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

Inhalt

Einleitung

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

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

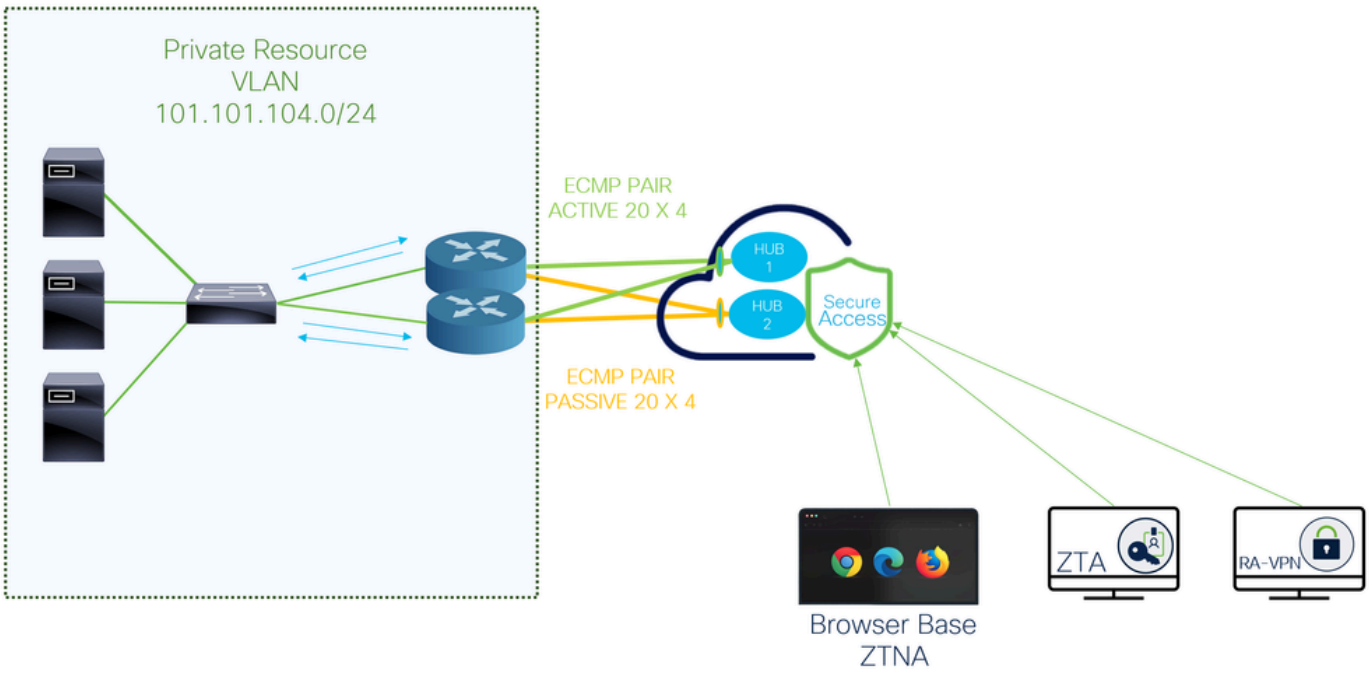
per Failover weitergeleitet werden.

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

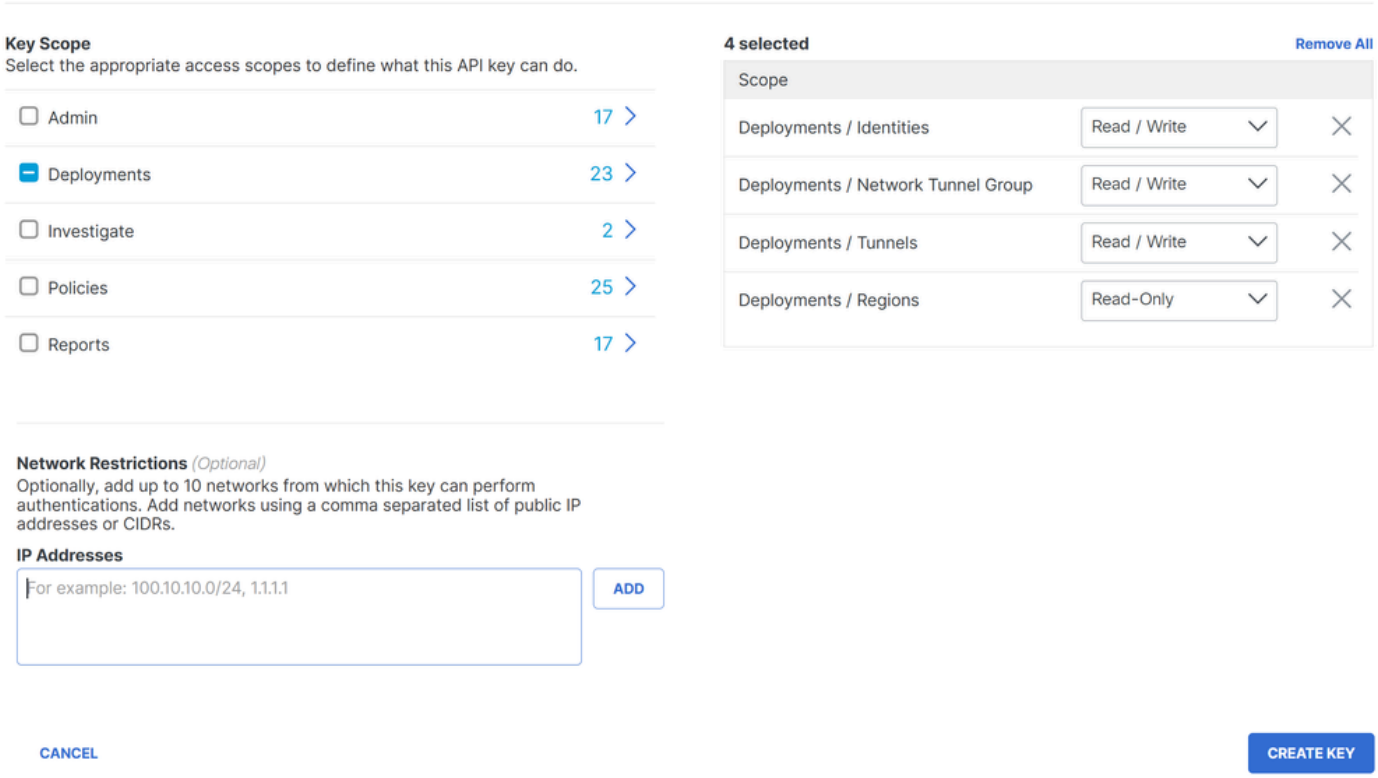
Konfiguration des sicheren Zugriffs

API-Erstellung

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

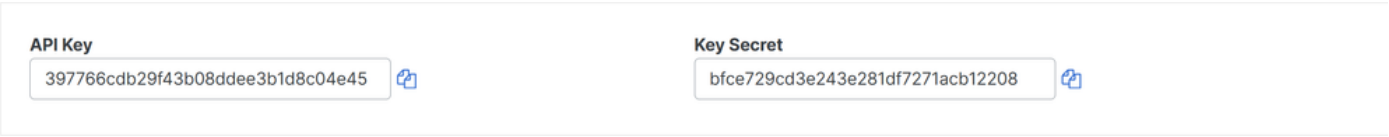
Navigieren Sie zum Dashboard für sicheren Zugriff.

- 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



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 klickenACCEPT AND CLOSE; Andernfalls müssen Sie sie erneut erstellen und die Dateien löschen, die nicht kopiert wurden.

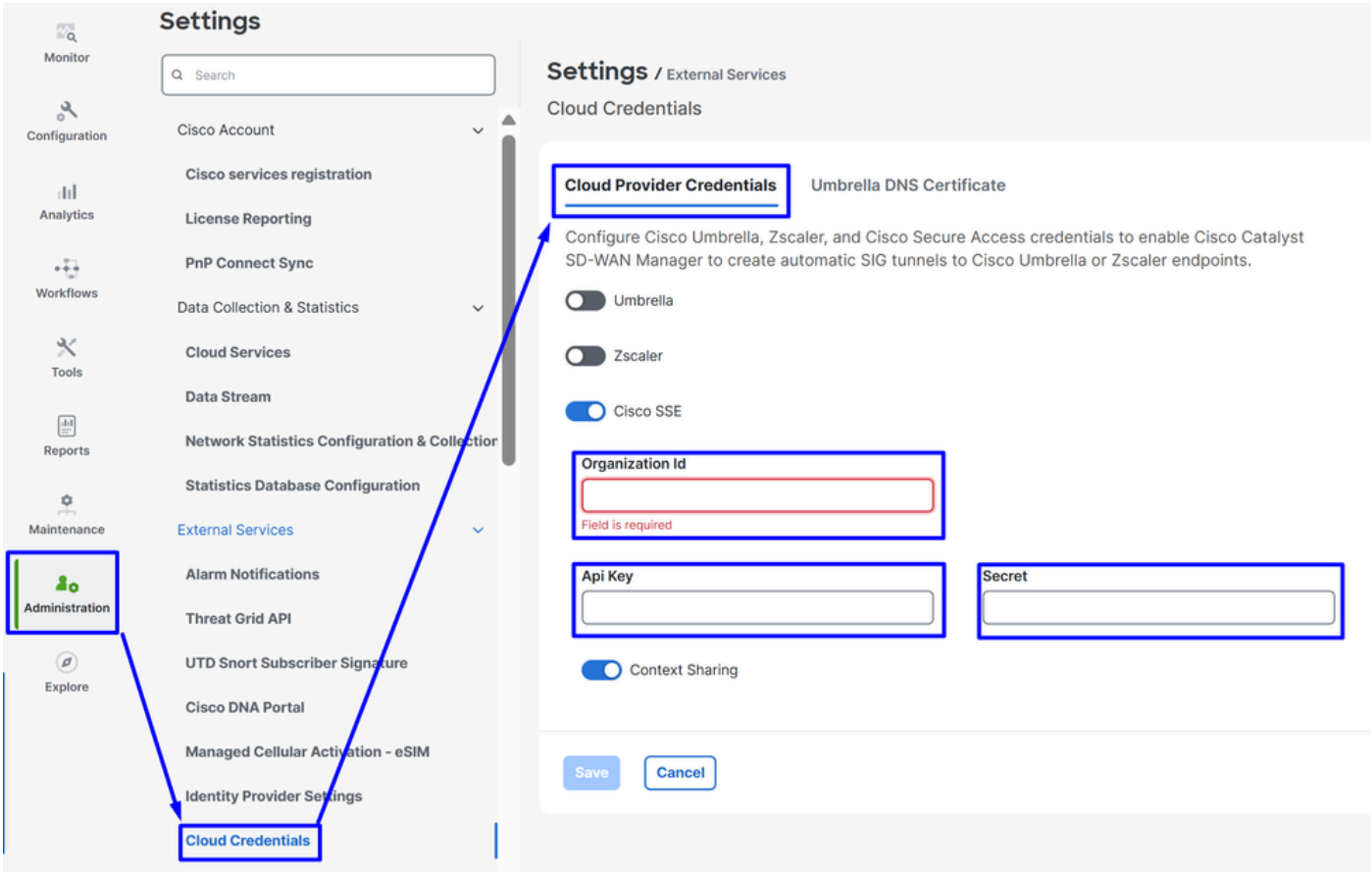
Dann zum Abschluss klicken Sie ACCEPT AND CLOSE.

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.



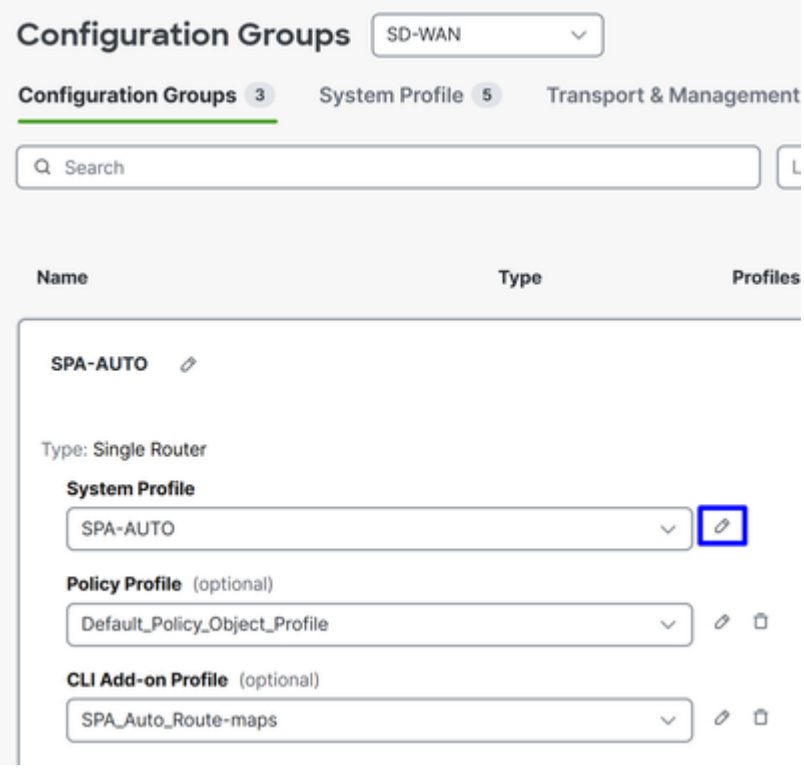
- **Organization ID**: Sie finden diese Informationen unter der URL Ihres SSE Dashboards https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Kopieren Sie es aus dem Schritt Secure Access Configuration.
- Secret: Kopieren Sie es aus dem Schritt Secure Access Configuration.

Danach klicken Sie auf den Save Button.

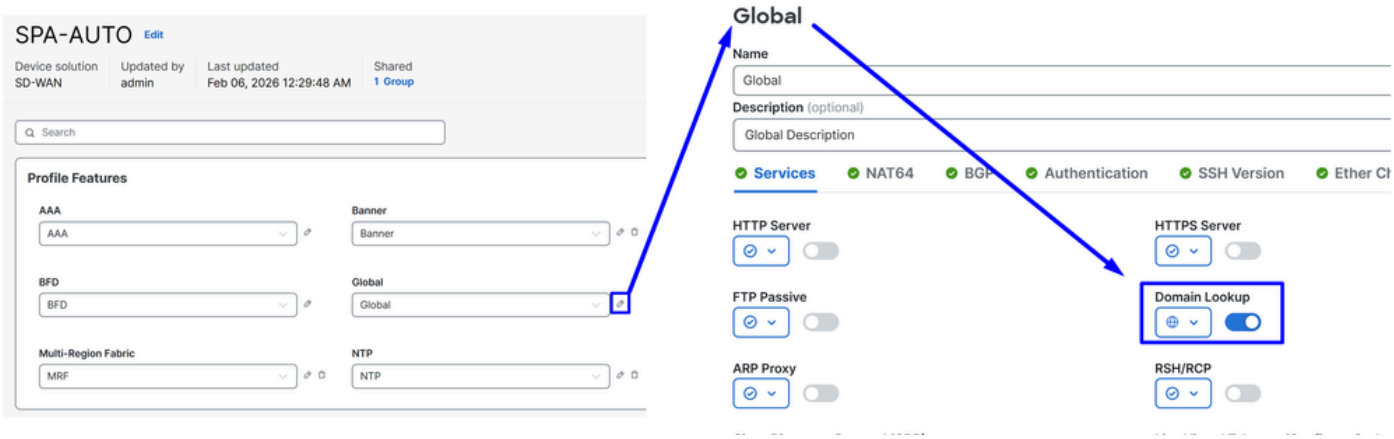
Anmerkung: Bevor Sie mit den nächsten Schritten fortfahren, müssen Sie sicherstellen, dass der SD-WAN-Manager und die Catalyst SD-WAN-Edges über eine DNS-Auflösung und einen Internetzugang verfügen.

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.



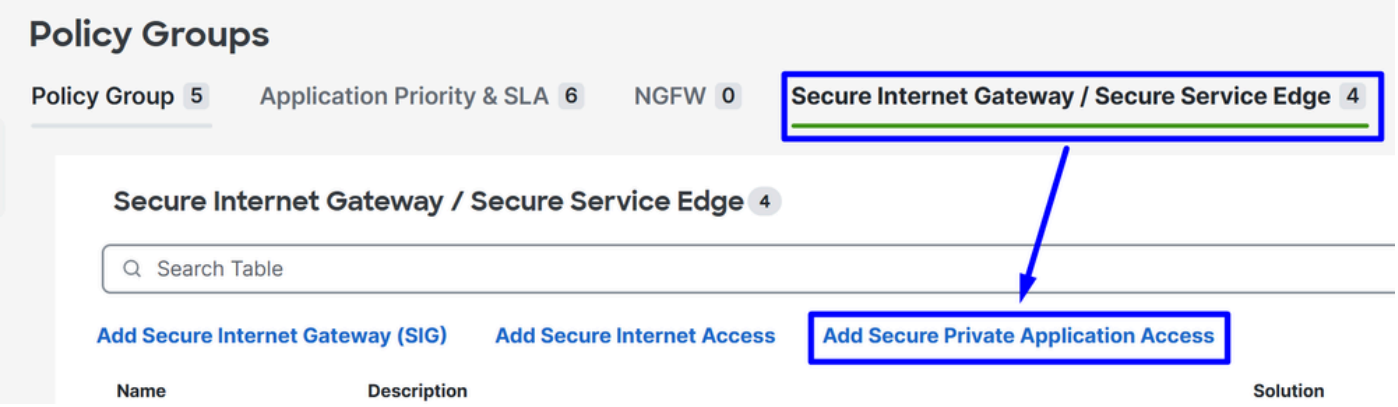
- Bearbeiten Sie dann die globale Option, und stellen Sie sicher, dass die Option Domänenauflösung aktiviert ist.



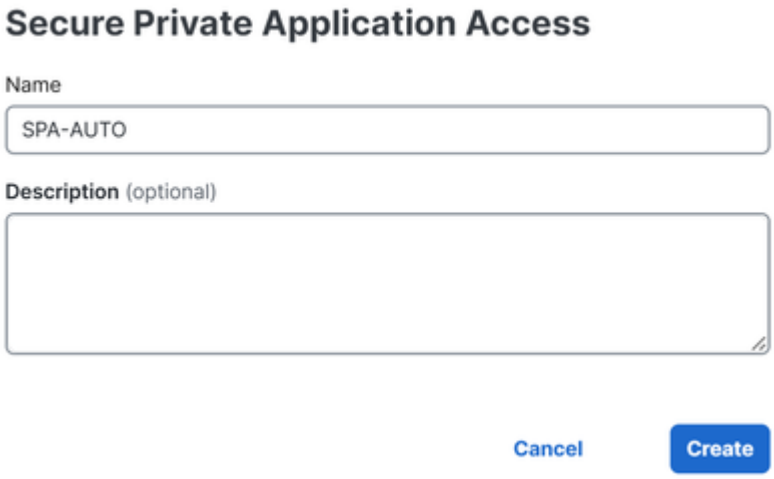
Konfigurieren der Richtliniengruppe

Navigieren Sie zuKonfiguration > Richtliniengruppen:

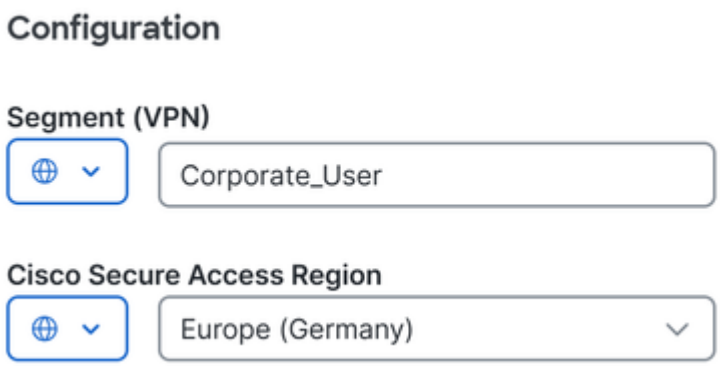
- Auf Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- Konfigurieren Sie einen Namen, 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:

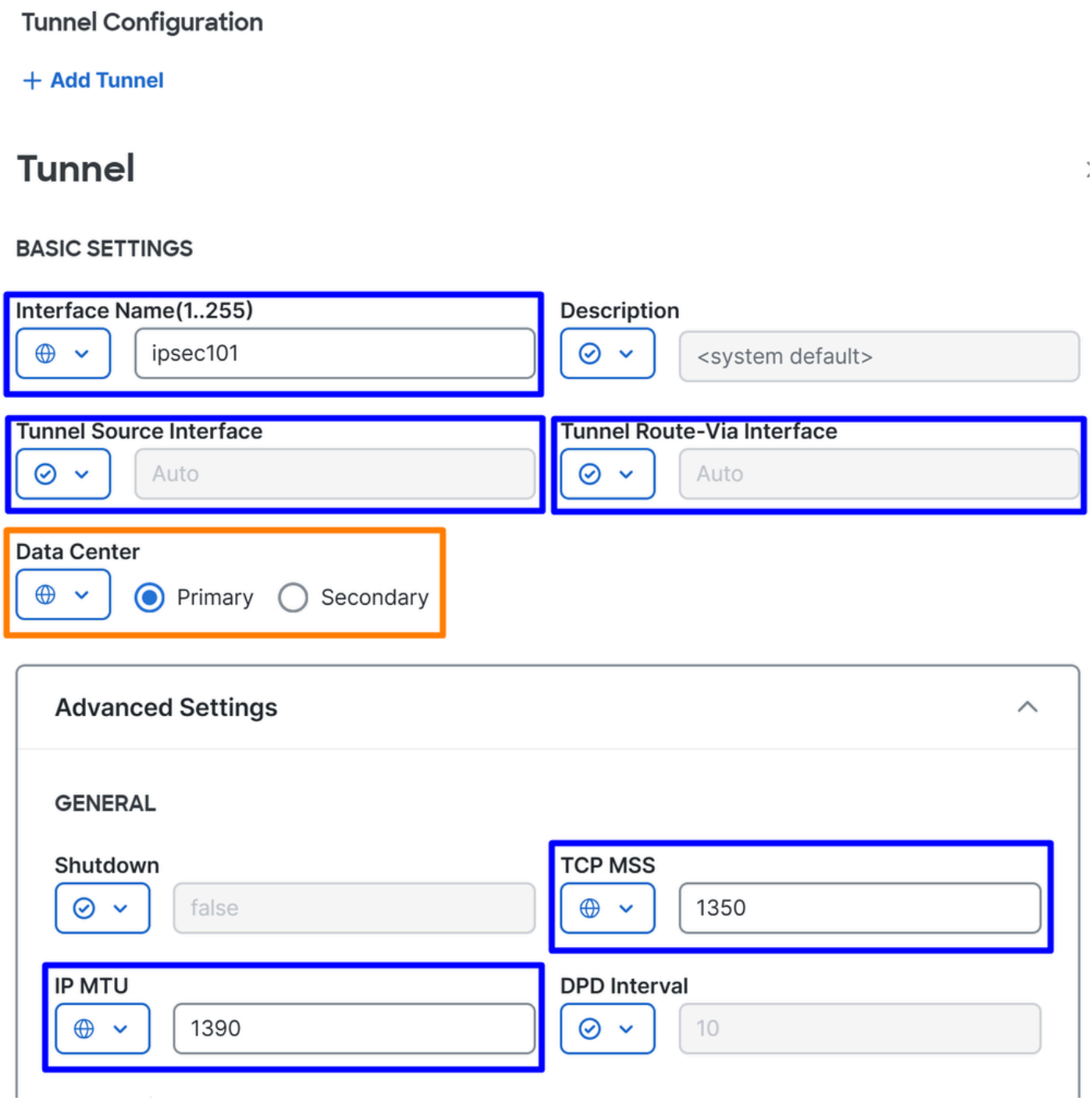


- Configuration
  - Segment (VPN): Wählen Sie die VRF-Instanz aus, die die Anwendungen hostet, auf die über sicheren Zugriff zugegriffen werden soll.
  - Cisco Secure Access Region: Wählen Sie die Region aus, die dem SD-WAN-Hub oder der Zweigstelle, in der die Anwendungen gehostet werden, am nächsten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

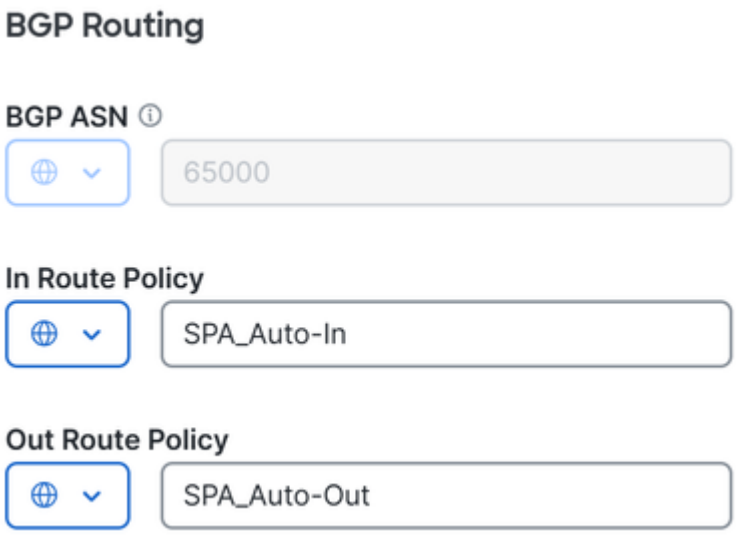
- Data Center: Wählen Sie entsprechend Primary oder Secondary aus. Wenn der primäre Tunnel bereits konfiguriert ist, wählen Sie Sekundär aus. In normalen Szenarien kann ein Tunnel als primär und ein anderer als sekundär konfiguriert werden.
- Advanced Settings
  - IP MTU: Verwenden 1390
  - TCP MSS: 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		MAXIMUM OF 10 TUNNELS PER HUB
ipsec110		Auto	Auto	Secondary		10 x 1 Primary
ipsec111		Auto	Auto	Primary		10 x 1 Secondary
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		

Hinweis: Wenn Sie mehrere Tunnel pro Router bereitstellen, stellen Sie sicher, dass die Transportschnittstelle die aggregierte Bandbreite aller aktiven Tunnel zusammengenommen 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: 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
  - 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 geändert werden, CLI Add-On Template 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 eine bearbeitet werden, um die entsprechenden Routen zuzulassen/zu verweigern CLI Add-On Template.

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 Groupgeändert haben.

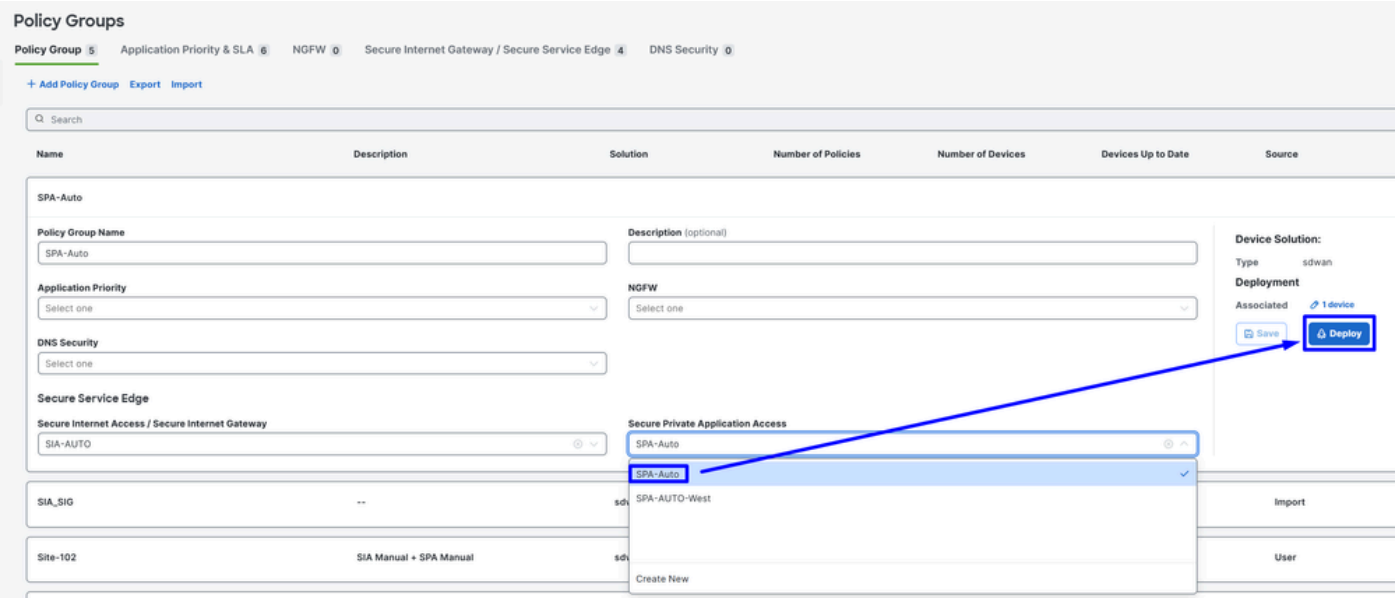
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

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 AbschließenDeployklicken



So prüfen Sie inSecure Access:

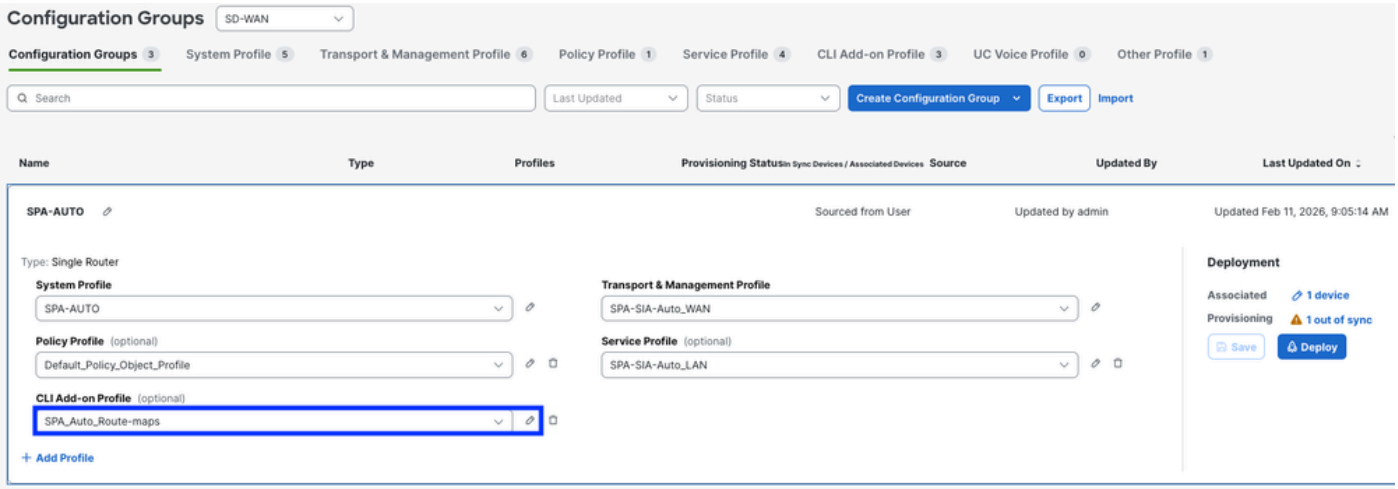
- Auf Connect> Network Connections

TUNNELEINRICHTUNG

Konfigurieren von Routing

Navigieren Sie zu Configure > Configuration Groups

- Klicken Sie auf Ihre Configuration Group und erstellen/bearbeiten Sie Ihre CLI Add-on Profile



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
```

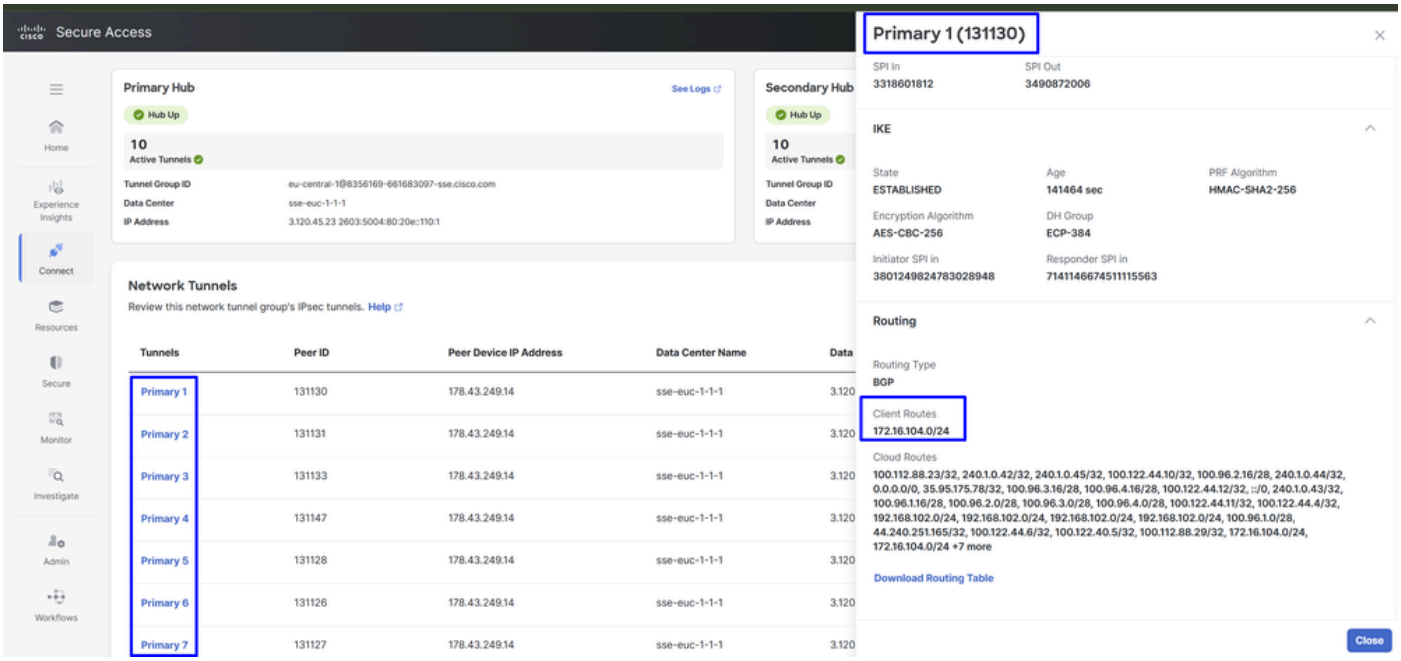
Warnung: Eine sorgfältige Planung ist erforderlich, wenn die Netzwerke definiert werden, die über BGP-Routing-Maps ein- und ausgehen dürfen. Das Zulassen aller Routen, wie im obigen Beispiel gezeigt, kann zu unbeabsichtigtem Routing-Verhalten führen. Geben Sie für eine optimale Bereitstellung explizit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

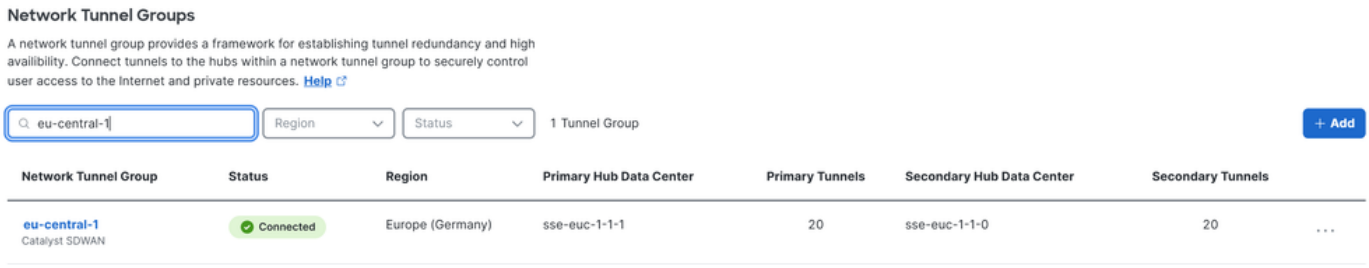
ROUTING-EINRICHTUNG



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.

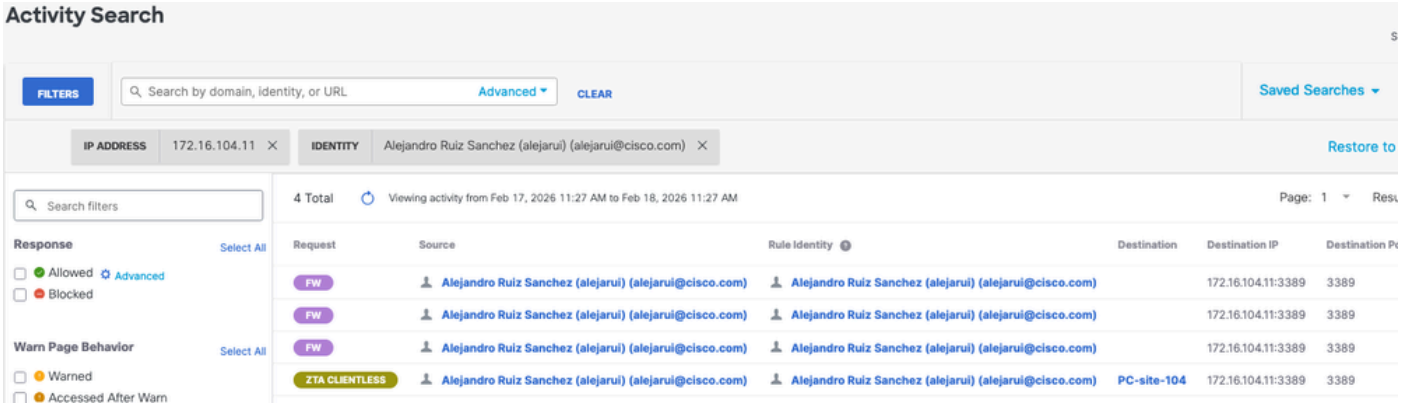


Überprüfung

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 Tunnelidentität:

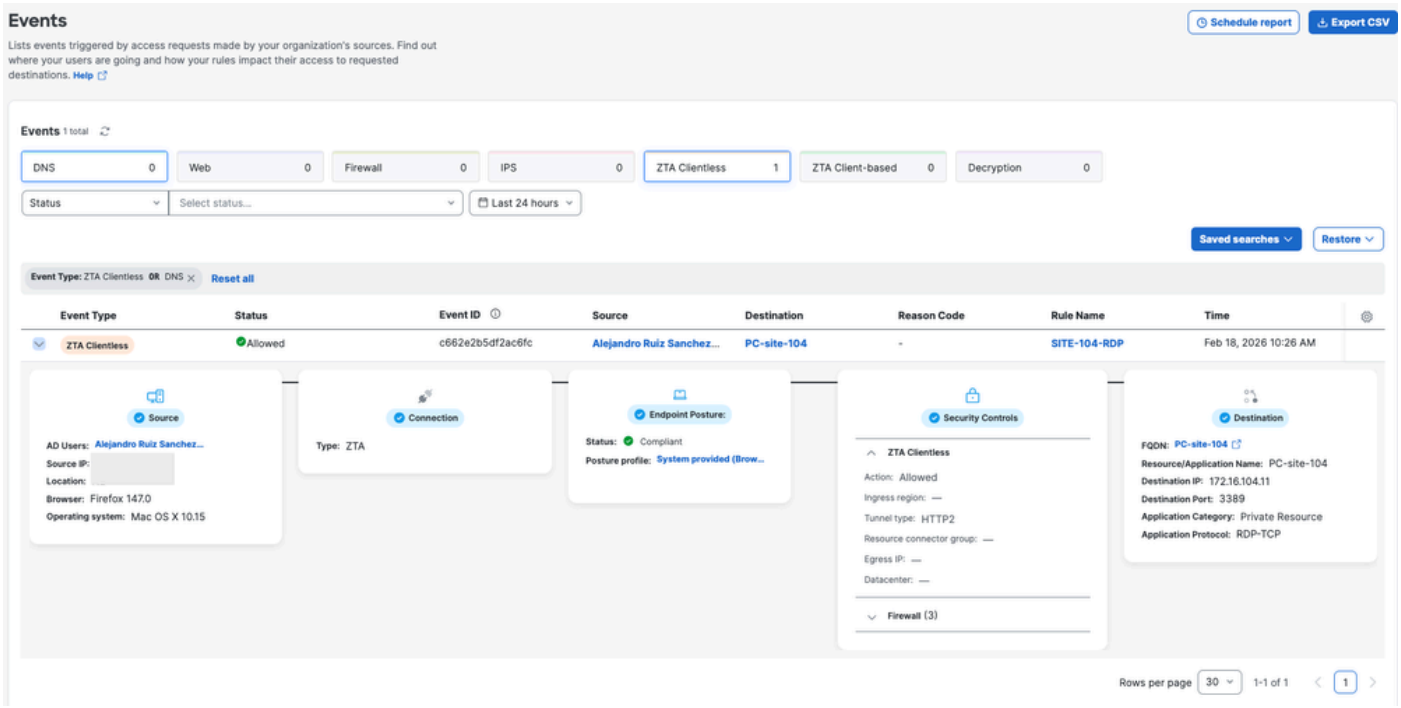
Sicherer Zugriff - Aktivitätssuche

Navigieren Sie zu Monitor>Activity Search :



Sicherer Zugriff - Veranstaltungen

Navigieren Sie zu Monitor>Events:

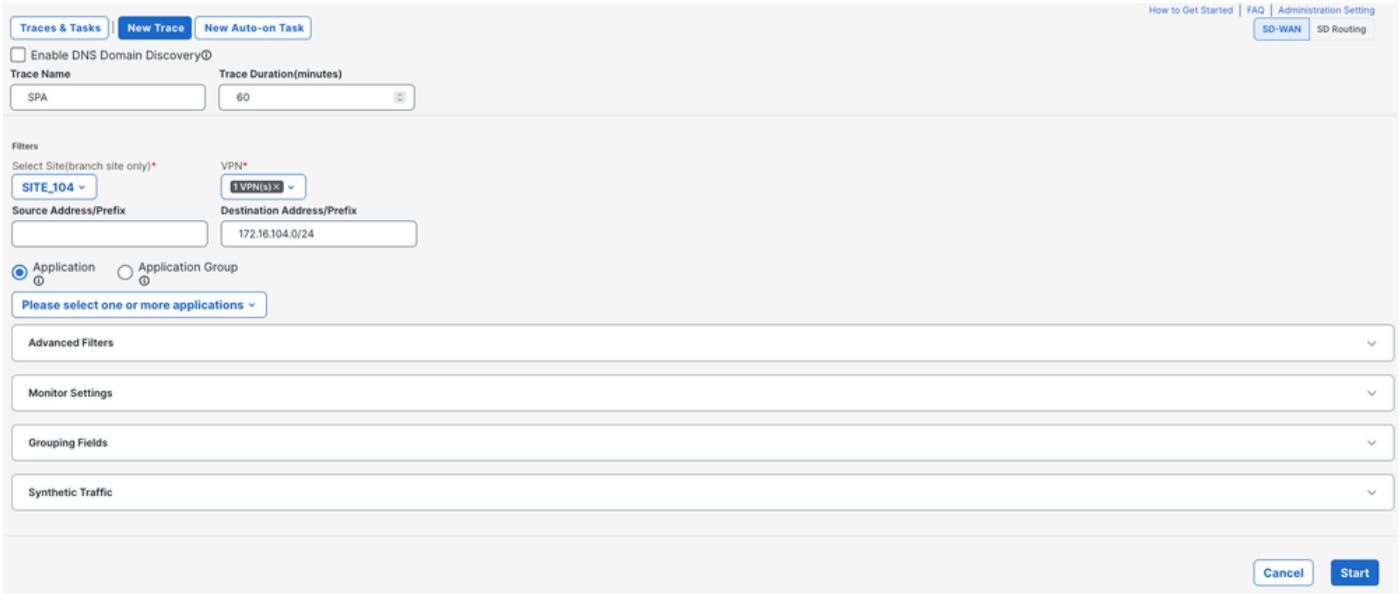


Anmerkung: Vergewissern Sie sich, dass Ihre Standardrichtlinie mit aktivierter Protokollierung standardmäßig deaktiviert ist.

Catalyst SD-WAN Manager - Netzwerkweite Pfadeinblicke

Navigieren Sie zum Catalyst SD-WAN Manager:

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

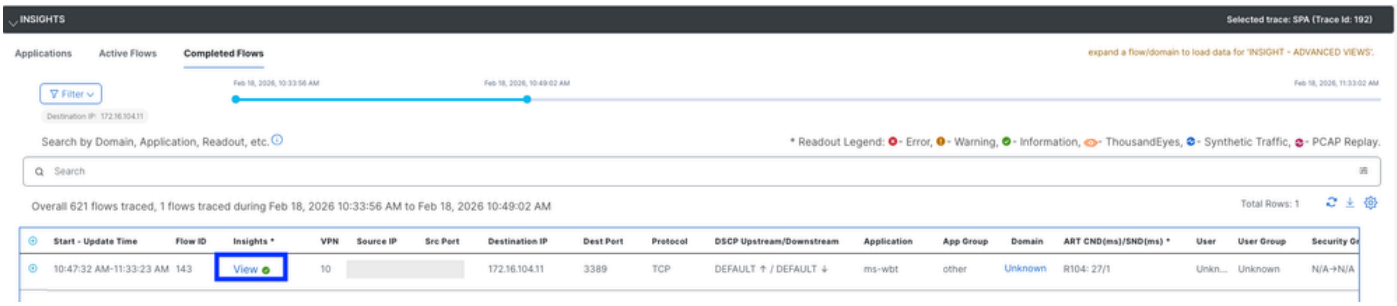


- Trace Name: (Optional) Trace-Name angeben

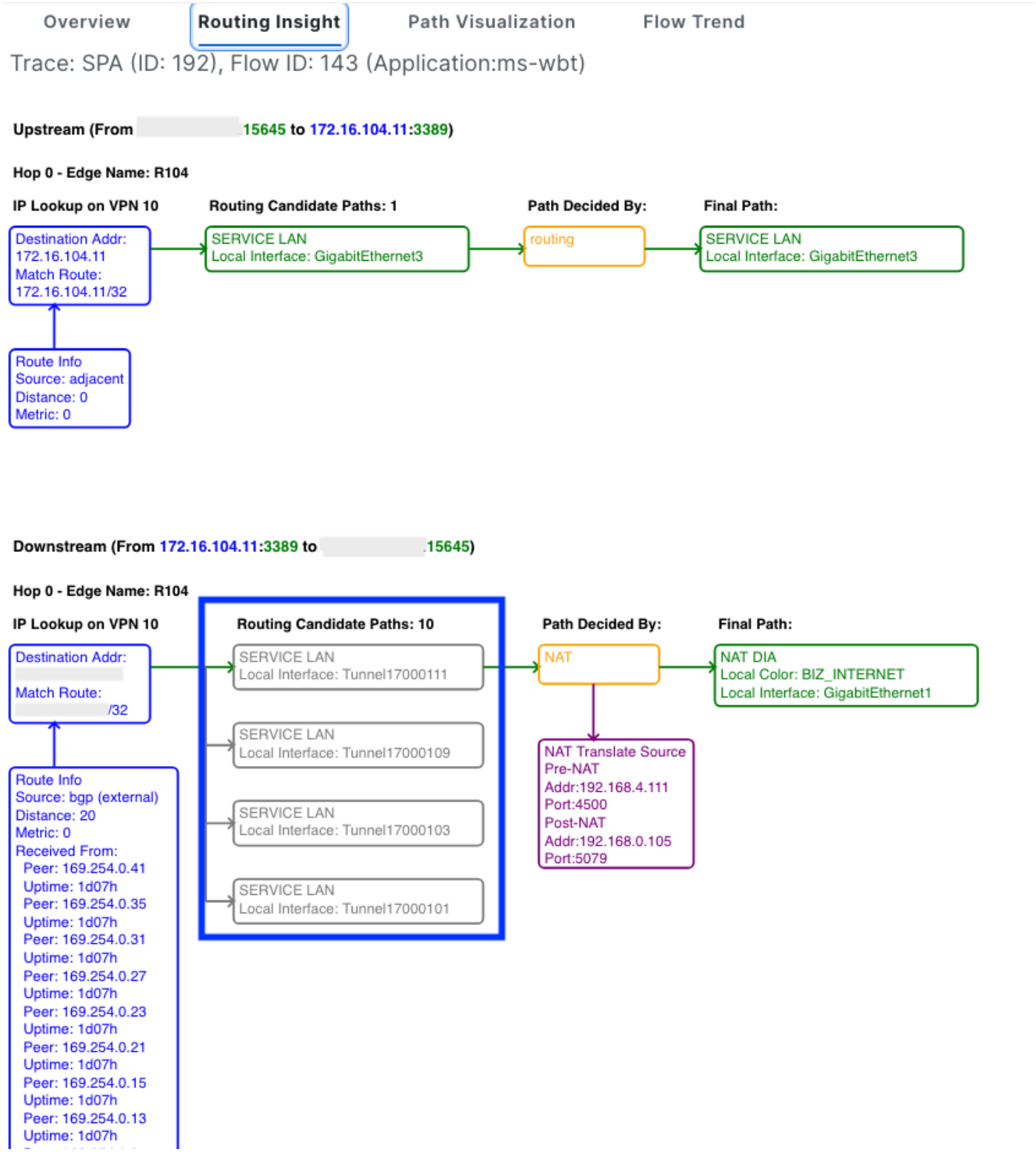
- Site: Standort auswählen, an dem sich die private Ressource befindet
- VPN: Wählen Sie die VPN-ID, in der sich die private Ressource befindet.
- Source/Destination Address: (Optional) Geben Sie die IP-Adresse ein, oder lassen Sie sie leer, um den gesamten Datenverkehr zu erfassen, der basierend auf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

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.



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.