Configure o acesso seguro com túneis automatizados Catalyst SD-WAN para acesso privado seguro

Contents

Introdução

Este documento descreve como configurar o acesso seguro com túneis automatizados Catalyst SD-WAN para acesso privado seguro.

Informações de Apoio

À medida que as organizações vão além das redes tradicionais baseadas em perímetro, o acesso seguro a recursos privados se torna tão importante quanto a proteção do tráfego da Internet. Os aplicativos não estão mais confinados a um único data center, eles agora vivem em ambientes locais, nuvens públicas e arquiteturas híbridas. Essa mudança exige uma abordagem mais flexível e moderna para o acesso privado.

É aqui que entra em cena uma arquitetura baseada em SASE e o Cisco Secure Access. Em vez de depender de concentradores de VPN legados e acesso de rede linear, o Cisco Secure Access fornece conectividade privada como um serviço fornecido em nuvem, combinando VPN-as-a-Service (VPNaaS) e Zero Trust Network Access (ZTNA).

Para acesso privado em nível de rede, o Cisco Secure Access integra-se com SD-WAN usando túneis IPsec site a site automatizados. Esses túneis permitem que o tráfego privado flua com segurança entre o Secure Access e as redes locais ou em nuvem, enquanto mantém a inspeção de segurança e a aplicação de políticas centralizadas na nuvem. De uma perspectiva operacional, isso elimina a necessidade de implantar e manter headends de VPN tradicionais e simplifica o dimensionamento conforme o ambiente cresce.

Em um modelo de VPNaaS, o Secure Access atua como o ponto de terminação de VPN na nuvem. A SD-WAN lida com roteamento inteligente e resiliência com acesso seguro e garante que o tráfego seja protegido e governado por políticas de segurança consistentes antes de atingir recursos privados.

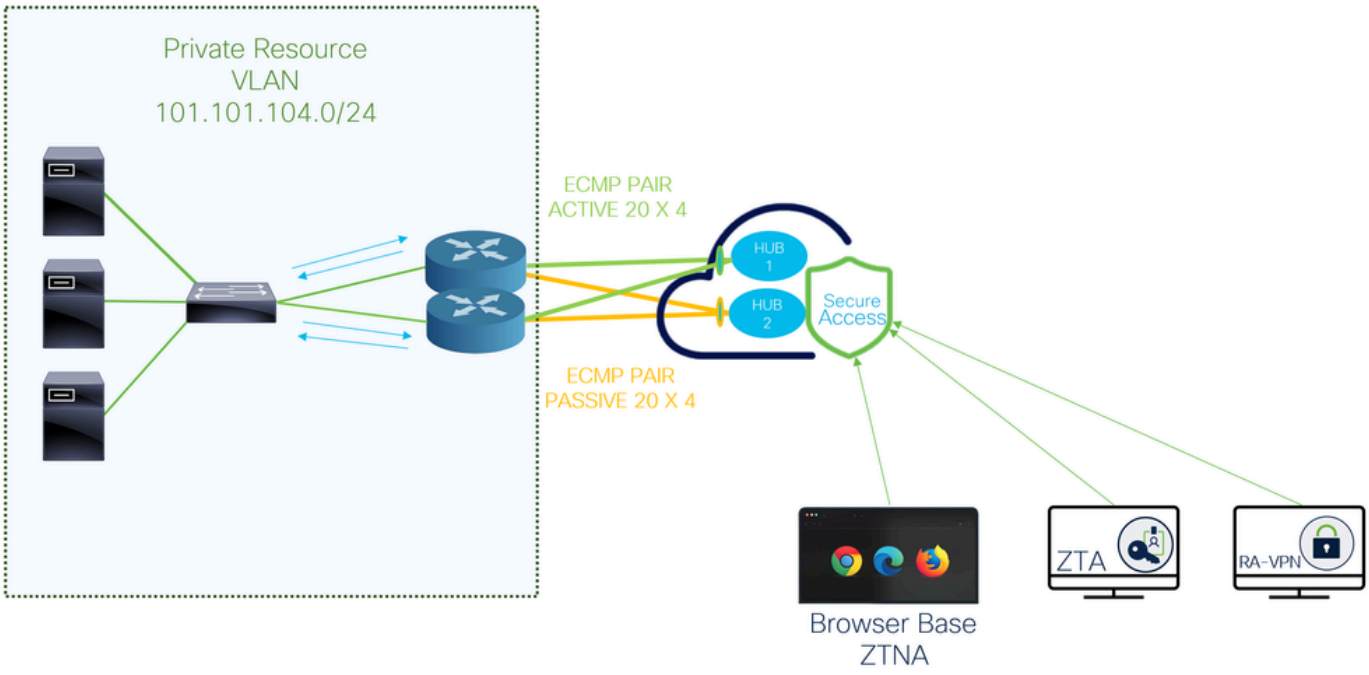
O Cisco Secure Access também suporta arquiteturas avançadas de túnel de site a site, incluindo backhaul multi-regional. Esse recurso permite que as organizações estabeleçam túneis para várias regiões do Secure Access simultaneamente, fornecendo redundância geográfica e maior disponibilidade. Ao se conectar a diferentes regiões, o tráfego pode falhar automaticamente em caso de interrupções regionais, degradação de latência ou eventos de manutenção.

Por exemplo, uma organização pode estabelecer túneis de site para site a partir de seu ambiente SD-WAN para regiões de acesso seguro em Londres e na Alemanha. Ambos os túneis permanecem ativos, permitindo acesso privado resiliente em todas as regiões e assegurando a continuidade, mesmo se uma região ficar indisponível. Esse design multirregional reforça a alta disponibilidade, melhora a tolerância a falhas e se alinha aos requisitos de resiliência de nível empresarial.

Para obter acesso mais granular, o Cisco Secure Access aplica o modelo Zero Trust Network Access (ZTNA). Em vez de conceder aos usuários ampla conectividade de rede, a ZTNA permite acesso apenas a aplicativos específicos, com base em identidade, postura do dispositivo e contexto. Essa abordagem reduz significativamente a superfície de ataque e se alinha aos princípios de Confiança Zero.

O acesso ZTNA é habilitado através de uma combinação de túneis de site a site e Conectores de Recursos. Os conectores de recursos são dispositivos virtuais leves que estabelecem conexões somente de saída para acesso seguro, o que significa que os recursos privados nunca precisam ser expostos diretamente à Internet.

Diagrama de Rede



Pré-requisitos

Requisitos

- Acesso seguro ao conhecimento
- Cisco Catalyst SD-WAN Manager versão 20.18.2 e Cisco IOS XE Catalyst SD-WAN versão 17.18.2 ou posterior
- Conhecimento intermediário de roteamento e comutação
- Conhecimento ECMP

- Conhecimento de VPN
- Como essa integração está na disponibilidade controlada, você precisa enviar um caso de TAC para solicitar a ativação do recurso no Cisco Secure Access

Componentes Utilizados

- Locatário de acesso seguro
- Catalyst SD-WAN Manager versão 20.18.2 e Cisco IOS XE Catalyst SD-WAN versão 17.18.2
- Gerenciador Catalyst SD-WAN

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

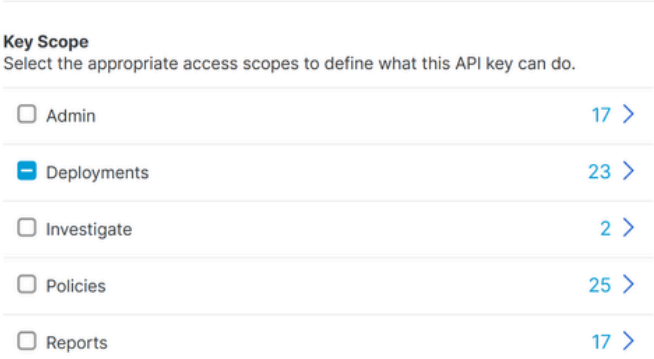
Configuração de acesso seguro

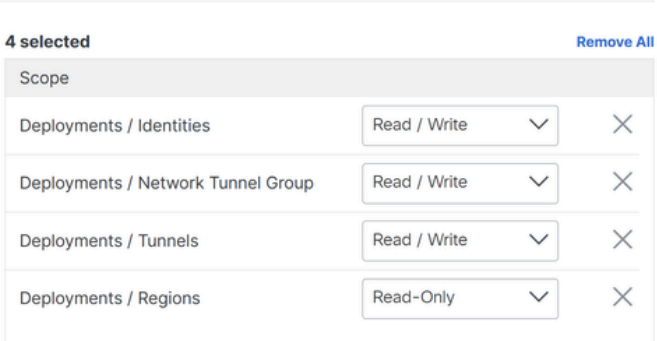
Criação de API

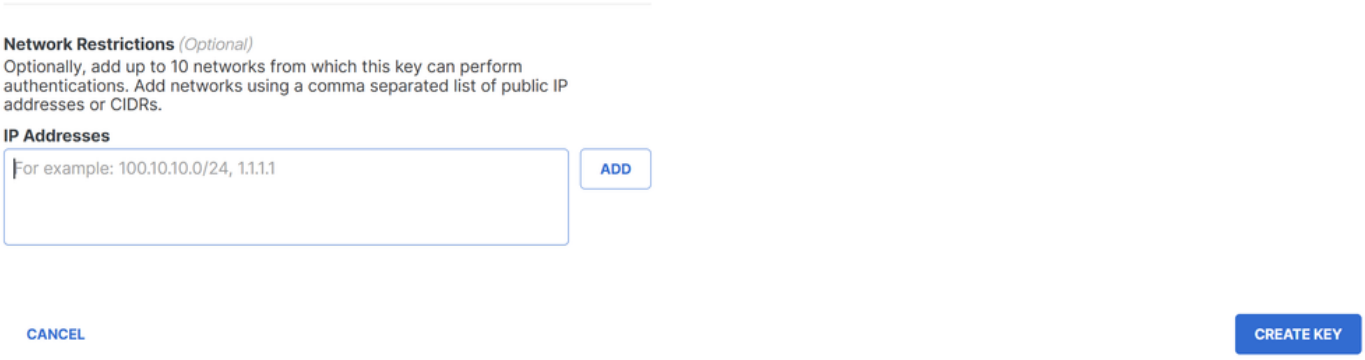
Para criar os túneis automatizados com o Secure Access, verifique as próximas etapas:

Navegue até Secure Access Dashboard.

- Clique em Admin > API Keys
- Clique em Add
- Escolha as próximas opções:
  - Deployments / Network Tunnel Group: Leitura/gravação
  - Deployments / Tunnels: Leitura/gravação
  - Deployments / Regions: Somente leitura
  - Deployments / Identities: Leitura/gravação
  - Expiry Date: Nunca expirar

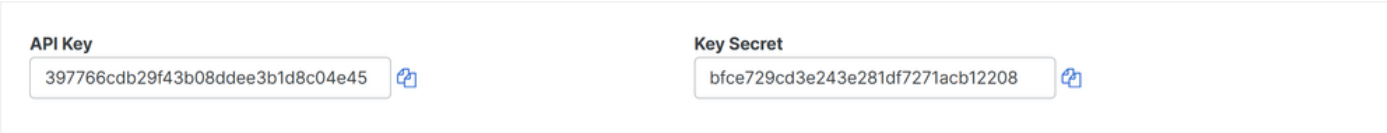






Note: Opcionalmente, adicione até 10 redes a partir das quais essa chave pode executar autenticações. Adicione redes usando uma lista separada por vírgulas de endereços IP públicos ou CIDRs.

- Clique CREATE KEY para finalizar a criação do API Key e Key Secret.



Caution: Copie-os antes de clicar em ACCEPT AND CLOSE; caso contrário, você precisará criá-los novamente e excluir aqueles que não foram copiados.

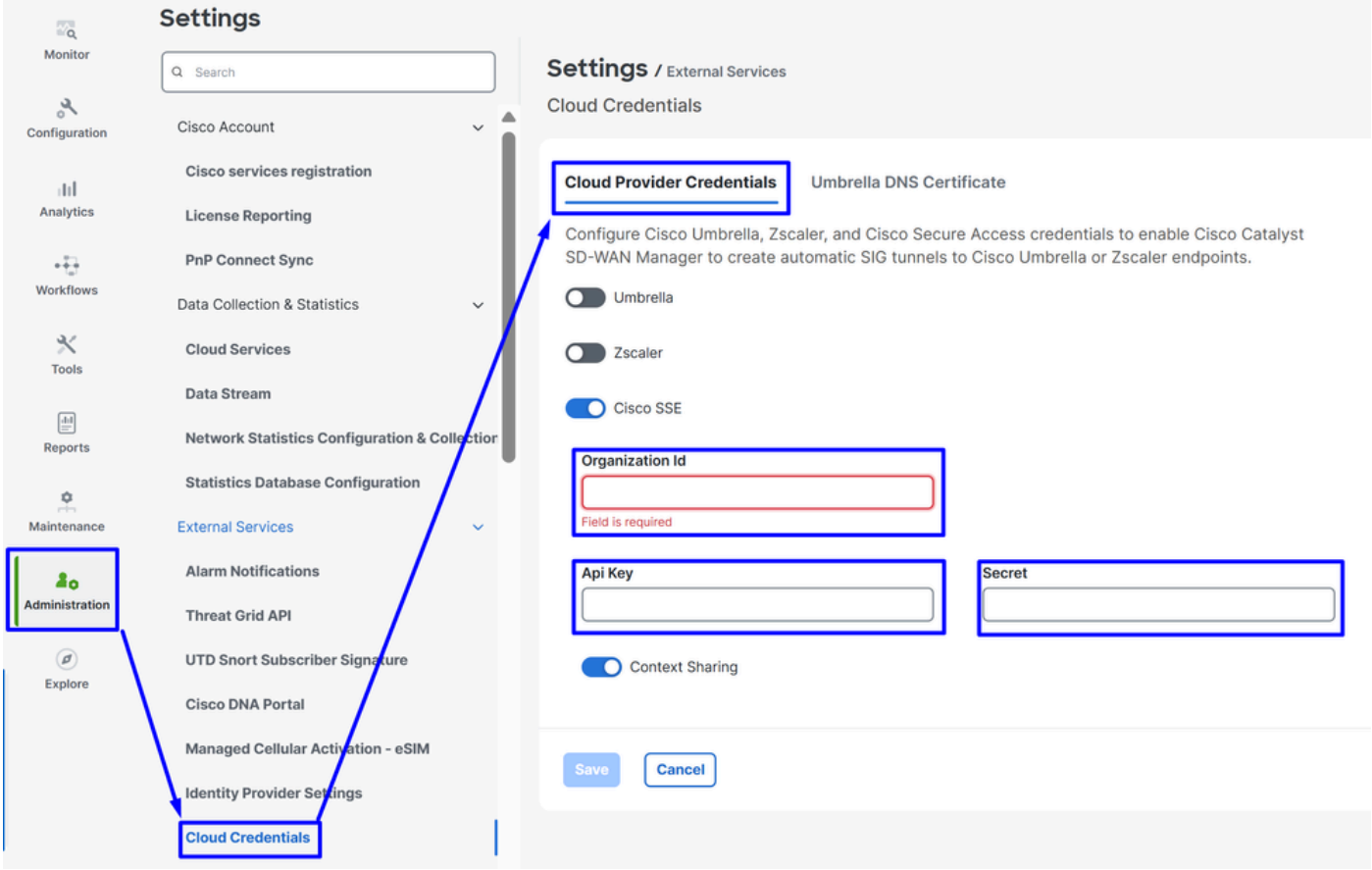
Para finalizar, clique em ACCEPT AND CLOSE.

Configuração de SD-WAN

Integração de API

Navegue até Catalyst SD-WAN Manager:

- Clique em **Administration** >Settings> Cloud Credentials
- Em seguida, clique em Cloud Provider Credentials e habilite Cisco SSEe preencha as configurações de API e organização



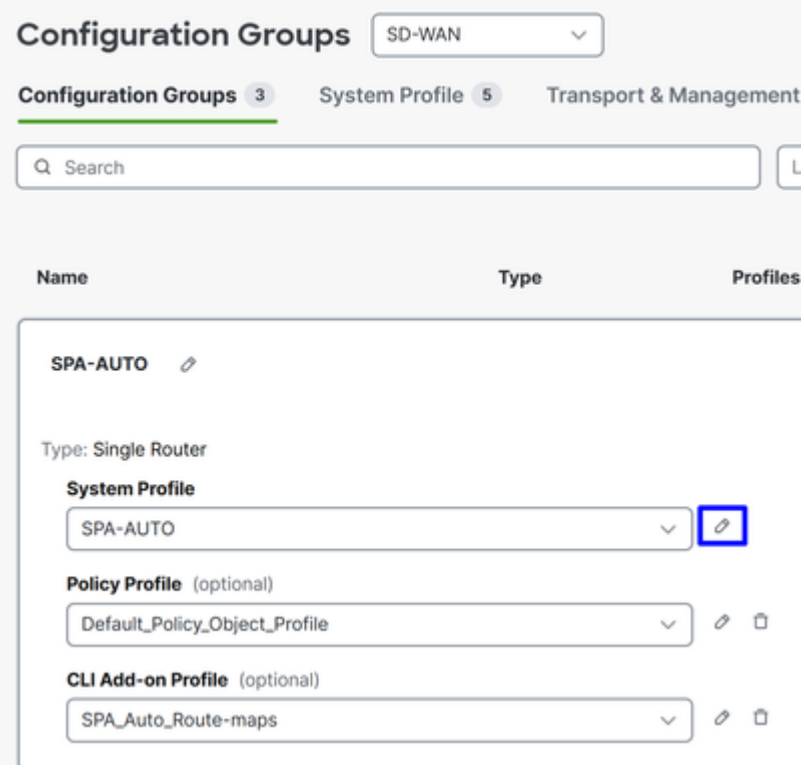
- **Organization ID**: Você pode obter isso no URL do seu Painel SSE https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Copie-o da etapa Secure Access Configuration
- Secret: Copie-o da etapa Secure Access Configuration

Depois disso, clique no botão Save.

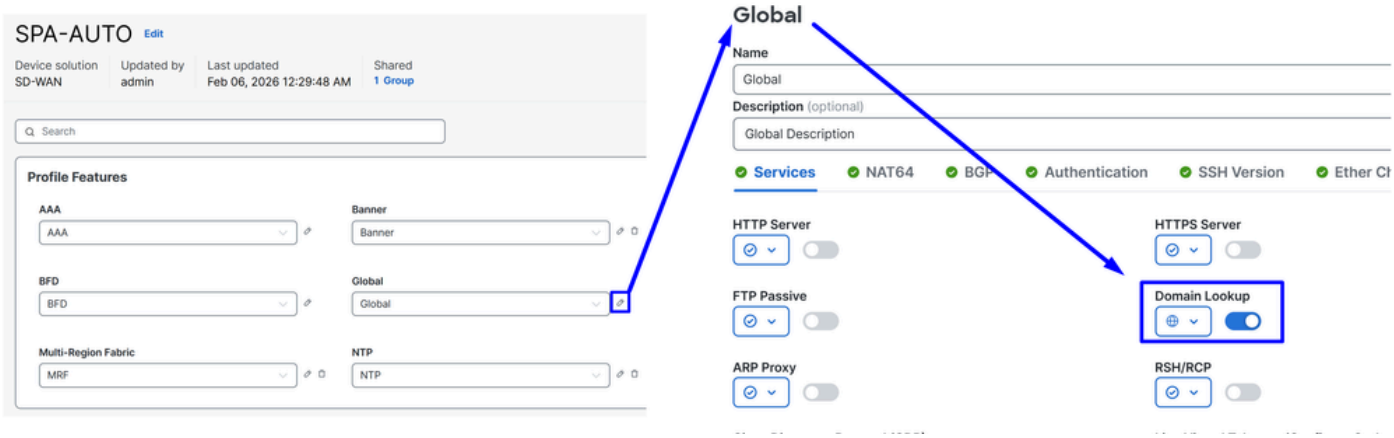
Note: Antes de prosseguir com as próximas etapas, você precisa ter certeza de que o Gerenciador de SD-WAN e as Bordas de SD-WAN do Catalyst possuem resolução DNS e acesso à Internet.

Para verificar se a pesquisa DNS está habilitada, navegue para:

- Clique em Configuration > Configuration Groups
- Clique no perfil de seus dispositivos de borda e edite o Perfil do sistema



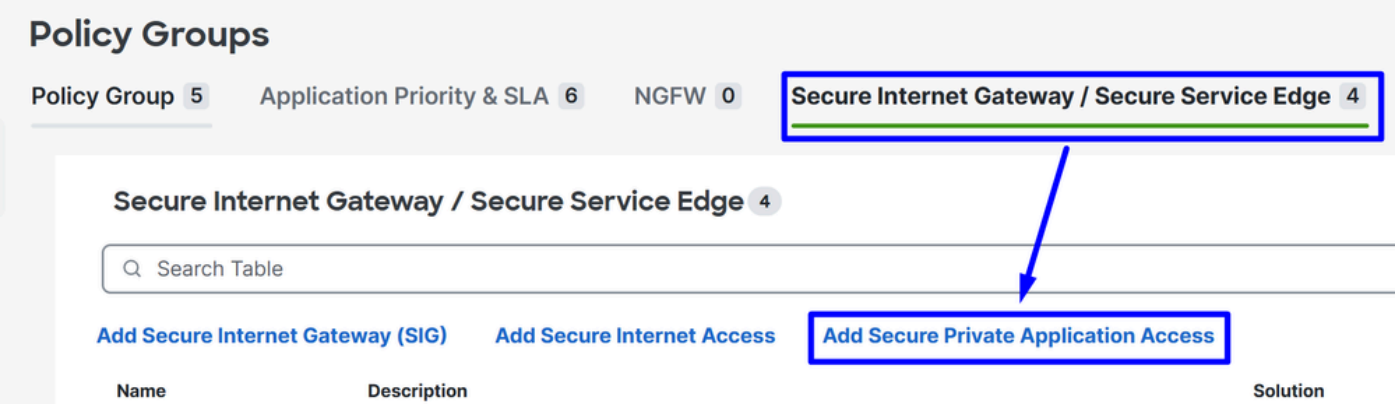
- Edite a opção Global e verifique se a opção Resolução de domínio está habilitada



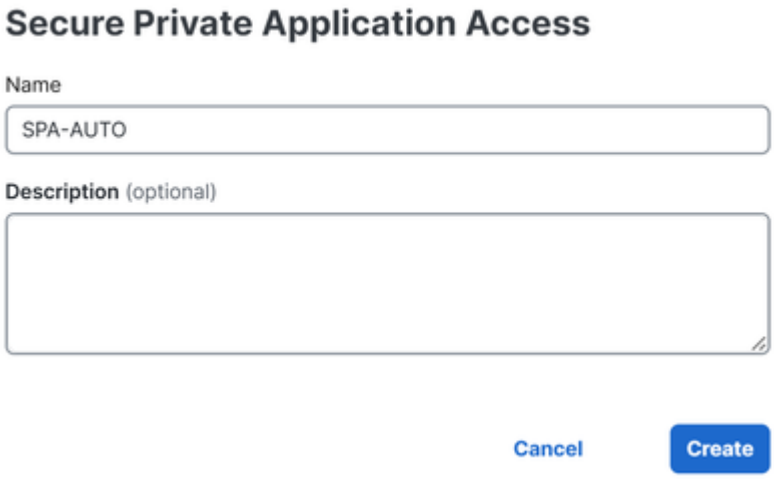
Configurar Grupo de Políticas

Navegue até Configuração > Grupos de política:

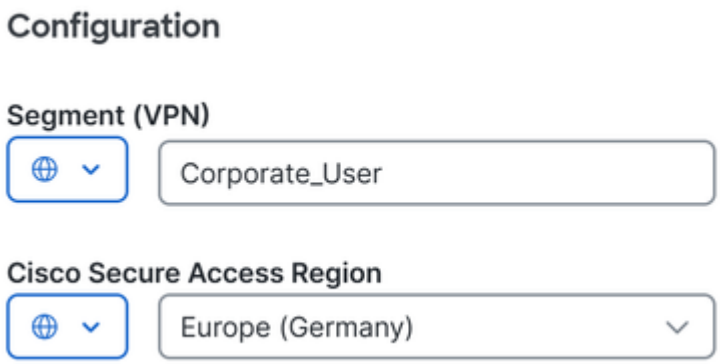
- Clique em Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- Configure um nome e clique em Create



As próximas configurações permitem que você crie os túneis depois de implantar a configuração nas Bordas Catalyst SD-WAN:

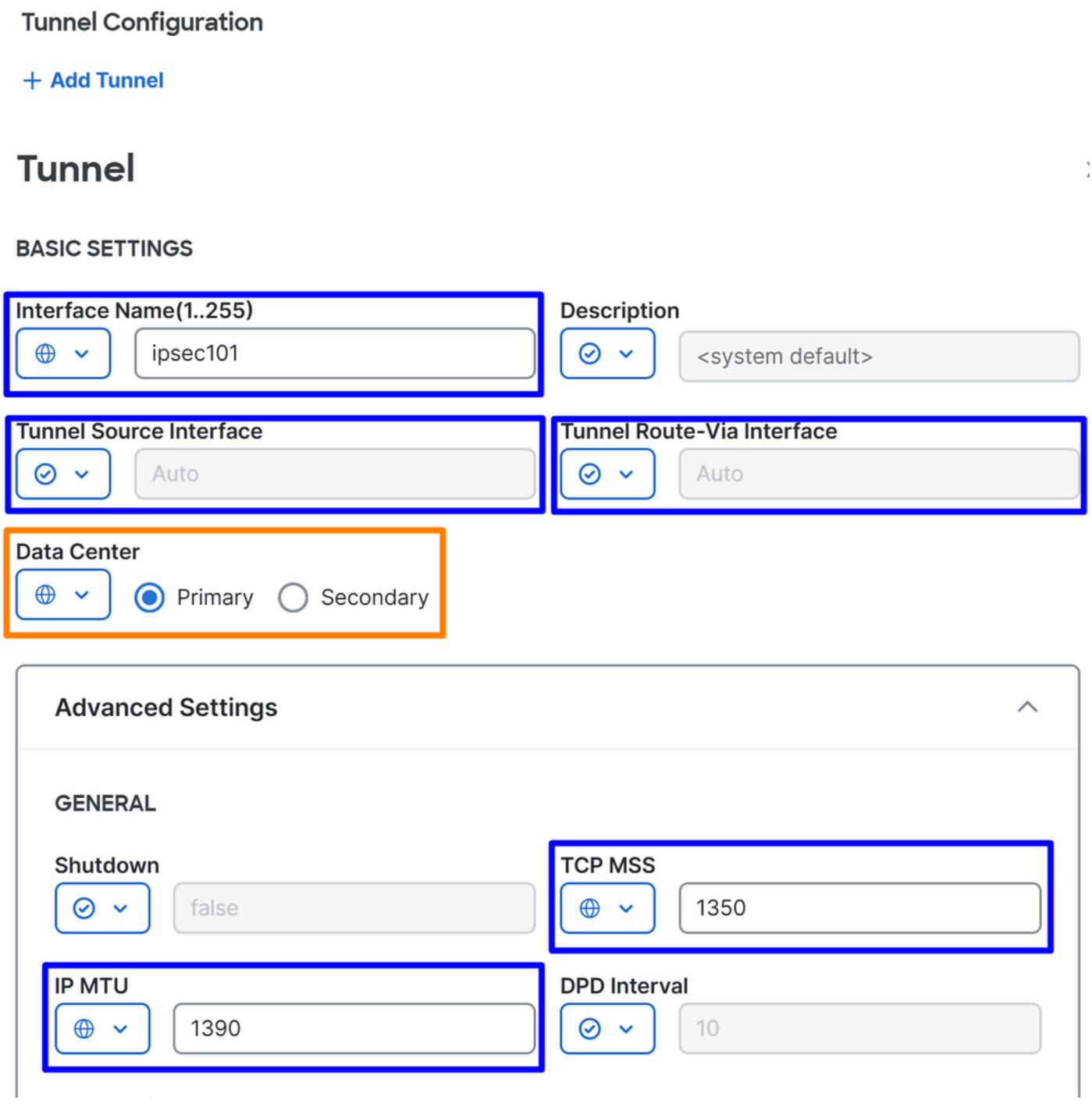


- Configuration
  - Segment (VPN): Escolha o VRF que hospeda os aplicativos a serem acessados por meio do Secure Access
  - Cisco Secure Access Region: Escolha a região mais próxima do hub ou filial SD-WAN onde os aplicativos estão hospedados

Em seguida, defina a configuração do túnel. Os túneis criados para o data center de acesso seguro primário estão ativos, enquanto os túneis criados para o data center de acesso seguro

secundário operam como backup.

Em Tunnel Configuration clique + Add Tunnel:



- Tunnel
  - Interface Name: Especifique o nome do túnel, que será atualizado automaticamente toda vez que um novo túnel for adicionado
  - Tunnel Source Interface: Não é necessário alterar essa configuração. Quando deixado como Auto, o sistema cria automaticamente uma interface de loopback com uma máscara /31.
  - Tunnel Route-Via Interface: Não é necessário alterar essa configuração. Por padrão, ele usa a primeira interface WAN física com NAT no roteador de borda, mas pode ser alterado se uma interface WAN específica for necessária

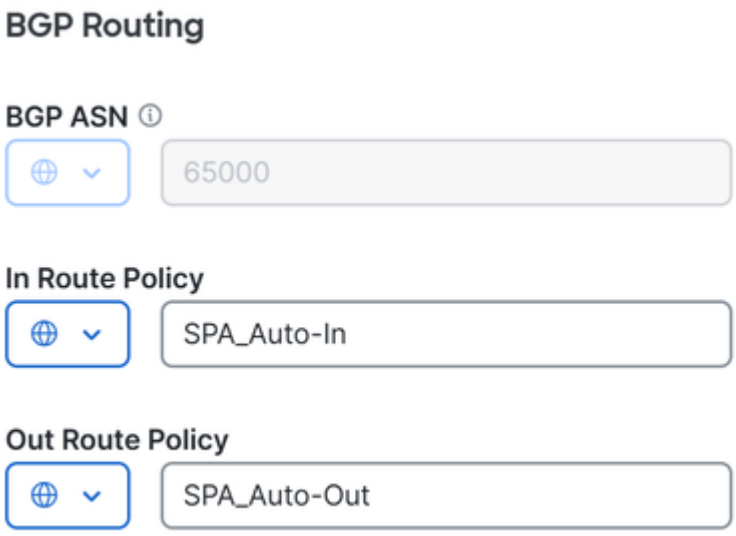
- Data Center: Selecione Principal ou Secundário de acordo. Se o túnel principal já estiver configurado, selecione Secondary (Secundário). Em cenários normais, um túnel pode ser configurado como primário e outro como secundário
- Advanced Settings
  - IP MTU: Usar 1390
  - TCP MSS: Usar 1350

Note: Se quiser criar vários túneis para ativar o ECMP e aumentar a capacidade do túnel, você pode configurar até 10 túneis ativos/10 túneis de backup por roteador. Isso fornece até 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:Se estiver implantando vários túneis por roteador, certifique-se de que a interface de transporte possa sustentar a largura de banda agregada de todos os túneis ativos combinados. Por exemplo, se dois túneis devem transportar até 1 Gbps cada, o link de transporte deve suportar pelo menos 2 Gbps de throughput.

Depois que os túneis estiverem configurados, continue com a configuração de BGP.



- **BGP Routing**
  - BGP ASN: Especifique o número AS para o hub SD-WAN. O 64512 AS é reservado para acesso seguro e não pode ser usado. Para obter mais informações sobre o BGP, consulte
  - In Route Policy: O sistema cria automaticamente essa política de rota de entrada com uma deny all instrução para evitar problemas de roteamento. Ele deve ser modificado manualmente por meio de um CLI Add-On Template para permitir/negar as rotas apropriadas.
  - Out Route Policy: O sistema cria essa política de rota de saída com uma deny all instrução para evitar problemas de roteamento. Ela deve ser editada manualmente por meio de uma CLI Add-On Template para permitir/negar as rotas apropriadas.

---

aviso: A partir de novembro de 2025, todas as organizações de acesso seguro recém-criadas usam o 32644 ASN público por padrão para peering BGP em grupos de túnel de rede. As organizações existentes estabelecidas antes de novembro de 2025 continuam a usar o 64512 ASN privado que anteriormente era reservado para pares BGP de acesso seguro. Se o número AS privado 64512 for atribuído a um dispositivo em sua rede, ele não poderá fazer peer com um grupo de túneis de rede configurado para o 64512 AS BGP de Peer (Acesso Seguro).

A configuração seguinte BGP e route-map é criada automaticamente para cada vizinho de BGP após você Deploy a nova política em seu Policy Group.

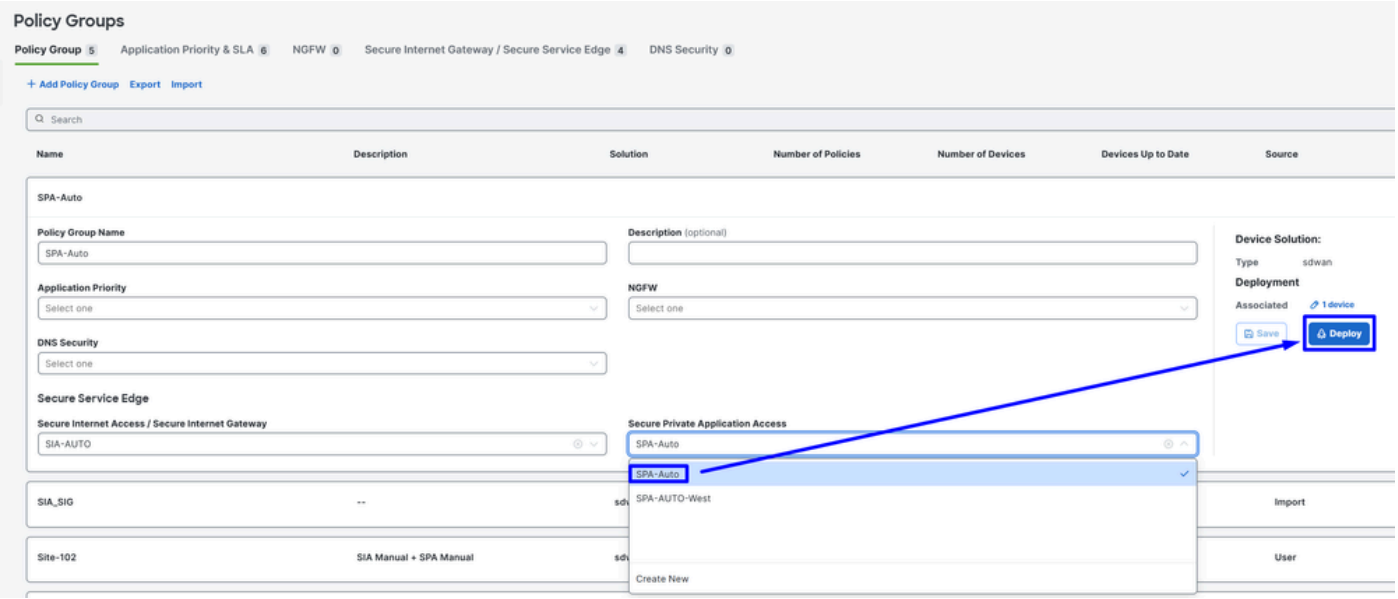
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

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
```

Depois disso, clique Save e continue com a implantação da política para ativar os túneis.

- Clique em Configuration > Policy Groups
- Escolha em Policy > Secure Service Edge > Secure Private Application Access e clique no perfil recente criado para o SPA.
- CliqueDeploypara finalizar



Para fazer o check-inSecure Access, execute as próximas etapas:

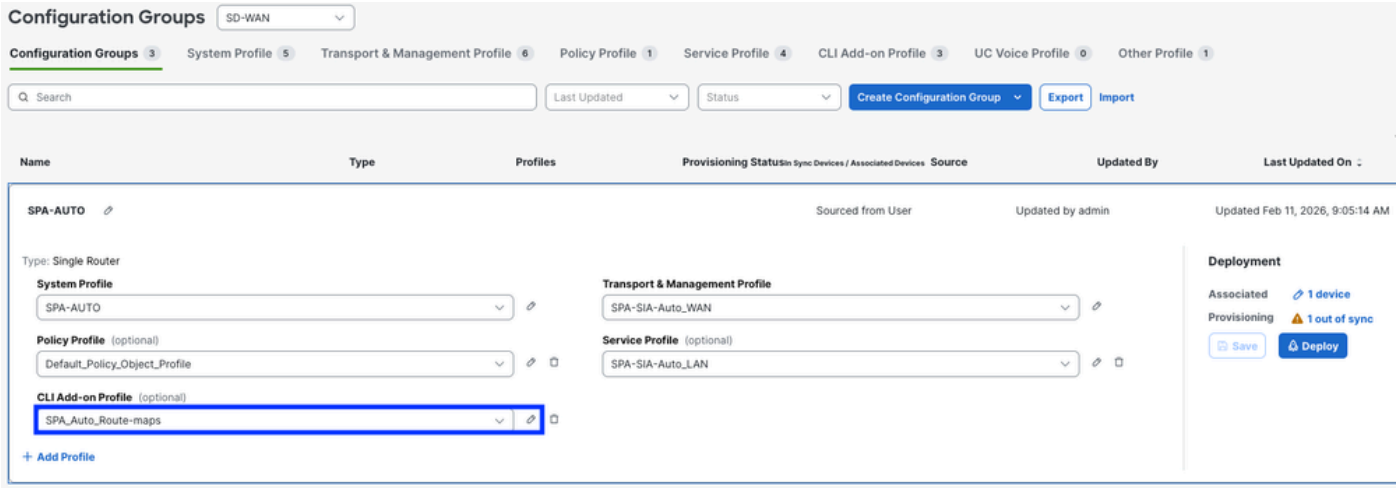
- Clique em Connect> Network Connections

ESTABELECIMENTO DE TÚNEL

Configurar roteamento

Navegue até Configure > Configuration Groups

- Clique em seu Configuration Group e em Criar/Editar seu CLI Add-on Profile



Para permitir a troca de rotas BGP, use o e o In Route Policy configurado anteriormente **Out Route Policy**. Você pode encontrar um exemplo básico para a configuração da CLI Add-On rota. Este modelo fornece um ponto de partida e deve ser personalizado conforme necessário:

```
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
```

---

aviso: É necessário um planejamento cuidadoso ao definir as redes permitidas de entrada e saída através de mapas de rota BGP. Permitir todas as rotas, como mostrado no exemplo acima, pode introduzir um comportamento de roteamento não intencional. Para

---

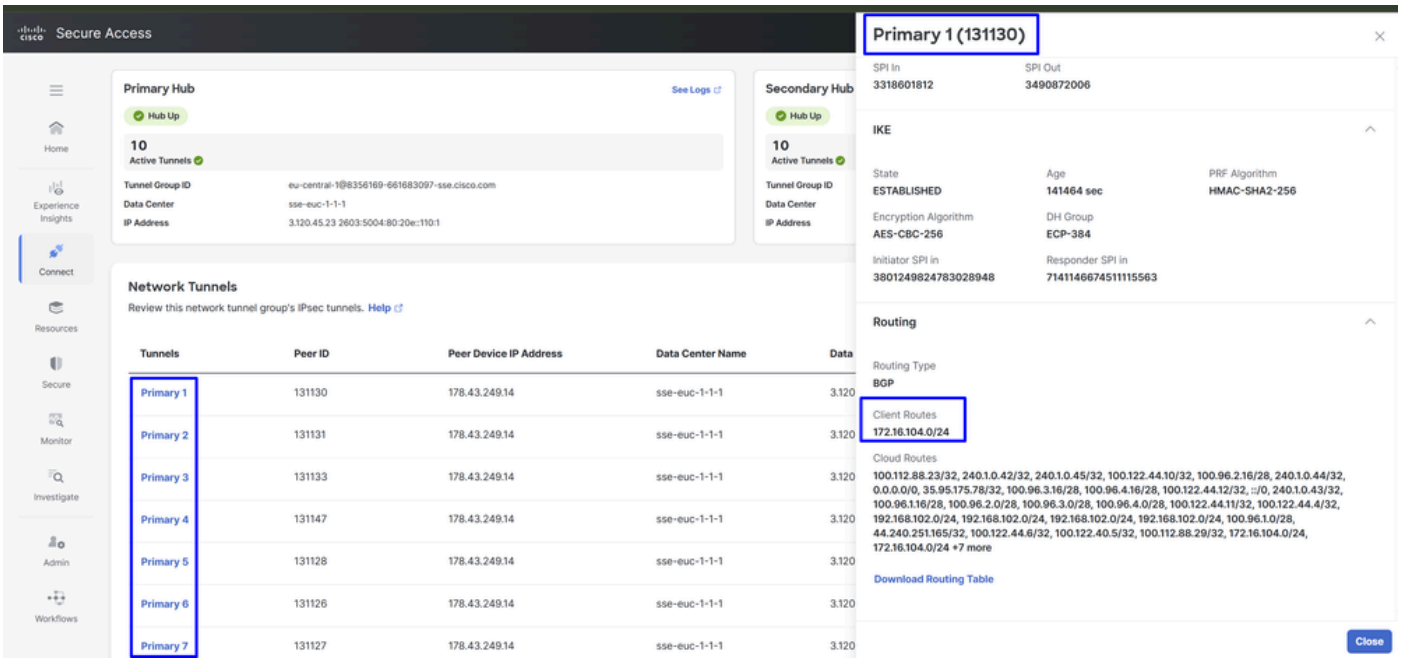
uma implantação ideal, especifique explicitamente apenas as redes necessárias em seus mapas de rota para garantir resultados de roteamento controlados e previsíveis

Agora você pode prosseguir para Deploy the changes

Para verificar se as rotas BGP são recebidas emSecure Access, verifique as próximas etapas:

- Clique em Connect> Network Connections > Network Tunnel Groups select e no nome do NTG

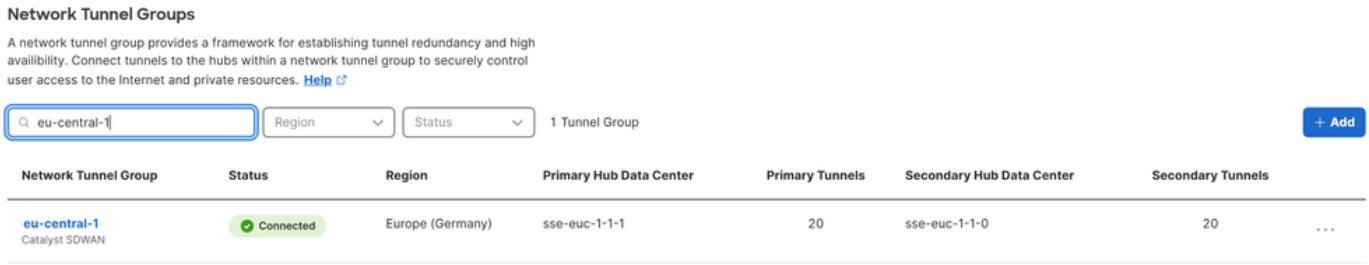
ESTABELECIMENTO DE ROTEAMENTO



Note: Neste exemplo, a sub-rede de usuário corporativo 172.16.104.0/24 é anunciada para Acesso Seguro através do BGP. Isso permite o roteamento apropriado entre o Catalyst SD-WAN e o ambiente SSE.

A mesma política pode ser aplicada a ambas as extremidades da WAN nos hubs Catalyst SD-WAN, resultando em 20 túneis ativos e 20 túneis em espera. O número total de túneis depende de quantos estão configurados em cada borda. Qualquer roteador conectado aos hubs de acesso seguro (hub 1 e hub 2) forma um par ECMP em todos os túneis estabelecidos.

Por exemplo, se o Catalyst SD-WAN Edge 1 tiver 10 túneis e o Catalyst SD-WAN Edge 2 tiver 10 túneis, o Secure Access formará o ECMP nos 20 túneis ativos. O mesmo comportamento se aplica ao hub SSE secundário.

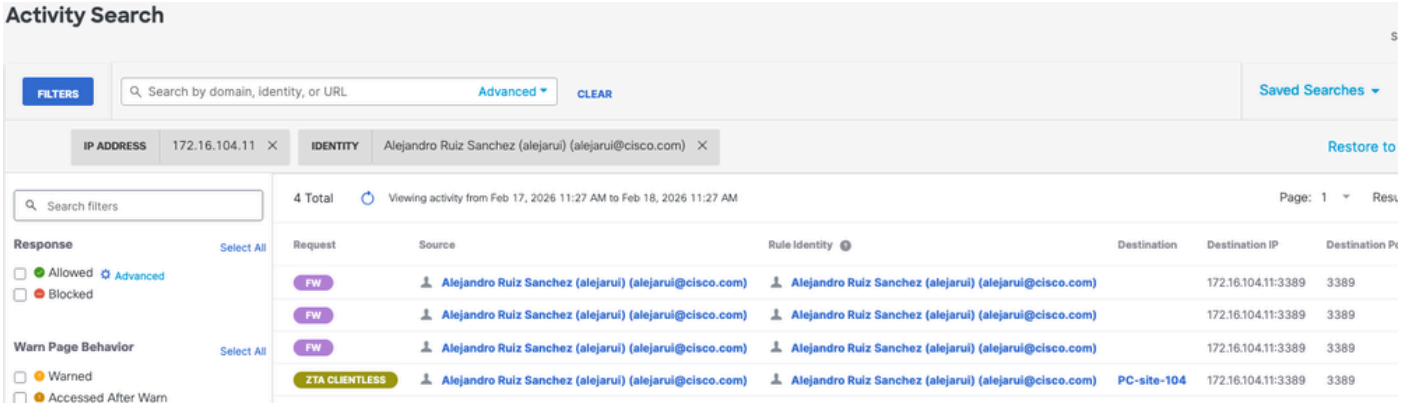


Verificar

para verificar se o tráfego está passando pelo Cisco Secure Access, navegue para Eventsou Activity Search ou Network-Wide Path Insightse filtre por sua identidade de túnel:

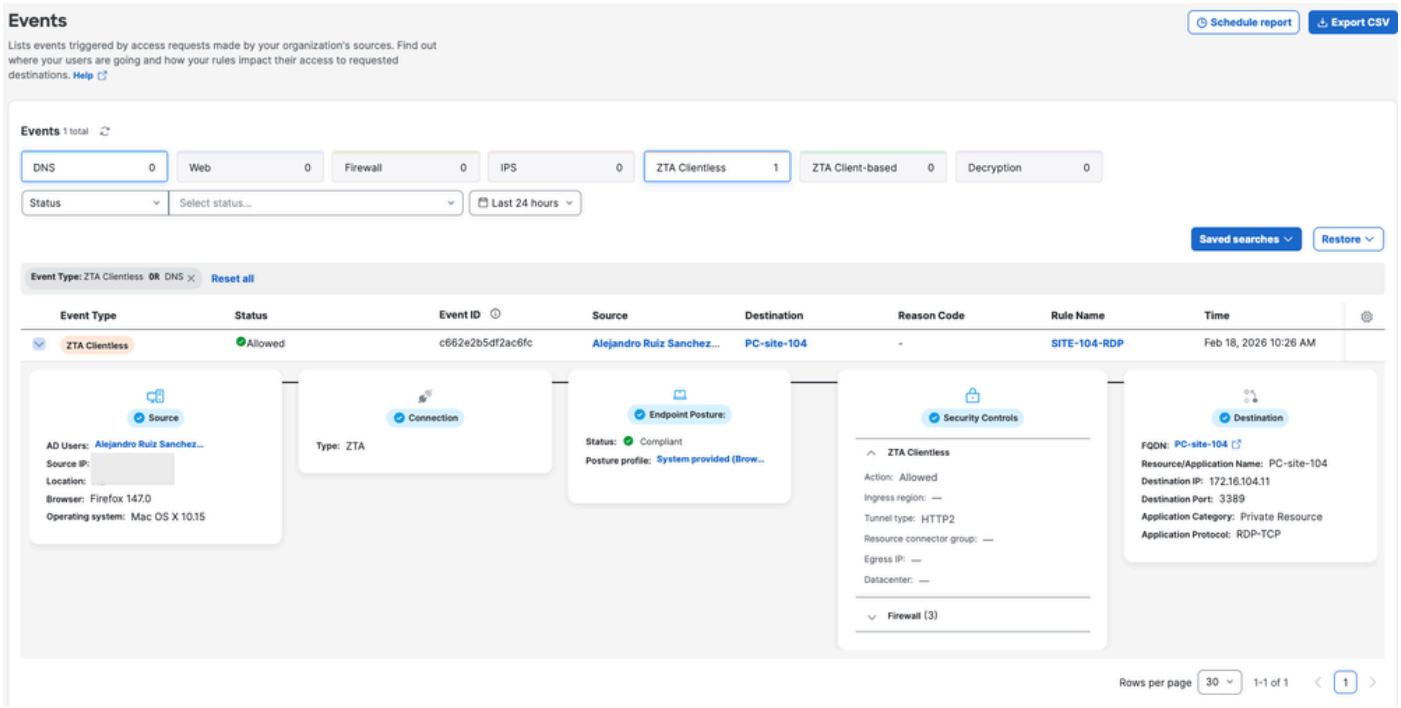
Acesso seguro - Pesquisa de atividades

Navegue até Monitor>Activity Search :



Acesso seguro - Eventos

Navegue até Monitor>Events:

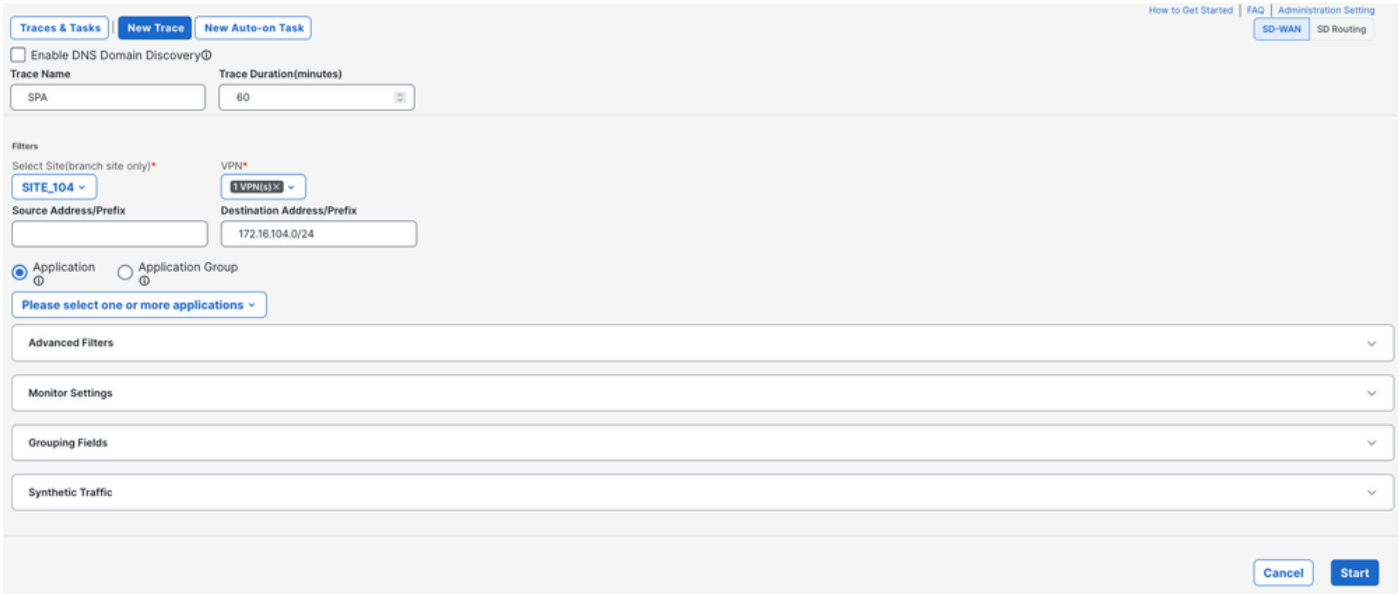


Note: Certifique-se de que sua política padrão esteja com o registro em log habilitado; por padrão, ela está desabilitada.

Catalyst SD-WAN Manager - Informações de caminho para toda a rede

Navegue até Catalyst SD-WAN Manager:

- Clique em Tools> Network-Wide Path Insights
- Clique em New Trace

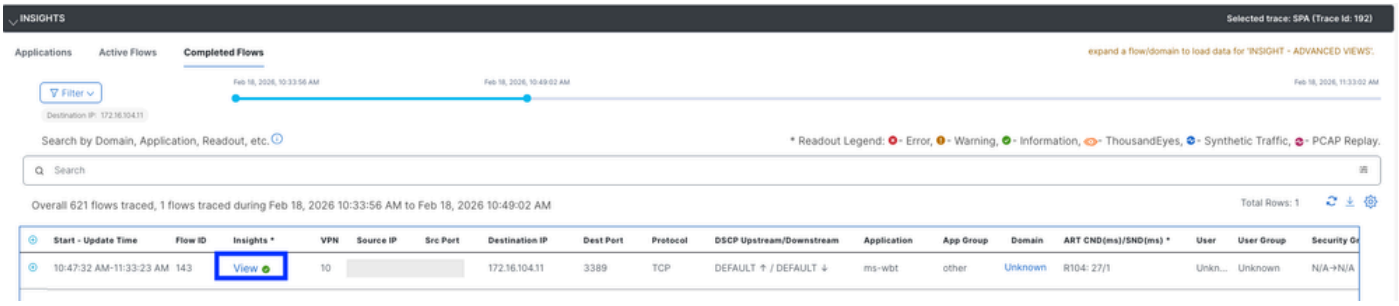


- Trace Name: (Opcional) Especificar o nome do rastreamento

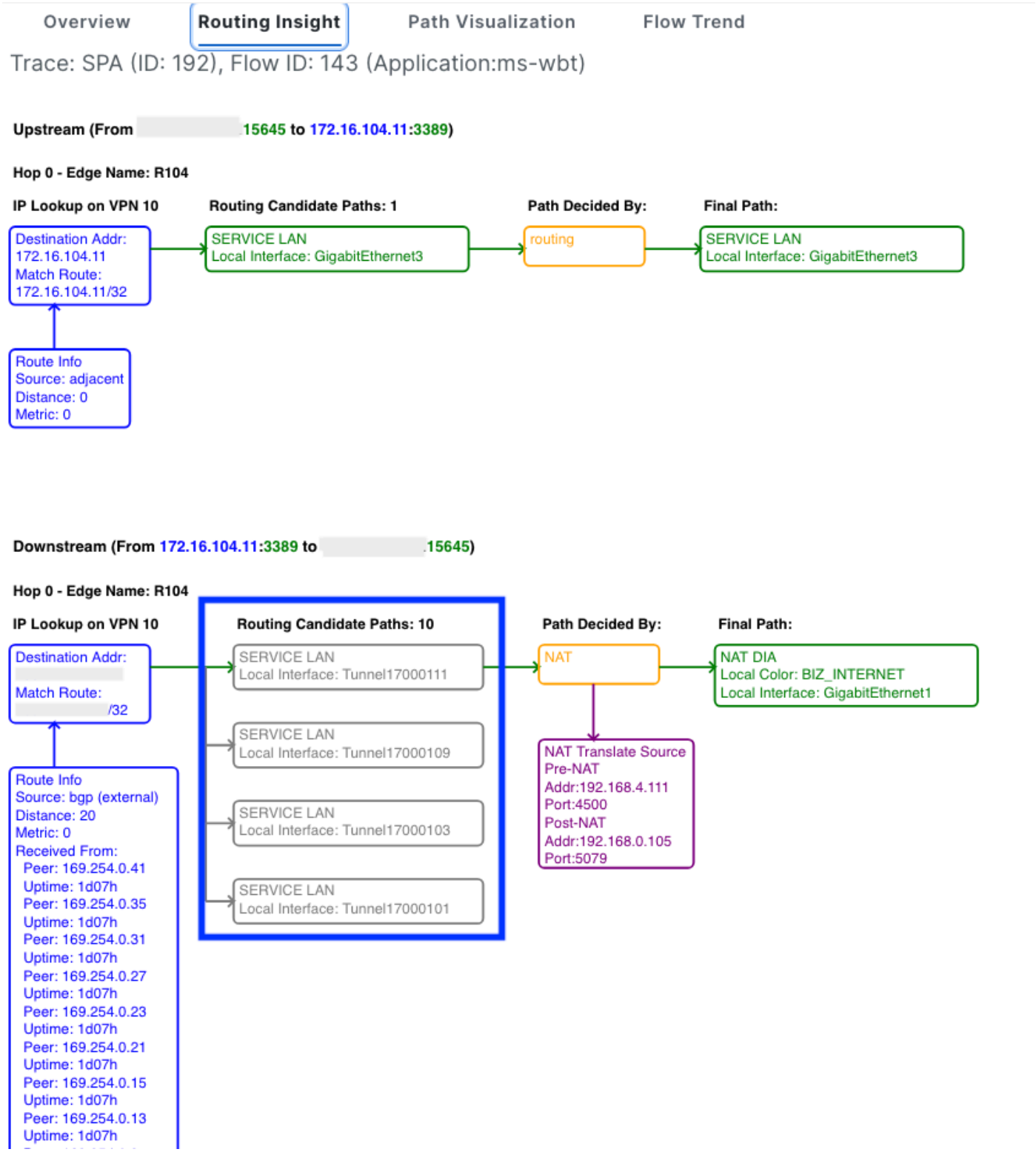
- Site: Escolha o site onde o recurso particular está localizado
- VPN: Escolha o ID da VPN onde o recurso privado está localizado
- Source/Destination Address: (Opcional) Insira o IP ou deixe-o em branco para capturar todo o tráfego filtrado com base em **Site**e VPNescolhido

Iniciar o rastreamento

Localize o fluxo de tráfego e clique em View na coluna Insights



A coluna Routing Insights exibe os caminhos candidatos e os túneis IPSec para Secure Access



Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Central de ajuda do Cisco Secure Access
- Guia de design do Cisco SASE
- Configure o acesso seguro com túneis automatizados SD-WAN para acesso seguro à Internet

- Guia de configuração de segurança do Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN versão 17.x
- Solução Cisco SASE: Resumo do Cisco Catalyst SD-WAN integrado ao Cisco Secure Access

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.