

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

Contents

[Introdução](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração de acesso seguro](#)

[Criação de API](#)

[Configuração de SD-WAN](#)

[Integração de API](#)

[Configurar Grupo de Políticas](#)

[Configurar roteamento](#)

[Verificar](#)

[Acesso seguro - Pesquisa de atividades](#)

[Acesso seguro - Eventos](#)

[Catalyst SD-WAN Manager - Informações de caminho para toda a rede](#)

[Informações Relacionadas](#)

Introdução

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



Secure Access and Catalyst SDWAN for Secure Private Access — with Automated Tunnels —

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.

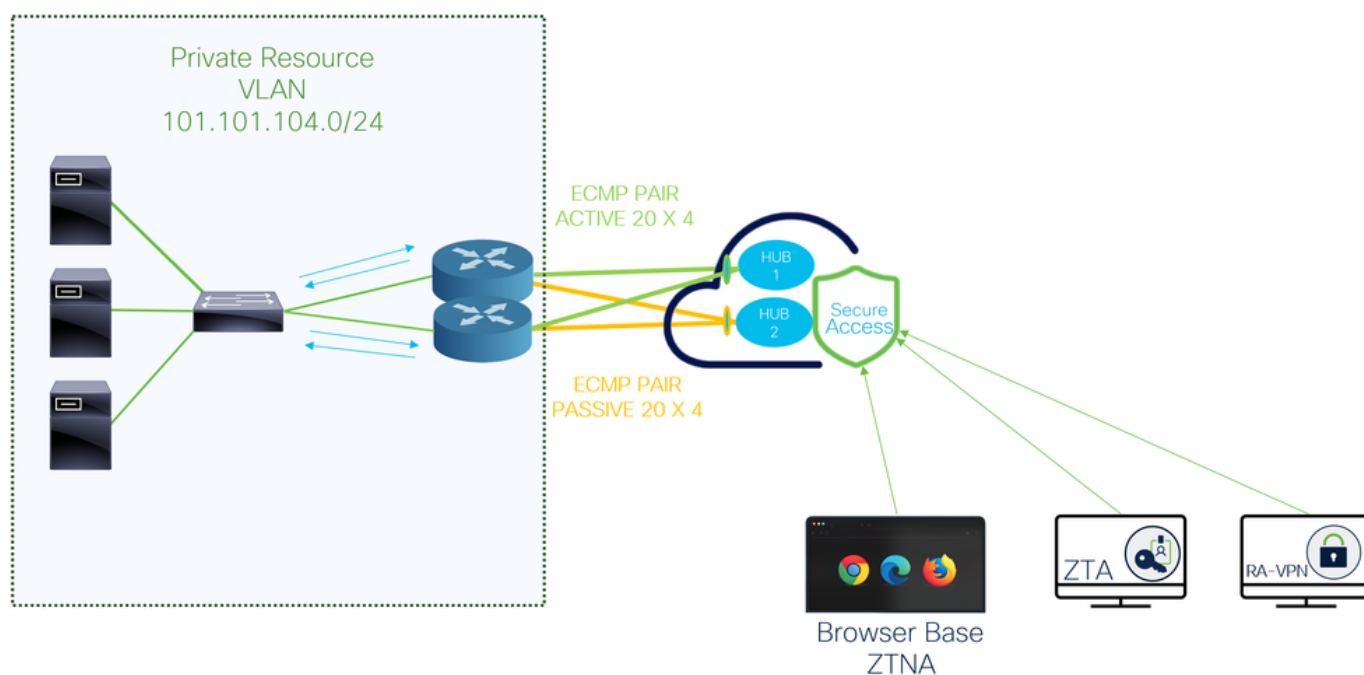
O Cisco Secure Access também suporta arquiteturas avançadas de túnel de site a site, incluindo backhaul multi-regional. Esse recurso permite que as organizações estabeleçam túneis para várias regiões do Secure Access simultaneamente, fornecendo redundância geográfica e maior disponibilidade. Ao se conectar 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**

Key Scope

Select the appropriate access scopes to define what this API key can do.

☐	Admin	17 >
☒	Deployments	23 >
☐	Investigate	2 >
☐	Policies	25 >
☐	Reports	17 >

4 selected

[Remove All](#)

Scope		
Deployments / Identities	Read / Write	×
Deployments / Network Tunnel Group	Read / Write	×
Deployments / Tunnels	Read / Write	×
Deployments / Regions	Read-Only	×

Network Restrictions *(Optional)*

Optionally, add up to 10 networks from which this key can perform authentications. Add networks using a comma separated list of public IP addresses or CIDRs.

IP Addresses

For example: 100.10.10.0/24, 1.1.1.1

ADD

CANCEL

CREATE KEY



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.

API Key

397766cdb29f43b08ddee3b1d8c04e45



Key Secret

bfce729cd3e243e281df7271acb12208



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 SSO** e preencha as configurações de API e organização

Settings

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

Explore

Search

Cisco Account

Cisco services registration

License Reporting

PnP Connect Sync

Data Collection & Statistics

Cloud Services

Data Stream

Network Statistics Configuration & Collection

Statistics Database Configuration

External Services

Alarm Notifications

Threat Grid API

UTD Snort Subscriber Signature

Cisco DNA Portal

Managed Cellular Activation - eSIM

Identity Provider Settings

Cloud Credentials

Settings / External Services

Cloud Credentials

Cloud Provider Credentials Umbrella DNS Certificate

Configure Cisco Umbrella, Zscaler, and Cisco Secure Access credentials to enable Cisco Catalyst SD-WAN Manager to create automatic SIG tunnels to Cisco Umbrella or Zscaler endpoints.

☐ Umbrella

☐ Zscaler

☒ Cisco SSE

Organization Id

Field is required

Api Key

Secret

☒ Context Sharing

Save **Cancel**

- **Organization ID:** Você pode obter isso no URL do seu Painei 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

Configuration Groups SD-WAN

Configuration Groups 3 **System Profile** 5 **Transport & Management**

Q Search

Name	Type	Profiles
SPA-AUTO		

Type: Single Router

System Profile

SPA-AUTO

Policy Profile (optional)

Default_Policy_Object_Profile

CLI Add-on Profile (optional)

SPA_Auto_Route-maps

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

SPA-AUTO [Edit](#)

Device solution: SD-WAN | Updated by: admin | Last updated: Feb 06, 2026 12:29:48 AM | Shared: 1 Group

Q Search

Profile Features

AAA	Banner
BFD	Global
Multi-Region Fabric	NTP

Global

Name: Global

Description (optional): Global Description

Services NAT64 BGP Authentication SSH Version Ether C

HTTP Server ☐

FTP Passive ☐

ARP Proxy ☐

HTTPS Server ☐

Domain Lookup ☒

RSH/RCP ☐

Configurar Grupo de Políticas

Navegue até Configuração > Grupos de política:

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

Policy Groups

Policy Group 5 Application Priority & SLA 6 NGFW 0 **Secure Internet Gateway / Secure Service Edge 4**

Secure Internet Gateway / Secure Service Edge 4

Q Search Table

[Add Secure Internet Gateway \(SIG\)](#) [Add Secure Internet Access](#) **[Add Secure Private Application Access](#)**

Name	Description	Solution
------	-------------	----------

- Configure um nome e clique em **Create**

Secure Private Application Access

Name

SPA-AUTO

Description (optional)

[Cancel](#) [Create](#)

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

Configuration

Segment (VPN)

  Corporate_User

Cisco Secure Access Region

  Europe (Germany) 

- 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 Configuration

[+ Add Tunnel](#)

Tunnel

BASIC SETTINGS

Interface Name(1..255) ipsec101	Description <system default>
Tunnel Source Interface Auto	Tunnel Route-Via Interface Auto
Data Center ☐ Primary ☐ Secondary	

Advanced Settings

GENERAL

Shutdown false	TCP MSS 1350
IP MTU 1390	DPD Interval 10

- 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	✎ 🗑
ipsec110	🔍	🔍 Auto	🔍 Auto	🔍 Secondary	✎ 🗑
ipsec111	🔍	🔍 Auto	🔍 Auto	🔍 Primary	✎ 🗑
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	✎ 🗑

MAXIMUM OF 10 TUNNELS PER HUB

10 x 1 Primary

10 x 1 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 ⓘ

 ▼

65000

In Route Policy

 ▼

SPA_Auto-In

Out Route Policy

 ▼

SPA_Auto-Out

- **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.
- Clique **Deploy** para finalizar

Policy Groups

Policy Group 5 Application Priority & SLA 6 NGFW 0 Secure Internet Gateway / Secure Service Edge 4 DNS Security 0

+ Add Policy Group Export Import

Q Search

Name	Description	Solution	Number of Policies	Number of Devices	Devices Up to Date	Source
SPA-Auto						
SIA_SIG	--	sdw				Import
Site-102	SIA Manual + SPA Manual	sdw				User

SPA-Auto Configuration:

Policy Group Name: SPA-Auto

Description (optional):

Application Priority: Select one

DNS Security: Select one

Secure Service Edge: Secure Internet Access / Secure Internet Gateway

Secure Private Application Access: SPA-Auto

Device Solution: Type: sdwan

Deployment: Associated: 1 device

Buttons: Save, Deploy

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

- Clique em **Connect> Network Connections**

ESTABELECIMENTO DE TÚNEL

eu-central-1

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

Summary

Region: Europe (Germany)

Device Type: Catalyst SD-WAN

Last Status Update: Feb 04, 2026 10:12 PM

Routing Type: Dynamic Routing (BGP)

Device BGP AS: 65000

Peer (Secure Access) BGP AS: 64512

BGP Peer (Secure Access) IP Addresses: 169.254.0.9, 169.254.0.5, 2a04:a4a:8::723:647:0000:120

Multipath BGP Addresses: --

Multipath TTL: --

MAX 20 TUNNELS PER DEVICE CONNECTED TO THE NETWORK TUNNEL GROUP

10 X 1 Primary Hub

10 X 1 Secondary Hub

Primary Hub

10 Active Tunnels

Tunnel Group ID: eu-central-108336169-661683087-aaa.cisco.com

Data Center: ssa-eu-1-1-1

IP Address: 3.120.45.23 2603:5004:80:20a::101

Secondary Hub

10 Active Tunnels

Tunnel Group ID: eu-central-108336169-661683089-aaa.cisco.com

Data Center: ssa-eu-1-1-0

IP Address: 16.156.145.74 2603:5004:80:20a::101

Configurar roteamento

Navegue até [Configure > Configuration Groups](#)

- Clique em seu [Configuration Group](#) e em [Criar/Editar seu CLI Add-on Profile](#)

The screenshot shows the 'Configuration Groups' page for the 'SD-WAN' group. The 'SPA-AUTO' configuration is displayed, showing various profiles assigned to it. The 'CLI Add-on Profile' is highlighted with a red box, showing 'SPA_Auto_Route-maps'. The 'Deployment' section on the right indicates that 1 device is associated and 1 out of sync.

Name	Type	Profiles	Provisioning Status	Sync Devices / Associated Devices	Source	Updated By	Last Updated On
SPA-AUTO	Single Router	System Profile: SPA-AUTO Policy Profile (optional): Default_Policy_Object_Profile CLI Add-on Profile (optional): SPA_Auto_Route-maps	Sourced from User	Updated by admin			Updated Feb 11, 2026, 9:05:14 AM

Para permitir a troca de rotas BGP, use 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 em [Secure Access](#), verifique as próximas etapas:

- Clique em [Connect](#) > [Network Connections](#) > [Network Tunnel Groups select](#) e no nome do NTG

ESTABELECIMENTO DE ROTEAMENTO

The screenshot displays the Cisco Secure Access interface. On the left, a sidebar contains navigation options: Home, Experience Insights, Connect (highlighted), Resources, Secure, Monitor, Investigate, Admin, and Workflows. The main content area is divided into two sections: 'Primary Hub' and 'Secondary Hub'. Both hubs show '10 Active Tunnels'. Below these, a 'Network Tunnels' table lists tunnels with columns: Tunnels, Peer ID, Peer Device IP Address, Data Center Name, and Data. The 'Primary 1' tunnel is highlighted. To the right, a detailed view for 'Primary 1 (131130)' is shown, including SPI In (3318601812), SPI Out (3490872006), IKE status (ESTABLISHED), Age (141464 sec), PRF Algorithm (HMAC-SHA2-256), Encryption Algorithm (AES-CBC-256), DH Group (ECP-384), Initiator SPI In (3801249824783028948), Responder SPI In (7141146674511115563), and Routing Type (BGP). Under 'Client Routes', the route '172.16.104.0/24' is highlighted. A 'Download Routing Table' link is also present.

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data
Primary 1	131130	178.43.249.14	sse-euc-1-1-1	3.120
Primary 2	131131	178.43.249.14	sse-euc-1-1-1	3.120
Primary 3	131133	178.43.249.14	sse-euc-1-1-1	3.120
Primary 4	131147	178.43.249.14	sse-euc-1-1-1	3.120
Primary 5	131128	178.43.249.14	sse-euc-1-1-1	3.120
Primary 6	131126	178.43.249.14	sse-euc-1-1-1	3.120
Primary 7	131127	178.43.249.14	sse-euc-1-1-1	3.120



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.

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

eu-central-1

Region

Status

1 Tunnel Group

+ Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
eu-central-1 Catalyst SDWAN	Connected	Europe (Germany)	sse-euc-1-1-1	20	sse-euc-1-1-0	20

Verificar

para verificar se o tráfego está passando pelo Cisco Secure Access, navegue para [Events](#) ou [Activity Search](#) ou [Network-Wide Path Insights](#) e filtre por sua identidade de túnel:

Acesso seguro - Pesquisa de atividades

Navegue até [Monitor](#) > [Activity Search](#) :

Activity Search

FILTERS

Q Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

IP ADDRESS172.16.104.11

IDENTITYAlejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)

Restore to

Search filters

Response

Allowed

Advanced

Blocked

Warn Page Behavior

Warned

Accessed After Warn

4 Total

Viewing activity from Feb 17, 2026 11:27 AM to Feb 18, 2026 11:27 AM

Page: 1

Resu

Request	Source	Rule Identity	Destination	Destination IP	Destination Po
FW	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)		172.16.104.11:3389	3389
FW	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)		172.16.104.11:3389	3389
FW	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)		172.16.104.11:3389	3389
ZTA CLIENTLESS	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	Alejandro Ruiz Sanchez (alejarui) (alejarui@cisco.com)	PC-site-104	172.16.104.11:3389	3389

Acesso seguro - Eventos

Navegue até [Monitor](#) > [Events](#):

Events

Lists events triggered by access requests made by your organization's sources. Find out where your users are going and how your rules impact their access to requested destinations. [Help](#)

[Schedule report](#)[Export CSV](#)

Events 1 total

DNS 0 Web 0 Firewall 0 IPS 0 ZTA Clientless 1 ZTA Client-based 0 Decryption 0

Status Select status... Last 24 hours

[Saved searches](#)[Restore](#)

Event Type: ZTA Clientless DNS x Reset all

Event Type	Status	Event ID	Source	Destination	Reason Code	Rule Name	Time
ZTA Clientless	Allowed	c662e2b5df2ac6fc	Alejandro Ruiz Sanchez...	PC-site-104	-	SITE-104-RDP	Feb 18, 2026 10:26 AM

Source

AD Users: Alejandro Ruiz Sanchez...

Source IP:

Location:

Browser: Firefox 147.0

Operating system: Mac OS X 10.15

Connection

Type: ZTA

Endpoint Posture:

Status: Compliant

Posture profile: System provided (Brow...

Security Controls

ZTA Clientless

Action: Allowed

Ingress region: —

Tunnel type: HTTP2

Resource connector group: —

Egress IP: —

Datacenter: —

Firewall (3)

Destination

FQDN: PC-site-104

Resource/Application Name: PC-site-104

Destination IP: 172.16.104.11

Destination Port: 3389

Application Category: Private Resource

Application Protocol: RDP-TCP

Rows per page 30 1-1 of 1 < 1 >



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**

Traces & Tasks **New Trace** New Auto-on Task

☐ Enable DNS Domain Discovery

Trace Name SPA Trace Duration(minutes) 60

Filters

Select Site(branch site only)* SITE_104 VPN* 1 VPN(s)

Source Address/Prefix Destination Address/Prefix 172.16.104.0/24

☒ Application ☐ Application Group

Please select one or more applications

Advanced Filters

Monitor Settings

Grouping Fields

Synthetic Traffic

Cancel Start

- 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 VPN escolhido

Iniciar o rastreamento

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

INSIGHTS

Selected trace: SPA (Trace Id: 192)

Applications

Active Flows

Completed Flows

Filter

Destination IP: 172.16.104.11

Search by Domain, Application, Readout, etc.

Search

Feb 18, 2026, 10:33:56 AM

Feb 18, 2026, 10:49:02 AM

Feb 18, 2026, 11:33:02 AM

expand a flow/domain to load data for 'INSIGHT' - ADVANCED VIEWS:

* Readout Legend: Error, Warning, Information, ThousandEyes, Synthetic Traffic, PCAP Replay.

Overall 621 flows traced, 1 flows traced during Feb 18, 2026 10:33:56 AM to Feb 18, 2026 10:49:02 AM

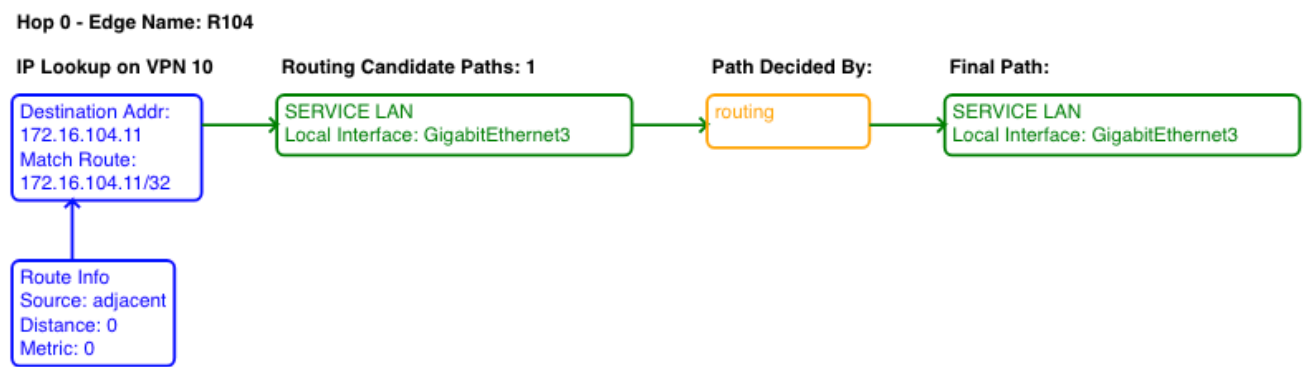
Total Rows: 1

Start - Update Time	Flow ID	Insights *	VPN	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	RTT CND(ms)/SND(ms) *	User	User Group	Security Gr
10:47:32 AM-11:33:23 AM	143	View	10			172.16.104.11	3389	TCP	DEFAULT ↑ / DEFAULT ↓	ms-wbt	other	Unknown	R104: 27/1	Unkn...	Unknown	N/A→N/A

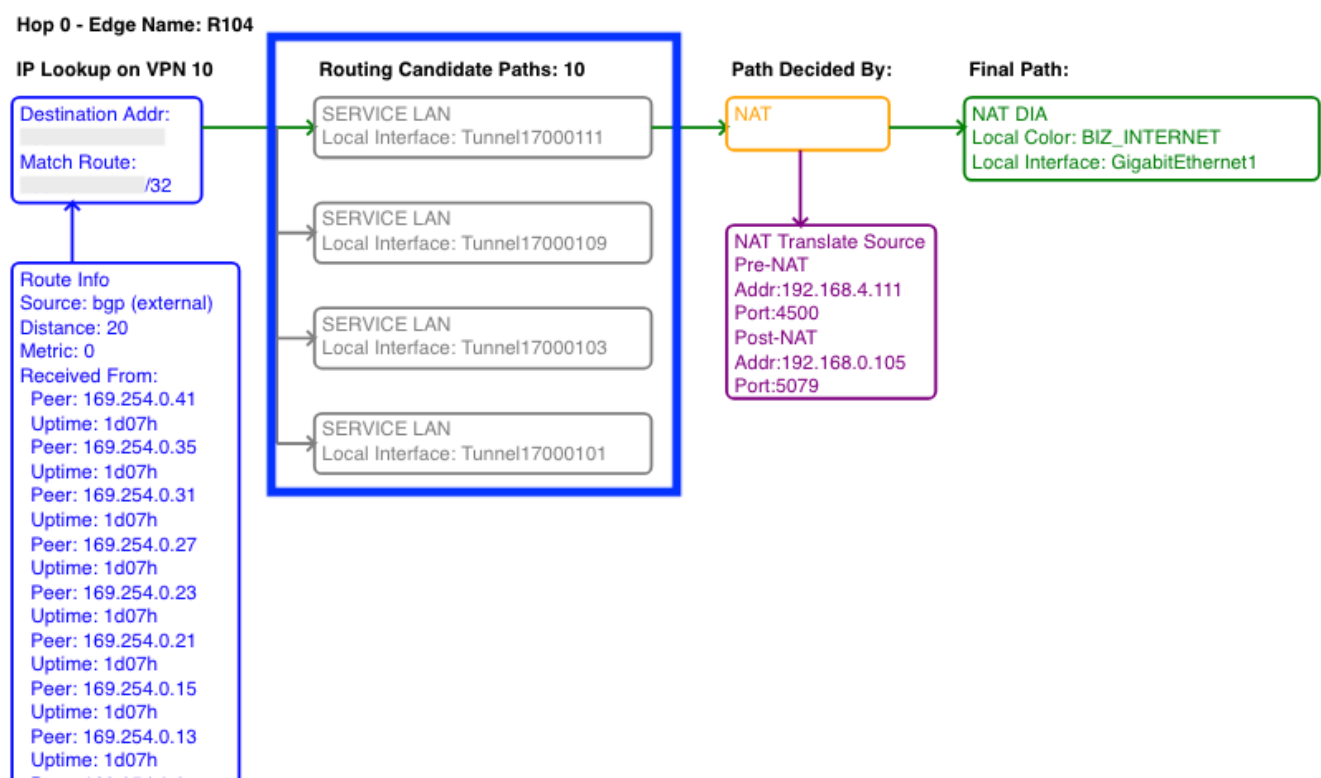
A coluna Routing Insights exibe os caminhos candidatos e os túneis IPsec para Secure Access

Trace: SPA (ID: 192), Flow ID: 143 (Application:ms-wbt)

Upstream (From 15645 to 172.16.104.11:3389)



Downstream (From 172.16.104.11:3389 to 15645)



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.