Configuración y solución de problemas de integración de Secure Access (SSE) en Catalyst SD-WAN

Contenido

Introducción

Este documento describe cómo configurar la integración SSE activo-activo en Catalyst SD-WAN y guía para la resolución de problemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) de Cisco
- Grupos de configuración
- Grupos de políticas

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C8000V versión 17.15.02
- vManage versión 20.15.02

- cuenta de Cisco Secure Access

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.

Acceso seguro de Cisco

Cisco Secure Access es una solución de extremo de servicios de seguridad (SSE) basada en la nube que converge varios servicios de seguridad de red y los proporciona desde la nube para dar cabida a un personal híbrido. Cisco SD-WAN Manager aprovecha las API REST para recuperar información de políticas de Cisco Secure Access y distribuye esta información a los dispositivos SD-WAN de Cisco IOS XE. Esta integración permite a los usuarios un acceso directo a Internet (DIA) seguro, transparente y fluido, lo que les permite conectarse desde cualquier dispositivo, en cualquier lugar y de forma segura.

Cisco SSE permite a los dispositivos SD-WAN establecer conexiones con los proveedores SSE mediante túneles IPSec. Este documento está dirigido a los usuarios de Cisco Secure Access.

Configuraciones preliminares

- Habilitar la búsqueda de dominios para el dispositivo: Navegue hasta Grupos de configuración > Perfil del sistema > Global y habilite Búsqueda de dominio.

Nota: De forma predeterminada, la búsqueda de dominios está deshabilitada.

- Configurar DNS: El router puede resolver el DNS y acceder a Internet en VPN 0.
- Configuración de DIA NAT: La configuración DIA debe estar presente en el router donde se crea el túnel SSE.

Crear interfaces de loopback

Si ambos túneles de una configuración Activo/Activo se conectan al mismo Data Center de destino y utilizan la misma interfaz WAN que el origen, es necesario crear dos direcciones IP de bucle invertido.

Nota: Cuando dos túneles se configuran con el mismo origen y destino, IKEv2 forma un par

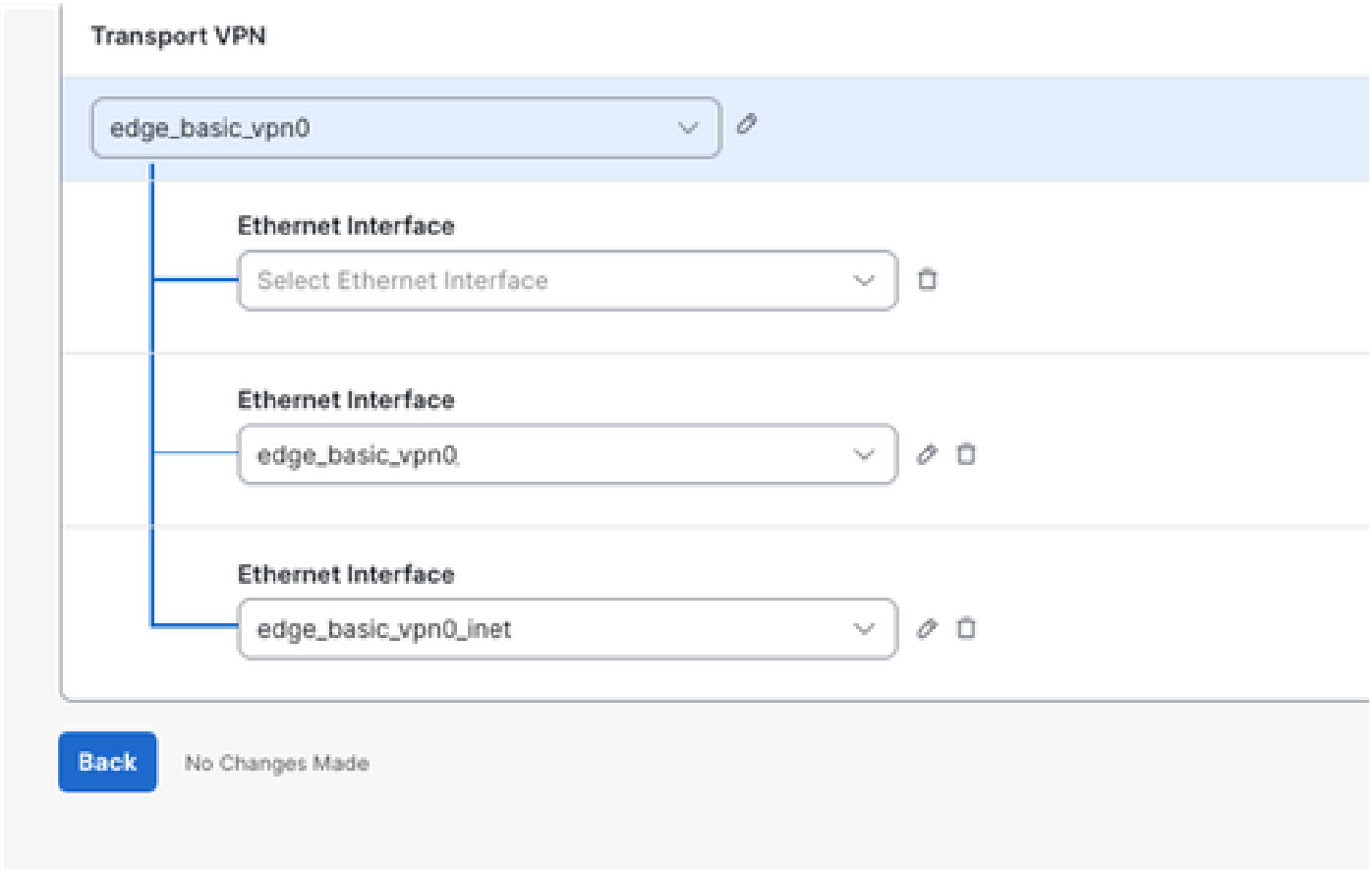
---

de identidad formado por un ID local y un ID remoto. De forma predeterminada, el ID local es la dirección IP de la interfaz de origen del túnel. Este par de identidades debe ser único y no puede compartirse entre dos túneles. Para evitar confusiones dentro del estado IKEv2, cada túnel utiliza una interfaz de bucle invertido diferente como origen. Aunque los paquetes IKE se traducen (NATed) en la interfaz DIA, el ID local no se modifica y conserva la dirección IP de bucle invertido original.

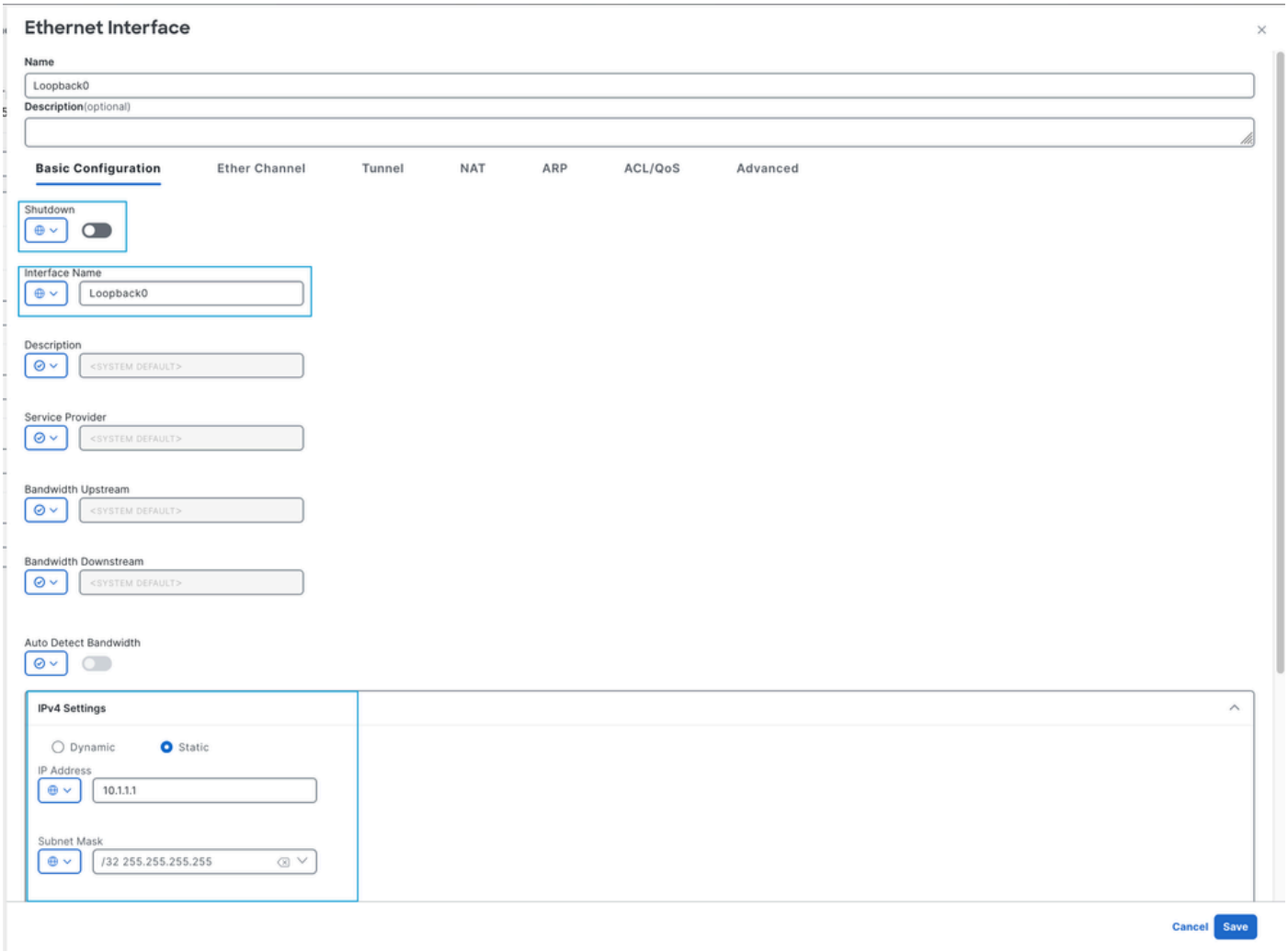
1. Vaya a Configuration > Configuration Groups > Configuration Group Name> Transport & Management Profile > haga clic en Edit.

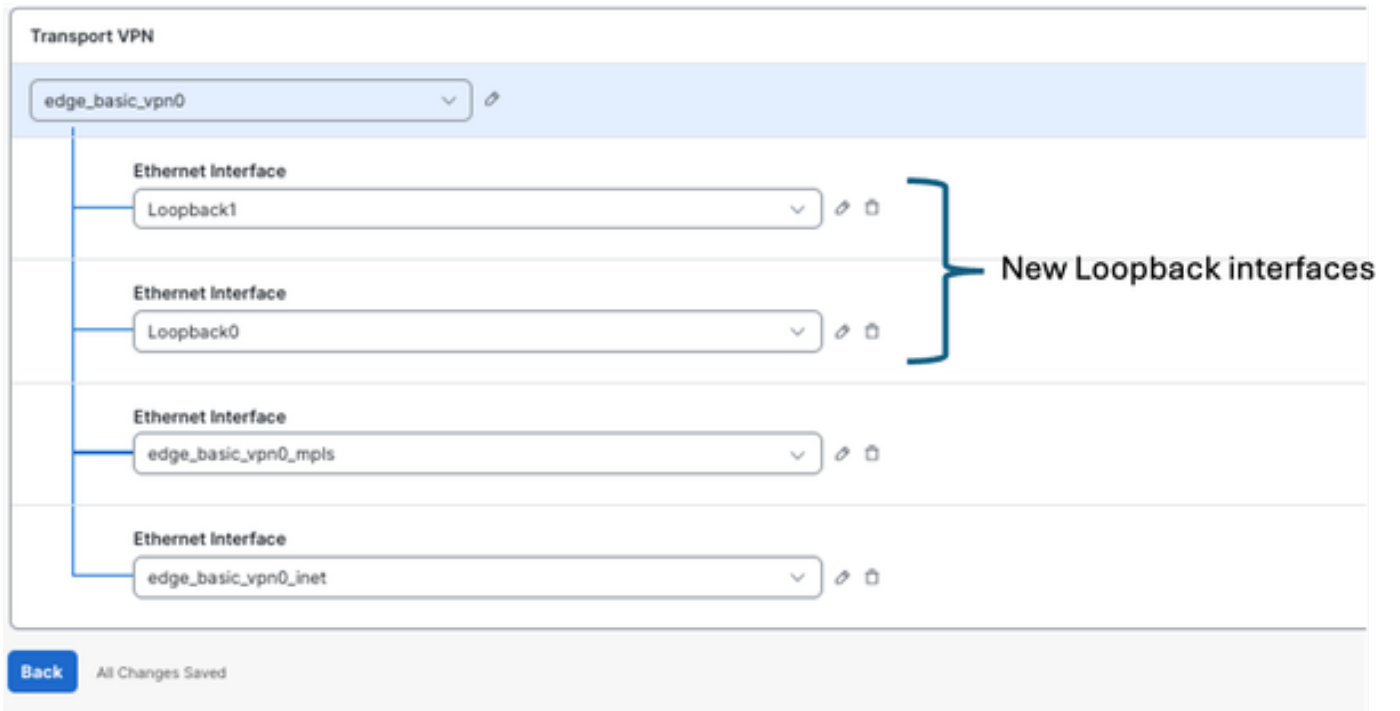
2. Haga clic en el signo más (+) en el lado derecho del perfil VPN de transporte (perfil principal). Se abrirá un menú Añadir función (Add Feature) situado en el extremo derecho.

3. Haga clic en Ethernet Interface. Agrega una nueva interfaz de Internet en Transport VPN.



4. Cree las dos interfaces de loopback utilizando las direcciones IPv4 RFC1918, como el ejemplo de loopback0 en la imagen.



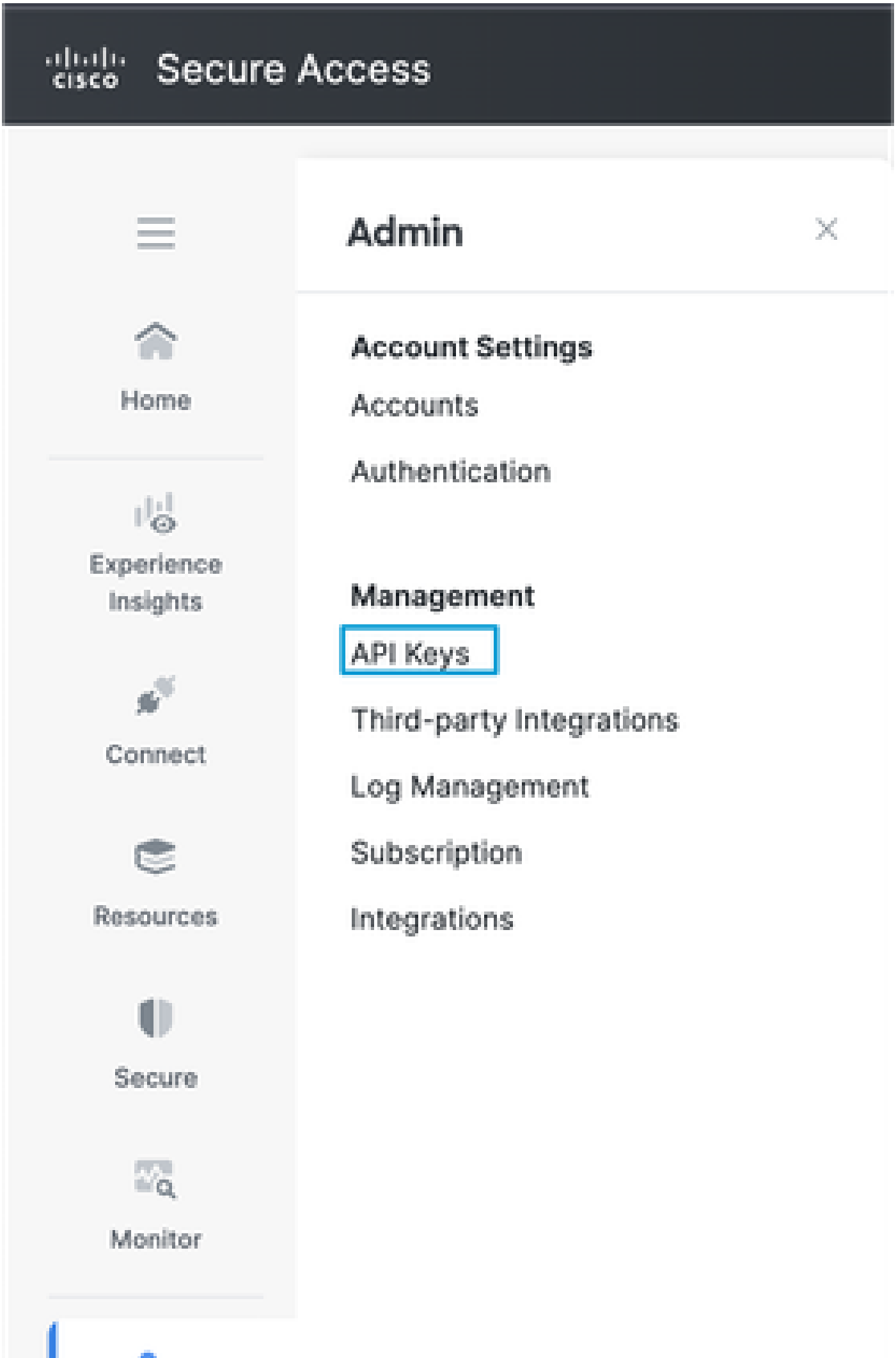


5. Después de aplicar la configuración de loopback, proceda a implementar el cambio de configuración en el dispositivo. Observe que el estado de aprovisionamiento cambia de 1/1 a 0/1.

Name	Type	Profile	Provisioning Status In Sync Devices / Associated Devices	Origin	Updated By
Hub2-SIG	Single Router	4	▲ 0 / 1	user	cisco

Configuración de nuevas claves de API en el portal SSE

1. Acceso al portal de SSE https://login.sse.cisco.com/
2. Navegue hasta Admin > API Keys .


Secure Access
Admin
Account Settings
Accounts
Authentication
Management
API Keys
Third-party Integrations
Log Management
Subscription
Integrations
Home
Experience Insights
Connect
Resources
Secure
Monitor

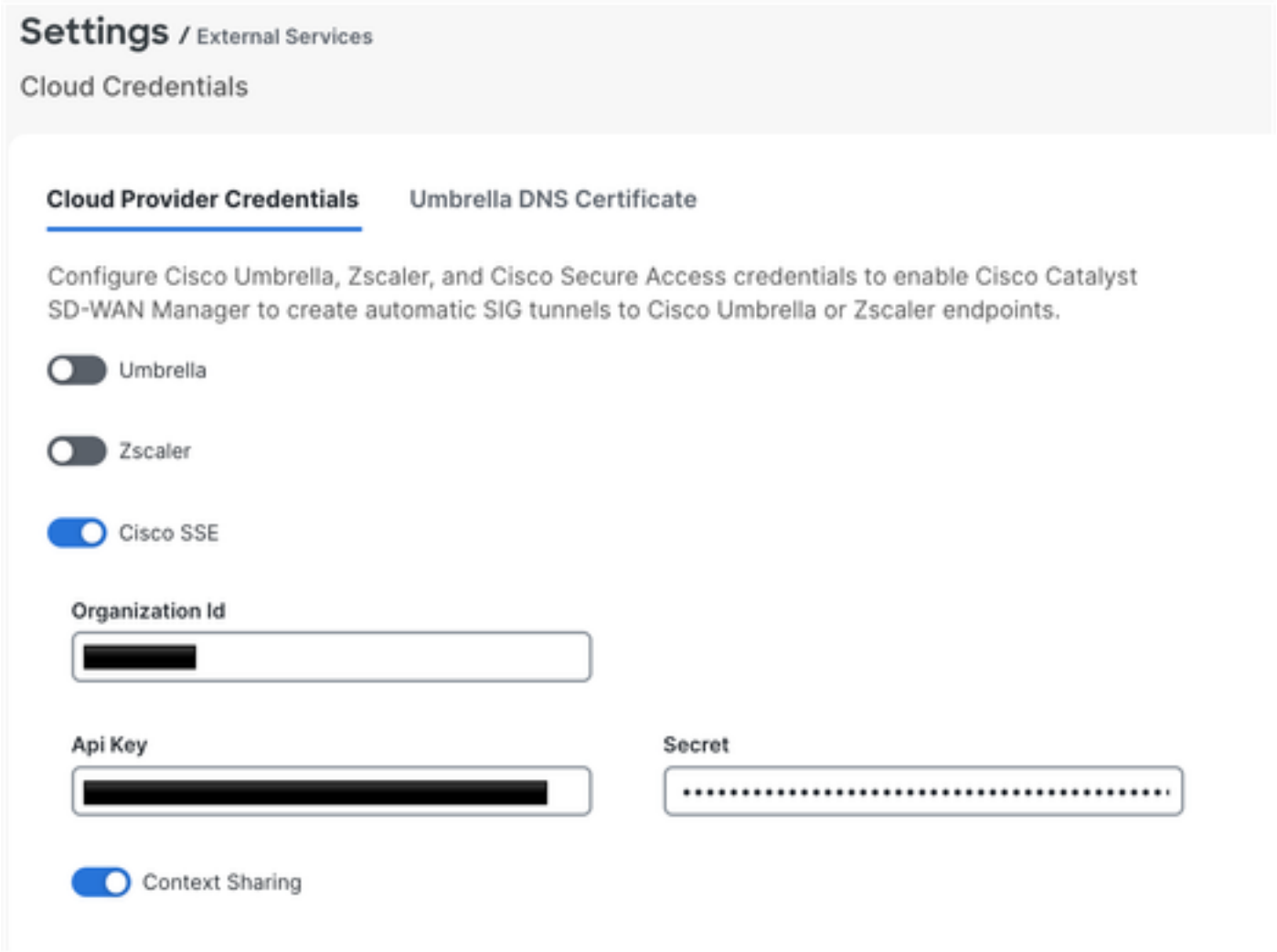
6. Copie la clave API y Key Secret en un bloc de notas y seleccione ACCEPT AND CLOSE

7. En la URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys, el#some-numbers# es su ID de organización. Copie también esa información en el bloc de notas.

Configuración de SSE en Catalyst Manager

Configurar credenciales de nube

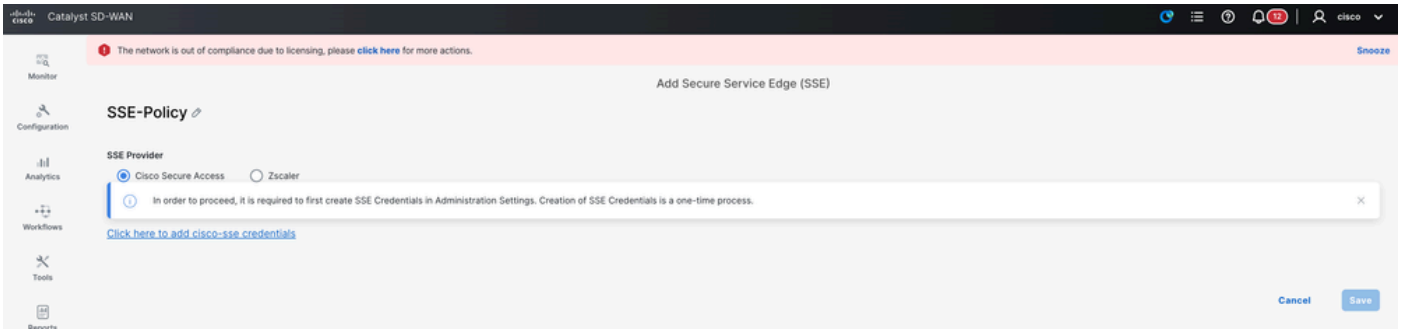
1. Navegue hasta Administración > Configuración > Credenciales de nube > Credenciales de proveedor de nube, y habilite Cisco Secure Access
e introduzca los detalles.



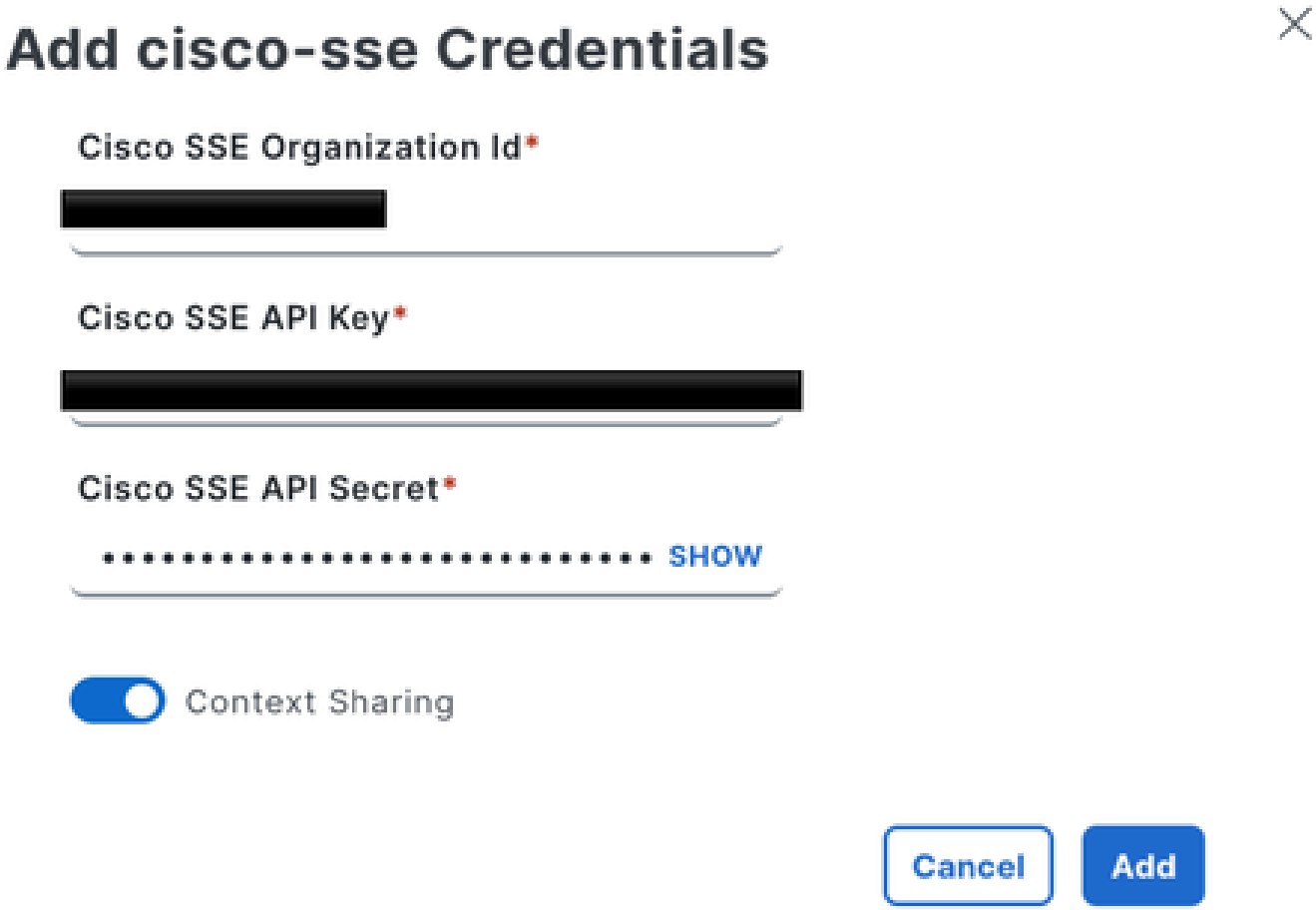
2. Opcional: Puede habilitar el uso compartido de contexto para mejorar la funcionalidad. Para obtener más información, consulte la guía del usuario de Cisco SSE sobre el uso compartido del contexto.

Configuración de Túneles SSE Usando el Grupo de Políticas

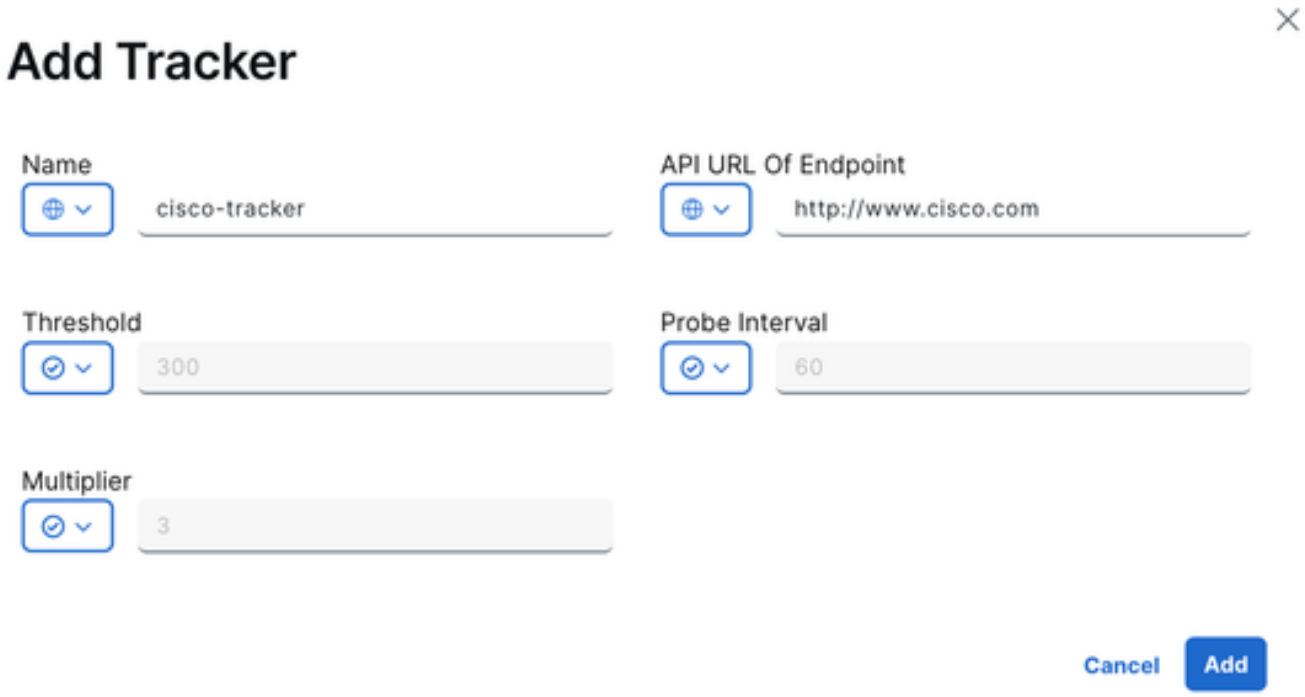
En el Administrador de SD-WAN, navegue hasta Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge y haga clic en Add Secure Service Edge (SSE).

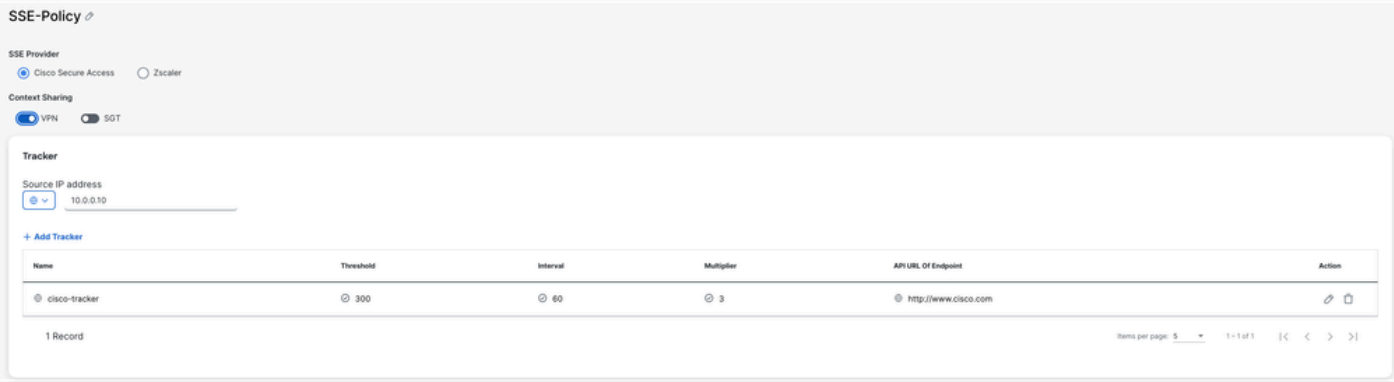


Nota: Si aún no se han configurado las credenciales de la nube, puede agregarlas en este paso. Si las credenciales ya se han configurado, se cargan automáticamente.



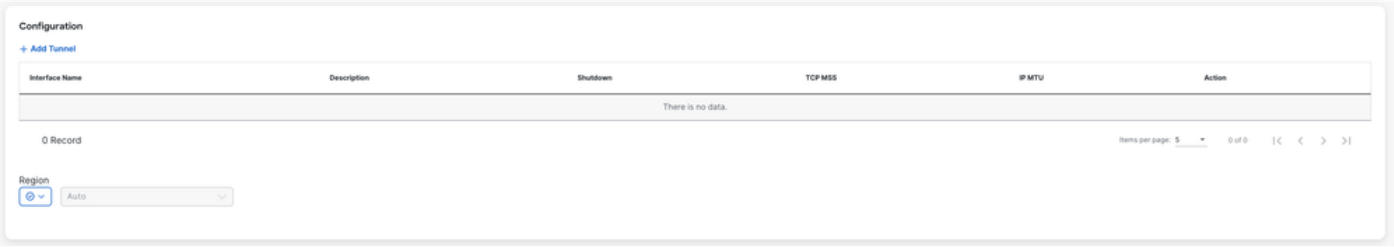
1. Configure el Rastreador SSE. En este ejemplo, la URL del rastreador se establece en http://www.cisco.com, y la dirección IP de origen se asigna desde una de las interfaces de loopback.



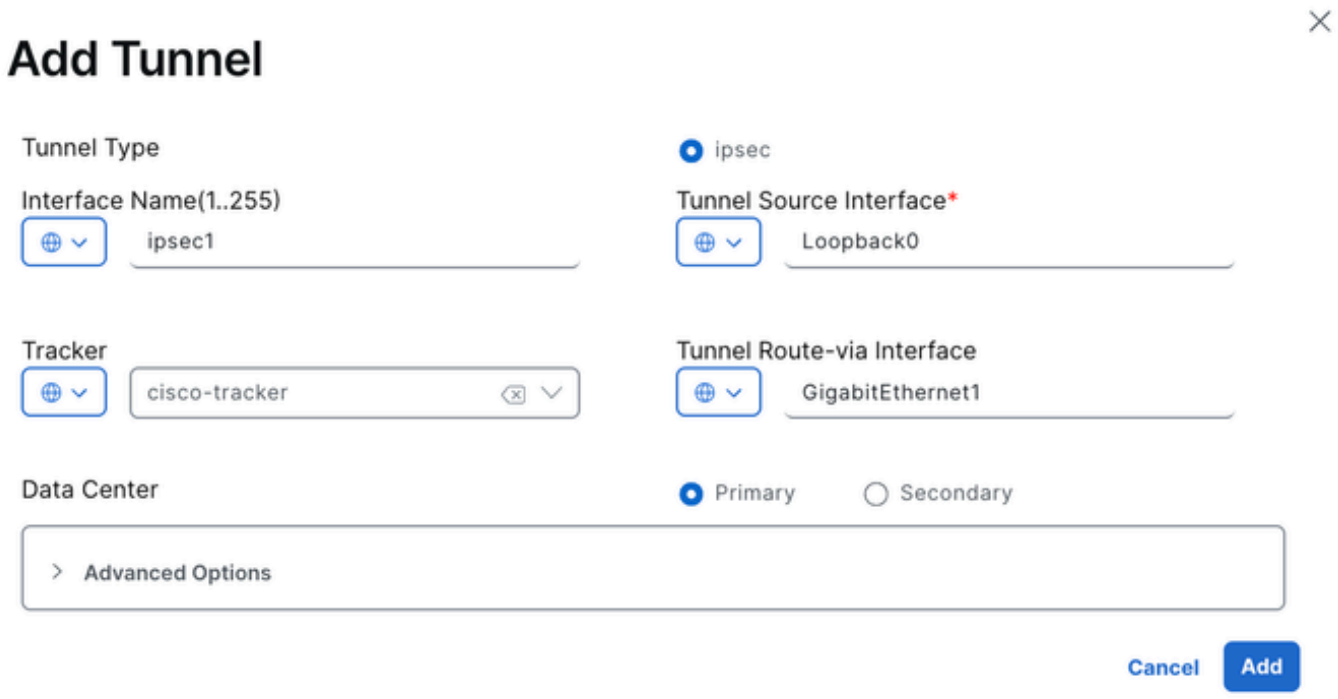


Opcionalmente, dado que el uso compartido del contexto se habilitó cuando se configuraron las credenciales de la nube, VPN se selecciona como la opción en este ejemplo.

2. Haga clic en Add Tunnel

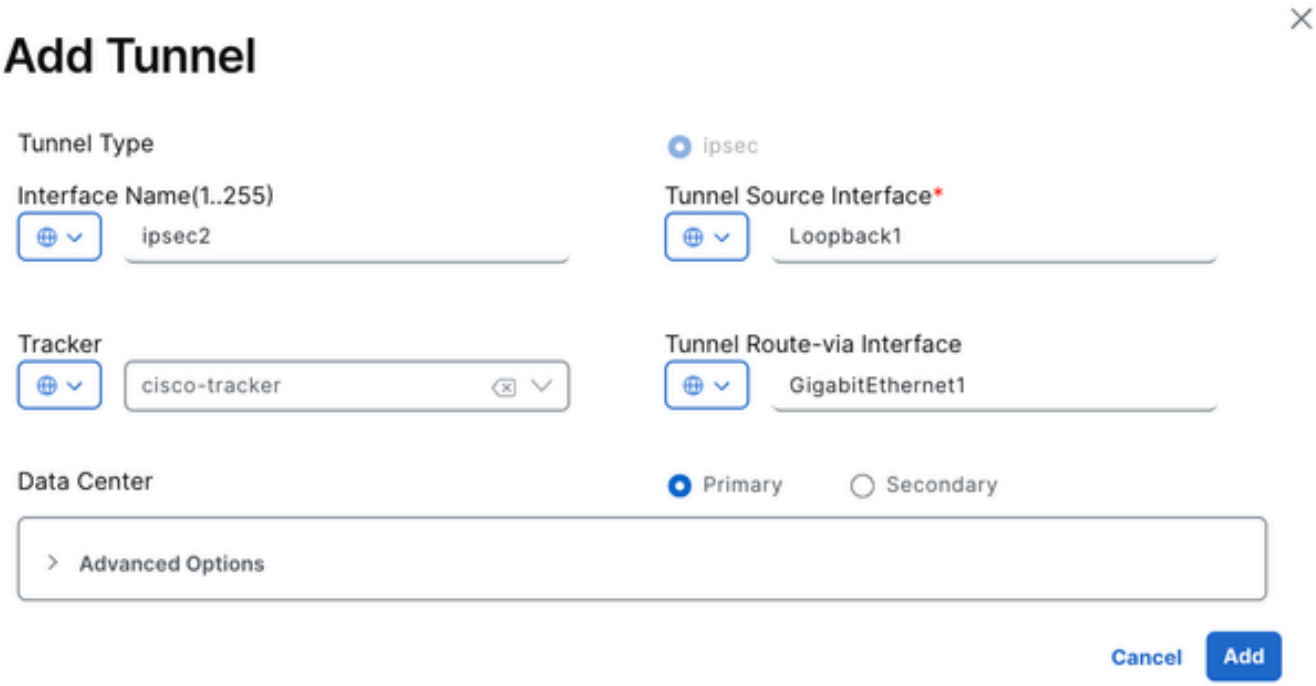


3. En este ejemplo, la interfaz Loopback0 se utiliza como origen del túnel, mientras que la interfaz GigabitEthernet1 sirve como interfaz WAN para enrutar el tráfico.



Dado que el rastreador se configuró en este ejemplo, la configuración se cambia a Global y se selecciona el rastreador de Cisco preconfigurado.

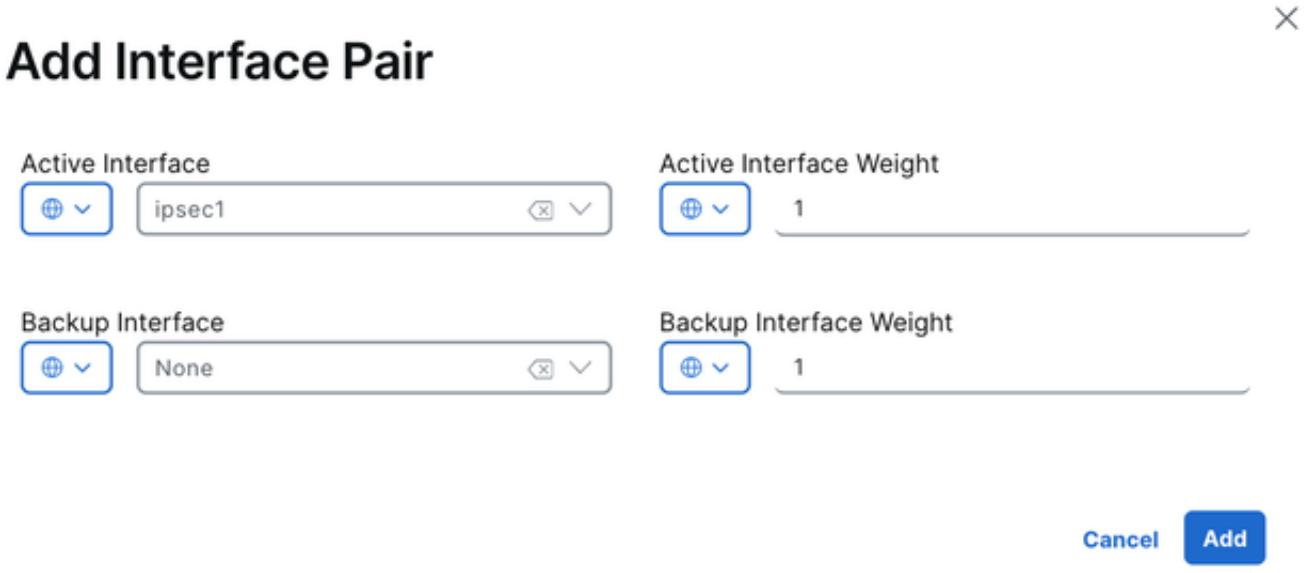
4. Para el segundo túnel, repita los mismos pasos utilizando los mismos parámetros, pero cambie el Nombre de la Interfaz de ipsec1 a ipsec2, y el Nombre de la Interfaz de Origen a Loopback1.



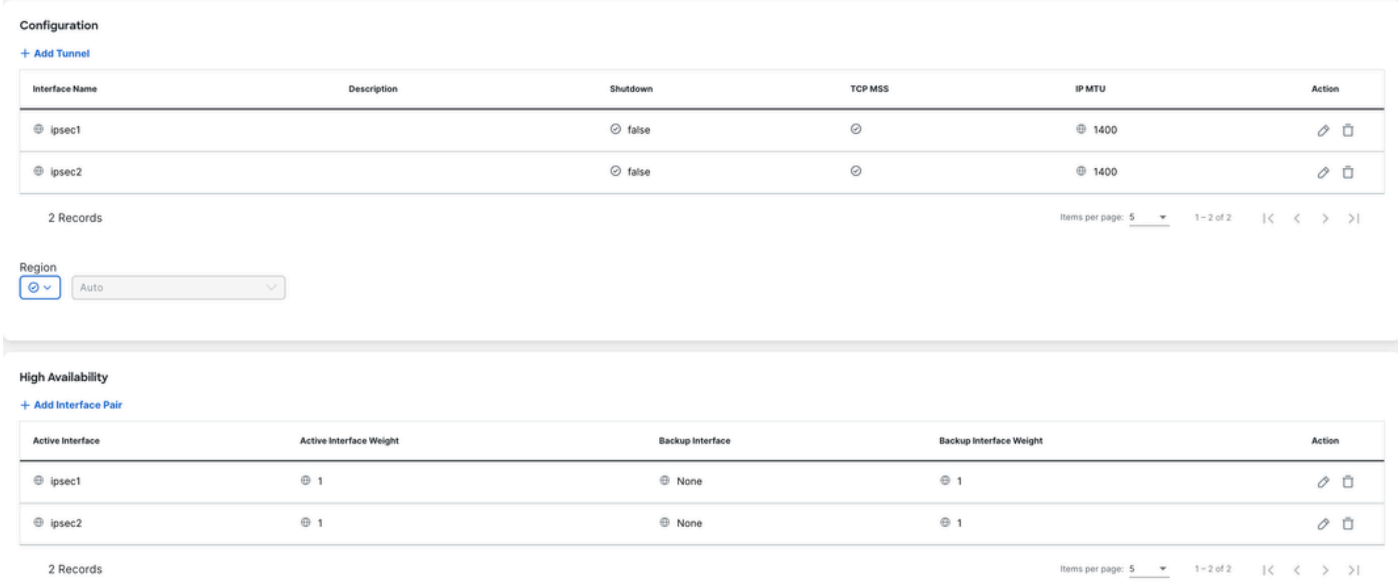
Ambos túneles están configurados para estar activos simultáneamente, sin una copia de seguridad.

5. Haga clic en Add Interface Pair.

6. Haga clic en Agregar. La interfaz activa se establece en ipsec1 y no se especifica ninguna interfaz de copia de seguridad.



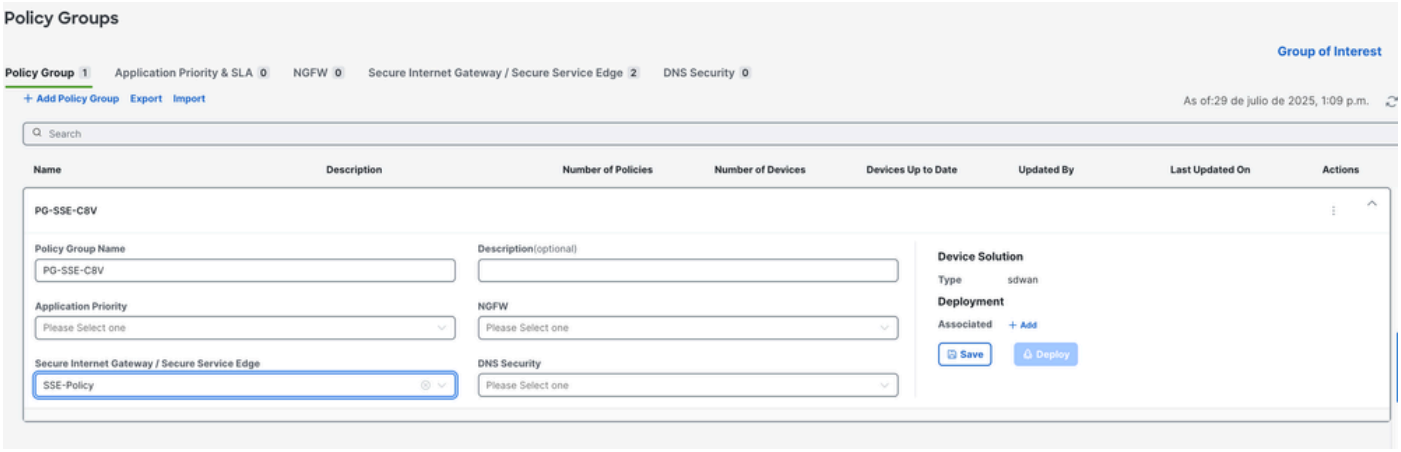
7. La misma operación se repite para el segundo túnel, ipsec2.



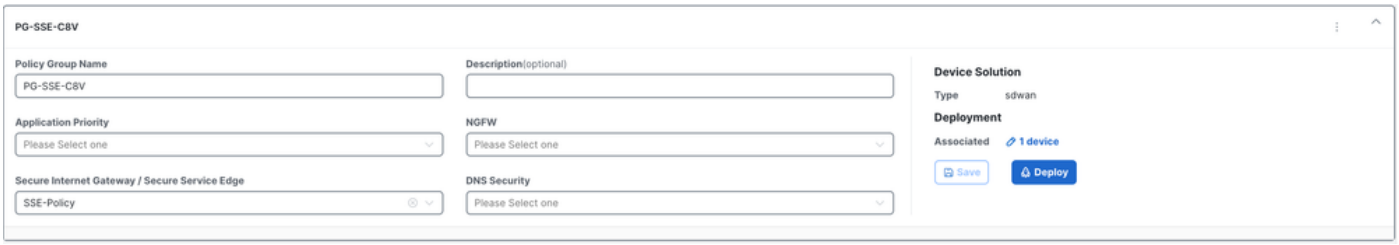
8. Guarde la configuración.

Configurar grupo de políticas

1. Sólo tiene que seleccionar la política creada anteriormente en el grupo de políticas y guardarla.



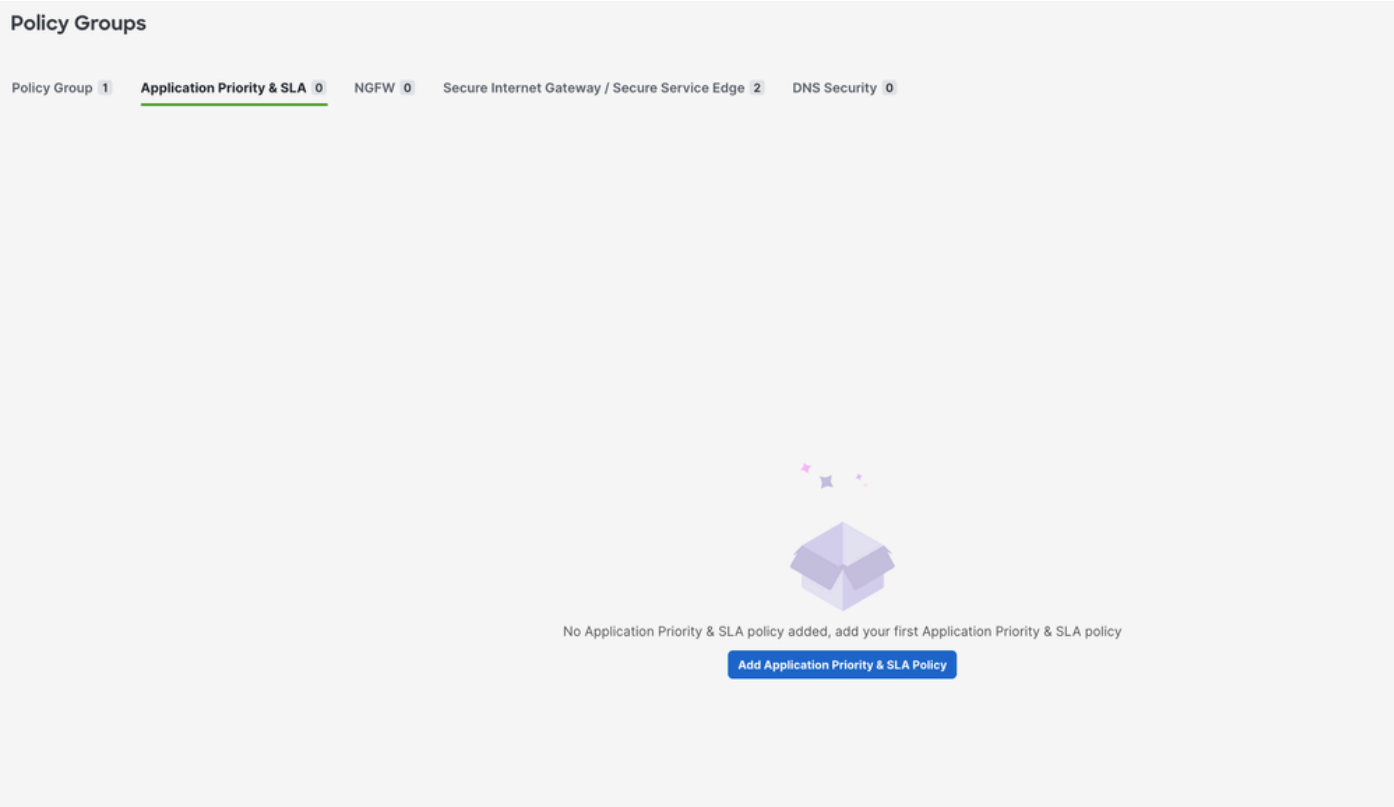
2. Una vez que el dispositivo o dispositivos se han asociado al grupo de políticas, proceda a implementar el grupo de políticas.



Configuración del grupo de políticas para redirigir el tráfico a SSE

1. En el Administrador de SD-WAN, navegue hasta Configuration > Policy Groups > Application Priority & SLA.

- Seleccione Agregar prioridad de aplicación y política de SLA
- Especifique un nombre para la directiva.

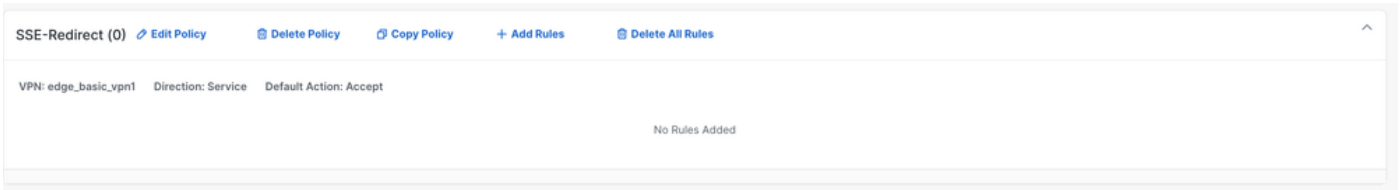


2. Una vez que se muestre la nueva política, seleccione el botón Diseño Avanzado.

3. Seleccione Agregar lista de políticas de tráfico.

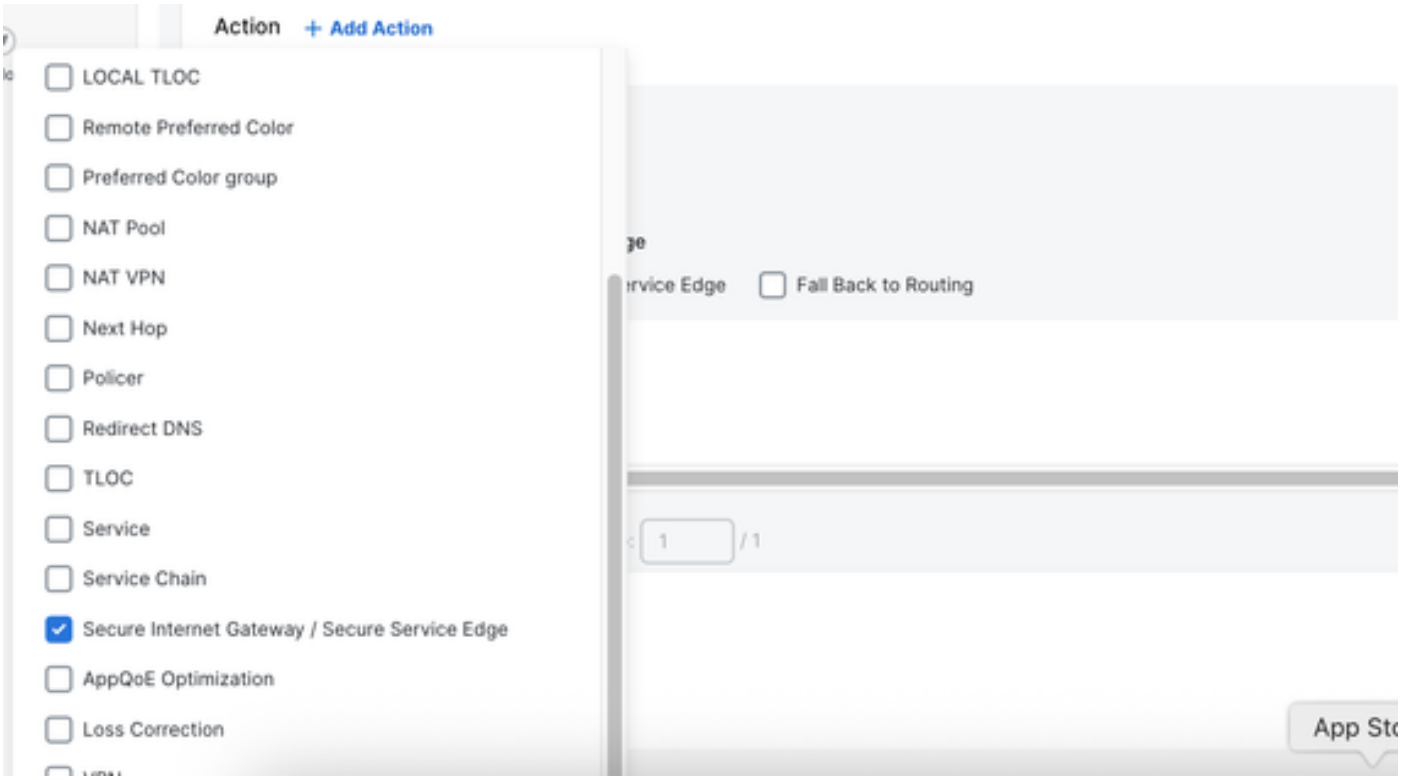
- Configure las VPN para redirigir el tráfico al túnel SSE.
- Establezca la dirección y la acción predeterminada según sea necesario y guárdelas.

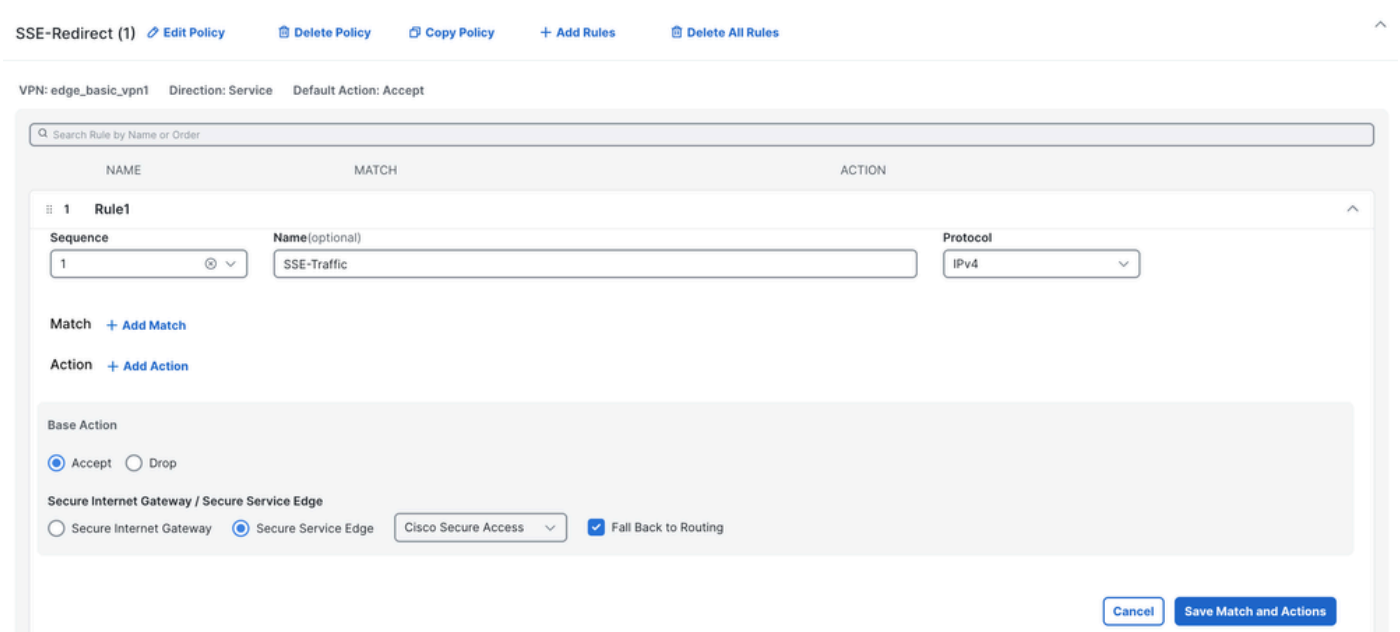
4. Seleccione + Agregar regla.



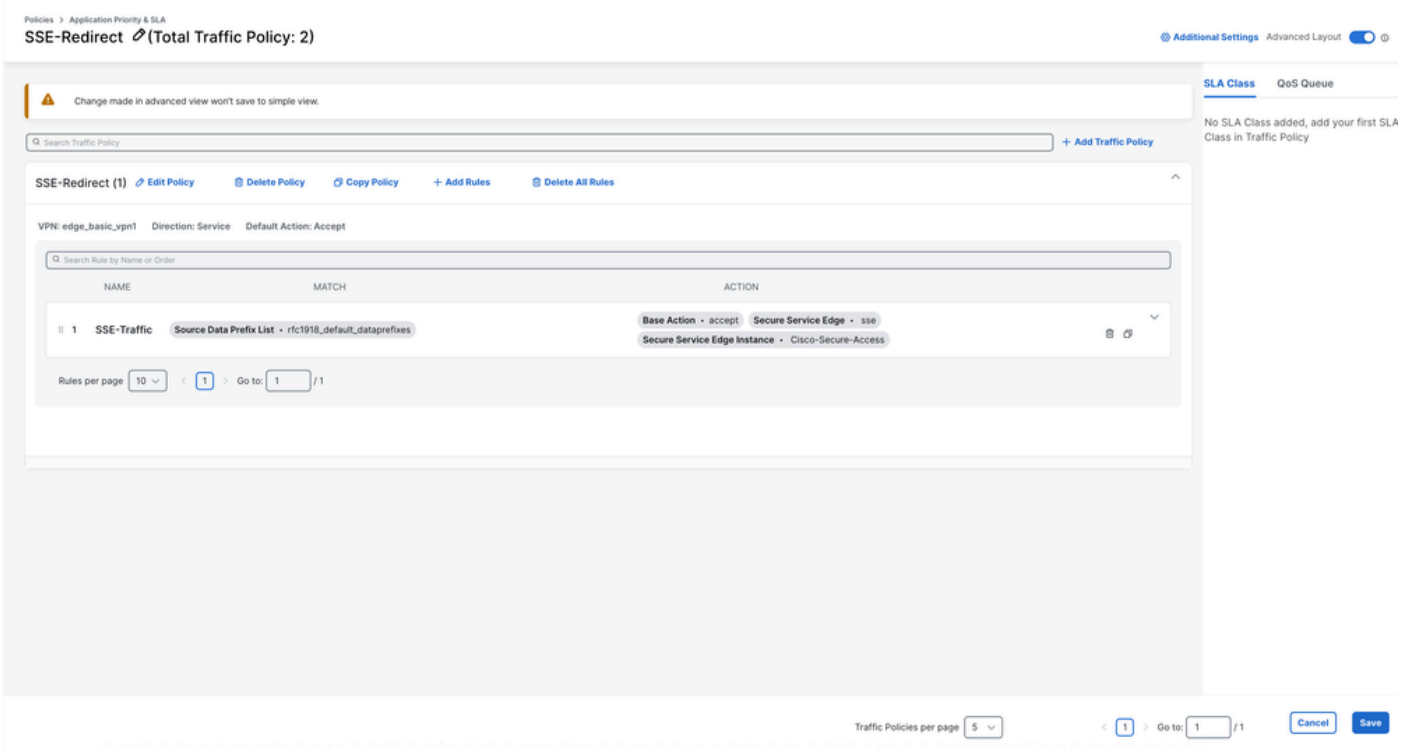
5. Configure los criterios de tráfico coincidentes para redirigir el tráfico al SSE.
6. Seleccione Aceptar como acción base y, a continuación, haga clic en + Acción.

7. Busque la acción Secure Internet Gateway / Secure Service Edge y establézcala en Secure Service Edge.



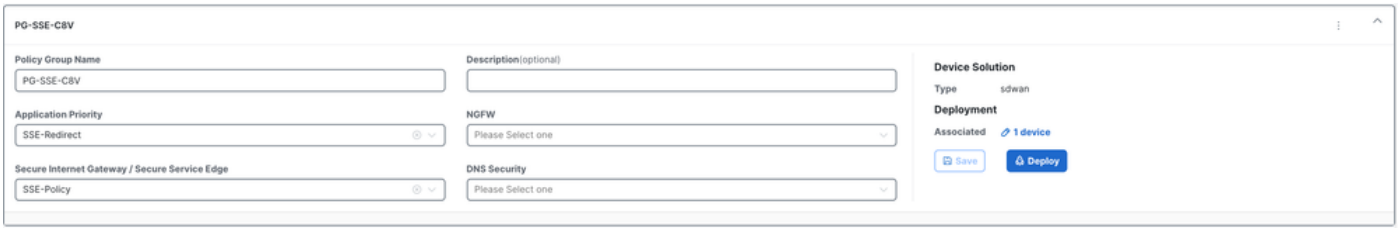


8. Haga clic en Guardar Coincidencia y Acciones



9. Haga clic en Guardar.

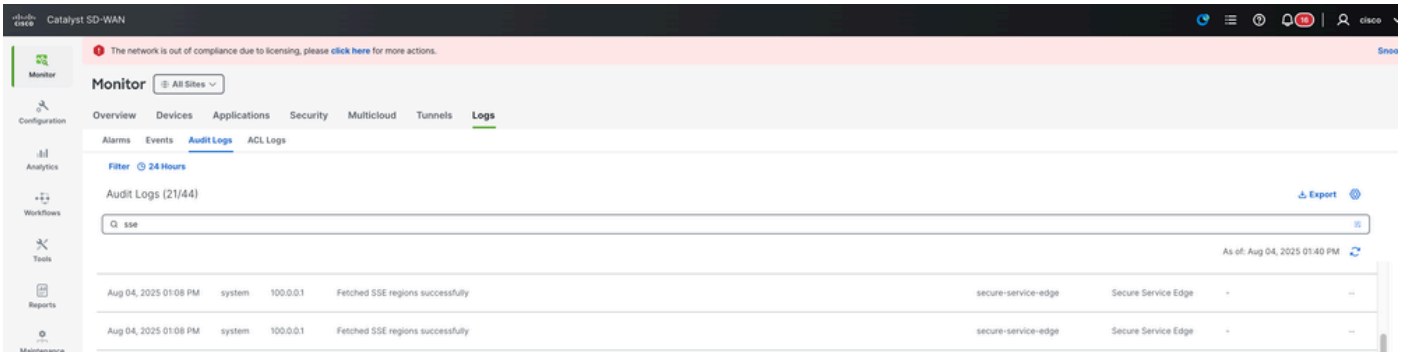
10. Navegue hasta Configuration > Policy Groups y seleccione la política Application Priority que acaba de crear. Guarde y, a continuación, implemente.



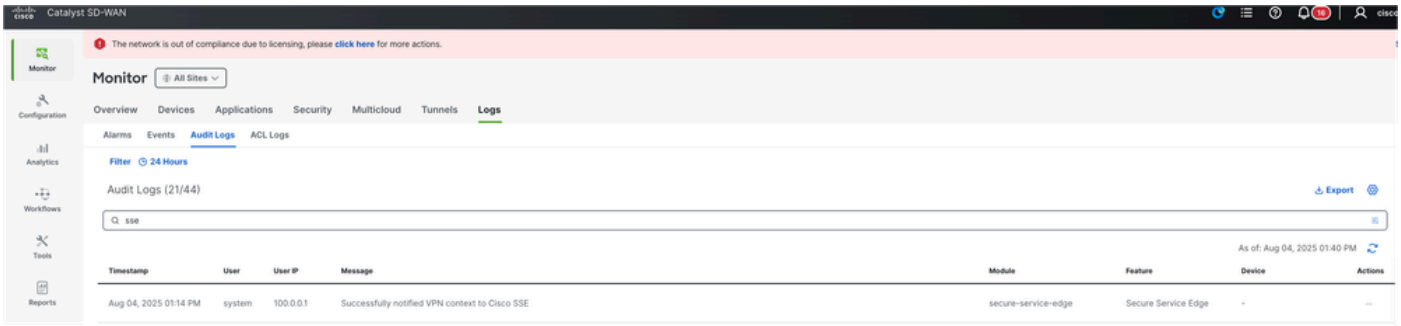
Verificación

Administrador

1. Supervisar > Registros > Registros de auditoría y buscar "sse".

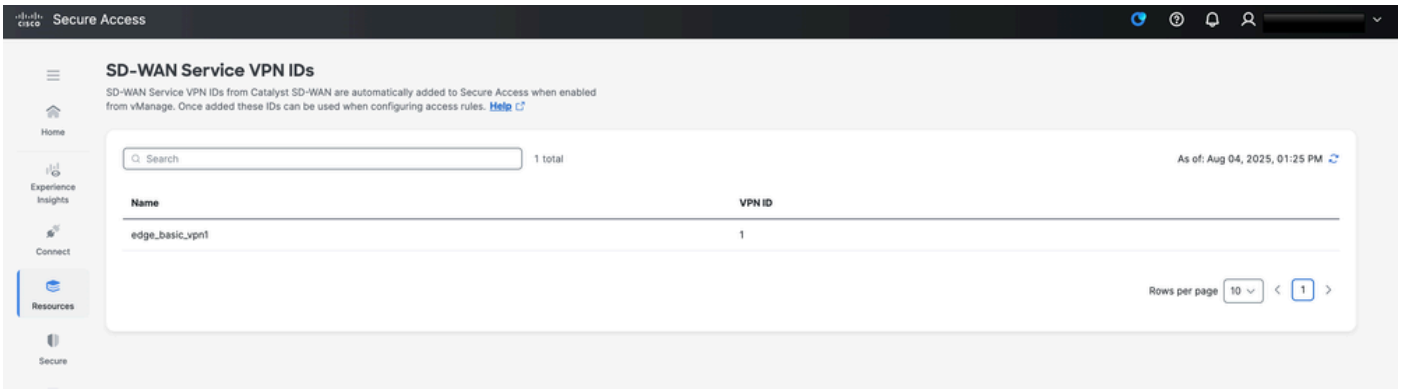


2. Puede verificar si la VPN de uso compartido de contexto está habilitada correctamente al verificar el Administrador.



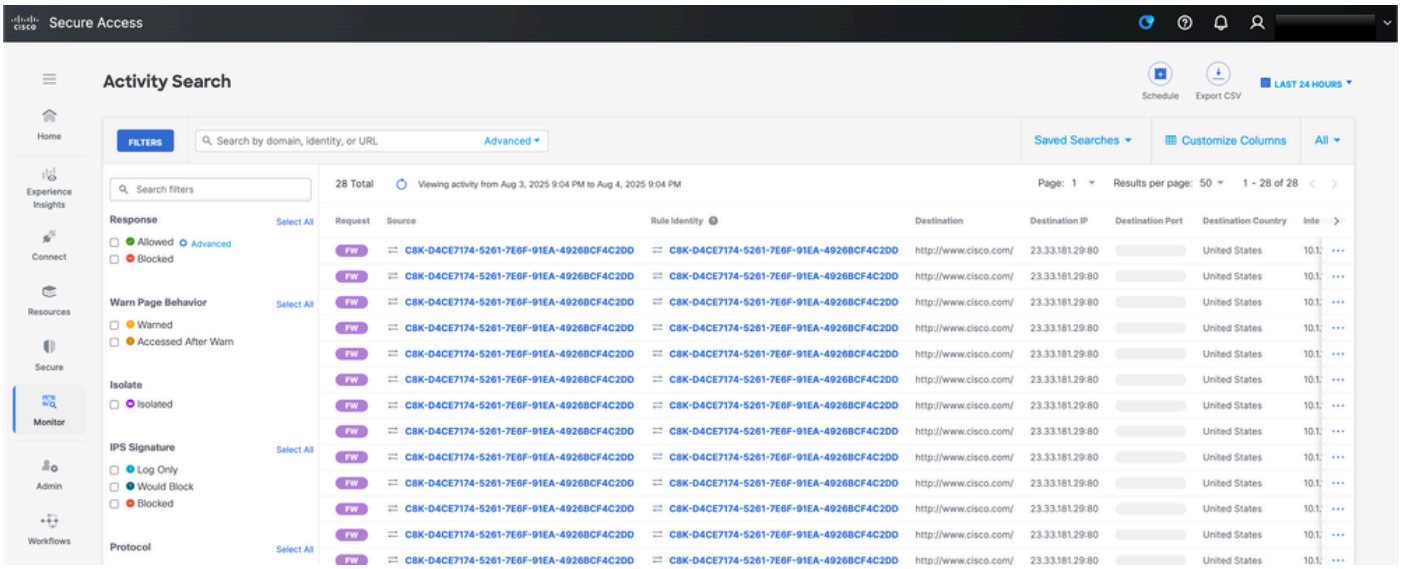
Panel de acceso seguro

Uso compartido de contexto
Puede verificar si la VPN de uso compartido de contexto se ha habilitado correctamente en el panel de SSE,Resources > ID de VPN de servicio SD-WAN



Túnel hacia arriba

Cuando el túnel está activo y el rastreador está operativo con tráfico fluyendo a través del túnel, puede validarlo navegando hasta Monitor > Búsqueda de actividad. En esta pantalla, puede ver el tráfico que pasa a través del túnel, como las solicitudes a www.cisco.com generadas por el rastreador. Esta visibilidad confirma que el rastreador está activo y monitorea activamente el tráfico a través del túnel



Comandos de la interfaz de línea de comandos (CLI)

<#root>

```
Hub2-SIG#show sse all
****************************************
SSE Instance Cisco-Secure-Access
****************************************
Tunnel name : Tunnel16000001
Site id: 2
Tunnel id: 655184839
SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD
HA role: Active
```

`Local state: Up`

`Tracker state: Up`

```
Destination Data Center: 44.217.195.188
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

Información Relacionada

- Configuración del uso compartido de contexto de SD-WAN
- Integración de Cisco Secure Access con routing SD
- Soporte Técnico y Documentación - Cisco Systems

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).