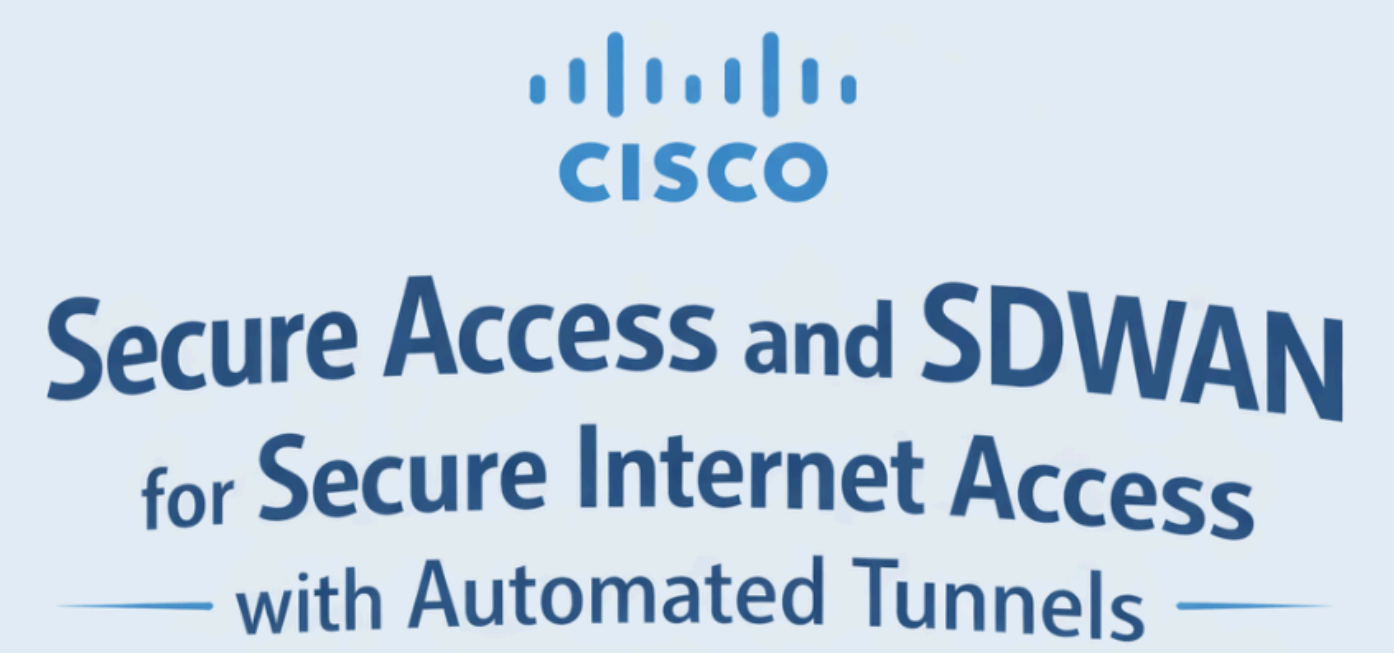
Konfigurieren eines sicheren Zugriffs mithilfe von automatisierten SD-WAN-Tunneln für einen sicheren Internetzugriff

Inhalt

Einleitung

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



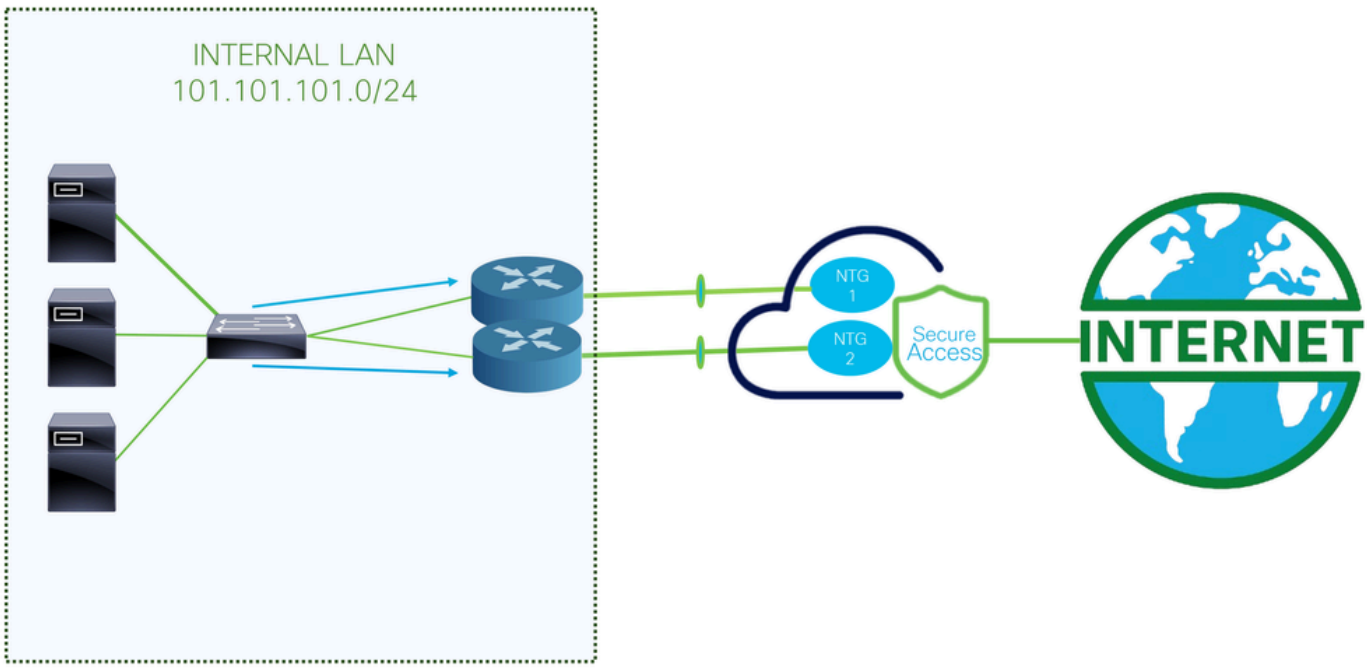
Hintergrundinformationen

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

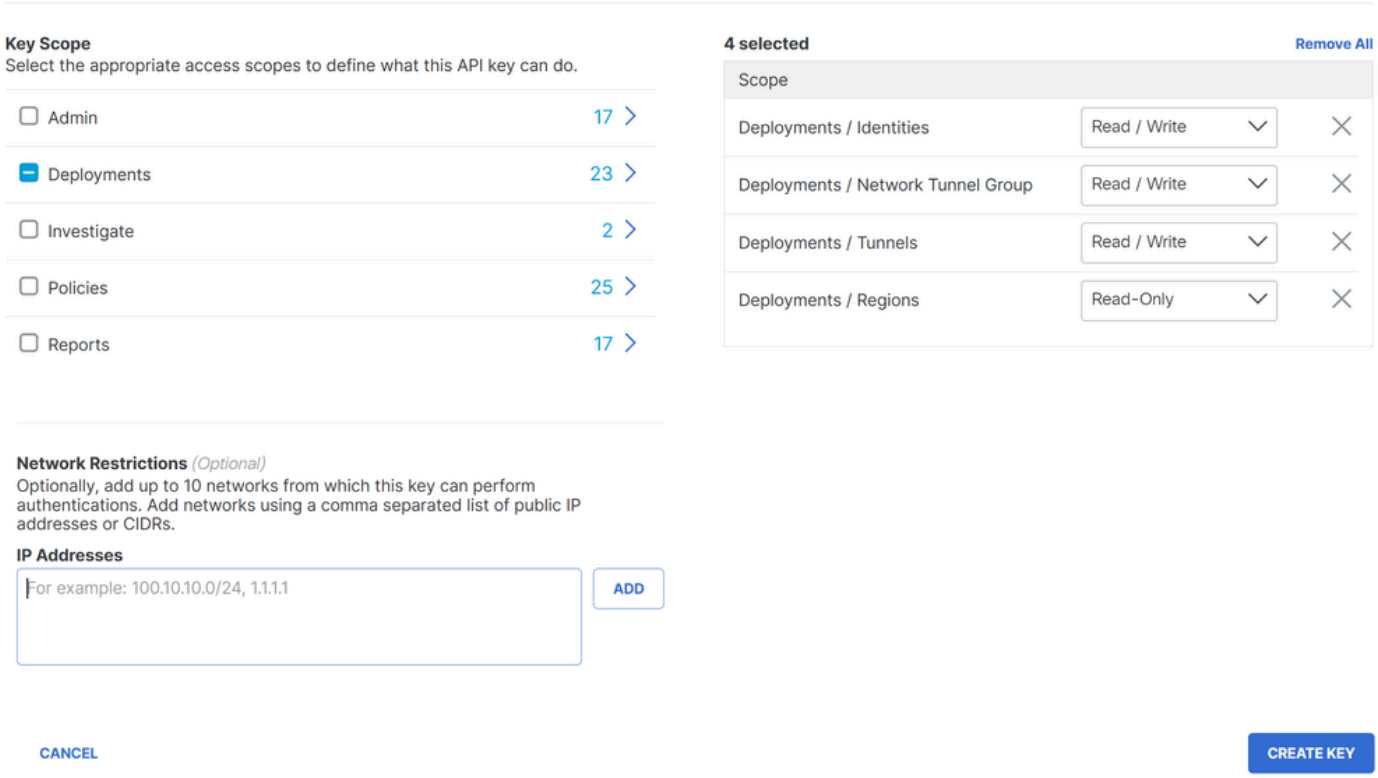
Konfiguration des sicheren Zugriffs

API-Erstellung

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

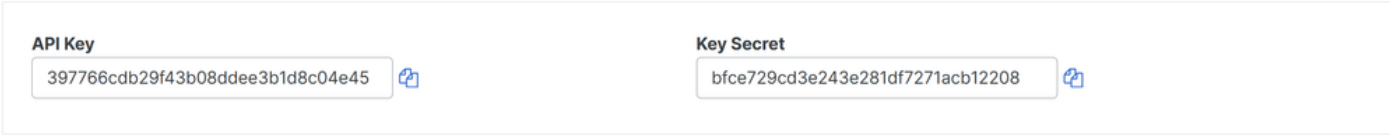
Navigieren Sie zum Dashboard für sicheren Zugriff.

- 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



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 Secretabzuschließen.



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

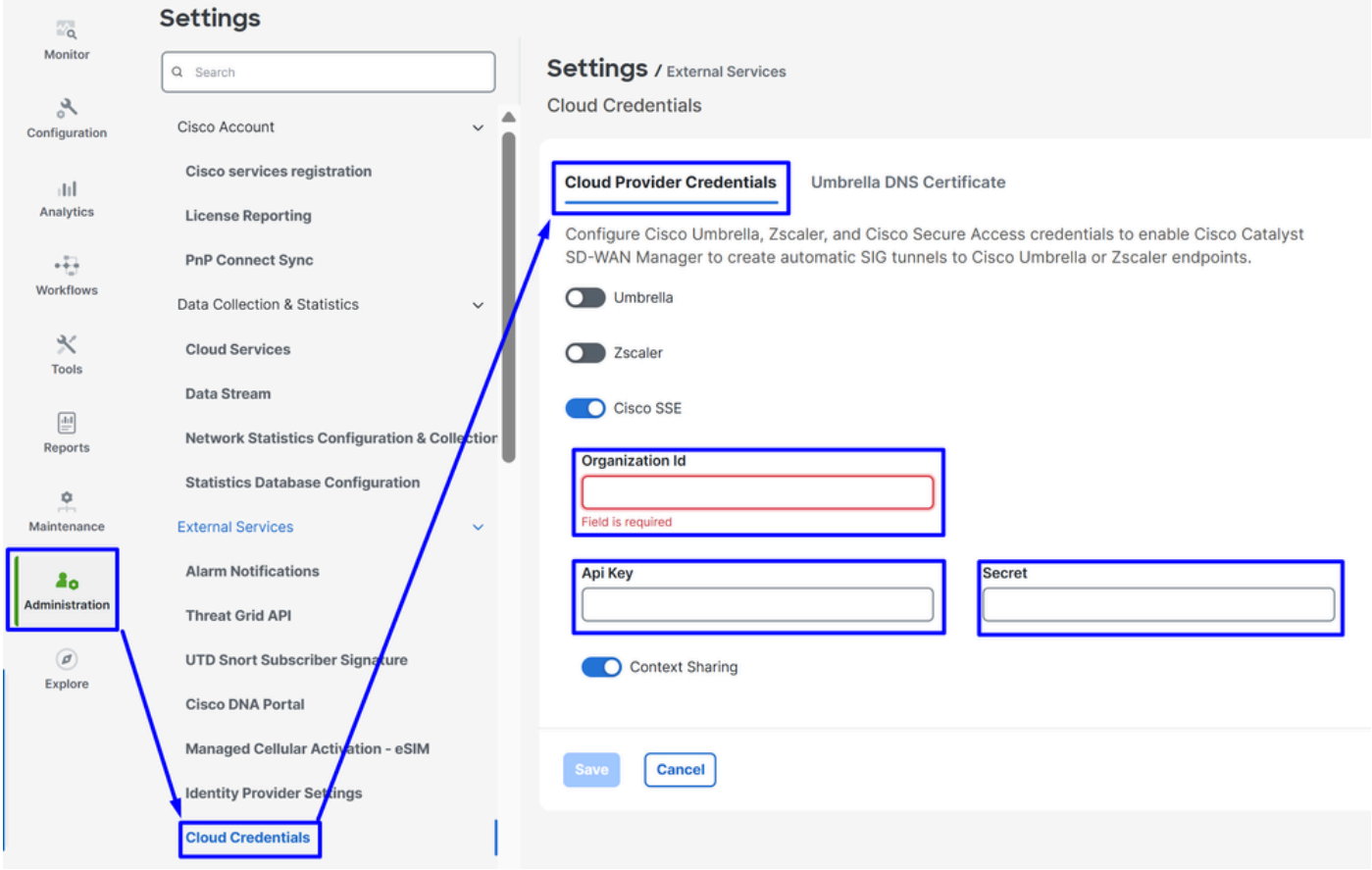
Dann zum Abschluss klicken Sie ACCEPT AND CLOSE.

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 SSEdie Einstellungen für die Organisation aus.



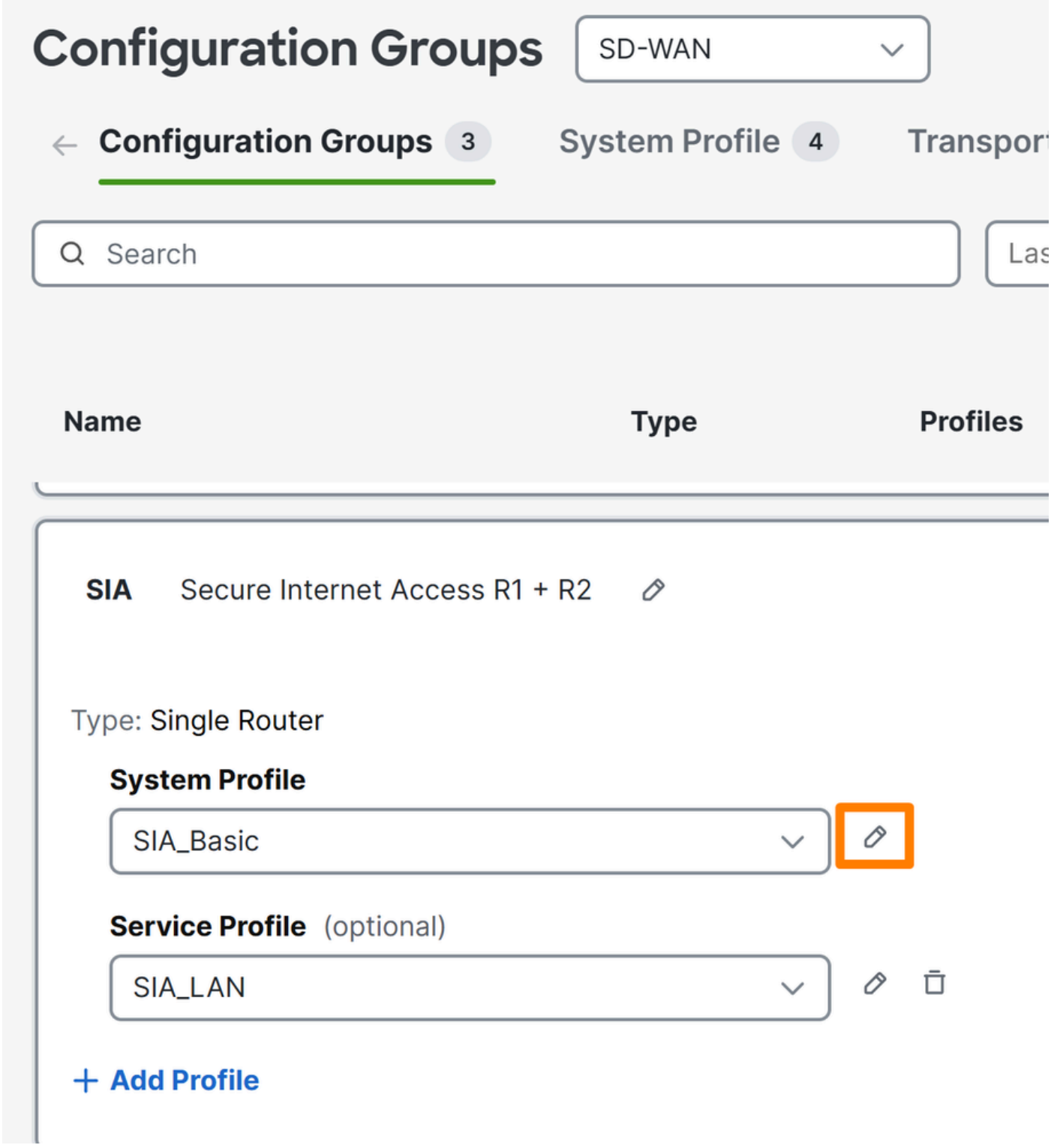
- Organization ID: Sie finden diese Informationen unter der URL Ihres SSE Dashboards https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Kopieren Sie es aus dem Schritt Secure Access Configuration.
- Secret: Kopieren Sie es aus dem Schritt Secure Access Configuration.

Danach klicken Sie auf den Save Button.

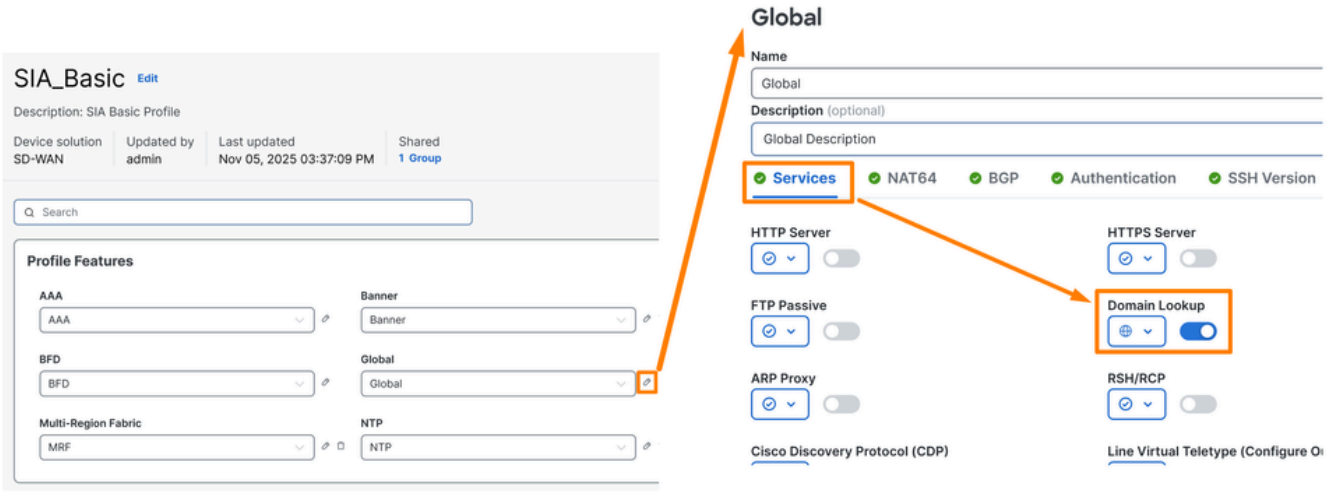
Anmerkung: Bevor Sie mit den nächsten Schritten fortfahren, müssen Sie sicherstellen, dass der SD-WAN-Manager und die Catalyst SD-WAN-Edges über eine DNS-Auflösung und einen Internetzugang verfügen.

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.



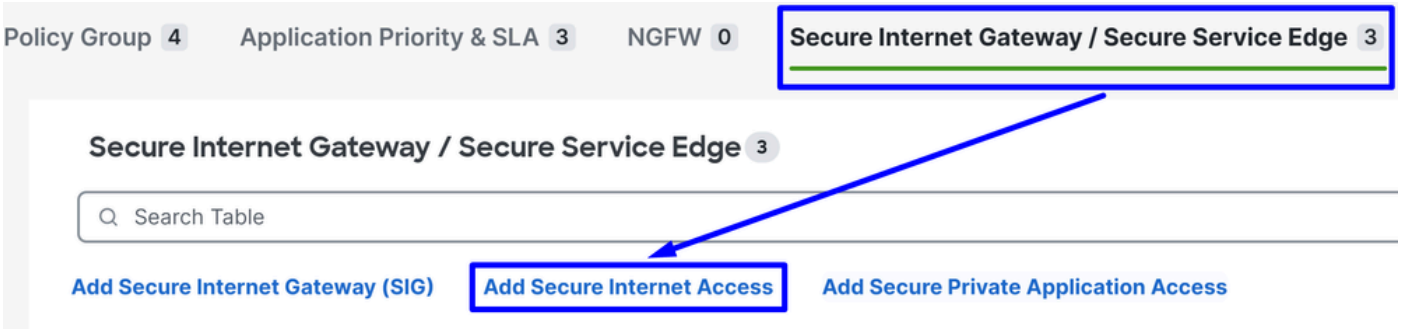
- Bearbeiten Sie dann die globale Option, und stellen Sie sicher, dass die Option Domänenauflösung aktiviert ist.



Konfigurieren der Richtliniengruppe

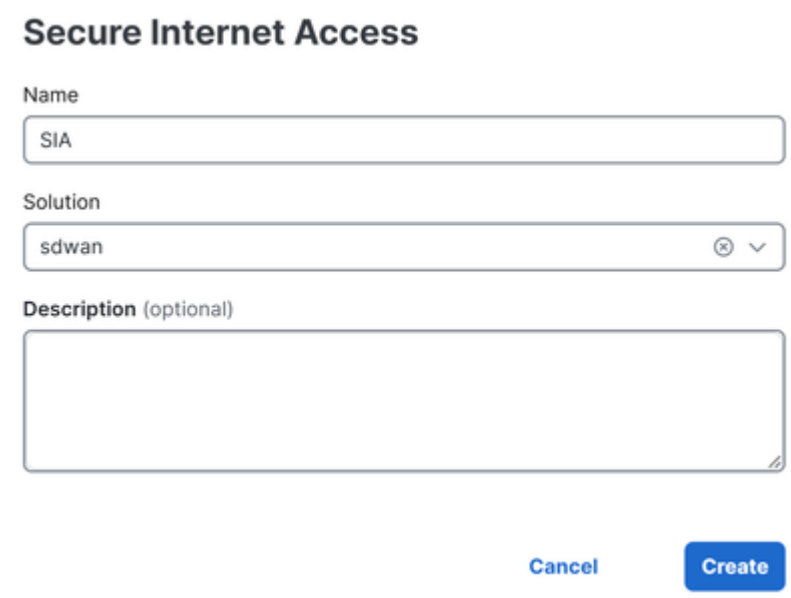
Navigieren Sie zu Konfiguration > Richtliniengruppen:

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

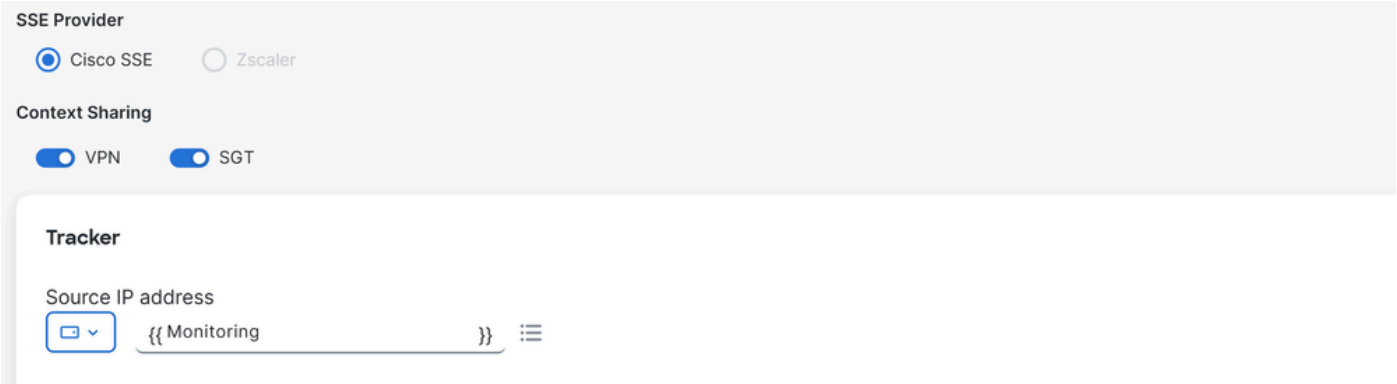


Anmerkung: In Versionen unter 20.18 heißt diese Option Add Secure Service Edge (SSE).

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

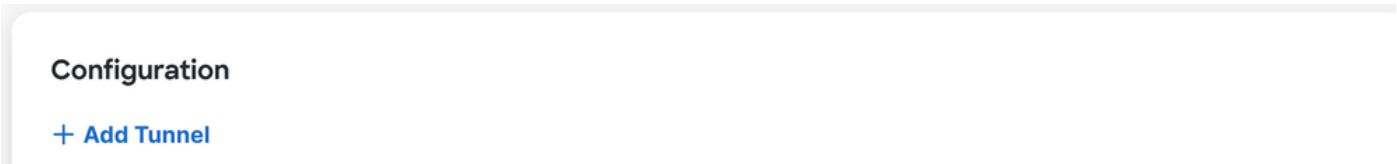


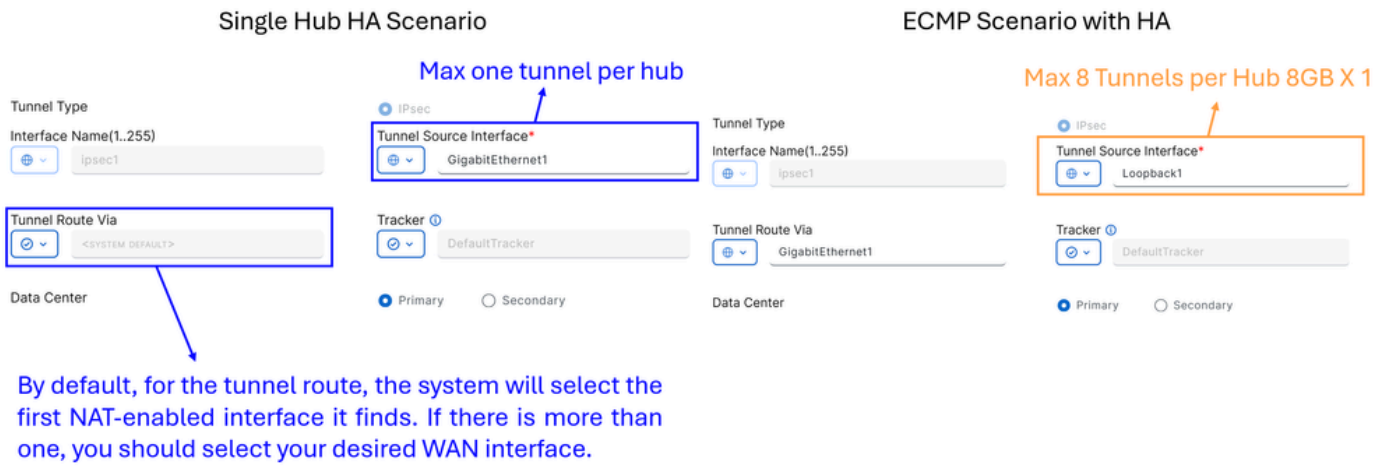
Mit den nächsten Konfigurationen können Sie die Tunnel erstellen, nachdem Sie die Konfiguration in Ihren Catalyst SD-WAN-Edges bereitgestellt haben:



- 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:



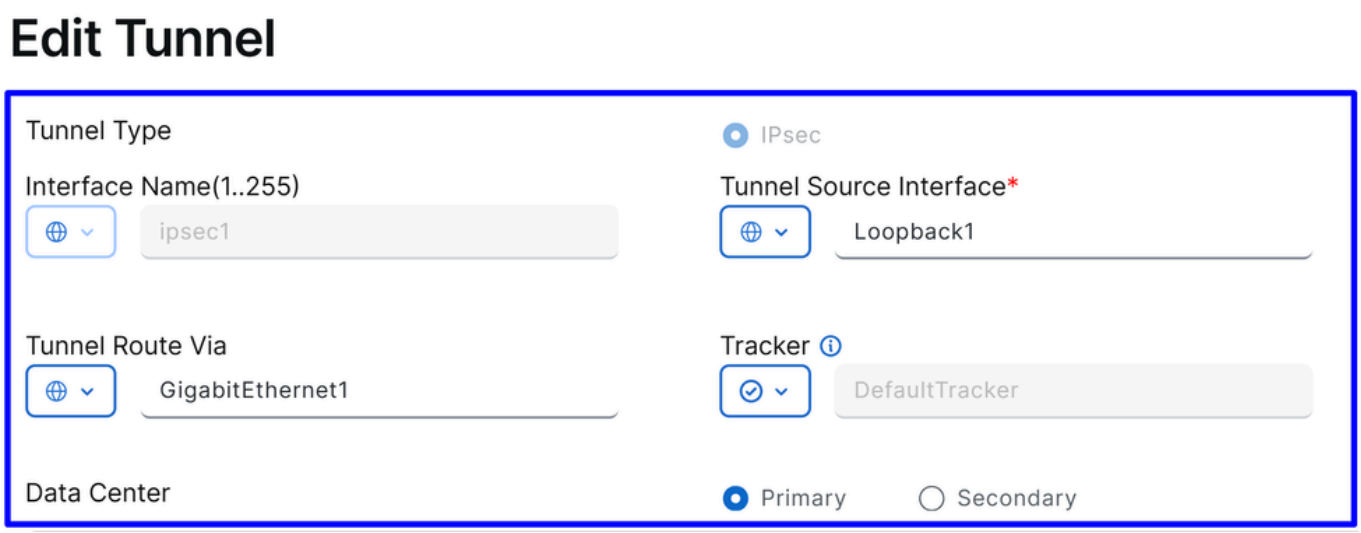


- **Single Hub HA Scenario**: In diesem Szenario können Sie eine hohe Verfügbarkeit konfigurieren, indem Sie ein NTG als aktives und ein anderes als passives Gerät mit einem maximalen Durchsatz von 1 Gbit/s pro NTG verwenden.
- ECMP Scenario with HA: In diesem Szenario können Sie bis zu 8 Tunnel pro 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.

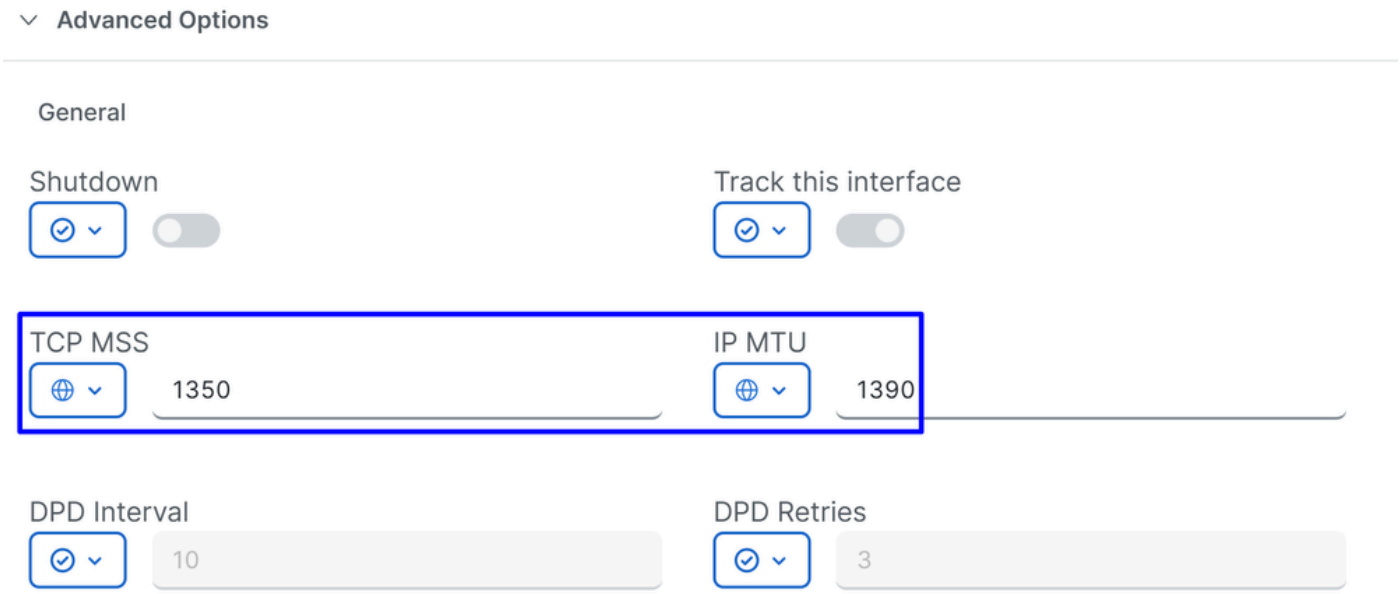
Warnung: Wenn Sie Loopback-Schnittstellen für ein ECMP-Szenario konfigurieren möchten, müssen Sie zunächst die Loopback-Schnittstellen in Configuration Groups > Transport & Management Profileunter der Richtlinie einrichten, die Sie in Ihrem Router verwenden.

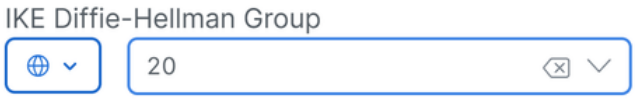
- Klicken SieAdd Tunnel



- 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.

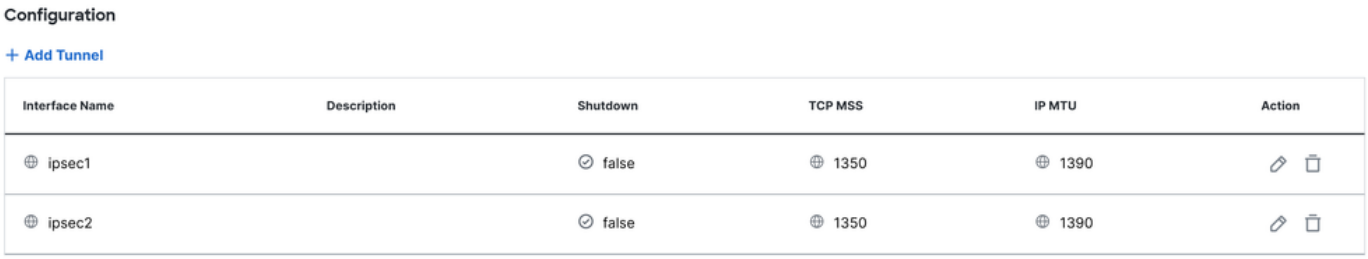




- TCP MSS: 1350
- IP MTU: 1390
- IKE Diffie-Hellman Group: 20

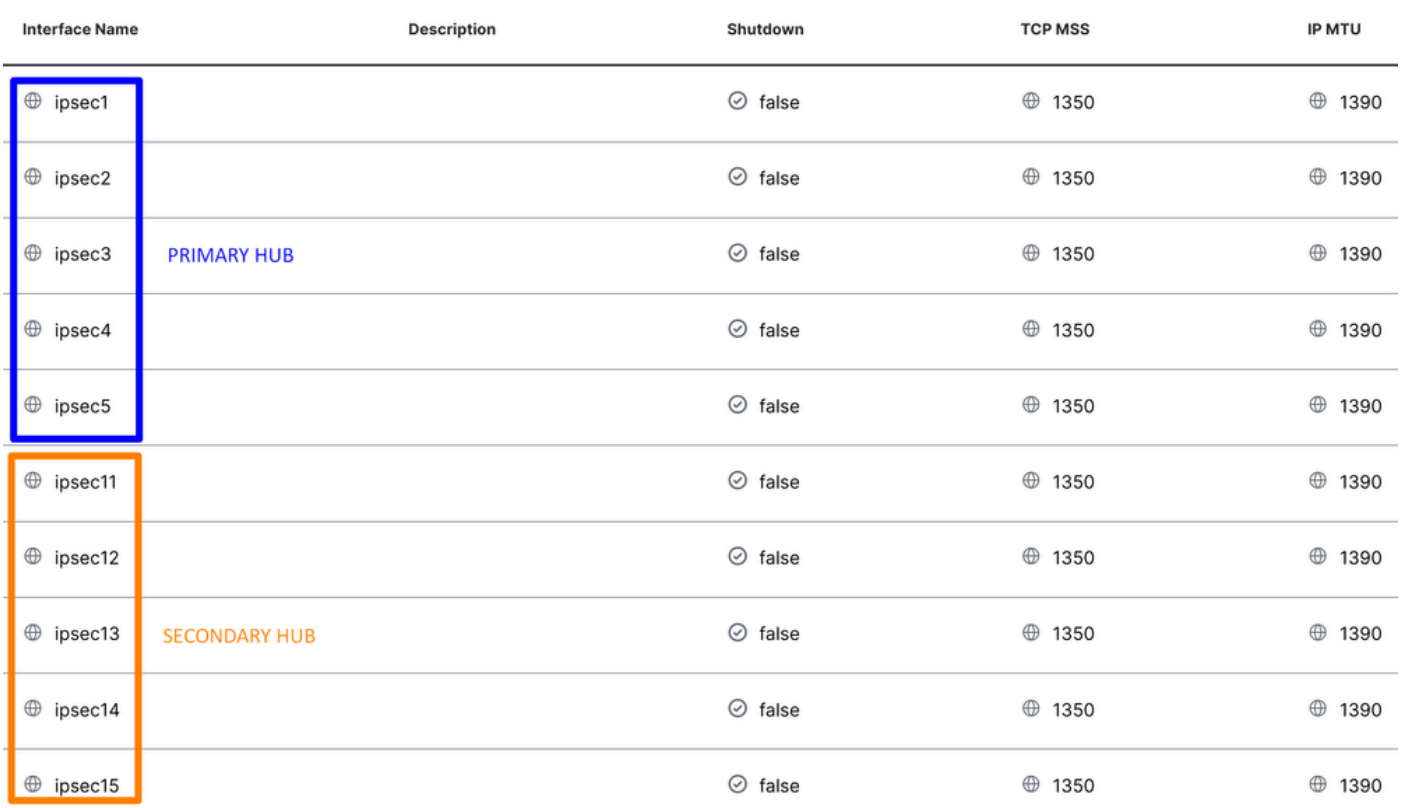
Danach müssen Sie den sekundären Tunnel konfigurieren, der auf das sekundäre Rechenzentrum verweist.

SINGLE HUB HA-SZENARIO



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

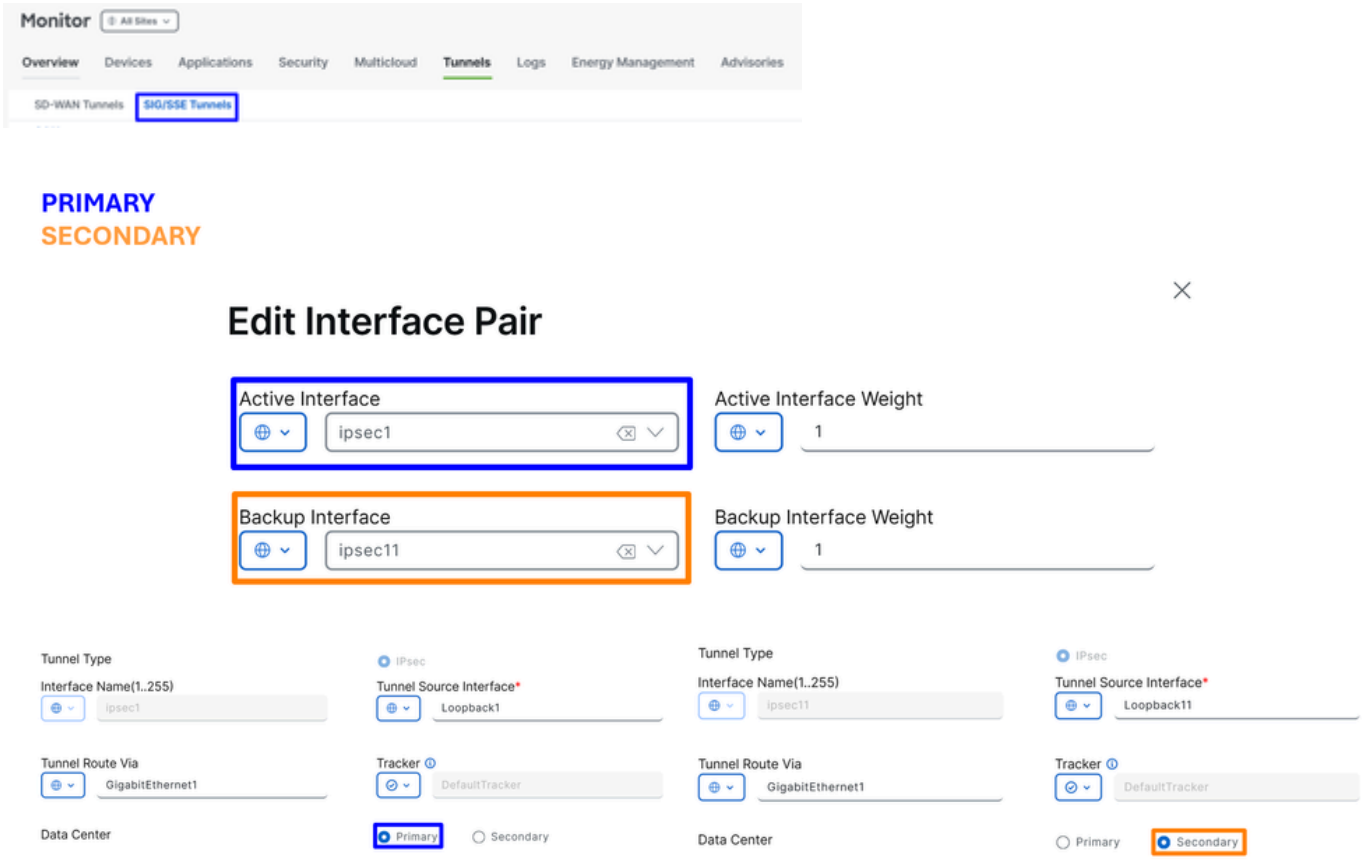
ECMP SCENARIO WITH HA



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

konfigurieren.

Klicken Sie auf Schnittstellenpaar hinzufügen:



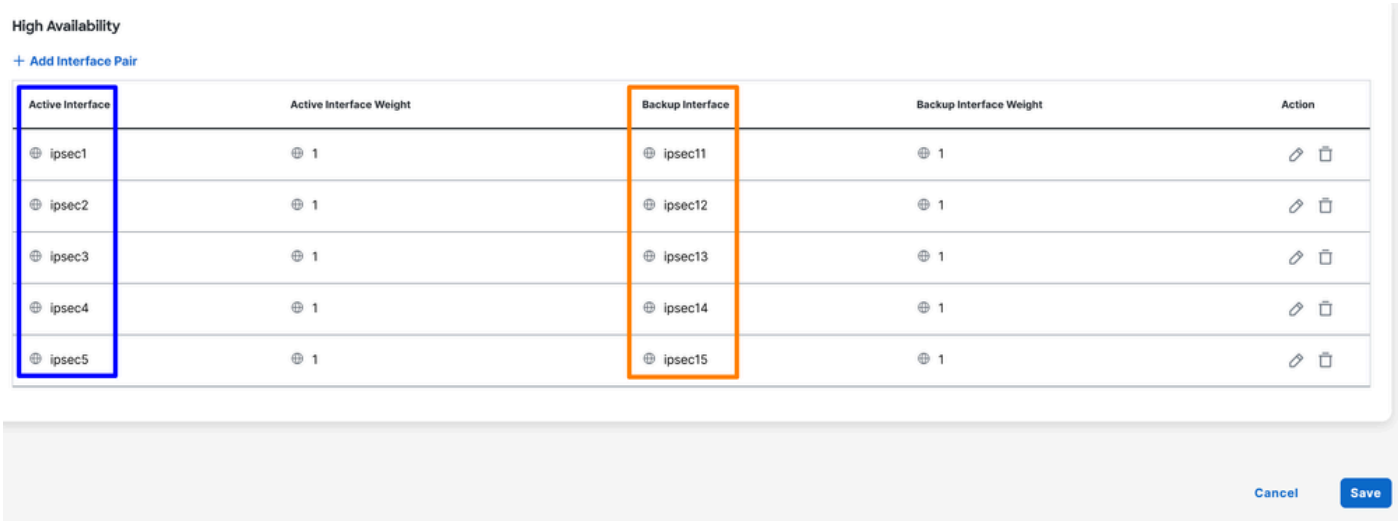
In diesem Schritt müssen Sie den primären und sekundären Tunnel für jedes einzurichtende Tunnelpaar konfigurieren. Das bedeutet, dass jeder Tunnel über ein eigenes Backup verfügt. Denken Sie daran, dass diese Tunnel genau zu diesem Zweck als primäre und sekundäre Tunnels erstellt wurden.
"Active interface"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



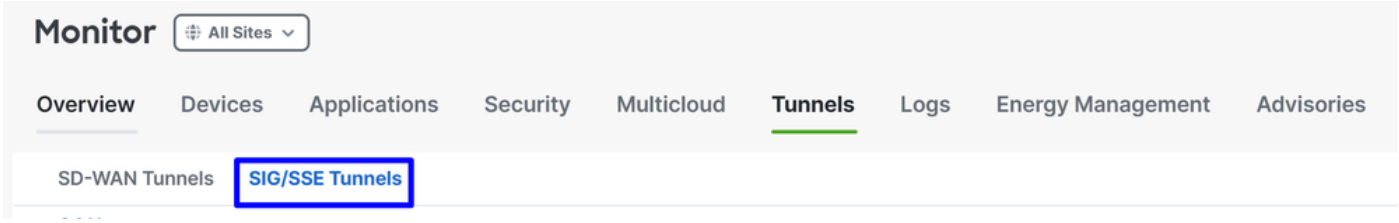
Anmerkung: Maximal 8 Tunnelpaare (16 Tunnel: 8 primäre und 8 sekundäre Ports) können in SD-WAN Catalyst vManage konfiguriert werden. Cisco Secure Access unterstützt bis zu 10 Tunnelpaare.

- 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 aufSIG/SSE Tunnels

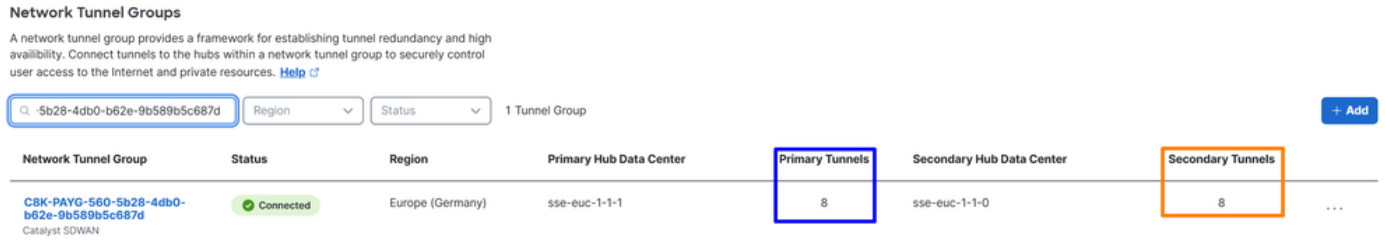


Außerdem können Sie sehen, ob die Tunnel für Cisco Secure Access verfügbar sind oder nicht.

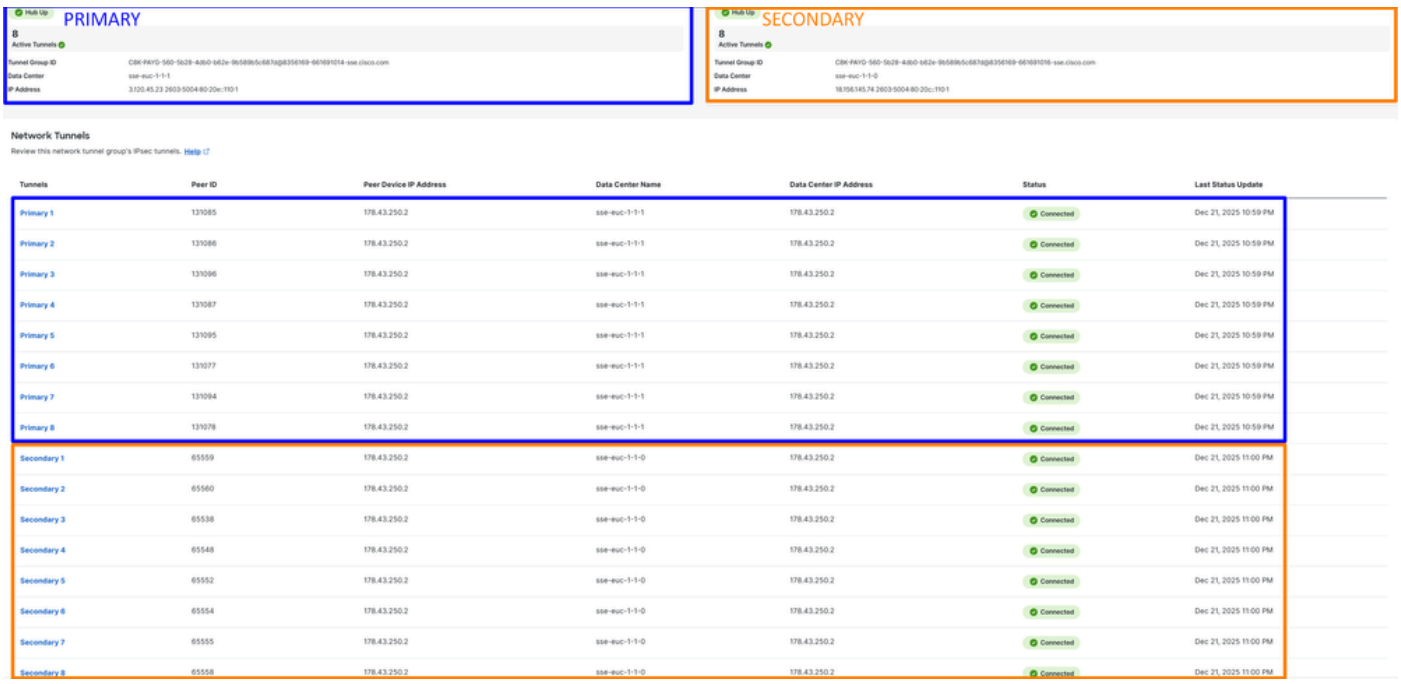
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public 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



Klicken Sie in einer Detailansicht auf den Namen des Tunnels:



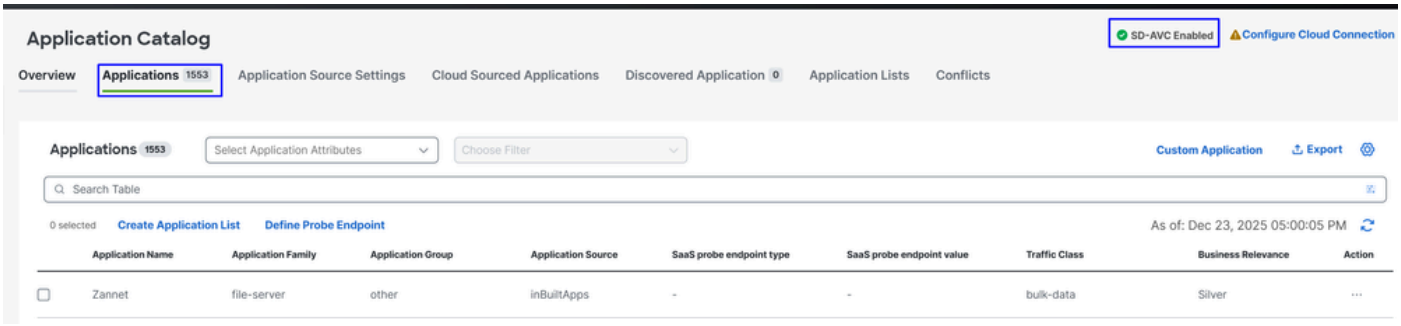
Danach können Sie mit dem Schritt fortfahren, Create your Custom Bypass FQDN or APP in SD-WAN

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:

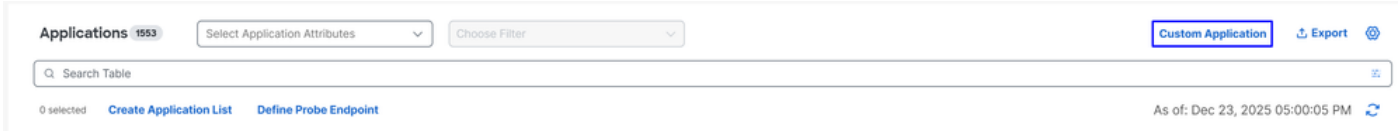
- Klicken Sie auf Configuration > Application Catalog > Applications



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

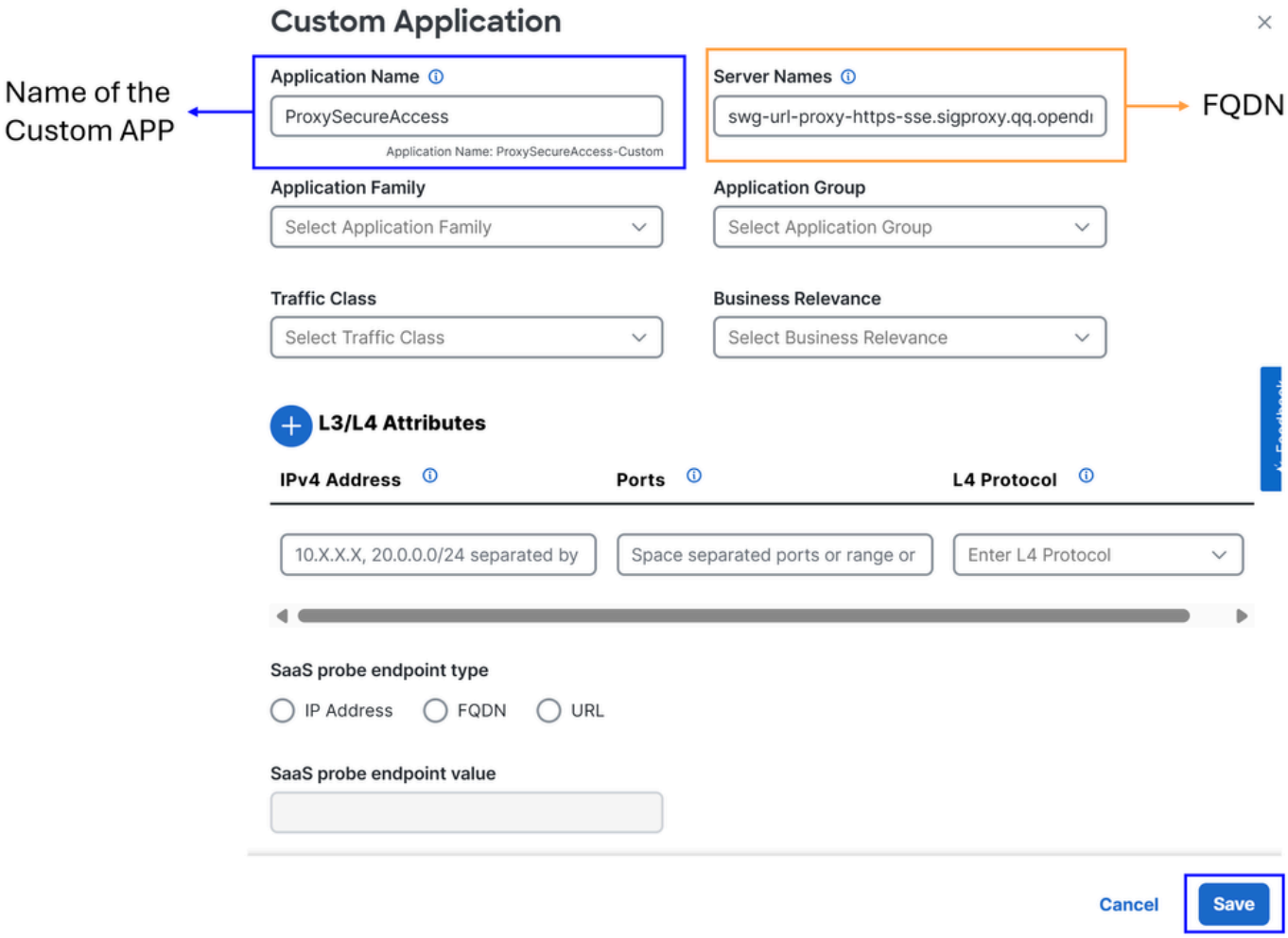
Anmerkung: Um auf den Anwendungskatalog zugreifen zu können, müssen Sie SD-AVC aktivieren.

- Klicken Sie Custom Application



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

ProxySecureAccess

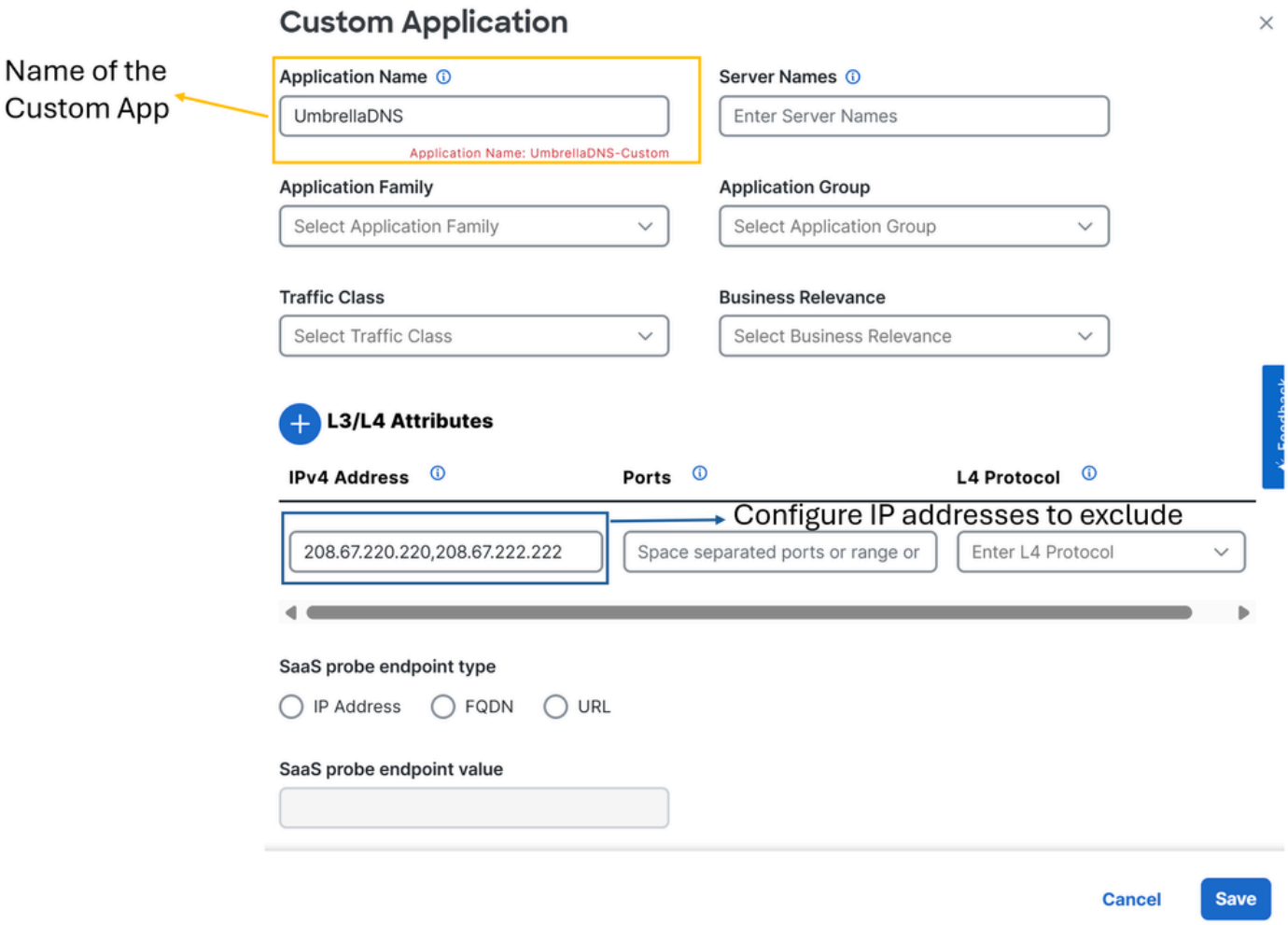


- Server Name: Verwenden Sie den FQDN, den Sie umgehen möchten (in diesem Beispiel sind die FQDN der SWG konfiguriert).
  - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Klicken Sie Save

Anmerkung: Ändern Sie ORGID mit Ihrer SSE-Organisationsnummer.

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

UmbrellaDNS



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:

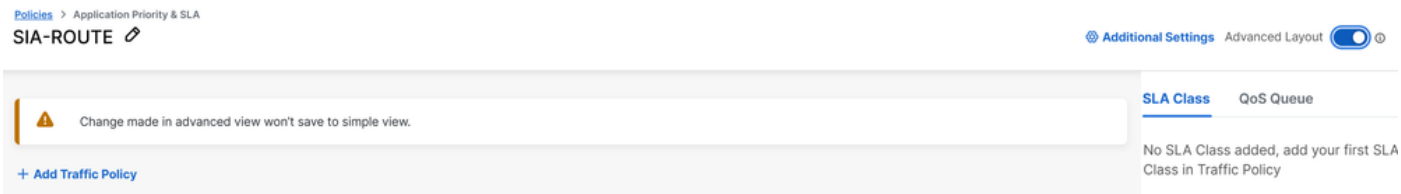
- Configuration > Configuration Groups > Service Profile > Service Route: Diese Methode ermöglicht das Routing zu Secure Access, bietet jedoch keine Flexibilität.
- **Configuration** > Policy Groups > Application Priority & SLA: Diese Methode bietet verschiedene Routing-Optionen innerhalb des SD-WAN 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

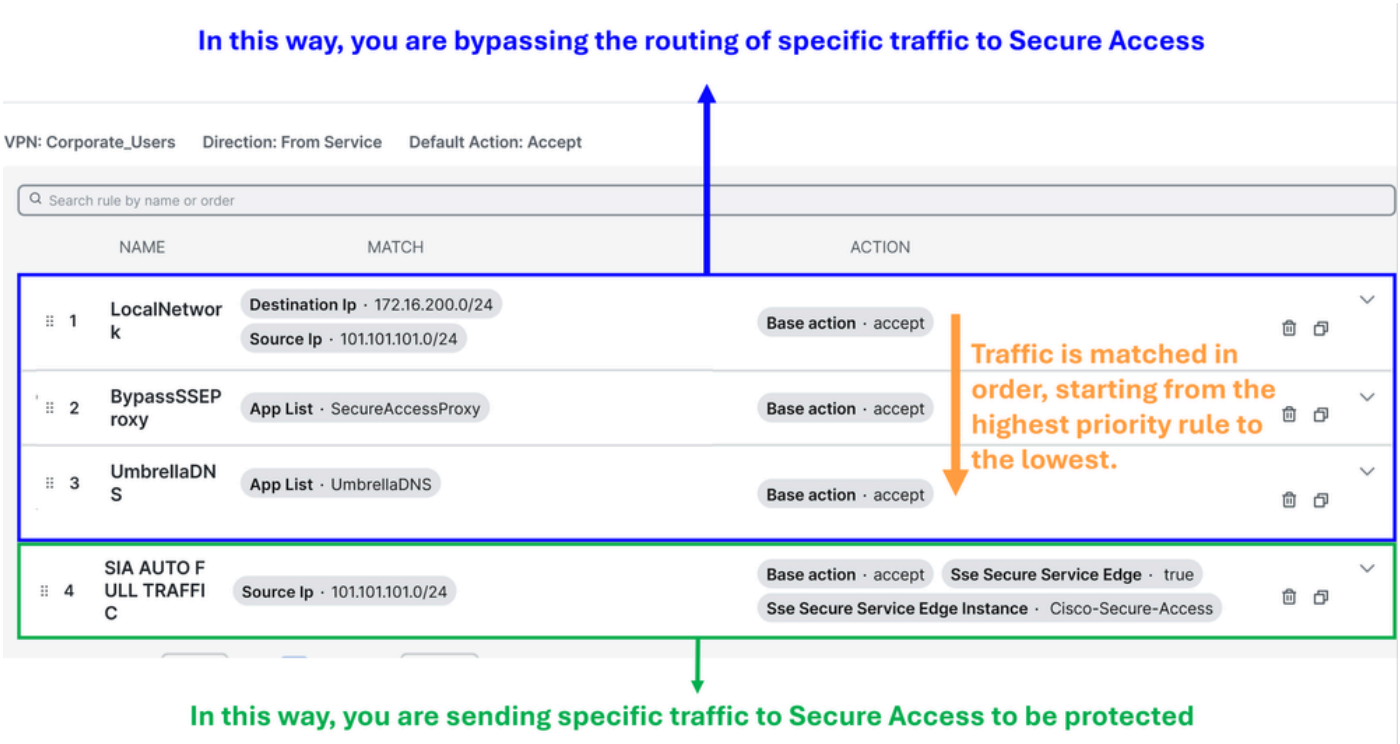
- Konfigurieren Sie einen Richtliniennamen, und klicken Sie auf Create

- Enable Advanced Layout
- Klicken Sie + Add Traffic Policy



- 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:



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).

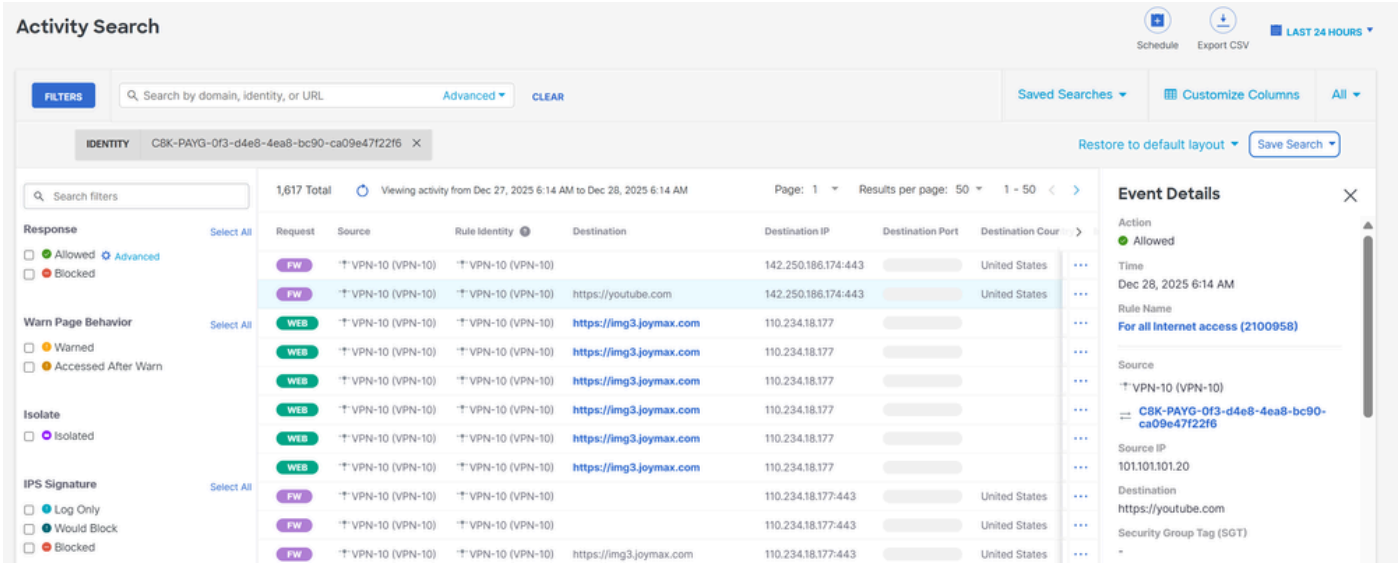
2. **BypassSSEProxy (Optional)**: Diese Richtlinie verhindert, dass interne Computer mit aktiviertem Cisco Umbrella-Modul im Secure Client und aktivierter SWG Proxy-Datenverkehr an die Cloud zurücksenden. Das erneute Routing von Proxy-Datenverkehr in die Cloud wird nicht als Best Practice erachtet.
3. 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 Tunnelidentität:

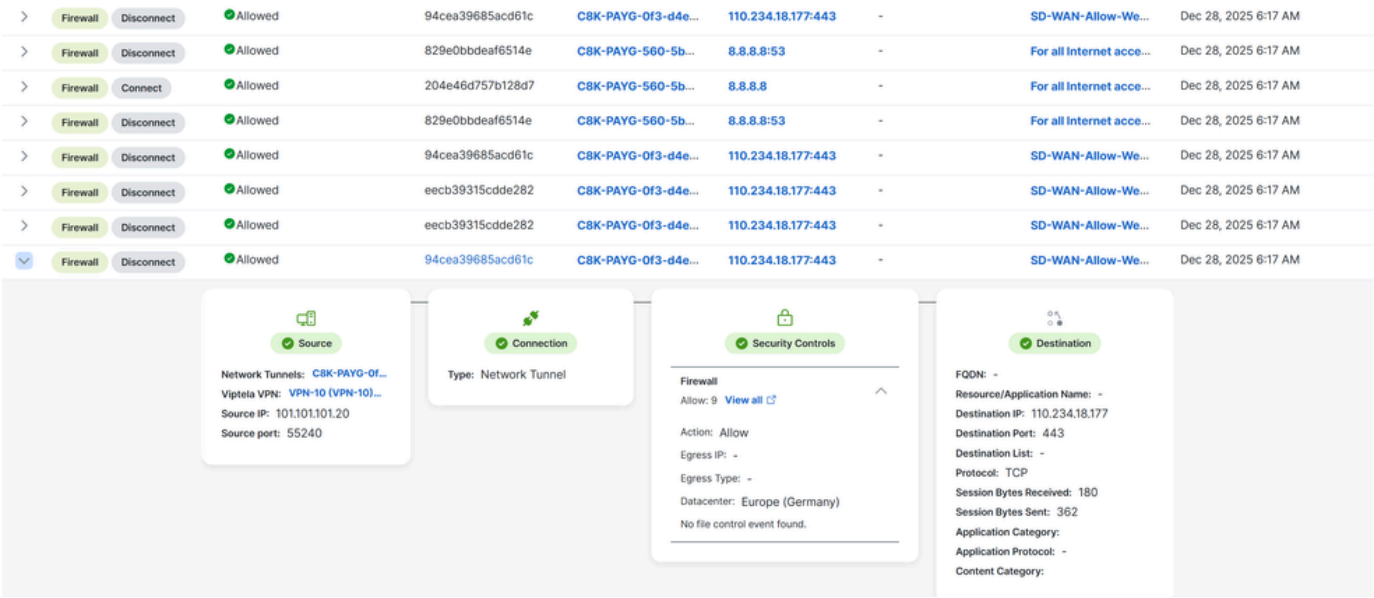
Sicherer Zugriff - Aktivitätssuche

Navigieren Sie zu Monitor > Activity Search:



Sicherer Zugriff - Veranstaltungen

Navigieren Sie zu Monitor > Events:

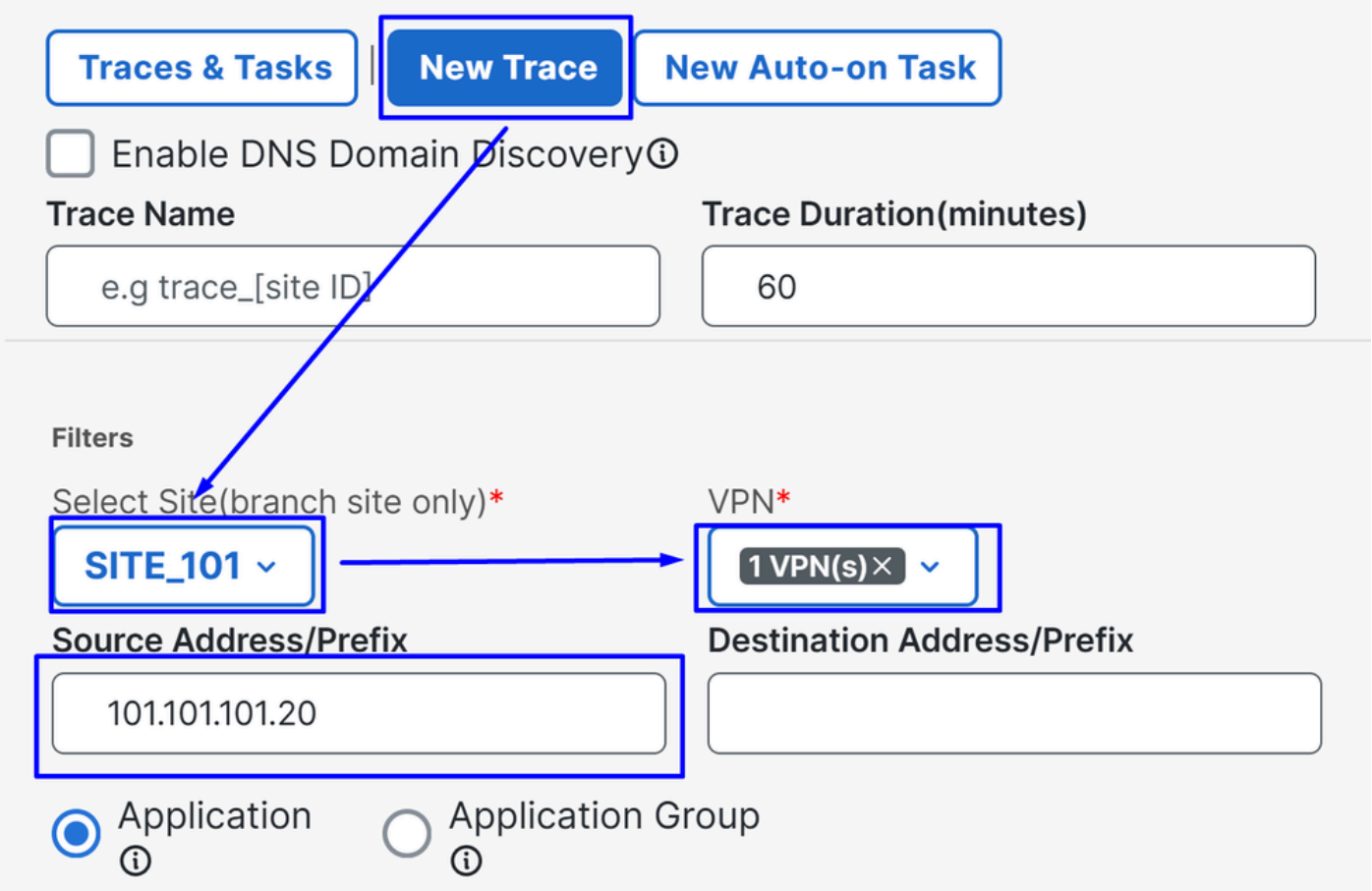


Anmerkung: Vergewissern Sie sich, dass Ihre Standardrichtlinie mit aktivierter Protokollierung standardmäßig deaktiviert ist.

Catalyst SD-WAN Manager - Netzwerkweite Pfadeinblicke

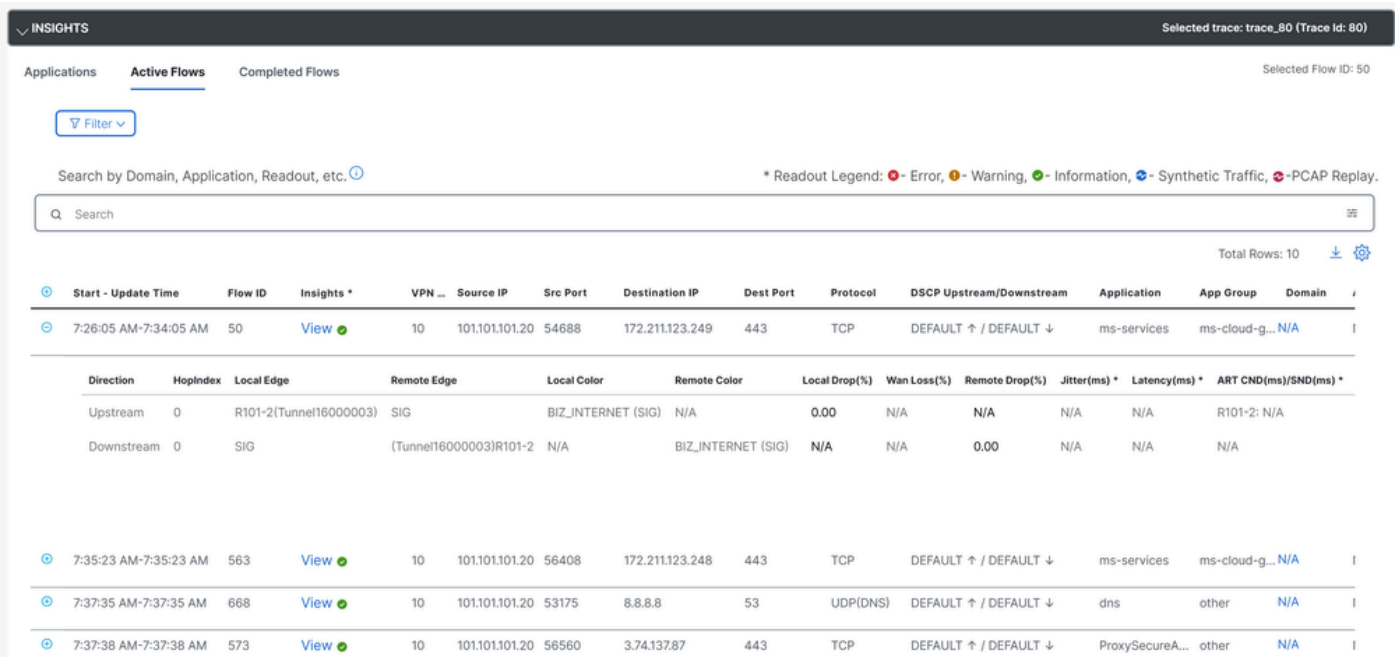
Navigieren Sie zum Catalyst SD-WAN Manager:

- Klicken Sie auf Tools > Network-Wide Path Insights
- Klicken Sie New Trace



- 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:



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.