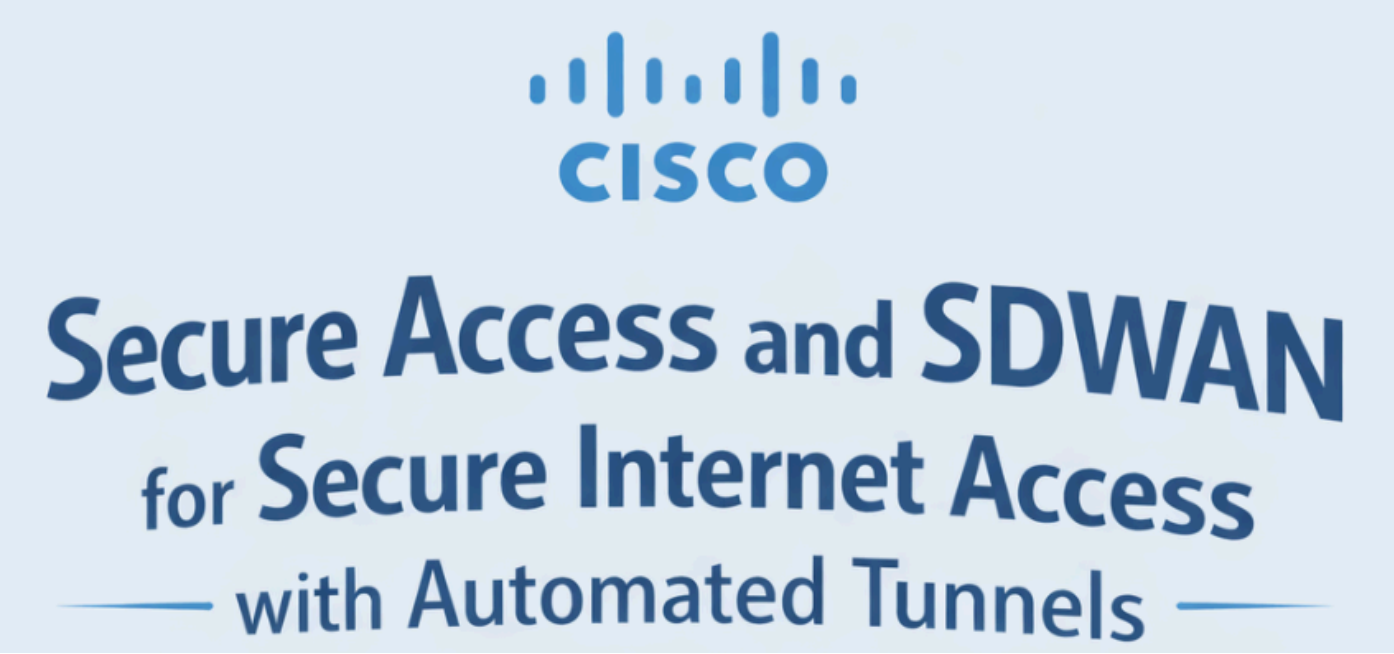
# Configuración del acceso seguro con túneles automatizados SD-WAN para un acceso seguro a Internet

## Contenido



## Introducción

Este documento describe cómo configurar Secure Access con túneles automatizados SD-WAN para Secure Internet Access.



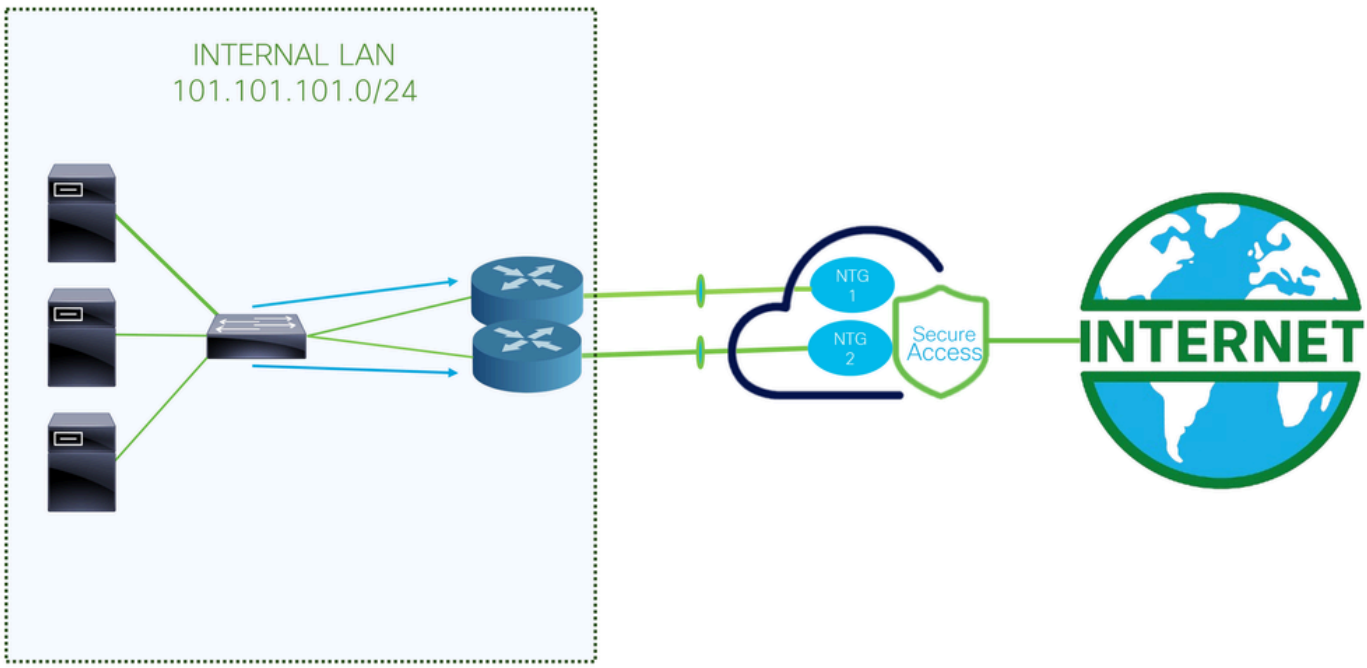

## Antecedentes

A medida que las organizaciones adoptan cada vez más aplicaciones basadas en la nube y prestan apoyo a los empleados distribuidos, las arquitecturas de red deben evolucionar para proporcionar un acceso seguro, fiable y escalable a los recursos. Secure Access Service Edge (SASE) es un marco que converge la red y la seguridad en un único servicio proporcionado en la nube, que combina las capacidades de SD-WAN con funciones de seguridad avanzadas como Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), seguridad de capa DNS, Zero Trust Network Access (ZTNA) o VPN integrada para un acceso remoto seguro.

La integración de Cisco Secure Access con SD-WAN a través de túneles automatizados permite a las organizaciones enrutar el tráfico de Internet de forma segura y eficiente. La SD-WAN ofrece una selección inteligente de rutas y una conectividad optimizada entre ubicaciones distribuidas, mientras que Cisco Secure Access garantiza que todo el tráfico se inspecciona y protege de acuerdo con las políticas de seguridad corporativas antes de llegar a Internet.

Al automatizar la configuración de túneles entre los dispositivos SD-WAN y Secure Access, las organizaciones pueden simplificar la implementación, mejorar la escalabilidad y garantizar una aplicación de seguridad uniforme para los usuarios, independientemente de dónde se encuentren. Esta integración es un componente clave de una arquitectura SASE moderna, que permite un acceso seguro a Internet para sucursales, sitios remotos y usuarios móviles.

## Diagrama de la red




Esta es la arquitectura utilizada para este ejemplo de configuración. Como puede ver, hay dos routers de borde:

Si decide implementar las políticas en dos dispositivos diferentes, se configura un NTG para cada router y se habilita NAT en el lado de Secure Access. Esto permite que ambos routers envíen tráfico desde la misma fuente a través de los túneles. Normalmente, esto no está permitido; sin embargo, habilitar la opción NAT para estos túneles permite que dos routers de borde envíen tráfico originado en la misma dirección de origen.

# Prerequisites

## Requirements

- Conocimiento de Secure Access
- Cisco Catalyst SD-WAN Manager versión 20.15.1 y Cisco IOS XE Catalyst SD-WAN versión 17.15.1 o posterior
- Conocimiento intermedio de routing y switching
- Conocimiento de ECMP
- Conocimiento de VPN

## Componentes Utilizados

- Arrendatario de acceso seguro
- Catalyst SD-WAN Manager versión 20.18.1 y Cisco IOS XE Catalyst SD-WAN versión 17.18.1
- 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

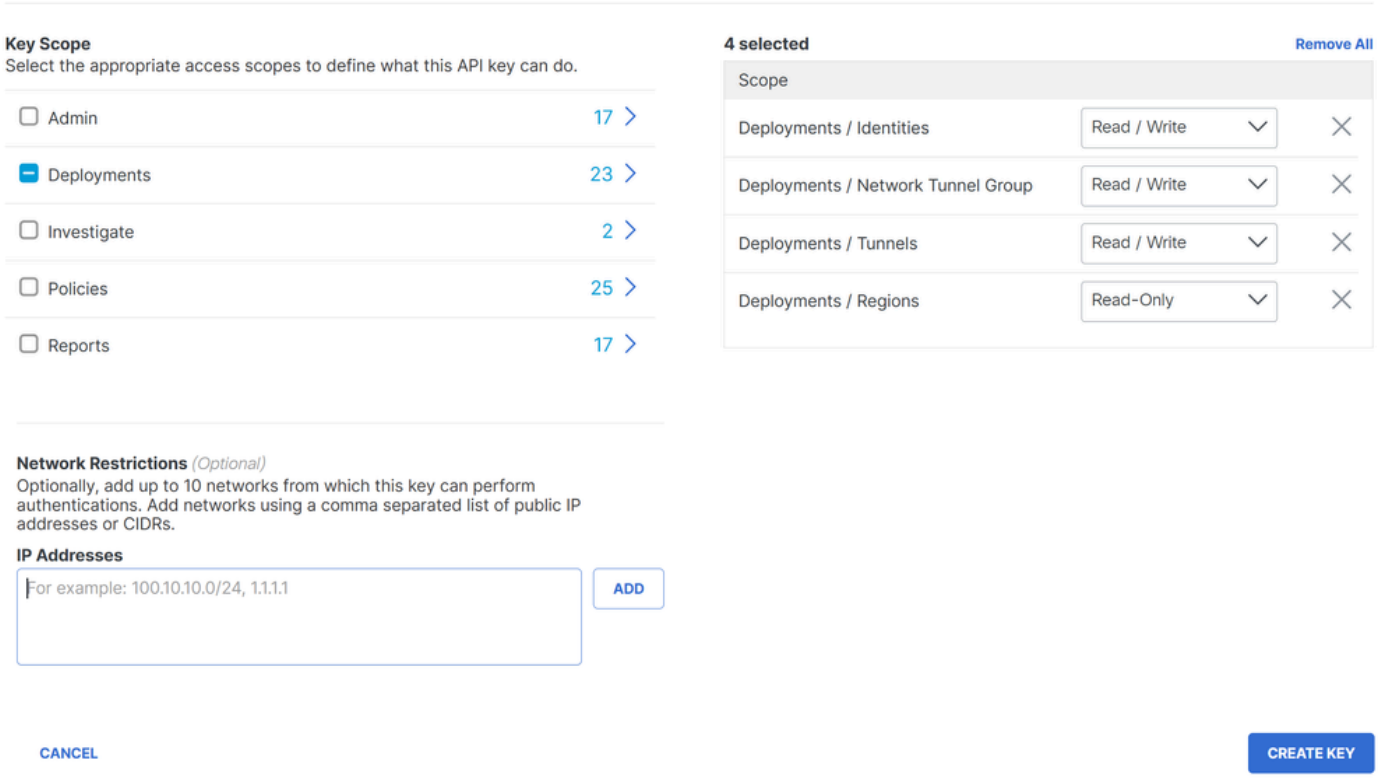
## Configuración de Secure Access

### Creación de API

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

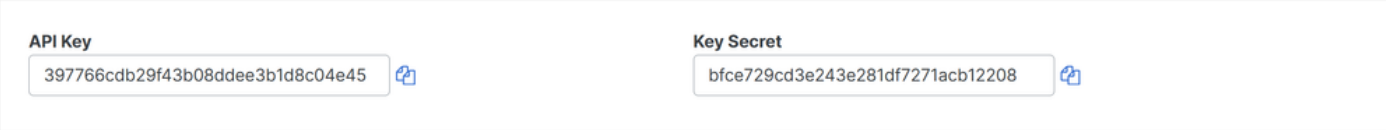
Vaya a [Panel de acceso seguro](#).

- 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.

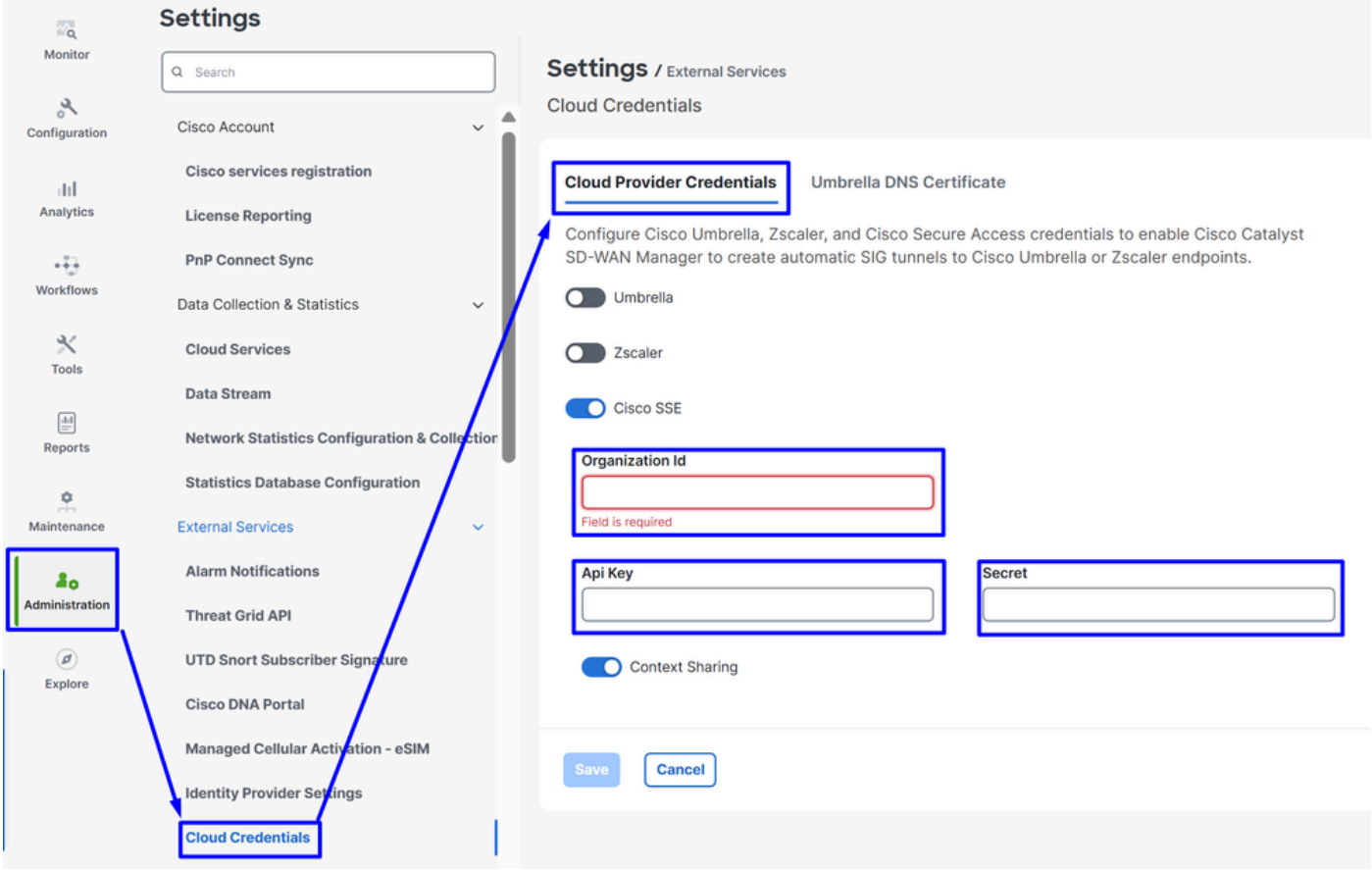
A continuación, para finalizar, haga clic en ACCEPT AND CLOSE.

## 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.

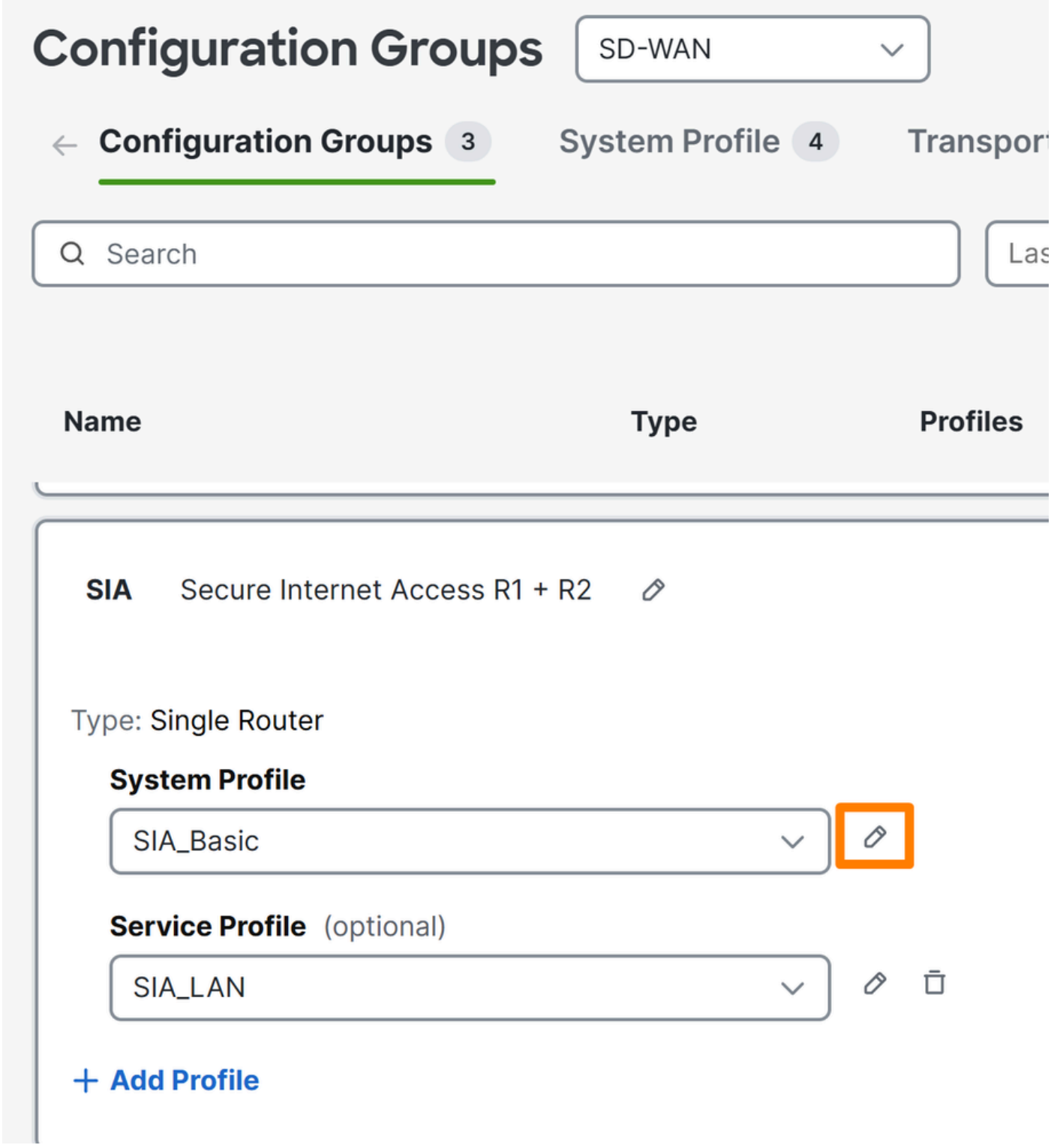
---

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.

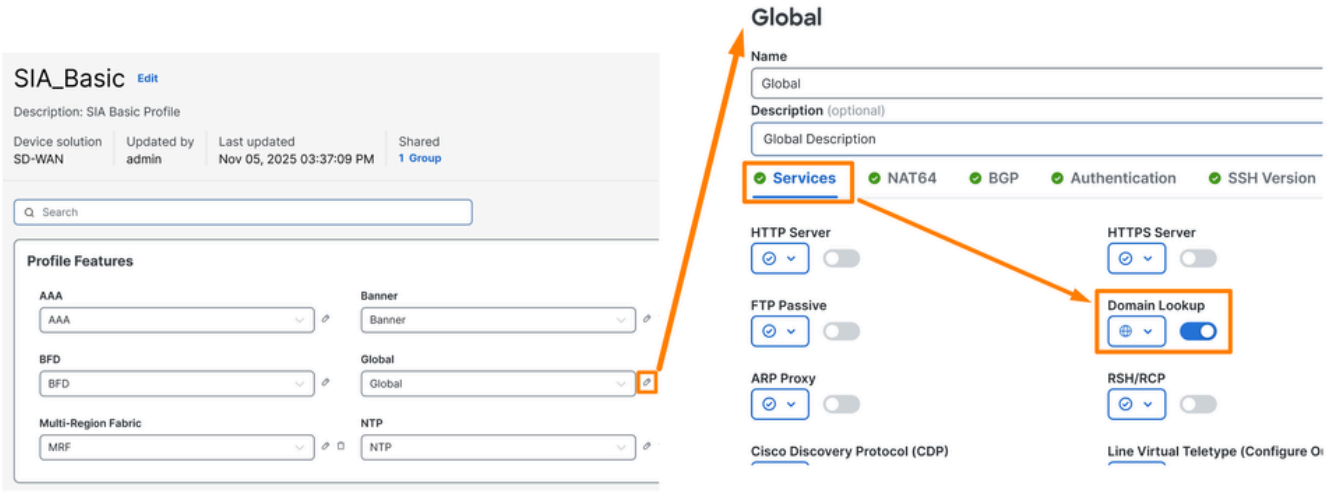
---

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



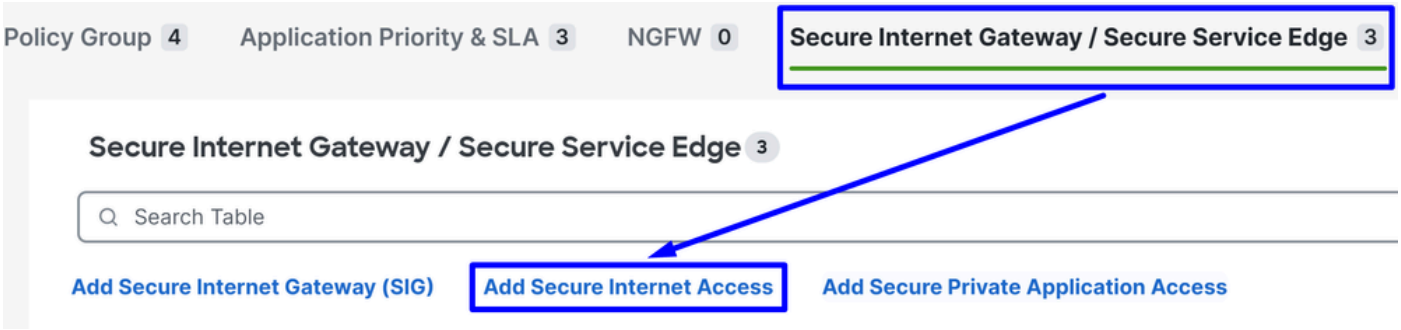

- A continuación, edite la opción Global y asegúrese de que la opción Domain Resolution esté habilitada




Configurar grupo de políticas

Vaya a Configuration > Policy Groups:

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

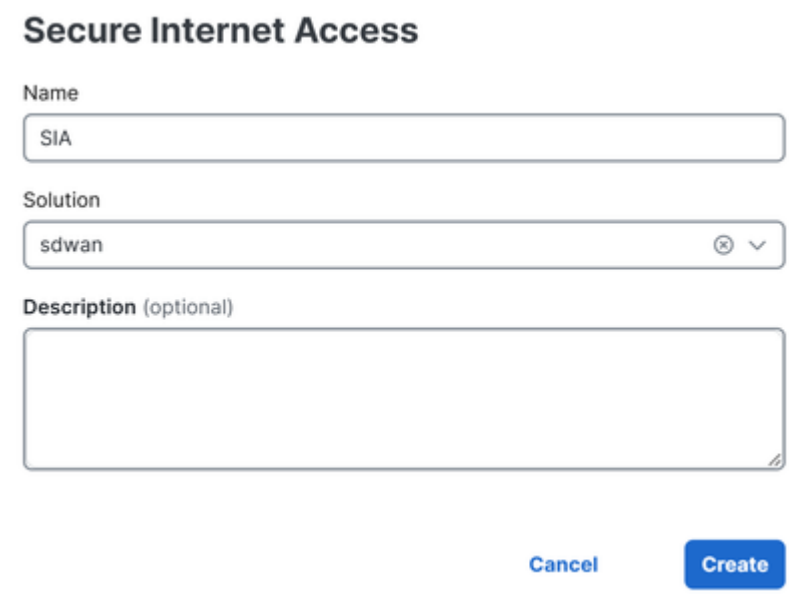



---

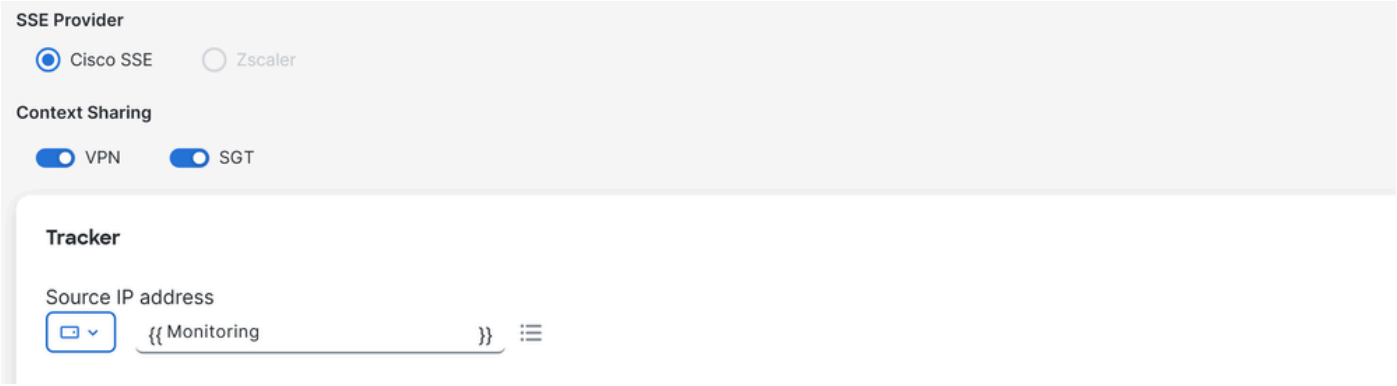
Nota: En versiones anteriores a la 20.18, esta opción se denomina Agregar extremo de servicio seguro (SSE)

---

- Configure un nombre, una solución y haga clic en Create

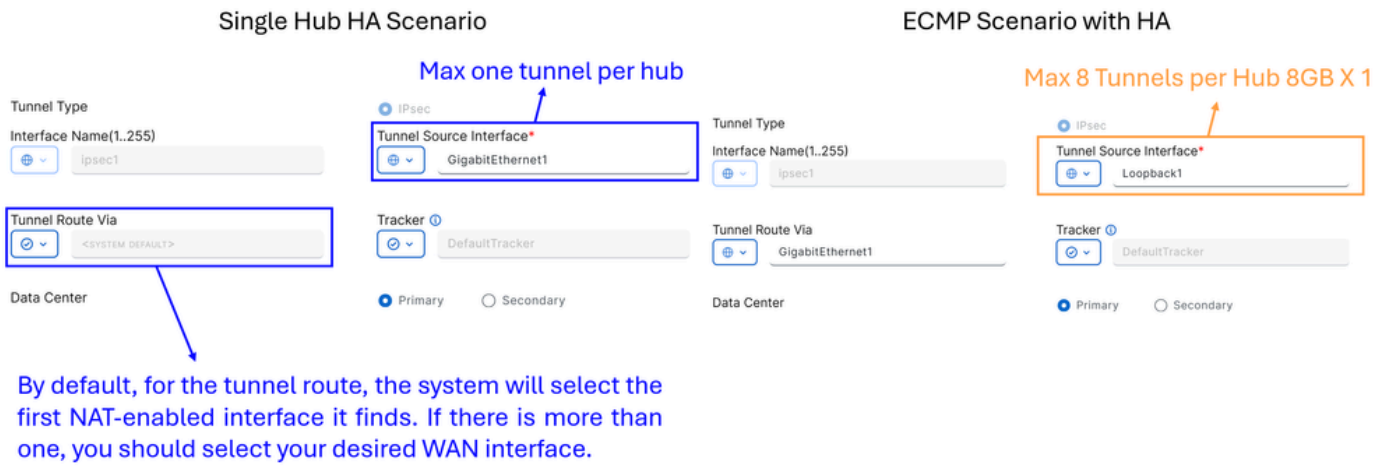



Las siguientes configuraciones le permiten crear los túneles después de implementar la configuración en sus Catalyst SD-WAN Edges:




- SSE Provider: SSE
- Context Sharing: Elija VPN o SGT según sus necesidades
- Tracker
  - **Source IP Address**: Elegir dispositivo específico (esto le permite modificarlo por dispositivo e identificar el caso práctico en la fase de implementación)

En el Configuration paso que configure los túneles:




- **Single Hub HA Scenario**: En esta situación, puede configurar la alta disponibilidad utilizando un NTG como activo y otro como pasivo, con un rendimiento máximo de 1 Gbps por NTG
- ECMP Scenario with HA: En este escenario, puede configurar hasta 8 túneles por hub, admitiendo un total de hasta 16 túneles por NTG. Esta configuración permite un mayor rendimiento en los túneles

---

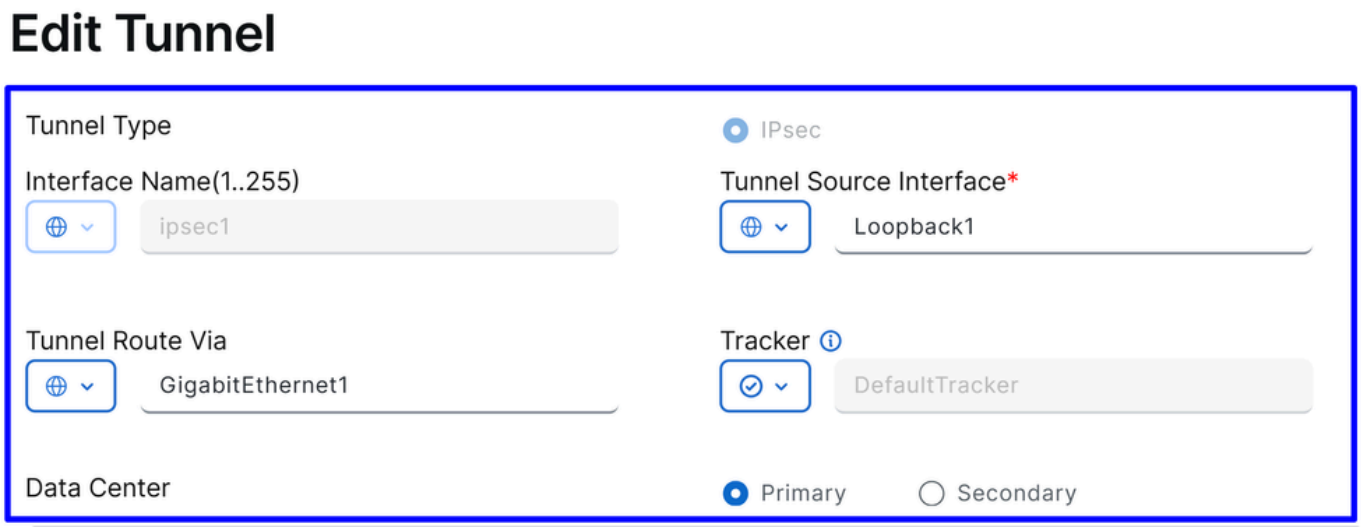
Nota: Si las interfaces de red tienen un rendimiento superior a 1 Gbps y necesita escalabilidad, debe utilizar interfaces de bucle invertido. De lo contrario, puede utilizar interfaces estándar en el dispositivo. Esto es para habilitar ECMP desde el lado de Secure Access.

---

Advertencia: Si desea configurar las interfaces de loopback para un escenario ECMP, primero debe configurar las interfaces de loopback en Configuration Groups > Transport & Management Profile, bajo la política que utilice en su router.

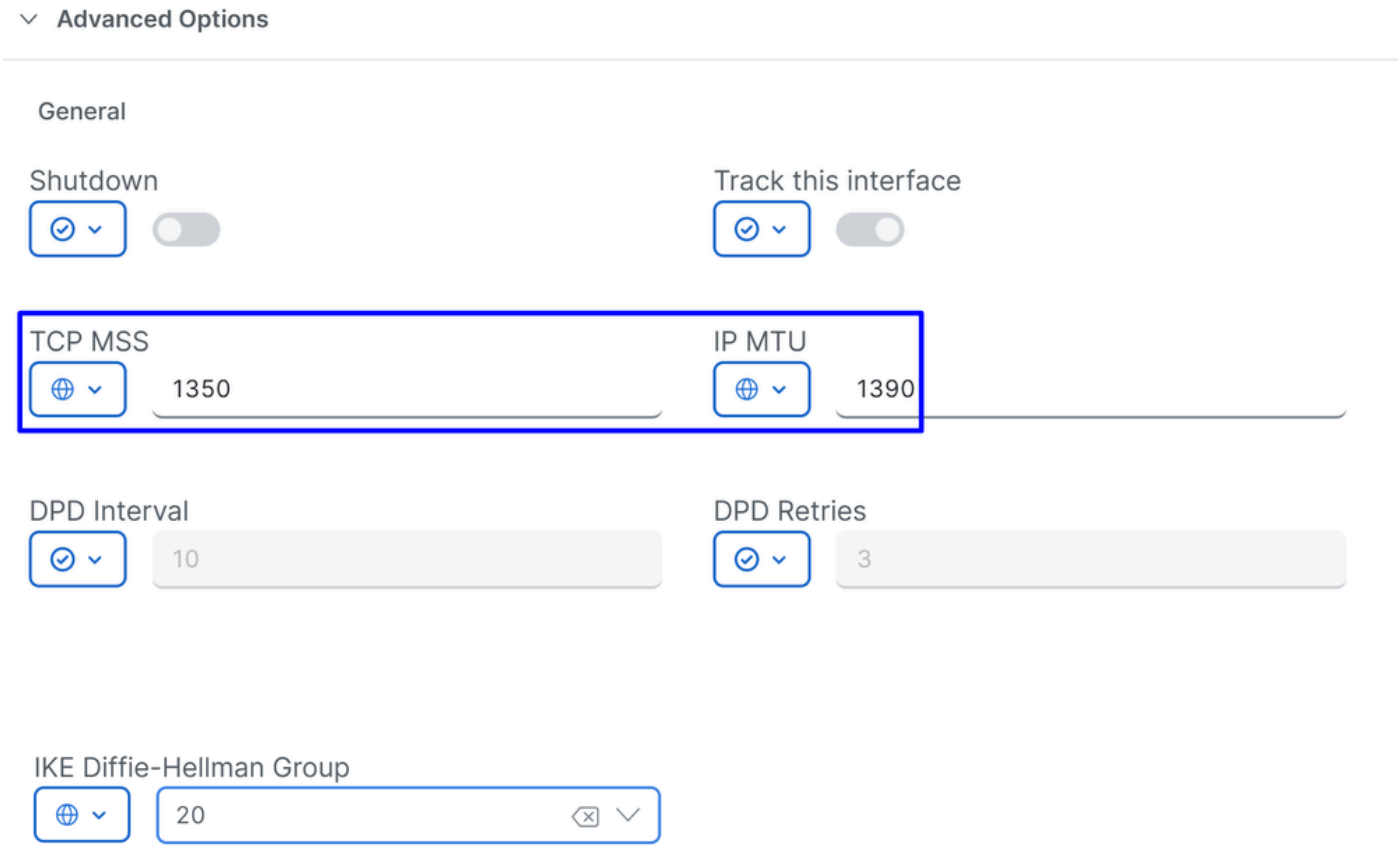
---

- Haga clic enAdd Tunnel




- Interface Name: ipsec1, ipsec2, ipsec3, etc.
- Tunnel Source Interface: Elija Interfaces de Loopback o una específica desde la que se establece el túnel
- **Tunnel Route Via**: Si elige Loopback, debe seleccionar la interfaz física desde la que desea rutear el tráfico. Si no selecciona Loopback, esta opción aparece atenuada y utiliza la primera interfaz habilitada para NAT que el sistema encuentra. Si hay más de una, debe seleccionar la interfaz WAN que desee
- **Data Center**: Esto significa a qué concentrador de Secure Access se establece la conexión

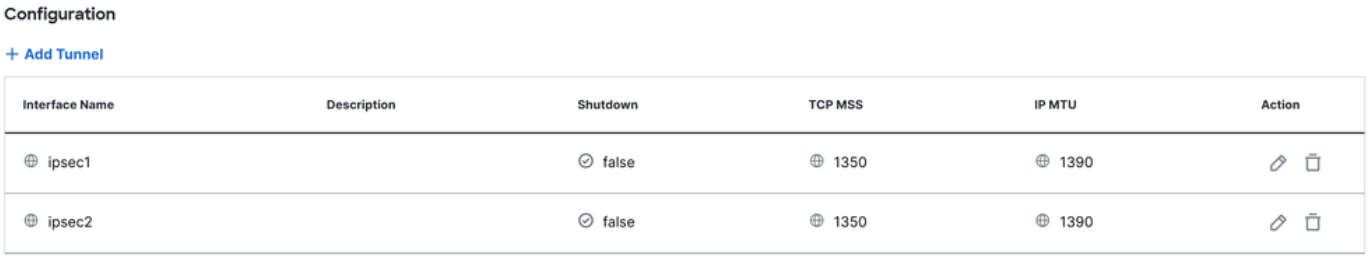
La siguiente parte de la configuración del túnel se configuran con las prácticas recomendadas proporcionadas por Cisco.



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

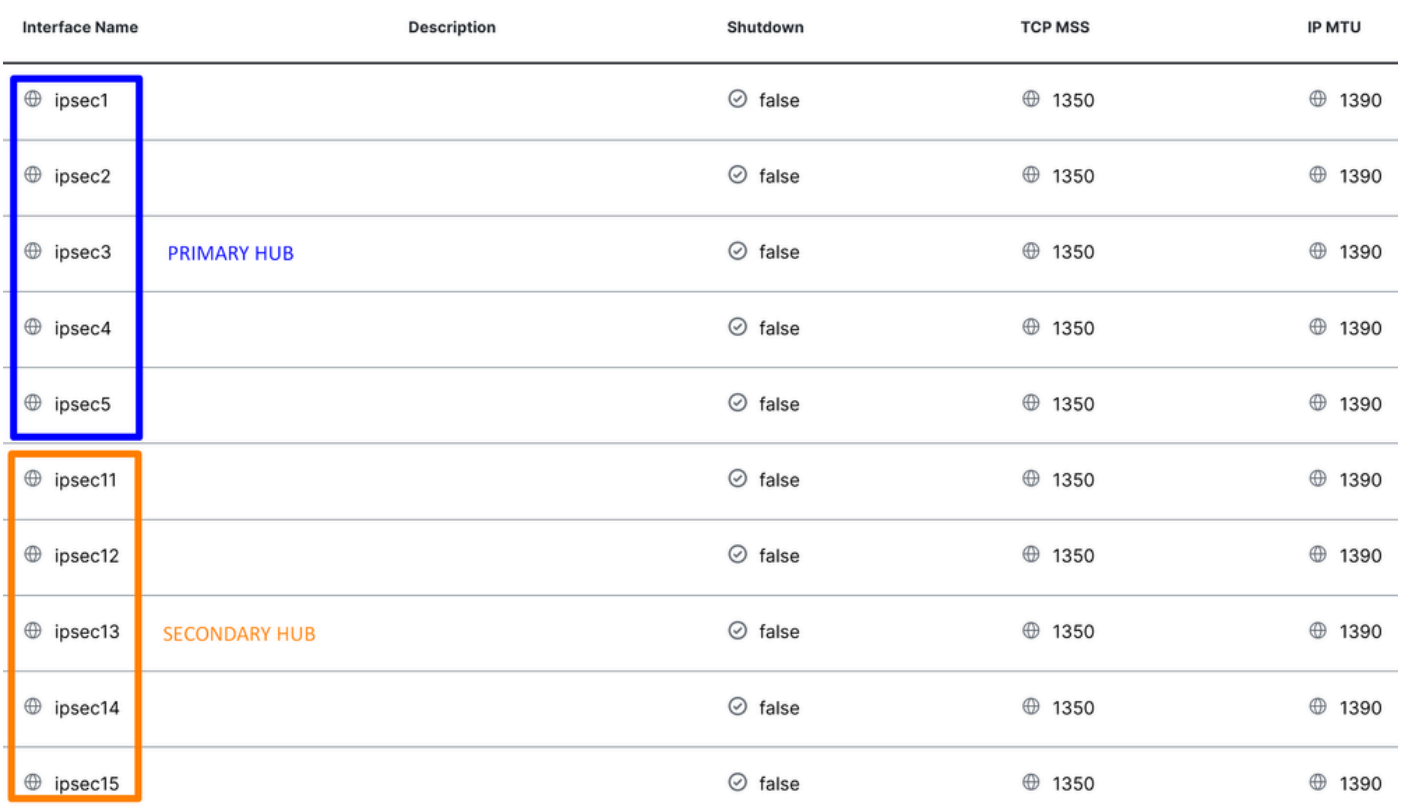
Después de esto, debe configurar el túnel secundario que apunta al centro de datos secundario.

ESCENARIO DE HA DE UN SOLO HUB

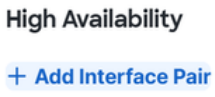



Este es el resultado final cuando se utiliza la implementación de escenario normal.

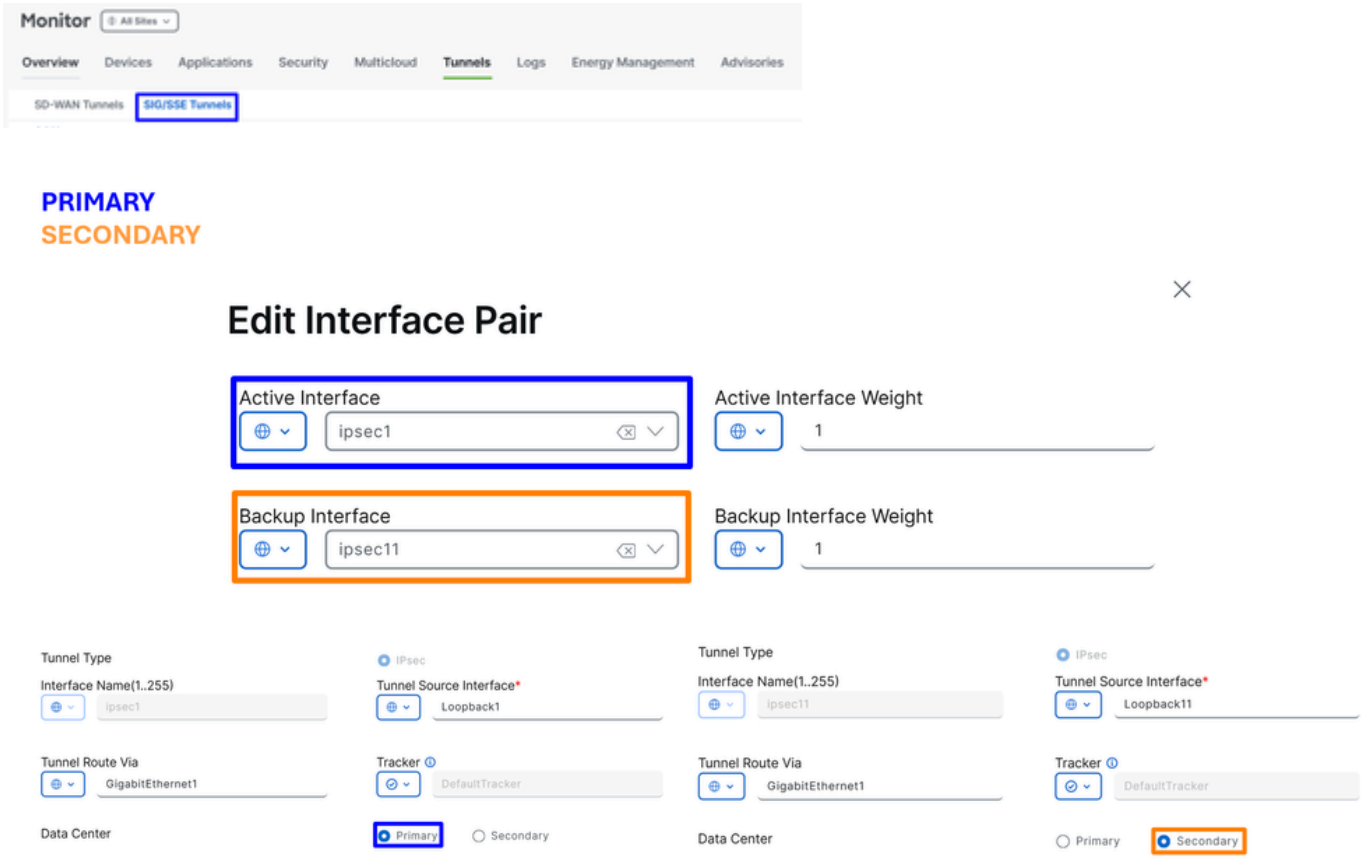
ECMP SCENARIO WITH HA




A continuación, debe configurar la alta disponibilidad en la directiva de Internet segura.




Haga clic en Agregar par de interfaces:




En este paso, debe configurar el túnel principal y el secundario para cada par de túneles que esté configurando. Esto significa que cada túnel tiene su propia copia de seguridad. Recuerde, estos túneles fueron creados como Primario y Secundario para este propósito exacto.
"Active interface" se refiere al túnel principal, mientras que "Backup interface" se refiere al túnel secundario:

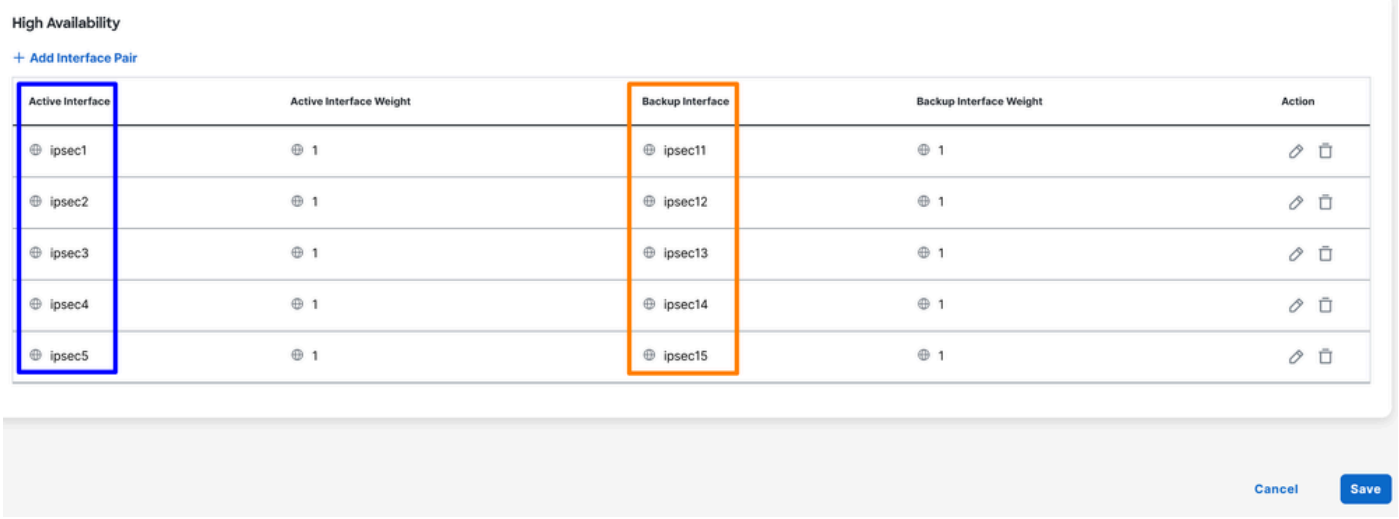
- Active Interface: Principal
- Backup Interface: Secundario

---

Advertencia: Si se omite este paso, los túneles no se activan y no se establece ninguna conexión desde los routers a Secure Access.

---

Después de configurar High Availability para los túneles, la configuración se muestra como se muestra en la siguiente imagen. En el ejemplo de laboratorio utilizado para esta guía, se muestran cinco túneles en HA. El número de túneles se puede ajustar según sea necesario.



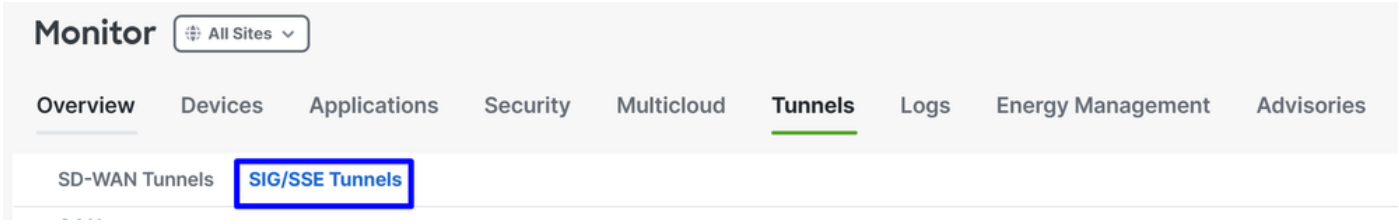

Nota: Un máximo de 8 pares de túneles (16 túneles: 8 principales y 8 secundarias) se pueden configurar en SD-WAN Catalyst vManage. Cisco Secure Access admite hasta 10 pares de túneles.

- Haga clic en Save

Después de este punto, si todo está correctamente configurado, los túneles aparecen como UP en el Administrador de SD-WAN y Secure Access.

Para verificar en SD-WAN, verifique los siguientes pasos:

- Haga clic en Monitor > Tunnels
- Haga clic enSIG/SSE Tunnels

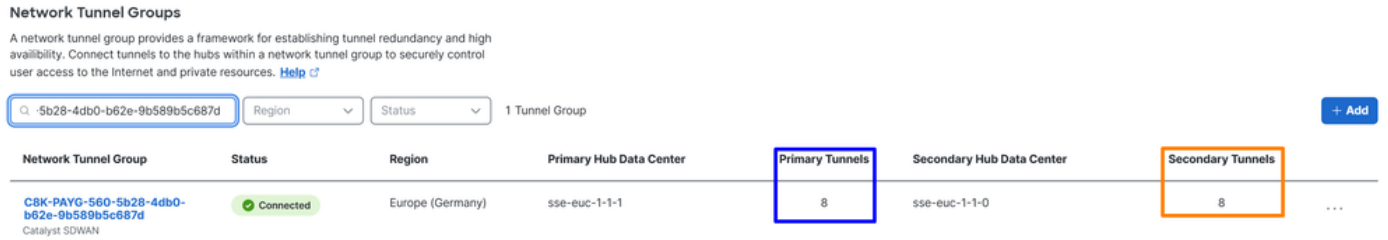



Además, podrá ver los túneles establecidos para Cisco Secure Access UP o no.

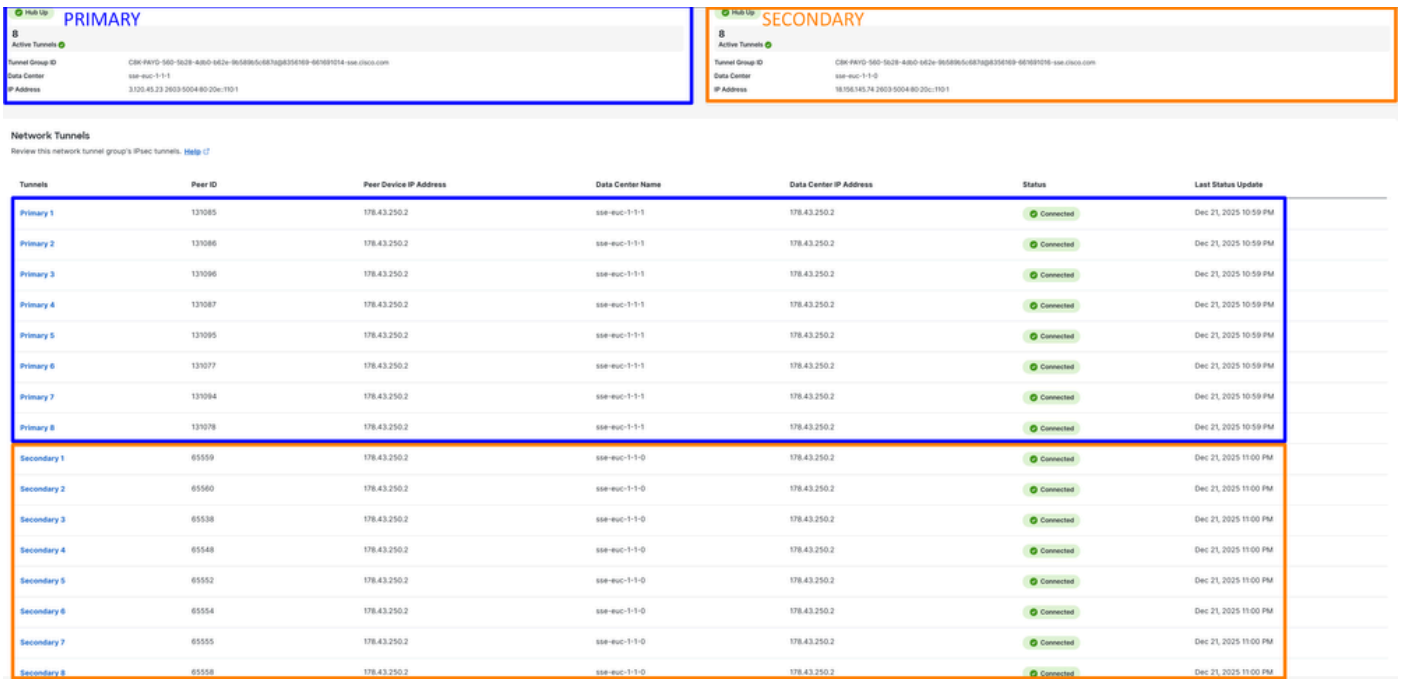
| Network Tunnel Group | Tunnel Name | Host Name | Site Name | Tunnel Group ID | Transport Type | Tunnel Type | HA Pair | Provider | Destination Data Center | Tunnel Status(Local) | Tunnel Status(Remote) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | R101-1 | SITE_101 | | | | | | | | |
| C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d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

Para verificar en Secure Access, marque los siguientes pasos:

- Haga clic en Connect > Network Connections




En una vista detallada, haga clic en el nombre del túnel:



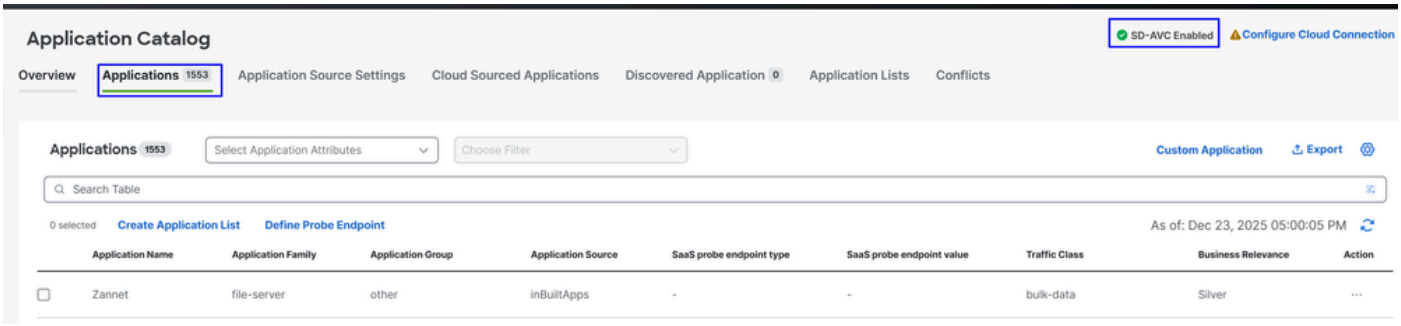

Después de esto, puede pasar al paso, Create your Custom Bypass FQDN or APP in SD-WAN

## Cree su FQDN o APP de bypass personalizado en SD-WAN (OPCIONAL)

Hay casos prácticos especiales en los que debe crear Application Bypass y FQDN o IP que puede aplicar a sus políticas de routing:

Vaya al portal de SD-WAN Manager:

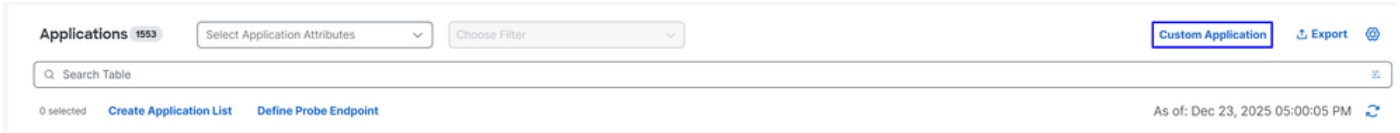
- Haga clic en Configuration > Application Catalog > Applications




Consejo: Si se ejecuta una versión inferior a 20.15, se pueden crear aplicaciones personalizadas en Listas de directivas

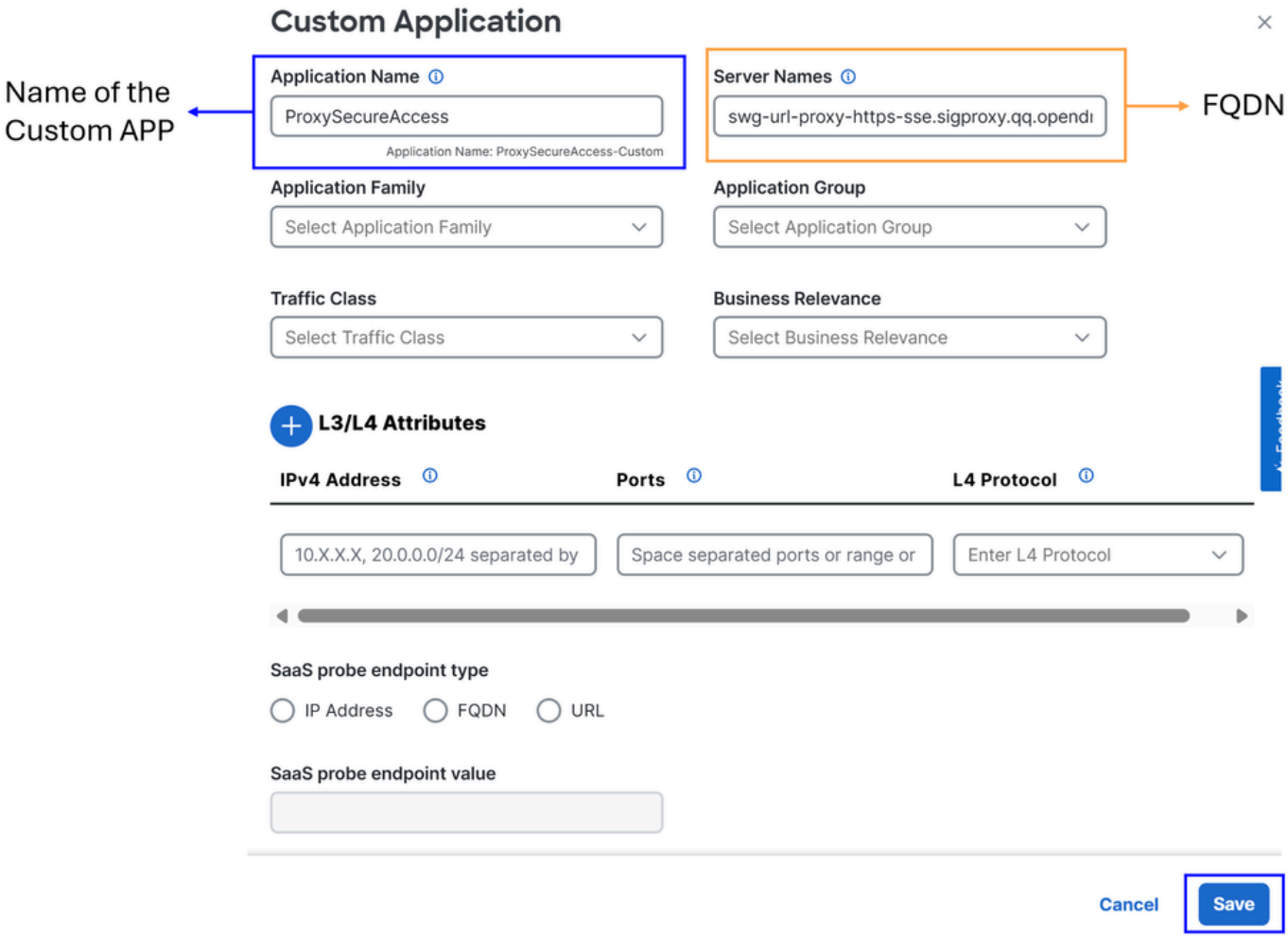
Nota: Para tener acceso al catálogo de aplicaciones, debe habilitar SD-AVC.

- Haga clic en Custom Application




En esta etapa, se configura una exclusión básica mediante el FQDN de SWG de Secure Client - Umbrella Module:

**ProxySecureAccess**




- Server Name: Utilice el FQDN que desea omitir (en este ejemplo se configura el FQDN de SWG)
  - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Haga clic en Save

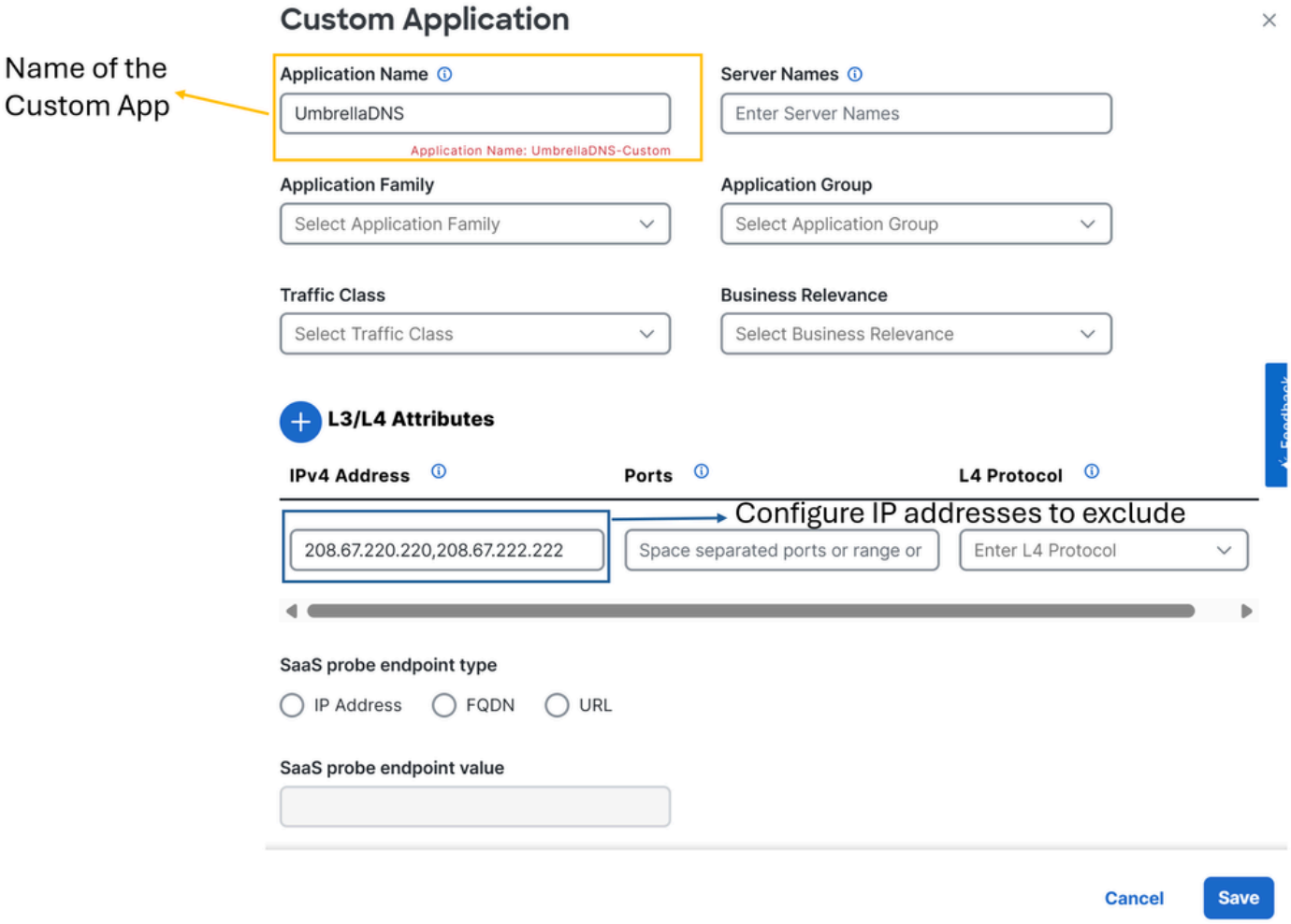
---

Nota: Cambie ORGID con su número de organización SSE.

---

A continuación, se crea una exclusión básica; en este caso, los servidores DNS de Umbrella:

UmbrellaDNS




Ahora puede continuar con las configuraciones de las políticas de ruteo.

## Enrutamiento del tráfico

En este paso, debe enrutar el tráfico de Internet a través de los túneles para protegerlo mediante Cisco Secure Access. En este caso, se utiliza una política de routing flexible que nos permite omitir cierto tráfico, lo que ayuda a evitar el envío de tráfico no deseado a través de Secure Access o evitar posibles malas prácticas.
En primer lugar, deje que defina los dos métodos de routing que se pueden utilizar:

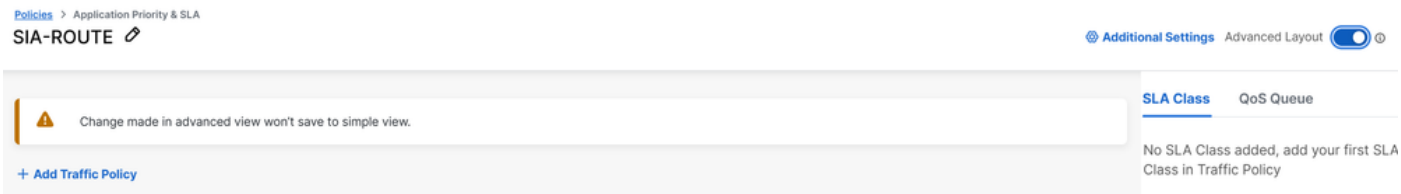
- Configuration > Configuration Groups > Service Profile > Service Route: Este método proporciona routing a Secure Access, pero carece de flexibilidad.
- **Configuration** > Policy Groups > Application Priority & SLA: Este método ofrece varias opciones de routing dentro de la SD-WAN y, lo que es más importante, le permite omitir tráfico específico para que no se envíe a través de Secure Access.

Para obtener flexibilidad y alineación con las prácticas recomendadas, se utiliza esta configuración, Application Priority & SLA:

- Haga clic en **Configuration** > Policy Groups > Application Priority & SLA
- Haga clic en Application Priority & SLA Policy

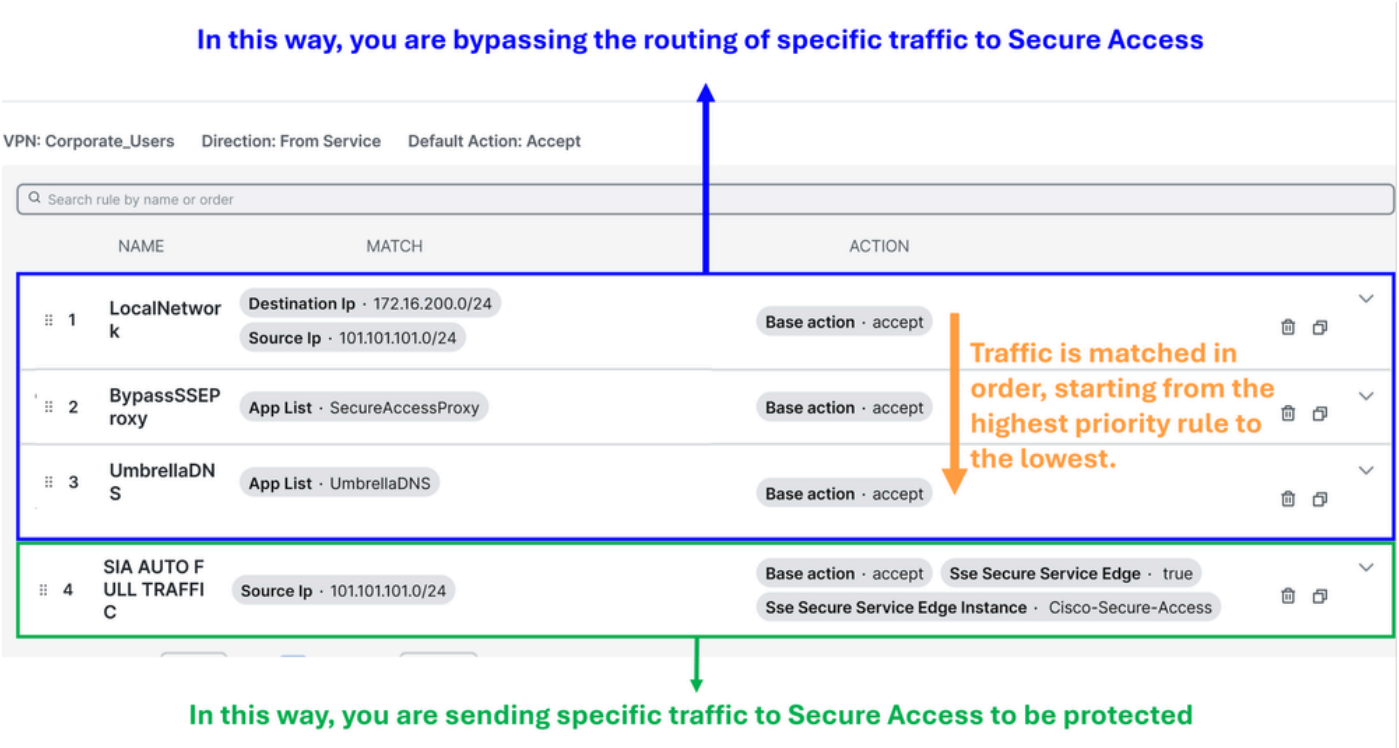

- Configure un nombre de directiva y haga clic en Create


- Habilitar Advanced Layout
- Haga clic en + Add Traffic Policy




- Policy Name: Nombre que lo ajusta al propósito de esta lista de políticas de tráfico
- VPN(s): Elija el servicio VPN del usuario desde el que enruta el tráfico
- **Direction**: Desde el servicio
- Default action: Aceptar

Después de esto, puede iniciar la creación de la política de tráfico:




1. Local Network Policy (Optional): Origen 101.101.101.0/24, Destino 172.16.200.0/24. Esta ruta evita que el tráfico dentro de la red se envíe a Cisco Secure Access. Normalmente, los clientes no lo hacen, ya que el routing interno lo gestiona normalmente el router de distribución en implementaciones SD-WAN. Esta configuración garantiza que el tráfico interno entre estas

subredes no se enrute a Secure Access, dependiendo de si su situación lo requiere (opcional, depende de su entorno de red)

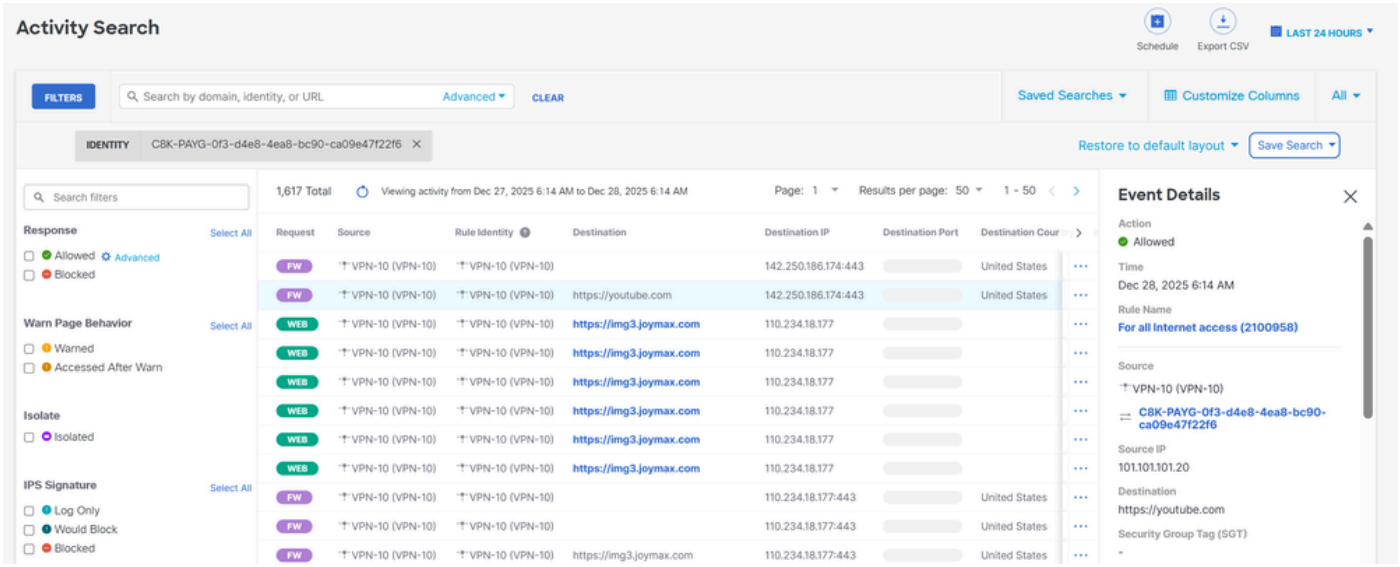
2. **BypassSSEProxy (Optional)**: Esta política impide que los ordenadores internos con el módulo Cisco Umbrella en Secure Client y SWG habilitados envíen tráfico proxy de vuelta a la nube. El routing del tráfico proxy a la nube de nuevo no se considera una práctica recomendada.
3. UmbrellaDNS (Best Practice): Esta directiva impide que las consultas DNS destinadas a Internet se envíen a través del túnel. No se recomienda enviar consultas de DNS a resolvers de Umbrella (208.67.222.222,208.67.220.220) a través del túnel.
4. SIA AUTO FULL TRAFFIC: Esta política dirige todo el tráfico desde el origen 101.101.101.0/24 a Internet a través de los túneles SSE que creó anteriormente, asegurándose de que este tráfico esté protegido en la nube.

# Verificación

para verificar si el tráfico ya se está inundando a través de Cisco Secure Access, navegue hasta Events o Activity Search o Network-Wide Path Insights y filtre por su identidad de túnel:

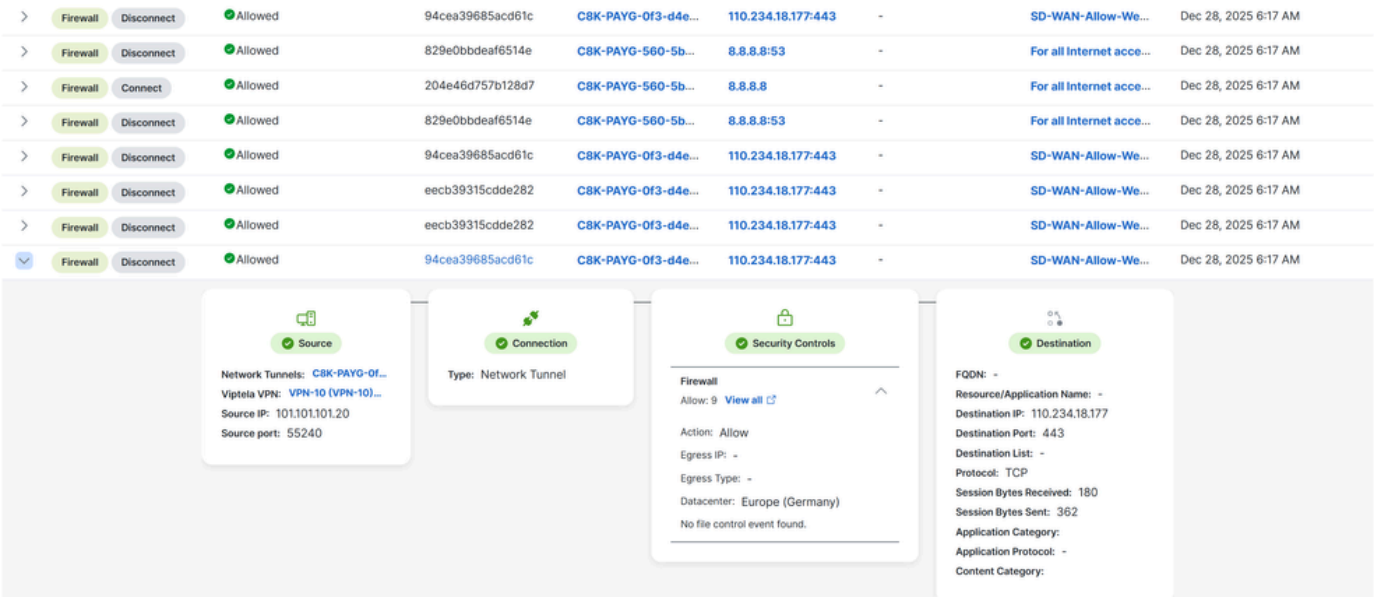
## Acceso seguro - Búsqueda de actividad

Vaya a Monitor > Activity Search:




## Acceso seguro - Eventos

Vaya a Monitor > Events:

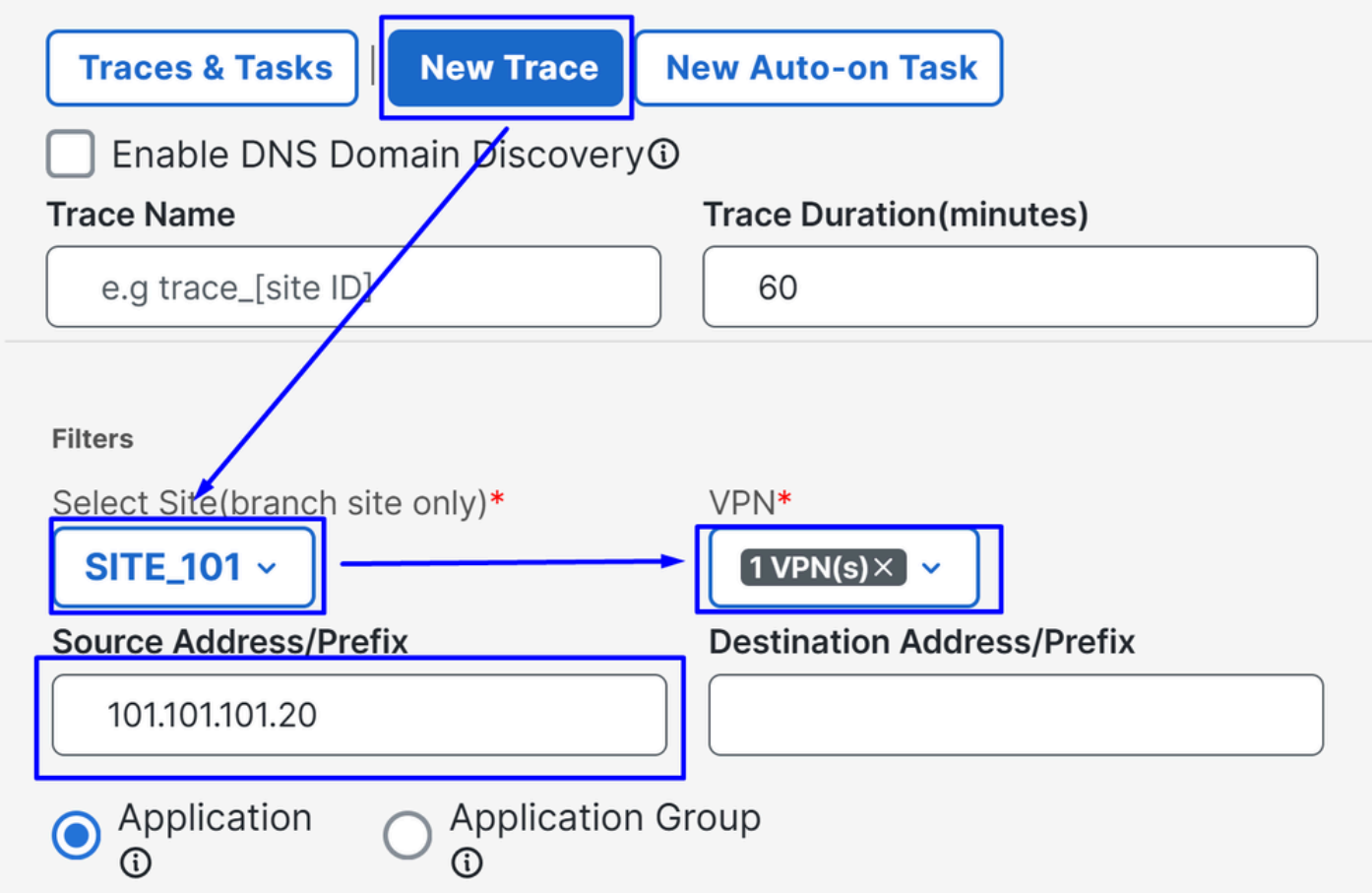



Nota: Asegúrese de que tiene la política predeterminada con el registro activado; de forma predeterminada, esta opción está desactivada.

## Catalyst SD-WAN Manager: Network-Wide Path Insights

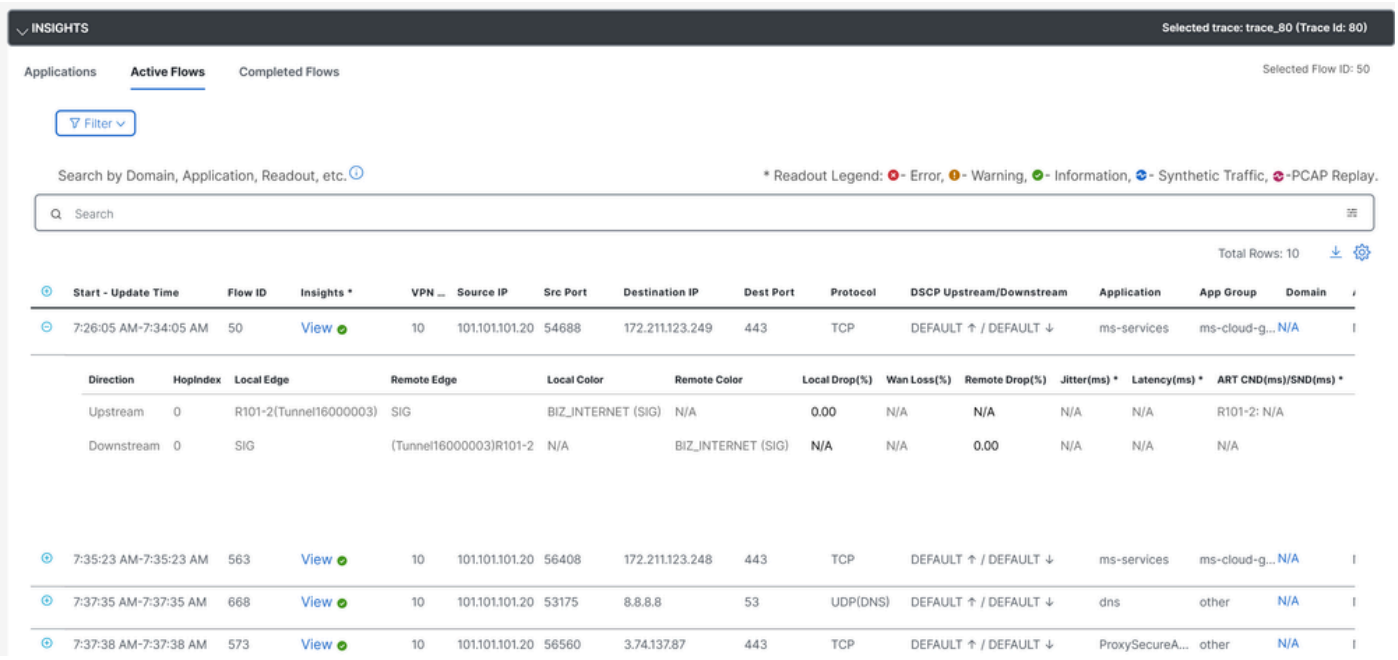
Vaya a Catalyst SD-WAN Manager:

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




- Site: Elija el sitio desde el que se origina el tráfico
- VPN: Elija el ID de VPN de su subred desde la que egresa el tráfico
- Source: Coloque la IP o déjela en blanco para filtrar todo el tráfico filtrado por el **Site** y VPN elegido

A continuación, en Insights podrá ver el tráfico que fluye a través de los túneles y el tipo de tráfico que va a Secure Access:



## Información Relacionada

- Soporte técnico y descargas de Cisco
- Centro de ayuda de Cisco Secure Access
- Guía de diseño de Cisco SASE
- 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).