Configuración de Secure Access con túneles automatizados Catalyst SD-WAN para acceso privado seguro

Contenido

Introducción

Este documento describe cómo configurar Secure Access con los túneles automatizados Catalyst SD-WAN para Secure Private Access.

Antecedentes

A medida que las organizaciones van más allá de las redes tradicionales basadas en perímetro, el acceso seguro a los recursos privados adquiere la misma importancia que la seguridad del tráfico de Internet. Las aplicaciones ya no se limitan a un único Data Center, sino que ahora se ejecutan en entornos in situ, nubes públicas y arquitecturas híbridas. Este cambio requiere un enfoque más flexible y moderno del acceso privado.

Aquí es donde entran en juego la arquitectura basada en SASE y Cisco Secure Access. En lugar de depender de concentradores VPN antiguos y de acceso de red plana, Cisco Secure Access proporciona conectividad privada como un servicio prestado en la nube, combinando VPN como servicio (VPNaaS) y acceso a red de confianza cero (ZTNA).

Para el acceso privado a nivel de red, Cisco Secure Access se integra con SD-WAN mediante túneles IPsec de sitio a sitio automatizados. Estos túneles permiten que el tráfico privado fluya de forma segura entre Secure Access y las redes en las instalaciones o en la nube, al tiempo que mantienen la inspección de seguridad y la aplicación de políticas centralizadas en la nube. Desde una perspectiva operativa, esto elimina la necesidad de implementar y mantener cabeceras VPN tradicionales y simplifica la escalabilidad a medida que crecen los entornos.

En un modelo de VPNaaS, Secure Access actúa como el punto de terminación de VPN en la nube. La SD-WAN gestiona el routing inteligente y la resistencia con Secure Access y garantiza que el tráfico esté protegido y regulado por políticas de seguridad coherentes antes de llegar a los recursos privados.

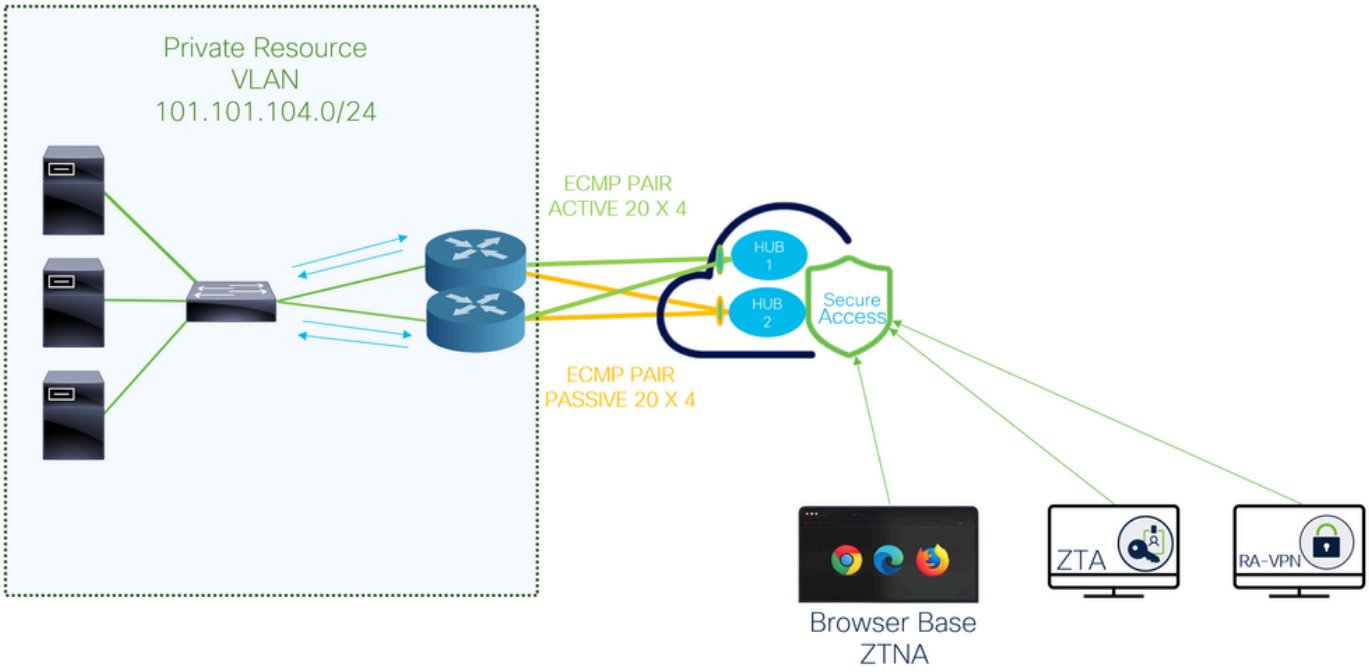
Cisco Secure Access también es compatible con arquitecturas avanzadas de túnel de sitio a sitio, incluida la red de retorno multiregional. Esta capacidad permite a las organizaciones establecer túneles a varias regiones de Secure Access simultáneamente, lo que proporciona redundancia geográfica y una mayor disponibilidad. Al conectarse a diferentes regiones, el tráfico puede fallar automáticamente en caso de interrupciones regionales, degradación de la latencia o eventos de mantenimiento.

Por ejemplo, una organización puede establecer túneles de sitio a sitio desde su entorno SD-WAN a las regiones Secure Access de Londres y Alemania. Ambos túneles permanecen activos, lo que permite un acceso privado resistente entre regiones y garantiza la continuidad incluso si una región deja de estar disponible. Este diseño multiregional refuerza la alta disponibilidad, mejora la tolerancia a fallos y se ajusta a los requisitos de resistencia de clase empresarial.

Para obtener un acceso más granular, Cisco Secure Access aplica el modelo de acceso a red de confianza cero (ZTNA). En lugar de conceder a los usuarios una amplia conectividad de red, ZTNA permite el acceso solo a aplicaciones específicas, en función de la identidad, el estado del dispositivo y el contexto. Este enfoque reduce significativamente la superficie de ataque y se alinea con los principios de confianza cero.

El acceso ZTNA se habilita a través de una combinación de túneles de sitio a sitio y conectores de recursos. Los conectores de recursos son appliances virtuales ligeros que establecen conexiones de salida únicamente a Secure Access, lo que significa que los recursos privados nunca tienen que exponerse directamente a Internet.

Diagrama de la red



Prerequisites

Requirements

- Conocimiento de Secure Access
- Cisco Catalyst SD-WAN Manager versión 20.18.2 y Cisco IOS XE Catalyst SD-WAN versión 17.18.2 o posterior
- Conocimiento intermedio de routing y switching
- Conocimiento de ECMP
- Conocimiento de VPN

- Dado que esta integración no está sujeta a disponibilidad controlada, debe enviar un caso de TAC para solicitar que se habilite la función en Cisco Secure Access

Componentes Utilizados

- Arrendatario de acceso seguro
- Catalyst SD-WAN Manager versión 20.18.2 y Cisco IOS XE Catalyst SD-WAN versión 17.18.2
- Administrador Catalyst SD-WAN

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

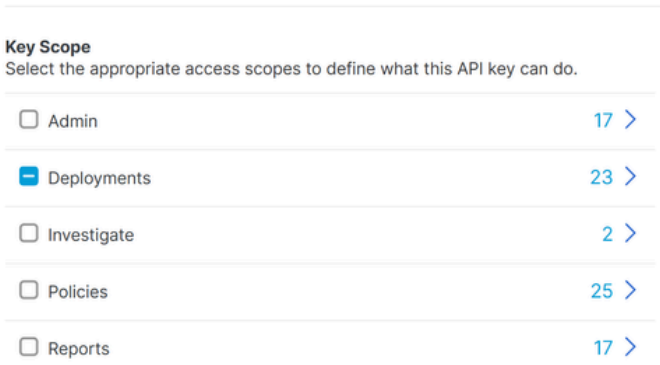
Configuración de Secure Access

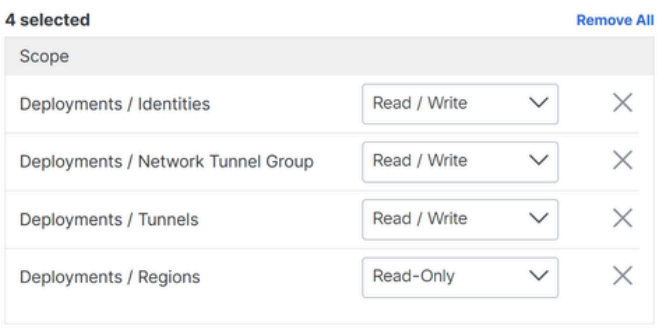
Creación de API

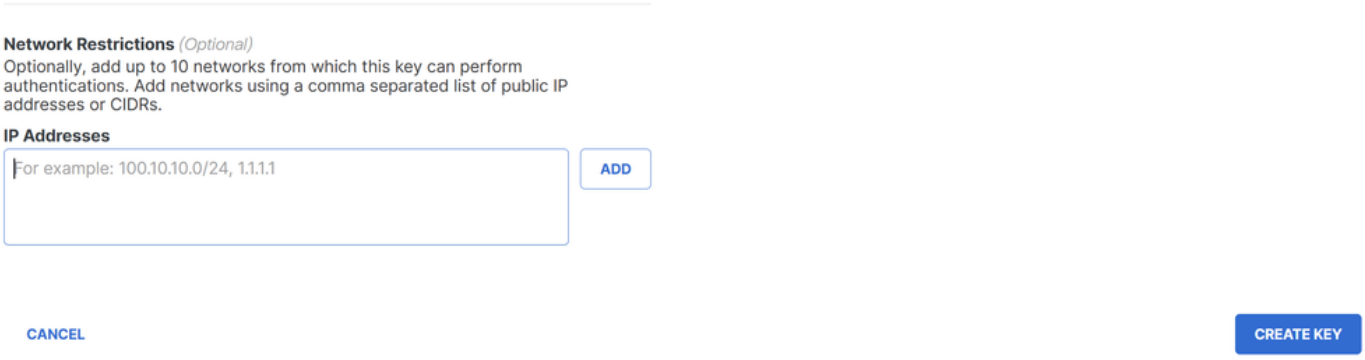
Para crear los túneles automatizados con Secure Access, marque los siguientes pasos:

Vaya a Panel de acceso seguro.

- Haga clic en Admin > API Keys
- Haga clic en Add
- Seleccione las siguientes opciones:
  - Deployments / Network Tunnel Group: Lectura/escritura
  - Deployments / Tunnels: Lectura/escritura
  - Deployments / Regions: Sólo-Lectura
  - Deployments / Identities: Lectura-escritura
  - Expiry Date: Nunca caduca

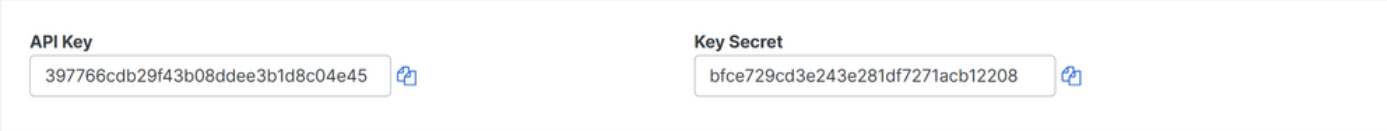






Nota: Opcionalmente, agregue hasta 10 redes desde las cuales esta clave puede realizar autenticaciones. Agregue redes mediante una lista de direcciones IP públicas o CIDR separadas por comas.

- Haga clic CREATE KEY para finalizar la creación de API Key y Key Secret.



Precaución: Copie antes de hacer clic en ACCEPT AND CLOSE; de lo contrario, tendrá que crearlos de nuevo y eliminar los que no se copiaron.

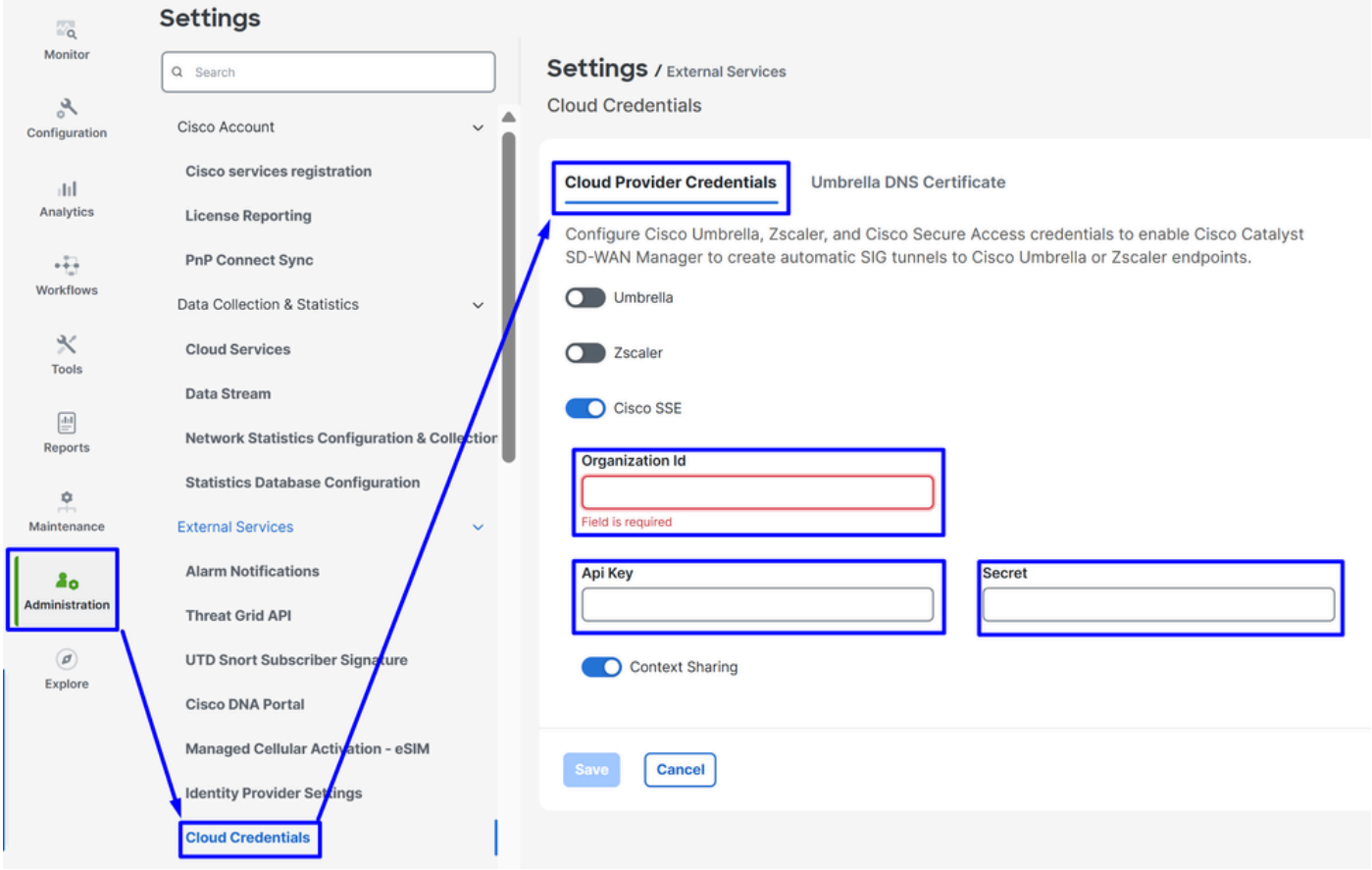
A continuación, para finalizar, haga clic en ACCEPT AND CLOSE.

Configuración de SD-WAN

Integración de API

Vaya a Catalyst SD-WAN Manager:

- Haga clic en **Administration** >Settings> Cloud Credentials
- A continuación, haga clic en Cloud Provider Credentials , active Cisco SSEy rellene los parámetros de organización y API



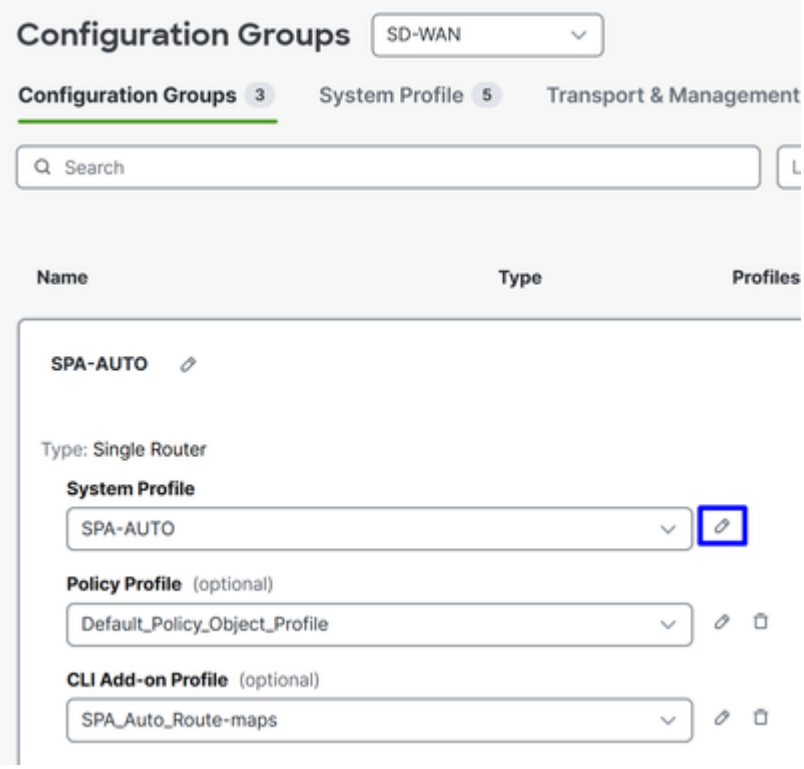
- **Organization ID**: Puede tomarlo de la URL del panel de SSE https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Cópielo del paso Configuración de Secure Access
- Secret: cópielo del paso Configuración de Secure Access

Luego, haga clic en el Save botón.

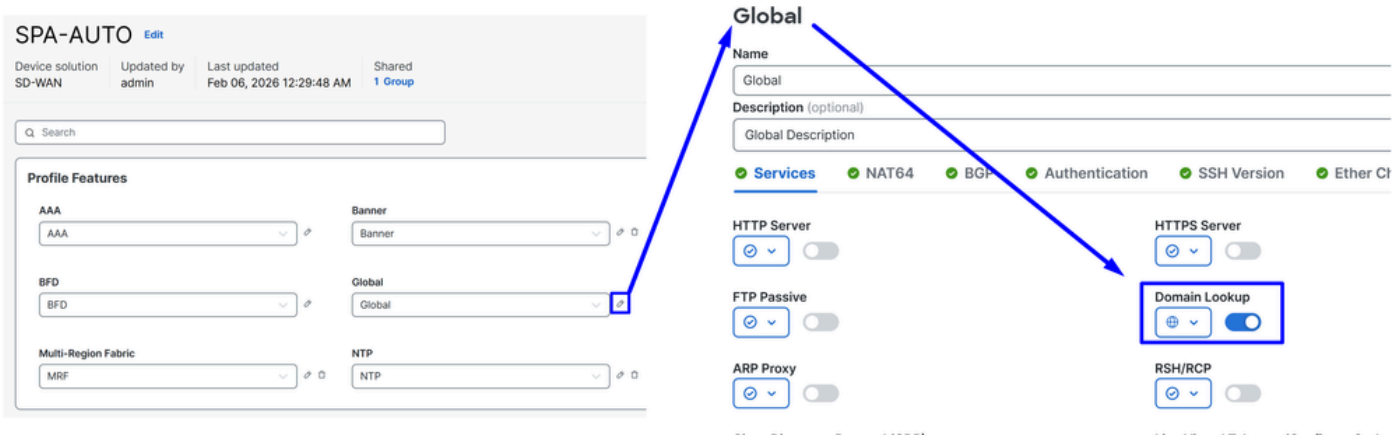
Nota: Antes de continuar con los siguientes pasos, debe asegurarse de que el administrador de SD-WAN y los extremos de Catalyst SD-WAN tengan resolución DNS y acceso a Internet.

Para comprobar si la búsqueda de DNS está activada, vaya a:

- Haga clic en Configuration > Configuration Groups .
- Haga clic en el perfil de sus dispositivos periféricos y edite el perfil del sistema



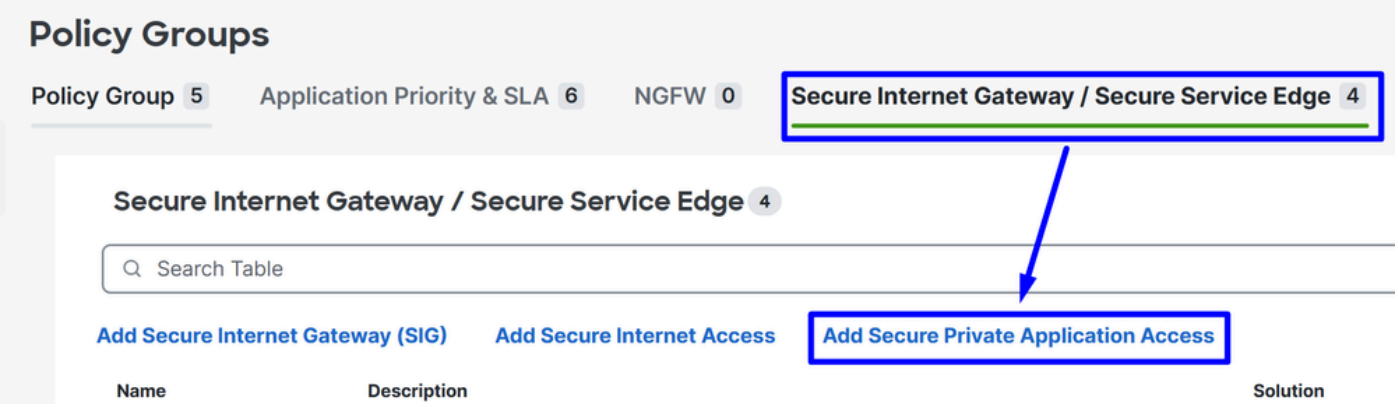
- A continuación, edite la opción Global y asegúrese de que la opción Domain Resolution esté habilitada



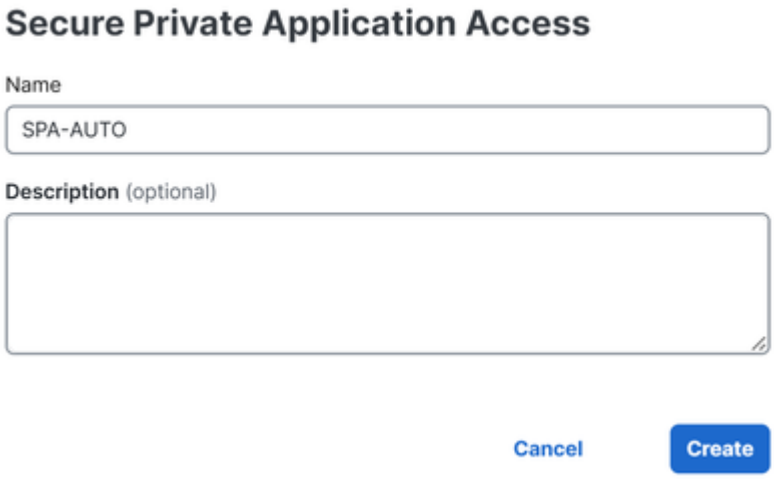
Configurar grupo de políticas

Vaya a Configuration > Policy Groups:

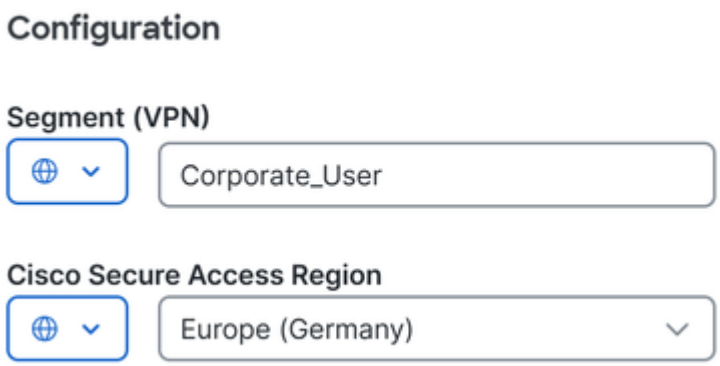
- Haga clic en Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- Configure un nombre y haga clic en Create



Las siguientes configuraciones le permiten crear los túneles después de implementar la configuración en sus Catalyst SD-WAN Edges:

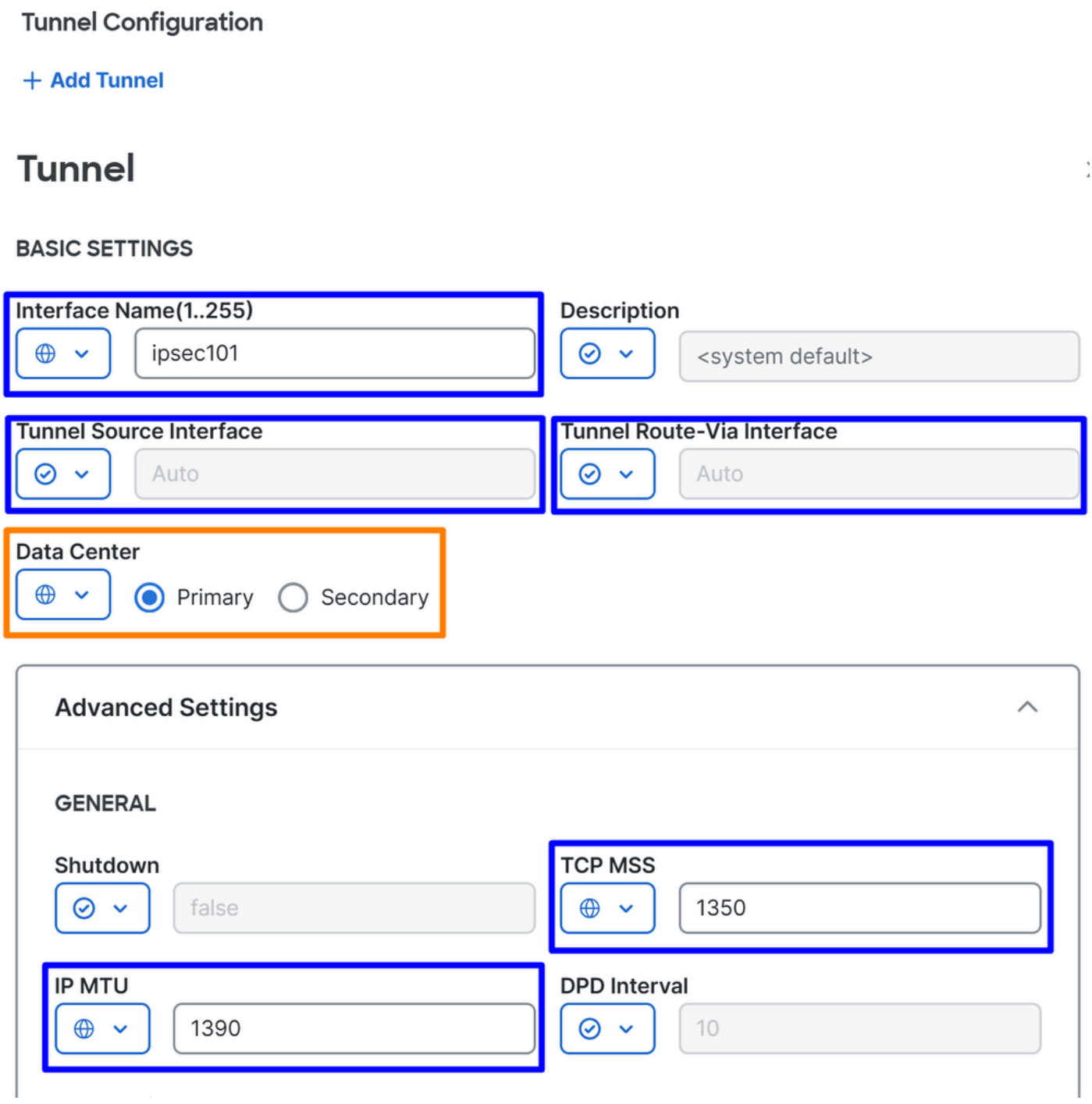


- Configuration
  - Segment (VPN): Elija el VRF que aloja las aplicaciones a las que se accederá a través de Secure Access
  - Cisco Secure Access Region: Elija la región más cercana al hub SD-WAN o la sucursal donde se alojan las aplicaciones

A continuación, defina la configuración del túnel. Los túneles creados para el Data Center de acceso seguro principal están activos, mientras que los túneles creados para el Data Center de

acceso seguro secundario funcionan como copia de seguridad.

En Tunnel Configuration haga clic en + Add Tunnel:



- Tunnel
  - Interface Name: Especifique el nombre del túnel, que se actualiza automáticamente cada vez que se agrega un nuevo túnel
  - Tunnel Source Interface: No es necesario cambiar esta configuración. Cuando se deja como Auto, el sistema crea automáticamente una interfaz de loopback con una máscara /31.
  - Tunnel Route-Via Interface: No es necesario cambiar esta configuración. De forma predeterminada, utiliza la primera interfaz WAN física NAT del router de extremo, pero se puede cambiar si se requiere una interfaz WAN específica
  - Data Center: Seleccione Primary (Primario) o Secondary (Secundario) según corresponda.

Si el túnel principal ya está configurado, seleccione Secundario. En escenarios normales, un túnel se puede configurar como primario y otro como secundario

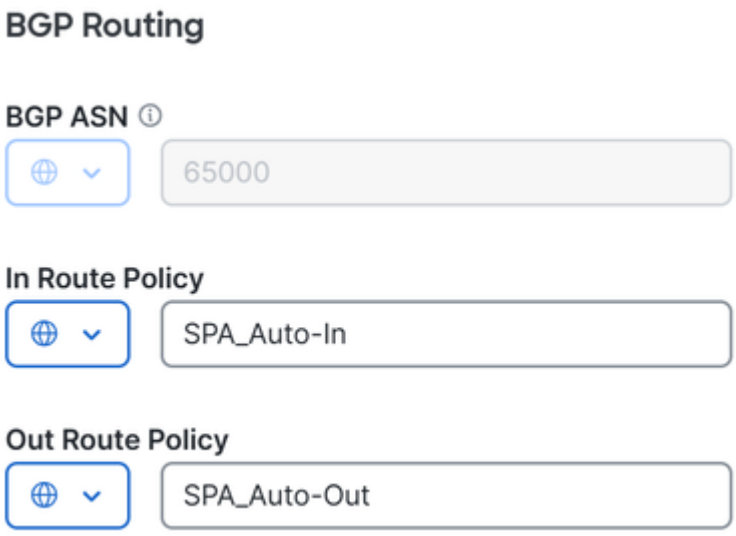
- Advanced Settings
  - IP MTU: Utilizar 1390
  - TCP MSS: Utilizar 1350

Nota: Si desea crear varios túneles para activar ECMP y aumentar la capacidad del túnel, puede configurar hasta 10 túneles de reserva activos/10 por router. Esto proporciona hasta 10 × 4 Gbps por NTG.

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action	
ipsec101		Auto	Auto	Primary		
ipsec102		Auto	Auto	Secondary		
ipsec103		Auto	Auto	Primary		
ipsec104		Auto	Auto	Secondary		
ipsec105		Auto	Auto	Primary		
ipsec106		Auto	Auto	Secondary		
ipsec107		Auto	Auto	Primary		
ipsec108		Auto	Auto	Secondary		
ipsec109		Auto	Auto	Primary		MAXIMUM OF 10 TUNNELS PER HUB
ipsec110		Auto	Auto	Secondary		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		

Nota: Si implementa varios túneles por router, asegúrese de que la interfaz de transporte pueda mantener el ancho de banda agregado de todos los túneles activos combinados. Por ejemplo, si se espera que dos túneles transmitan hasta 1 Gbps cada uno, el enlace de transporte debe admitir al menos 2 Gbps de rendimiento.

Una vez configurados los túneles, continúe con la configuración de BGP.



- **BGP Routing**
  - BGP ASN: Especifique el número AS para el hub SD-WAN. El AS 64512 está reservado para Secure Access y no se puede utilizar. Para obtener más información sobre BGP, consulte
  - In Route Policy: El sistema crea automáticamente esta política de ruta entrante con una deny all sentencia para evitar problemas de ruteo. Se debe modificar manualmente mediante un CLI Add-On Template para permitir/denegar las rutas apropiadas.
  - Out Route Policy: El sistema crea esta política de rutas salientes con una deny all sentencia para evitar problemas de ruteo. Debe editarse manualmente a través de un CLI Add-On Template para permitir/denegar las rutas apropiadas.

Advertencia: A partir de noviembre de 2025, todas las organizaciones Secure Access recién creadas utilizan el ASN 32644 público de forma predeterminada para el peering BGP en los grupos de túnel de red. Las organizaciones existentes establecidas antes de noviembre de 2025 siguen utilizando el ASN 64512 privado que se reservaba anteriormente para los peers BGP de acceso seguro. Si el número AS privado 64512 está asignado a un dispositivo en su red, no podrá establecer un par con un grupo de túnel de red configurado para Peer (Secure Access) BGP AS 64512.

La siguiente configuración BGP y route-map se crea automáticamente para cada vecino BGP después de que usted Deploy la nueva política en su Policy Group.

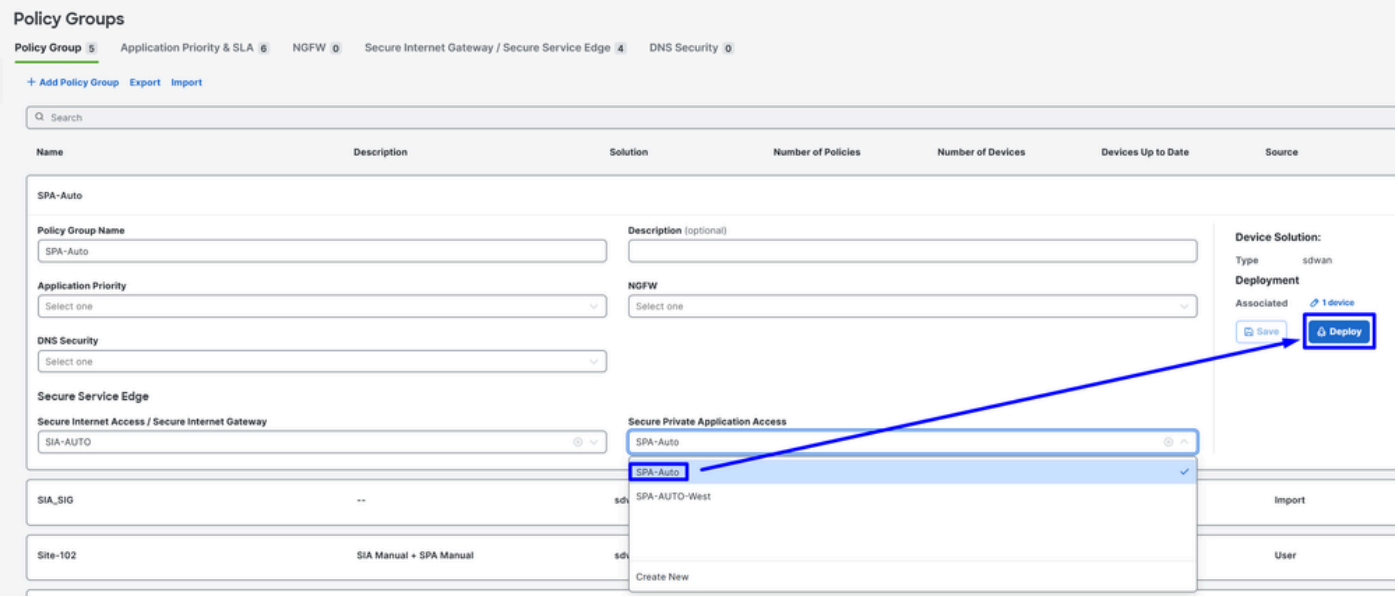
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

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
```

Después de esto, haga clic en Save y continúe con la implementación de la política para activar los túneles.

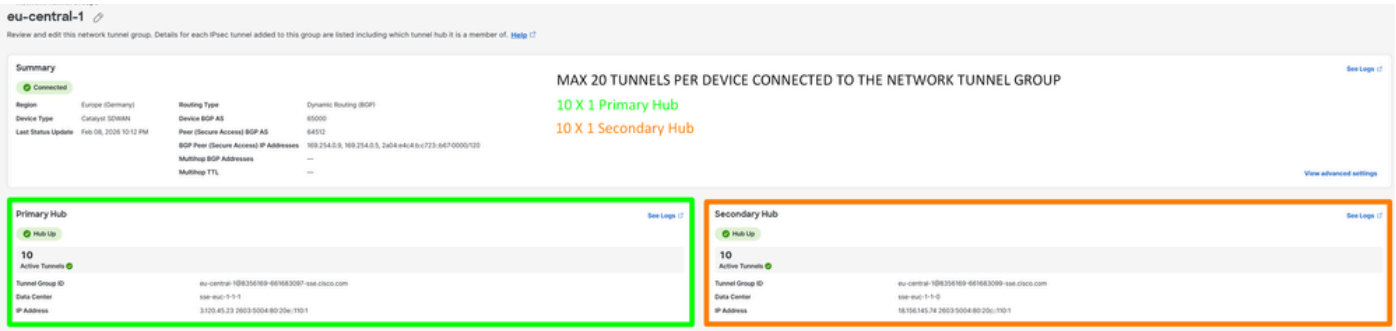
- Haga clic en Configuration > Policy Groups
- Elija en Policy > Secure Service Edge > y haga clic en el perfil creado recientemente para SPA Secure Private Application Access.
- Haga clicDeploypara finalizar



Para verificar enSecure Access, realice los siguientes pasos:

- Haga clic en Connect> Network Connections

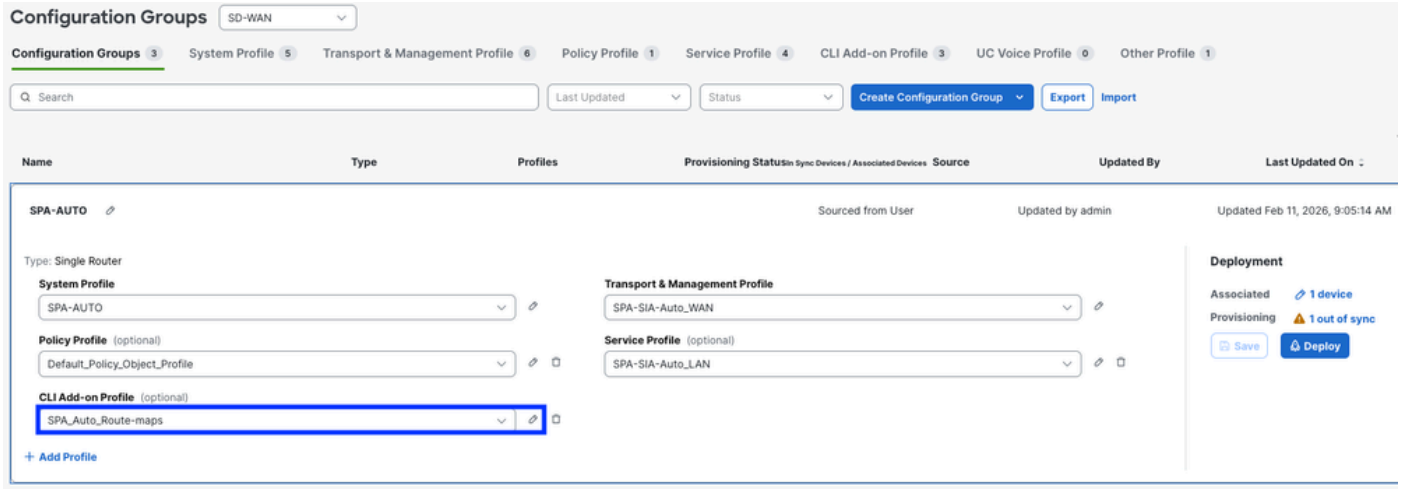
ESTABLECIMIENTO DE TÚNEL



Configuración de

Vaya a Configure > Configuration Groups

- Haga clic en el Configuration Group y cree/edite su CLI Add-on Profile



Para permitir el intercambio de rutas BGP, utilice el In Route Policy y **Out Route Policy**. Puede encontrar un ejemplo básico de la configuración de la CLI Add-On ruta. Esta plantilla proporciona un punto de partida y se debe personalizar según sea necesario:

```
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
```

Advertencia: Se requiere una planificación cuidadosa al definir las redes permitidas dentro y fuera a través de los route-maps BGP. Permitir todas las rutas, como se muestra en el ejemplo anterior, puede introducir un comportamiento de ruteo no deseado. Para una

---

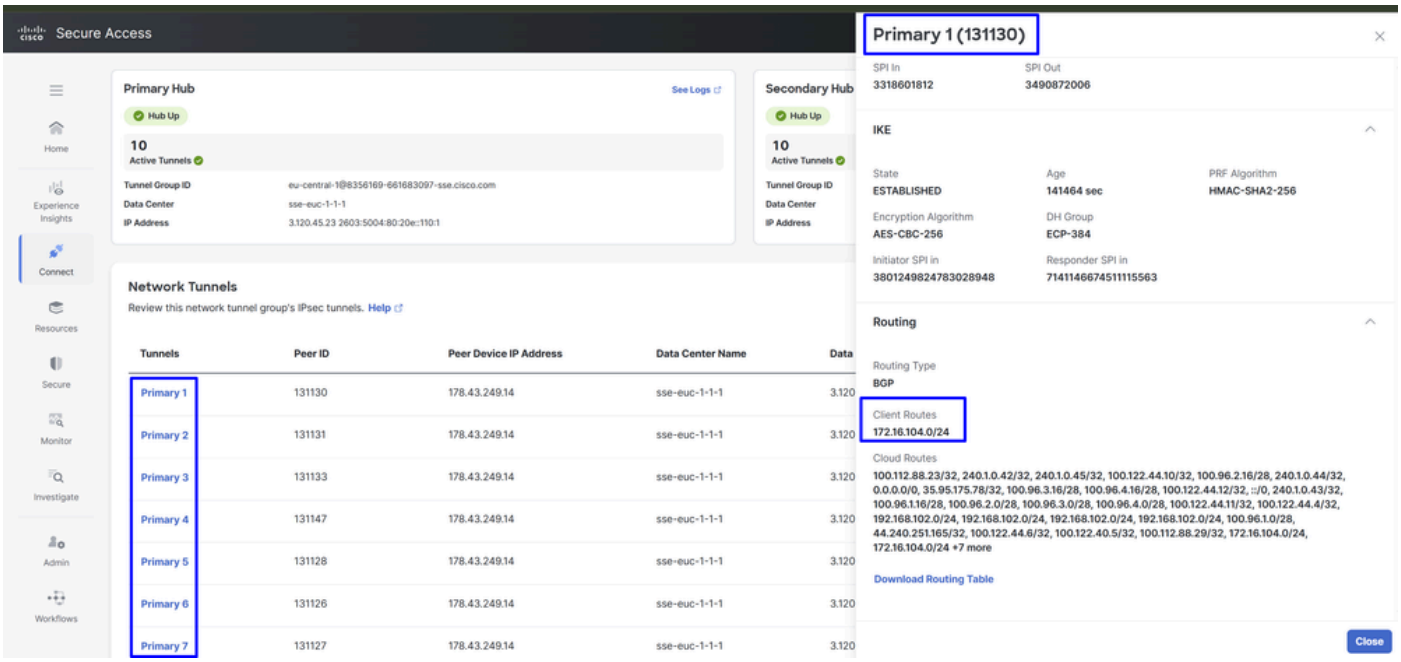
implementación óptima, especifique explícitamente solo las redes necesarias en sus route-maps para garantizar resultados de ruteo controlados y predecibles

Ahora puede continuar con la Deploy the changes

Para verificar si las rutas BGP se reciben enSecure Access, verifique los siguientes pasos:

- Haga clic en Connect> Network Connections > Network Tunnel Groups y escriba select el nombre de NTG

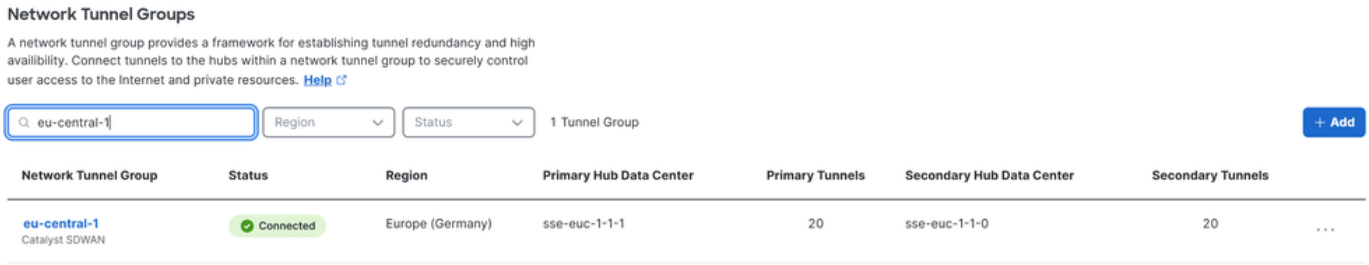
ESTABLECIMIENTO DE RUTEO



Nota: En este ejemplo, la subred del usuario corporativo 172.16.104.0/24 se anuncia a Secure Access a través de BGP. Esto permite un routing adecuado entre Catalyst SD-WAN y el entorno SSE.

La misma política se puede aplicar a ambos extremos de la WAN en los hubs Catalyst SD-WAN, lo que da como resultado 20 túneles activos y 20 túneles en espera. El número total de túneles depende de la cantidad configurada en cada borde. Cualquier router conectado a ambos hubs de acceso seguro (Hub 1 y Hub 2) forma un par ECMP a través de todos los túneles establecidos.

Por ejemplo, si Catalyst SD-WAN Edge 1 tiene 10 túneles y Catalyst SD-WAN Edge 2 tiene 10 túneles, Secure Access forma ECMP a través de los 20 túneles activos. El mismo comportamiento se aplica al hub SSE secundario.

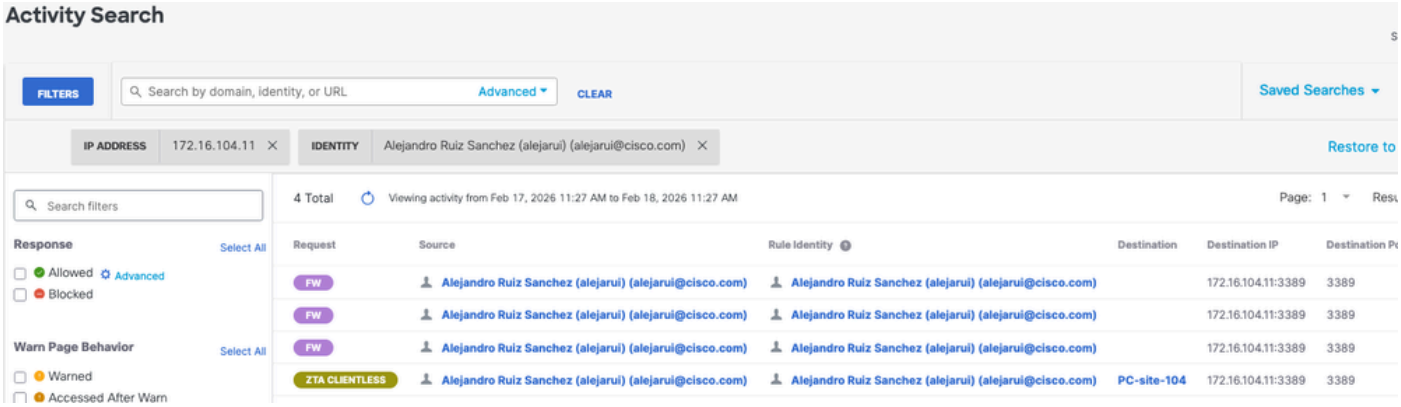


Verificación

para verificar si el tráfico pasa a través de Cisco Secure Access, navegue hasta Eventso Activity Search o y Network-Wide Path Insightsfiltre por su identidad de túnel:

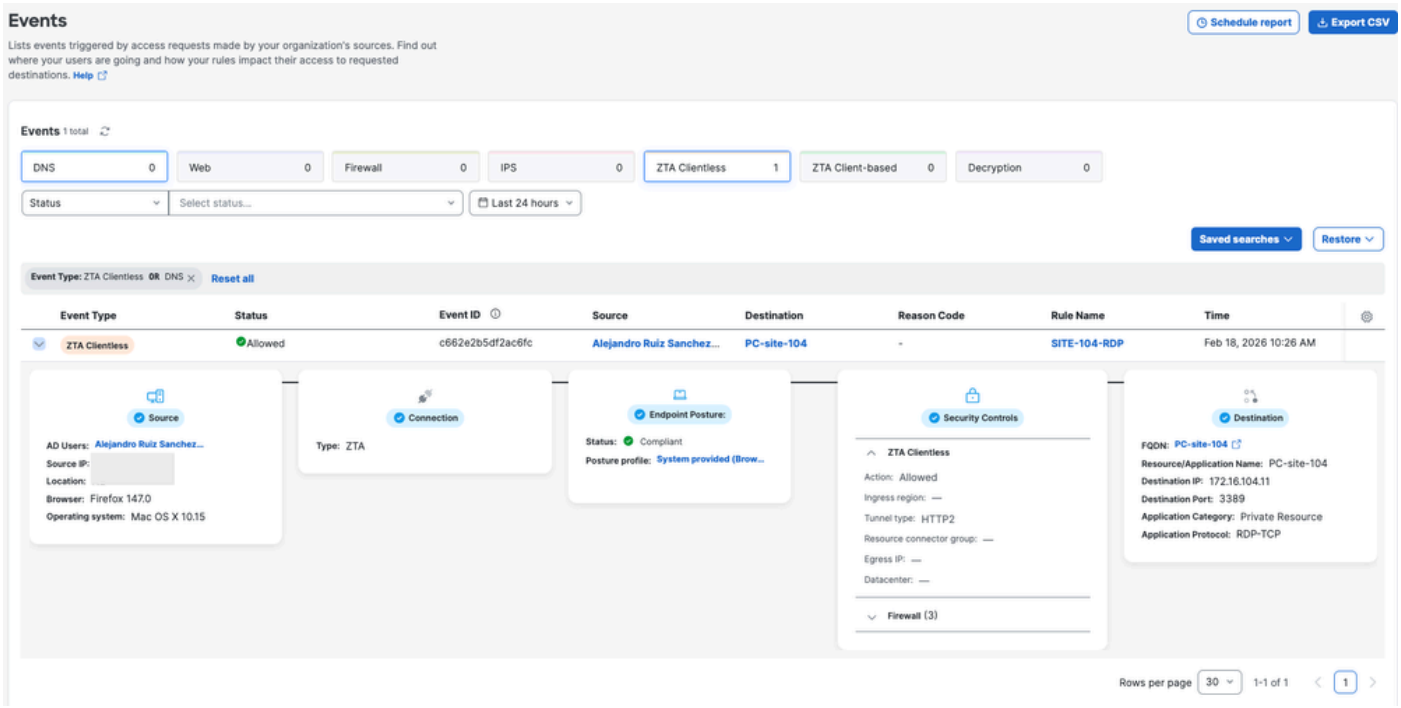
Acceso seguro - Búsqueda de actividad

Vaya a Monitor>Activity Search :



Acceso seguro - Eventos

Vaya a Monitor>Events:

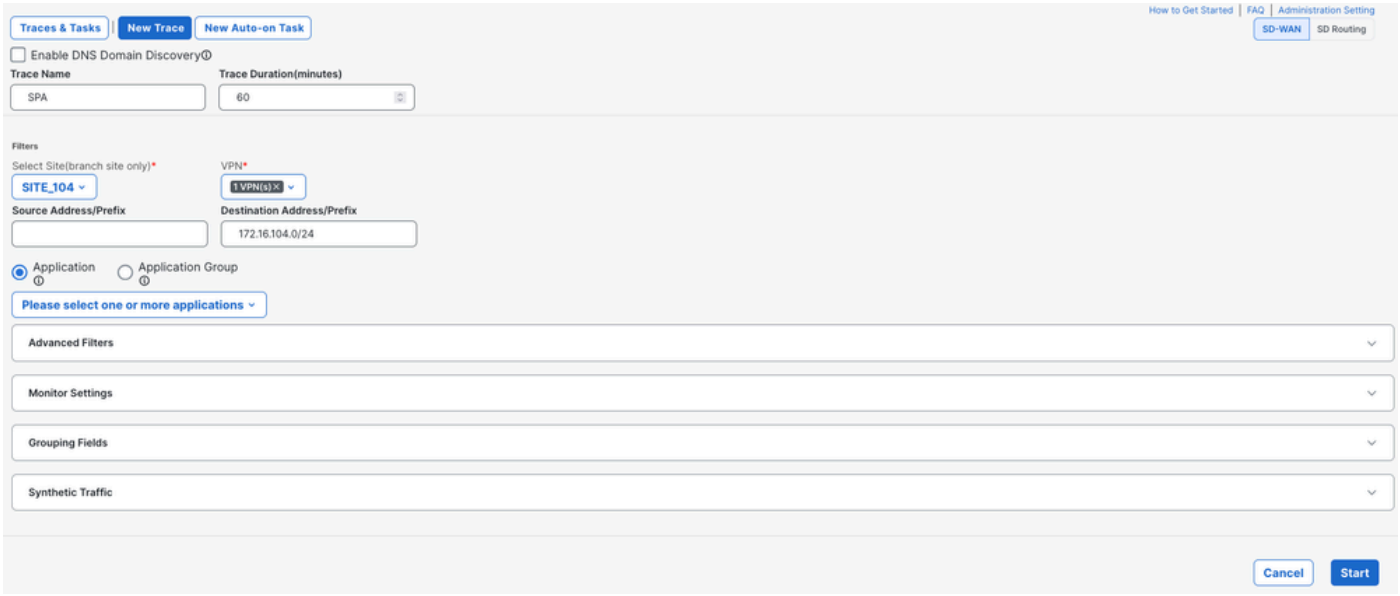


Nota: Asegúrese de que tiene la política predeterminada con el registro activado; de forma predeterminada, esta opción está desactivada.

Catalyst SD-WAN Manager: Network-Wide Path Insights

Vaya a Catalyst SD-WAN Manager:

- Haga clic en Tools> Network-Wide Path Insights
- Haga clic en New Trace

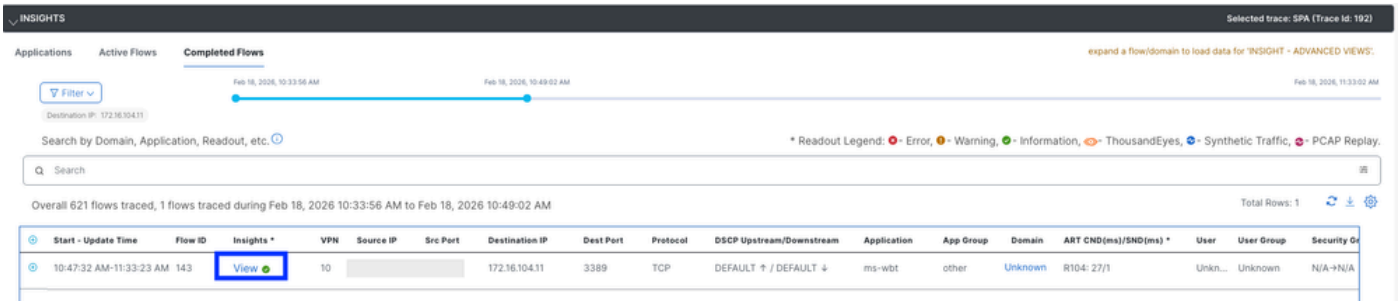


- Trace Name: (Opcional) Especifique el nombre de seguimiento

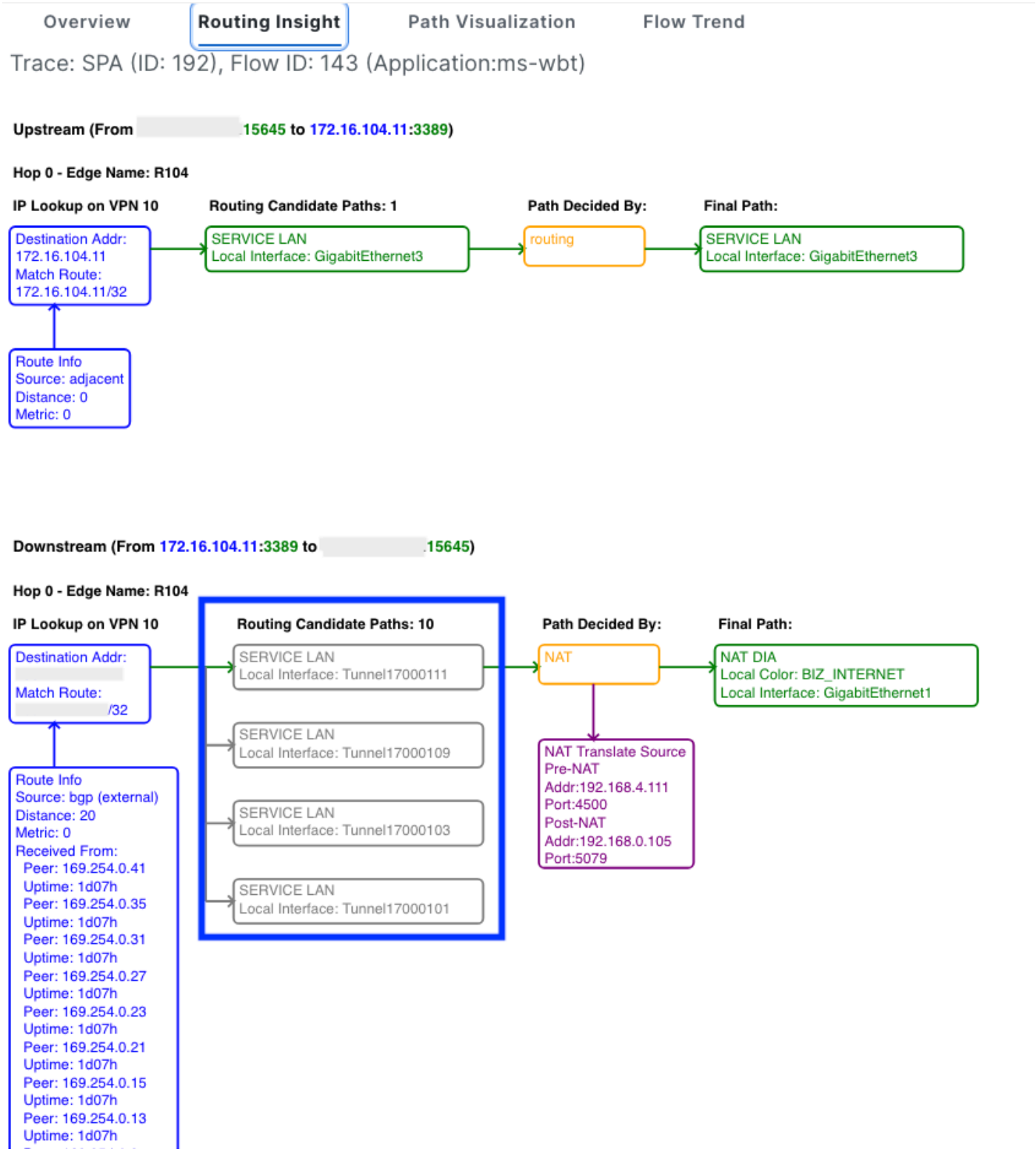
- Site: Elija el sitio donde se encuentra el recurso privado
- VPN: Elija el ID de VPN donde se encuentra el recurso privado
- Source/Destination Address: (Opcional) Introduzca la IP o déjela en blanco para capturar todo el tráfico filtrado basado en **Site** y VPN elegido

Iniciar el seguimiento

Localice el flujo de tráfico y haga clic en Ver en la columna Perspectivas.



La columna routing Insights muestra las rutas candidatas y los túneles IPSec para Secure Access



Información Relacionada

- Soporte técnico y descargas de Cisco
- Centro de ayuda de Cisco Secure Access
- Guía de diseño de Cisco SASE
- Configuración del acceso seguro con túneles automatizados SD-WAN para un acceso seguro a Internet

- Guía de Configuración de Seguridad de Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN Release 17.x
- Solución Cisco SASE: Guía rápida de Cisco Catalyst SD-WAN integrado con Cisco Secure Access

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).