

# Beveiligde toegang configureren met automatische Catalyst SD-WAN-tunnels voor beveiligde privétoegang

## Inhoud

---

[Inleiding](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Beveiligde toegangsconfiguratie](#)

[API maken](#)

[SD-WAN-configuratie](#)

[API-integratie](#)

[Beleidsgroep configureren](#)

[Routing configureren](#)

[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 Catalyst SD-WAN-tunnels voor beveiligde privétoegang.



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

## Achtergrondinformatie

Naarmate organisaties verder gaan dan traditionele perimeter-gebaseerde netwerken, wordt veilige toegang tot privébronnen net zo belangrijk als het beveiligen van internetverkeer. Toepassingen zijn niet langer beperkt tot één enkel datacenter, ze leven nu in on-premises omgevingen, openbare clouds en hybride architecturen. Deze verschuiving vereist een flexibelere en modernere benadering van particuliere toegang.

Dit is waar een op SASE gebaseerde architectuur en Cisco Secure Access een rol spelen. In plaats van te vertrouwen op legacy VPN-concentrators en platte netwerktoegang, biedt Cisco Secure Access privéconnectiviteit als een cloud-geleverde service, waarbij VPN-as-a-Service (VPNaaS) en Zero Trust Network Access (ZTNA) worden gecombineerd.

Voor private toegang op netwerkniveau integreert Cisco Secure Access met SD-WAN met behulp van geautomatiseerde site-to-site IPsec-tunnels. Deze tunnels zorgen ervoor dat privéverkeer veilig kan stromen tussen Secure Access en on-premises of cloudnetwerken, terwijl de beveiligingsinspectie en beleidshandhaving gecentraliseerd blijven in de cloud. Vanuit operationeel oogpunt neemt dit de noodzaak weg om traditionele VPN-headends te implementeren en te onderhouden en vereenvoudigt het schalen naarmate omgevingen groeien.

In een VPNaaS-model fungeert Secure Access als het VPN-terminatiepunt in de cloud. SD-WAN behandelt intelligente routing en veerkracht met Secure Access en zorgt ervoor dat het verkeer wordt beschermd en beheerd door een consistent beveiligingsbeleid voordat het particuliere bronnen bereikt.

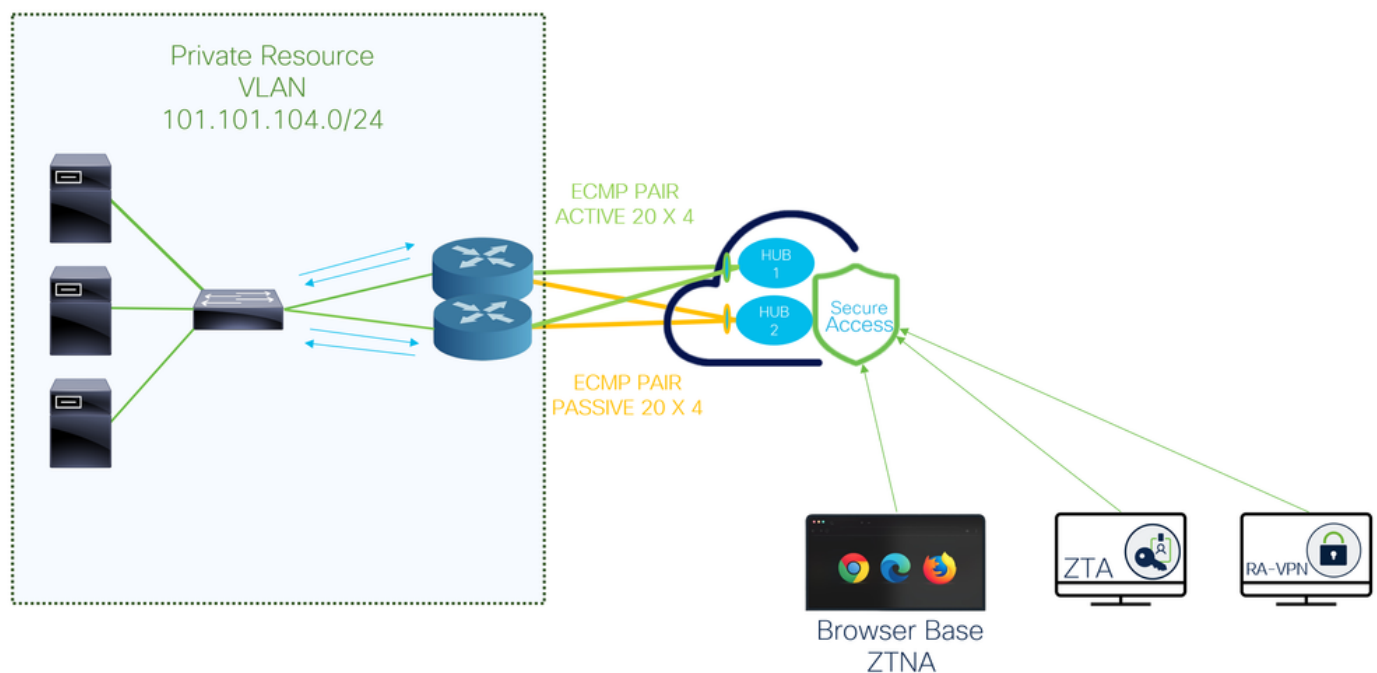
Cisco Secure Access ondersteunt ook geavanceerde site-to-site tunnelarchitecturen, waaronder multiregionale backhaul. Deze mogelijkheid stelt organisaties in staat om tunnels te bouwen naar meerdere Secure Access-regio's tegelijk, wat zorgt voor geografische redundantie en een hogere beschikbaarheid. Door verbinding te maken met verschillende regio's, kan het verkeer automatisch uitvallen in geval van regionale uitval, latetievermindering of onderhoudsgebeurtenissen.

Een organisatie kan bijvoorbeeld site-to-site tunnels opzetten vanuit haar SD-WAN-omgeving naar Secure Access-regio's in Londen en Duitsland. Beide tunnels blijven actief, waardoor veerkrachtige particuliere toegang over regio's mogelijk wordt en continuïteit wordt gewaarborgd, zelfs als één regio niet beschikbaar is. Dit multiregionale ontwerp versterkt de hoge beschikbaarheid, verbetert de fouttolerantie en sluit aan bij de vereisten voor veerkracht op bedrijfsniveau.

Cisco Secure Access dwingt het Zero Trust Network Access (ZTNA)-model af voor meer granulaire toegang. In plaats van gebruikers brede netwerkconnectiviteit te bieden, biedt ZTNA alleen toegang tot specifieke toepassingen, op basis van identiteit, apparaathouding en context. Deze aanpak vermindert het aanvalsoppervlak aanzienlijk en sluit aan bij de Zero Trust-principes.

ZTNA-toegang wordt mogelijk gemaakt door een combinatie van site-to-site tunnels en Resource Connectors. Resource Connectors zijn lichtgewicht virtuele apparaten die alleen uitgaande verbindingen tot stand brengen met Secure Access, wat betekent dat privébronnen nooit rechtstreeks aan internet hoeven te worden blootgesteld.

## Netwerkdigram



## Voorwaarden

### Vereisten

- Veilige toegang tot kennis
- Cisco Catalyst SD-WAN Manager release 20.18.2 en Cisco IOS XE Catalyst SD-WAN release 17.18.2 of hoger
- Tussentijdse kennis van routing en switching
- ECMP-kennis
- VPN-kennis

- Aangezien deze integratie is gebaseerd op gecontroleerde beschikbaarheid, moet u een TAC-geval indienen om te vragen of u de functie in Cisco Secure Access wilt inschakelen

## Gebruikte componenten

- Secure Access-huurder
- Catalyst SD-WAN Manager Release 20.18.2 en Cisco IOS XE Catalyst SD-WAN Release 17.18.2
- 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.

|                                     |             |      |
|-------------------------------------|-------------|------|
| <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



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

397766cdb29f43b08ddee3b1d8c04e45



##### 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 SSE organisatieinstellingen in en vul deze in

- **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** 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

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

**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 Cl**

**HTTP Server** **HTTPS Server**

**FTP Passive** **Domain Lookup**

**ARP Proxy** **RSH/RCP**

## Beleidsgroep configureren

Navigeer naar Configuratie > Beleidsgroepen:

- Klik op 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 |
|------|-------------|----------|
|------|-------------|----------|

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

## Secure Private Application Access

Name

SPA-AUTO

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:

## Configuration

### Segment (VPN)

  Corporate\_User

### Cisco Secure Access Region

  Europe (Germany) 

- Configuration
  - Segment (VPN): Kies de VRF die de toepassing(en) host die toegankelijk is via Secure Access
  - Cisco Secure Access Region: Kies de regio die het dichtst bij de SD-WAN-hub of -tak ligt waar de toepassingen worden gehost

Definieer vervolgens de tunnelconfiguratie. Tunnels die zijn gemaakt voor het primaire beveiligde toegangscentrum zijn actief, terwijl tunnels die zijn gemaakt voor het secundaire beveiligde

toegangscentrum fungeren als back-up.

Klik onder Tunnel Configuration klik + Add Tunnel op:

## Tunnel Configuration

[+ Add Tunnel](#)

# Tunnel

### BASIC SETTINGS

|                                                                                     |                                                                           |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Interface Name(1..255)</b><br><input type="text" value="ipsec101"/>              | <b>Description</b><br><input type="text" value="&lt;system default&gt;"/> |
| <b>Tunnel Source Interface</b><br><input type="text" value="Auto"/>                 | <b>Tunnel Route-Via Interface</b><br><input type="text" value="Auto"/>    |
| <b>Data Center</b><br><input type="radio"/> Primary <input type="radio"/> Secondary |                                                                           |

**Advanced Settings**

**GENERAL**

|                                                       |                                                        |
|-------------------------------------------------------|--------------------------------------------------------|
| <b>Shutdown</b><br><input type="text" value="false"/> | <b>TCP MSS</b><br><input type="text" value="1350"/>    |
| <b>IP MTU</b><br><input type="text" value="1390"/>    | <b>DPD Interval</b><br><input type="text" value="10"/> |

- Tunnel
  - Interface Name: Geef de tunnelnaam op, deze wordt automatisch bijgewerkt telkens wanneer een nieuwe tunnel wordt toegevoegd
  - Tunnel Source Interface: U hoeft deze instelling niet te wijzigen. Als Auto het systeem wordt verlaten, maakt het automatisch een loopback-interface met een /31-masker.
  - Tunnel Route-Via Interface: U hoeft deze instelling niet te wijzigen. Standaard gebruikt het de eerste NATed fysieke WAN-interface op de edge-router, maar deze kan worden gewijzigd als een specifieke WAN-interface vereist is
  - Data Center: Selecteer Primair of Secundair. Als de primaire tunnel al is geconfigureerd,

selecteert u Secundair. In normale scenario's kan de ene tunnel worden geconfigureerd als Primair en een andere als Secundair

- Advanced Settings
  - IP MTU **Gebruik 1390**
  - TCP MSS **Gebruik 1350**



Opmerking: als u meerdere tunnels wilt maken om ECMP in te schakelen en de tunnelcapaciteit te verhogen, kunt u maximaal 10 actieve/10 back-uptunnels per router configureren. Dit levert tot 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 | ✎ 🗑    |                               |



Opmerking: Als u meerdere tunnels per router implementeert, moet u ervoor zorgen dat de transportinterface de totale bandbreedte van alle actieve tunnels samen kan behouden. Als twee tunnels naar verwachting elk maximaal 1 Gbps vervoeren, moet de transportverbinding ten minste 2 Gbps doorvoer ondersteunen.

Nadat de tunnels zijn geconfigureerd, gaat u verder met de BGP-configuratie.

## BGP Routing

### BGP ASN ⓘ

 ▼

65000

### In Route Policy

 ▼

SPA\_Auto-In

### Out Route Policy

 ▼

SPA\_Auto-Out

- **BGP Routing**

- BGP ASN: AS-nummer opgeven voor de SD-WAN-hub. De AS 64512 is gereserveerd voor beveiligde toegang en kan niet worden gebruikt. Voor meer informatie over BGP, zie
- In Route Policy: Het systeem maakt automatisch dit inkomende routebeleid met een `deny all` instructie om routeringsproblemen te voorkomen. Het moet handmatig worden gewijzigd door middel van een [CLI Add-On Template](#) protocol om de juiste routes toe te staan/te weigeren.
- Out Route Policy: Het systeem maakt dit uitgaande routebeleid met een `deny all` verklaring om routeringsproblemen te voorkomen. Het moet handmatig worden bewerkt via een [CLI Add-On Template](#) link om de juiste routes toe te staan/te weigeren.



Waarschuwing: vanaf november 2025 gebruiken alle nieuw opgerichte organisaties voor beveiligde toegang standaard de openbare ASN 32644 voor BGP-peering in netwerktunnelgroepen. Bestaande organisaties die vóór november 2025 zijn opgericht, blijven gebruikmaken van de private ASN 64512 die voorheen was gereserveerd voor Secure Access BGP-peers. Als het privé-AS-nummer 64512 is toegewezen aan een apparaat in uw netwerk, kan het niet peer met een netwerktunnelgroep die is geconfigureerd voor Peer (Secure Access) BGP AS 64512.

---

De volgende BGP en route-map configuratie wordt automatisch gemaakt voor elke BGP-buur nadat u het nieuwe beleid hebt Deploy ingevoerd in uw Policy Groupwebsite.

```
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

```

Hierna klikt u op **Save** en gaat u verder met de beleidsimplementatie om de tunnels naar boven te brengen.

- Klik op **Configuration > Policy Groups**
- Kies onder uw **Policy > Secure Service Edge > Secure Private Application Access** en klik op het recente profiel dat is gemaakt voor SPA.
- Klik **Deploy** om te voltooien

The screenshot shows the 'Policy Groups' configuration interface. The 'Secure Private Application Access' dropdown menu is open, displaying a list of policy groups. 'SPA-Auto' is highlighted in blue, and a blue arrow points from it to the 'Deploy' button in the 'Device Solution' section on the right. The 'Device Solution' section also shows 'Type: sdwan' and 'Deployment: Associated 1 device'.

Voer de volgende stappen uit om inSecure Access te controleren:

- Klik op **Connect > Network Connections**

## TUNNELINRICHTING

eu-central-1

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

**Summary**

Connected

Region: Europe (Germany)

Device Type: Cisco IOS-XR

Last Status Update: Feb 08, 2026 10:12 PM

Routing Type: Dynamic Routing (BGP)

Device BGP AS: 65000

Peer (Secure Access) BGP AS: 64512

BGP Peer (Secure Access) IP Addresses: 193.254.0.8, 193.254.0.5, 2404-a44-bx723-647-0000/32

Multipoint BGP Addresses: ---

Multipoint TTL: ---

MAX 20 TUNNELS PER DEVICE CONNECTED TO THE NETWORK TUNNEL GROUP

10 X 1 Primary Hub

10 X 1 Secondary Hub

[View advanced settings](#)

**Primary Hub**

Hub Up

10 Active Tunnels

Tunnel Group ID: eu-central-1083346169-661683097-aaa.cisco.com

Data Center: ssa-eu-1-1-0

IP Address: 193.254.0.8/32

**Secondary Hub**

Hub Up

10 Active Tunnels

Tunnel Group ID: eu-central-1083346169-661683099-aaa.cisco.com

Data Center: ssa-eu-1-1-0

IP Address: 193.254.0.5/32

## Routing configureren

Navigeer naar **Configure > Configuration Groups**

- Klik op je Configuration Group **website** en maak/bewerk je CLI Add-on Profile

**Configuration Groups** SD-WAN

**Configuration Groups** 3 **System Profile** 5 **Transport & Management Profile** 6 **Policy Profile** 1 **Service Profile** 4 **CLI Add-on Profile** 3 **UC Voice Profile** 0 **Other Profile** 1

Last Updated Status Create Configuration Group Export Import

| Name            | Type          | Profiles                                                                                                                                                                                                                                   | Provisioning Status | In Sync Devices / Associated Devices | Source | Updated By       | Last Updated On                  |
|-----------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------------------|--------|------------------|----------------------------------|
| <b>SPA-AUTO</b> | Single Router | <div> <div>System Profile</div> <div>SPA-AUTO</div> </div> <div> <div>Policy Profile (optional)</div> <div>Default_Policy_Object_Profile</div> </div> <div> <div>CLI Add-on Profile (optional)</div> <div>SPA_Auto_Route-maps</div> </div> | Sourced from User   |                                      |        | Updated by admin | Updated Feb 11, 2026, 9:05:14 AM |

Deployment

Associated 1 device

Provisioning 1 out of sync

Save Deploy

Als u BGP-routes wilt laten uitwisselen, gebruikt u de eerder geconfigureerde **In Route Policy** en **Out Route Policy**geconfigureerde. U kunt een basisvoorbeeld vinden voor de configuratie van de CLI Add-On route. Deze sjabloon biedt een startpunt en moet naar behoefte worden aangepast:

```
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



Waarschuwing: Een zorgvuldige planning is vereist bij het definiëren van de netwerken die zijn toegestaan in en uit via BGP routekaarten. Het toestaan van alle routes, zoals getoond in het bovenstaande voorbeeld, kan onbedoeld routegedrag introduceren. Geef voor een optimale implementatie expliciet alleen de benodigde netwerken op in uw routekaarten om gecontroleerde en voorspelbare routeringsuitkomsten te garanderen

Nu kunt u doorgaan naar [Deploy the changes](#)

Om te controleren of BGP-routes zijn ontvangen Secure Access, controleert u de volgende stappen:

- Klik op [Connect](#) > [Network Connections](#) > en [Network Tunnel Groups](#) select de NTG-naam

## ROUTERENDE INRICHTING

The screenshot displays the Cisco Secure Access management console. On the left, a sidebar contains navigation options: Home, Experience Insights, Connect, 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 a specific tunnel group: Tunnel Group ID (eu-central-1@8356169-661683097-sse.cisco.com), 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 for the selected group.

| 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 |

A detailed view of 'Primary 1 (131130)' is shown on the right. It includes fields for SPI In (3318601812) and SPI Out (3490872006). The 'IKE' section shows 'State: ESTABLISHED', 'Age: 141464 sec', and 'PRF Algorithm: HMAC-SHA2-256'. The 'Encryption Algorithm' is 'AES-CBC-256' and the 'DH Group' is 'ECP-384'. The 'Routing' section shows 'Routing Type: BGP' and 'Client Routes: 172.16.104.0/24'. A list of 'Cloud Routes' is also visible, including various IP ranges. A 'Download Routing Table' link is present at the bottom of the routing section.



Opmerking: In dit voorbeeld wordt het subnet voor zakelijke gebruikers 172.16.104.0/24 geadverteerd voor Secure Access via BGP. Dit maakt een goede routing tussen Catalyst SD-WAN en de SSE-omgeving mogelijk.

Hetzelfde beleid kan worden toegepast op beide WAN-randen in de Catalyst SD-WAN-hubs, wat resulteert in 20 actieve tunnels en 20 standby-tunnels. Het totale aantal tunnels hangt af van het aantal dat op elke rand is geconfigureerd. Elke router die is aangesloten op beide Secure Access-hubs (Hub 1 en Hub 2) vormt een ECMP-paar in alle gevestigde tunnels.

Als bijvoorbeeld Catalyst SD-WAN Edge 1 10 tunnels heeft en Catalyst SD-WAN Edge 2 10 tunnels, vormt Secure Access ECMP in de 20 actieve tunnels. Hetzelfde geldt voor de secundaire SSE-hub.

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<br>Catalyst SDWAN | Connected | Europe (Germany) | sse-euc-1-1-1           | 20              | sse-euc-1-1-0             | 20                |

## Verifiëren

Om te controleren of het verkeer via Cisco Secure Access verloopt, navigeert u naar [Events of Activity Search](#) of [Network-Wide Path Insights](#) en filtert u op uw tunnelidentiteit:

## Veilige toegang - zoeken naar activiteiten

Navigeer naar [Monitor](#) > [Activity Search](#) :

Activity Search

FILTERS

Q Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

IP ADDRESS

172.16.104.11

IDENTITY

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

Restore to

Search filters

4 Total

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

Page: 1

Resu

| Response                                                           | Request        | Source                                                 | Rule Identity                                          | Destination | Destination IP     | Destination Po |
|--------------------------------------------------------------------|----------------|--------------------------------------------------------|--------------------------------------------------------|-------------|--------------------|----------------|
| <div><div>Allowed</div><div>Advanced</div><div>Blocked</div></div> | 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           |
| <div><div>Warned</div><div>Accessed After Warn</div></div>         | 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           |

## Veilige toegang - Evenementen

Navigeer naar [Monitor](#) > [Events](#):

Events

Schedule report

Export CSV

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

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 (Brow...

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

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

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

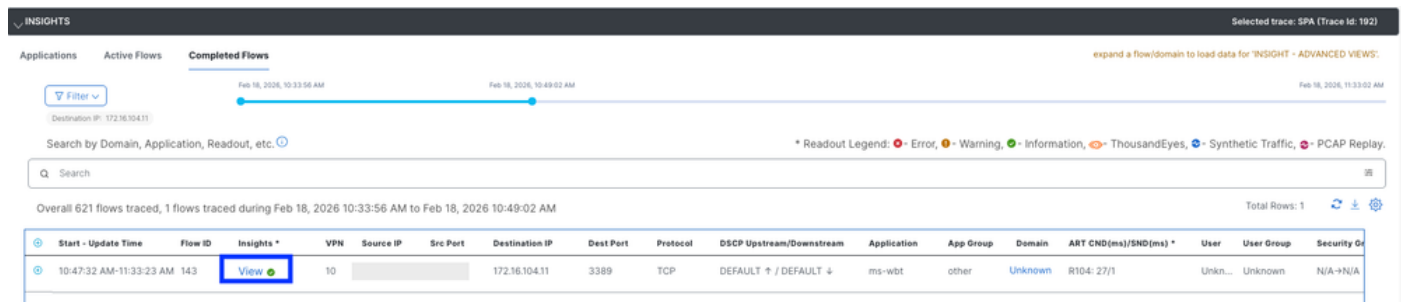
Start

- Trace Name: (optioneel) Trace-naam opgeven

- Site: Kies de site waar de privébron zich bevindt
- VPN: Kies de VPN-ID waar de privébron zich bevindt
- Source/Destination Address: (Optioneel) Voer het IP-adres in of laat het leeg om al het verkeer vast te leggen dat is gefilterd op basis van site en VPN gekozen

Start het spoor

Zoek de verkeersstroom en klik op Weergave in de kolom Inzichten



De kolom Inzichten routing geeft de kandidaatpaden weer en geeft de IPSec-tunnels voor beveiligde toegang weer

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

Upstream (From 15645 to 172.16.104.11:3389)

Hop 0 - Edge Name: R104

IP Lookup on VPN 10

Destination Addr:  
172.16.104.11  
Match Route:  
172.16.104.11/32

Route Info  
Source: adjacent  
Distance: 0  
Metric: 0

Routing Candidate Paths: 1

SERVICE LAN  
Local Interface: GigabitEthernet3

Path Decided By:

routing

Final Path:

SERVICE LAN  
Local Interface: GigabitEthernet3

Downstream (From 172.16.104.11:3389 to 15645)

Hop 0 - Edge Name: R104

IP Lookup on VPN 10

Destination Addr:  
Match Route:  
/32

Route Info  
Source: bgp (external)  
Distance: 20  
Metric: 0  
Received From:  
Peer: 169.254.0.41  
Uptime: 1d07h  
Peer: 169.254.0.35  
Uptime: 1d07h  
Peer: 169.254.0.31  
Uptime: 1d07h  
Peer: 169.254.0.27  
Uptime: 1d07h  
Peer: 169.254.0.23  
Uptime: 1d07h  
Peer: 169.254.0.21  
Uptime: 1d07h  
Peer: 169.254.0.15  
Uptime: 1d07h  
Peer: 169.254.0.13  
Uptime: 1d07h

Routing Candidate Paths: 10

SERVICE LAN  
Local Interface: Tunnel17000111

SERVICE LAN  
Local Interface: Tunnel17000109

SERVICE LAN  
Local Interface: Tunnel17000103

SERVICE LAN  
Local Interface: Tunnel17000101

Path Decided By:

NAT

NAT Translate Source  
Pre-NAT  
Addr:192.168.4.111  
Port:4500  
Post-NAT  
Addr:192.168.0.105  
Port:5079

Final Path:

NAT DIA  
Local Color: BIZ\_INTERNET  
Local Interface: GigabitEthernet1

## Gerelateerde informatie

- [Cisco Technical Support en downloads](#)
- [Cisco Secure Access Help Center](#)
- [Cisco SASE-ontwerphandleiding](#)
- [Beveiligde toegang configureren met automatische SD-WAN-tunnels voor beveiligde internettoegang](#)

- [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.