

Beveiligde toegang configureren met automatische SD-WAN-tunnels voor beveiligde internettoegang

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Beveiligde toegangsconfiguratie](#)

[API maken](#)

[SD-WAN-configuratie](#)

[API-integratie](#)

[Beleidsgroep configureren](#)

[Maak uw aangepaste Bypass FQDN of APP in SD-WAN \(OPTIONEEL\)](#)

[Uw verkeer routeren](#)

[Verifiëren](#)

[Veilige toegang - zoeken naar activiteiten](#)

[Veilige toegang - Evenementen](#)

[Catalyst SD-WAN Manager - inzicht in netwerkbrede paden](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u Secure Access configureert met automatische SD-WAN-tunnels voor beveiligde internettoegang.



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

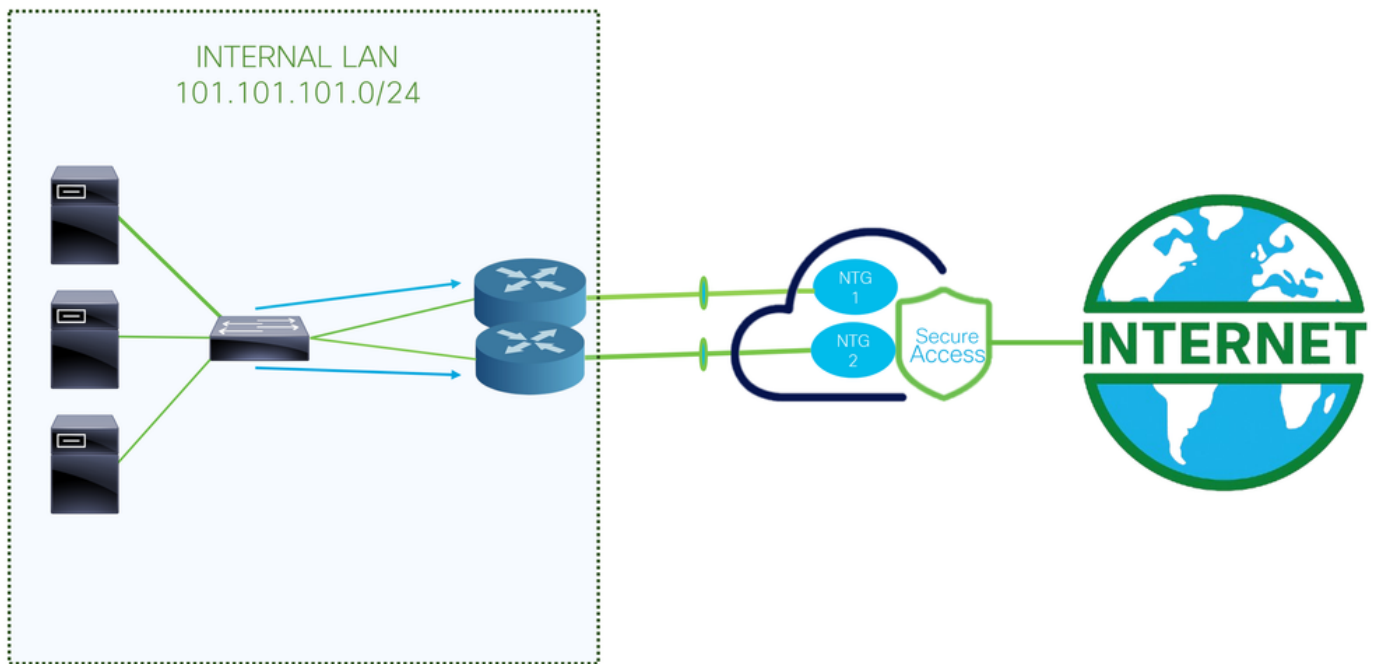
Achtergrondinformatie

Naarmate organisaties steeds meer cloud-gebaseerde applicaties gebruiken en gedistribueerde werknemers ondersteunen, moeten netwerkarchitecturen evolueren om veilige, betrouwbare en schaalbare toegang tot bronnen te bieden. Secure Access Service Edge (SASE) is een framework dat netwerken en beveiliging converteert naar één cloud-geleverde service, waarbij SD-WAN-mogelijkheden worden gecombineerd met geavanceerde beveiligingsfuncties zoals Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), DNS-layer beveiliging, Zero Trust Network Access (ZTNA) of geïntegreerde VPN voor beveiligde externe toegang.

De integratie van Cisco Secure Access met SD-WAN via geautomatiseerde tunnels stelt organisaties in staat om internetverkeer veilig en efficiënt te routeren. SD-WAN biedt intelligente padselectie en geoptimaliseerde connectiviteit op gedistribueerde locaties, terwijl Cisco Secure Access ervoor zorgt dat al het verkeer wordt geïnspecteerd en beschermd volgens het beveiligingsbeleid van het bedrijf voordat het internet wordt bereikt.

Door tunnelconfiguratie tussen SD-WAN-apparaten en Secure Access te automatiseren, kunnen organisaties de implementatie vereenvoudigen, de schaalbaarheid verbeteren en zorgen voor consistente handhaving van de beveiliging voor gebruikers, ongeacht waar ze zich bevinden. Deze integratie is een belangrijk onderdeel van een moderne SASE-architectuur, die veilige internettoegang mogelijk maakt voor filialen, externe sites en mobiele gebruikers.

Netwerkdigram



Dit is de architectuur die voor dit configuratievoorbeeld wordt gebruikt. Zoals je kunt zien zijn er twee edge routers:

Als u ervoor kiest om het beleid op twee verschillende apparaten te implementeren, wordt voor elke router een NTG geconfigureerd en wordt NAT ingeschakeld aan de kant van Secure Access. Hierdoor kunnen beide routers verkeer van dezelfde bron door de tunnels sturen. Normaal gesproken is dit niet toegestaan, maar door de NAT-optie voor deze tunnels in te schakelen, kunnen twee edge-routers verkeer verzenden dat afkomstig is van hetzelfde bronadres.

Voorwaarden

Vereisten

- Veilige toegang tot kennis
- Cisco Catalyst SD-WAN Manager Release 20.15.1 en Cisco IOS XE Catalyst SD-WAN Release 17.15.1 of hoger
- Tussentijdse kennis van routing en switching
- ECMP-kennis
- VPN-kennis

Gebruikte componenten

- Secure Access-huurder
- Catalyst SD-WAN Manager Release 20.18.1 en Cisco IOS XE Catalyst SD-WAN Release 17.18.1
- Catalyst SD-WAN Manager

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Beveiligde toegangsconfiguratie

API maken

Om de geautomatiseerde tunnels met Secure Access te maken, controleert u de volgende stappen:

Navigeer naar het [Secure Access Dashboard](#).

- Klik op **Admin > API Keys**
- Klik op **Add**
- Kies de volgende opties:
 - Deployments / Network Tunnel Group: **lezen/schrijven**
 - Deployments / Tunnels: **lezen/schrijven**
 - Deployments / Regions: **Alleen-lezen**
 - Deployments / Identities: **Betreft: Lezen-schrijven**
 - Expiry Date: **Nooit verlopen**

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](#)



Opmerking: Voeg optioneel maximaal 10 netwerken toe van waaruit deze sleutel verificaties kan uitvoeren. Voeg netwerken toe met behulp van een door komma's gescheiden lijst met openbare IP-adressen of CIDR's.

- Klik **CREATE KEY** om de creatie van de API Key en Key Secret te voltooien.

API Key 397766cdb29f43b08dde3b1d8c04e45 	Key Secret bfce729cd3e243e281df7271acb12208 
---	---



Let op: Kopieer ze voordat u klikt **ACCEPT AND CLOSE**; anders moet u ze opnieuw maken en degenen verwijderen die niet zijn gekopieerd.

Om vervolgens te finaliseren klik **ACCEPT AND CLOSE**.

SD-WAN-configuratie

API-integratie

Navigeer naar Catalyst SD-WAN Manager:

- Klik op **Administration** > **Settings** > **Cloud Credentials**
- Klik vervolgens op **Cloud Provider Credentials** en schakel de API- en Cisco SSEorganisatieinstellingen in en vul deze in

The screenshot displays the 'Settings / External Services' page in the Cisco Catalyst SD-WAN Manager. The left sidebar contains a navigation menu with categories like Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, and Administration. The 'Administration' category is selected, and the 'Cloud Credentials' option is highlighted. The main content area shows the 'Cloud Provider Credentials' tab, which includes instructions for configuring Cisco Umbrella, Zscaler, and Cisco Secure Access credentials. There are input fields for 'Organization Id', 'Api Key', and 'Secret', and toggle switches for 'Umbrella', 'Zscaler', and 'Cisco SSE'. A 'Context Sharing' toggle is also present. 'Save' and 'Cancel' buttons are at the bottom.

- Organization ID: U kunt dat uit de URL van uw SSE Dashboard <https://dashboard.sse.cisco.com/org/xxxxx>
- Api Key: Kopieer het vanuit de stap [Beveiligde toegangsconfiguratie](#)
- Secret: Kopieer het vanuit de stap [Beveiligde toegangsconfiguratie](#)

Daarna klik je op de Save knop.



Opmerking: Voordat u verder gaat met de volgende stappen, moet u ervoor zorgen dat de SD-WAN-manager en de Catalyst SD-WAN-randen DNS-resolutie en internettoegang hebben.

Als u wilt controleren of DNS-Lookup is ingeschakeld, gaat u naar:

- Klik op Configuratie > Configuratiegroepen
- Klik op het profiel van uw Edge-apparaten en bewerk het systeemprofiel

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

- Bewerk vervolgens de optie Globaal en zorg ervoor dat de optie Domeinresolutie is ingeschakeld

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 ☐ ☐
 FTP Passive ☐ ☐
 ARP Proxy ☐ ☐
 Cisco Discovery Protocol (CDP)

HTTPS Server ☐ ☐
 Domain Lookup ☒ ☒
 RSH/RCP ☐ ☐
 Line Virtual Teletype (Configure O)

Beleidsgroep configureren

Navigeer naar Configuratie > Beleidsgroepen:

- Klik op 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](#)



Opmerking: in releases lager dan 20,18 wordt deze optie Secure Service Edge (SSE) toevoegen genoemd

- Configureer een naam, oplossing en klik op [Create](#)

Secure Internet Access

Name

SIA

Solution

sdwan

Description (optional)

Cancel

Create

Met de volgende configuraties kunt u de tunnels maken nadat u de configuratie in uw Catalyst SD-WAN-randen hebt geïmplementeerd:

SSE Provider

☒ Cisco SSE ☐ Zscaler

Context Sharing

☒ VPN ☒ SGT

Tracker

Source IP address

{{ Monitoring }}

- SSE Provider: **SSE**
- Context SharingKies: VPN of/en SGT is afhankelijk van uw behoeften
- Tracker
 - **Source IP Address:** Kies Apparaatspecifiek (hiermee kunt u het per apparaat wijzigen en de gebruikssituatie voor het apparaat in de implementatiefase identificeren)

Onder de Configuration trede zet je de tunnels:

Configuration

+ Add Tunnel

Single Hub HA Scenario

ECMP Scenario with HA

Single Hub HA Scenario

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface*: GigabitEthernet1 (Max one tunnel per hub)

Tunnel Route Via: <SYSTEM DEFAULT> (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.)

Tracker: DefaultTracker

Data Center: Primary

ECMP Scenario with HA

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface*: Loopback1 (Max 8 Tunnels per Hub 8GB X 1)

Tunnel Route Via: GigabitEthernet1

Tracker: DefaultTracker

Data Center: Primary

- **Single Hub HA Scenario:** In dit scenario kunt u hoge beschikbaarheid configureren met de ene NTG als actief en de andere als passief, met een maximale doorvoer van 1 Gbps per NTG
- **ECMP Scenario with HA:** In dit scenario kunt u maximaal 8 tunnels per hub configureren, met ondersteuning van in totaal maximaal 16 tunnels per NTG. Deze opstelling zorgt voor een hogere doorvoer over de tunnels



Opmerking: als uw netwerkinterfaces een doorvoer hebben van meer dan 1 Gbps en u schaalbaarheid nodig hebt, moet u loopback-interfaces gebruiken. Anders kunt u standaardinterfaces op uw apparaat gebruiken. Dit is om ECMP in te schakelen vanaf de kant met beveiligde toegang.



Waarschuwing: Als u loopback-interfaces wilt configureren voor een ECMP-scenario, moet u eerst de loopback-interfaces instellen in Configuration Groups > Transport & Management Profile, onder het beleid dat u in uw router gebruikt.

- Klik op [Add Tunnel](#)

Edit Tunnel

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

- Interface Name: IPSec1, IPSec2, IPSec3 enzovoort
- Tunnel Source Interface Kies Loopback Interfaces of een specifieke interface van waaruit u de tunnel instelt
- Tunnel Route Via: Als u Loopback kiest, moet u de fysieke interface selecteren van waaruit u het verkeer wilt routeren. Als u Loopback niet selecteert, wordt deze optie grijs weergegeven en wordt de eerste interface met NAT gebruikt die door het systeem wordt gevonden. Als er meerdere zijn, moet u de gewenste WAN-interface selecteren
- Data Center: Dit betekent met welke Hub in Secure Access u de verbinding tot stand brengt

In het volgende deel van de tunnelconfiguratie configureert u de tunnels volgens de best practices van 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

Daarna moet u de secundaire tunnel configureren die naar het secundaire datacenter wijst.

SINGLE HUB HA-SCENARIO

Configuration

+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
 ipsec1		 false	 1350	 1390	 
 ipsec2		 false	 1350	 1390	 

Dit is het uiteindelijke resultaat wanneer u de normale scenario-implementatie gebruikt.

ECMP SCENARIO WITH HA

Interface Name	Description	Shutdown	TCP MSS	IP MTU
 ipsec1		 false	 1350	 1390
 ipsec2		 false	 1350	 1390
 ipsec3	PRIMARY HUB	 false	 1350	 1390
 ipsec4		 false	 1350	 1390
 ipsec5		 false	 1350	 1390
 ipsec11		 false	 1350	 1390
 ipsec12		 false	 1350	 1390
 ipsec13	SECONDARY HUB	 false	 1350	 1390
 ipsec14		 false	 1350	 1390
 ipsec15		 false	 1350	 1390

Vervolgens moet u High Availability configureren in het beleid voor veilig internet.

High Availability

+ Add Interface Pair

Klik op Interfacepaar toevoegen:

PRIMARY
SECONDARY

Edit Interface Pair



Active Interface ⊕ ipsec1 ⊗ v		Active Interface Weight ⊕ 1	
Backup Interface ⊕ ipsec11 ⊗ v		Backup Interface Weight ⊕ 1	

Tunnel Type Interface Name(1..255) ⊕ ipsec1	Tunnel Type: IPsec Tunnel Source Interface* ⊕ Loopback1	Tunnel Type Interface Name(1..255) ⊕ ipsec11	Tunnel Type: IPsec Tunnel Source Interface* ⊕ Loopback11
Tunnel Route Via ⊕ GigabitEthernet1	Tracker ⓘ ⊕ DefaultTracker	Tunnel Route Via ⊕ GigabitEthernet1	Tracker ⓘ ⊕ DefaultTracker
Data Center ☒ Primary ☐ Secondary		Data Center ☐ Primary ☒ Secondary	

In deze stap moet u de primaire en secundaire tunnel configureren voor elk tunnelpaar dat u instelt. Dit betekent dat elke tunnel zijn eigen back-up heeft. Vergeet niet dat deze tunnels werden gemaakt als Primair en Secundair voor dit exacte doel.

"Active interface" verwijst naar de primaire tunnel, terwijl "Backup interface" verwijst naar de secundaire tunnel:

- Active Interface: Primair
- Backup Interface: Secundair



Waarschuwing: Als deze stap wordt overgeslagen, komen de tunnels niet naar boven en wordt er geen verbinding tot stand gebracht van de routers naar Secure Access.

Nadat High Availability is geconfigureerd voor de tunnels, wordt de installatie weergegeven zoals weergegeven in de onderstaande afbeelding. In het labvoorbeeld dat voor deze gids wordt gebruikt, worden vijf tunnels getoond in HA. Het aantal tunnels kan naar behoefte worden aangepast.

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



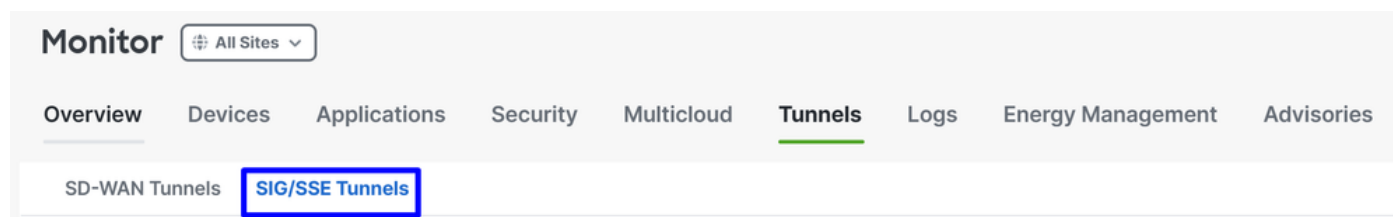
Opmerking: Er kunnen maximaal 8 tunnelparen (16 tunnels: 8 primaire en 8 secundaire) worden geconfigureerd in SD-WAN Catalyst vManage. Cisco Secure Access ondersteunt maximaal 10 tunnelparen.

- Klik op de knop **Save**

Na dit punt, als alles correct is geconfigureerd, worden de tunnels weergegeven als UP in de SD-WAN Manager en Secure Access.

Controleer de volgende stappen voor verificatie in SD-WAN:

- Klik op **Monitor > Tunnels**
- Klik vervolgens op **SIG/SSE Tunnels**



En u kunt de tunnels zien die zijn ingesteld om Cisco Secure Access UP te gebruiken of niet.

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

Controleer de volgende stappen om in Secure Access te controleren:

- Klik op 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](#)

Q -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	...

Klik in een gedetailleerde weergave op de naam van de 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

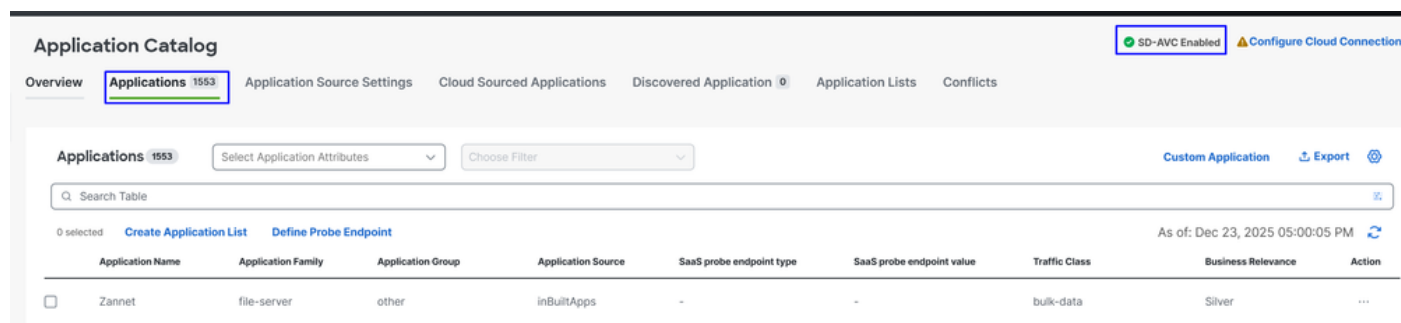
Daarna kun je de stap zetten, Create your Custom Bypass FQDN or APP in SD-WAN

Maak uw aangepaste Bypass FQDN of APP in SD-WAN (OPTIONEEL)

Er zijn speciale gebruikssituaties waarin u Application Bypass en FQDN of IP moet maken die u kunt toepassen op uw routeringsbeleid:

Navigeer naar de SD-WAN Manager portal:

- Klik op Configuration > Application Catalog > Applications



The screenshot shows the 'Application Catalog' page. At the top, there's a navigation bar with 'Overview', 'Applications 1553', 'Application Source Settings', 'Cloud Sourced Applications', 'Discovered Application 0', 'Application Lists', and 'Conflicts'. The 'Applications 1553' tab is active. Below the navigation bar, there's a search bar and filters. The main table has columns: Application Name, Application Family, Application Group, Application Source, SaaS probe endpoint type, SaaS probe endpoint value, Traffic Class, Business Relevance, and Action. One application is listed: 'Zannet' with family 'file-server', group 'other', source 'inBuiltApps', and traffic class 'bulk-data'. The 'Custom Application' button is highlighted in the top right corner.

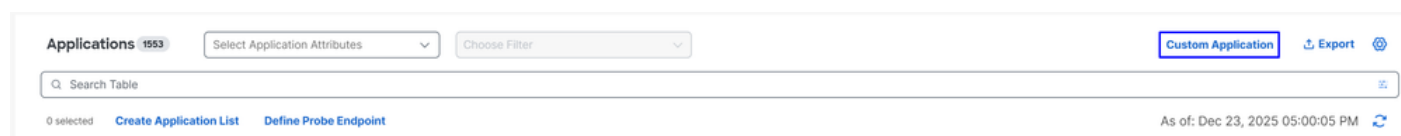


Tip: Als u een versie gebruikt die lager is dan 20.15, kunnen aangepaste toepassingen worden gemaakt onder Beleidslijsten



Opmerking: om toegang te krijgen tot de toepassingscatalogus moet u SD-AVC inschakelen.

- Klik op Custom Application



This screenshot is similar to the previous one, but the 'Custom Application' button is highlighted with a red box. The table and other interface elements are the same.

In dit stadium wordt een basisuitsluiting geconfigureerd met behulp van de SWG FQDN-module Secure Client – Umbrella Module:

ProxySecureAccess

✕

Custom Application

Name of the Custom APP

Application Name ⓘ

Application Name: ProxySecureAccess-Custom

Server Names ⓘ

FQDN

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 ⓘ
10.X.X.X, 20.0.0.0/24 separated by	Space separated ports or range or	Enter L4 Protocol ▼

SaaS probe endpoint type

☐ IP Address
☐ FQDN
☐ URL

SaaS probe endpoint value

Cancel Save

- Server Name: Gebruik de FQDN die u wilt omzeilen (In dit voorbeeld zijn FQDN van SWG geconfigureerd)
 - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
 - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Klik op Save



Opmerking: wijzig ORGID met uw SSE-organisatienummer.

Vervolgens wordt een basisuitsluiting gemaakt; in dit geval de Umbrella DNS-servers:

UmbrellaDNS

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

Nu kunt u doorgaan met de configuraties van het routeringsbeleid.

Uw verkeer routeren

In deze stap moet u internetverkeer door de tunnels leiden om het te beschermen via Cisco Secure Access. In dit geval gebruikt u een flexibel routeringsbeleid waarmee we bepaalde verkeersstromen kunnen omzeilen om te voorkomen dat ongewenst verkeer via Secure Access wordt verzonden of om mogelijke slechte praktijken te voorkomen.

Laat het eerst de twee routeringsmethoden definiëren die kunnen worden gebruikt:

- **Configuration > Configuration Groups > Service Profile > Service Route:** Deze methode biedt routing naar Secure Access, maar mist flexibiliteit.
- **Configuration > Policy Groups > Application Priority & SLA:** Deze methode biedt verschillende routeringsopties binnen SD-WAN en, belangrijker nog, stelt u in staat om specifiek verkeer te omzeilen, zodat het niet via Secure Access wordt verzonden.

Voor flexibiliteit en afstemming op best practices wordt deze configuratie gebruikt, Application Priority & SLA:

- Klik op **Configuration > Policy Groups > Application Priority & SLA**
- Klik vervolgens op **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

- Configureer een beleidsnaam en klik op **Create**

Application Priority & SLA Policy

Policy Name

SIA-ROUTE

Description (optional)

Cancel

Create

- Inschakelen **Advanced Layout**
- Klik op **+ 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: Naam die dit aanpast aan het doel van deze lijst met verkeersbeleid
- VPN(s): Kies de VPN-service van de gebruiker van waar u het verkeer routeert
- Direction: Uit dienst
- Default action: accepteren

Daarna kunt u beginnen met het opstellen van het verkeersbeleid:

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

VPN: Corporate_Users Direction: From Service Default Action: Accept

	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 F ULL TRAFFI C	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) Bron: 101.101.101.0/24, bestemming 172.16.200.0/24. Deze route voorkomt dat verkeer binnen het netwerk wordt verzonden naar Cisco Secure Access. Doorgaans doen klanten dit niet, omdat interne routing meestal wordt afgehandeld door de distributierouter in SD-WAN-implementaties. Deze configuratie zorgt ervoor dat intern

verkeer tussen deze subnetten niet wordt gerouteerd naar Secure Access, afhankelijk van of uw scenario dit vereist (optioneel, afhankelijk van uw netwerkomgeving)

2. **BypassSSEProxy (Optional):** Dit beleid voorkomt dat interne computers met de Cisco Umbrella-module in Secure Client en SWG ingeschakeld, proxyverkeer terugsturen naar de cloud. Het opnieuw routeren van proxy-verkeer naar de cloud wordt niet als beste praktijk beschouwd.
3. **UmbrellaDNS (Best Practice):** Dit beleid voorkomt dat DNS-query's die bestemd zijn voor het internet door de tunnel worden verzonden. Het verzenden van DNS-query's naar Umbrella resolvers (208.67.222.222,208.67.220.220) via de tunnel wordt niet aanbevolen.
4. **SIA AUTO FULL TRAFFIC:** Dit beleid routeert al het verkeer van de bron 101.101.101.0/24 naar het internet via de SSE-tunnels die u eerder hebt gemaakt, zodat dit verkeer in de cloud wordt beschermd.

Verifiëren

Om te controleren of het verkeer al overstroomt via Cisco Secure Access, navigeert u naar **Events** of **Activity Search** of **Network-Wide Path Insights** filtert u op uw tunnelidentiteit:

Veilige toegang - zoeken naar activiteiten

Navigeer naar **Monitor > Activity Search**:

Activity Search

Search by domain, identity, or URL **Advanced** **CLEAR** **Saved Searches** **Customize Columns** **All**

IDENTITY CBK-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6 **Restore to default layout** **Save Search**

1,617 Total Viewing activity from Dec 27, 2025 6:14 AM to Dec 28, 2025 6:14 AM Page: 1 Results per page: 50 1 - 50

Response **Select All**

- ☐ Allowed **Advanced**
- ☐ Blocked

Warn Page Behavior **Select All**

- ☐ Warned
- ☐ Accessed After Warn

Isolate

- ☐ Isolated

IPS Signature **Select All**

- ☐ Log Only
- ☐ Would Block
- ☐ Blocked

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

Event Details

Action: Allowed

Time: Dec 28, 2025 6:14 AM

Rule Name: For all Internet access (2100958)

Source: * VPN-10 (VPN-10)

Source IP: CBK-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6

Source IP: 101.101.101.20

Destination: https://youtube.com

Security Group Tag (SGT):

Veilige toegang - Evenementen

Navigeer naar **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: -



Opmerking: zorg ervoor dat uw standaardbeleid met logboekregistratie is ingeschakeld, standaard is uitgeschakeld.

Catalyst SD-WAN Manager - inzicht in netwerkbrede paden

Navigeer naar Catalyst SD-WAN Manager:

- Klik op **Tools** > **Network-Wide Path Insights**
- Klik op **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: Kies de site van waar uw verkeer zich voortzet
- VPN: Kies de VPN-ID van uw subnet waar uw verkeer zich bevindt
- Source: Zet het IP-adres of laat het leeg om al het verkeer te filteren dat door de site en VPN gekozen

Vervolgens kun je in Insights het verkeer zien dat door de tunnels stroomt en het type verkeer dat naar Secure Access gaat:

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(Tunnel16000003)	SIG	BIZ_INTERNET (SIG)	N/A	0.00	N/A	N/A	N/A	N/A	R101-2: N/A
Downstream	0	SIG	(Tunnel16000003)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

Gerelateerde informatie

- [Cisco Technical Support en downloads](#)
- [Cisco Secure Access Help Center](#)
- [Cisco SASE-ontwerphandleiding](#)
- [Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x](#)
- [Cisco SASE-oplossing: Cisco Catalyst SD-WAN geïntegreerd met Cisco Secure Access in één oogopslag](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.