

セキュアインターネットアクセスのためのSD-WAN自動トンネルを使用したセキュアアクセスの設定

内容

[はじめに](#)

[背景説明](#)

[ネットワーク図](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[セキュアアクセスの設定](#)

[APIの作成](#)

[SD-WANの設定](#)

[APIの統合](#)

[ポリシーグループの設定](#)

[SD-WANでのカスタムバイパスFQDNまたはアプリケーションの作成（オプション）](#)

[トラフィックのルーティング](#)

[確認](#)

[セキュアアクセス - アクティビティ検索](#)

[セキュアなアクセス : イベント](#)

[Catalyst SD-WAN Manager - ネットワーク全体のバスインサイト](#)

[関連情報](#)

はじめに

このドキュメントでは、セキュアインターネットアクセスのためのSD-WAN自動トンネルを使用してセキュアアクセスを設定する方法について説明します。



Secure Access and SDWAN

for Secure Internet Access

— with Automated Tunnels —

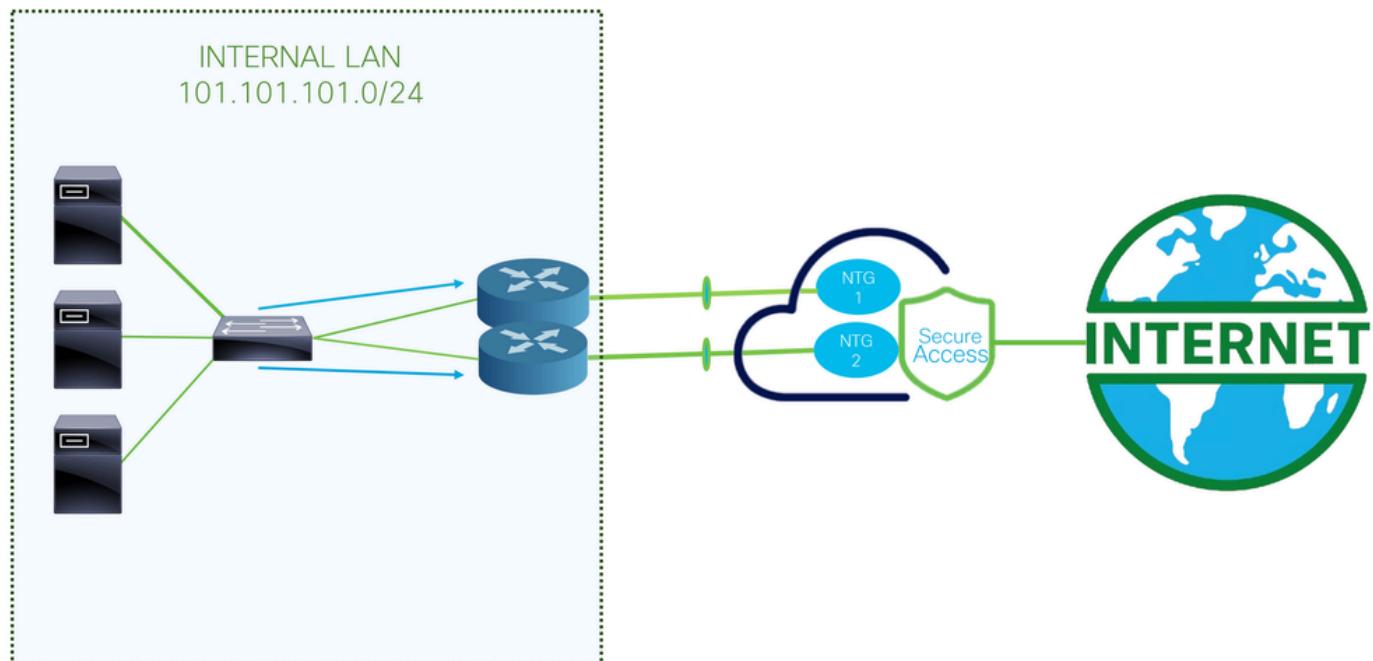
背景説明

組織がクラウドベースのアプリケーションを採用し、分散した従業員をサポートする傾向が強まるにつれ、ネットワークアーキテクチャは、リソースへのセキュアで信頼性が高く、スケーラブルなアクセスを提供するように進化する必要があります。Secure Access Service Edge(SASE)は、ネットワーキングとセキュリティを単一のクラウド提供サービスに統合するフレームワークです。SD-WAN機能を、Secure Web Gateway(SWG)、Cloud Access Security Broker(CASB)、DNS層セキュリティ、Zero Trust Network Access(ZTNA)、セキュアなリモートアクセスのための統合VPNなどの高度なセキュリティ機能と組み合わせます。

自動化されたトンネルを通じてCisco Secure AccessとSD-WANを統合することで、組織はインターネットトラフィックを安全かつ効率的にルーティングできるようになります。SD-WANは、インテリジェントなパス選択を提供し、分散した場所での接続を最適化します。Cisco Secure Accessは、インターネットに到達する前に、すべてのトラフィックが企業のセキュリティポリシーに従って検査および保護されることを保証します。

SD-WANデバイスとSecure Access間のトンネル設定を自動化することで、組織は、ユーザの所在地に関係なく、導入の簡素化、拡張性の向上、一貫性のあるセキュリティの適用を実現できます。この統合は、最新のSASEアーキテクチャの主要なコンポーネントであり、ブランチオフィス、リモートサイト、およびモバイルユーザのセキュアなインターネットアクセスを可能にします。

ネットワーク図



この設定例で使用するアーキテクチャを次に示します。ご覧のように、エッジルータは2つあります。

2つの異なるデバイスにポリシーを展開することを選択した場合は、ルータごとにNTGが設定され、セキュアアクセス側でNATが有効になります。これにより、両方のルータがトンネルを介して同じ送信元からトラフィックを送信できます。通常、これは許可されません。ただし、これらのトンネルに対してNATオプションを有効にすると、2つのエッジルータが同じ送信元アドレスから発信されたトラフィックを送信できるようになります。

前提条件

要件

- セキュアアクセスの知識
- Cisco Catalyst SD-WAN Manager Release 20.15.1およびCisco IOS XE Catalyst SD-WAN Release 17.15.1以降
- ルーティングとスイッチングに関する中級レベルの知識
- ECMPの知識
- VPNに関する知識

使用するコンポーネント

- セキュアアクセステナント
- Catalyst SD-WAN Managerリリース20.18.1およびCisco IOS XE Catalyst SD-WANリリース 17.18.1
- Catalyst SD-WAN Manager

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

セキュアアクセスの設定

APIの作成

セキュアアクセスを使用して自動トンネルを作成するには、次の手順を確認します。

[Secure Access Dashboard](#)に移動します。

- Admin > API Keys の順にクリックします。
- Add をクリックします。
- 次のオプションを選択します。
 - 展開/ネットワークトンネルグループ : 読み取り/書き込み
 - 導入/トンネル : 読み取り/書き込み
 - 展開/リージョン : 読み取り専用
 - 展開/ID : 読み取り/書き込み
 - Expiry Date : 無期限

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

<input type="checkbox"/> Admin	17 >
<input checked="" type="checkbox"/> Deployments	23 >
<input type="checkbox"/> Investigate	2 >
<input type="checkbox"/> Policies	25 >
<input type="checkbox"/> Reports	17 >

4 selected		Remove All
Scope		X
Deployments / Identities	Read / Write	X
Deployments / Network Tunnel Group	Read / Write	X
Deployments / Tunnels	Read / Write	X
Deployments / Regions	Read-Only	X

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



注：オプションで、このキーが認証を実行できるネットワークを10個まで追加できます。パブリックIPアドレスまたはCIDRのカンマ区切りリストを使用してネットワークを追加します。

- CREATE KEYをクリックして、API KeyとKey Secretの作成を終了します。

API Key	Key Secret
397766cdb29f43b08ddee3b1d8c04e45	bfce729cd3e243e281df7271acb12208



注意：コピーしてからACCEPT AND CLOSEをクリックしてください。そうしないと、再度作成して、コピーされなかったコピーを削除する必要があります。

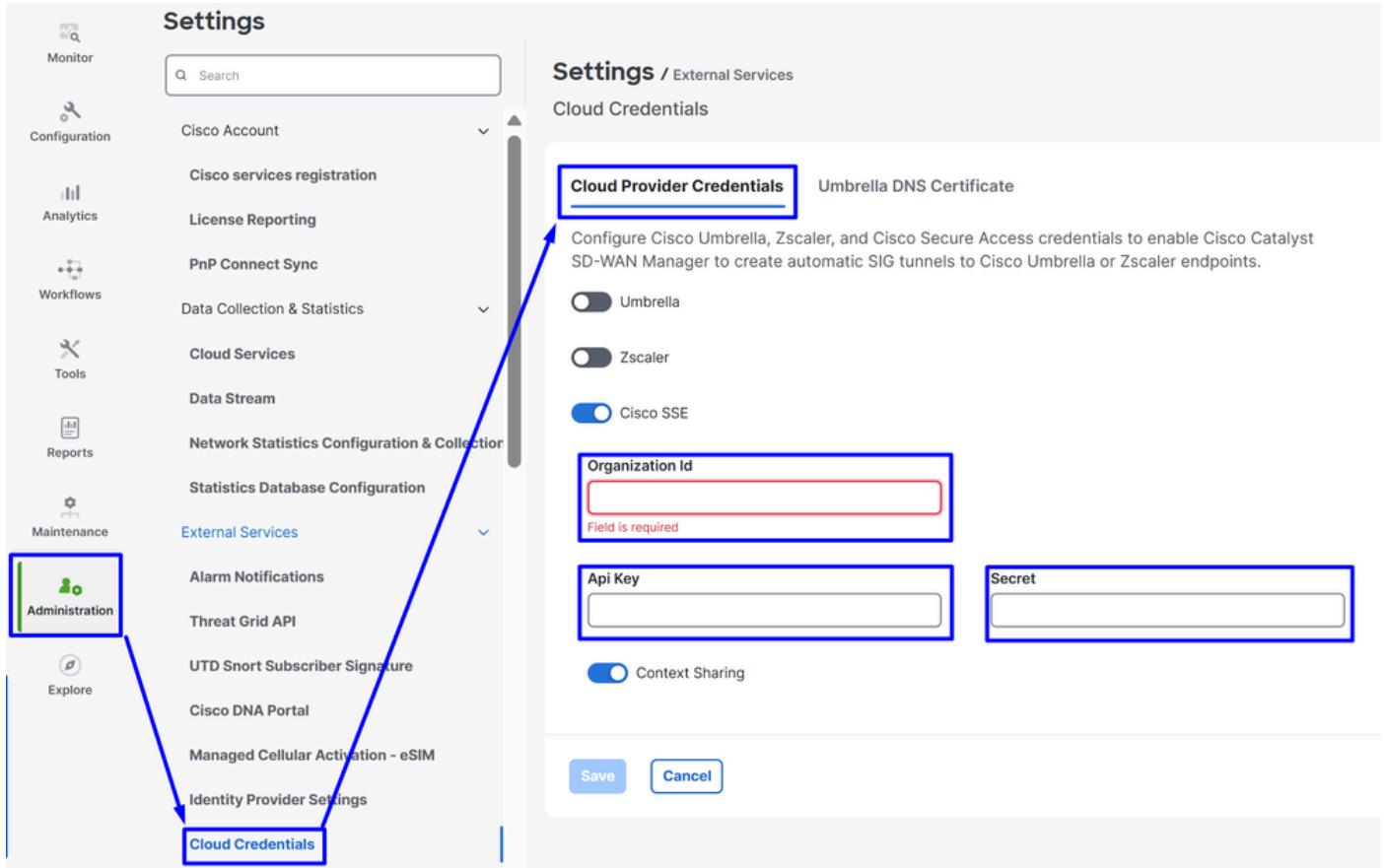
次に、ACCEPT AND CLOSEをクリックして完了します。

SD-WANの設定

APIの統合

Catalyst SD-WAN Managerに移動します。

- Administration > Settings > Cloud Credentialsの順にクリックします。
- 次に、Cloud Provider CredentialsをクリックしてCisco SSEを有効にし、APIと組織の設定を入力します



- 組織ID:SSEダッシュボードのURL(<https://dashboard.sse.cisco.com/org/xxxxx>)から取得できます。
- Apiキー：[セキュアアクセス設定](#)の手順からコピーします。
- 秘密：セキュアアクセス設定の手順からコピーします。

その後、Saveボタンをクリックします。



注：次の手順に進む前に、SD-WAN ManagerとCatalyst SD-WANエッジにDNS解決とインターネットアクセスがあることを確認する必要があります。

DNSルックアップが有効になっているかどうかを確認するには、次の場所に移動します。

- Configuration > Configuration Groupsの順にクリックします。
- エッジデバイスのプロファイルをクリックして、システムプロファイルを編集します。

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

- 次に、Globalオプションを編集して、Domain Resolutionオプションが有効になっていることを確認します

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	Banner		
BFD	Global		
Multi-Region Fabric	NTP		

Global

Name: Global
Description (optional)
Global Description

Services NAT64 BGP Authentication SSH Version

HTTP Server
FTP Passive
ARP Proxy
Cisco Discovery Protocol (CDP)

HTTPS Server
Domain Lookup
RSH/RCP
Line Virtual Teletype (Configure Options)

ポリシーグループの設定

Configuration > Policy Groupsの順に移動します。

- Secure Internet Gateway / Secure Service Edge > Add Secure Internet Accessの順にクリックします

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



注:20.18より前のリリースでは、このオプションはAdd Secure Service Edge(SSE)と呼ばれていました

- 名前とソリューションを設定し、Createをクリックします。

Secure Internet Access

Name

SIA

Solution

sdwan



Description (optional)

Cancel

Create

次の設定では、Catalyst SD-WANエッジに設定を展開した後にトンネルを作成できます。

SSE Provider

Cisco SSE Zscaler

Context Sharing

VPN SGT

Tracker

Source IP address

{{ Monitoring }}

- SSEプロバイダー:SSE
- コンテキスト共有：ニーズに応じてVPNまたはSGTを選択
- トラッカー
 - 送信元IPアドレス：デバイス固有を選択します（これにより、デバイスごとに変更でき、導入段階での使用例を特定できます）。

設定手順で、トンネルをセットアップします。

Configuration

[+ Add Tunnel](#)



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.

- シングルハブHAのシナリオ：このシナリオでは、1つのNTGをアクティブとして、別のNTGをパッシブとして使用し、NTGあたり最大1 Gbpsのスループットでハイアベイラビリティを設定できます
- HAを使用したECMPのシナリオ：このシナリオでは、ハブごとに最大8つのトンネルを設定でき、NTGごとに合計で最大16のトンネルをサポートします。この設定により、トンネル間のスループットが向上します



注：ネットワークインターフェイスのスループットが1 Gbpsを超え、拡張性が必要な場合は、ループバックインターフェイスを使用する必要があります。それ以外の場合は、デバイスで標準インターフェイスを使用できます。これは、セキュアアクセス側からECMPをイネーブルにするためです。



警告: ECMPシナリオ用のループバックインターフェイスを設定する場合は、最初に、ルータで使用するポリシーの下で、Configuration Groups > Transport & Management Profileでループバックインターフェイスを設定する必要があります。

- onAdd Tunnelをクリックします

Edit Tunnel

Tunnel Type	<input checked="" type="radio"/> IPsec
Interface Name(1..255)	<input type="text"/> ipsec1
Tunnel Source Interface*	<input type="text"/> Loopback1
Tunnel Route Via	<input type="text"/> GigabitEthernet1
Tracker	<input checked="" type="checkbox"/> DefaultTracker
Data Center	<input checked="" type="radio"/> Primary <input type="radio"/> Secondary

- インターフェイス名:ipsec1、ipsec2、ipsec3など
- トンネル発信元インターフェイス：ループバックインターフェイスを選択するか、トンネルを確立する場所から特定のインターフェイスを選択します
- Tunnel Route Via:Loopbackを選択した場合、トラフィックのルーティング元の物理インターフェイスを選択する必要があります。Loopbackを選択しない場合、このオプションはグレーブ表示され、システムで検出された最初のNAT対応インターフェイスを使用します。複数ある場合は、目的のWANインターフェイスを選択する必要があります
- データセンター：これは、セキュアアクセスのどのハブに接続を確立するかを意味します

トンネル設定の次の部分では、シスコが提供するベストプラクティスを使用してトンネルを設定します。

Advanced Options

General

Shutdown

Track this interface

TCP MSS

 1350

IP MTU

 1390

DPD Interval

 10

DPD Retries

 3

IKE Diffie-Hellman Group

 20

- TCP MSS:1350
- IP MTU:1390
- IKE Diffie-Hellmanグループ:20

その後、セカンダリデータセンターを指すセカンダリトンネルを設定する必要があります。

シングルハブHAのシナリオ

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	 

これは、通常のシナリオ導入を使用した場合の最終結果です。

HAでのECMPのシナリオ

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

次に、セキュアインターネットポリシーでハイアベイラビリティを設定する必要があります。

High Availability

[+ Add Interface Pair](#)

Add Interface Pairをクリックします。

PRIMARY
SECONDARY

Edit Interface Pair

Primary Interface	Secondary Interface
ipsec1	ipsec11
Loopback1	Loopback11
GigabitEthernet1	GigabitEthernet1
DefaultTracker	DefaultTracker
Primary	Secondary

この手順では、セットアップするトンネルペアごとにプライマリおよびセカンダリトンネルを設定する必要があります。これは、各トンネルに独自のバックアップがあることを意味します。これらのトンネルは、厳密にこの目的のためにプライマリおよびセカンダリとして作成されていることに注意してください。

「アクティブインターフェイス」はプライマリトンネルを指し、「バックアップインターフェイス」はセカンダリトンネルを指します。

- アクティブインターフェイス：プライマリ
- バックアップインターフェイス：セカンダリ



警告：この手順をスキップすると、トンネルが確立されず、ルータからセキュアアクセスへの接続が確立されません。

トンネルにハイアベイラビリティを設定すると、次の図のように設定が表示されます。このガイドで使用するラボの例では、5つのトンネルがHAに表示されています。必要に応じてトンネルの数を調整できます。

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](#)



注:SD-WAN Catalyst vManageでは、最大8つのトンネルペア（16のトンネル：プライマリX 8とセカンダリX 8）を設定できます。Cisco Secure Accessは、最大10のトンネルペアをサポートします。

- [Save] をクリックします。

この後、すべてが正しく設定されると、SD-WAN ManagerおよびSecure AccessでトンネルがUPと表示されます。

SD-WANで確認するには、次の手順を確認します。

- Monitor > Tunnels の順にクリックします
- 次に onSIG/SSE Tunnels をクリックします。

Monitor All Sites ▾

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

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

Cisco Secure Accessに確立されたトンネルがUPになっているかどうかを確認できます。

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

セキュアアクセスで確認するには、次の手順を確認します。

- Connect > Network Connectionsの順にクリックします

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	Add
CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Connected	Europe (Germany)	sse-euc-1-1-1	8	sse-euc-1-1-0	8	...

詳細ビューで、トンネルの名前をクリックします。

PRIMARY		SECONDARY	
Hub Up	Active Tunnels	Hub Up	Active Tunnels
Tunnel Group ID	CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel Group ID	CBK-PAYG-560-5b28-4db0-b62e-9b589b5c687d
Data Center	sse-euc-1-1-1	Data Center	sse-euc-1-1-0
IP Address	3.120.45.23.2603.5004.80.20:c.1101	IP Address	18.156.145.74.2603.5004.80.20:c.1101
Network Tunnels			
Review this network tunnel group's IPsec tunnels. Help			
Tunnels	Peer ID	Peer Device IP Address	Data Center Name
Primary 1	131085	178.43.250.2	sse-euc-1-1-1
Primary 2	131086	178.43.250.2	sse-euc-1-1-1
Primary 3	131096	178.43.250.2	sse-euc-1-1-1
Primary 4	131087	178.43.250.2	sse-euc-1-1-1
Primary 5	131095	178.43.250.2	sse-euc-1-1-1
Primary 6	131077	178.43.250.2	sse-euc-1-1-1
Primary 7	131094	178.43.250.2	sse-euc-1-1-1
Primary 8	131078	178.43.250.2	sse-euc-1-1-1
Secondary 1	65559	178.43.250.2	sse-euc-1-1-0
Secondary 2	65560	178.43.250.2	sse-euc-1-1-0
Secondary 3	65538	178.43.250.2	sse-euc-1-1-0
Secondary 4	65548	178.43.250.2	sse-euc-1-1-0
Secondary 5	65552	178.43.250.2	sse-euc-1-1-0
Secondary 6	65554	178.43.250.2	sse-euc-1-1-0
Secondary 7	65555	178.43.250.2	sse-euc-1-1-0
Secondary 8	65558	178.43.250.2	sse-euc-1-1-0

その後、手順「SD-WANでカスタムバイパスのFQDNまたはアプリケーションを作成する」に進みます。

SD-WANでのカスタムバイパスFQDNまたはアプリケーションの作成（オプション）

アプリケーションバイパスと、ルーティングポリシーに適用できるFQDNまたはIPを作成する必要がある特別な使用例があります。

SD-WAN Managerポータルに移動します。

- Configuration > Application Catalog > Applicationsの順にクリックします

The screenshot shows the Application Catalog interface. At the top, there are tabs for Overview, Applications (which is highlighted with a blue border), Application Source Settings, Cloud Sourced Applications, Discovered Application (0), Application Lists, and Conflicts. On the right, there are buttons for 'SD-AVC Enabled' (with a green checkmark) and 'Configure Cloud Connection'. Below the tabs, there's a search bar with 'Applications 1553' and dropdown menus for 'Select Application Attributes' and 'Choose Filter'. To the right of the search bar are buttons for 'Custom Application', 'Export', and a refresh icon. A sub-header '0 selected' includes links for 'Create Application List' and 'Define Probe Endpoint'. The main table has columns: Application Name, Application Family, Application Group, Application Source, SaaS probe endpoint type, SaaS probe endpoint value, Traffic Class, Business Relevance, and Action. A single row is visible for 'Zannet'.



ヒント: 20.15より前のバージョンを実行している場合は、ポリシーリストでカスタムアプリケーションを作成できます



注：アプリケーションカタログにアクセスするには、SD-AVCを有効にする必要があります。

- カスタムアプリケーションをクリックします。

This screenshot is identical to the one above, showing the Application Catalog interface with the Applications tab selected. It includes the same search bar, filter options, and table structure. The table shows a single row for 'Zannet'.

この段階では、基本的な除外をSecure Client - UmbrellaモジュールSWG FQDNを使用して設定します。

プロキシ SecureAccess

Custom Application

Name of the Custom APP

Application Name ⓘ
ProxySecureAccess
Application Name: ProxySecureAccess-Custom

Server Names ⓘ
swg-url-proxy-https-sse.sigproxy.qq.opendns.com

FQDN

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 ⓘ	Ports ⓘ	L4 Protocol ⓘ
10.X.X.X, 20.0.0.0/24 separated by	Space separated ports or range or	Enter L4 Protocol

SaaS probe endpoint type
 IP Address FQDN URL

SaaS probe endpoint value

Cancel Save

- Server Name：バイパスするFQDNを使用します（この例では、SWGのFQDNが設定されています）。
 - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
 - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- [Save] をクリックします。



注：ORGIDをSSE組織番号に変更してください。

次に、基本的な除外が作成されます。この場合、Umbrella DNSサーバは次のようになります。

包括DNS

Custom Application

Name of the Custom App

Application Name: UmbrellaDNS

Server Names: Enter Server Names

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: [Text input field]

Cancel Save

これで、ルーティングポリシーの設定に進むことができます。

トラフィックのルーティング

この手順では、Cisco Secure Access経由で保護するために、トンネルを介してインターネットトラフィックをルーティングする必要があります。このケースでは、特定のトラフィックをバイパスできる柔軟なルーティングポリシーを使用して、セキュアアクセス経由で不要なトラフィックが送信されないようにしたり、潜在的な悪習を回避したりします。

まず、使用できる2つのルーティング方式を定義します。

- Configuration > Configuration Groups > Service Profile > Service Route : この方法では、セキュアなアクセスにルーティングできますが、柔軟性がありません。
- Configuration > Policy Groups > Application Priority & SLA : この方法では、SD-WAN内でさまざまなルーティングオプションが提供されます。また、最も重要な点として、特定のトラフィックがセキュアアクセスを介して送信されないように、そのトラフィックをバイパスすることができます。

柔軟性とベストプラクティスとの整合性を確保するため、アプリケーションの優先度とSLAの設定を使用します。

- Configuration > Policy Groups > Application Priority & SLA の順にクリックします
- 次に、Application Priority & SLA Policy をクリックします。

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
------	-------------	------------	--------

- ポリシー名を設定し、Createをクリックします。

Application Priority & SLA Policy

Policy Name

Description (optional)

Cancel Create

- 高度なレイアウトの有効化
- +トラフィックポリシーの追加をクリックします。

Policies > Application Priority & SLA
SIA-ROUTE ⓘ Additional Settings Advanced Layout

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

+ Add Traffic Policy 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 : このトラフィックポリシーリストの目的に合わせてこれを調整する名前
- VPN(s) : トラフィックのルーティング元ユーザのサービスVPNを選択します。
- 方向 : サービスから
- 既定の操作 : 受け入れ

その後、トラフィックポリシーの作成を開始できます。

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

VPN: Corporate_Users Direction: From Service Default Action: Accept		
<input type="text"/> Search rule by name or order		
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. ローカルネットワークポリシー (オプション) : 送信元101.101.101.0/24、宛先172.16.200.0/24。このルートにより、ネットワーク内トラフィックがCisco Secure Accessに送信されなくなります。通常、内部ルーティングはSD-WAN展開ではディストリビューションルータによって処理されるため、お客様はこれを行いません。この設定では、シナリオで必要かどうかによっ

て、これらのサブネット間の内部トラフィックがセキュアアクセスにルーティングされないようにします（オプション、ネットワーク環境によって異なります）

2. BypassSSEProxy（オプション）：このポリシーは、Secure ClientおよびSWGが有効なCisco Umbrellaモジュールを持つ内部コンピュータが、プロキシトラフィックをクラウドに送信し直すことを防ぎます。プロキシトラフィックをクラウドに再ルーティングすることは、ベストプラクティスとは見なされません。
3. UmbrellaDNS（ベストプラクティス）：このポリシーは、インターネット宛てのDNSクエリがトンネル経由で送信されるのを防ぎます。トンネル経由でUmbrellaリゾルバ（208.67.222.222, 208.67.220.220）にDNSクエリを送信することは推奨されません。
4. SIA AUTO FULL TRAFFIC：このポリシーにより、送信元101.101.101.0/24からのすべてのトラフィックは、先ほど作成したSSEトンネルを経由してインターネットにルーティングされ、このトラフィックはクラウドで保護されます。

確認

トラフィックがCisco Secure Access経由ですでにフラッディングしているかどうかを確認するには、イベント、アクティビティ検索、またはネットワーク全体のパスインサイトに移動し、トンネルIDでフィルタリングします。

セキュアアクセス – アクティビティ検索

Monitor > Activity Searchの順に移動します。

The screenshot shows the 'Activity Search' interface with the following details:

- Filters:** Identity: C8K-PAYG-0f3-d4e8-4ea8-bc90-ca09e47f22f6.
- Event Details:** Action: Allowed, Time: Dec 28, 2025 6:14 AM, Rule Name: For all Internet access (2100958), Source: +VPN-10 (VPN-10), Destination: https://img3.joymax.com, Security Group Tag (SGT): -.
- Table Headers:** Response, Select All, Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Destination Country.
- Table Data:** A list of events including:
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (142.250.186.174:443, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (142.250.186.174:443, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)
 - +VPN-10 (VPN-10) → +VPN-10 (VPN-10) → https://img3.joymax.com (110.234.18.177, United States)

セキュアなアクセス : イベント

Monitor > Eventsの順に移動します。

>	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



注：ロギングが有効（デフォルトでは無効）になっているデフォルトポリシーがあることを確認してください。

Catalyst SD-WAN Manager – ネットワーク全体のパスインサイト

Catalyst SD-WAN Managerに移動します。

- Tools > Network-Wide Path Insights の順にクリックします
- New Trace をクリックします。

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

Enable DNS Domain Discovery ⓘ

Trace Name e.g trace_[site ID]

Trace Duration(minutes) 60

Filters

Select Site(branch site only)* SITE_101 *

VPN* 1 VPN(s) ×

Source Address/Prefix 101.101.101.20

Destination Address/Prefix

Application ⓘ Application Group ⓘ

- Site (サイト) : トラフィックが発生しているサイトを選択します。
- VPN : トラフィックが発生しているサブネットのVPN IDを選択します
- 送信元: サイトおよびVPNの選択でフィルタリングされたすべてのトラフィックをフィルタリングするため、IPを配置するか、空白にします。

Insightsでは、トンネルを通過するトラフィックフラッディングと、セキュアアクセスに送られるトラフィックのタイプを確認できます。

INSIGHTS Selected trace: trace_80 (Trace Id: 80)

Applications Active Flows Completed Flows Selected Flow ID: 50

Filter ▾

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	View ⓘ	10	101.101.101.20	54688	172.211.123.249	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g... N/A		
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	
7:35:23 AM-7:35:23 AM	563	View ⓘ	10	101.101.101.20	56408	172.211.123.248	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-services	ms-cloud-g... N/A		
7:37:35 AM-7:37:35 AM	668	View ⓘ	10	101.101.101.20	53175	8.8.8.8	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	N/A	
7:37:38 AM-7:37:38 AM	573	View ⓘ	10	101.101.101.20	56560	3.74.137.87	443	TCP	DEFAULT ↑ / DEFAULT ↓	ProxySecureA...	other	N/A	

関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [Cisco Secure Accessヘルプセンター](#)
- [Cisco SASE設計ガイド](#)
- [Cisco Catalyst SD-WANセキュリティコンフィギュレーションガイド、Cisco IOS XE Catalyst SD-WANリリース17.x](#)
- [Cisco SASEソリューション : Cisco Secure Accessと統合されたCisco Catalyst SD-WAN At-a-Glance](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。