

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

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](#)

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

[Instradamento del traffico](#)

[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 SD-WAN Automated Tunnels per Secure Internet Access.



Secure Access and SDWAN for Secure Internet Access — with Automated Tunnels —

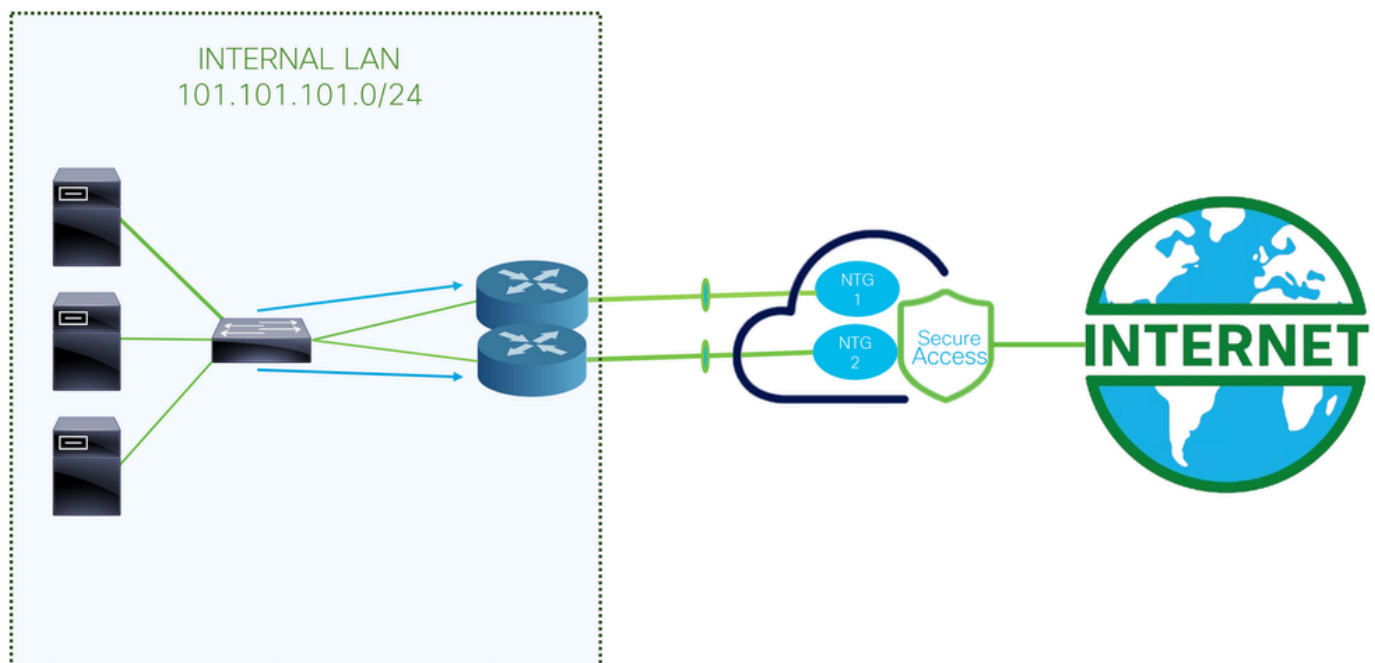
Premesse

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**

Key Scope

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

<input type="checkbox"/>	Admin	17 >
<input checked="" type="checkbox"/>	Deployments	23 >
<input type="checkbox"/>	Investigate	2 >
<input type="checkbox"/>	Policies	25 >
<input type="checkbox"/>	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 4

Transport

Q Search

Las

Name

Type

Profiles

SIA Secure Internet Access R1 + R2



Type: Single Router

System Profile

SIA_Basic



Service Profile (optional)

SIA_LAN



[+ Add Profile](#)

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

SIA_Basic [Edit](#)

Description: SIA Basic Profile

Device solution: SD-WAN Updated by: admin Last updated: Nov 05, 2025 03:37:09 PM Shared: 1 Group

Q Search

Profile Features

AAA: AAA Banner: Banner

BFD: BFD Global: Global

Multi-Region Fabric: MRF NTP: NTP

Global

Name: Global

Description (optional): Global Description

Services NAT64 BGP Authentication SSH Version

HTTP Server: ☐ HTTPS Server: ☐

FTP Passive: ☐ Domain Lookup: ☒

ARP Proxy: ☐ RSH/RCP: ☐

Cisco Discovery Protocol (CDP) Line Virtual Teletype (Configure O)

Configura gruppo di criteri

Passare a Configurazione > Gruppi di criteri:

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

Policy Group 4 Application Priority & SLA 3 NGFW 0 **Secure Internet Gateway / Secure Service Edge 3**

Secure Internet Gateway / Secure Service Edge 3

Q Search Table

Add Secure Internet Gateway (SIG) **Add Secure Internet Access** Add Secure Private Application 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

Secure Internet Access

Name

SIA

Solution

sdwan

Description (optional)

Cancel

Create

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

SSE Provider

☒ Cisco SSE ☐ Zscaler

Context Sharing

☒ VPN ☒ SGT

Tracker

Source IP address

{{ Monitoring }}

- 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:

Configuration

[+ Add Tunnel](#)

Single Hub HA Scenario

ECMP Scenario with HA

Max one tunnel per hub

Max 8 Tunnels per Hub 8GB X 1

Single Hub HA Scenario Configuration:

- Tunnel Type: IPsec
- Interface Name(1..255): ipsec1
- Tunnel Source Interface*: GigabitEthernet1
- Tunnel Route Via: <SYSTEM DEFAULT>
- Tracker: DefaultTracker
- Primary: ☒ Secondary: ☐

ECMP Scenario with HA Configuration:

- Tunnel Type: IPsec
- Interface Name(1..255): ipsec1
- Tunnel Source Interface*: Loopback1
- Tunnel Route Via: GigabitEthernet1
- Tracker: DefaultTracker
- Primary: ☒ Secondary: ☐

By default, for the tunnel route, the system will select the first NAT-enabled interface it finds. If there is more than one, you should select your desired WAN interface.

- **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 su Add Tunnel

Edit Tunnel

Tunnel Type	<input checked="" type="radio"/> IPsec
Interface Name(1..255)	Tunnel Source Interface*
<input type="text" value="ipsec1"/>	<input type="text" value="Loopback1"/>
Tunnel Route Via	Tracker ⓘ
<input type="text" value="GigabitEthernet1"/>	<input type="text" value="DefaultTracker"/>
Data Center	<input checked="" type="radio"/> Primary <input type="radio"/> Secondary

- 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.

Advanced Options

General

Shutdown

☒ ☐

Track this interface

☒ ☐

TCP MSS

IP MTU

DPD Interval

DPD Retries

IKE Diffie-Hellman Group

- 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

Configuration

+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		<input checked="" type="checkbox"/> false	1350	1390	
ipsec2		<input checked="" type="checkbox"/> false	1350	1390	

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

ECMP SCENARIO WITH HA

Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1		<input checked="" type="checkbox"/> false	1350	1390
ipsec2		<input checked="" type="checkbox"/> false	1350	1390
ipsec3	PRIMARY HUB	<input checked="" type="checkbox"/> false	1350	1390
ipsec4		<input checked="" type="checkbox"/> false	1350	1390
ipsec5		<input checked="" type="checkbox"/> false	1350	1390
ipsec11		<input checked="" type="checkbox"/> false	1350	1390
ipsec12		<input checked="" type="checkbox"/> false	1350	1390
ipsec13	SECONDARY HUB	<input checked="" type="checkbox"/> false	1350	1390
ipsec14		<input checked="" type="checkbox"/> false	1350	1390
ipsec15		<input checked="" type="checkbox"/> false	1350	1390

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

High Availability

+ Add Interface Pair

Fare clic su Add Interface Pair:

PRIMARY
SECONDARY

Edit Interface Pair



Active Interface <input type="text" value="ipsec1"/>		Active Interface Weight <input type="text" value="1"/>	
Backup Interface <input type="text" value="ipsec11"/>		Backup Interface Weight <input type="text" value="1"/>	

Tunnel Type <input type="text" value="ipsec1"/>	<input checked="" type="radio"/> IPsec Tunnel Source Interface* <input type="text" value="Loopback1"/>	Tunnel Type <input type="text" value="ipsec11"/>	<input checked="" type="radio"/> IPsec Tunnel Source Interface* <input type="text" value="Loopback11"/>
Tunnel Route Via <input type="text" value="GigabitEthernet1"/>	Tracker <input checked="" type="radio"/> DefaultTracker	Tunnel Route Via <input type="text" value="GigabitEthernet1"/>	Tracker <input checked="" type="radio"/> DefaultTracker
Data Center <input checked="" type="radio"/> Primary <input type="radio"/> Secondary		Data Center <input type="radio"/> Primary <input checked="" type="radio"/> Secondary	

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.

High Availability

+ Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	1	ipsec11	1	 
ipsec2	1	ipsec12	1	 
ipsec3	1	ipsec13	1	 
ipsec4	1	ipsec14	1	 
ipsec5	1	ipsec15	1	 

Cancel

Save



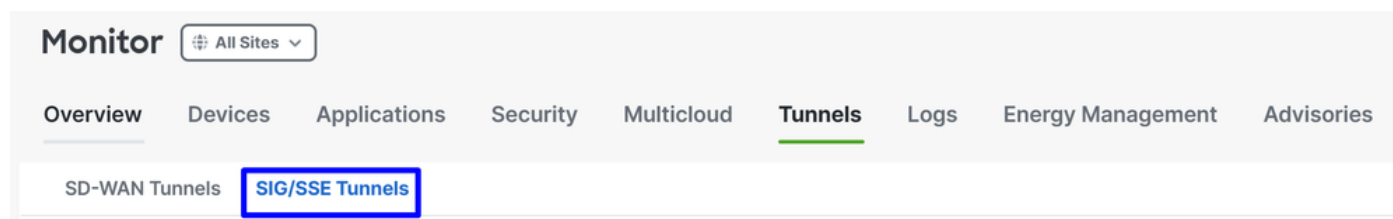
Nota: Un massimo di 8 coppie di tunnel (16 tunnel: 8 primario e 8 secondario) può essere configurato in SD-WAN Catalyst vManage. Cisco Secure Access supporta fino a 10 coppie di tunnel.

- 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 su **SIG/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_301								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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_301	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

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](#)

5b28-4db0-b62e-9b589b5c687d

Region

Status

1 Tunnel Group

+ Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels	
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d Catalyst SD-WAN	Connected	Europe (Germany)	SSE-euc-1-1-1	8	SSE-euc-1-1-0	8	...

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

PRIMARY

8 Active Tunnels

Tunnel Group ID: C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d

Data Center: SSE-euc-1-1-1

IP Address: 3.120.45.23

SECONDARY

8 Active Tunnels

Tunnel Group ID: C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d

Data Center: SSE-euc-1-1-0

IP Address: 18.156.145.74

Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#)

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	137085	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 2	137086	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 3	137096	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 4	137087	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 5	137095	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 6	137077	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 7	137084	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Primary 8	137078	178.43.250.2	SSE-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM
Secondary 1	65559	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 2	65560	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 3	65538	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 4	65548	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 5	65552	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 6	65554	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 7	65555	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Secondary 8	65558	178.43.250.2	SSE-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM

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

Application Catalog

SD-AVC Enabled

Configure Cloud Connection

Overview

Applications 1553

Application Source Settings

Cloud Sourced Applications

Discovered Application 0

Application Lists

Conflicts

Applications 1553

Select Application Attributes

Choose Filter

Custom Application

Export

Search Table

0 selected

Create Application List

Define Probe Endpoint

As of: Dec 23, 2025 05:00:05 PM

	Application Name	Application Family	Application Group	Application Source	SaaS probe endpoint type	SaaS probe endpoint value	Traffic Class	Business Relevance	Action
<input type="checkbox"/>	Zannet	file-server	other	inBuiltApps	-	-	bulk-data	Silver	...



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

Applications 1553

Select Application Attributes

Choose Filter

Custom Application

Export

Search Table

0 selected

Create Application List

Define Probe Endpoint

As of: Dec 23, 2025 05:00:05 PM

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

ProxySecureAccess

Custom Application ✕

Name of the Custom App → **Application Name** ⓘ

UmbrellaDNS
Application Name: UmbrellaDNS-Custom

Server Names ⓘ
Enter Server Names

Application Family
Select Application Family ▼

Application Group
Select Application Group ▼

Traffic Class
Select Traffic Class ▼

Business Relevance
Select Business Relevance ▼

+ L3/L4 Attributes

IPv4 Address ⓘ	Ports ⓘ	L4 Protocol ⓘ
208.67.220.220,208.67.222.222	Space separated ports or range or	Enter L4 Protocol ▼

Configure IP addresses to exclude

SaaS probe endpoint type
☐ IP Address ☐ FQDN ☐ URL

SaaS probe endpoint value

Cancel Save

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**

Policy Groups

Policy Group 4

Application Priority & SLA 4

NGFW 0

Secure Internet Gateway / Secure Service Edge 3

DNS Security 0

Application Priority & SLA Policy 4

Q Search Table

Application Priority & SLA Policy

Name

Description

References

Update

- Configurare il nome di un criterio e fare clic su [Create](#)

Application Priority & SLA Policy

Policy Name

SIA-ROUTE

Description (optional)

Cancel


Create

- Abilita [Advanced Layout](#)
- Fare clic su [+ Add Traffic Policy](#)

[Policies](#) > Application Priority & SLA

SIA-ROUTE [✎](#)

[Additional Settings](#) [Advanced Layout](#) [ⓘ](#)

 Change made in advanced view won't save to simple view.

[+ Add Traffic Policy](#)

[SLA Class](#) [QoS Queue](#)

No SLA Class added, add your first SLA Class in Traffic Policy

Add Traffic Policy List

Policy Name

VPN(s)

Direction

Default action

☒ Accept ☐ Drop

Cancel

Add

- 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:

In this way, you are bypassing the routing of specific traffic to Secure Access

VPN: Corporate_Users Direction: From Service Default Action: Accept

Search rule by name or order

	NAME	MATCH	ACTION	
1	LocalNetwork	Destination Ip · 172.16.200.0/24 Source Ip · 101.101.101.0/24	Base action · accept	⌵
2	BypassSSEP	App List · SecureAccessProxy	Base action · accept	⌵
3	UmbrellaDNS	App List · UmbrellaDNS	Base action · accept	⌵
4	SIA AUTO FULL TRAFFIC	Source Ip · 101.101.101.0/24	Base action · accept Sse Secure Service Edge · true Sse Secure Service Edge Instance · Cisco-Secure-Access	⌵

Traffic is matched in order, starting from the highest priority rule to the lowest.

In this way, you are sending specific traffic to Secure Access to be protected

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** **Activity Search** **Network-Wide Path Insights** e filtrare in base all'identità del tunnel:

Accesso sicuro - Ricerca attività

Passare a **Monitor** > **Activity Search**:

The screenshot displays the Cisco Secure Access Activity Search interface. At the top, there's a search bar with filters and a 'CLEAR' button. Below the search bar, a table lists activity results. The table has columns for Request, Source, Rule Identity, Destination, Destination IP, Destination Port, and Destination Country. The results show activity from Dec 27, 2025 6:14 AM to Dec 28, 2025 6:14 AM. The table is filtered by 'IDENTITY' with the value 'C8K-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6'. The table shows 1,617 total results. The results are grouped by 'Response' (Allowed, Blocked) and 'Warn Page Behavior' (Warned, Accessed After Warn). The 'Event Details' sidebar on the right shows details for the selected event, including the Action (Allowed), Time (Dec 28, 2025 6:14 AM), Rule Name (For all Internet access (2100958)), Source (VPN-10 (VPN-10)), Source IP (101.101.101.20), Destination (https://youtube.com), and Security Group Tag (SGT).

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)		142.250.186.174-443		United States
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://youtube.com	142.250.186.174-443		United States
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
WEB	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177		
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)		110.234.18.177-443		United States
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)		110.234.18.177-443		United States
FW	* VPN-10 (VPN-10)	* VPN-10 (VPN-10)	https://img3.joymax.com	110.234.18.177-443		United States

Accesso sicuro - Eventi

Passare a **Monitor** > **Events**:

>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	829e0bbdeaf6514e	C8K-PAYG-560-5b...	8.8.8.8:53	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Connect	Allowed	204e46d757b128d7	C8K-PAYG-560-5b...	8.8.8.8	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	829e0bbdeaf6514e	C8K-PAYG-560-5b...	8.8.8.8:53	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	eecb39315cdde282	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	eecb39315cdde282	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
✓	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-0f3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM

Source

Network Tunnels: C8K-PAYG-0f3-d4e...

Viptela VPN: VPN-10 (VPN-10)...

Source IP: 101.101.101.20

Source port: 55240

Connection

Type: Network Tunnel

Security Controls

Firewall

Allow: 9 [View all](#)

Action: Allow

Egress IP: -

Egress Type: -

Datacenter: Europe (Germany)

No file control event found.

Destination

FQDN: -

Resource/Application Name: -

Destination IP: 110.234.18.177

Destination Port: 443

Destination List: -

Protocol: TCP

Session Bytes Received: 180

Session Bytes Sent: 362

Application Category: -

Application Protocol: -

Content Category: -



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**

Traces & Tasks

New Trace

New Auto-on Task

☐ Enable DNS Domain Discovery ⓘ

Trace Name

e.g trace_[site ID]

Trace Duration(minutes)

60

Filters

Select Site(branch site only)*

SITE_101 ▾

VPN*

1 VPN(s) × ▾

Source Address/Prefix

101.101.101.20

Destination Address/Prefix

☒ Application ⓘ
 ☐ Application Group ⓘ

- 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:

INSIGHTS Selected trace: trace_80 (Trace Id: 80)

Applications

Active Flows

Completed Flows

Selected Flow ID: 50

Filter ▾

Search by Domain, Application, Readout, etc. ⓘ

Q Search

* Readout Legend: ● Error, ● Warning, ● Information, ● Synthetic Traffic, ● PCAP Replay.

Total Rows: 10

Start - Update Time	Flow ID	Insights *	VPN ...	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	
7:26:05 AM-7:34:05 AM	50	View ●	10	101.101.101.20	54688	172.211.123.249	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g...	N/A	I

Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms) *	Latency(ms) *	ART CND(ms)/SND(ms) *
Upstream	0	R101-2(Tunnel160000003)	SIG	BIZ_INTERNET (SIG)	N/A	0.00	N/A	N/A	N/A	N/A	R101-2: N/A
Downstream	0	SIG	(Tunnel160000003)R101-2	N/A	BIZ_INTERNET (SIG)	N/A	N/A	0.00	N/A	N/A	N/A

7:35:23 AM-7:35:23 AM	563	View ●	10	101.101.101.20	56408	172.211.123.248	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g...	N/A	I
7:37:35 AM-7:37:35 AM	668	View ●	10	101.101.101.20	53175	8.8.8.8	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	N/A	I
7:37:38 AM-7:37:38 AM	573	View ●	10	101.101.101.20	56560	3.74.137.87	443	TCP	DEFAULT ↑ / DEFAULT ↓	ProxySecureA...	other	N/A	I

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).