Configurazione dell'accesso sicuro con i tunnel automatizzati Catalyst SD-WAN per l'accesso privato sicuro

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Access con i tunnel automatizzati Catalyst SD-WAN per un accesso privato sicuro.

Premesse

Man mano che le organizzazioni si spostano al di là delle tradizionali reti perimetrali, accedere in modo sicuro alle risorse private diventa altrettanto importante della sicurezza del traffico Internet. Le applicazioni non sono più limitate a un singolo centro dati, ma si basano su ambienti locali, cloud pubblici e architetture ibride. Questo cambiamento richiede un approccio più flessibile e moderno all'accesso privato.

In questo contesto entrano in gioco un'architettura basata su SASE e Cisco Secure Access. Anziché fare affidamento sui concentratori VPN legacy e sull'accesso alla rete flat, Cisco Secure Access offre una connettività privata come servizio fornito tramite cloud, combinando VPN-as-a-Service (VPNaaS) e Zero Trust Network Access (ZTNA).

Per l'accesso privato a livello di rete, Cisco Secure Access si integra con SD-WAN utilizzando tunnel IPsec da sito a sito automatizzati. Questi tunnel consentono il flusso sicuro del traffico privato tra Secure Access e le reti locali o cloud, mantenendo l'ispezione di sicurezza e l'applicazione delle policy centralizzate nel cloud. Da un punto di vista operativo, questo elimina la necessità di installare e mantenere headend VPN tradizionali e semplifica la scalabilità in base alla crescita degli ambienti.

In un modello VPNaaS, Secure Access funge da punto di terminazione VPN nel cloud. SD-WAN gestisce il routing intelligente e la resilienza con Secure Access e garantisce che il traffico sia protetto e gestito da policy di sicurezza coerenti prima di raggiungere le risorse private.

Cisco Secure Access supporta inoltre architetture tunnel avanzate da sito a sito, tra cui il backhaul multiregionale. Questa funzionalità consente alle organizzazioni di stabilire tunnel per più aree di accesso sicuro contemporaneamente, fornendo ridondanza geografica e maggiore disponibilità. La connessione a aree diverse consente il failover automatico del traffico in caso di interruzioni delle attività a livello di area, riduzione della latenza o eventi di manutenzione.

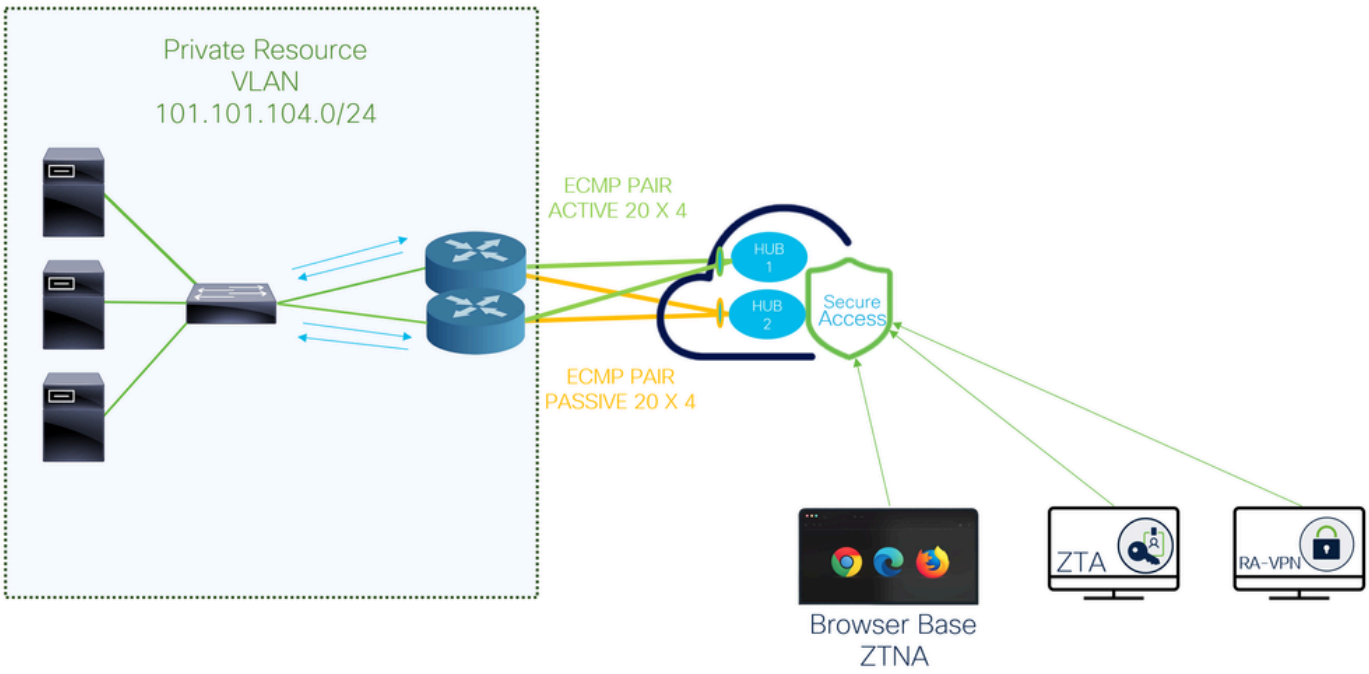
Ad esempio, un'organizzazione può stabilire tunnel da sito a sito dal proprio ambiente SD-WAN

alle aree Secure Access di Londra e Germania. Entrambi i tunnel rimangono attivi, consentendo l'accesso privato resiliente tra le regioni e garantendo la continuità anche se una regione non è più disponibile. Questo design multi-regionale rafforza l'elevata disponibilità, migliora la tolleranza di errore e si allinea ai requisiti di resilienza di livello enterprise.

Per un accesso più granulare, Cisco Secure Access applica il modello ZTNA (Zero Trust Network Access). Anziché concedere agli utenti un'ampia connettività di rete, ZTNA consente l'accesso solo ad applicazioni specifiche, in base all'identità, alla postura del dispositivo e al contesto. Questo approccio riduce in modo significativo la superficie di attacco e si allinea ai principi di Zero Trust.

L'accesso ZTNA è abilitato tramite una combinazione di tunnel da sito a sito e connettori di risorse. I connettori di risorse sono appliance virtuali leggere che stabiliscono connessioni di accesso sicuro solo in uscita, il che significa che le risorse private non devono mai essere esposte direttamente a Internet.

Esempio di rete



Prerequisiti

Requisiti

- Secure Access Knowledge
- Cisco Catalyst SD-WAN Manager release 20.18.2 e Cisco IOS XE Catalyst SD-WAN release 17.18.2 o successive
- Conoscenze intermedie di routing e switching
- Knowledge Base ECMP
- Conoscenza VPN
- Poiché questa integrazione è basata sulla disponibilità controllata, è necessario inviare una

richiesta TAC per richiedere l'abilitazione della funzionalità in Cisco Secure Access

Componenti usati

- Tenant accesso sicuro
- Catalyst SD-WAN Manager release 20.18.2 e Cisco IOS XE Catalyst SD-WAN release 17.18.2
- 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

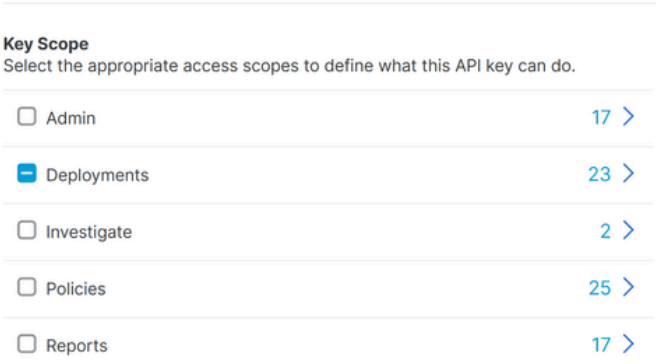
Configurazione accesso sicuro

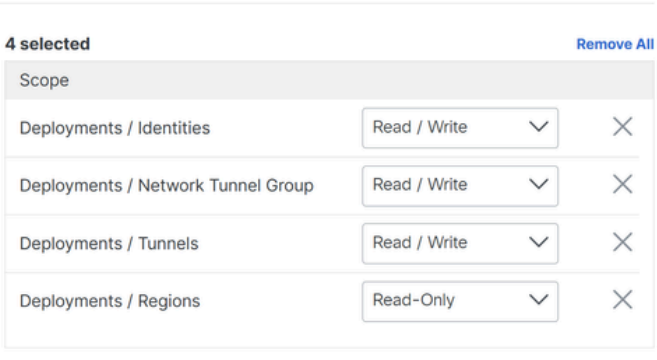
Creazione API

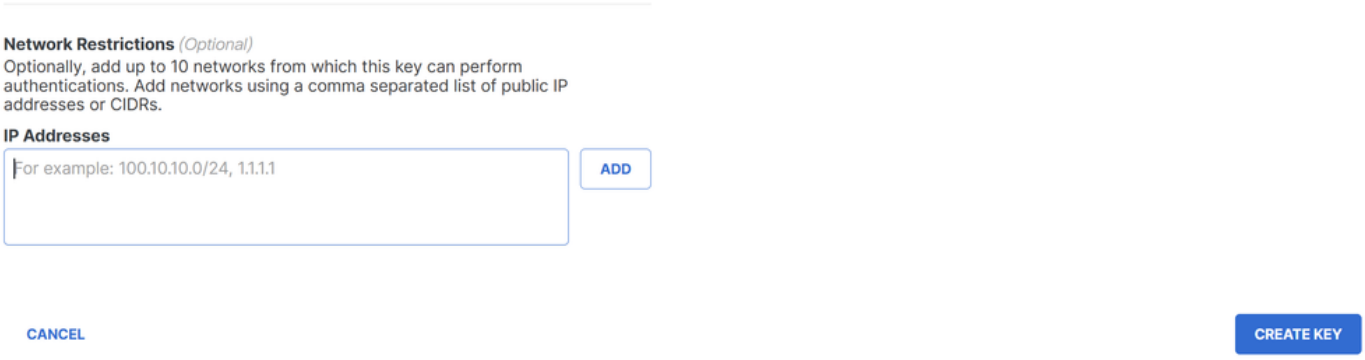
Per creare i tunnel automatizzati con Secure Access, verificare i passaggi successivi:

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

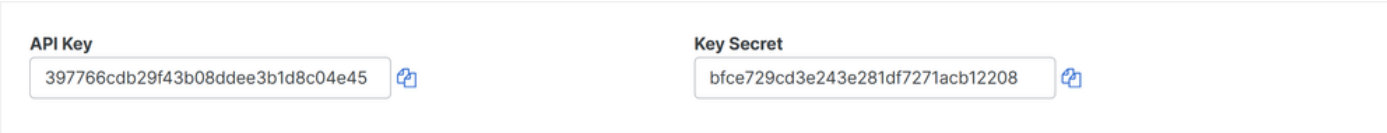






Nota: Facoltativamente, aggiungere fino a 10 reti da cui questa chiave può eseguire autenticazioni. Aggiungere reti utilizzando un elenco separato da virgole di indirizzi IP pubblici o CIDR.

- 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.

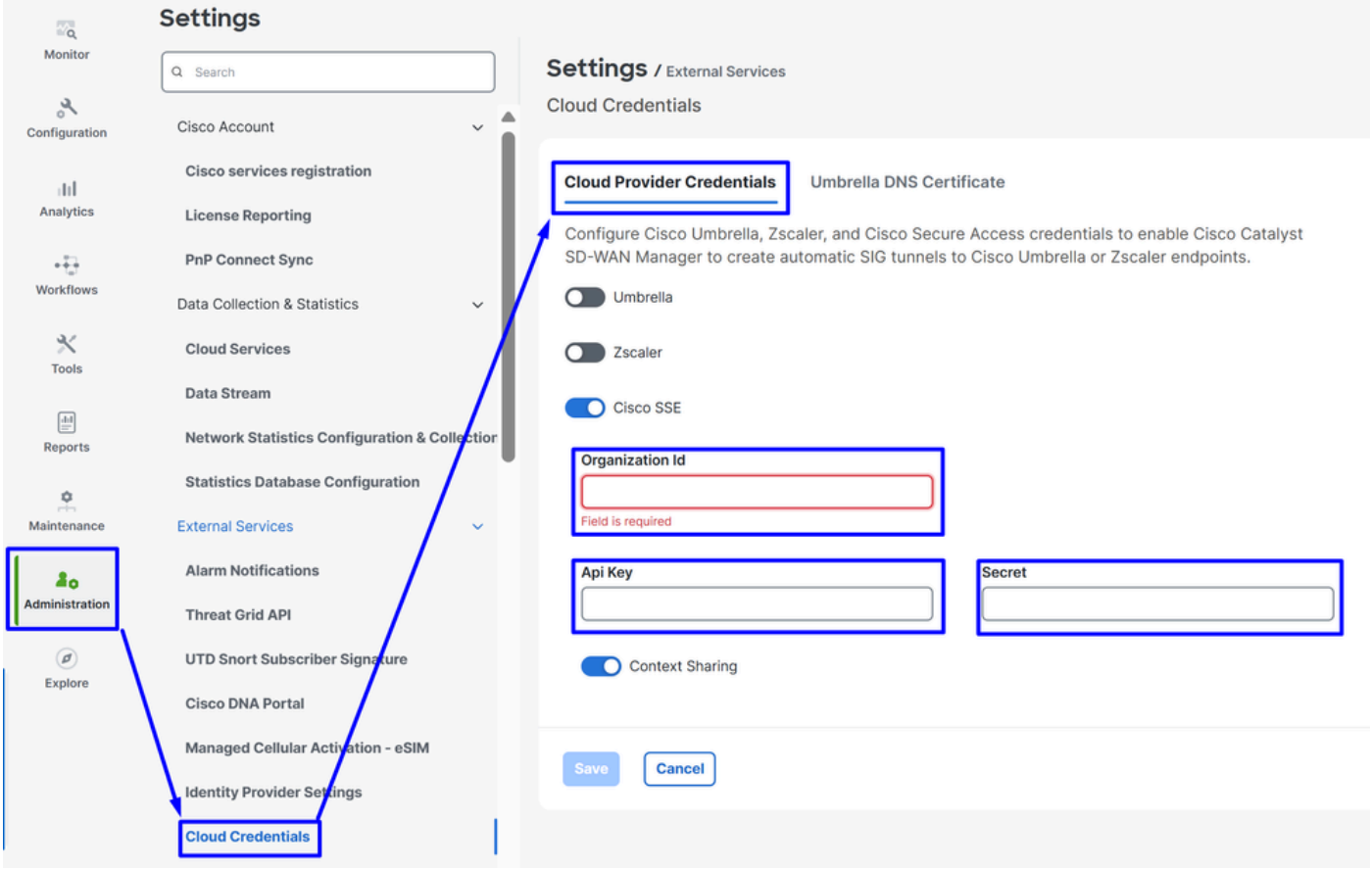
Quindi, per finalizzare, fare clic su ACCEPT AND CLOSE.

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



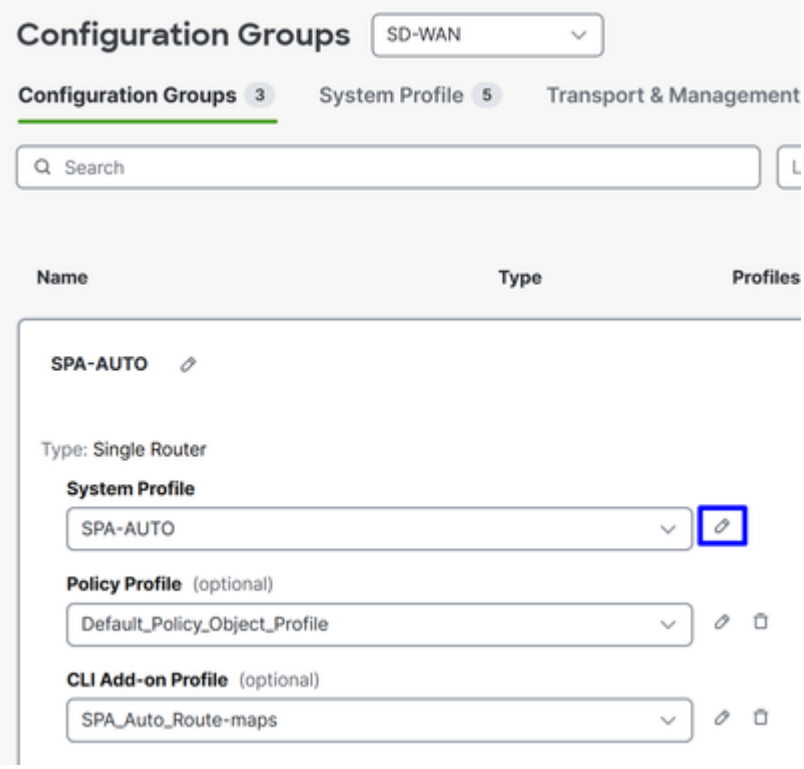
- **Organization ID**: È possibile ottenere questo dall'URL del dashboard SSE https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Copiarlo dalla fase Configurazione accesso sicuro
- Secret: copiarlo dalla fase Configurazione accesso sicuro

Quindi clicca sul Save pulsante.

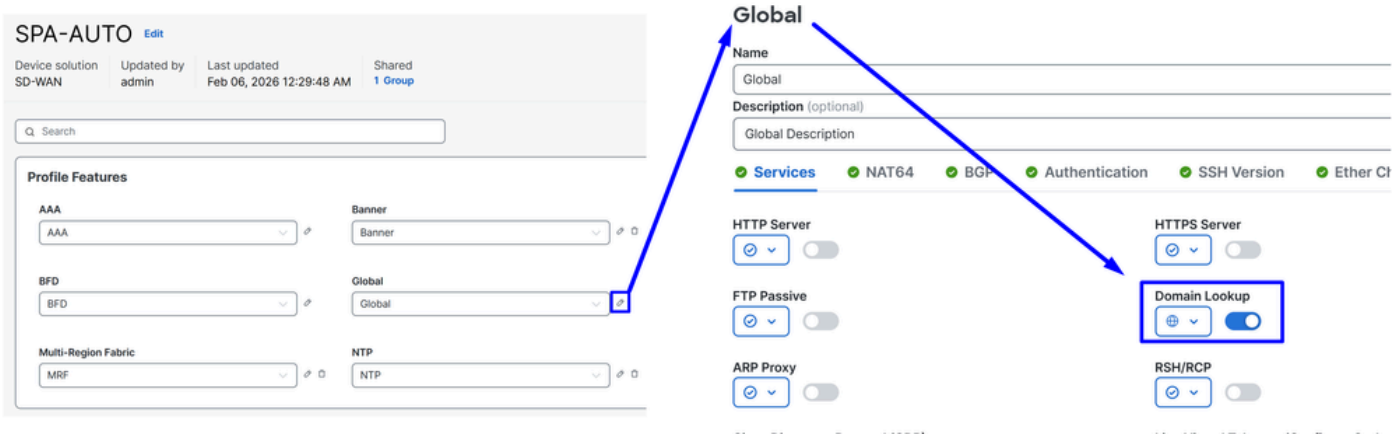
Nota: Prima di procedere con i passaggi successivi, è necessario verificare che SD-WAN Manager e Catalyst SD-WAN Edge dispongano della risoluzione DNS e dell'accesso a Internet.

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



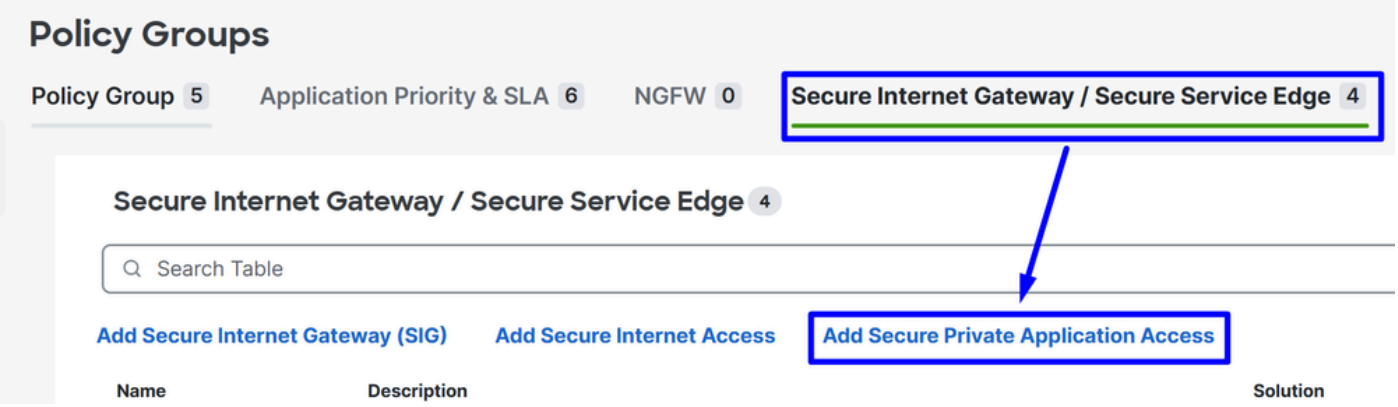
- Modificare quindi l'opzione Global e assicurarsi che l'opzione Domain Resolution sia abilitata



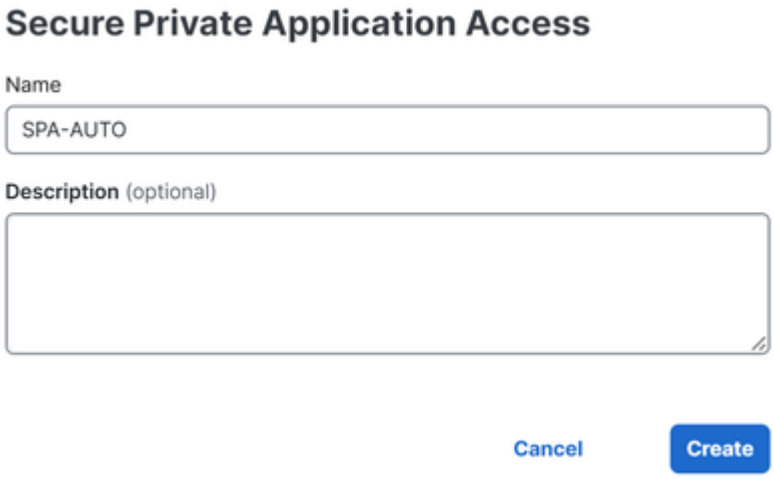
Configura gruppo di criteri

Passare a Configurazione > Gruppi di criteri:

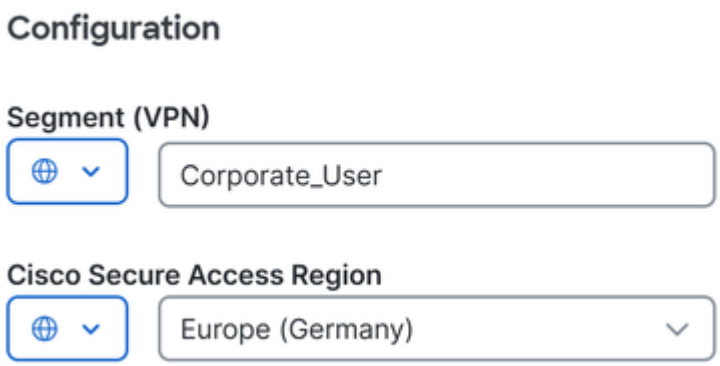
- Fai clic su Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- Configurare un nome e fare clic su Create



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

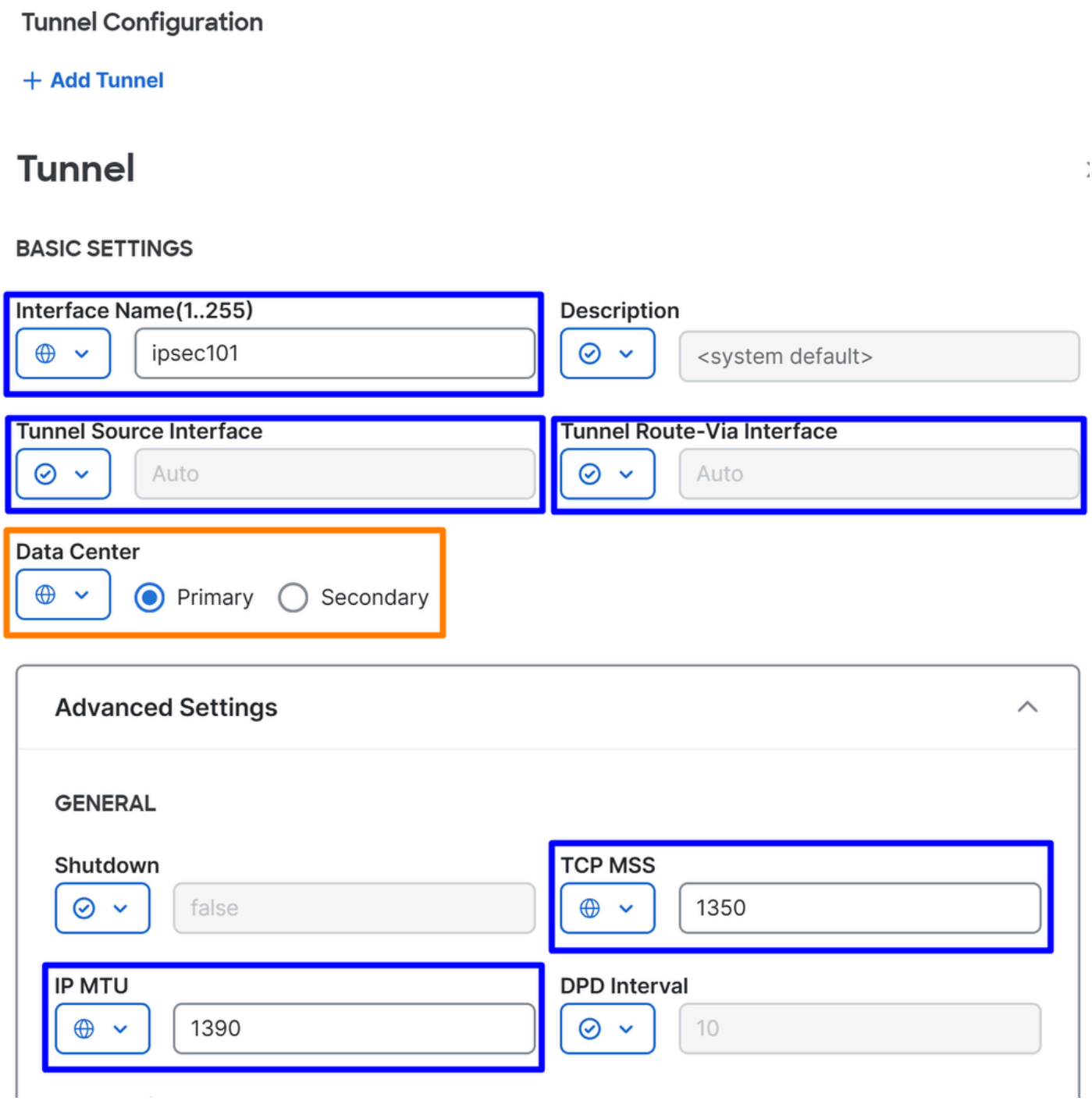


- Configuration
  - Segment (VPN): Scegliere il VRF che ospita l'applicazione o le applicazioni a cui accedere tramite Secure Access
  - Cisco Secure Access Region: Scegliere l'area più vicina all'hub o alla filiale SD-WAN in cui sono ospitate le applicazioni

Quindi, definire la configurazione del tunnel. I tunnel creati nel centro dati primario ad accesso sicuro sono attivi, mentre i tunnel creati nel centro dati secondario ad accesso sicuro funzionano

come backup.

In fare Tunnel Configuration clic su + Add Tunnel:



- Tunnel
  - Interface Name: specificare il nome del tunnel. Il nome verrà aggiornato automaticamente a ogni aggiunta di un nuovo tunnel.
  - Tunnel Source Interface: Non è necessario modificare questa impostazione. Se lasciato come Auto, il sistema crea automaticamente un'interfaccia di loopback con una maschera /31.
  - Tunnel Route-Via Interface: non è necessario modificare questa impostazione. Per impostazione predefinita, usa la prima interfaccia WAN fisica NAT sul router perimetrale, ma può essere modificata se è richiesta un'interfaccia WAN specifica
  - Data Center: selezionare Primario o Secondario. Se il tunnel primario è già configurato,

selezionare Secondario. In scenari normali, un tunnel può essere configurato come primario e un altro come secondario

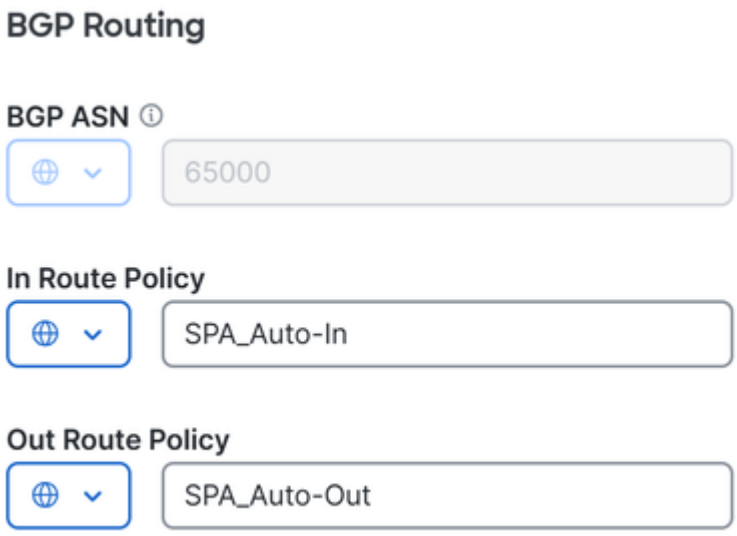
- Advanced Settings
  - IP MTU: Usa 1390
  - TCP MSS: Usa 1350

Nota: Se si desidera creare più tunnel per abilitare l'ECMP e aumentare la capacità del tunnel, è possibile configurare fino a 10 tunnel attivi/10 tunnel di backup per router. Ciò fornisce fino a 10 × 4 Gbps per NTG.

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action	
ipsec101		Auto	Auto	Primary		
ipsec102		Auto	Auto	Secondary		
ipsec103		Auto	Auto	Primary		
ipsec104		Auto	Auto	Secondary		
ipsec105		Auto	Auto	Primary		
ipsec106		Auto	Auto	Secondary		
ipsec107		Auto	Auto	Primary		
ipsec108		Auto	Auto	Secondary		
ipsec109		Auto	Auto	Primary		MAXIMUM OF 10 TUNNELS PER HUB
ipsec110		Auto	Auto	Secondary		10 x 1 Primary
ipsec111		Auto	Auto	Primary		10 x 1 Secondary
ipsec112		Auto	Auto	Secondary		
ipsec113		Auto	Auto	Primary		
ipsec114		Auto	Auto	Secondary		
ipsec115		Auto	Auto	Primary		
ipsec116		Auto	Auto	Secondary		
ipsec117		Auto	Auto	Primary		
ipsec118		Auto	Auto	Secondary		
ipsec119		Auto	Auto	Primary		
ipsec120		Auto	Auto	Secondary		

Nota:se si distribuiscono più tunnel per router, verificare che l'interfaccia di trasporto possa sostenere la larghezza di banda aggregata di tutti i tunnel attivi messi insieme. Ad esempio, se si prevede che due tunnel trasportino fino a 1 Gb/s ciascuno, il collegamento di trasporto deve supportare almeno 2 Gb/s di velocità effettiva.

Una volta configurati i tunnel, procedere con la configurazione BGP.



- **BGP Routing**
  - BGP ASN: specificare il numero AS per l'hub SD-WAN. AS 64512 è riservato per l'accesso sicuro e non può essere utilizzato. Per ulteriori informazioni su BGP, vedere
  - In Route Policy: Il sistema crea automaticamente questo criterio di instradamento in entrata con un deny all'istruzione per evitare problemi di instradamento. Deve essere modificato manualmente tramite un CLI Add-On Template per consentire/negare i percorsi appropriati.
  - Out Route Policy: Il sistema crea questo criterio di route in uscita con un' deny all istruzione per evitare problemi di routing. È necessario modificarlo manualmente tramite un'istruzione per consentire o negare le route appropriate. CLI Add-On Template

---

Avviso: A partire da novembre 2025, tutte le nuove organizzazioni Secure Access utilizzano la rete pubblica ASN 32644 per impostazione predefinita per il peering BGP nei gruppi di tunnel di rete. Le organizzazioni esistenti create prima di novembre 2025 continuano a utilizzare la licenza privata ASN 64512 che era precedentemente riservata ai peer BGP Secure Access. Se il numero AS privato 64512 è assegnato a un dispositivo della rete, non sarà possibile eseguire il peer con un gruppo di tunnel di rete configurato per il protocollo BGP AS 64512 peer (accesso protetto).

La configurazione successiva BGP e route-map viene creata automaticamente per ogni BGP adiacente dopo aver Deploy definito il nuovo criterio nel Policy Groupserver.

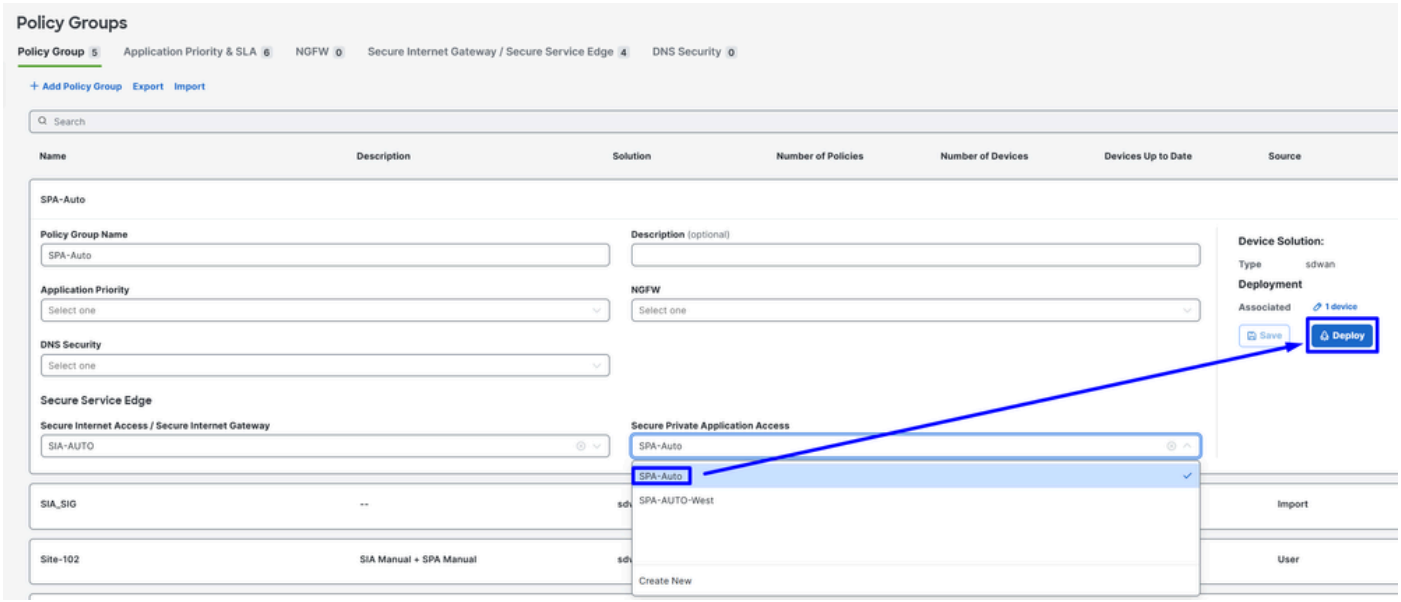
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

R104#sh run | s r b
router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
```

```
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
 ...
 maximum-paths 32
exit-address-family
```

Quindi, fare clic Save su e procedere con la distribuzione dei criteri per attivare i tunnel.

- Fare clic su Configuration > Policy Groups
- Scegliere sotto Policy > Secure Service Edge > Secure Private Application Access e fare clic sul profilo recente creato per SPA.
- Fare clicDeployper finalizzare



Per eseguire la verifica inSecure Access, effettuare le seguenti operazioni:

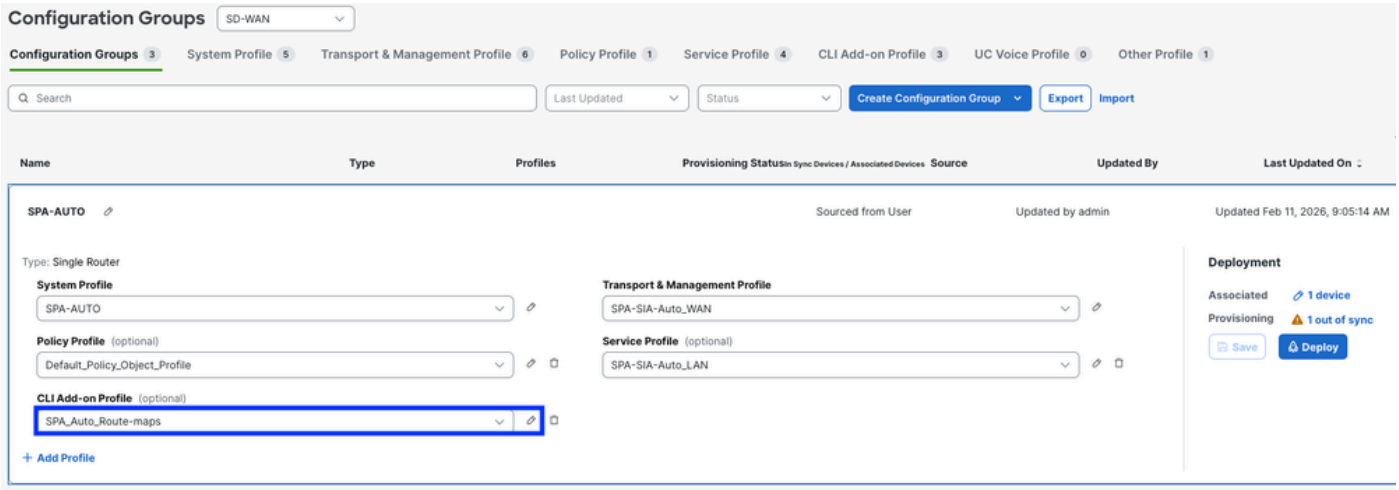
- Fai clic su Connect> Network Connections

INSTALLAZIONE TUNNEL

Configura routing

Passare a Configure > Configuration Groups

- Fate clic sul vostro Configuration Group pulsante e create/Edit your CLI Add-on Profile



Per consentire lo scambio di route BGP, utilizzare i protocolli In Route Policy e **Out Route Policy**BGP configurati in precedenza. È possibile trovare un esempio di base per la configurazione del CLI Add-On ciclo di lavorazione. Questo modello costituisce un punto di partenza e deve essere personalizzato in base alle esigenze:

```
ip bgp-community new-format
ip prefix-list ALL-ROUTES seq 5 permit 0.0.0.0/0 le 32

route-map SPA_Auto-In permit 10
match ip address prefix-list ALL-ROUTES
route-map SPA_Auto-In deny 65534
description Default Deny Configured from Secure Private Application Access feature

route-map SPA_Auto-Out permit 10
match ip address prefix-list ALL-ROUTES
description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
description Default Deny Configured from Secure Private Application Access feature

router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
network 172.16.104.0 mask 255.255.255.0
```

Avviso: Un'attenta pianificazione è richiesta quando si definiscono le reti consentite in entrata e in uscita tramite le route map BGP. L'autorizzazione di tutte le route, come mostrato nell'esempio precedente, può introdurre un comportamento di routing non desiderato. Per una distribuzione ottimale, specificare in modo esplicito solo le reti

---

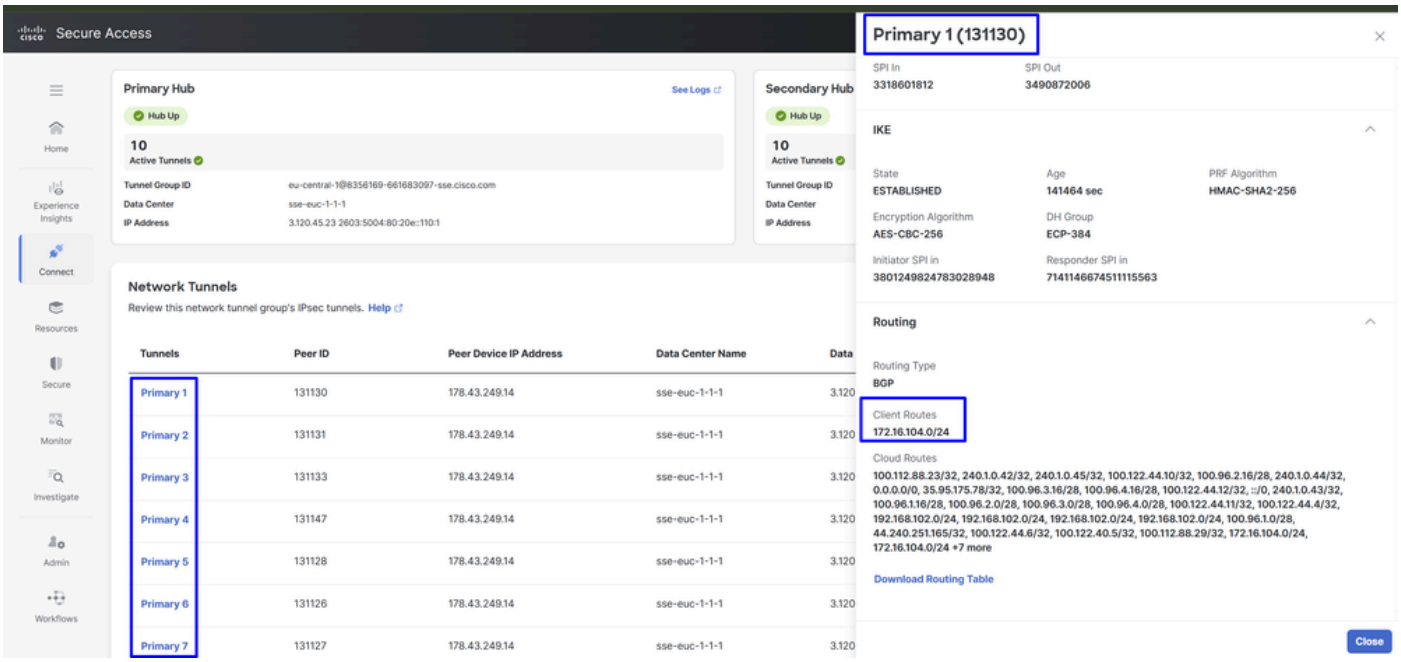
necessarie nelle route map per garantire risultati di routing controllati e prevedibili

Ora è possibile passare a Deploy the changes

Per verificare se le route BGP sono state ricevute inSecure Access, controllare la procedura seguente:

- Fare clic su Connect> Network Connections > Network Tunnel Groups e select il nome NTG

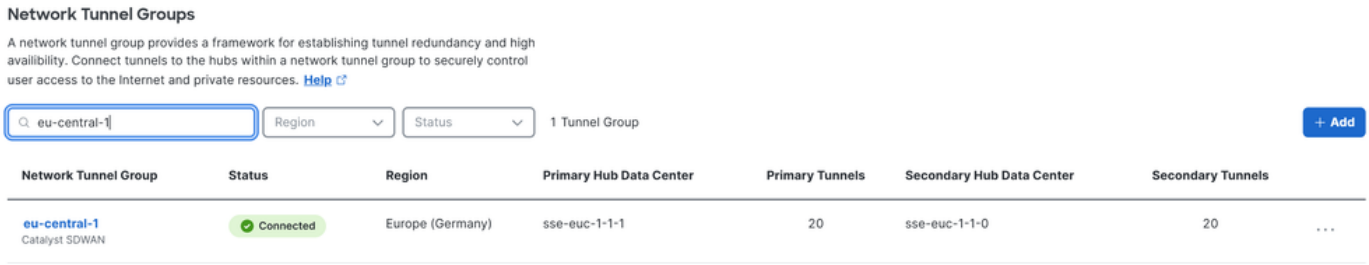
STESURA



Nota: Nell'esempio, la subnet 172.16.104.0/24 dell'utente aziendale viene pubblicizzata per l'accesso protetto tramite BGP. Ciò consente il corretto routing tra Catalyst SD-WAN e l'ambiente SSE.

La stessa policy può essere applicata a entrambi i bordi della WAN negli hub Catalyst SD-WAN, dando luogo a 20 tunnel attivi e 20 tunnel in standby. Il numero totale di tunnel dipende dal numero di tunnel configurati su ciascun edge. I router connessi agli hub di accesso sicuro (hub 1 e hub 2) formano una coppia ECMP su tutti i tunnel stabiliti.

Ad esempio, se Catalyst SD-WAN Edge 1 ha 10 tunnel e Catalyst SD-WAN Edge 2 ha 10 tunnel, Secure Access crea un protocollo ECMP sui 20 tunnel attivi. Lo stesso comportamento si applica all'hub SSE secondario.

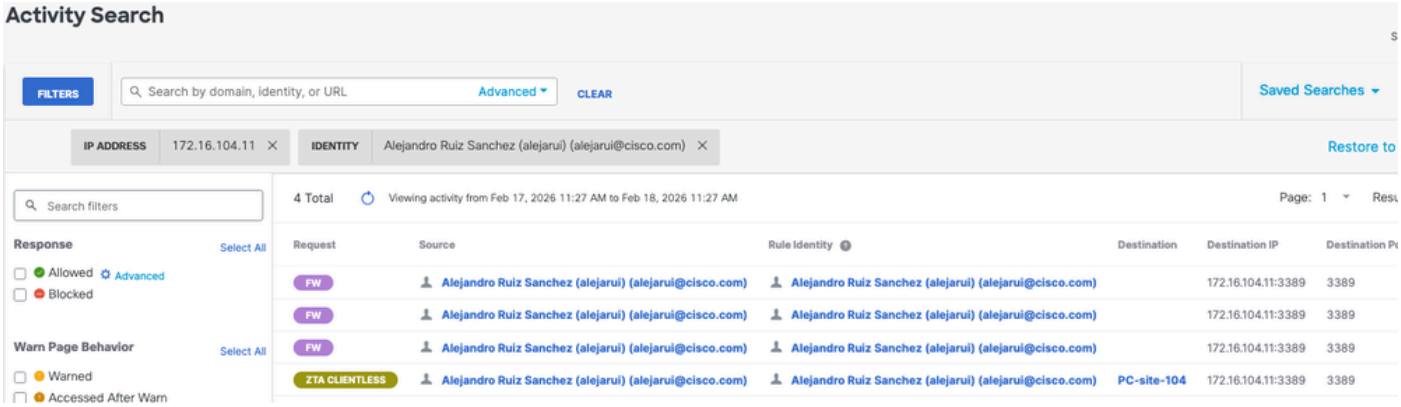


Verifica

per verificare se il traffico sta attraversando Cisco Secure Access, passare a Eventsor Activity Search o Network-Wide Path Insightse filtrare in base all'identità del tunnel:

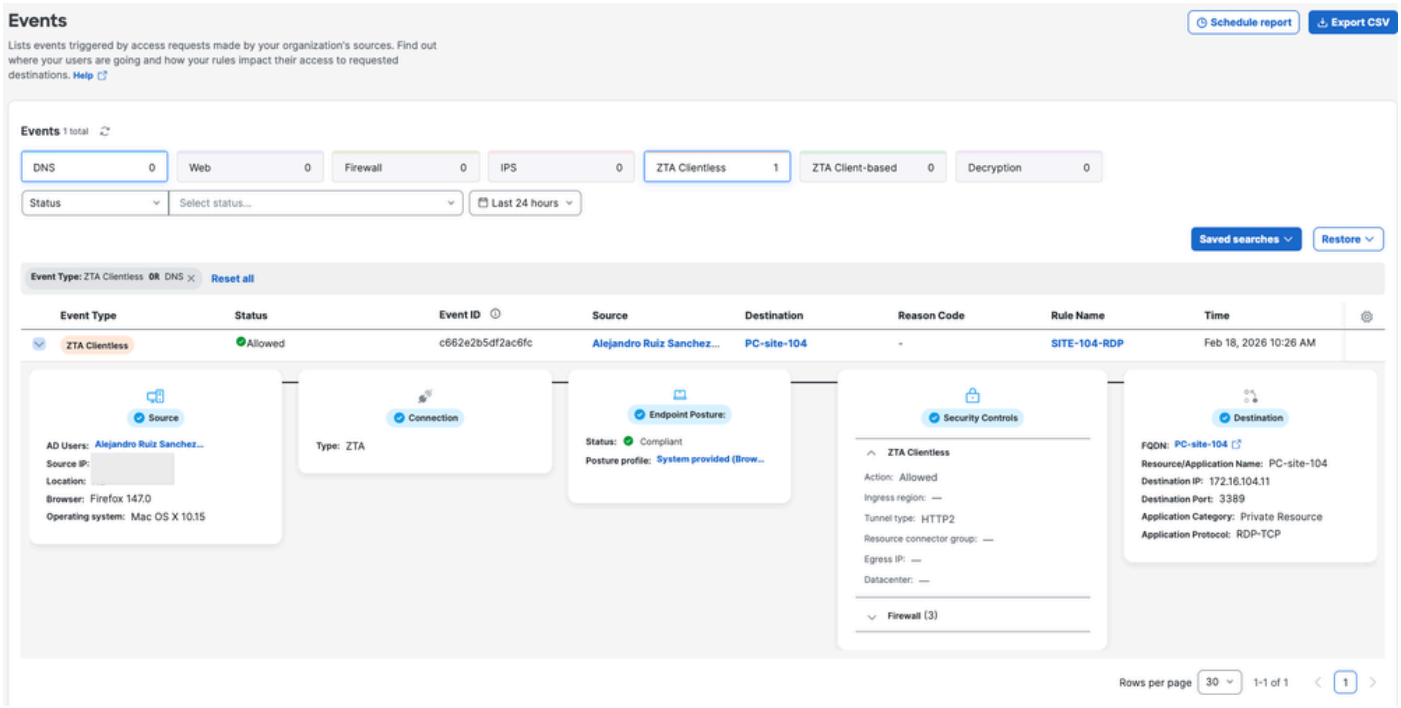
Accesso sicuro - Ricerca attività

Passa a Monitor>Activity Search :



Accesso sicuro - Eventi

Passare a Monitor>Events:

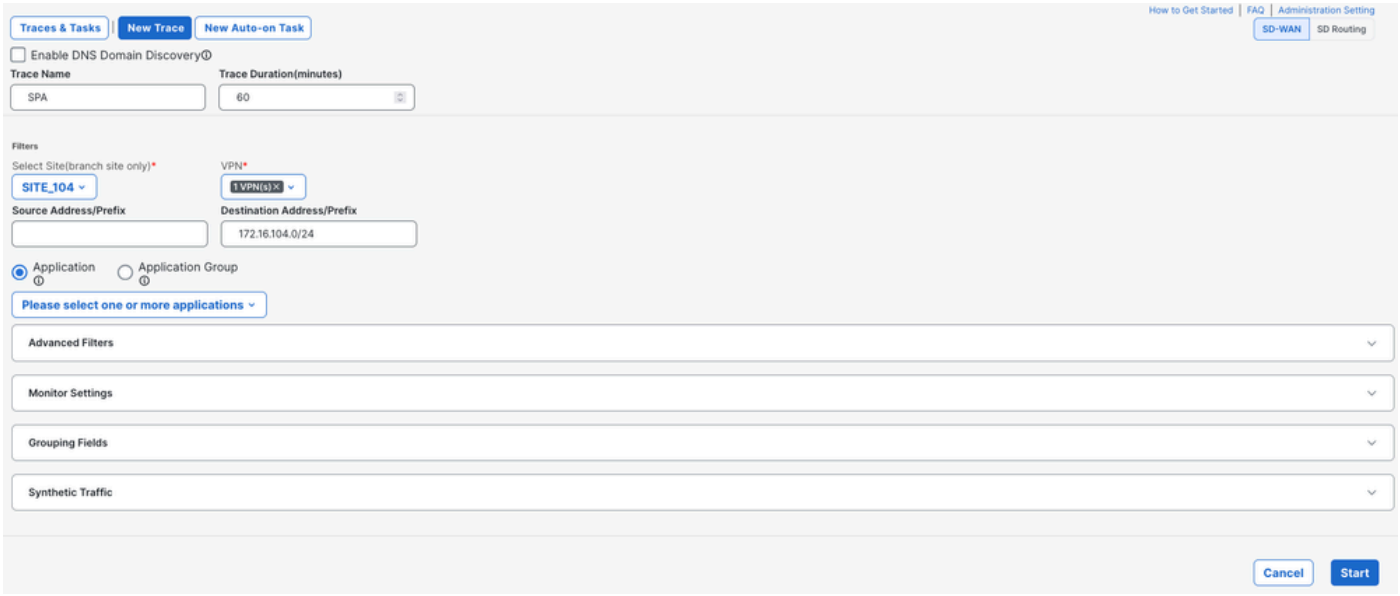


Nota: Accertarsi di disporre del criterio predefinito con la registrazione attivata. Per impostazione predefinita, questa opzione è disattivata.

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

Passare a Catalyst SD-WAN Manager:

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

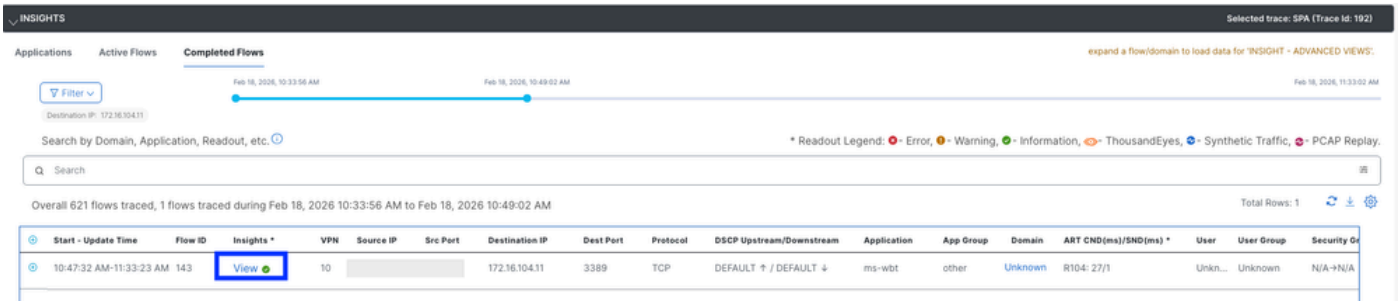


- Trace Name: (Facoltativo) Specificare il nome della traccia

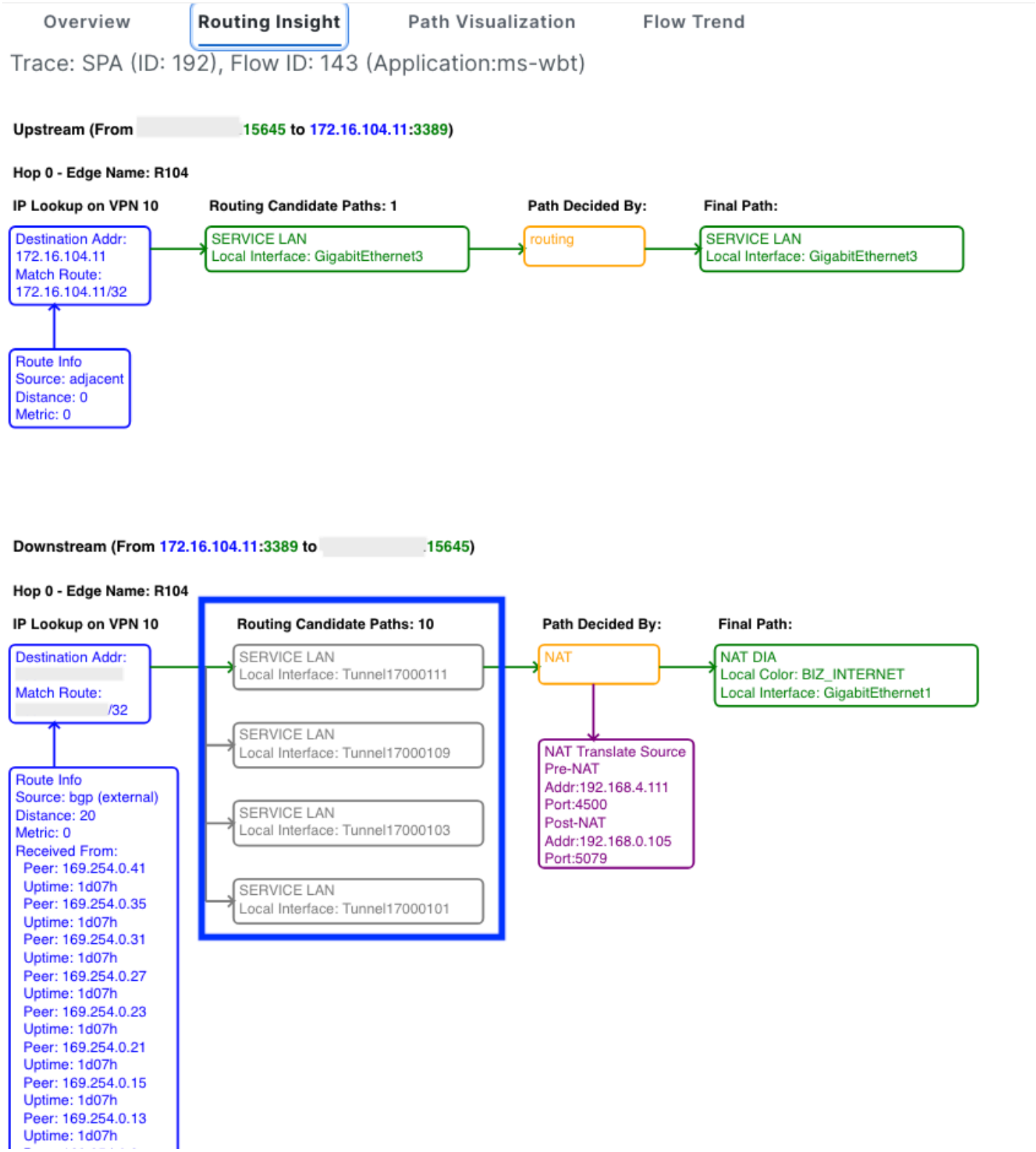
- Site: Scegliere il sito in cui si trova la risorsa privata
- VPN: Scegliere l'ID VPN in cui si trova la risorsa privata
- Source/Destination Address: (Facoltativo) Immettere l'indirizzo IP o lasciarlo in bianco per acquisire tutto il traffico filtrato in base a **Site**e VPNscegliere

Avvia la traccia

Individuare il flusso del traffico e fare clic su Visualizza nella colonna Informazioni dettagliate



Nella colonna Routing Insights vengono visualizzati i percorsi candidati e i tunnel IPSec per l'accesso protetto



Informazioni correlate

- [Supporto tecnico Cisco e download]
- [Cisco Secure Access Help Center]
- [Guida alla progettazione di Cisco BASE]
- [Configurazione dell'accesso sicuro con i tunnel automatizzati SD-WAN per l'accesso sicuro a Internet]

- 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).