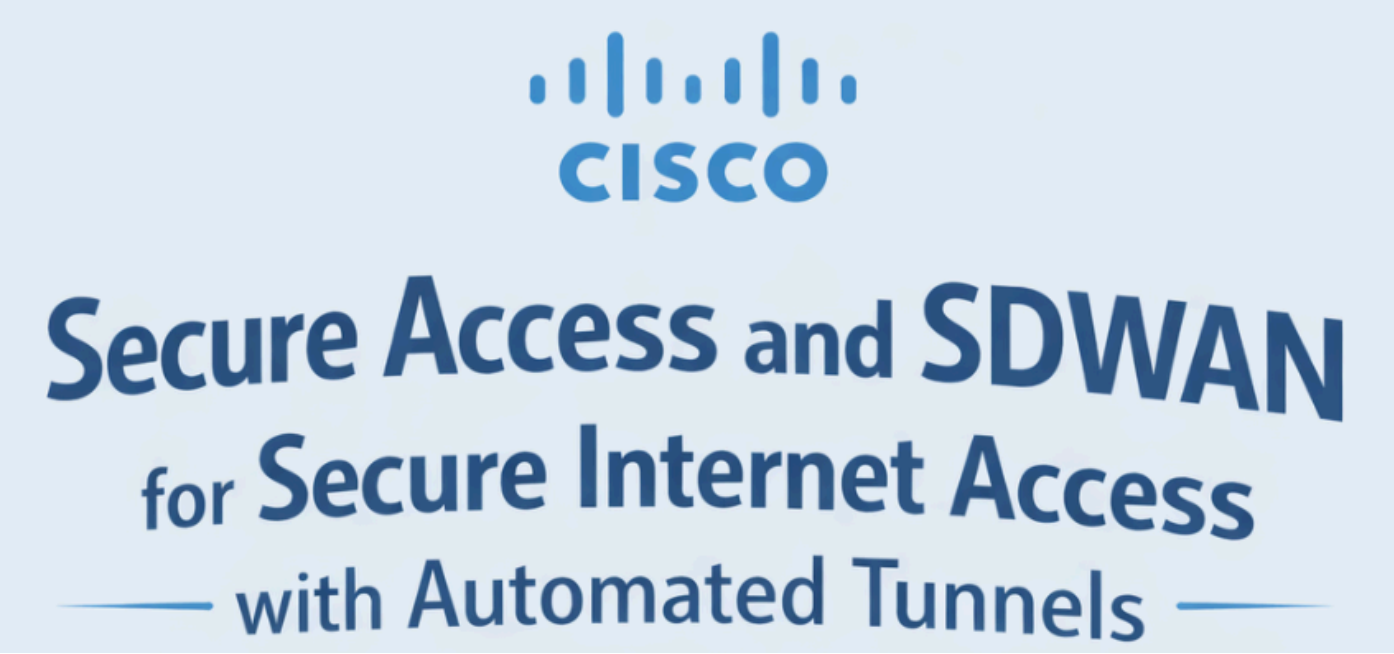
セキュアインターネットアクセスのためのSD-WAN自動トンネルを使用したセキュアアクセスの設定

内容

はじめに

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。



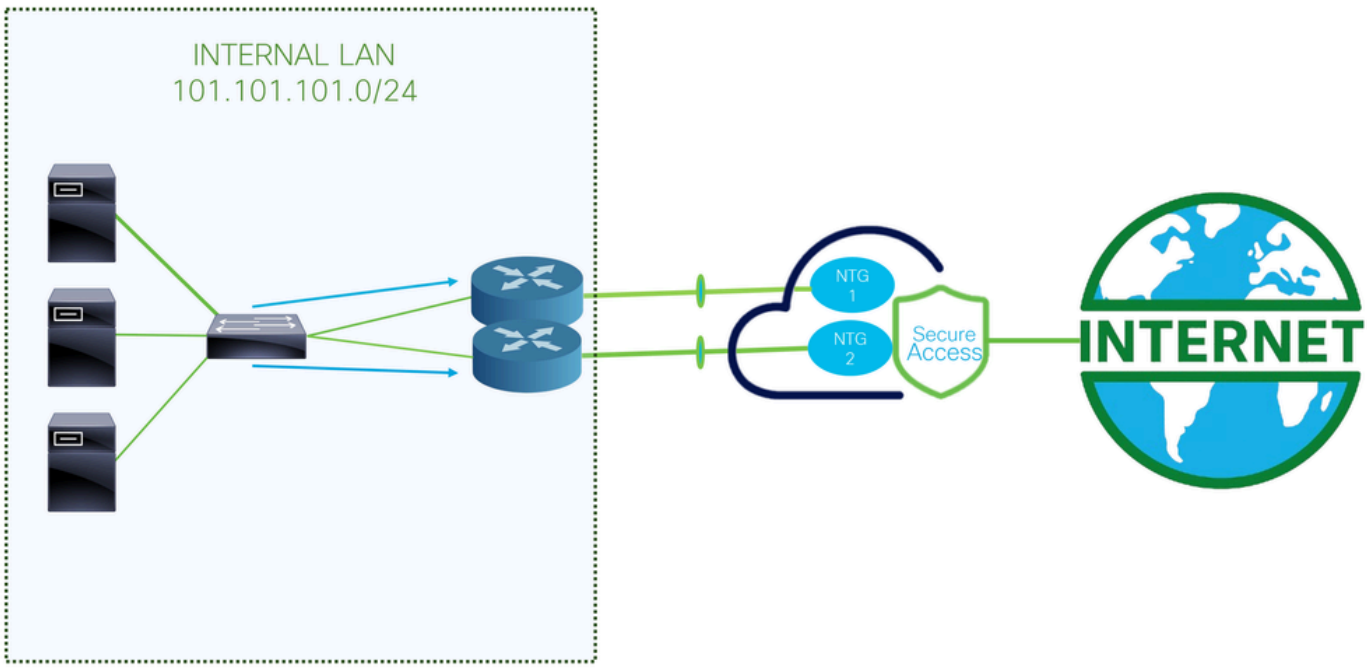
背景説明

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

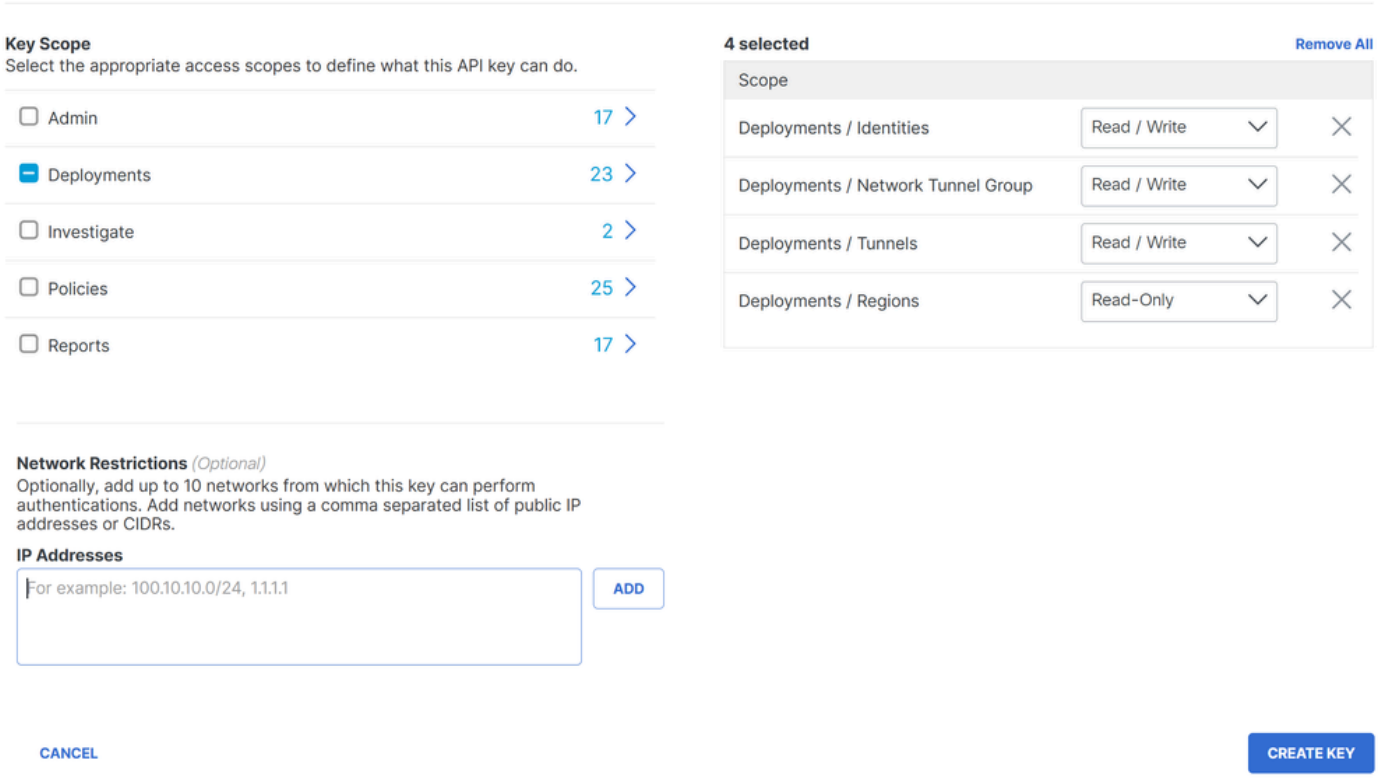
セキュアアクセスの設定

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。

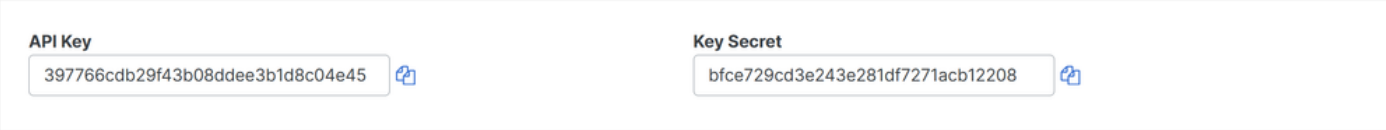
Secure Access Dashboardに移動します。

- 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



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。



⚠ 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。

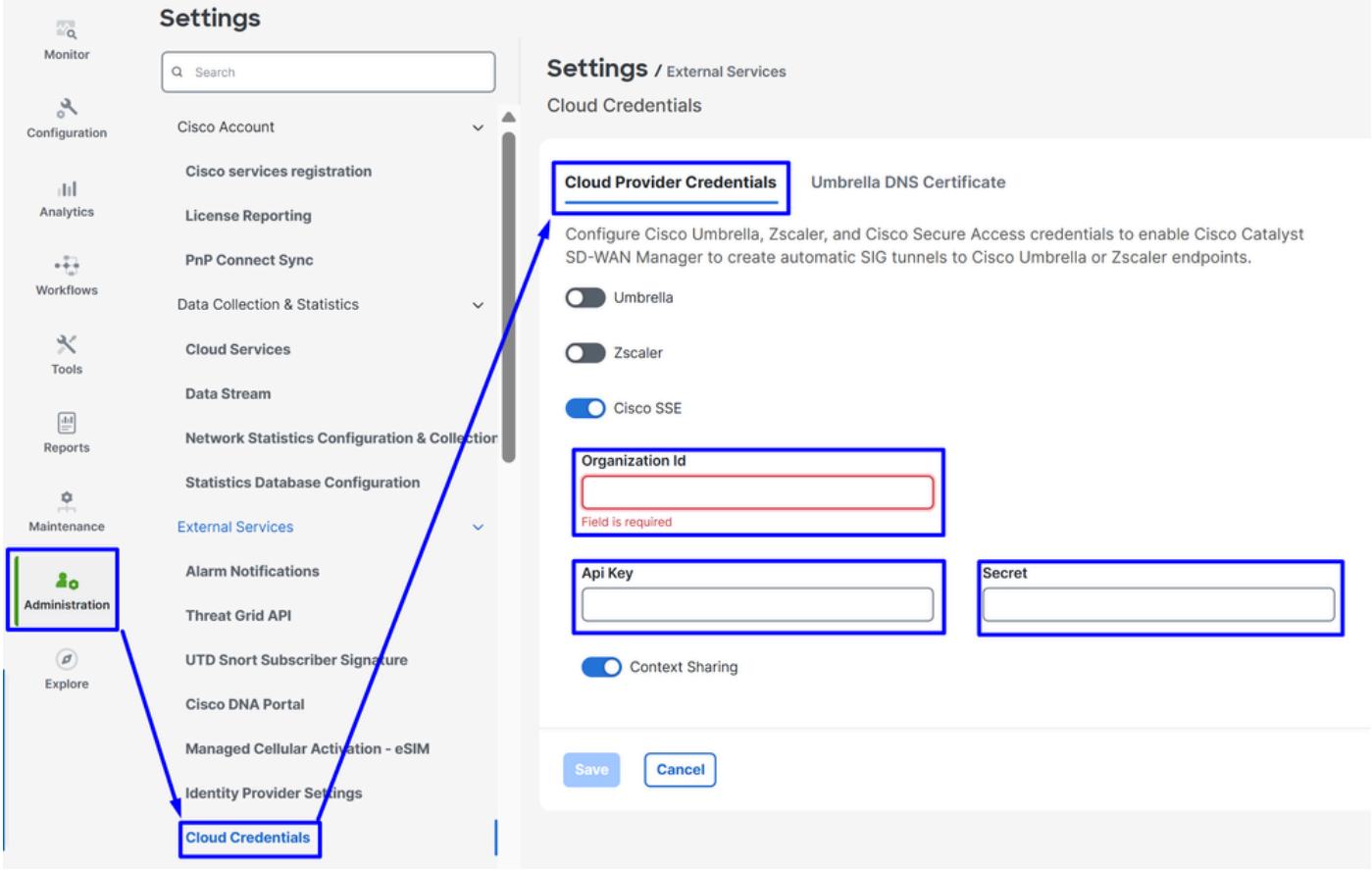
次に、ACCEPT AND CLOSEをクリックして完了します。

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



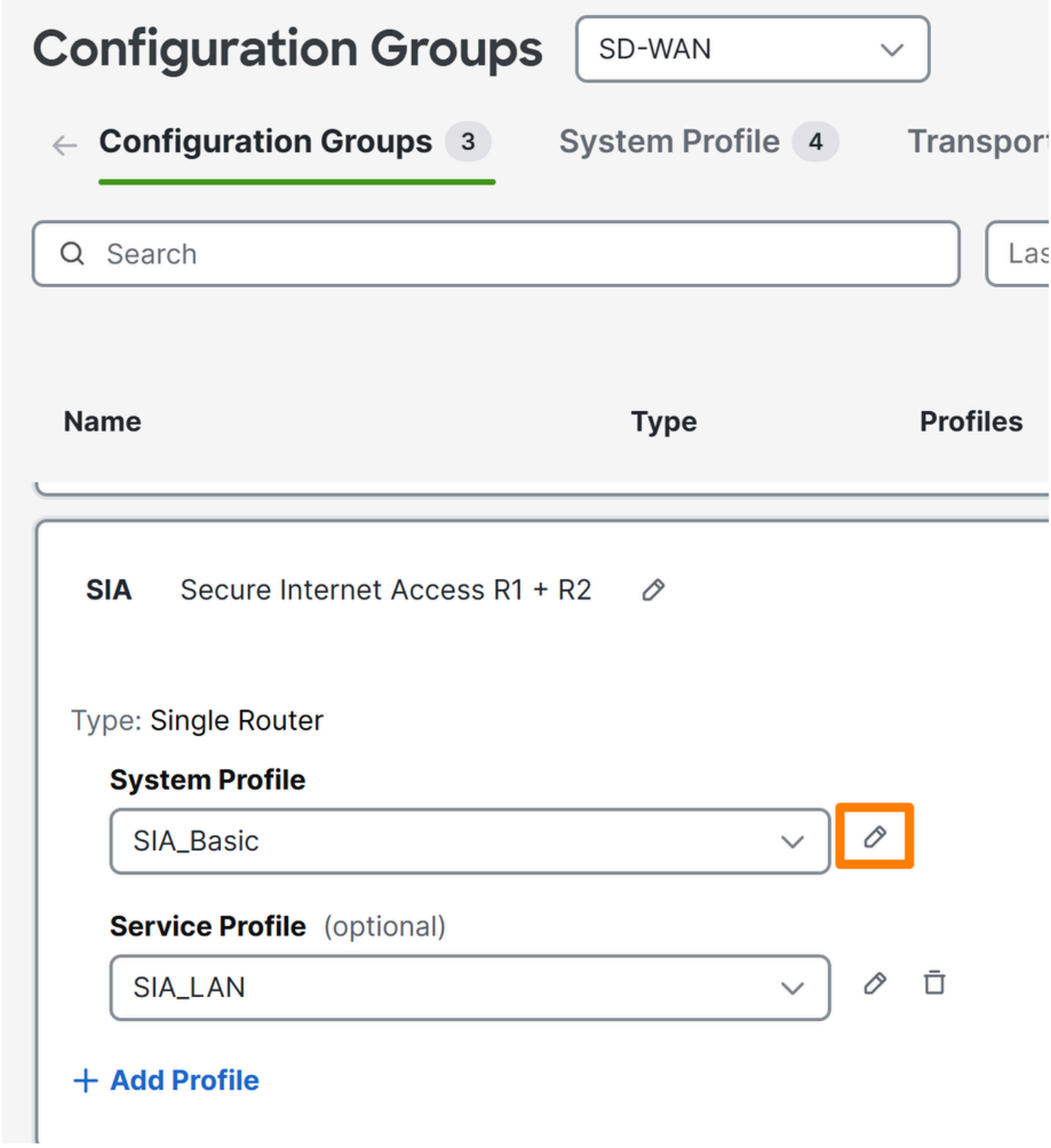
- 組織ID:SSEダッシュボードのURL(https://dashboard.sse.cisco.com/org/xxxxx)から取得できます。
- Apiキー:セキュアアクセス設定の手順からコピーします。
- 秘密：セキュアアクセス設定の手順からコピーします。

その後、Saveボタンをクリックします。

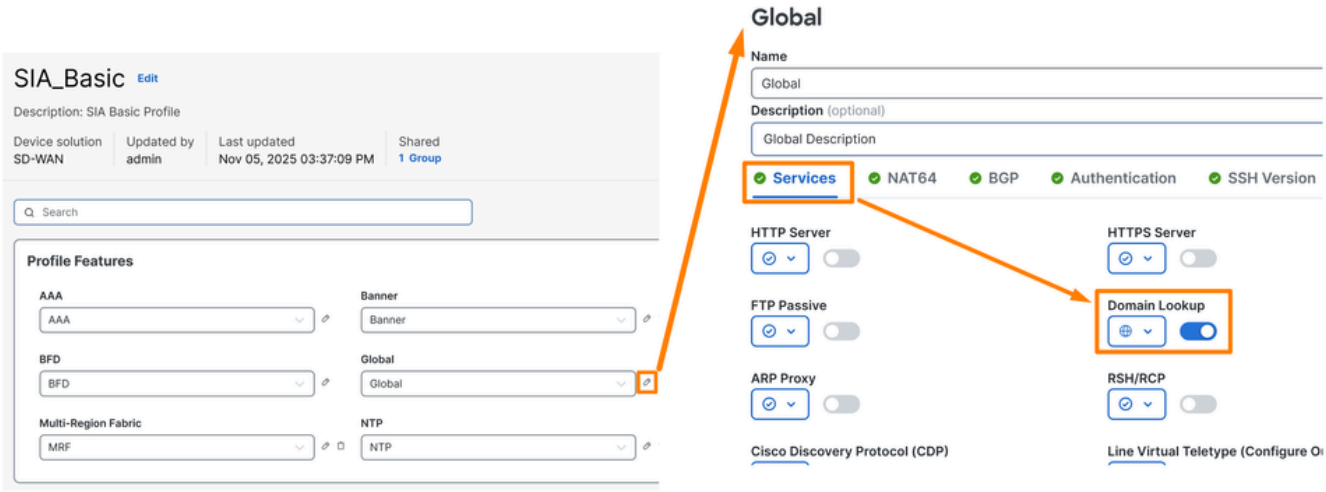
注：次の手順に進む前に、SD-WAN ManagerとCatalyst SD-WANエッジにDNS解決とインターネットアクセスがあることを確認する必要があります。

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。



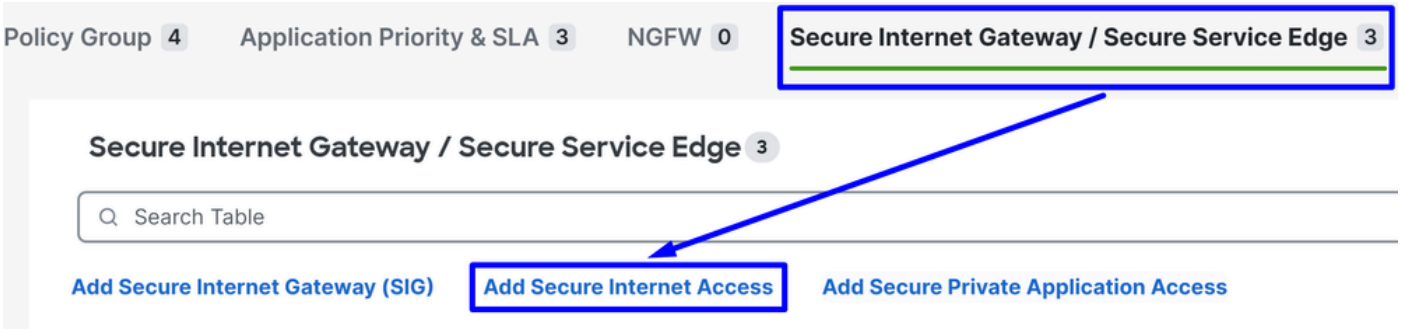
- 次に、Globalオプションを編集して、Domain Resolutionオプションが有効になっていることを確認します



ポリシーグループの設定

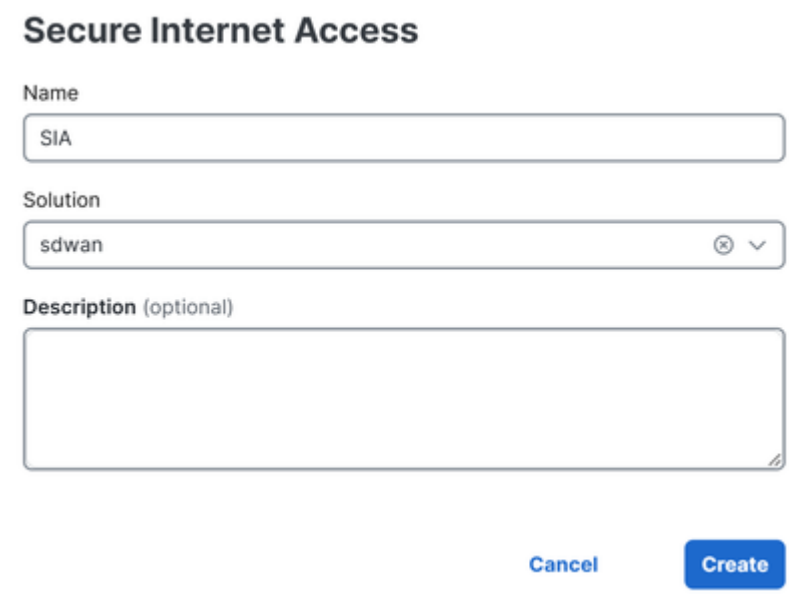
Configuration > Policy Groupsの順に移動します。

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

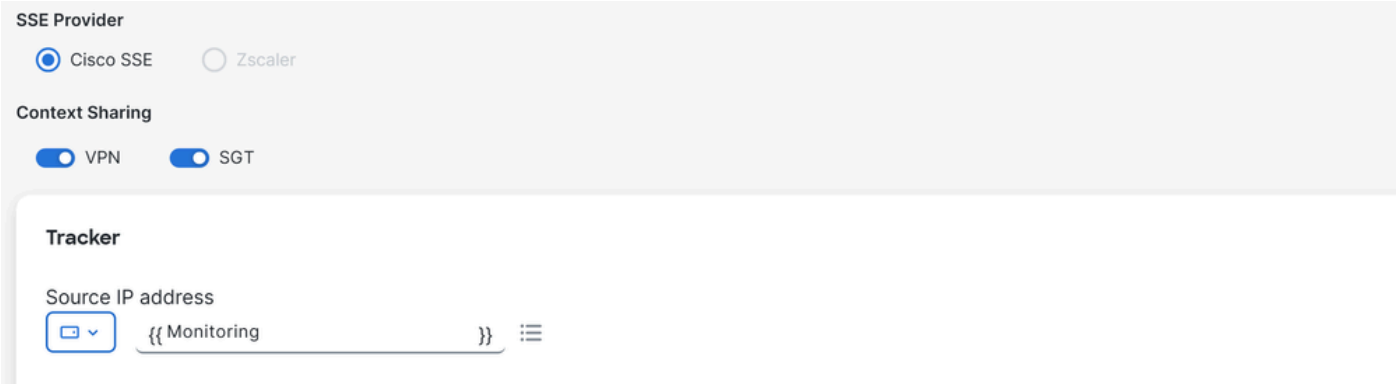


注:20.18より前のリリースでは、このオプションはAdd Secure Service Edge(SSE)と呼ばれています

- 名前とソリューションを設定し、Createをクリックします。

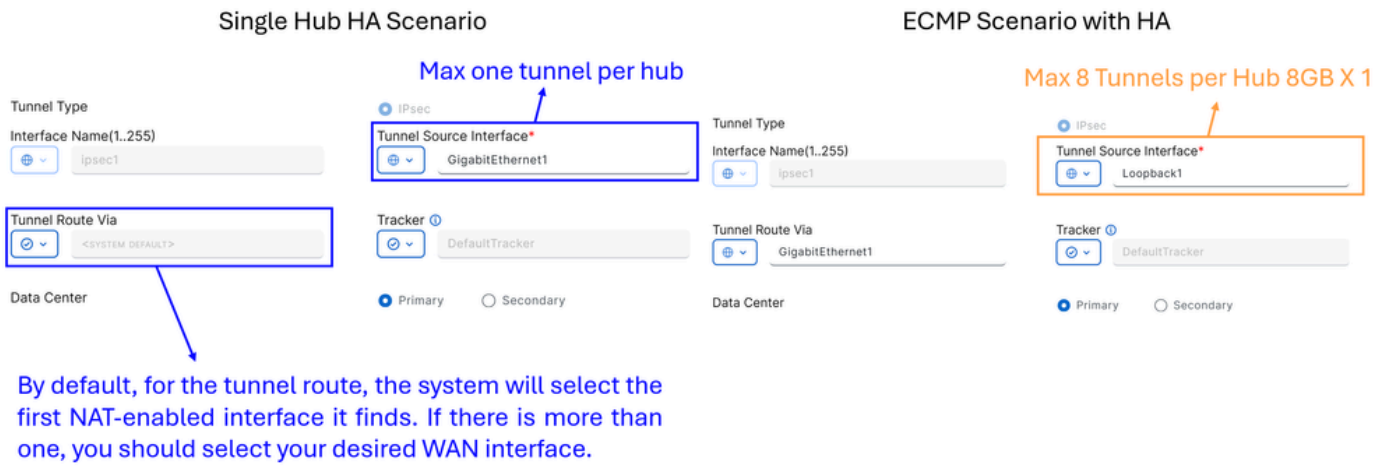


次の設定では、Catalyst SD-WANエッジに設定を展開した後にトンネルを作成できます。



- 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。

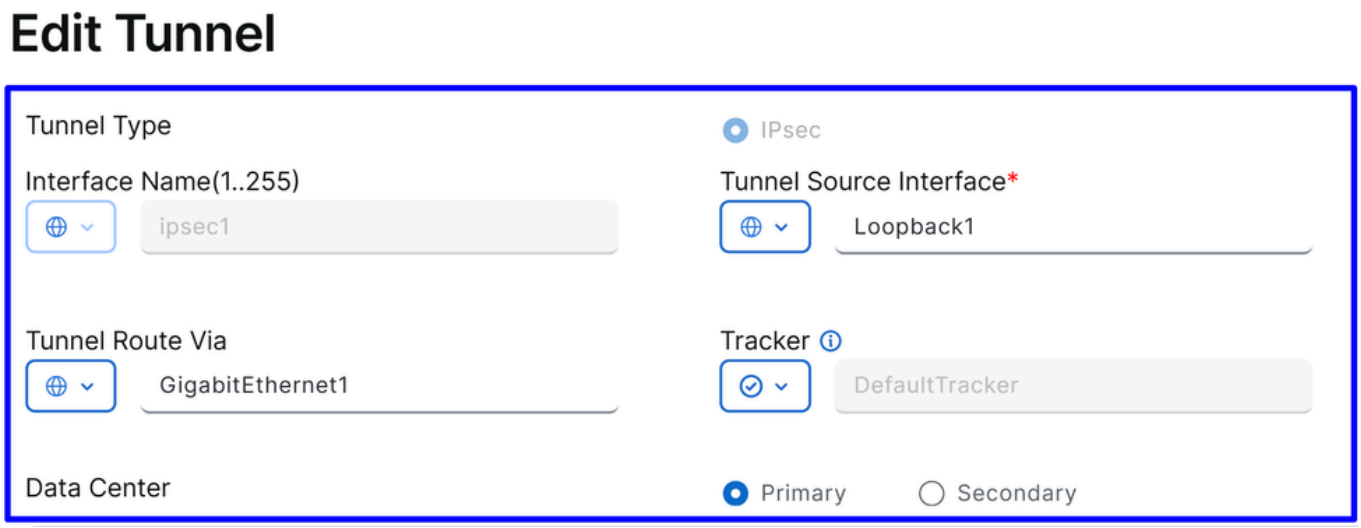


- シングルハブHAのシナリオ：このシナリオでは、1つのNTGをアクティブとして、別のNTGをパッシブとして使用し、NTGあたり最大1 Gbpsのスループットでハイアベイラビリティを設定できます
- HAを使用したECMPのシナリオ：このシナリオでは、ハブごとに最大8つのトンネルを設定でき、NTGごとに合計で最大16のトンネルをサポートします。この設定により、トンネル間のスループットが向上します

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。

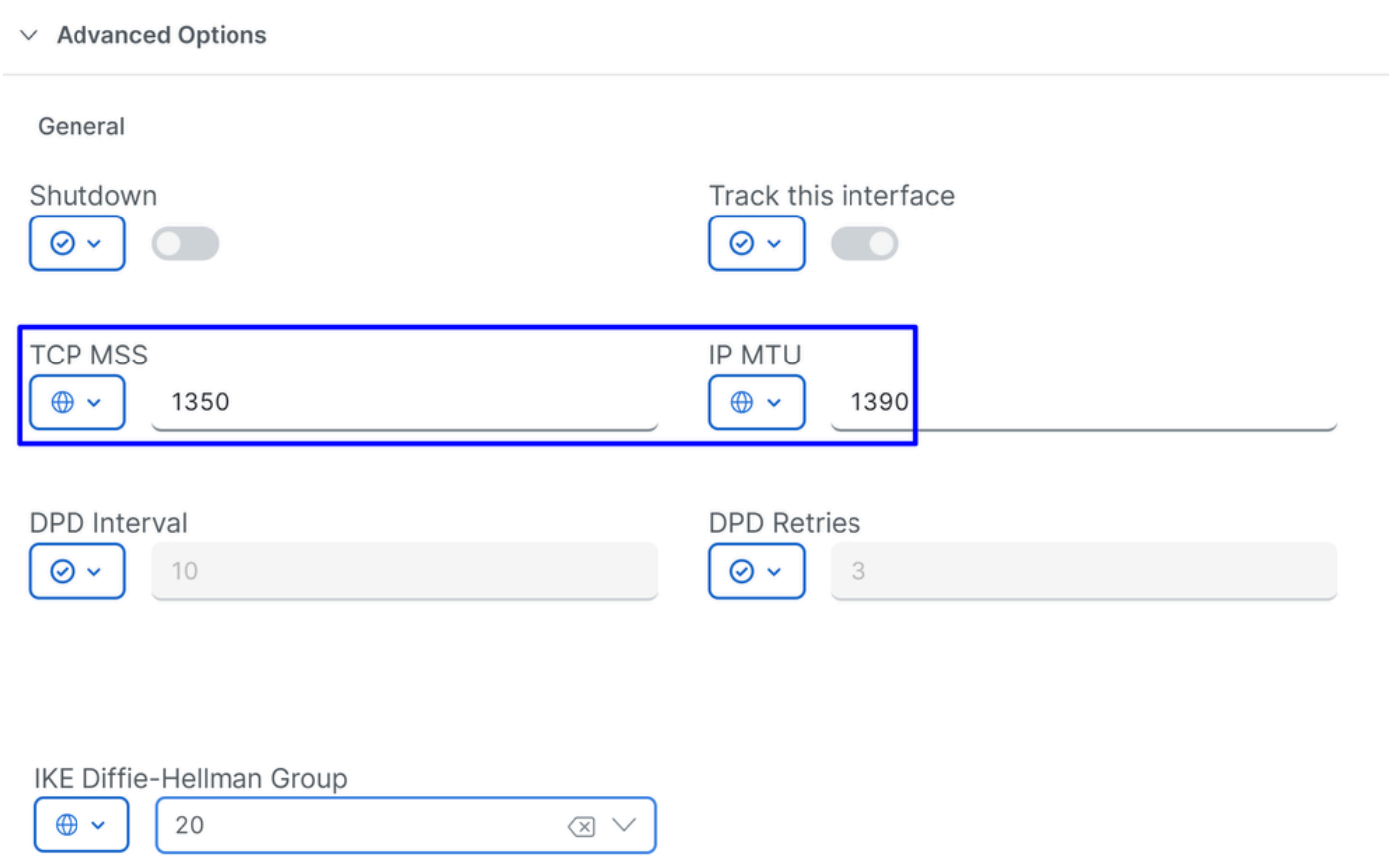
警告:ECMPシナリオ用のループバックインターフェイスを設定する場合は、最初に、ルータで使用するポリシーの下で、Configuration Groups > Transport & Management Profileでループバックインターフェイスを設定する必要があります。

- onAdd Tunnelをクリックします



- 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

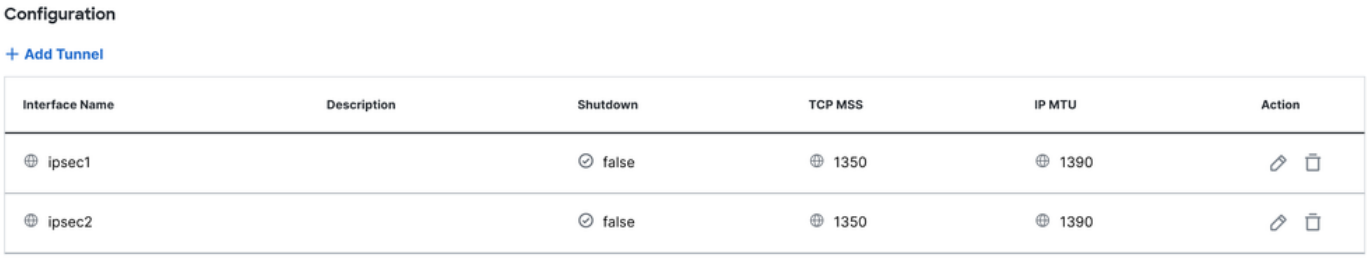
トンネル設定の次の部分では、シスコが提供するベストプラクティスを使用してトンネルを設定します。



- 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

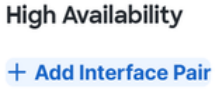


これは、通常のシナリオ導入を使用した場合の最終結果です。

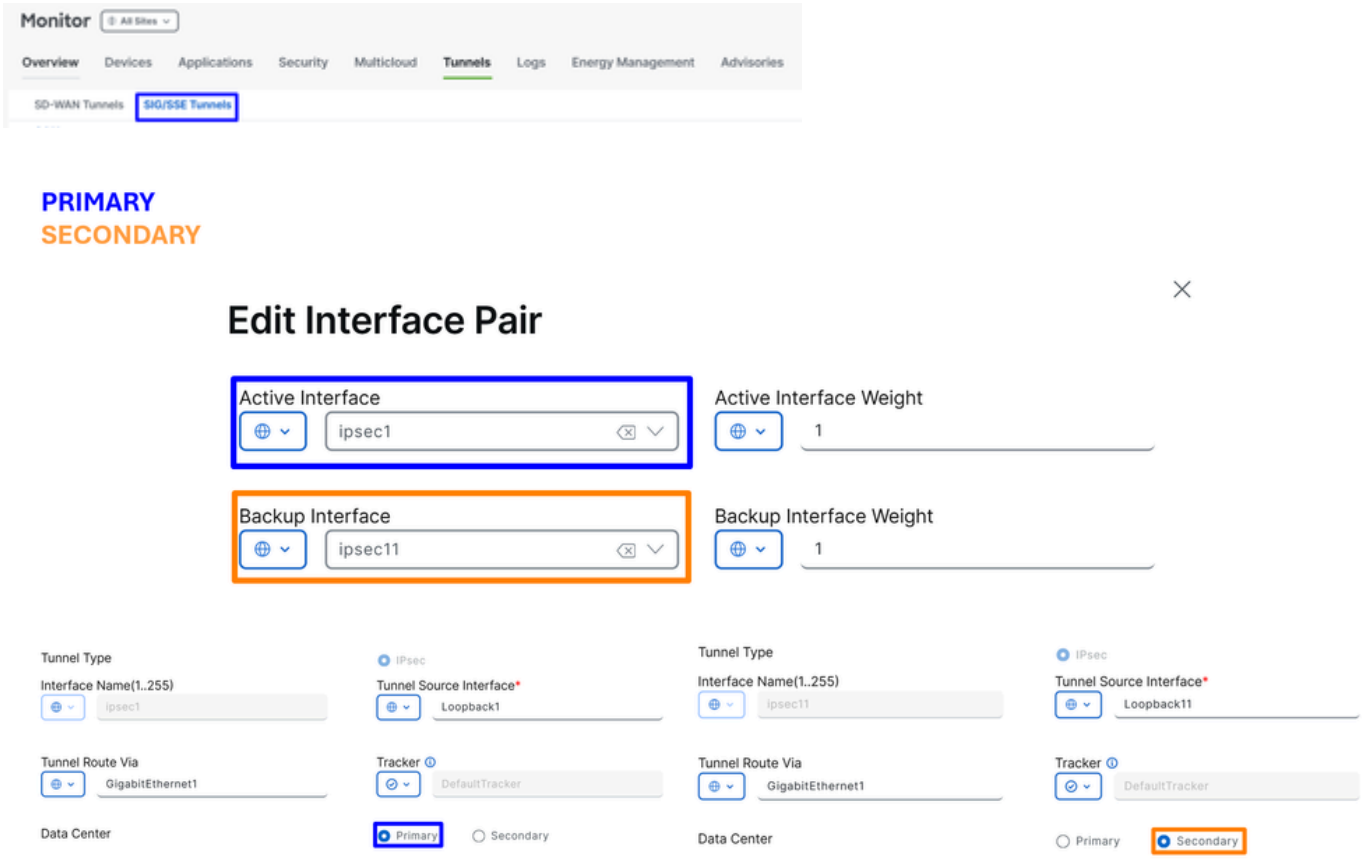
HAでのECMPのシナリオ

Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1		false	1350	1390
ipsec2		false	1350	1390
ipsec3	PRIMARY HUB	false	1350	1390
ipsec4		false	1350	1390
ipsec5		false	1350	1390
ipsec11		false	1350	1390
ipsec12		false	1350	1390
ipsec13	SECONDARY HUB	false	1350	1390
ipsec14		false	1350	1390
ipsec15		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。



Add Interface Pairをクリックします。

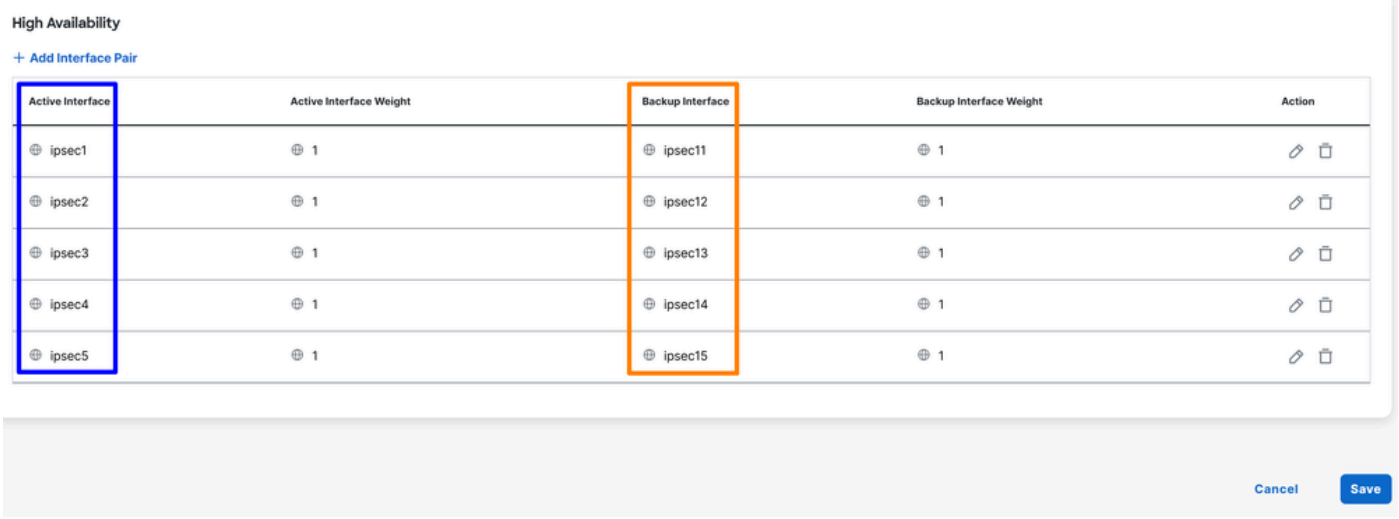


この手順では、セットアップするトンネルペアごとにプライマリおよびセカンダリトンネルを設定する必要があります。これは、各トンネルに独自のバックアップがあることを意味します。これらのトンネルは、厳密にこの目的のためにプライマリおよびセカンダリとして作成されていることに注意してください。
「アクティブインターフェイス」はプライマリトンネルを指し、「バックアップインターフェイス」はセカンダリトンネルを指します。

- 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。



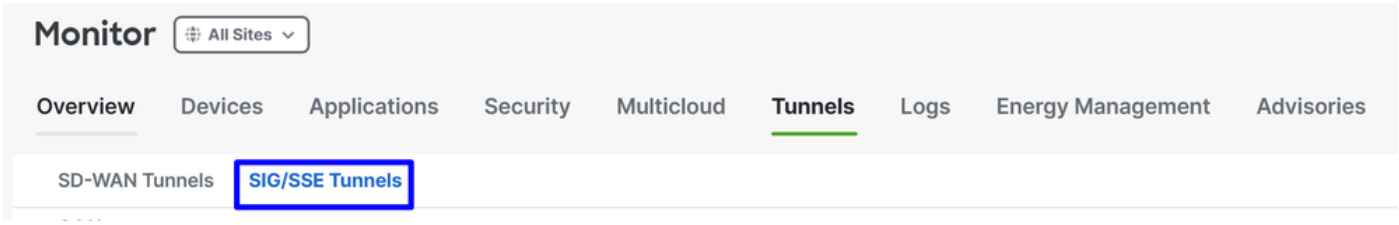
注:SD-WAN Catalyst vManageでは、最大8つのトンネルペア（16のトンネル：プライマリX 8とセカンダリX 8）を設定できます。Cisco Secure Accessは、最大10のトンネルペアをサポートします。

- [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。

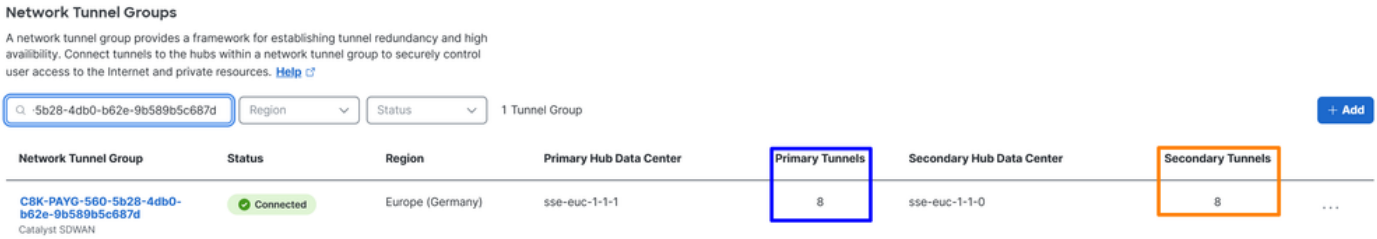


Cisco Secure Accessに確立されたトンネルがUPになっているかどうかを確認できます。

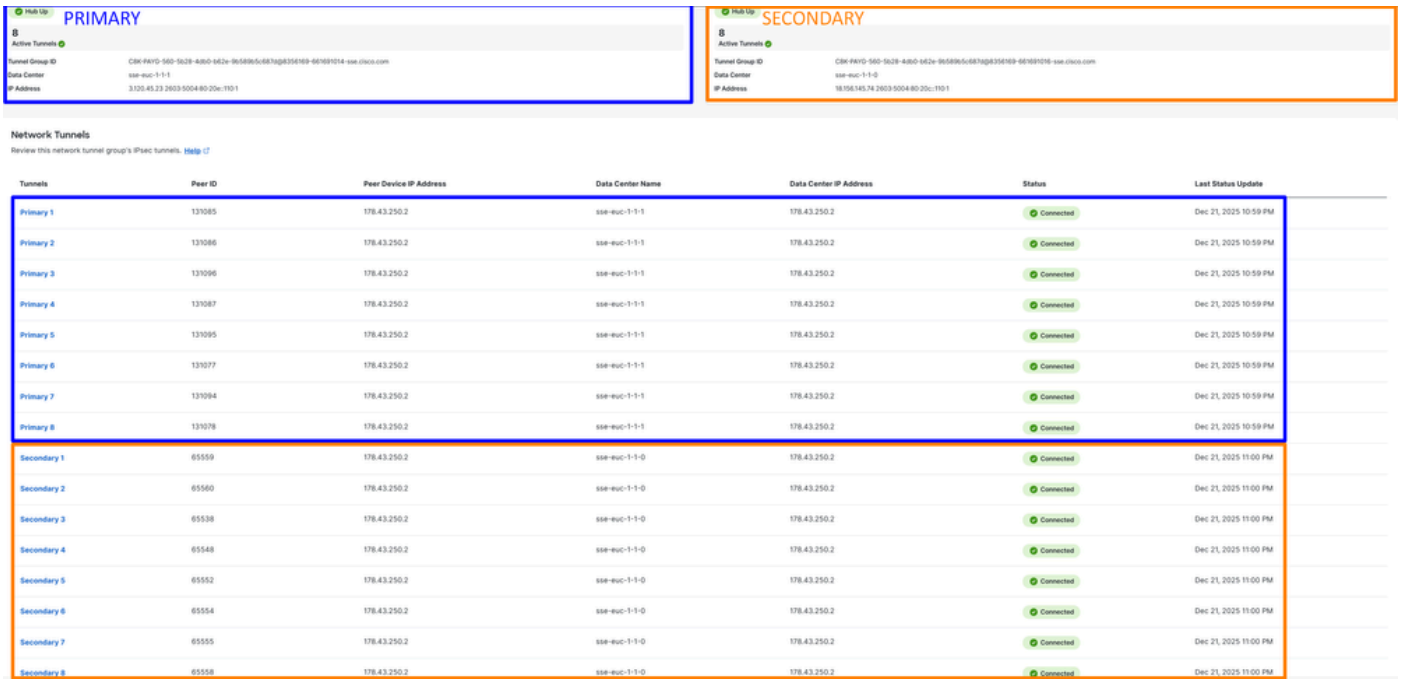
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public 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



詳細ビューで、トンネルの名前をクリックします。



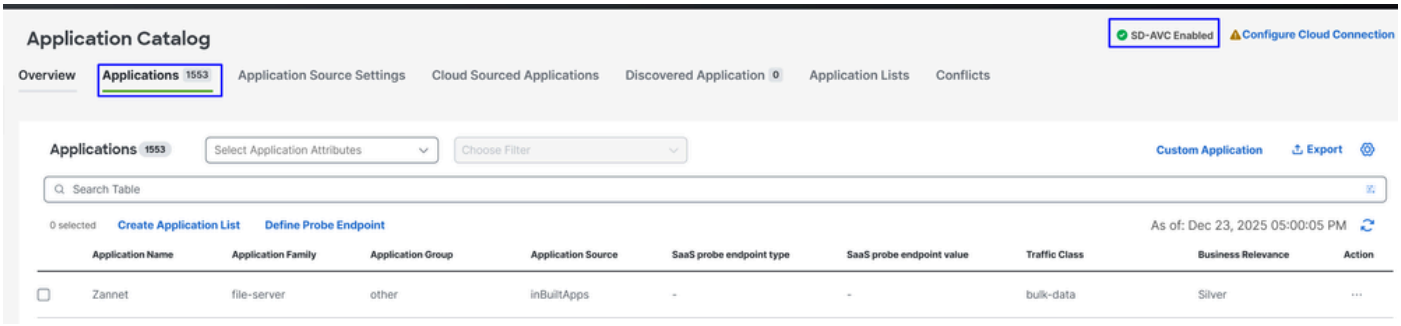
その後、手順「SD-WANでカスタムバイパスのFQDNまたはアプリケーションを作成する」に進みます。

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。

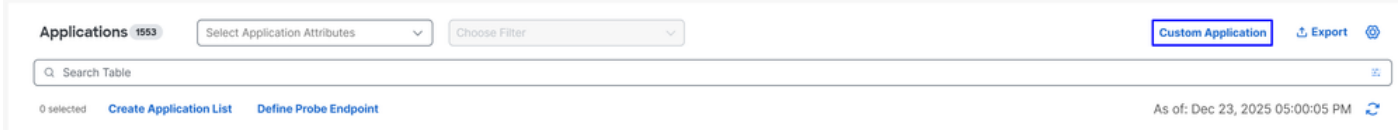
- Configuration > Application Catalog > Applicationsの順にクリックします



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

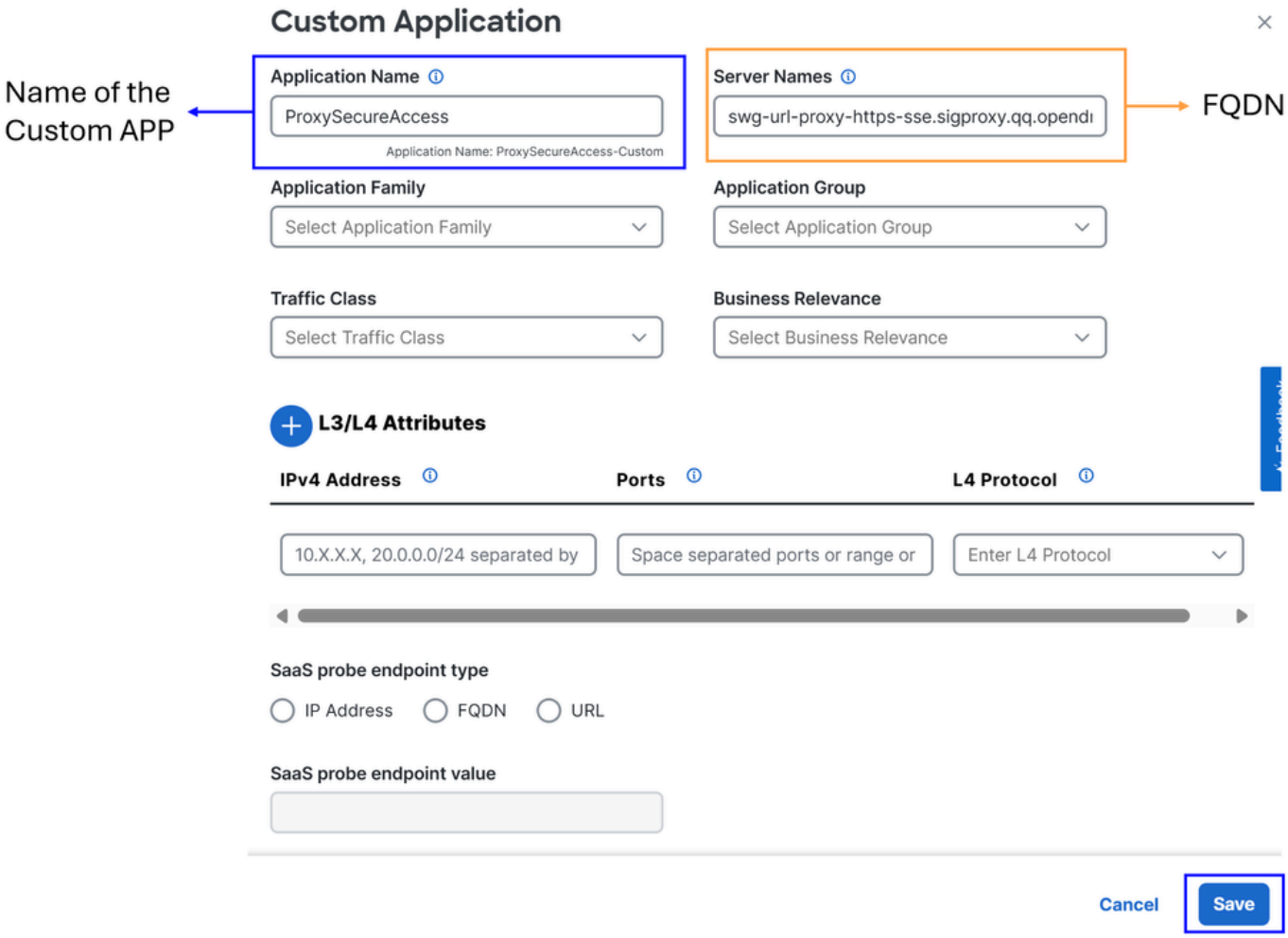
注：アプリケーションカタログにアクセスするには、SD-AVCを有効にする必要があります。

- カスタムアプリケーションをクリックします。



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

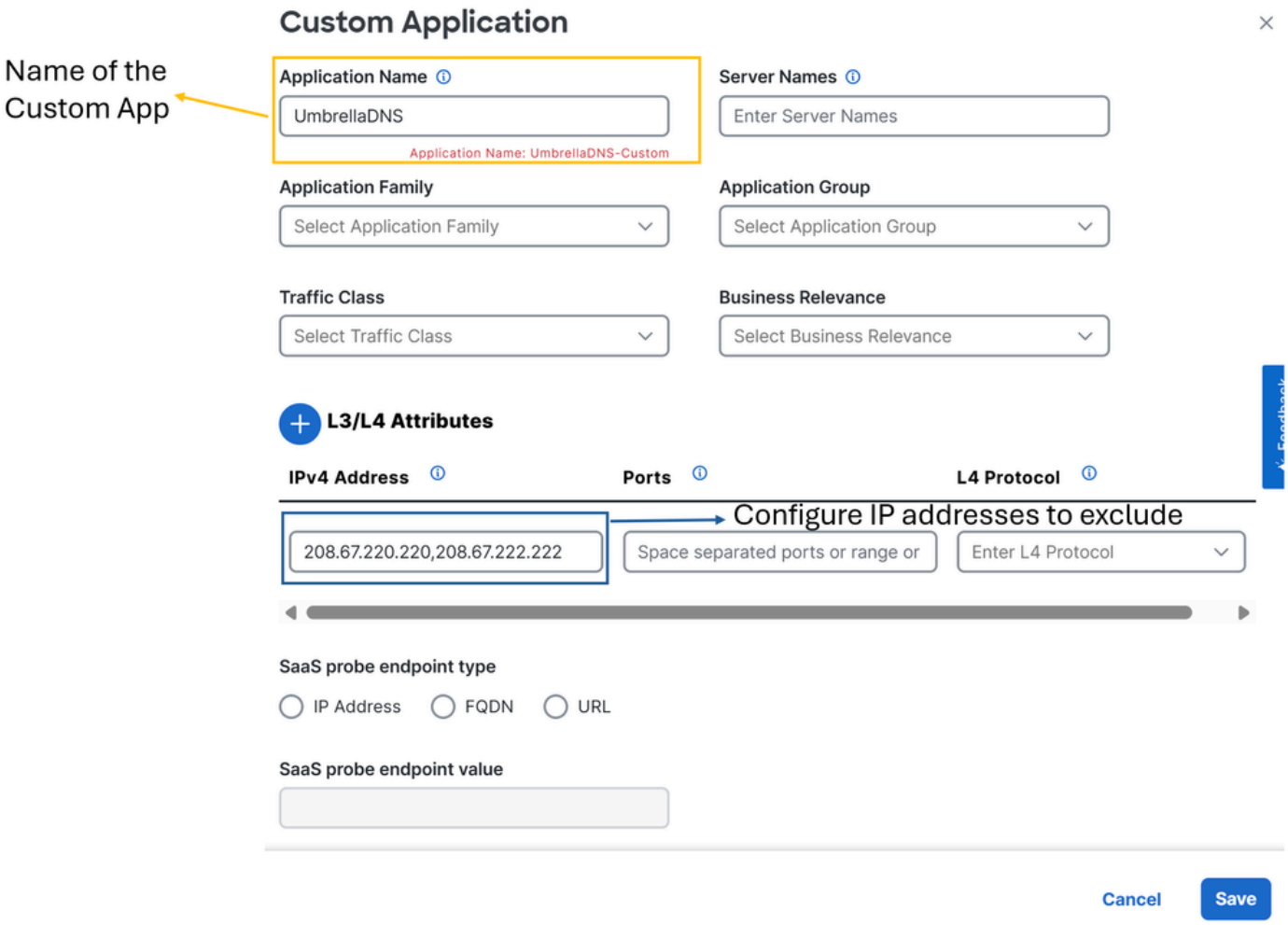


- Server Name：バイパスするFQDNを使用します（この例では、SWGのFQDNが設定されています）。
  - swg-url-proxy-https-sse.sigproxy.qq.op endns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.op endns.com
- [Save] をクリックします。

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



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。

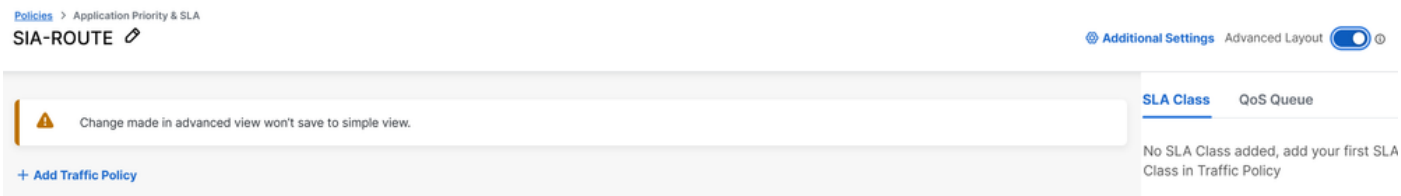
- Configuration > Configuration Groups > Service Profile > Service Route：この方法では、セキュアなアクセスにルーティングできますが、柔軟性がありません。
- **Configuration** > Policy Groups > Application Priority & SLA：この方法では、SD-WAN内でさまざまなルーティングオプションが提供されます。また、最も重要な点として、特定のトラフィックがセキュアアクセスを介して送信されないように、そのトラフィックをバイパスすることができます。

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。

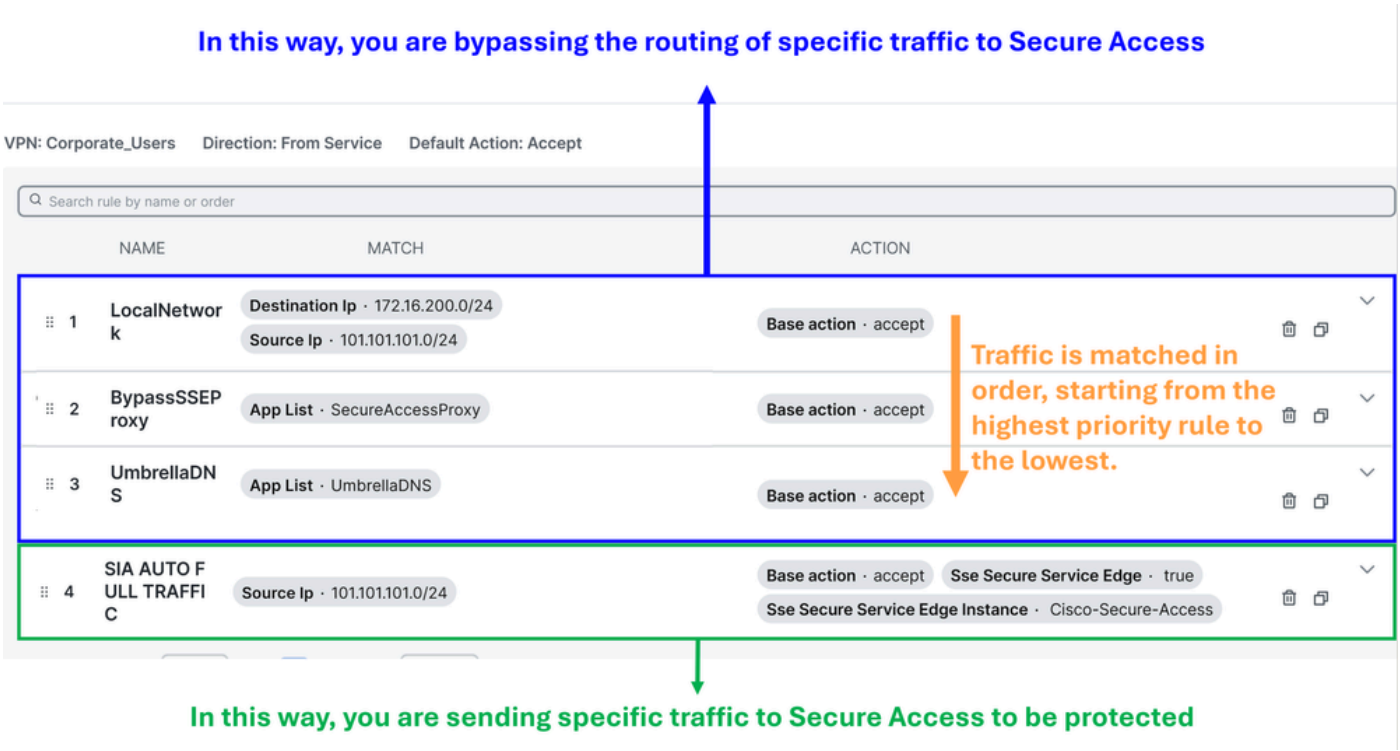
- ポリシー名を設定し、Createをクリックします。

- 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。



- 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。



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）

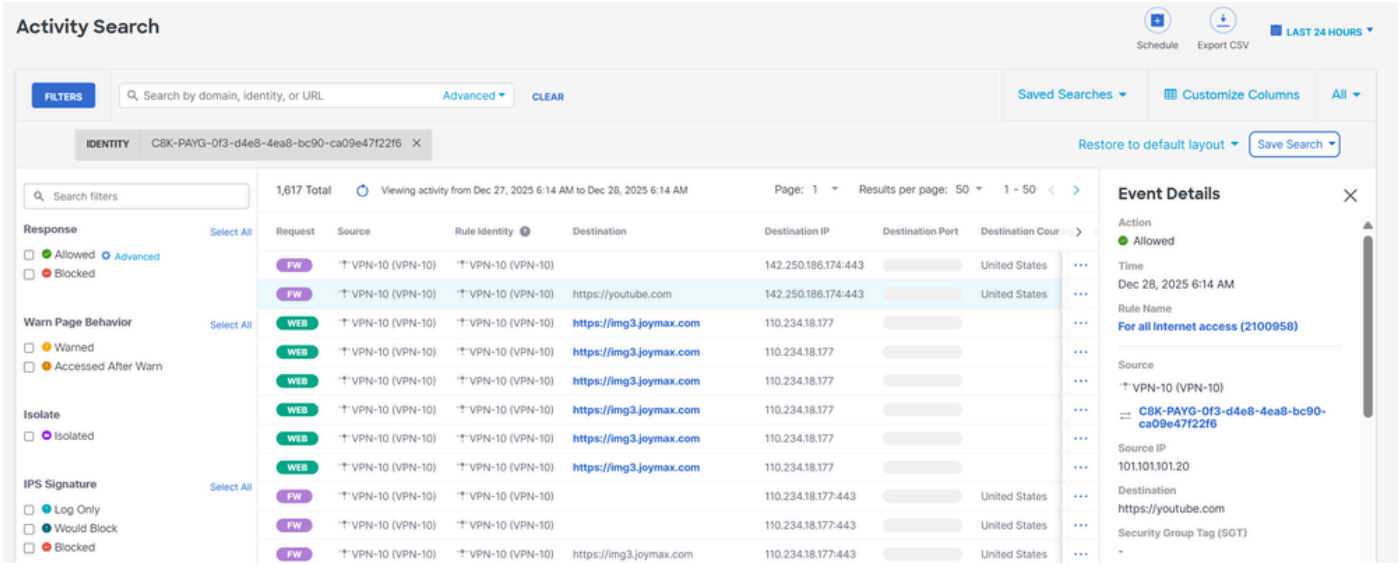
2. **BypassSSEProxy**（オプション）：このポリシーは、Secure ClientおよびSWGが有効なCisco Umbrellaモジュールを持つ内部コンピュータが、プロキシトラフィックをクラウドに送信し直すことを防ぎます。プロキシトラフィックをクラウドに再ルーティングすることは、ベストプラクティスとは見なされません。
3. UmbrellaDNS（ベストプラクティス）：このポリシーは、インターネット宛てのDNSクエリがトンネル経由で送信されるのを防ぎます。トンネル経由でUmbrellaリゾルバ(208.67.222.222,208.67.220.220)にDNSクエリを送信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。

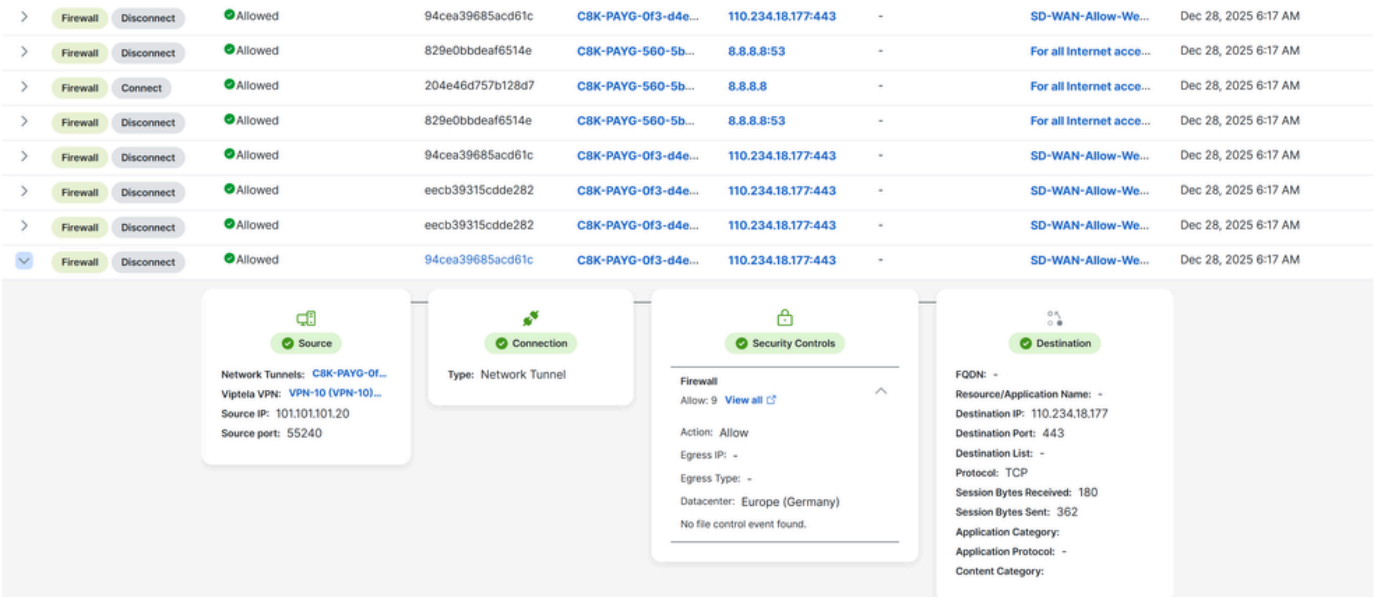
セキュアアクセス – アクティビティ検索

Monitor > Activity Searchの順に移動します。



セキュアなアクセス：イベント

Monitor > Eventsの順に移動します。

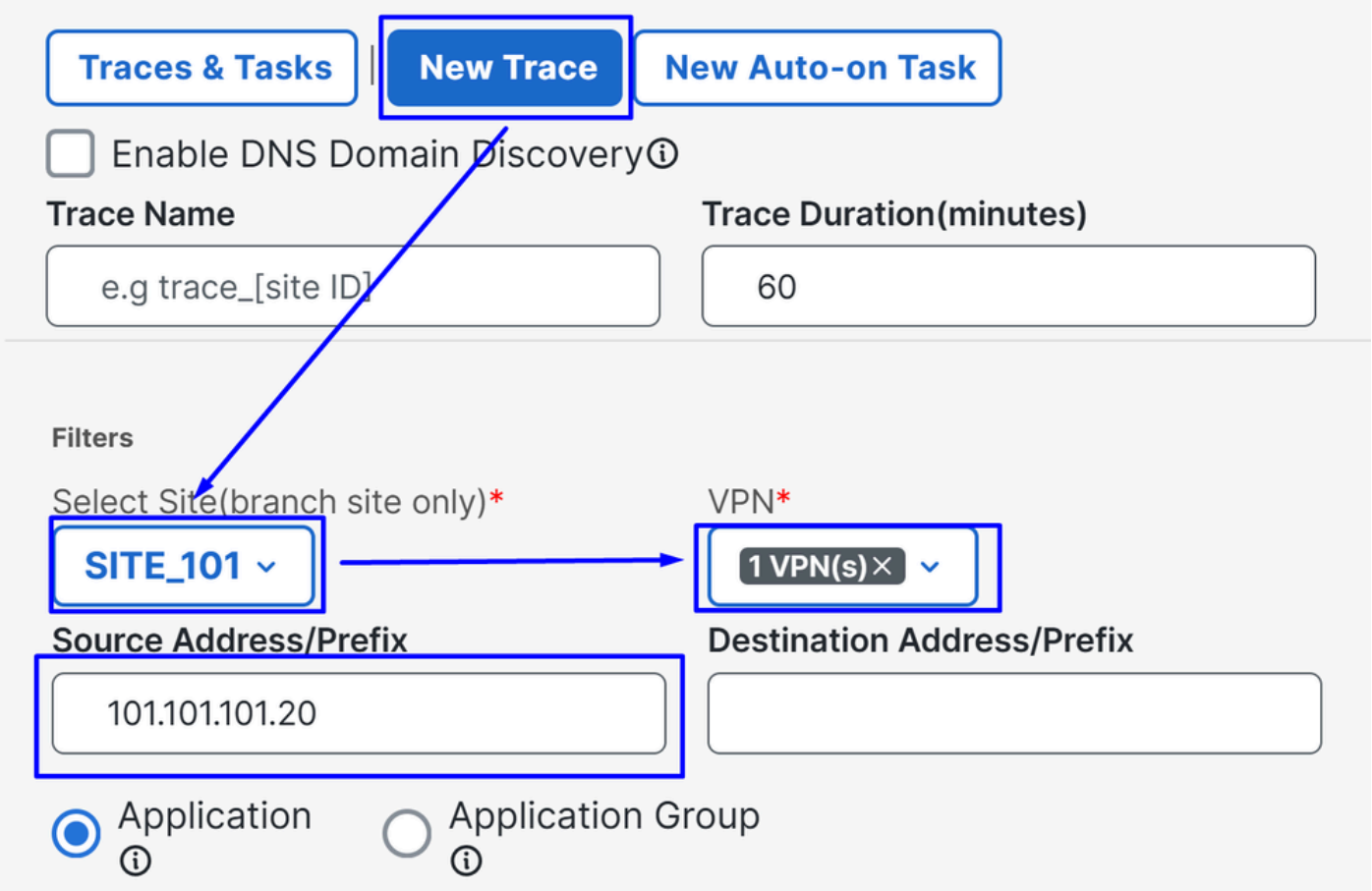


注：ロギングが有効（デフォルトでは無効）になっているデフォルトポリシーがあることを確認してください。

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

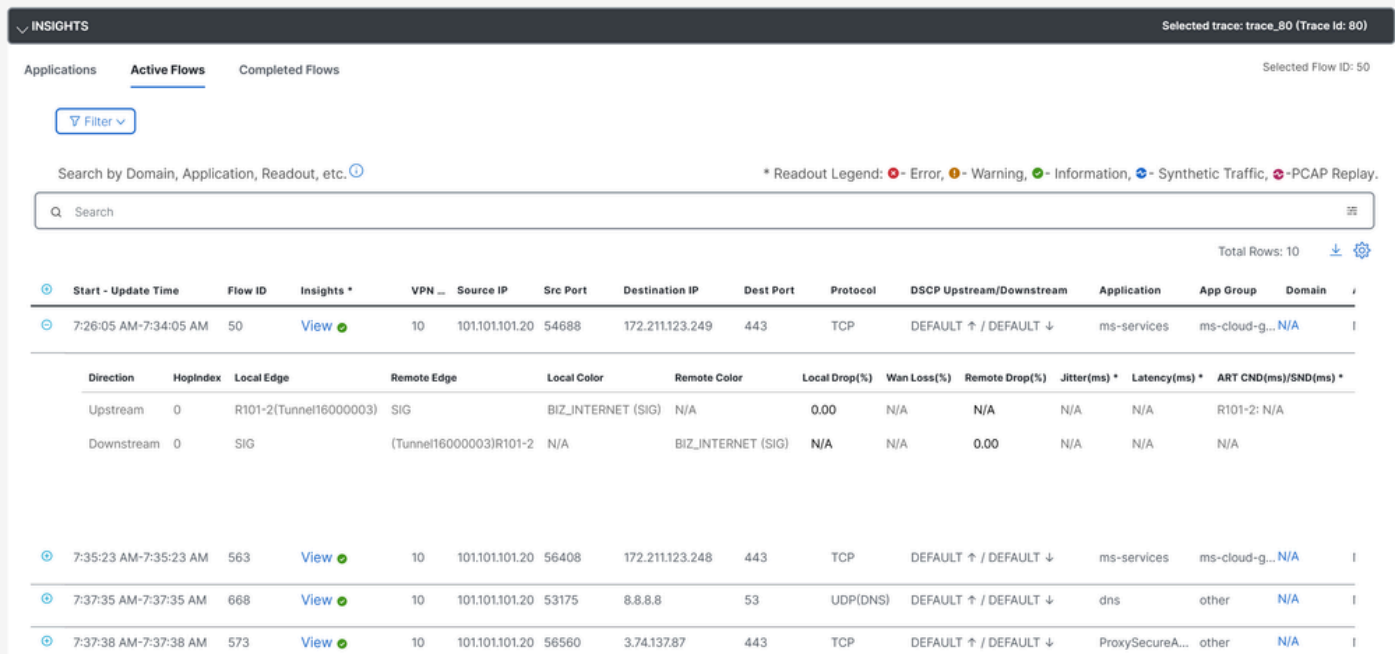
Catalyst SD-WAN Managerに移動します。

- 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。



- 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。



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。