

Konfigurieren von sicherem Zugriff mit automatisierten Catalyst SD-WAN-Tunneln für sicheren privaten Zugriff

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfiguration des sicheren Zugriffs](#)

[API-Erstellung](#)

[SD-WAN-Konfiguration](#)

[API-Integration](#)

[Konfigurieren der Richtliniengruppe](#)

[Konfigurieren von Routing](#)

[Überprüfung](#)

[Sicherer Zugriff - Aktivitätssuche](#)

[Sicherer Zugriff - Veranstaltungen](#)

[Catalyst SD-WAN Manager - Netzwerkweite Pfadeinblicke](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration von sicherem Zugriff mit automatisierten Catalyst SD-WAN-Tunneln für sicheren privaten Zugriff beschrieben.



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

Hintergrundinformationen

Da Unternehmen über herkömmliche Perimeter-basierte Netzwerke hinausgehen, wird der sichere Zugriff auf private Ressourcen ebenso wichtig wie die Sicherung des Internetdatenverkehrs. Anwendungen sind nicht mehr auf ein einziges Rechenzentrum beschränkt, sondern laufen heute über standortbasierte Umgebungen, Public Clouds und Hybrid-Architekturen hinweg. Dieser Wandel erfordert einen flexibleren und moderneren Ansatz für den privaten Zugang.

An dieser Stelle kommen eine SASE-basierte Architektur und Cisco Secure Access ins Spiel. Statt sich auf ältere VPN-Konzentratoren und flachen Netzwerkzugriff zu verlassen, bietet Cisco Secure Access eine private Anbindung als Cloud-fähiger Service, der VPN-as-a-Service (VPNaaS) und Zero Trust Network Access (ZTNA) kombiniert.

Für den privaten Zugriff auf Netzwerkebene lässt sich Cisco Secure Access über automatisierte Site-to-Site-IPsec-Tunnel in das SD-WAN integrieren. Durch diese Tunnel kann privater Datenverkehr sicher zwischen Secure Access und standortbasierten oder Cloud-Netzwerken übertragen werden. Gleichzeitig werden Sicherheitsüberprüfungen und die Durchsetzung von Richtlinien in der Cloud zentralisiert. Aus betrieblicher Sicht macht dies die Bereitstellung und Wartung traditioneller VPN-Headends überflüssig und vereinfacht die Skalierung entsprechend wachsender Umgebungen.

Bei einem VPNaaS-Modell fungiert Secure Access als VPN-Terminierungspunkt in der Cloud. SD-WAN sorgt für intelligentes Routing und Ausfallsicherheit mit sicherem Zugriff und stellt sicher, dass der Datenverkehr geschützt und durch konsistente Sicherheitsrichtlinien geregelt wird, bevor er private Ressourcen erreicht.

Cisco Secure Access unterstützt darüber hinaus erweiterte Site-to-Site-Tunnelarchitekturen, darunter Multi-Regional Backhaul. Diese Funktion ermöglicht die gleichzeitige Einrichtung von Tunneln zu mehreren Secure Access-Regionen und sorgt so für geografische Redundanz und eine höhere Verfügbarkeit. Durch die Verbindung mit verschiedenen Regionen kann der Datenverkehr bei regionalen Ausfällen, Latenzverlusten oder Wartungsereignissen automatisch

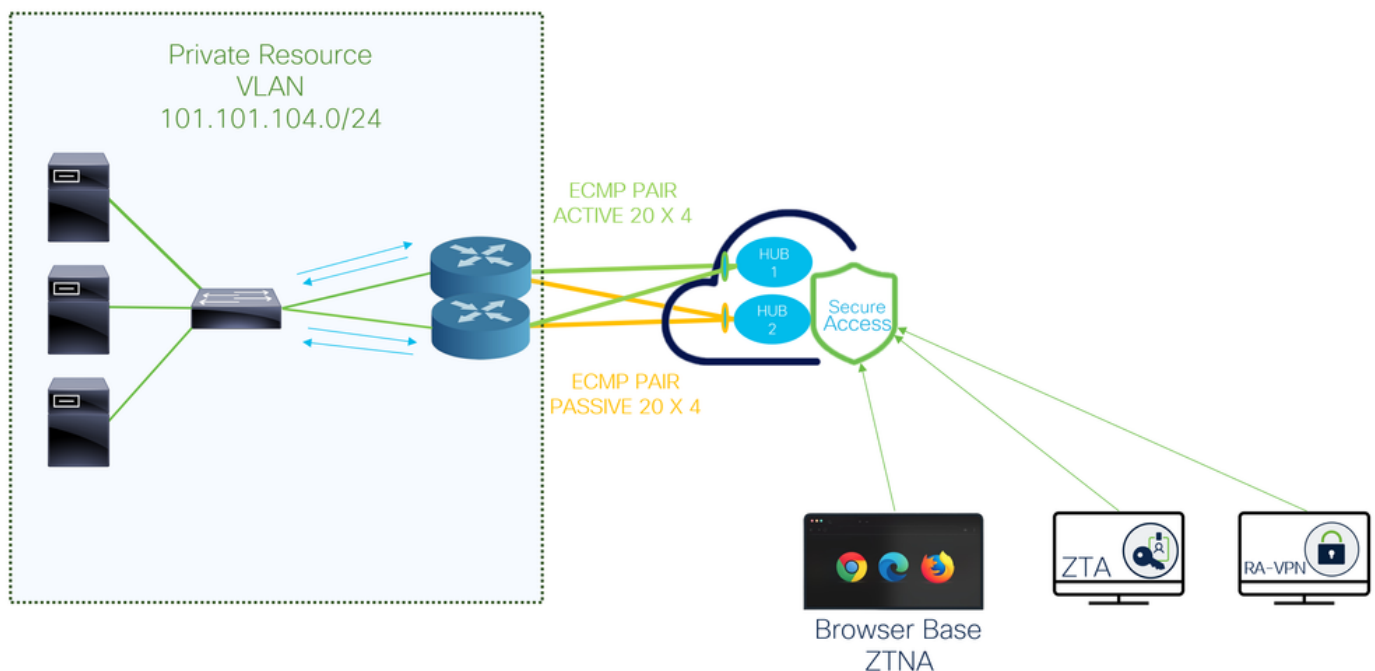
per Failover weitergeleitet werden.

So kann ein Unternehmen z. B. standortübergreifende Tunnel von seiner SD-WAN-Umgebung zu Secure Access-Regionen in London und Deutschland einrichten. Beide Tunnel bleiben aktiv und ermöglichen einen ausfallsicheren privaten Zugriff über mehrere Regionen hinweg. Außerdem wird die Kontinuität auch dann gewährleistet, wenn eine Region nicht mehr verfügbar ist. Dieses multiregionale Design stärkt die hohe Verfügbarkeit, verbessert die Fehlertoleranz und ist auf die Anforderungen der Enterprise-Klasse an Ausfallsicherheit ausgerichtet.

Für einen detaillierteren Zugriff setzt Cisco Secure Access das ZTNA-Modell (Zero Trust Network Access) durch. Anstatt Benutzern eine umfassende Netzwerkverbindung zu ermöglichen, erlaubt ZTNA den Zugriff nur auf bestimmte Anwendungen, basierend auf Identität, Gerätestatus und Kontext. Dieser Ansatz reduziert die Angriffsfläche erheblich und entspricht den Zero Trust-Prinzipien.

Der ZTNA-Zugriff wird durch eine Kombination aus Site-to-Site-Tunneln und Resource Connectors ermöglicht. Resource Connectors sind leichte virtuelle Appliances, die ausgehende Verbindungen mit sicherem Zugriff herstellen, d. h. private Ressourcen müssen nie direkt mit dem Internet verbunden werden.

Netzwerkdiagramm



Voraussetzungen

Anforderungen

- Sicherer Zugriff auf Informationen
- Cisco Catalyst SD-WAN Manager Version 20.18.2 und Cisco IOS XE Catalyst SD-WAN Version 17.18.2 oder höher

- Grundkenntnisse in Routing und Switching
- ECMP-Kenntnisse
- VPN-Kenntnisse
- Da diese Integration eine kontrollierte Verfügbarkeit aufweist, müssen Sie ein TAC-Ticket erstellen, um die Funktion in Cisco Secure Access zu aktivieren.

Verwendete Komponenten

- Tenant für sicheren Zugriff
- Catalyst SD-WAN Manager Version 20.18.2 und Cisco IOS XE Catalyst SD-WAN Version 17.18.2
- Catalyst SD-WAN-Manager

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Konfiguration des sicheren Zugriffs

API-Erstellung

Überprüfen Sie zur Erstellung der automatisierten Tunnel mit sicherem Zugriff die folgenden Schritte:

Navigieren Sie zum [Dashboard für sicheren Zugriff](#).

- Klicken Sie **Admin > API Keys**
- Klicken Sie **Add**
- Wählen Sie die nächsten Optionen aus:
 - Deployments / Network Tunnel Group: **Lese-/Schreibzugriff**
 - Deployments / Tunnels: **Lese-/Schreibzugriff**
 - Deployments / Regions: **Schreibgeschützt**
 - Deployments / Identities: **Lese-/Schreibzugriff**
 - Expiry Date: **Läuft nie ab**

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](#)

Anmerkung: Sie können optional bis zu 10 Netzwerke hinzufügen, über die dieser Schlüssel Authentifizierungen durchführen kann. Fügen Sie Netzwerke mithilfe einer kommagetrennten Liste mit öffentlichen IP-Adressen oder CIDRs hinzu.

- Klicken Sie [CREATE KEY](#) hier, um die Erstellung des API Key und Key Secret abzuschließen.

API Key

397766cdb29f43b08ddee3b1d8c04e45

Key Secret

bfce729cd3e243e281df7271acb12208



Vorsicht: Kopieren Sie sie, bevor Sie auf [ACCEPT AND CLOSE](#) klicken; Andernfalls müssen Sie sie erneut erstellen und die Dateien löschen, die nicht kopiert wurden.

Dann zum Abschluss klicken Sie [ACCEPT AND CLOSE](#).

SD-WAN-Konfiguration

API-Integration

Navigieren Sie zum Catalyst SD-WAN Manager:

- Klicken Sie auf **Administration** > Settings > Cloud Credentials
- Klicken Sie anschließend auf Cloud Provider Credentials, aktivieren Sie die API, und füllen Sie die Einstellungen für die Organisation aus.

- **Organization ID:** Sie finden diese Informationen unter der URL Ihres SSE Dashboards <https://dashboard.sse.cisco.com/org/xxxxx>
- **Api Key:** Kopieren Sie es aus dem Schritt [Secure Access Configuration](#).
- **Secret:** Kopieren Sie es aus dem Schritt [Secure Access Configuration](#).

Danach klicken Sie auf den **Save** Button.



Anmerkung: Bevor Sie mit den nächsten Schritten fortfahren, müssen Sie sicherstellen, dass der SD-WAN-Manager und die Catalyst SD-WAN-Edges über eine DNS-Auflösung und einen Internetzugang verfügen.

Um zu überprüfen, ob die DNS-Suche aktiviert ist, navigieren Sie zu:

- Klicken Sie auf **Konfiguration** > Konfigurationsgruppen.
- Klicken Sie auf das Profil Ihrer Edge-Geräte, und bearbeiten Sie das Systemprofil.

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		

- Bearbeiten Sie dann die globale Option, und stellen Sie sicher, dass die Option Domänenauflösung aktiviert ist.

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: 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 Ether Cl

HTTP Server: ☐	HTTPS Server: ☐
FTP Passive: ☐	Domain Lookup : ☒
ARP Proxy: ☐	RSH/RCP: ☐

Konfigurieren der Richtliniengruppe

Navigieren Sie zu Konfiguration > Richtliniengruppen:

- Auf 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
------	-------------	----------

- Konfigurieren Sie einen Namen, und klicken Sie auf **Create**

Secure Private Application Access

Name

SPA-AUTO

Description (optional)

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

Mit den nächsten Konfigurationen können Sie die Tunnel erstellen, nachdem Sie die Konfiguration in Ihren Catalyst SD-WAN-Edges bereitgestellt haben:

Configuration

Segment (VPN)

  Corporate_User

Cisco Secure Access Region

  Europe (Germany) 

- Configuration
 - Segment (VPN): Wählen Sie die VRF-Instanz aus, die die Anwendungen hostet, auf die über sicheren Zugriff zugegriffen werden soll.
 - Cisco Secure Access Region: Wählen Sie die Region aus, die dem SD-WAN-Hub oder der Zweigstelle, in der die Anwendungen gehostet werden, am nächsten liegt.

Definieren Sie anschließend die Tunnelkonfiguration. Tunnel, die zum primären Rechenzentrum für sicheren Zugriff erstellt wurden, sind aktiv, während Tunnel, die zum sekundären

Rechenzentrum für sicheren Zugriff erstellt wurden, als Backup dienen.

Klicken Sie unter Tunnel Configuration auf **+ Add Tunnel**:

Tunnel Configuration

[+ Add Tunnel](#)

Tunnel

BASIC SETTINGS

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

Advanced Settings

GENERAL

Shutdown false	TCP MSS 1350
IP MTU 1390	DPD Interval 10

- Tunnel
 - Interface Name: Tunnelnamen angeben, wird er automatisch aktualisiert, wenn ein neuer Tunnel hinzugefügt wird.
 - Tunnel Source Interface: Sie müssen diese Einstellung nicht ändern. Wenn das System als Auto gelassen wird, erstellt es automatisch eine Loopback-Schnittstelle mit einer /31-Maske.
 - Tunnel Route-Via Interface: Sie müssen diese Einstellung nicht ändern. Standardmäßig wird die erste NAT-basierte physische WAN-Schnittstelle am Edge-Router verwendet. Sie kann jedoch geändert werden, wenn eine bestimmte WAN-Schnittstelle erforderlich ist.

- Data Center: Wählen Sie entsprechend Primary oder Secondary aus. Wenn der primäre Tunnel bereits konfiguriert ist, wählen Sie Sekundär aus. In normalen Szenarien kann ein Tunnel als primär und ein anderer als sekundär konfiguriert werden.
- Advanced Settings
 - IP MTU: Verwenden 1390
 - TCP MSS: Verwenden 1350



Anmerkung: Wenn Sie mehrere Tunnel erstellen möchten, um ECMP zu aktivieren und die Tunnelkapazität zu erhöhen, können Sie bis zu 10 aktive/10 Backup-Tunnel pro Router konfigurieren. Dadurch werden bis zu 10×4 Gbit/s pro NTG erreicht.

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	✎ 🗑
ipsec110	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑
ipsec111	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑
ipsec112	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑
ipsec113	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑
ipsec114	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑
ipsec115	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑
ipsec116	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑
ipsec117	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑
ipsec118	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑
ipsec119	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑
ipsec120	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑

MAXIMUM OF 10 TUNNELS PER HUB

10 x 1 Primary

10 x 1 Secondary



Hinweis: Wenn Sie mehrere Tunnel pro Router bereitstellen, stellen Sie sicher, dass die Transportschnittstelle die aggregierte Bandbreite aller aktiven Tunnel zusammengekommen aufrechterhalten kann. Wenn beispielsweise zwei Tunnel jeweils bis zu 1 Gbit/s übertragen sollen, muss die Transportverbindung einen Durchsatz von mindestens 2 Gbit/s unterstützen.

Fahren Sie nach der Konfiguration der Tunnel mit der BGP-Konfiguration fort.

BGP Routing

BGP ASN ⓘ

65000

In Route Policy

SPA_Auto-In

Out Route Policy

SPA_Auto-Out

- **BGP Routing**

- **BGP ASN:** Geben Sie die AS-Nummer für den SD-WAN-Hub an. Das AS 64512 ist für sicheren Zugriff reserviert und kann nicht verwendet werden. Weitere Informationen zum BGP finden Sie unter [SD-WAN BGP](#).
- **In Route Policy:** Das System erstellt diese Richtlinie für eingehende Routen automatisch mit einer Anweisung, um Routing-Probleme zu vermeiden `deny all`. Sie muss manuell über einen [CLI Add-On Template](#) geändert werden, um die entsprechenden Routen zuzulassen/zu verweigern.
- **Out Route Policy:** Das System erstellt diese Richtlinie für ausgehende Routen mit einer `deny all` Anweisung, um Routing-Probleme zu vermeiden. Sie muss manuell über einen [CLI Add-On Template](#) bearbeitet werden, um die entsprechenden Routen zuzulassen/zu verweigern.



Warnung: Ab November 2025 verwenden alle neu erstellten Organisationen für sicheren Zugriff standardmäßig das öffentliche ASN 32644 für BGP-Peering in Netzwerk-Tunnelgruppen. Bestehende Unternehmen, die vor November 2025 gegründet wurden, nutzen weiterhin das private ASN 64512, das zuvor für BGP-Peers mit sicherem Zugriff reserviert war. Wenn die private AS-Nummer 64512 einem Gerät in Ihrem Netzwerk zugewiesen ist, kann keine Peer-Verbindung mit einer Netzwerk-Tunnelgruppe hergestellt werden, die für Peer (Secure Access) BGP AS 64512 konfiguriert ist.

Die nächste BGP und die nächste `route-map` Konfiguration wird automatisch für jeden BGP-Nachbarn erstellt, nachdem Sie `Deploy` die neue Richtlinie in Ihrem `Policy Group` geändert haben.

```
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

```

Klicken Sie anschließend auf **Save** , und fahren Sie mit der Richtlinienbereitstellung fort, um die Tunnel zu aktivieren.

- Klicken Sie auf **Configuration > Policy Groups**
- Wählen Sie unter **Policy > Secure Service Edge > Secure Private Application Access** aus, und klicken Sie auf das zuletzt für SPA erstellte Profil.
- Zum Abschließen **Deploy** klicken

Policy Groups

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

+ Add Policy Group Export Import

Q Search

Name	Description	Solution	Number of Policies	Number of Devices	Devices Up to Date	Source
SPA-Auto						
SIA_SIG	--	sdw				Import
Site-102	SIA Manual + SPA Manual	sdw				User

SPA-Auto Configuration:

Policy Group Name: SPA-Auto

Description (optional):

Application Priority: Select one

NGFW: Select one

DNS Security: Select one

Secure Service Edge: Secure Internet Access / Secure Internet Gateway

Secure Private Application Access: SPA-Auto

Device Solution: Type: sdwan

Deployment: Associated: 1 device

Buttons: Save, Deploy

So prüfen Sie inSecure Access:

- Auf **Connect > Network Connections**

TUNNELEINRICHTUNG

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 IOSX

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 Address: 193.254.0.8, 193.254.0.5, 2404-a44-b723-667-0000/120

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-1083346169-661683007-aaa.cisco.com

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

IP Address: 193.254.0.8, 193.254.0.5, 2404-a44-b723-667-0000/120

Secondary Hub

Hub Up

10 Active Tunnels

Tunnel Group ID: eu-central-1083346169-661683009-aaa.cisco.com

Data Center: ssa-eu-1-1-2

IP Address: 193.254.0.9, 193.254.0.6, 2404-a44-b723-667-0000/120

Konfigurieren von Routing

Navigieren Sie zu **Configure > Configuration Groups**

- Klicken Sie auf Ihre **Configuration Group** und erstellen/bearbeiten Sie Ihre 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
SPA-AUTO	Single Router	System Profile SPA-AUTO Policy Profile (optional) Default_Policy_Object_Profile CLI Add-on Profile (optional) SPA_Auto_Route-maps	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

Um den Austausch von BGP-Routen zu ermöglichen, verwenden Sie die zuvor konfigurierten **In Route Policy** und **Out Route Policy**. Hier finden Sie ein einfaches Beispiel für die CLI Add-On Routenkonfiguration. Diese Vorlage bietet einen Ausgangspunkt und muss bei Bedarf angepasst werden:

```
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



Warnung: Eine sorgfältige Planung ist erforderlich, wenn die Netzwerke definiert werden, die über BGP-Routing-Maps ein- und ausgehen dürfen. Das Zulassen aller Routen, wie im obigen Beispiel gezeigt, kann zu unbeabsichtigtem Routing-Verhalten führen. Geben Sie für eine optimale Bereitstellung explizit nur die erforderlichen Netzwerke in Ihren Routing-Karten an, um kontrollierte und vorhersagbare Routing-Ergebnisse zu gewährleisten.

Jetzt können Sie Deploy the changes

Um zu überprüfen, ob BGP-Routen in empfangenSecure Accesswerden, gehen Sie wie folgt vor:

- Klicken Sie auf Connect > Network Connections > Network Tunnel Groups , und select wählen Sie NTG aus.

ROUTING-EINRICHTUNG

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: 'Primary Hub' and 'Secondary Hub', both showing '10 Active Tunnels'. Below these is a 'Network Tunnels' table with columns: Tunnels, Peer ID, Peer Device IP Address, Data Center Name, and Data. The table lists seven tunnels, with 'Primary 1' selected. A detailed view for 'Primary 1 (131130)' is shown on the right, including IKE configuration (State: ESTABLISHED, Age: 141464 sec, PRF Algorithm: HMAC-SHA2-256), BGP configuration (Routing Type: BGP, Client Routes: 172.16.104.0/24), and Cloud Routes. A 'Download Routing Table' link is also present.

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



Anmerkung: In diesem Beispiel wird das Subnetz 172.16.104.0/24 für Unternehmensbenutzer über BGP für sicheren Zugriff angekündigt. Dies ermöglicht ein angemessenes Routing zwischen dem Catalyst SD-WAN und der SSE-Umgebung.

Dieselbe Richtlinie kann auf beide WAN-Edges in den Catalyst SD-WAN-Hubs angewendet werden. Das Ergebnis sind 20 aktive und 20 Standby-Tunnel. Die Gesamtzahl der Tunnel hängt davon ab, wie viele für jeden Edge konfiguriert sind. Jeder mit beiden Secure Access-Hubs (Hub 1 und Hub 2) verbundene Router bildet ein ECMP-Paar für alle gängigen Tunnel.

Wenn beispielsweise der Catalyst SD-WAN-Edge 1 zehn Tunnel und der Catalyst SD-WAN-Edge 2 zehn Tunnel hat, bildet Secure Access den ECMP für die 20 aktiven Tunnel. Dasselbe Verhalten gilt für den sekundären 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 Catalyst SDWAN	Connected	Europe (Germany)	sse-euc-1-1-1	20	sse-euc-1-1-0	20

Überprüfung

um zu überprüfen, ob der Datenverkehr über Cisco Secure Access läuft, navigieren Sie zu Eventsoder Activity Search oder Network-Wide Path Insightsund filtern Sie nach Ihrer Tunnellidentität:

Sicherer Zugriff - Aktivitätssuche

Navigieren Sie zu Monitor>Activity Search :

Activity Search

FILTERS

Q Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

IP ADDRESS172.16.104.11

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

Restore to

Search filters

Response

Allowed

Blocked

Warn Page Behavior

Warned

Accessed After Warn

4 Total

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

Page: 1

Resu

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

Sicherer Zugriff - Veranstaltungen

Navigieren Sie zu Monitor>Events:

Events

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

[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 DNS x Reset all

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

Source

AD Users: Alejandro Ruiz Sanchez...

Source IP:

Location:

Browser: Firefox 147.0

Operating system: Mac OS X 10.15

Connection

Type: ZTA

Endpoint Posture:

Status: Compliant

Posture profile: System provided (Browse...)

Security Controls

ZTA Clientless

Action: Allowed

Ingress region:

Tunnel type: HTTP2

Resource connector group:

Egress IP:

Datacenter:

Firewall (3)

Destination

FQDN: PC-site-104

Resource/Application Name: PC-site-104

Destination IP: 172.16.104.11

Destination Port: 3389

Application Category: Private Resource

Application Protocol: RDP-TCP

Rows per page 30 1-1 of 1 < 1 >



Anmerkung: Vergewissern Sie sich, dass Ihre Standardrichtlinie mit aktivierter Protokollierung standardmäßig deaktiviert ist.

Catalyst SD-WAN Manager - Netzwerkweite Pfadeinblicke

Navigieren Sie zum Catalyst SD-WAN Manager:

- Auf Tools> Network-Wide Path Insights
- Klicken Sie 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

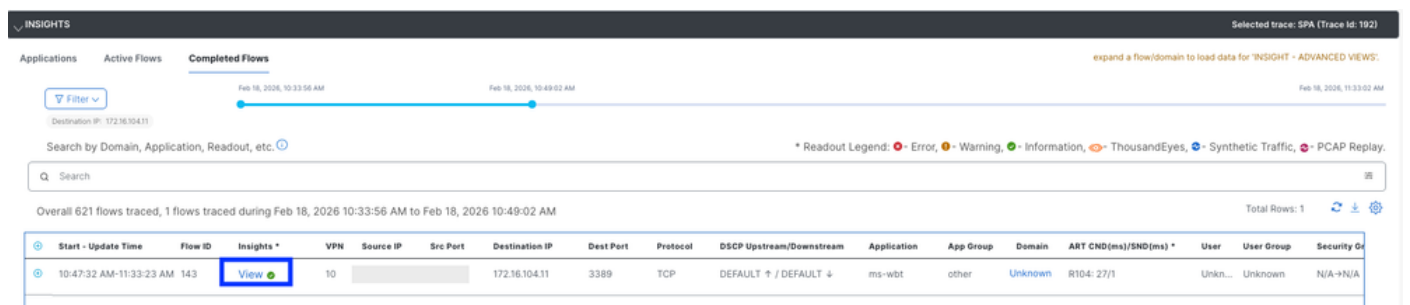
Cancel Start

- Trace Name: (Optional) Trace-Name angeben

- Site: Standort auswählen, an dem sich die private Ressource befindet
- VPN: Wählen Sie die VPN-ID, in der sich die private Ressource befindet.
- Source/Destination Address: (Optional) Geben Sie die IP-Adresse ein, oder lassen Sie sie leer, um den gesamten Datenverkehr zu erfassen, der basierend auf site und VPN ausgewählt

Ablaufverfolgung starten

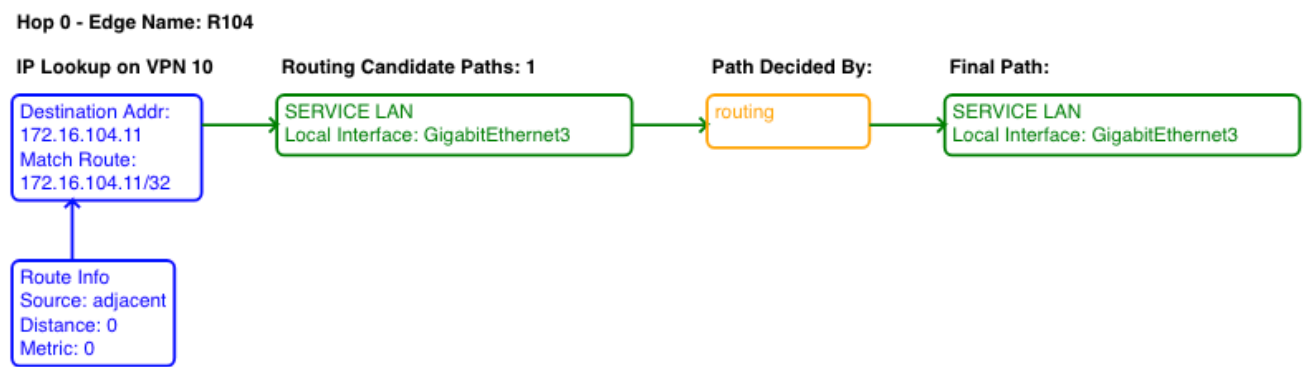
Suchen Sie den Datenverkehrsfluss, und klicken Sie in der Spalte Insights (Einblicke) auf View (Anzeigen).



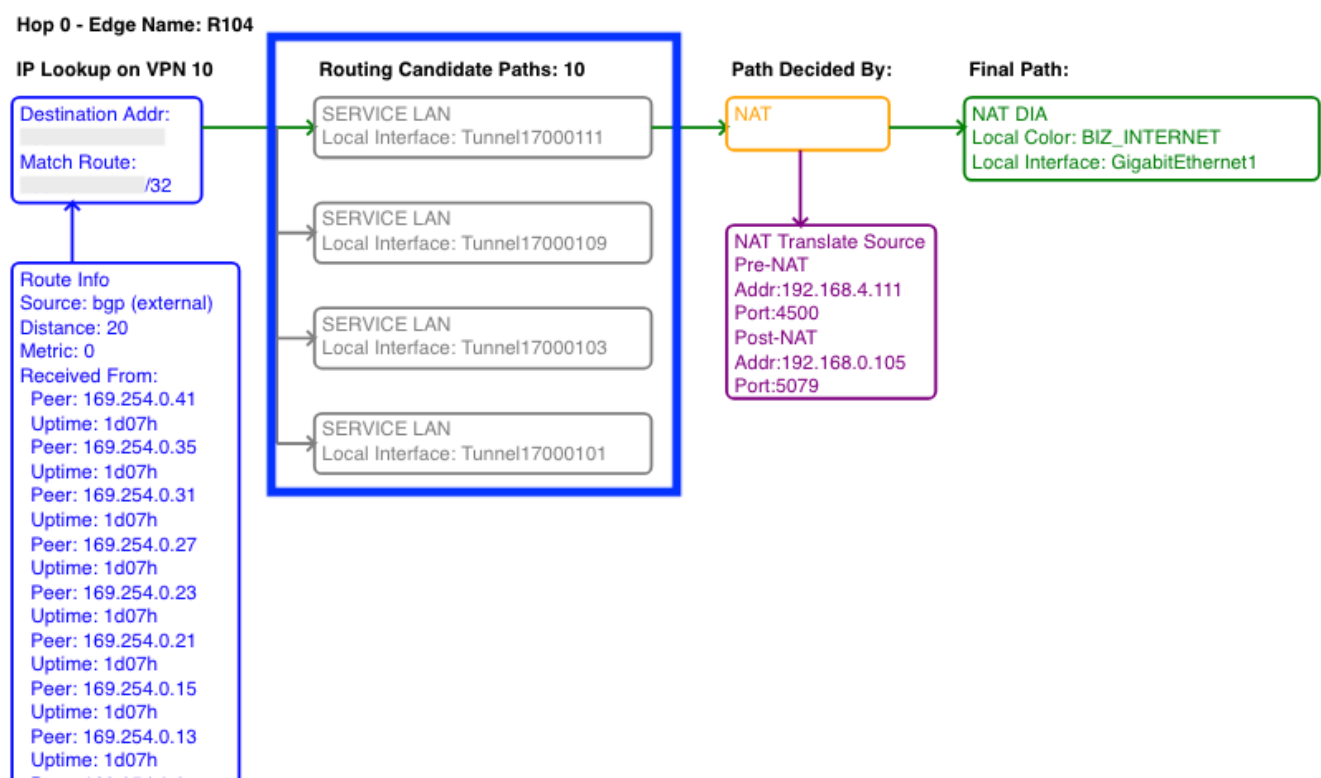
In der Spalte Routing Insights (Routing-Informationen) werden die möglichen Pfade und die IPsec-Tunnel für den sicheren Zugriff angezeigt.

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

Upstream (From 15645 to 172.16.104.11:3389)



Downstream (From 172.16.104.11:3389 to 15645)



Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [Cisco Secure Access-Hilfecenter](#)
- [Cisco SASE Designleitfaden](#)
- [Konfigurieren eines sicheren Zugriffs mithilfe von automatisierten SD-WAN-Tunneln für einen sicheren Internetzugriff](#)

- [Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Version 17.x](#)
- [Cisco SASE-Lösung: Cisco Catalyst SD-WAN integriert mit Cisco Secure Access - Informationen auf einen Blick](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.