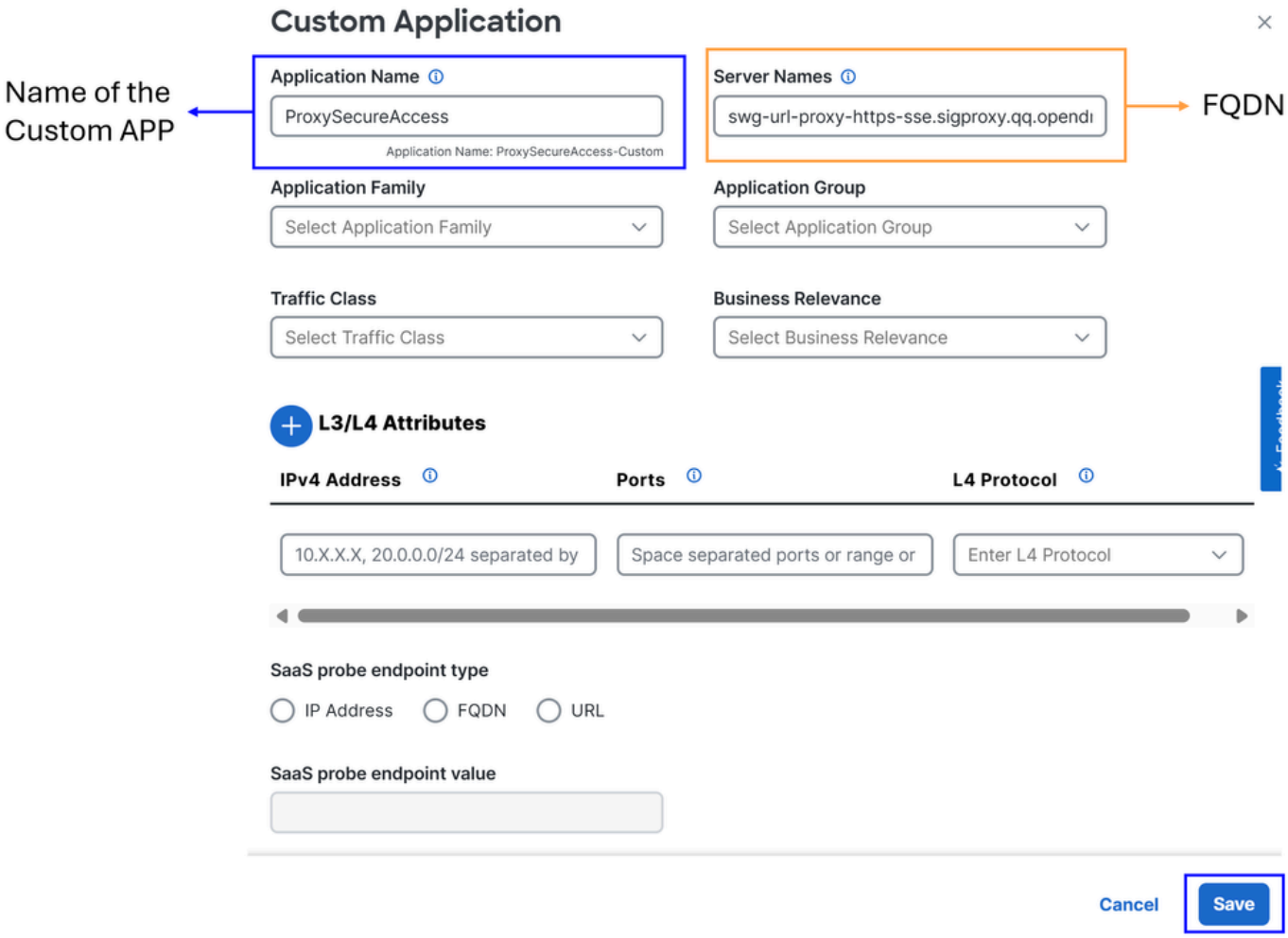
Nota: Per poter accedere al Catalogo applicazioni, è necessario abilitare SD-AVC.

- Fare clic su Custom Application



In questa fase, viene configurata un'esclusione di base utilizzando l'FQDN Secure Client - Umbrella Module SWG:

ProxySecureAccess

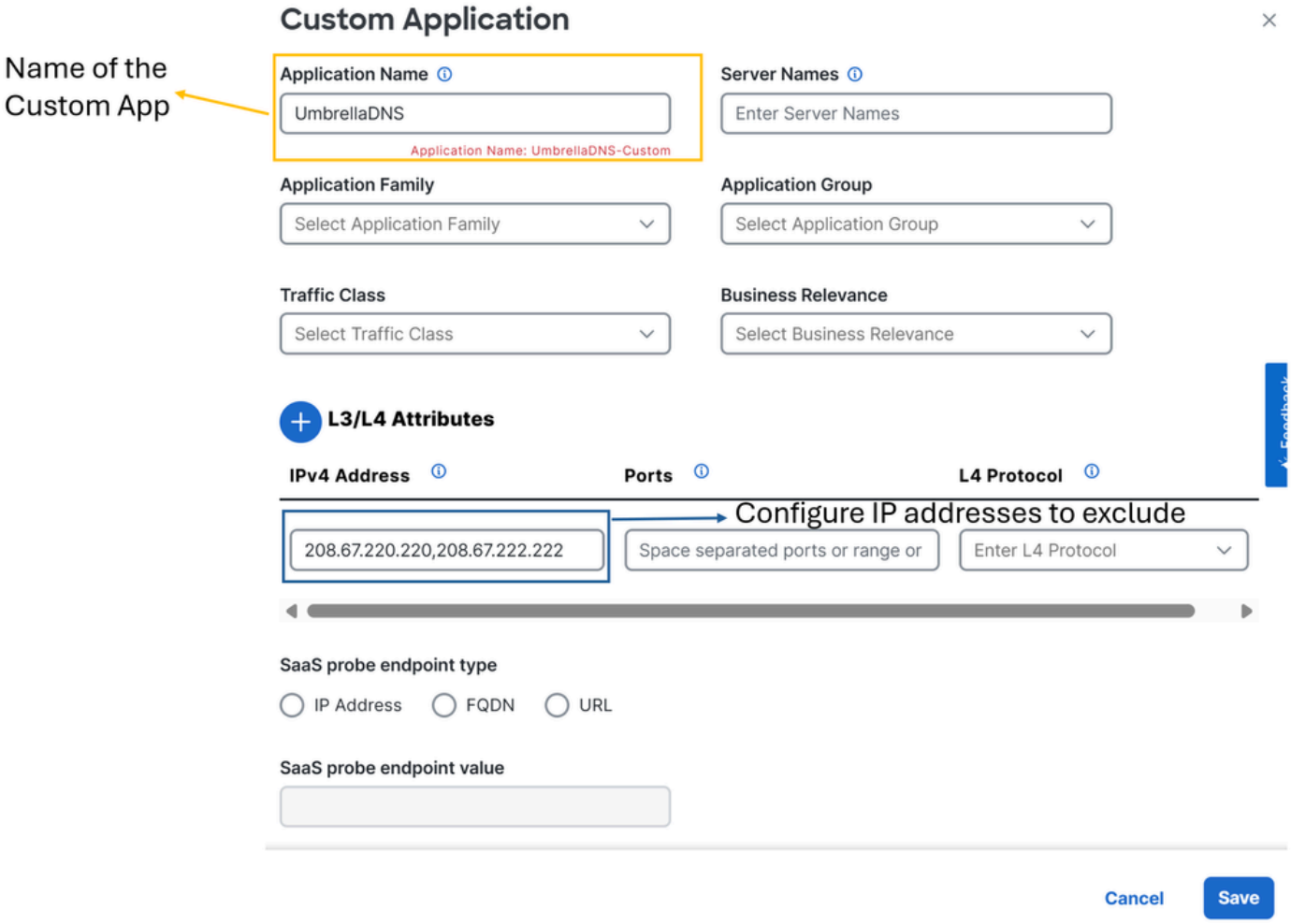


- Server Name: Usare l'FQDN che si desidera ignorare (in questo esempio sono configurati l'FQDN di SWG)
  - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Fare clic su Save

Nota: Modificare ORGID con il numero dell'organizzazione SSE.

Successivamente, viene creata un'esclusione di base; in questo caso, i server DNS Umbrella:

UmbrellaDNS



È ora possibile procedere con le configurazioni dei criteri di routing.

Instradamento del traffico

In questo passaggio, è necessario indirizzare il traffico Internet attraverso i tunnel per proteggerlo tramite Cisco Secure Access. In questo caso, si utilizza una policy di routing flessibile che consente di ignorare determinati tipi di traffico, evitando in tal modo l'invio di traffico indesiderato tramite l'accesso sicuro o evitando potenziali errori.
Innanzitutto, è necessario definire i due metodi di instradamento che è possibile utilizzare:

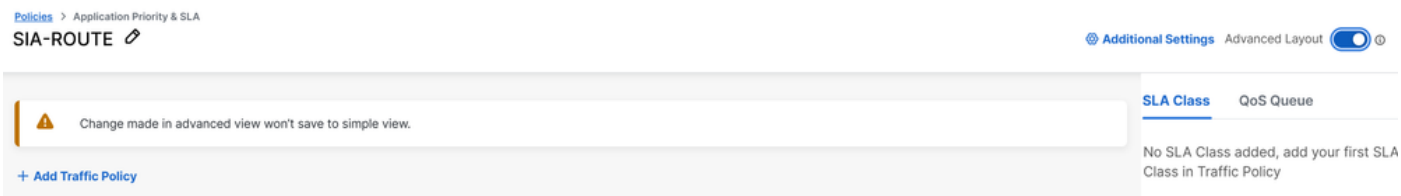
- Configuration > Configuration Groups > Service Profile > Service Route: Questo metodo fornisce l'indirizzamento a Secure Access, ma non è flessibile.
- **Configuration** > Policy Groups > Application Priority & SLA: Questo metodo offre diverse opzioni di routing all'interno di SD-WAN e, cosa più importante, consente di evitare il traffico specifico in modo che non venga inviato tramite Secure Access.

Per la flessibilità e l'allineamento con le best practice, viene utilizzata questa configurazione, Application Priority & SLA:

- Fare clic su **Configuration** > Policy Groups > Application Priority & SLA
- Quindi fai clic su Application Priority & SLA Policy

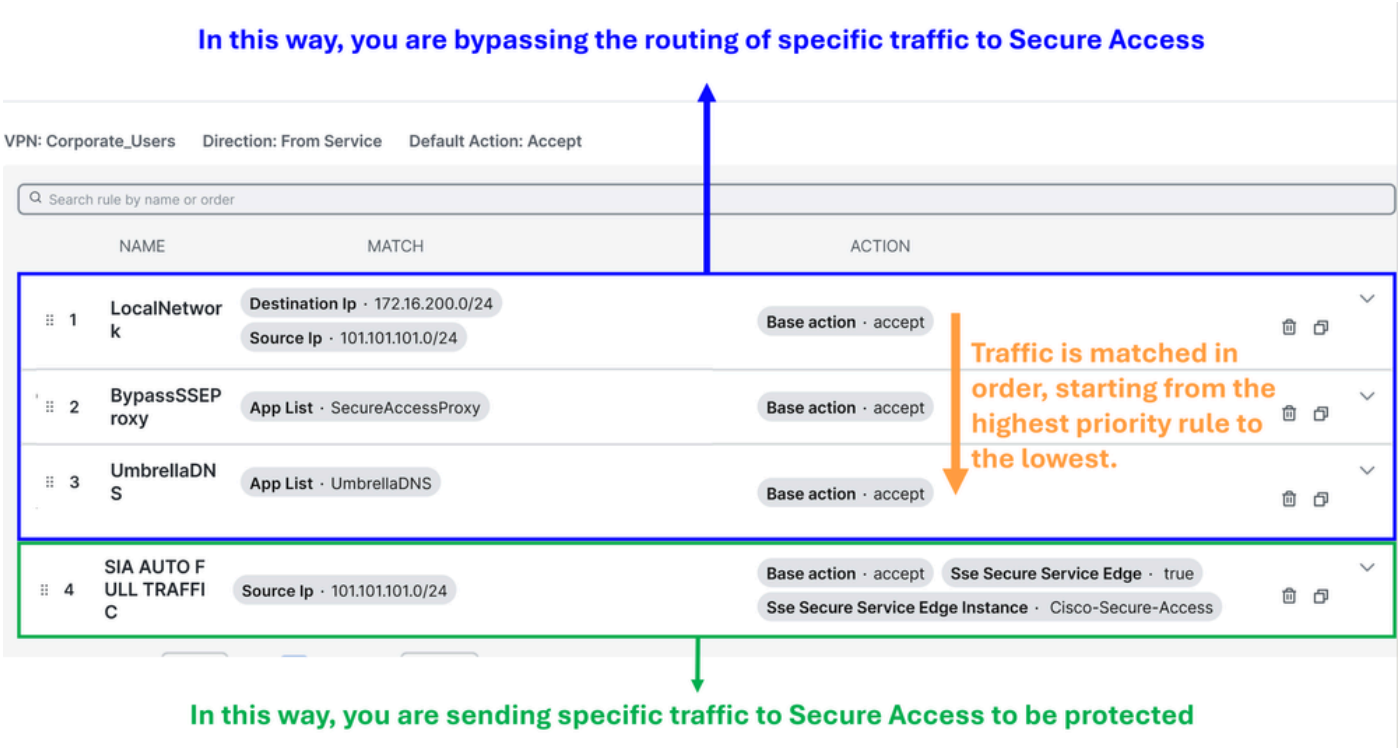
- Configurare il nome di un criterio e fare clic su Create

- Abilita Advanced Layout
- Fare clic su + Add Traffic Policy



- Policy Name: Nome che regola l'elemento allo scopo dell'elenco di criteri per il traffico
- VPN(s): Scegliere la VPN del servizio dell'utente da cui instradare il traffico
- **Direction**: Dal servizio
- Default action: Accetta

A questo punto è possibile iniziare a creare la politica sul traffico:



1. Local Network Policy (Optional): Origine 101.101.101.0/24, Destinazione 172.16.200.0/24. Questa route impedisce l'invio del traffico all'interno della rete a Cisco Secure Access. In genere, i clienti non eseguono questa operazione, in quanto il routing interno viene in genere gestito dal router di distribuzione nelle installazioni SD-WAN. Questa configurazione garantisce che

il traffico interno tra queste subnet non venga instradato ad Accesso sicuro, a seconda che lo scenario lo richieda o meno (facoltativo, in base all'ambiente di rete)

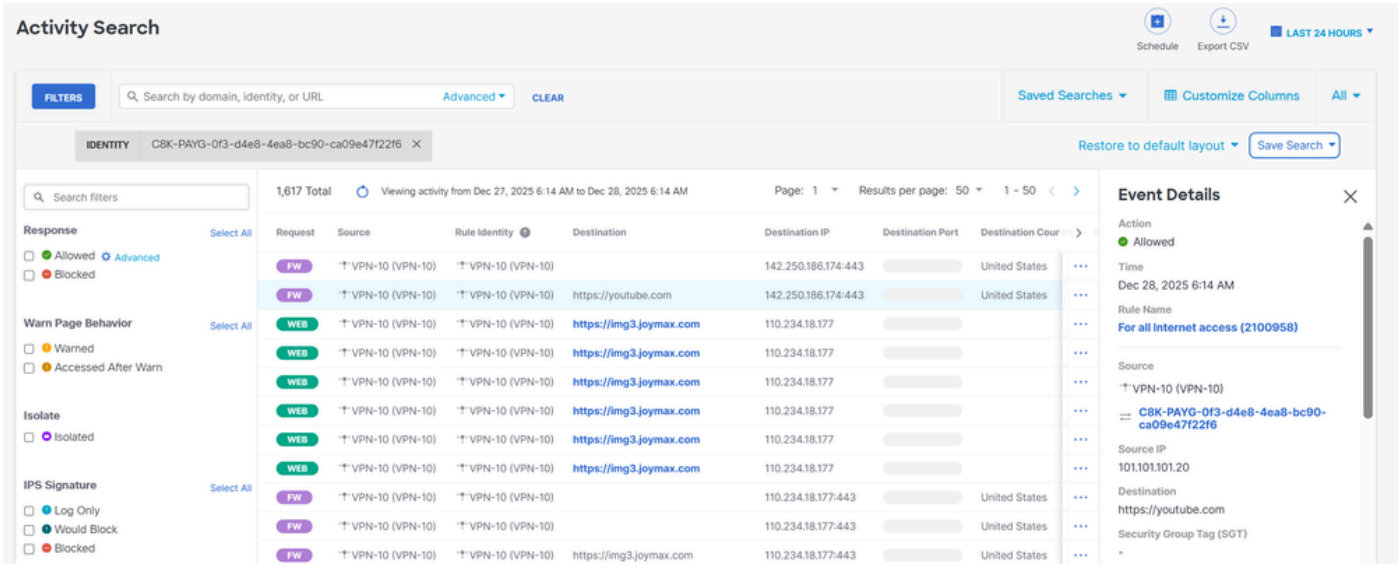
2. **BypassSSEProxy (Optional)**: Questa policy impedisce ai computer interni con il modulo Cisco Umbrella in Secure Client e SWG abilitato di inviare nuovamente il traffico proxy al cloud. Il routing del traffico proxy al cloud non è considerato una procedura ottimale.
3. UmbrellaDNS (Best Practice): Questo criterio impedisce l'invio tramite tunnel delle query DNS destinate a Internet. Non è consigliabile inviare query DNS ai resolver Umbrella (208.67.222.222,208.67.220.220) tramite il tunnel.
4. SIA AUTO FULL TRAFFIC: Questo criterio consente di instradare tutto il traffico dall'origine 101.101.101.0/24 a Internet attraverso i tunnel SSE creati in precedenza, garantendo che il traffico sia protetto nel cloud.

Verifica

per verificare se il traffico sta già inondando tramite Cisco Secure Access, passare al percorso Events o Activity Search o Network-Wide Path Insights e filtrare in base all'identità del tunnel:

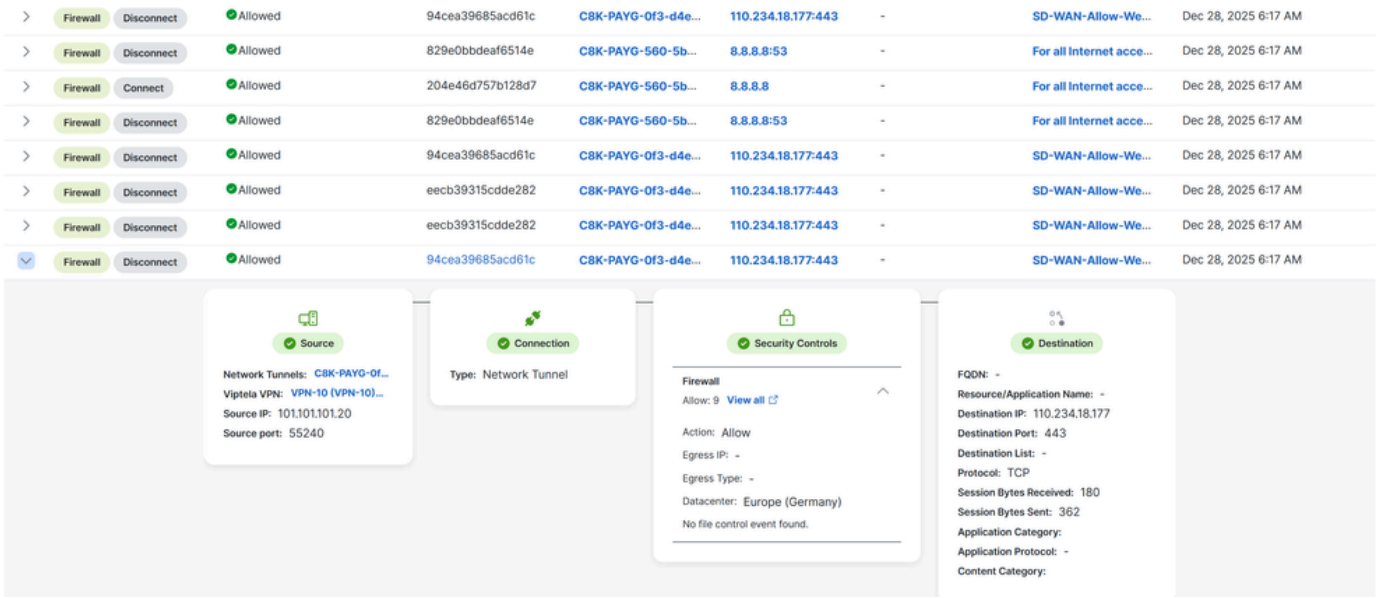
Accesso sicuro - Ricerca attività

Passare a Monitor > Activity Search:



Accesso sicuro - Eventi

Passare a Monitor > Events:

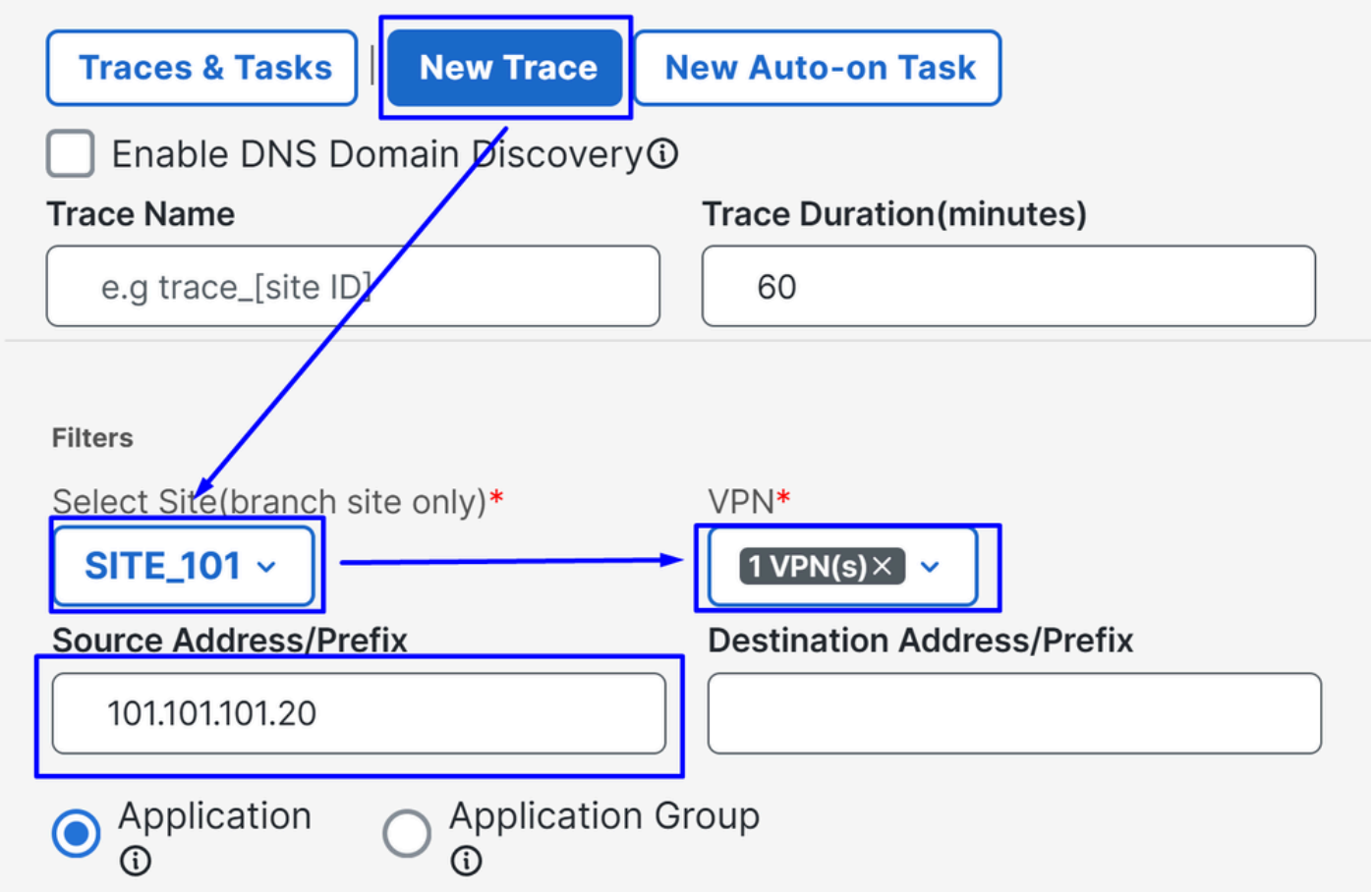


Nota: Accertarsi di disporre del criterio predefinito con la registrazione attivata. Per impostazione predefinita, questa opzione è disattivata.

Catalyst SD-WAN Manager - Informazioni dettagliate sul percorso di rete

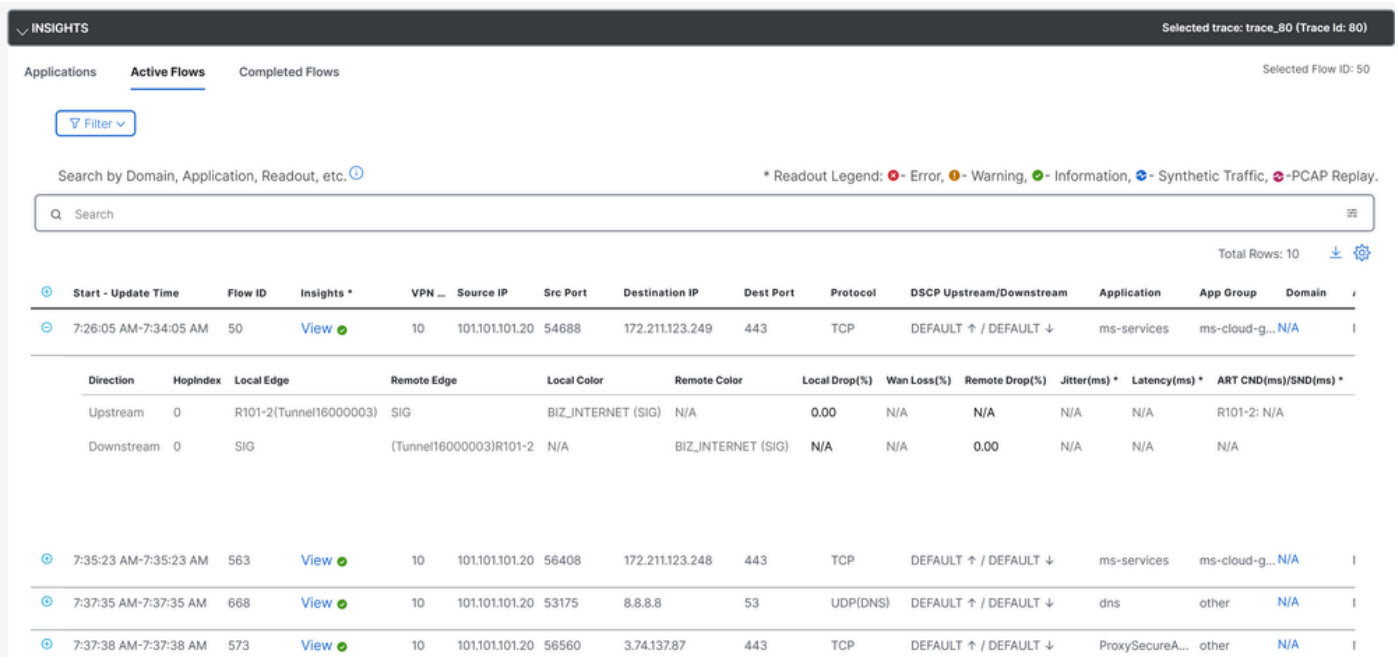
Passare a Catalyst SD-WAN Manager:

- Fare clic su Tools > Network-Wide Path Insights
- Fare clic su New Trace



- Site: Scegli il sito da cui il traffico sta diminuendo
- VPN: Scegli l'ID VPN della subnet da cui il traffico è in aumento
- Source: Inserire l'indirizzo IP o lasciarlo in bianco per filtrare tutto il traffico filtrato dall'indirizzo **Site** e VPN scegliere

Quindi in Insights puoi vedere il traffico che attraversa i tunnel e il tipo di traffico che va verso Secure Access:



Informazioni correlate

- Supporto tecnico Cisco e download
- Cisco Secure Access Help Center
- Guida alla progettazione di Cisco BASE
- Guida alla configurazione della sicurezza di Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN release 17.x
- Soluzione Cisco SASE: Cisco Catalyst SD-WAN integrato con Cisco Secure Access in breve

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).