

Konfigurieren eines sicheren Zugriffs mithilfe von automatisierten SD-WAN-Tunneln für einen sicheren Internetzugriff

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfiguration des sicheren Zugriffs](#)

[API-Erstellung](#)

[SD-WAN-Konfiguration](#)

[API-Integration](#)

[Konfigurieren der Richtliniengruppe](#)

[Erstellen Sie Ihren benutzerdefinierten Bypass-FQDN oder APP im SD-WAN \(OPTIONAL\).](#)

[Weiterleiten des Datenverkehrs](#)

[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 SD-WAN-Tunneln für sicheren Internetzugriff beschrieben.



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

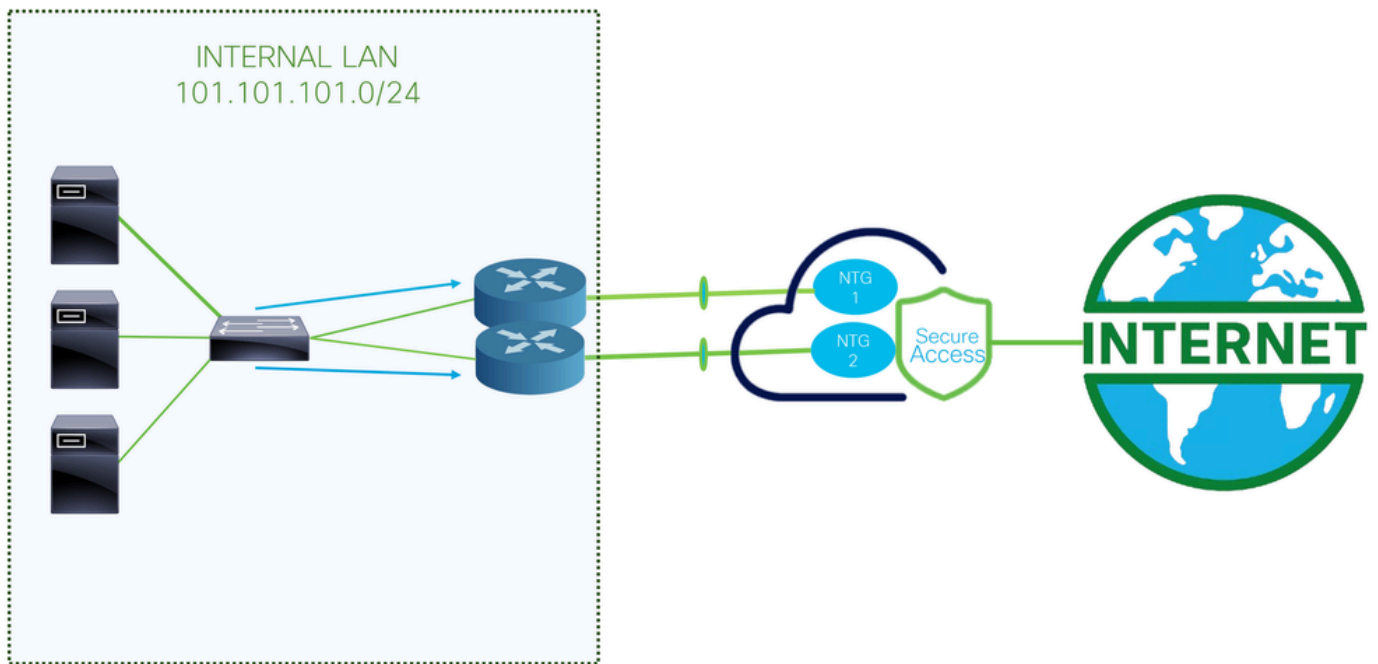
Hintergrundinformationen

Mit der zunehmenden Einführung Cloud-basierter Anwendungen und der Unterstützung von Mitarbeitern an unterschiedlichen Standorten ist eine Weiterentwicklung der Netzwerkarchitektur erforderlich, um einen sicheren, zuverlässigen und skalierbaren Zugriff auf Ressourcen zu ermöglichen. Secure Access Service Edge (SASE) ist ein Framework, das Netzwerk und Sicherheit in einem einzigen Cloud-basierten Service zusammenführt und SD-WAN-Funktionen mit erweiterten Sicherheitsfunktionen wie Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), DNS-Layer-Sicherheit, Zero Trust Network Access (ZTNA) oder integriertem VPN für sicheren Remote-Zugriff kombiniert.

Durch die Integration von Cisco Secure Access in das SD-WAN über automatisierte Tunnel wird ein sicheres und effizientes Routing des Internetdatenverkehrs ermöglicht. SD-WAN bietet eine intelligente Pfadauswahl und optimierte Konnektivität über verteilte Standorte hinweg. Cisco Secure Access stellt sicher, dass der gesamte Datenverkehr vor dem Erreichen des Internets gemäß den Sicherheitsrichtlinien des Unternehmens geprüft und geschützt wird.

Durch die Automatisierung der Tunnelkonfiguration zwischen SD-WAN-Geräten und sicherem Zugriff können Organisationen die Bereitstellung vereinfachen, die Skalierbarkeit verbessern und eine konsistente Durchsetzung von Sicherheitsrichtlinien für Benutzer gewährleisten - unabhängig von ihrem Standort. Diese Integration ist eine Schlüsselkomponente einer modernen SASE-Architektur und ermöglicht einen sicheren Internetzugang für Zweigstellen, Außenstellen und mobile Benutzer.

Netzwerkdiagramm



Dies ist die für dieses Konfigurationsbeispiel verwendete Architektur. Wie Sie sehen, gibt es zwei Edge-Router:

Wenn Sie die Richtlinien auf zwei verschiedenen Geräten bereitstellen, wird für jeden Router ein NTG konfiguriert, und NAT wird für den sicheren Zugriff aktiviert. Dadurch können beide Router Datenverkehr von derselben Quelle durch die Tunnel senden. Dies ist in der Regel nicht zulässig. Wenn jedoch die NAT-Option für diese Tunnel aktiviert ist, können zwei Edge-Router Datenverkehr senden, der von derselben Quelladresse stammt.

Voraussetzungen

Anforderungen

- Sicherer Zugriff auf Informationen
- Cisco Catalyst SD-WAN Manager Version 20.15.1 und Cisco IOS XE Catalyst SD-WAN Version 17.15.1 oder höher
- Grundkenntnisse in Routing und Switching
- ECMP-Kenntnisse
- VPN-Kenntnisse

Verwendete Komponenten

- Tenant für sicheren Zugriff
- Catalyst SD-WAN Manager Version 20.18.1 und Cisco IOS XE Catalyst SD-WAN Version 17.18.1
- 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.

<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



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 397766cdb29f43b08dde3b1d8c04e45 	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 **Cisco S** 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 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](#)

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

The image shows two parts of a configuration interface. On the left is the 'SIA_Basic' profile configuration page, which includes a search bar and a 'Profile Features' section with dropdown menus for AAA, BFD, Multi-Region Fabric, Banner, Global, and NTP. An orange box highlights the 'Global' dropdown menu. An orange arrow points from this box to the 'Global' configuration page on the right. The 'Global' page has a 'Name' field set to 'Global', a 'Description' field, and a 'Global Description' field. Below these are several service status indicators: Services (checked), NAT64 (checked), BGP (checked), Authentication (checked), and SSH Version (checked). The 'Services' indicator is highlighted with an orange box. An orange arrow points from this box to the 'Domain Lookup' option in the 'Services' section, which is also highlighted with an orange box. The 'Domain Lookup' option is a toggle switch that is currently turned on.

Konfigurieren der Richtliniengruppe

Navigieren Sie zu Konfiguration > Richtliniengruppen:

- Klicken Sie auf **Secure Internet Gateway / Secure Service Edge** > *Add Secure Internet Access*

The image shows the 'Policy Group' configuration page. At the top, there are tabs for 'Policy Group 4', 'Application Priority & SLA 3', 'NGFW 0', and 'Secure Internet Gateway / Secure Service Edge 3'. The 'Secure Internet Gateway / Secure Service Edge 3' tab is selected and highlighted with a blue box. Below the tabs, there is a search bar labeled 'Search Table'. Underneath the search bar, there are three buttons: 'Add Secure Internet Gateway (SIG)', 'Add Secure Internet Access', and 'Add Secure Private Application Access'. The 'Add Secure Internet Access' button is highlighted with a blue box. A blue arrow points from the 'Secure Internet Gateway / Secure Service Edge 3' tab to this button.



Anmerkung: In Versionen unter 20.18 heißt diese Option Add Secure Service Edge (SSE).

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

Secure Internet Access

Name

SIA

Solution

sdwan

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:

SSE Provider

☒ Cisco SSE ☐ Zscaler

Context Sharing

☒ VPN ☒ SGT

Tracker

Source IP address

{{ Monitoring }}

- SSE Provider: **SSE**
- Context Sharing: Auswahl von VPN oder/und SGT je nach Ihren Anforderungen
- Tracker
 - **Source IP Address:** Wählen Sie Device Specific (Gerätespezifisch) (Diese Option ermöglicht Ihnen, sie für jedes Gerät zu ändern und den Anwendungsfall dafür in der Bereitstellungsphase zu identifizieren).

Unter dem **Configuration** Schritt richten Sie die Tunnel ein:

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

Tunnel Route Via: <SYSTEM DEFAULT>

Tracker: DefaultTracker

Primary: ☒ Secondary: ☐

Data Center

Max one tunnel per hub

ECMP Scenario with HA

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface*: Loopback1

Tunnel Route Via: GigabitEthernet1

Tracker: DefaultTracker

Primary: ☒ Secondary: ☐

Data Center

Max 8 Tunnels per Hub 8GB X 1

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

- **Single Hub HA Scenario:** In diesem Szenario können Sie eine hohe Verfügbarkeit konfigurieren, indem Sie ein NTG als aktives und ein anderes als passives Gerät mit einem maximalen Durchsatz von 1 Gbit/s pro NTG verwenden.
- **ECMP Scenario with HA:** In diesem Szenario können Sie bis zu 8 Tunnel pro Hub konfigurieren, sodass insgesamt bis zu 16 Tunnel pro NTG unterstützt werden. Diese Konfiguration ermöglicht einen höheren Durchsatz in den Tunneln.



Anmerkung: Wenn Ihre Netzwerkschnittstellen einen Durchsatz von mehr als 1 Gbit/s aufweisen und Sie Skalierbarkeit benötigen, müssen Sie Loopback-Schnittstellen verwenden. Andernfalls können Sie Standardschnittstellen auf Ihrem Gerät verwenden. Dadurch wird ECMP auf der Seite für den sicheren Zugriff aktiviert.



Warnung: Wenn Sie Loopback-Schnittstellen für ein ECMP-Szenario konfigurieren möchten, müssen Sie zunächst die Loopback-Schnittstellen in Configuration Groups > Transport & Management Profile unter der Richtlinie einrichten, die Sie in Ihrem Router verwenden.

- Klicken Sie **Add Tunnel**

Edit Tunnel

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

- Interface Name: ipsec1, ipsec2, ipsec3 usw.
- Tunnel Source Interface: Wählen Sie Loopback-Schnittstellen oder eine bestimmte Schnittstelle aus, über die Sie den Tunnel einrichten möchten.
- Tunnel Route Via: Wenn Sie Loopback auswählen, müssen Sie die physische Schnittstelle auswählen, von der Sie den Datenverkehr routen möchten. Wenn Sie Loopback nicht auswählen, erscheint diese Option ausgegraut und verwendet die erste NAT-aktivierte Schnittstelle, die vom System gefunden wird. Wenn mehrere Schnittstellen vorhanden sind, müssen Sie die gewünschte WAN-Schnittstelle auswählen.
- Data Center: Das bedeutet, mit welchem Hub in Secure Access Sie die Verbindung herstellen

Im nächsten Teil der Tunnelkonfiguration konfigurieren Sie die Tunnel mithilfe der von Cisco bereitgestellten Best Practices.

Advanced Options

General

Shutdown

☐ ☐

Track this interface

☐ ☐

TCP MSS

IP MTU

DPD Interval

DPD Retries

IKE Diffie-Hellman Group

20

- TCP MSS: 1350
- IP MTU: 1390
- IKE Diffie-Hellman Group: 20

Danach müssen Sie den sekundären Tunnel konfigurieren, der auf das sekundäre Rechenzentrum verweist.

SINGLE HUB HA-SZENARIO

Configuration

[+ Add Tunnel](#)

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

Dies ist das Endergebnis, wenn Sie das normale Bereitstellungsszenario verwenden.

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

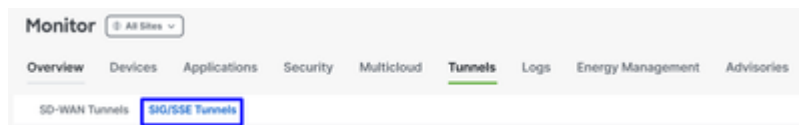
Anschließend müssen Sie die hohe Verfügbarkeit in der Richtlinie für ein sicheres Internet

konfigurieren.

High Availability

[+ Add Interface Pair](#)

Klicken Sie auf Schnittstellenpaar hinzufügen:



PRIMARY
SECONDARY

Edit Interface Pair

×

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

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

In diesem Schritt müssen Sie den primären und sekundären Tunnel für jedes einzurichtende Tunnelpaar konfigurieren. Das bedeutet, dass jeder Tunnel über ein eigenes Backup verfügt. Denken Sie daran, dass diese Tunnel genau zu diesem Zweck als primäre und sekundäre Tunnels erstellt wurden.

"Active interface" bezieht sich auf den primären Tunnel, "Backup interface" bezieht sich auf den sekundären Tunnel:

- Active Interface: **Primary**
- Backup Interface: **Sekundär**



Warnung: Wenn Sie diesen Schritt überspringen, werden die Tunnel nicht geöffnet, und es wird keine Verbindung zwischen den Routern und Secure Access hergestellt.

Nachdem die hohe Verfügbarkeit für die Tunnel konfiguriert wurde, wird die Einrichtung angezeigt, wie in der Abbildung unten gezeigt. Im Beispiel der für diesen Leitfaden verwendeten Übung

werden fünf Tunnel in der Hochverfügbarkeit dargestellt. Die Anzahl der Tunnel kann nach Bedarf angepasst werden.

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](#)



Anmerkung: Maximal 8 Tunnelpaare (16 Tunnel: 8 primäre und 8 sekundäre Ports) können in SD-WAN Catalyst vManage konfiguriert werden. Cisco Secure Access unterstützt bis zu 10 Tunnelpaare.

- Klicken Sie auf [Save](#)

Nach diesem Zeitpunkt werden die Tunnel bei korrekter Konfiguration im SD-WAN-Manager und in Secure Access als UP angezeigt.

Um die Konfiguration im SD-WAN zu überprüfen, gehen Sie wie folgt vor:

- Klicken Sie auf [Monitor](#) > [Tunnels](#)
- Klicken Sie dann auf [SIG/SSE Tunnels](#)

Monitor [All Sites](#)

[Overview](#) [Devices](#) [Applications](#) [Security](#) [Multicloud](#) [Tunnels](#) [Logs](#) [Energy Management](#) [Advisories](#)

[SD-WAN Tunnels](#) [SIG/SSE Tunnels](#)

Außerdem können Sie sehen, ob die Tunnel für Cisco Secure Access verfügbar sind oder nicht.

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_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	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_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

Um in zu überprüfen, gehen Sie wie folgt vorSecure Access:

- Klicken Sie auf **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](#)

<input type="text" value="5b28-4db0-b62e-9b589b5c687d"/>	<div>Region</div>	<div>Status</div>	1 Tunnel Group			<div>+ Add</div>
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	<div>Connected</div>	Europe (Germany)	sse-euc-1-1-1	8	sse-euc-1-1-0	8

Klicken Sie in einer Detailansicht auf den Namen des Tunnels:

8

Hub Up

Active Tunnels

Tunnel Group ID

C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d83356769-68f8f070-see-aws.com

Data Center

sse-euc-1-1-1

IP Address

3.120.45.23 3053-5004-80-20c-1101

8

Hub Up

Active Tunnels

Tunnel Group ID

C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d83356769-68f8f070-see-aws.com

Data Center

sse-euc-1-1-0

IP Address

18.106.145.74 2903-5004-80-20c-1101

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

Danach können Sie mit dem Schritt fortfahren, Create your Custom Bypass FQDN or APP in SD-WAN

Erstellen Sie Ihren benutzerdefinierten Bypass-FQDN oder APP im SD-WAN (OPTIONAL).

Es gibt spezielle Anwendungsfälle, bei denen Sie Application Bypass und FQDN oder IP erstellen müssen, die Sie auf Ihre Routing-Richtlinien anwenden können:

Navigieren Sie zum SD-WAN Manager-Portal:

- Klicken Sie auf Configuration > Application Catalog > Applications

Application Catalog

SD-AVC Enabled

Configure Cloud Connection

Overview

Applications 1553

Application Source Settings

Cloud Sourced Applications

Discovered Application 0

Application Lists

Conflicts

Applications 1553

Select Application Attributes

Choose Filter

Custom Application

Export

Search Table

0 selected

Create Application List

Define Probe Endpoint

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

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



Tipp: Wenn eine ältere Version als 20.15 ausgeführt wird, können benutzerdefinierte Anwendungen unter Richtlinienlisten erstellt werden.



Anmerkung: Um auf den Anwendungskatalog zugreifen zu können, müssen Sie SD-AVC aktivieren.

- Klicken Sie Custom Application

Applications 1553

Select Application Attributes

Choose Filter

Custom Application

Export

Search Table

0 selected

Create Application List

Define Probe Endpoint

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

Zu diesem Zeitpunkt wird mithilfe des FQDN des Secure Client - Umbrella Module SWG ein einfacher Ausschluss konfiguriert:

ProxySecureAccess

Custom Application ×

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

ProxySecureAccess
Application Name: ProxySecureAccess-Custom

Server Names ⓘ → FQDN

swg-url-proxy-https-sse.sigproxy.qq.opendi

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: Verwenden Sie den FQDN, den Sie umgehen möchten (in diesem Beispiel sind die FQDN der SWG konfiguriert).
 - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
 - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Klicken Sie **Save**



Anmerkung: Ändern Sie ORGID mit Ihrer SSE-Organisationsnummer.

Als Nächstes wird ein grundlegender Ausschluss geschaffen; in diesem Fall die Umbrella DNS-Server:

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

Nun können Sie mit den Konfigurationen der Routing-Richtlinien fortfahren.

Weiterleiten des Datenverkehrs

In diesem Schritt müssen Sie den Internet-Datenverkehr durch die Tunnel leiten, um ihn über Cisco Secure Access zu schützen. In diesem Fall verwenden Sie eine flexible Routing-Richtlinie, die es uns ermöglicht, bestimmten Datenverkehr zu umgehen. Auf diese Weise wird verhindert, dass unerwünschter Datenverkehr über Secure Access gesendet wird, oder es werden potenzielle "Bad Practices" vermieden.

Definieren Sie zunächst die beiden Routing-Methoden, die verwendet werden können:

- **Configuration > Configuration Groups > Service Profile > Service Route:** Diese Methode ermöglicht das Routing zu Secure Access, bietet jedoch keine Flexibilität.
- **Configuration > Policy Groups > Application Priority & SLA:** Diese Methode bietet verschiedene Routing-Optionen innerhalb des SD-WAN und, was am wichtigsten ist, ermöglicht Ihnen, bestimmten Datenverkehr zu umgehen, damit er nicht über sicheren Zugriff gesendet wird.

Um Flexibilität zu gewährleisten und Best Practices einzuhalten, wird diese Konfiguration wie folgt verwendet **Application Priority & SLA**:

- Klicken Sie auf **Configuration > Policy Groups > Application Priority & SLA**
- Klicken Sie dann auf **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

- Konfigurieren Sie einen Richtliniennamen, und klicken Sie auf [Create](#)

Application Priority & SLA Policy

Policy Name

SIA-ROUTE

Description (optional)

Cancel


Create

- **Enable** Advanced Layout
- Klicken Sie [+ 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

SSE

VPN(s)

Corporate_Users

Direction

From Service

Default action

☒ Accept ☐ Drop

Cancel

Add

- Policy Name: Name, der dies an den Zweck dieser Datenverkehrsrichtlinienliste anpasst
- VPN(s): Wählen Sie das Service-VPN des Benutzers aus, von dem aus Sie den Datenverkehr weiterleiten.
- Direction: Vom Dienst
- Default action: Akzeptieren

Anschließend können Sie mit der Erstellung der Datenverkehrsrichtlinie beginnen:

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

VPN: Corporate_Users Direction: From Service Default Action: Accept

Q Search rule by name or order

	NAME	MATCH	ACTION	
1	LocalNetwork	Destination Ip · 172.16.200.0/24 Source Ip · 101.101.101.0/24	Base action · accept	⋮
2	BypassSSEP	App List · SecureAccessProxy	Base action · accept	⋮
3	UmbrellaDN	App List · UmbrellaDNS	Base action · accept	⋮
4	SIA AUTO F	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): Quelle: 101.101.101.0/24, Ziel: 172.16.200.0/24. Diese Route verhindert, dass netzwerkinterner Datenverkehr an Cisco Secure Access gesendet wird. In der Regel ist dies beim Kunden nicht der Fall, da das interne Routing in SD-WAN-

Bereitstellungen in der Regel vom Distribution Router übernommen wird. Durch diese Konfiguration wird sichergestellt, dass der interne Datenverkehr zwischen diesen Subnetzen nicht an den sicheren Zugriff weitergeleitet wird, je nachdem, ob Ihr Szenario dies erfordert (optional, abhängig von der Netzwerkumgebung).

2. **BypassSSEProxy (Optional):** Diese Richtlinie verhindert, dass interne Computer mit aktiviertem Cisco Umbrella-Modul im Secure Client und aktivierter SWG Proxy-Datenverkehr an die Cloud zurücksenden. Das erneute Routing von Proxy-Datenverkehr in die Cloud wird nicht als Best Practice erachtet.
3. **UmbrellaDNS (Best Practice):** Diese Richtlinie verhindert, dass DNS-Abfragen, die für das Internet bestimmt sind, durch den Tunnel gesendet werden. Das Senden von DNS-Abfragen an Umbrella Resolver (208.67.222.222, 208.67.220.220) über den Tunnel wird nicht empfohlen.
4. **SIA AUTO FULL TRAFFIC:** Diese Richtlinie leitet den gesamten Datenverkehr von der Quelle 101.101.101.0/24 über die zuvor von Ihnen erstellten SSE-Tunnel an das Internet weiter. So wird sichergestellt, dass dieser Datenverkehr in der Cloud geschützt ist.

Überprüfung

um zu überprüfen, ob der Datenverkehr bereits durch Cisco Secure Access geleitet wird, navigieren Sie zu **Events** oder **Activity Search** oder **Network-Wide Path Insights** und filtern Sie nach Ihrer Tunnellidentität:

Sicherer Zugriff - Aktivitätssuche

Navigieren Sie zu **Monitor > Activity Search**:

The screenshot displays the 'Activity Search' interface. At the top, there's a search bar with the text 'Search by domain, identity, or URL' and a 'CLEAR' button. Below the search bar, there's a filter section with 'IDENTITY' selected, showing a specific identity: 'C8K-PAYG-Of3-d4e8-4ea8-bc90-ca09e47f22f6'. The main table shows a list of events with columns: Request, Source, Rule Identity, Destination, Destination IP, Destination Port, and Destination Country. The table is filtered to show 1,617 total results. On the right side, there's a 'Event Details' panel showing the details of the selected event, including the Action (Allowed), Time (Dec 28, 2025 6:14 AM), Rule Name (For all Internet access (2100958)), Source (VPN-10 (VPN-10)), Source IP (101.101.101.20), Destination (https://youtube.com), and Security Group Tag (SGT).

Sicherer Zugriff - Veranstaltungen

Navigieren Sie zu **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: -



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:

- Klicken Sie auf **Tools** > **Network-Wide Path Insights**
- Klicken Sie **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: Wählen Sie den Standort, von dem aus Ihr Datenverkehr ausgeht
- VPN: Wählen Sie die VPN-ID Ihres Subnetzes aus, von dem aus der Datenverkehr ausgeht.
- Source: Setzen Sie die IP-Adresse ein, oder lassen Sie sie leer, um den gesamten Datenverkehr zu filtern, der durch die gefiltert site und VPN ausgewählt wurde.

In Insights sehen Sie dann den Datenverkehr, der durch die Tunnel fließt, und die Art des Datenverkehrs, der zu Secure Access gelangt:

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

Total Rows: 10

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

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

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

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

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [Cisco Secure Access-Hilfecenter](#)
- [Cisco SASE Designleitfaden](#)
- [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.