

# Configure o acesso seguro com túneis automatizados SD-WAN para acesso seguro à Internet

## 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](#)

[Crie seu FQDN ou APP de desvio personalizado em SD-WAN \(OPCIONAL\)](#)

[Roteamento do tráfego](#)

[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 de SD-WAN para acesso seguro à Internet.



# Secure Access and SDWAN

## for Secure Internet Access

### — with Automated Tunnels —

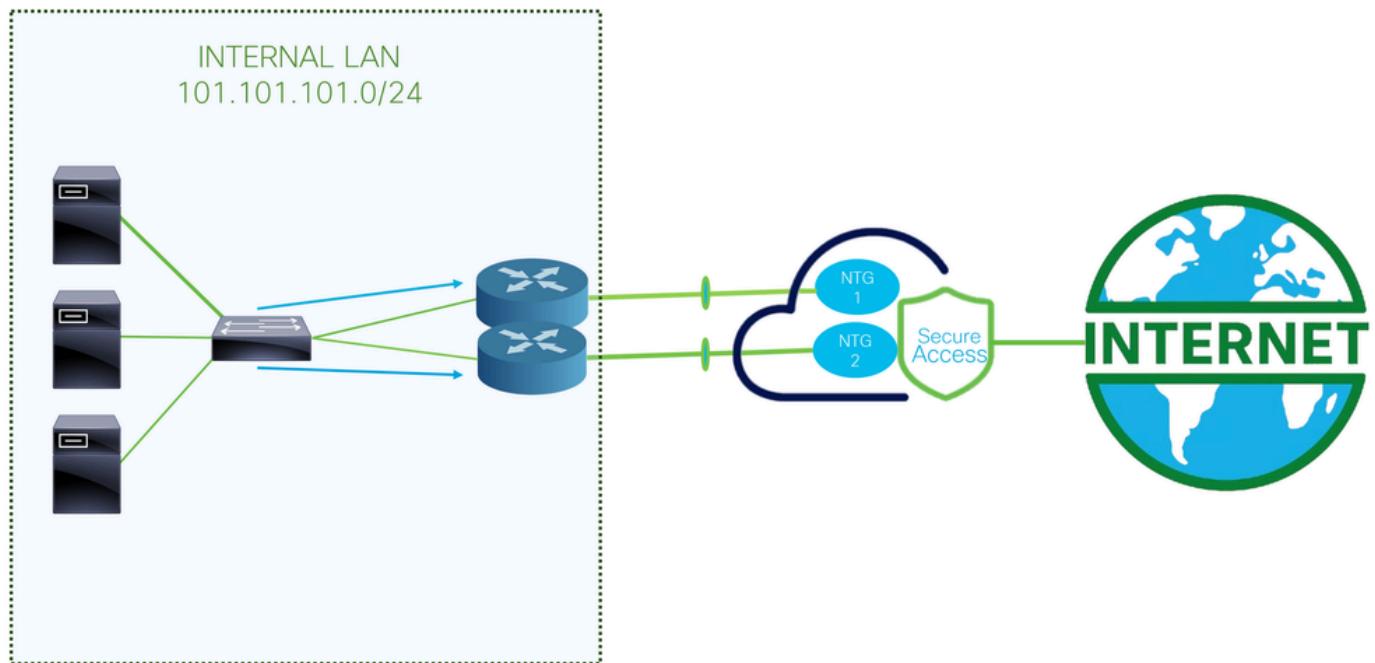
#### Informações de Apoio

À medida que as organizações adotam cada vez mais aplicativos baseados em nuvem e dão suporte a forças de trabalho distribuídas, as arquiteturas de rede devem evoluir para fornecer acesso seguro, confiável e escalável aos recursos. O Secure Access Service Edge (SASE) é uma estrutura que converge rede e segurança em um único serviço fornecido em nuvem, combinando recursos de SD-WAN com funções de segurança avançadas, como Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), segurança de camada DNS, Zero Trust Network Access (ZTNA) ou VPN integrada para acesso remoto seguro.

A integração do Cisco Secure Access com SD-WAN através de túneis automatizados permite que as organizações roteiem o tráfego da Internet de forma segura e eficiente. A SD-WAN fornece seleção de caminho inteligente e conectividade otimizada em locais distribuídos, enquanto o Cisco Secure Access garante que todo o tráfego seja inspecionado e protegido de acordo com as políticas de segurança corporativas antes de acessar a Internet.

Ao automatizar a configuração do túnel entre os dispositivos SD-WAN e o acesso seguro, as organizações podem simplificar a implantação, melhorar a escalabilidade e garantir a aplicação consistente da segurança para os usuários, independentemente de onde eles estejam localizados. Essa integração é um componente-chave de uma arquitetura SASE moderna, permitindo acesso seguro à Internet para filiais, locais remotos e usuários móveis.

#### Diagrama de Rede



Esta é a arquitetura usada para este exemplo de configuração. Como você pode ver, há dois roteadores de borda:

Se você optar por implantar as políticas em dois dispositivos diferentes, um NTG será configurado para cada roteador e o NAT será habilitado no lado do acesso seguro. Isso permite que ambos os roteadores enviem tráfego da mesma origem através dos túneis. Normalmente, isso não é permitido; no entanto, habilitar a opção NAT para esses túneis permite que dois roteadores de borda enviem tráfego originário do mesmo endereço de origem.

## Pré-requisitos

### Requisitos

- Acesso seguro ao conhecimento
- Cisco Catalyst SD-WAN Manager versão 20.15.1 e Cisco IOS XE Catalyst SD-WAN versão 17.15.1 ou posterior
- Conhecimento intermediário de roteamento e comutação
- Conhecimento ECMP
- Conhecimento de VPN

### Componentes Utilizados

- Locatário de acesso seguro
- Catalyst SD-WAN Manager versão 20.18.1 e Cisco IOS XE Catalyst SD-WAN versão 17.18.1
- 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.

<input type="checkbox"/> Admin	<a href="#">17 &gt;</a>
<input checked="" type="checkbox"/> Deployments	<a href="#">23 &gt;</a>
<input type="checkbox"/> Investigate	<a href="#">2 &gt;</a>
<input type="checkbox"/> Policies	<a href="#">25 &gt;</a>
<input type="checkbox"/> Reports	<a href="#">17 &gt;</a>

**4 selected** [Remove All](#)

Scope	Access Level	Remove
Deployments / Identities	Read / Write	<a href="#">X</a>
Deployments / Network Tunnel Group	Read / Write	<a href="#">X</a>
Deployments / Tunnels	Read / Write	<a href="#">X</a>
Deployments / Regions	Read-Only	<a href="#">X</a>

**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.

<b>API Key</b> 397766cdb29f43b08ddee3b1d8c04e45 	<b>Key Secret</b> 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 SSE e 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

# Configuration Groups

SD-WAN

← Configuration Groups 3

System Profile 4

Transport

Q Search

Last

Name	Type	Profiles
------	------	----------

SIA	Secure Internet Access R1 + R2	
-----	--------------------------------	---

Type: Single Router

## System Profile

SIA\_Basic



## Service Profile (optional)

SIA\_LAN



[+ Add Profile](#)

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

SIA\_Basic [Edit](#)

Description: SIA Basic Profile

Device solution SD-WAN	Updated by admin	Last updated Nov 05, 2025 03:37:09 PM	Shared 1 Group
------------------------	------------------	---------------------------------------	----------------

Q. Search

**Profile Features**

- AAA: AAA
- Banner: Banner
- BFD: BFD
- Global: Global
- Multi-Region Fabric: MRF
- NTP: NTP

**Global**

Name: Global

Description (optional):

Global Description:

Services  NAT64  BGP  Authentication  SSH Version

HTTP Server:

FTP Passive:

ARP Proxy:

Domain Lookup:

HTTPS Server:

RSH/RCP:

Cisco Discovery Protocol (CDP):

Line Virtual Teletype (Configure Options):

## Configurar Grupo de Políticas

Navegue até Configuration > Policy Groups:

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

Policy Group 4 Application Priority & SLA 3 NGFW 0 **Secure Internet Gateway / Secure Service Edge 3**

**Secure Internet Gateway / Secure Service Edge 3**

Q. Search Table

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



Note: Em versões anteriores a 20.18, essa opção é chamada de Adicionar Borda de Serviço Segura (SSE)

- Configure um nome, uma solução e clique em *Create*

## Secure Internet Access

Name

SIA

Solution

sdwan



Description (optional)

[Cancel](#)

[Create](#)

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

**SSE Provider**

Cisco SSE  Zscaler

**Context Sharing**

VPN  SGT

**Tracker**

Source IP address

{{ Monitoring }}

- SSE Provider: SSE
- Context Sharing: Escolha VPN ou/e SGT dependendo das suas necessidades
- Tracker
  - Source IP Address: Escolher Específico do Dispositivo (Isso permite que você o modifique por dispositivo e identifique o caso de uso para ele no estágio de implantação)

Na etapa, Configuration você configurará os túneis:

**Configuration**

[+ Add Tunnel](#)

Single Hub HA Scenario

**Max one tunnel per hub**

ECMP Scenario with HA

**Max 8 Tunnels per Hub 8GB X 1**

By default, for the tunnel route, the system will select the first NAT-enabled interface it finds. If there is more than one, you should select your desired WAN interface.

- **Single Hub HA Scenario:** Neste cenário, você pode configurar a alta disponibilidade usando um NTG como ativo e outro como passivo, com um throughput máximo de 1Gbps por NTG
- **ECMP Scenario with HA:** Neste cenário, você pode configurar até 8 túneis por hub, suportando um total de até 16 túneis por NTG. Essa configuração permite maior throughput nos túneis



Note: Se suas interfaces de rede tiverem um throughput superior a 1Gbps e você precisar de escalabilidade, use interfaces de loopback. Caso contrário, você poderá usar interfaces padrão no dispositivo. Isso é para ativar o ECMP do lado do acesso seguro.



aviso: Se desejar configurar interfaces de loopback para um cenário ECMP, você deve primeiro configurar as interfaces de loopback em Configuration Groups > Transport & Management Profile, sob a política que você usa em seu roteador.

- Clique em **Add Tunnel**

## Edit Tunnel

- Interface Name: **ipsec1, ipsec2, ipsec3** e assim por diante
- Tunnel Source Interface: **Escolha Interfaces de Loopback ou uma específica de onde você estabelece o túnel**
- Tunnel Route Via: Se você escolher Loopback, precisará selecionar a interface física a partir da qual deseja rotear o tráfego. Se você não selecionar Loopback, essa opção aparecerá esmaecida e usará a primeira interface habilitada para NAT encontrada pelo sistema. Se houver mais de uma, você deverá selecionar a interface WAN desejada
- Data Center: Isso significa para qual hub do Secure Access você estabelece a conexão

A próxima parte da configuração do túnel você configura os túneis com as melhores práticas fornecidas pela Cisco.

▼ Advanced Options

General

Shutdown

(✓)

Track this interface

(✓)

TCP MSS

(⊕)

IP MTU

(⊕)

DPD Interval

(✓)

DPD Retries

(✓)

IKE Diffie-Hellman Group

(⊕)

(⊖)

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

Depois disso, você deve configurar o túnel secundário apontando para o datacenter secundário.

## CENÁRIO DE HA DE HUB ÚNICO

## Configuration

[+ Add Tunnel](#)

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		<input checked="" type="checkbox"/> false	1350	1390	 
ipsec2		<input checked="" type="checkbox"/> false	1350	1390	 

Este é o resultado final quando você usa a implantação do cenário normal.

## ECMP SCENARIO WITH HA

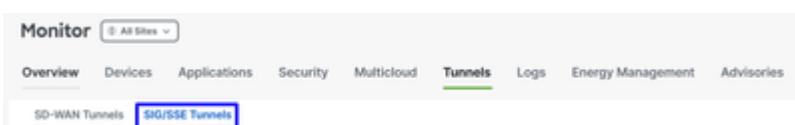
Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1		<input checked="" type="checkbox"/> false	1350	1390
ipsec2		<input checked="" type="checkbox"/> false	1350	1390
ipsec3	PRIMARY HUB	<input checked="" type="checkbox"/> false	1350	1390
ipsec4		<input checked="" type="checkbox"/> false	1350	1390
ipsec5		<input checked="" type="checkbox"/> false	1350	1390
ipsec11		<input checked="" type="checkbox"/> false	1350	1390
ipsec12		<input checked="" type="checkbox"/> false	1350	1390
ipsec13	SECONDARY HUB	<input checked="" type="checkbox"/> false	1350	1390
ipsec14		<input checked="" type="checkbox"/> false	1350	1390
ipsec15		<input checked="" type="checkbox"/> false	1350	1390

Em seguida, você precisa configurar a Alta disponibilidade na Política de Internet segura.

## High Availability

[+ Add Interface Pair](#)

Clique em Add Interface Pair:



PRIMARY  
SECONDARY

## Edit Interface Pair

Active Interface: ipsec1 (highlighted with a blue box)

Active Interface Weight: 1

Backup Interface: ipsec11 (highlighted with an orange box)

Backup Interface Weight: 1

Tunnel Type: IPsec

Interface Name(1..255): ipsec1

Tunnel Source Interface\*: Loopback1

Tunnel Type: IPsec

Interface Name(1..255): ipsec11

Tunnel Source Interface\*: Loopback11

Tunnel Route Via: GigabitEthernet1

Tracker: DefaultTracker

Data Center: Primary

Data Center: Secondary (highlighted with an orange box)

Nesta etapa, você precisa configurar os túneis primário e secundário para cada par de túneis que estiver configurando. Isso significa que cada túnel tem seu próprio backup. Lembre-se de que esses túneis foram criados como primário e secundário para essa finalidade exata.

"Active interface" refere-se ao túnel primário, enquanto "Backup interface" refere-se ao túnel secundário:

- Active Interface: Preliminar
- Backup Interface: Secundário



aviso: Se essa etapa for ignorada, os túneis não serão ativados e nenhuma conexão será estabelecida dos roteadores para o Secure Access.

Depois que a Alta Disponibilidade for configurada para os túneis, a configuração será exibida conforme mostrado na imagem abaixo. No exemplo de laboratório usado para este guia, cinco túneis são mostrados em HA. O número de túneis pode ser ajustado conforme necessário.

## High Availability

+ Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	1	ipsec11	1	 
ipsec2	1	ipsec12	1	 
ipsec3	1	ipsec13	1	 
ipsec4	1	ipsec14	1	 
ipsec5	1	ipsec15	1	 

 Cancel

Save



Note: No máximo 8 pares de túneis (16 túneis: 8 principais e 8 secundários) podem ser configurados no Catalyst vManage para SD-WAN. O Cisco Secure Access suporta até 10 pares de túneis.

- Clique em Save

Depois desse ponto, se tudo estiver configurado corretamente, os túneis aparecerão como UP no SD-WAN Manager e no Secure Access.

Para verificar na SD-WAN, verifique as próximas etapas:

- Clique em Monitor > Tunnels
- Em seguida, clique em SIG/SSE Tunnels

Monitor All Sites ▾

Overview Devices Applications Security Multicloud **Tunnels** Logs Energy Management Advisories

SD-WAN Tunnels **SIG/SSE Tunnels**

E você poderá ver os túneis estabelecidos para o Cisco Secure Access UP ou não.

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 em Secure Access, verifique as próximas etapas:

- Clique em Connect > Network Connections

#### 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](#)

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Connected	Europe (Germany)	sse-euc-1-1-1	8	sse-euc-1-1-0	8

Em uma exibição detalhada, clique no nome do túnel:

PRIMARY							SECONDARY						
Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update	Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	131085	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 1	65559	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 2	131086	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 2	65560	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 3	131096	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 3	65538	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 4	131087	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 4	65548	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 5	131095	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 5	65552	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 6	131077	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 6	65554	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 7	131094	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 7	65555	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM
Primary 8	131078	178.43.250.2	sse-euc-1-1-1	178.43.250.2	Connected	Dec 21, 2025 10:59 PM	Secondary 8	65558	178.43.250.2	sse-euc-1-1-0	178.43.250.2	Connected	Dec 21, 2025 11:00 PM

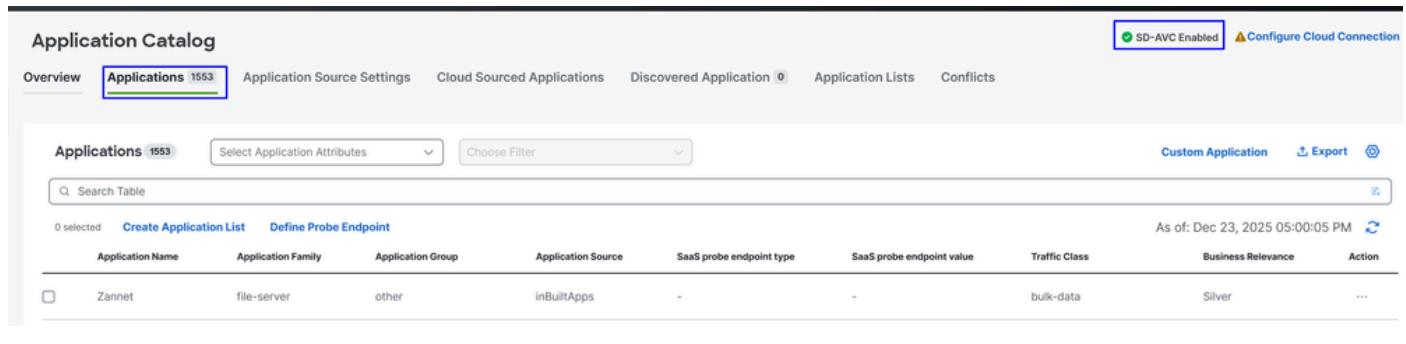
Depois disso, você pode ir para a etapa, Create your Custom Bypass FQDN or APP in SD-WAN

## Crie seu FQDN ou APP de desvio personalizado em SD-WAN (OPCIONAL)

Há casos de uso especiais em que você precisa criar Application Bypass e FQDN ou IP que você pode aplicar às suas políticas de roteamento:

Navegue até o portal SD-WAN Manager:

- Clique em Configuration > Application Catalog > Applications



Application Name	Application Family	Application Group	Application Source	SaaS probe endpoint type	SaaS probe endpoint value	Traffic Class	Business Relevance	Action
Zannet	file-server	other	inBuiltApps	-	-	bulk-data	Silver	...



Tip: Se estiver executando uma versão anterior à 20.15, os aplicativos personalizados poderão ser criados em Listas de políticas



Note: Para ter acesso ao Catálogo de Aplicativos, você deve habilitar o SD-AVC.

- Clique em Custom Application



Application Name	Application Family	Application Group	Application Source	SaaS probe endpoint type	SaaS probe endpoint value	Traffic Class	Business Relevance	Action
Zannet	file-server	other	inBuiltApps	-	-	bulk-data	Silver	...

Neste estágio, uma exclusão básica é configurada usando o FQDN SWG do Secure Client - Umbrella Module:

**ProxySecureAccess**

### Custom Application

**Application Name** ⓘ  


Application Name: ProxySecureAccess-Custom

**Server Names** ⓘ

←
→
FQDN

**Application Family**

**Application Group**

**Traffic Class**

**Business Relevance**

+ **L3/L4 Attributes**

IPv4 Address ⓘ
 Ports ⓘ
 L4 Protocol ⓘ

◀
▶

**SaaS probe endpoint type**

IP Address
 FQDN
 URL

**SaaS probe endpoint value**

Cancel
Save

- **Server Name:** Use o FQDN que você gostaria de ignorar (Neste exemplo, o FQDN do SWG está configurado)
  - [swg-url-proxy-https-sse.sigproxy.qq.opendns.com](https://swg-url-proxy-https-sse.sigproxy.qq.opendns.com)
  - [swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com](https://swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com)
- Clique em **Save**

Note: Altere ORGID com o número da sua organização SSE.

Em seguida, é criada uma exclusão básica; neste caso, os servidores DNS Umbrella:

UmbrellaDNS

Custom Application

Name of the Custom App

Application Name: UmbrellaDNS

Application Family: Select Application Family

Application Group: Select Application Group

Traffic Class: Select Traffic Class

Business Relevance: Select Business Relevance

**L3/L4 Attributes**

IPv4 Address: 208.67.220.220,208.67.222.222

Ports: Configure IP addresses to exclude

L4 Protocol: Enter L4 Protocol

SaaS probe endpoint type: IP Address, FQDN, URL

SaaS probe endpoint value: [empty input]

Cancel Save

Agora você pode prosseguir com as configurações das políticas de roteamento.

## Roteamento do tráfego

Nesta etapa, você precisa rotear o tráfego da Internet através dos túneis para protegê-lo através do Cisco Secure Access. Nesse caso, você usa uma política de roteamento flexível que nos permite contornar certos tráfegos, ajudando a evitar o envio de tráfego indesejado através do Secure Access ou a evitar possíveis práticas ruins.

Primeiro, deixe-o definir os dois métodos de roteamento que podem ser usados:

- Configuration > Configuration Groups > Service Profile > Service Route: Esse método fornece roteamento para acesso seguro, mas carece de flexibilidade.
- Configuration > Policy Groups > Application Priority & SLA: Esse método oferece várias opções de roteamento dentro da SD-WAN e, o mais importante, permite que você ignore tráfego específico para que ele não seja enviado pelo Secure Access.

Para flexibilidade e alinhamento com as práticas recomendadas, esta configuração é usada, Application Priority & SLA:

- Clique em Configuration > Policy Groups > Application Priority & SLA
- Em seguida, clique em Application Priority & SLA Policy

## Policy Groups

Policy Group 4 **Application Priority & SLA 4** NGFW 0 Secure Internet Gateway / Secure Service Edge 3 DNS Security 0

Application Priority & SLA Policy 4

Search Table

**Application Priority & SLA Policy**

Name	Description	References	Update
------	-------------	------------	--------

- Configure um nome de diretiva e clique em Create

## Application Priority & SLA Policy

Policy Name

Description (optional)

Cancel **Create**

- Enable Advanced Layout
- Clique em + Add Traffic Policy

Policies > Application Priority & SLA

SIA-ROUTE

Change made in advanced view won't save to simple view.

+ Add Traffic Policy

Advanced Layout

SLA Class QoS Queue

No SLA Class added, add your first SLA Class in Traffic Policy

## Add Traffic Policy List

Policy Name  
SSE

VPN(s)  
Corporate\_Users

Direction  
From Service

Default action  
 Accept  Drop

Cancel Add

- Policy Name: Nome que o ajusta à finalidade desta Lista de políticas de tráfego
- VPN(s): Escolha a VPN de serviço do usuário de onde você roteia o tráfego
- Direction: Do serviço
- Default action: Aceitar

Depois disso, você poderá iniciar a criação da Política de tráfego:

**In this way, you are bypassing the routing of specific traffic to Secure Access**

VPN: Corporate\_Users Direction: From Service Default Action: Accept

NAME	MATCH	ACTION
1 LocalNetwork	Destination Ip - 172.16.200.0/24 Source Ip - 101.101.101.0/24	Base action - accept
2 BypassSSEP roxy	App List - SecureAccessProxy	Base action - accept
3 UmbrellaDN S	App List - UmbrellaDNS	Base action - accept
4 SIA AUTO F ULL TRAFFI C	Source Ip - 101.101.101.0/24	Base action - accept Sse Secure Service Edge - true Sse Secure Service Edge Instance - Cisco-Secure-Access

Traffic is matched in order, starting from the highest priority rule to the lowest.

In this way, you are sending specific traffic to Secure Access to be protected

1. Local Network Policy (Optional): Origem 101.101.101.0/24, Destino 172.16.200.0/24. Essa rota impede que o tráfego entre redes seja enviado para o Cisco Secure Access. Normalmente, os clientes não fazem isso, pois o roteamento interno é geralmente processado pelo roteador de distribuição em implantações de SD-WAN. Essa configuração garante que o

tráfego interno entre essas sub-redes não seja roteado para o acesso seguro, dependendo se o seu cenário o exige (opcional, depende do seu ambiente de rede)

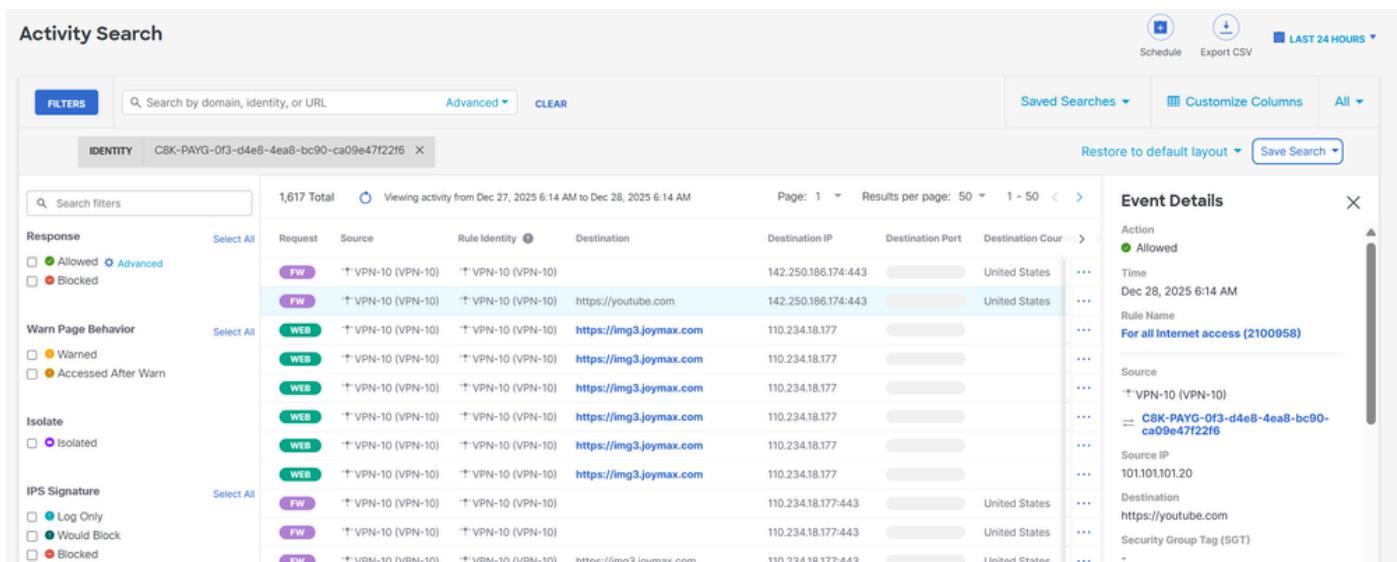
2. **BypassSSEProxy (Optional):** Essa política impede que computadores internos com o módulo Cisco Umbrella no Secure Client e SWG habilitado enviem tráfego de proxy de volta para a nuvem. O roteamento do tráfego proxy para a nuvem novamente não é considerado uma prática recomendada.
3. **UmbrellaDNS (Best Practice):** Essa política impede que consultas DNS destinadas à Internet sejam enviadas pelo túnel. O envio de consultas DNS para resolvidores de Umbrella (208.67.222.222, 208.67.220.220) através do túnel não é recomendado.
4. **SIA AUTO FULL TRAFFIC:** Essa política roteia todo o tráfego da origem 101.101.101.0/24 para a Internet por meio dos túneis SSE criados anteriormente, garantindo que esse tráfego esteja protegido na nuvem.

## Verificar

para verificar se o tráfego já está inundando através do 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**:



The screenshot shows the Cisco Umbrella Activity Search interface. The top navigation bar includes 'Activity Search', 'Schedule', 'Export CSV', and a 'LAST 24 HOURS' button. The main search bar contains the identity 'C8K-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6'. The left sidebar has filters for 'IDENTITY' (selected), 'Response' (Allowed, Blocked), 'Warn Page Behavior' (Warned, Accessed After Warn), 'Isolate' (Isolated), and 'IPS Signature' (Log Only, Would Block, Blocked). The main table displays 1,617 total events from Dec 27, 2025 6:14 AM to Dec 28, 2025 6:14 AM. The columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, and Destination Country. The table shows several entries for 'FW' (Firewall) and 'WEB' (Web) requests from 'VPN-10 (VPN-10)' to various destinations like 'https://youtube.com' and 'https://img3.joymax.com'. The right panel, titled 'Event Details', shows a single event for 'For all Internet access (2100958)' with details: Action (Allowed), Time (Dec 28, 2025 6:14 AM), Rule Name (For all Internet access (2100958)), Source ('VPN-10 (VPN-10)'), Destination ('C8K-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6'), Source IP ('101.101.101.20'), Destination ('https://youtube.com'), and Security Group Tag (SGT) ('').

### Acesso seguro - Eventos

Navegue até **Monitor > Events**:

>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-Of3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	829e0bbdeaf6514e	C8K-PAYG-560-5b...	8.8.8.8:53	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Connect	Allowed	204e46d757b128d7	C8K-PAYG-560-5b...	8.8.8.8	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	829e0bbdeaf6514e	C8K-PAYG-560-5b...	8.8.8.8:53	-	For all Internet acce...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-Of3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	eeeb39315cdde282	C8K-PAYG-Of3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	eeeb39315cdde282	C8K-PAYG-Of3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM
>	Firewall	Disconnect	Allowed	94cea39685acd61c	C8K-PAYG-Of3-d4e...	110.234.18.177:443	-	SD-WAN-Allow-We...	Dec 28, 2025 6:17 AM



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 Duration(minutes)**

**Trace Name**

**Filters**

**Trace Duration(minutes)**

**Select Site(branch site only)\***

**VPN\***

**Source Address/Prefix**

**Destination Address/Prefix**

Application  ⓘ

Application Group  ⓘ

- Site: Escolha o site de onde seu tráfego está sendo egresso
- VPN: Escolha o ID da VPN da sua sub-rede de onde o tráfego está sendo egresso
- Source: Coloque o IP ou deixe-o em branco para filtrar todo o tráfego filtrado pelo site e escolha VPN

Em Insights, você pode ver o tráfego inundando os túneis e o tipo de tráfego que vai para o acesso seguro:

INSIGHTS Selected trace: trace\_80 (Trace Id: 80)

Applications Active Flows Completed Flows Selected Flow ID: 50

Search by Domain, Application, Readout, etc.  ⓘ

\* Readout Legend: ●- Error, ●- Warning, ●- Information, ●- Synthetic Traffic, ●-PCAP Replay.

Start - Update Time	Flow ID	Insights *	VPN --	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain
7:26:05 AM-7:34:05 AM	50	<a href="#">View <span style="color: green;">●</span></a>	10	101.101.101.20	54688	172.211.123.249	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g... <span style="color: blue;">N/A</span>	<span style="color: blue;">N/A</span>
Direction HopIndex Local Edge      Remote Edge      Local Color      Remote Color      Local Drop(%)      Wan Loss(%)      Remote Drop(%)      Jitter(ms) *      Latency(ms) *      ART CND(ms)/SND(ms) *												
Upstream	0	R101-2(Tunnel16000003)	SIG	BIZ_INTERNET (SIG)	N/A		0.00	N/A	N/A	N/A	N/A	R101-2: N/A
Downstream	0	SIG	(Tunnel16000003)R101-2	N/A	BIZ_INTERNET (SIG)	N/A	N/A	0.00	N/A	N/A	N/A	N/A
Total Rows: 10 <span style="color: blue;">↓</span> <span style="color: blue;">⟳</span>												
7:35:23 AM-7:35:23 AM	563	<a href="#">View <span style="color: green;">●</span></a>	10	101.101.101.20	56408	172.211.123.248	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g... <span style="color: blue;">N/A</span>	<span style="color: blue;">N/A</span>
7:37:35 AM-7:37:35 AM	668	<a href="#">View <span style="color: green;">●</span></a>	10	101.101.101.20	53175	8.8.8.8	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	<span style="color: blue;">N/A</span>
7:37:38 AM-7:37:38 AM	573	<a href="#">View <span style="color: green;">●</span></a>	10	101.101.101.20	56560	3.74.137.87	443	TCP	DEFAULT ↑ / DEFAULT ↓	ProxySecureA... other	<span style="color: blue;">N/A</span>	<span style="color: blue;">N/A</span>

## Informações Relacionadas

- [Supporte técnico e downloads da Cisco](#)
- [Central de ajuda do Cisco Secure Access](#)
- [Guia de design do Cisco SASE](#)
- [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.