

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

Sommario

[Introduzione](#)

[Premesse](#)

[Esempio di rete](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione accesso sicuro](#)

[Creazione API](#)

[Configurazione SD-WAN](#)

[Integrazione API](#)

[Configura gruppo di criteri](#)

[Configura routing](#)

[Verifica](#)

[Accesso sicuro - Ricerca attività](#)

[Accesso sicuro - Eventi](#)

[Catalyst SD-WAN Manager - Informazioni dettagliate sul percorso di rete](#)

[Informazioni correlate](#)

Introduzione

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



Secure Access and Catalyst SDWAN for Secure Private Access — with Automated Tunnels —

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. Aniché 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.

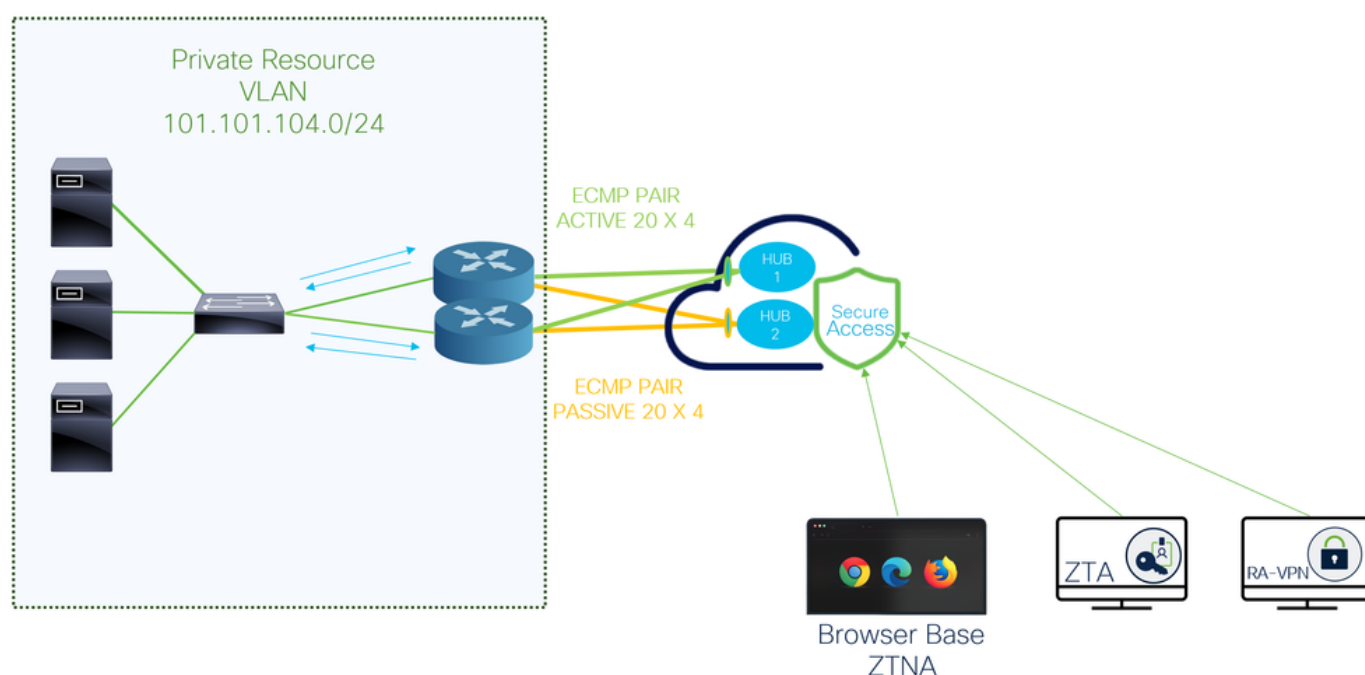
Ad esempio, un'organizzazione può stabilire tunnel da sito a sito dal proprio ambiente SD-WAN

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**

Key Scope

Select the appropriate access scopes to define what this API key can do.

☐ Admin	17 >
☒ Deployments	23 >
☐ Investigate	2 >
☐ Policies	25 >
☐ Reports	17 >

4 selected

[Remove All](#)

Scope		
Deployments / Identities	Read / Write	×
Deployments / Network Tunnel Group	Read / Write	×
Deployments / Tunnels	Read / Write	×
Deployments / Regions	Read-Only	×

Network Restrictions *(Optional)*

Optionally, add up to 10 networks from which this key can perform authentications. Add networks using a comma separated list of public IP addresses or CIDRs.

IP Addresses

For example: 100.10.10.0/24, 1.1.1.1

ADD

CANCEL

CREATE KEY



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**.

API Key

397766cdb29f43b08ddee3b1d8c04e45 

Key Secret

bfce729cd3e243e281df7271acb12208 



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 SSE** e compilare **API** e **Impostazioni di organizzazione**

Settings

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

Explore

Search

Cisco Account

Cisco services registration

License Reporting

PnP Connect Sync

Data Collection & Statistics

Cloud Services

Data Stream

Network Statistics Configuration & Collection

Statistics Database Configuration

External Services

Alarm Notifications

Threat Grid API

UTD Snort Subscriber Signature

Cisco DNA Portal

Managed Cellular Activation - eSIM

Identity Provider Settings

Cloud Credentials

Settings / External Services

Cloud Credentials

Cloud Provider Credentials Umbrella DNS Certificate

Configure Cisco Umbrella, Zscaler, and Cisco Secure Access credentials to enable Cisco Catalyst SD-WAN Manager to create automatic SIG tunnels to Cisco Umbrella or Zscaler endpoints.

☐ Umbrella

☐ Zscaler

☒ Cisco SSE

Organization Id

Field is required

Api Key

Secret

☒ Context Sharing

Save Cancel

- **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

Configuration Groups SD-WAN

Configuration Groups 3 **System Profile** 5 **Transport & Management**

Q Search

Name	Type	Profiles
SPA-AUTO		

Type: Single Router

System Profile

SPA-AUTO

Policy Profile (optional)

Default_Policy_Object_Profile

CLI Add-on Profile (optional)

SPA_Auto_Route-maps

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

SPA-AUTO [Edit](#)

Device solution: SD-WAN | Updated by: admin | Last updated: Feb 06, 2026 12:29:48 AM | Shared: 1 Group

Q Search

Profile Features

AAA	Banner
BFD	Global
Multi-Region Fabric	NTP

Global

Name: Global

Description (optional): Global Description

Services NAT64 BGP Authentication SSH Version Ether CF

HTTP Server

FTP Passive

ARP Proxy

HTTPS Server

Domain Lookup

RSH/RCP

Configura gruppo di criteri

Passare a Configurazione > Gruppi di criteri:

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

Policy Groups

Policy Group 5 Application Priority & SLA 6 NGFW 0 **Secure Internet Gateway / Secure Service Edge 4**

Secure Internet Gateway / Secure Service Edge 4

Q Search Table

[Add Secure Internet Gateway \(SIG\)](#) [Add Secure Internet Access](#) **[Add Secure Private Application Access](#)**

Name	Description	Solution
------	-------------	----------

- Configurare un nome e fare clic su **Create**

Secure Private Application Access

Name

SPA-AUTO

Description (optional)

[Cancel](#) [Create](#)

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

Configuration

Segment (VPN)

  Corporate_User

Cisco Secure Access Region

  Europe (Germany) 

- 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 Configuration

+ Add Tunnel

Tunnel

BASIC SETTINGS

Interface Name(1..255) ipsec101	Description <system default>
Tunnel Source Interface Auto	Tunnel Route-Via Interface Auto
Data Center ☐ Primary ☐ Secondary	

Advanced Settings

GENERAL

Shutdown false	TCP MSS 1350
IP MTU 1390	DPD Interval 10

- 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	✎ 🗑	
ipsec111	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑	10 x 1 Primary
ipsec112	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑	10 x 1 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 ⓘ

 ▼

65000

In Route Policy

 ▼

SPA_Auto-In

Out Route Policy

 ▼

SPA_Auto-Out

- **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 Group server.

```
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 clic **Deploy** per finalizzare

Per eseguire la verifica in **Secure 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

The screenshot shows the 'Configuration Groups' page. At the top, there's a search bar and filters for 'Last Updated' and 'Status'. Below this is a table of configuration groups. The 'SPA-AUTO' group is highlighted. To the right of the table, the details for the 'SPA-AUTO' group are shown. It includes a 'Type' of 'Single Router' and several profile dropdowns: 'System Profile' (SPA-AUTO), 'Policy Profile' (optional, Default_Policy_Object_Profile), 'CLI Add-on Profile' (optional, SPA_Auto_Route-maps), 'Transport & Management Profile' (SPA-SIA-Auto_WAN), and 'Service Profile' (optional, SPA-SIA-Auto_LAN). On the far right, there's a 'Deployment' section with 'Associated' (1 device) and 'Provisioning' (1 out of sync) status, along with 'Save' and 'Deploy' buttons.

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

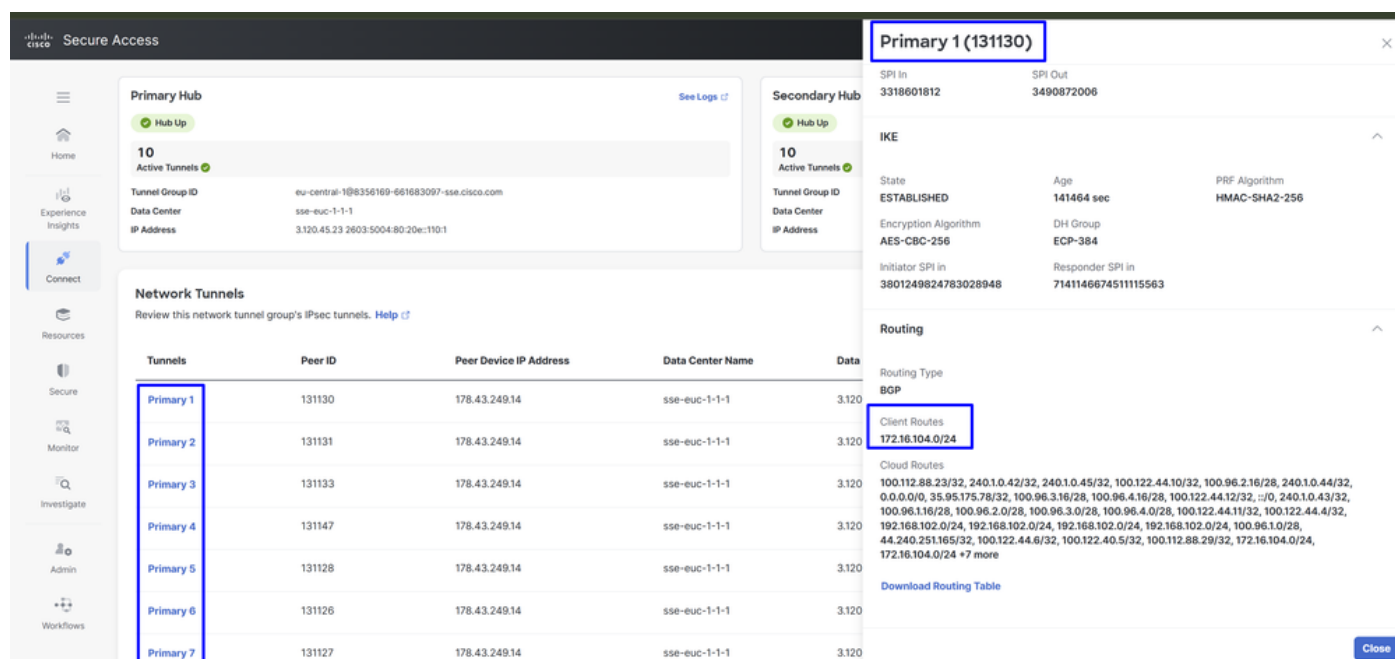
necessarie nelle route map per garantire risultati di routing controllati e prevedibili

Ora è possibile passare a Deploy the changes

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

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

STESURA



The screenshot displays the Cisco Secure Access management console. On the left, a sidebar contains navigation options: Home, Experience Insights, Connect (highlighted), Resources, Secure, Monitor, Investigate, Admin, and Workflows. The main content area is divided into two sections. The top section, 'Primary Hub', shows '10 Active Tunnels' and details for the 'eu-central-1@8356169-661683097-ssc.cisco.com' tunnel group, including Data Center 'sse-euc-1-1-1' and IP Address '3.120.45.23 2603:5004:80:20::110:1'. The bottom section, 'Network Tunnels', provides a table of tunnels. A modal window on the right, titled 'Primary 1 (131130)', provides detailed information for the selected tunnel. It includes SPI In (3318601812) and SPI Out (3490872006), IKE status (ESTABLISHED), Age (141464 sec), PRF Algorithm (HMAC-SHA2-256), Encryption Algorithm (AES-CBC-256), DH Group (ECP-384), Initiator SPI In (3801249824783028948), and Responder SPI In (7141146674511115563). The 'Routing' section shows 'Routing Type BGP' and 'Client Routes' including '172.16.104.0/24'. A 'Download Routing Table' link is also present.

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data
Primary 1	131130	178.43.249.14	sse-euc-1-1-1	3.120
Primary 2	131131	178.43.249.14	sse-euc-1-1-1	3.120
Primary 3	131133	178.43.249.14	sse-euc-1-1-1	3.120
Primary 4	131147	178.43.249.14	sse-euc-1-1-1	3.120
Primary 5	131128	178.43.249.14	sse-euc-1-1-1	3.120
Primary 6	131126	178.43.249.14	sse-euc-1-1-1	3.120
Primary 7	131127	178.43.249.14	sse-euc-1-1-1	3.120



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.

Network Tunnel Groups

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

eu-central-1

Region

Status

1 Tunnel Group

+ Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
eu-central-1 Catalyst SDWAN	Connected	Europe (Germany)	sse-euc-1-1-1	20	sse-euc-1-1-0	20

Verifica

per verificare se il traffico sta attraversando Cisco Secure Access, passare a [Events](#) o [Activity Search](#) o [Network-Wide Path Insights](#) e filtrare in base all'identità del tunnel:

Accesso sicuro - Ricerca attività

Passa a [Monitor](#) > [Activity Search](#) :

Activity Search

FILTERS

Q Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

IP ADDRESS172.16.104.11

IDENTITYAlejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)

Restore to

Search filters

Response

Allowed

Blocked

Warn Page Behavior

Warned

Accessed After Warn

4 Total

Viewing activity from Feb 17, 2026 11:27 AM to Feb 18, 2026 11:27 AM

Page: 1

Results

Request	Source	Rule Identity	Destination	Destination IP	Destination Port
FW	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)		172.16.104.11:3389	3389
FW	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)		172.16.104.11:3389	3389
FW	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)		172.16.104.11:3389	3389
ZTA CLIENTLESS	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	PC-site-104	172.16.104.11:3389	3389

Accesso sicuro - Eventi

Passare a [Monitor](#) > [Events](#):

Events

Schedule report

Export CSV

Lists events triggered by access requests made by your organization's sources. Find out where your users are going and how your rules impact their access to requested destinations. [Help](#)

Events 1 total

DNS 0

Web 0

Firewall 0

IPS 0

ZTA Clientless 1

ZTA Client-based 0

Decryption 0

Status

Select status...

Last 24 hours

Saved searches

Restore

Event Type: ZTA Clientless OR DNS

Reset all

Event Type	Status	Event ID	Source	Destination	Reason Code	Rule Name	Time
ZTA Clientless	Allowed	c662e2b5df2ac6fc	Alejandro Ruiz Sanchez...	PC-site-104	-	SITE-104-RDP	Feb 18, 2026 10:26 AM

Source

AD Users: Alejandro Ruiz Sanchez...

Source IP:

Location:

Browser: Firefox 147.0

Operating system: Mac OS X 10.15

Connection

Type: ZTA

Endpoint Posture:

Status: Compliant

Posture profile: System provided (Browse...)

Security Controls

ZTA Clientless

Action: Allowed

Ingress region:

Tunnel type: HTTP2

Resource connector group:

Egress IP:

Datacenter:

Firewall (3)

Destination

FQDN: PC-site-104

Resource/Application Name: PC-site-104

Destination IP: 172.16.104.11

Destination Port: 3389

Application Category: Private Resource

Application Protocol: RDP-TCP

Rows per page 30

1-1 of 1

1



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

Traces & Tasks

New Trace

New Auto-on Task

How to Get Started

FAQ

Administration Setting

SD-WAN

SD Routing

Enable DNS Domain Discovery

Trace Name

SPA

Trace Duration(minutes)

60

Filters

Select Site(branch site only)*

SITE_104

VPN*

1 VPN(s)

Source Address/Prefix

Destination Address/Prefix

172.16.104.0/24

Application

Application Group

Please select one or more applications

Advanced Filters

Monitor Settings

Grouping Fields

Synthetic Traffic

Cancel

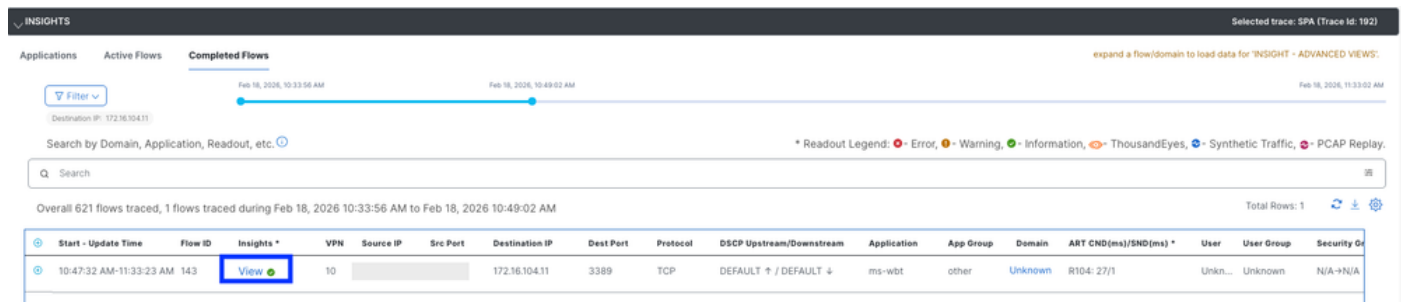
Start

- 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 VPN scegliere

Avvia la traccia

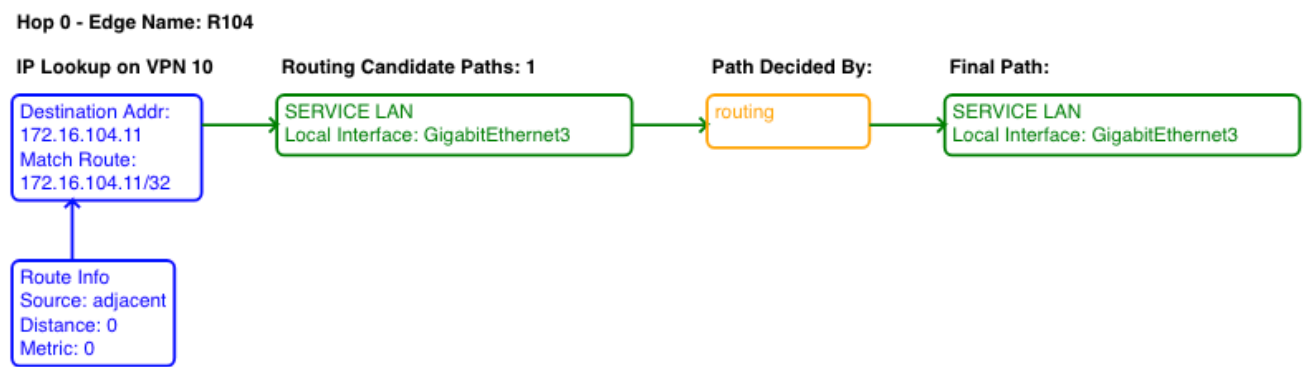
Individuare il flusso del traffico e fare clic su Visualizza nella colonna Informazioni dettagliate



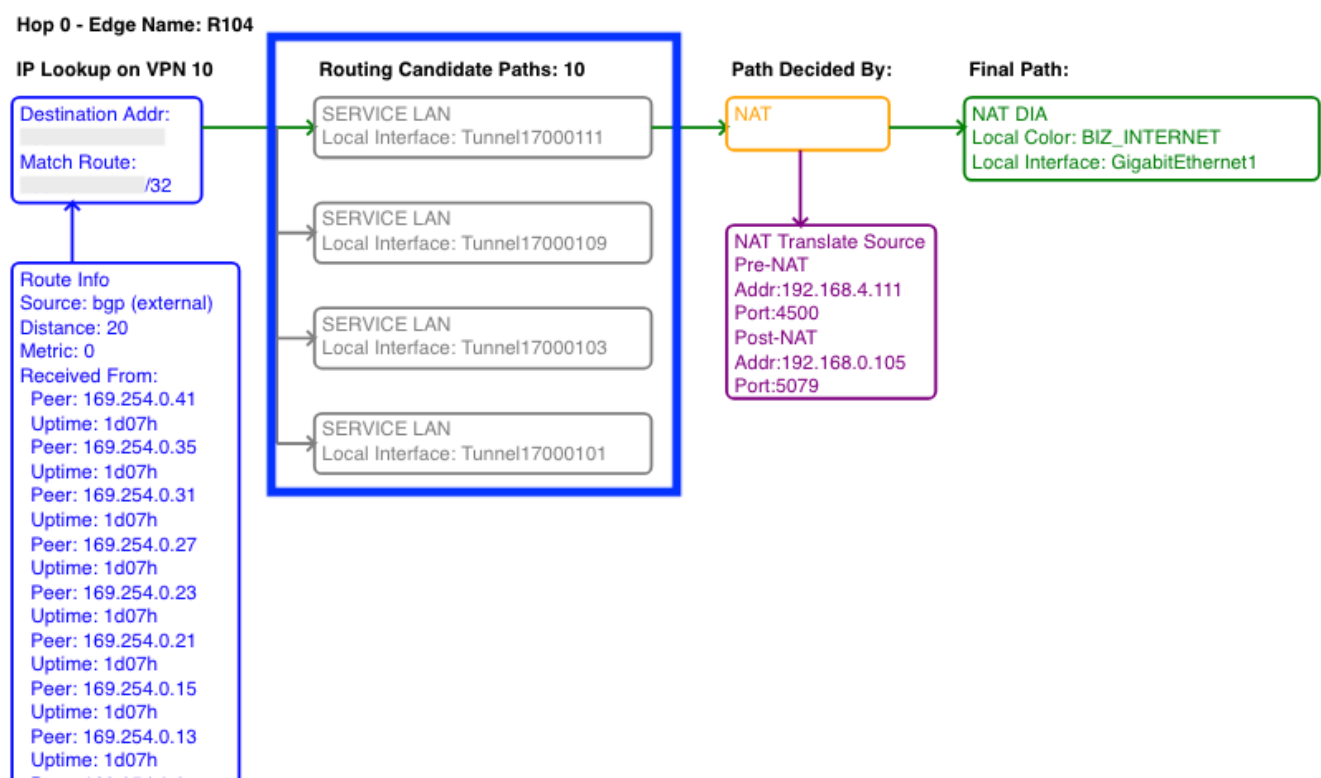
Nella colonna Routing Insights vengono visualizzati i percorsi candidati e i tunnel IPsec per l'accesso protetto

Trace: SPA (ID: 192), Flow ID: 143 (Application:ms-wbt)

Upstream (From 15645 to 172.16.104.11:3389)



Downstream (From 172.16.104.11:3389 to 15645)



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).