セキュアプライベートアクセスのためのCatalyst 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、セキュアプライベートアクセスのためのCatalyst 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。

バックグラウンド情報

組織が従来の境界ベースのネットワークを越えて移動するにつれて、プライベートリソースへの安全なアクセスは、インターネットトラフィックのセキュリティ保護と同様に重要になります。アプリケーションは単一のデータセンターに限定されなくなり、現在ではオンプレミス環境、パブリッククラウド、ハイブリッドアーキテクチャにまたがって使用されています。この変化に対応するには、プライベートアクセスに対してより柔軟で現代的なアプローチが必要です。

ここで、SASEベースのアーキテクチャとCisco Secure Accessが関係します。従来のVPNコンセントレータやフラットネットワークアクセスに依存するのではなく、Cisco Secure Accessは、VPN-as-a-Service(VPNaaS)とZero Trust Network Access(ZTNA)を組み合わせて、プライベート接続をクラウド配信サービスとして提供します。

ネットワークレベルのプライベートアクセスでは、Cisco Secure Accessは自動化されたサイト間IPsecトンネルを使用してSD-WANと統合されます。これらのトンネルを使用すると、セキュリティインスペクションとポリシー適用をクラウド内で一元化した状態を維持しながら、プライベートトラフィックをセキュアアクセスとオンプレミスまたはクラウドネットワークの間で安全に流すことができます。運用の観点から見ると、これにより従来のVPNヘッドエンドを導入して維持する必要がなくなり、環境の拡大に伴う拡張が簡素化されます。

VPNaaSモデルでは、セキュアアクセスはクラウド内のVPNターミネーションポイントとして機能します。SD-WANは、Secure Accessを使用してインテリジェントなルーティングと復元力を処理し、プライベートリソースに到達する前にトラフィックが一貫したセキュリティポリシーによって保護および制御されるようにします。

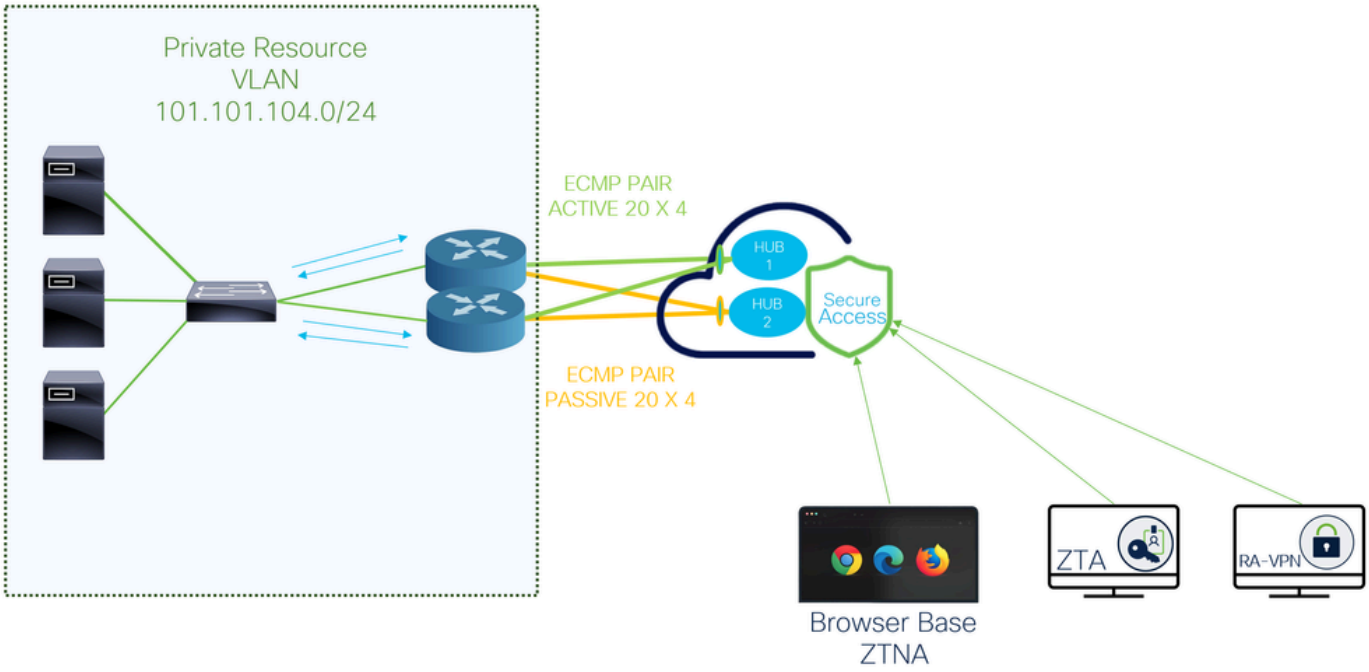
Cisco Secure Accessは、マルチリージョナルバックホールなど、高度なサイト間トンネルアーキテクチャもサポートします。この機能により、組織は複数のセキュアアクセス領域へのトンネルを同時に確立でき、地理的な冗長性とより高いアベイラビリティを提供できます。異なるリージョンに接続することにより、リージョンの停止、遅延の悪化、またはメンテナンスイベントが発生した場合に、トラフィックが自動的にフェールオーバーする可能性があります。

たとえば、組織はSD-WAN環境からロンドンとドイツのSecure Accessリージョンへのサイト間トンネルを確立できます。両方のトンネルがアクティブなままで、リージョン間の復元力のあるプライベートアクセスを可能にし、1つのリージョンが使用不能になっても継続性を確保します。このマルチリージョン設計により、ハイアベイラビリティが強化され、耐障害性が向上し、エンタープライズグレードの耐障害性要件に対応できます。

より詳細なアクセスについては、Cisco Secure AccessではZero Trust Network Access(ZTNA)モデルが適用されます。ユーザに広範なネットワーク接続を許可する代わりに、ZTNAでは、ID、デバイスポスチャ、コンテキストに基づいて、特定のアプリケーションへのアクセスのみが許可されます。このアプローチは、攻撃対象領域を大幅に縮小し、ゼロトラストの原則に沿っています。

ZTNAアクセスは、サイト間トンネルとリソースコネクタの組み合わせによって有効になります。リソースコネクタは、セキュアアクセスへのアウトバウンド専用接続を確立する軽量の仮想アプライアンスです。つまり、プライベートリソースをインターネットに直接公開する必要はありません。

ネットワーク図



前提条件

要 件

- セキュアアクセスの知識
- Cisco Catalyst SD-WAN Managerリリース20.18.2およびCisco IOS XE Catalyst SD-WANリリース17.18.2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

- この統合は制御されたアベイラビリティに基づいているため、TACケースを提出して、Cisco Secure Accessでこの機能を有効にするように依頼する必要があります

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20.18.2およびCisco IOS XE Catalyst SD-WANリリース17.18.2
- 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たものです。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

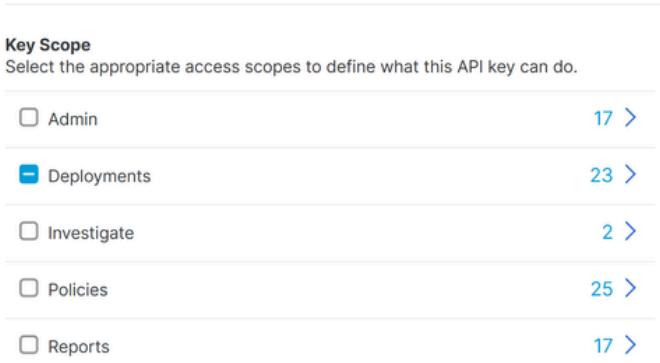
セキュアアクセスの設定

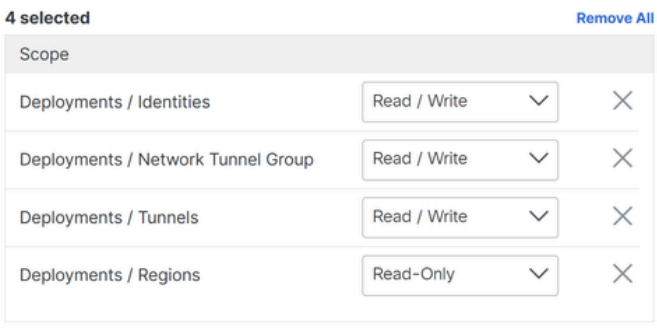
APIの作成

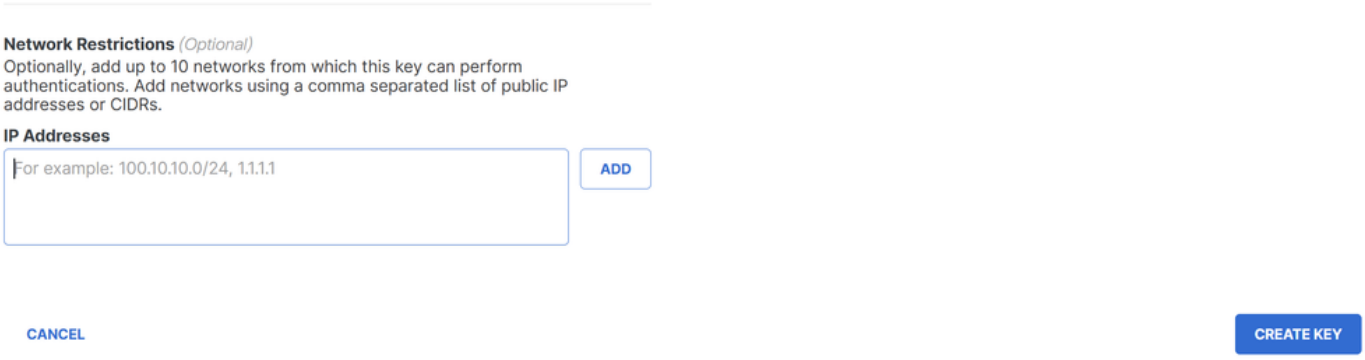
セキュアアクセスを使用して自動トンネルを作成するには、次の手順を確認します。

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

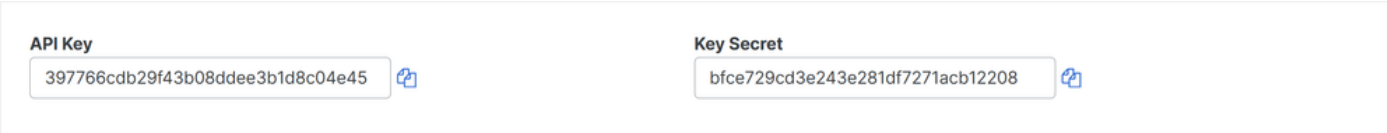






注：オプションで、このキーが認証を実行できるネットワークを10個まで追加できます。パブリックIPアドレスまたはCIDRのカンマ区切りリストを使用してネットワークを追加します。

- 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。

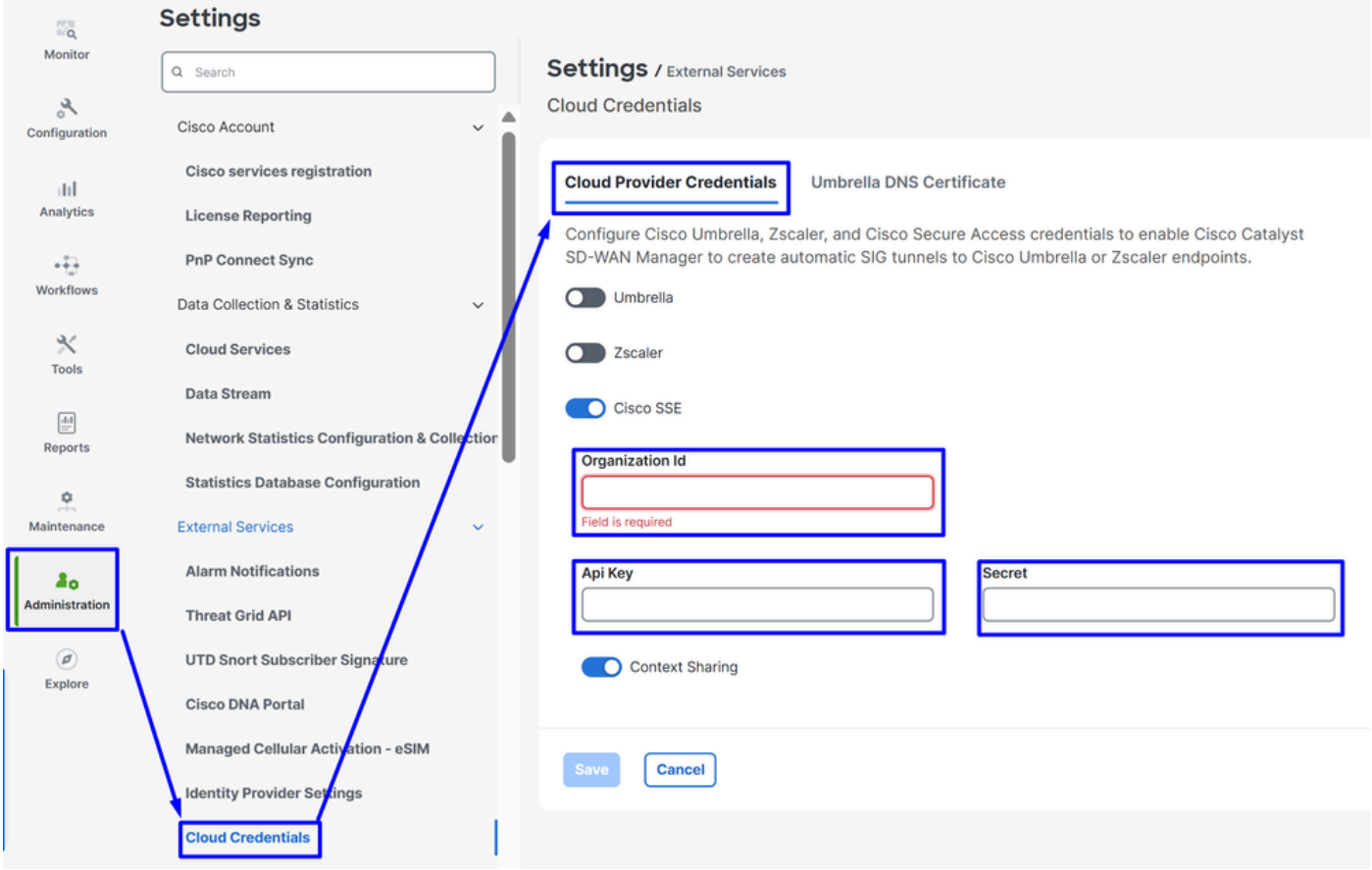
次に、ACCEPT AND CLOSEをクリックして完了します。

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



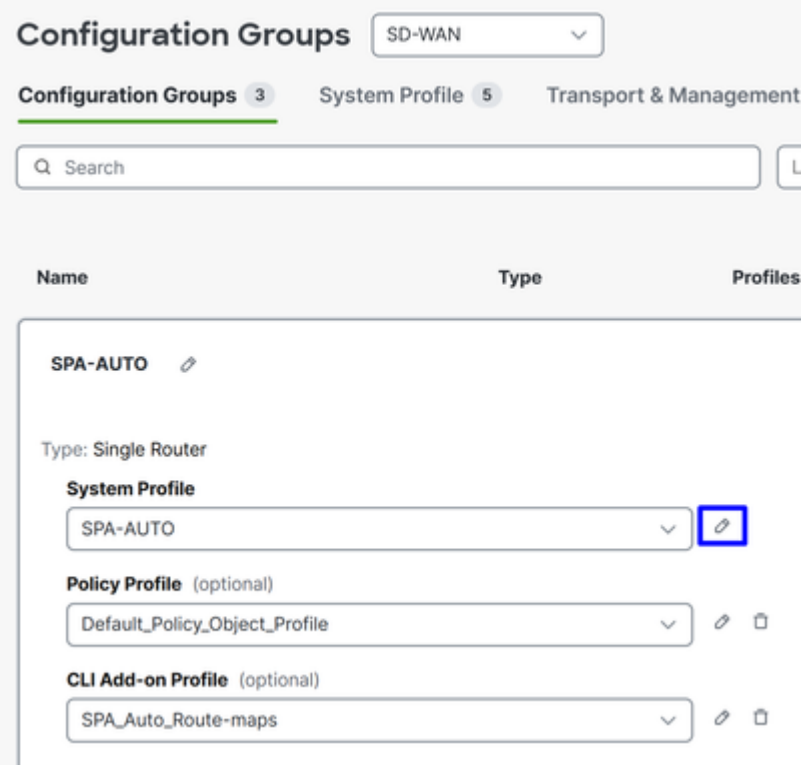
- 組織ID:SSEダッシュボードのURL(https://dashboard.sse.cisco.com/org/xxxxx)から取得できます。
- Apiキー:セキュアアクセス設定の手順からコピーします。
- 秘密：セキュアアクセス設定の手順からコピーします。

その後、Saveボタンをクリックします。

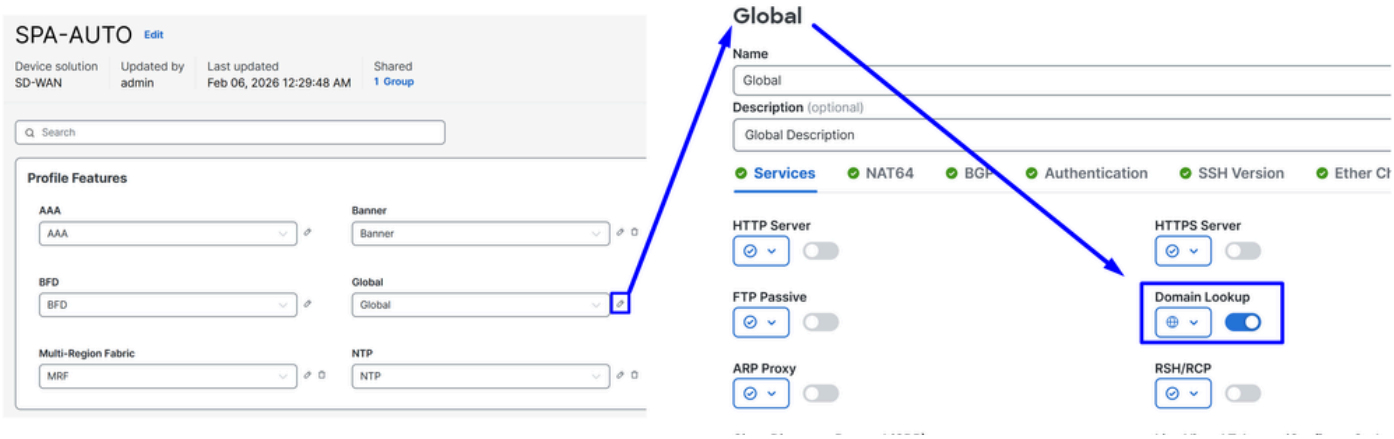
注：次の手順に進む前に、SD-WAN ManagerとCatalyst SD-WANエッジにDNS解決とインターネットアクセスがあることを確認する必要があります。

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。



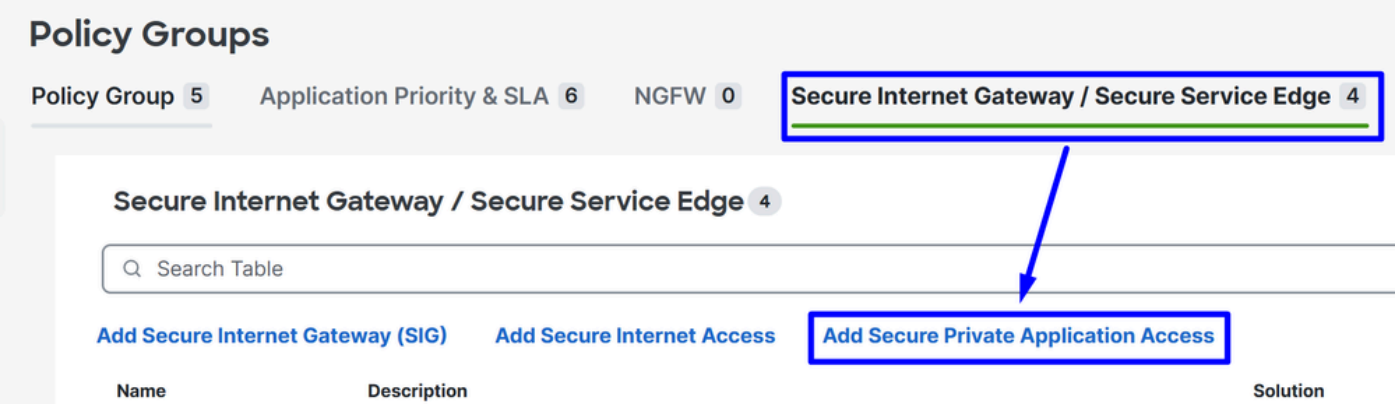
- 次に、Globalオプションを編集して、Domain Resolutionオプションが有効になっていることを確認します



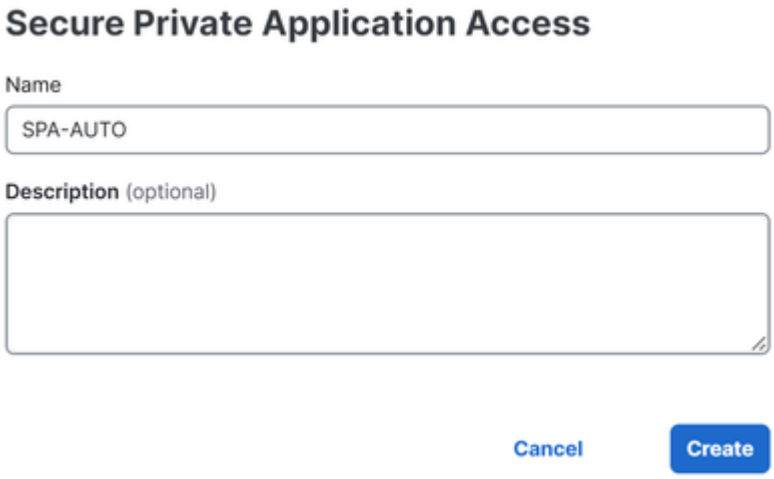
ポリシーグループの設定

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

- Secure Internet Gateway / Secure Service Edge>Add Secure Private Accessをクリックします。



- 名前を設定して、Createをクリックします。

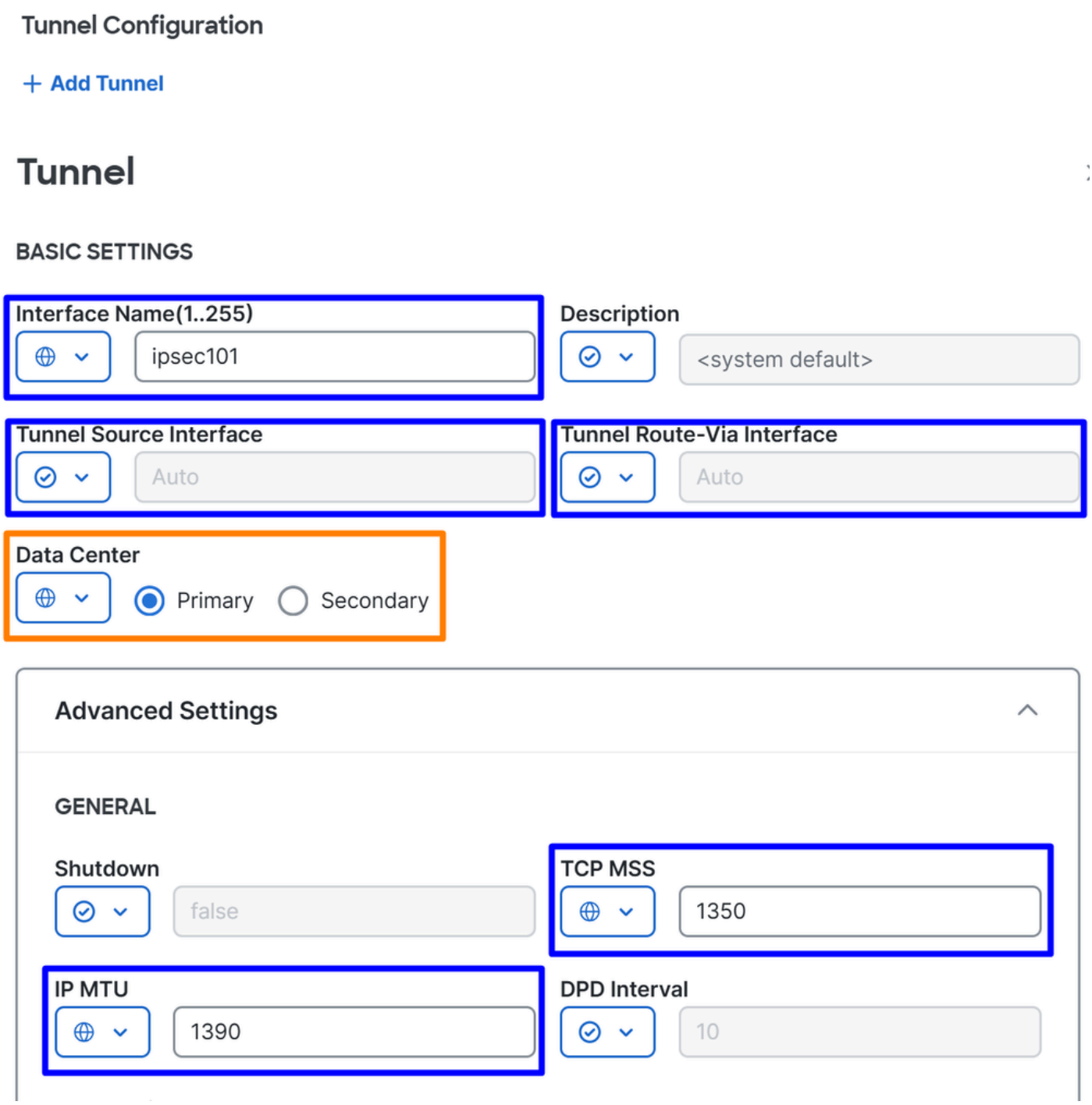


次の設定では、Catalyst SD-WANエッジに設定を展開した後にトンネルを作成できます。

- コンフィギュレーション
  - セグメント(VPN)：セキュアアクセスを介してアクセスされるアプリケーションをホストするVRFを選択します。
  - Cisco Secure Access Region：アプリケーションがホストされているSD-WANハブまたはブランチに最も近いリージョンを選択します。

次に、トンネル設定を定義します。プライマリセキュアアクセスデータセンターに作成されたトンネルはアクティブですが、セカンダリセキュアアクセスデータセンターに作成されたトンネルはバックアップとして動作します。

Tunnel Configurationの下で、+ Add Tunnelをクリックします。



- Tunnel（トンネル）
  - Interface Name:トンネル名を指定します。新しいトンネルが追加されるたびに自動的に更新されます。
  - トンネル送信元インターフェイス:この設定を変更する必要はありません。Autoのままにすると、ループバックインターフェイスが/31マスクで自動的に作成されます。
  - トンネルRoute-Viaインターフェイス:この設定を変更する必要はありません。デフォルトでは、エッジルータの最初のNAT適用物理WANインターフェイスが使用されますが、特定のWANインターフェイスが必要な場合は変更できます
  - データセンター:必要に応じて、プライマリまたはセカンダリを選択します。プライマリトンネルがすでに設定されている場合、Secondaryを選択します。通常のシナリオでは、1つのトンネルをプライマリとして、別のトンネルをセカンダリとして設定できます
  - 高度な設定

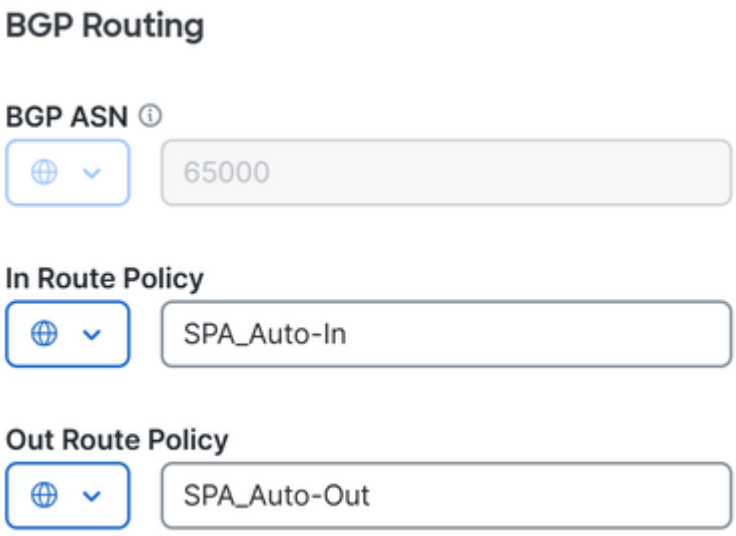
- IP MTU:1390を使用
- TCP MSS:1350を使用

注：複数のトンネルを作成してECMPを有効にし、トンネル容量を増やす場合は、ルータごとに最大10個のアクティブ/10個のバックアップトンネルを設定できます。これにより、NTGあたり最大10 × 4 Gbpsが提供されます。

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action	
ipsec101		Auto	Auto	Primary		
ipsec102		Auto	Auto	Secondary		
ipsec103		Auto	Auto	Primary		
ipsec104		Auto	Auto	Secondary		
ipsec105		Auto	Auto	Primary		
ipsec106		Auto	Auto	Secondary		
ipsec107		Auto	Auto	Primary		
ipsec108		Auto	Auto	Secondary		
ipsec109		Auto	Auto	Primary		MAXIMUM OF 10 TUNNELS PER HUB
ipsec110		Auto	Auto	Secondary		10 x 1 Primary
ipsec111		Auto	Auto	Primary		10 x 1 Secondary
ipsec112		Auto	Auto	Secondary		
ipsec113		Auto	Auto	Primary		
ipsec114		Auto	Auto	Secondary		
ipsec115		Auto	Auto	Primary		
ipsec116		Auto	Auto	Secondary		
ipsec117		Auto	Auto	Primary		
ipsec118		Auto	Auto	Secondary		
ipsec119		Auto	Auto	Primary		
ipsec120		Auto	Auto	Secondary		

注：ルータごとに複数のトンネルを展開する場合は、トランスポートインターフェイスで、結合されたすべてのアクティブなトンネルの集約帯域幅を維持できることを確認してください。たとえば、2つのトンネルがそれぞれ最大1 Gbpsを伝送すると想定される場合、トランスポートリンクは少なくとも2 Gbpsのスループットをサポートする必要があります。

トンネルを設定したら、BGPの設定に進みます。



- **BGP**ルーティング
  - BGP ASN:SD-WANハブのAS番号を指定します。AS 64512はセキュアアクセス用に予約されているため、使用できません。BGPの詳細については、を参照してください。
  - ルートポリシー内:ルーティングの問題を防ぐために、システムは自動的にdeny allステートメントを使用してこの着信ルートポリシーを作成します。適切なルートを許可/拒否するには、CLIアドオンテンプレートを使用して手動で変更する必要があります。
  - 発信ルートポリシー:ルーティングの問題を回避するため、システムはdeny all文を使用してこの発信ルートポリシーを作成します。 適切なルートを許可/拒否するには、CLIアドオンテンプレートを使用して手動で編集する必要があります。

警告:2025年11月以降、新しく作成されたすべてのセキュアアクセス組織では、ネットワークトンネルグループのBGPピアリングにデフォルトでパブリックASN 32644が使用されます。2025年11月より前に設立された既存の組織は、以前はSecure Access BGPピア用に予約されていたプライベートASN 64512を引き続き使用します。プライベートAS番号64512がネットワーク上のデバイスに割り当てられている場合、ピア（セキュアアクセス）BGP AS 64512用に設定されたネットワークトンネルグループとピアリングできません。

ポリシーグループに新しいポリシーを導入した後、各BGPネイバーに対して次のBGPおよびroute-map設定が自動的に作成されます。

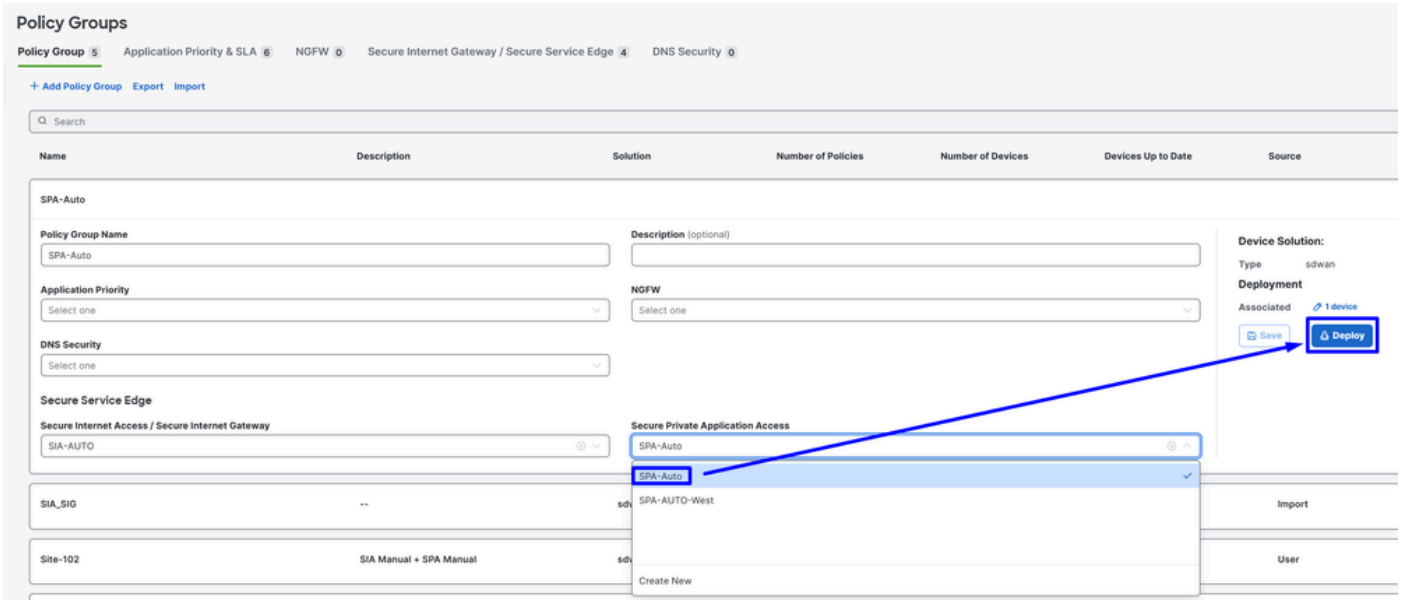
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

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
```

その後、Saveをクリックし、ポリシーの導入を続行してトンネルを起動します。

- Configuration > Policy Groupsの順にクリックします。
- Policy > Secure Service Edge > Secure Private Application Accessの順に選択し、SPA用に作成した最新のプロファイルをクリックします。
- Deployをクリックして完了します



inSecure Accessを確認するには、次の手順を実行します。

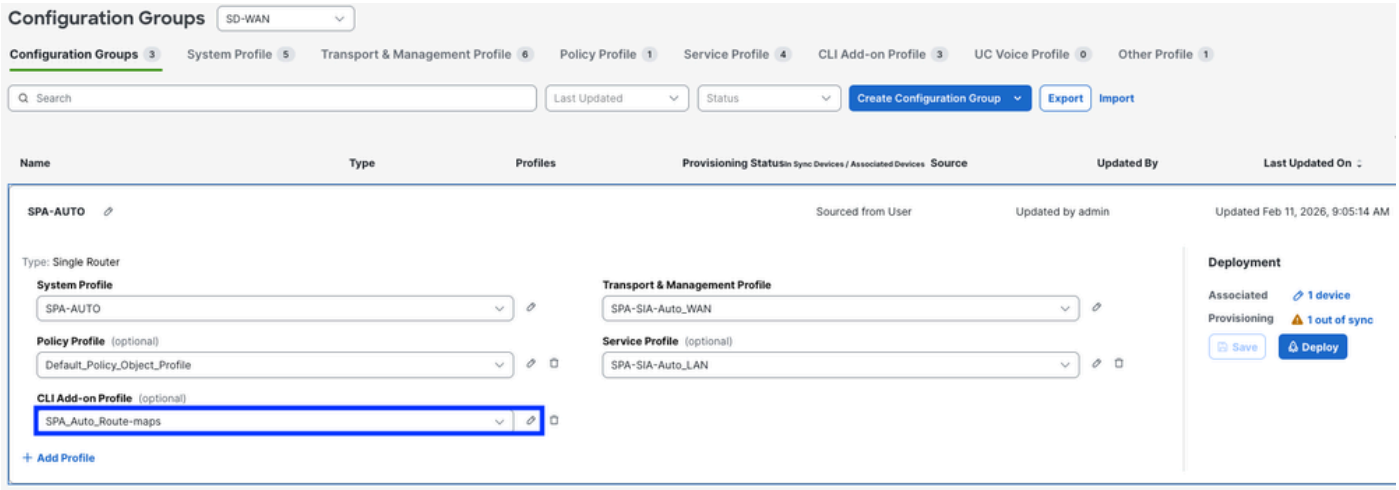
- Connect> Network Connectionsの順にクリックします。

トンネルの確立

ルーティングの設定

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

- 設定グループをクリックし、CLIアドオンプロファイルを作成/編集します。



BGPルート交換を許可するには、事前に設定したIn Route Policyと**Out Route Policy**を使用します。 CLIアドオンルート設定の基本的な例を紹介しています。このテンプレートは出発点となるもので、必要に応じてカスタマイズする必要があります。

```
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
```

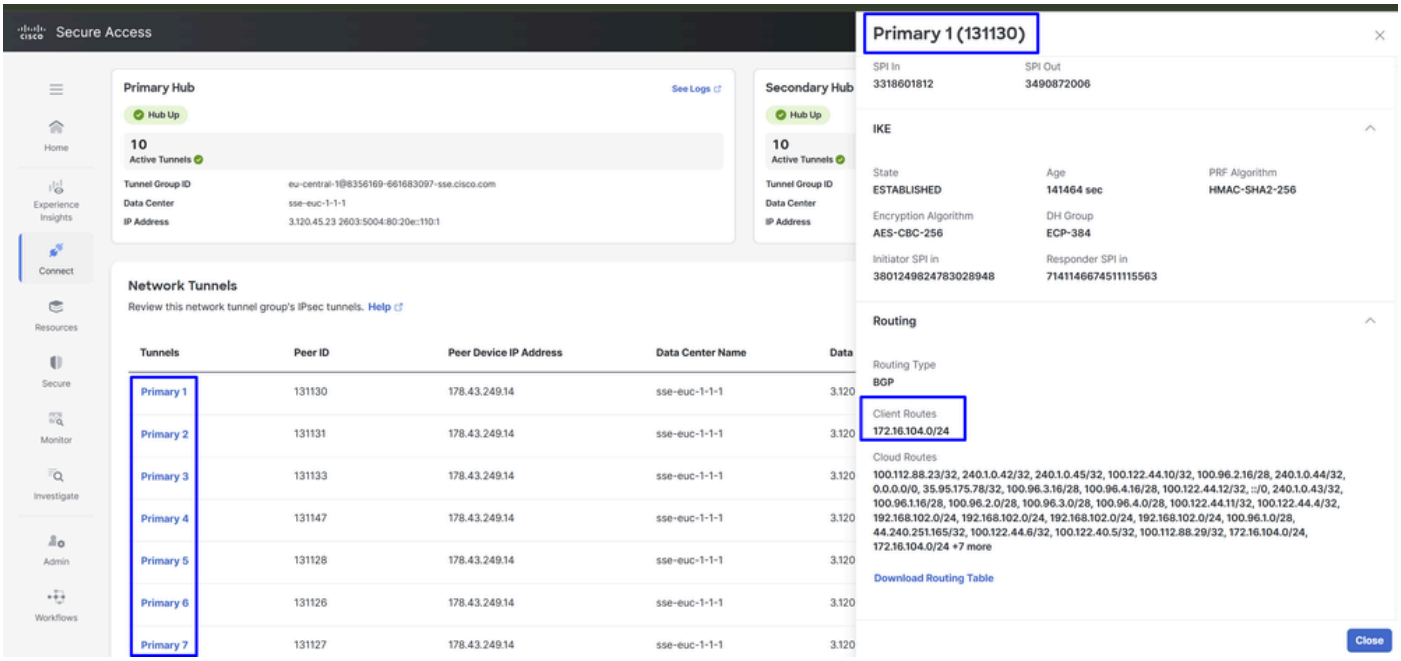
警告:BGPルートマップを介した送受信が許可されるネットワークを定義する際には、慎重な計画が必要です。上記の例に示すとおり、すべてのルートを許可すると、意図しないルーティング動作が引き起こされる可能性があります。最適な導入のためには、ルートマップで必要なネットワークのみを明示的に指定し、ルーティングの結果を制御して予測可能にします

これで、「変更の導入」に進むことができます

BGPルートがSecure Accessで受信されているかどうかを確認するには、次の手順を確認します。

- Connect> Network Connections > Network Tunnel Groupsの順にクリックして、NTG名を選択します

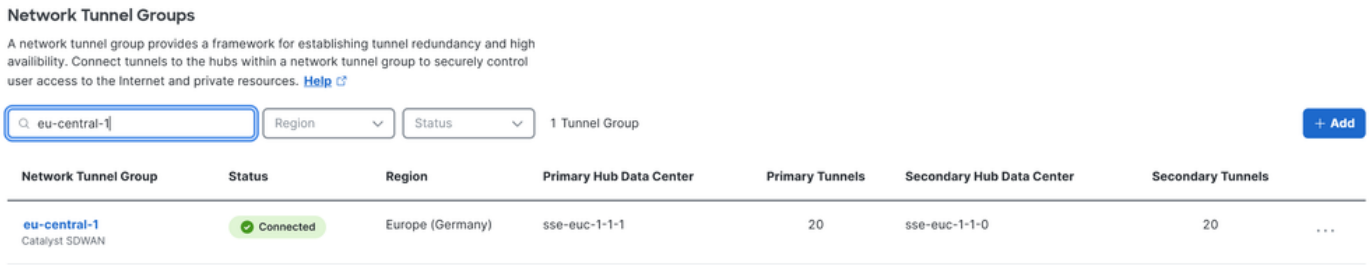
ルーティングの確立



注：この例では、企業ユーザサブネット172.16.104.0/24が、BGPを介したセキュアアクセスにアドバタイズされています。これにより、Catalyst SD-WANとSSE環境の間で適切なルーティングが可能になります。

Catalyst SD-WANハブの両方のWANエッジに同じポリシーを適用できるため、アクティブなトンネルは20個、スタンバイのトンネルは20個になります。トンネルの合計数は、各エッジに設定されている数によって異なります。両方のセキュアアクセスハブ（ハブ1とハブ2）に接続されたルータは、確立されたすべてのトンネルでECMPペアを形成します。

たとえば、Catalyst SD-WAN Edge 1に10のトンネルがあり、Catalyst SD-WAN Edge 2に10のトンネルがある場合、セキュアアクセスは20のアクティブなトンネルにわたってECMPを形成します。同じ動作がセカンダリSSEハブにも適用されます。

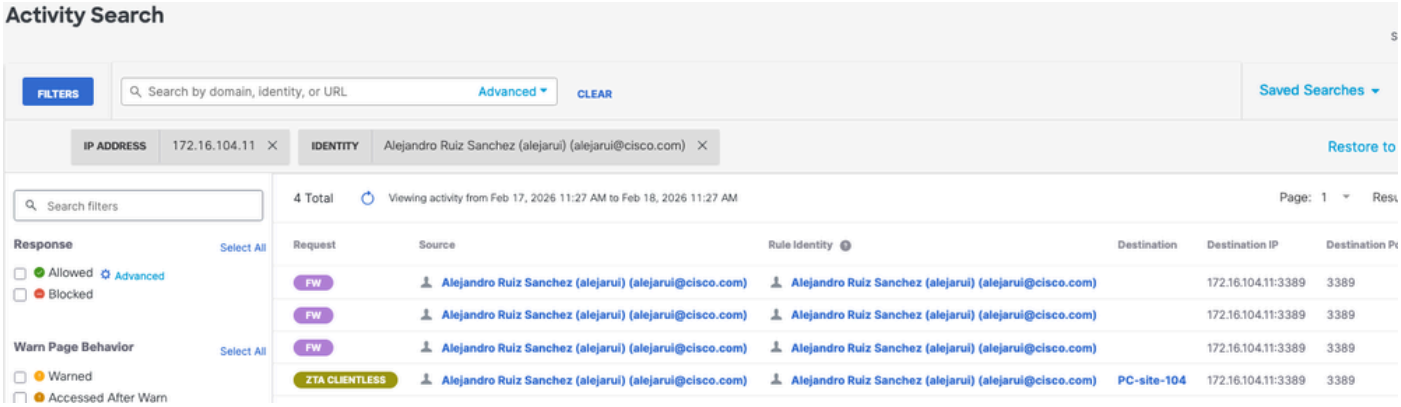


確認

トラフィックがCisco Secure Accessを通過しているかどうかを確認するには、Eventsor Activity SearchまたはNetwork-Wide Path Inspectingに移動し、トンネルIDでフィルタリングします。

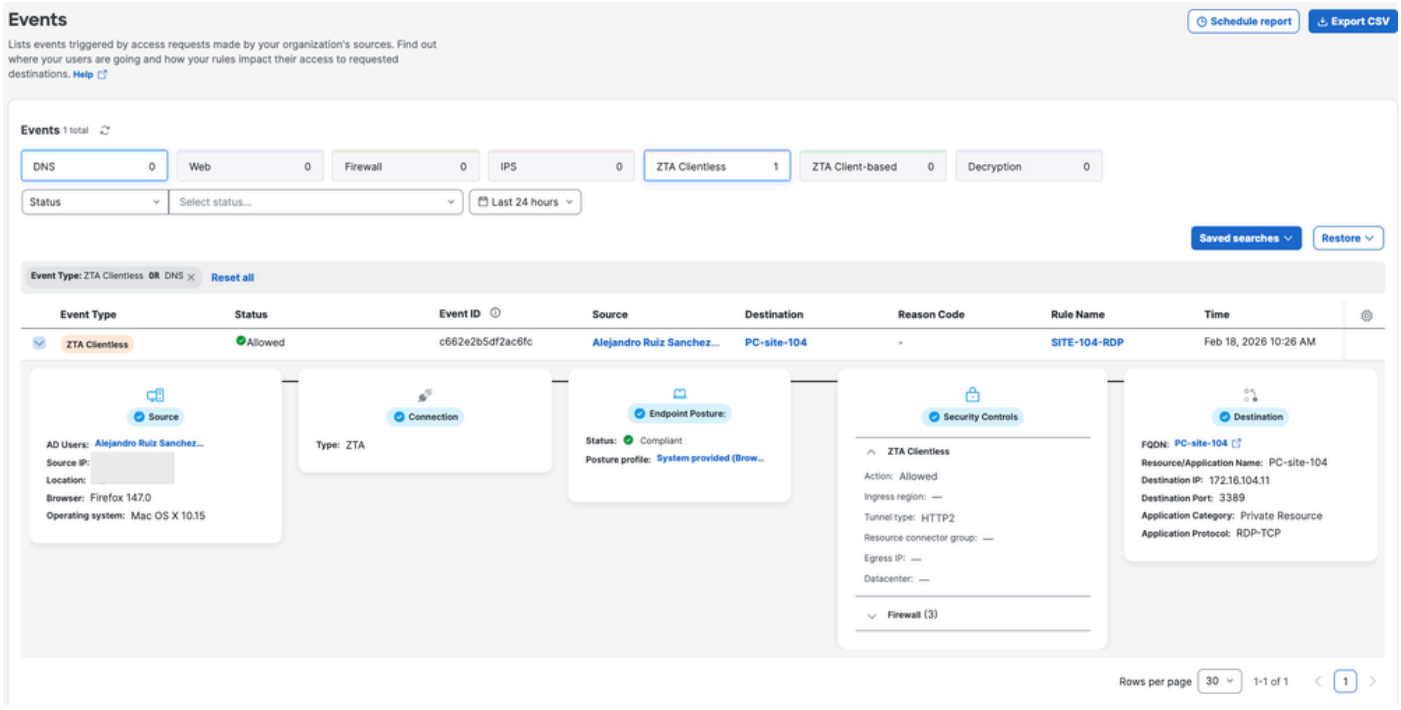
セキュアアクセス – アクティビティ検索

Monitor>Activity Search :



セキュアなアクセス：イベント

Monitor>Eventsの順に移動します。

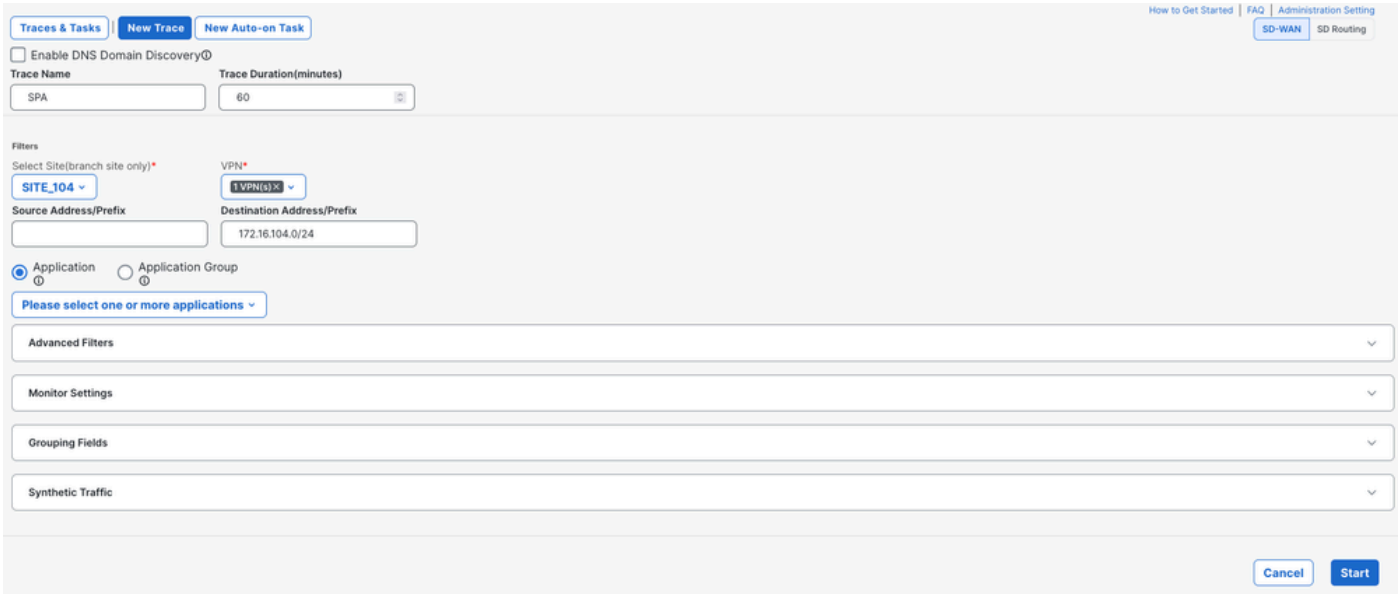


注：ロギングが有効（デフォルトでは無効）になっているデフォルトポリシーがあることを確認してください。

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。

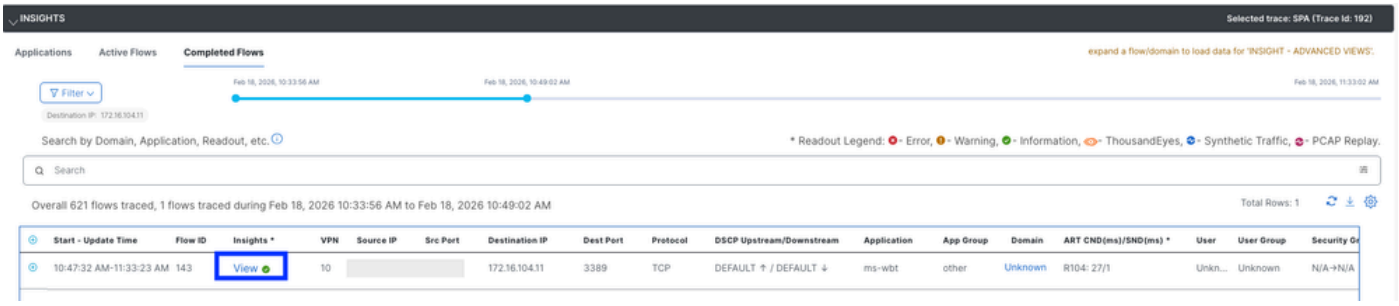
- Tools> Network-Wide Path Insightsをクリックします。
- New Traceをクリックします。



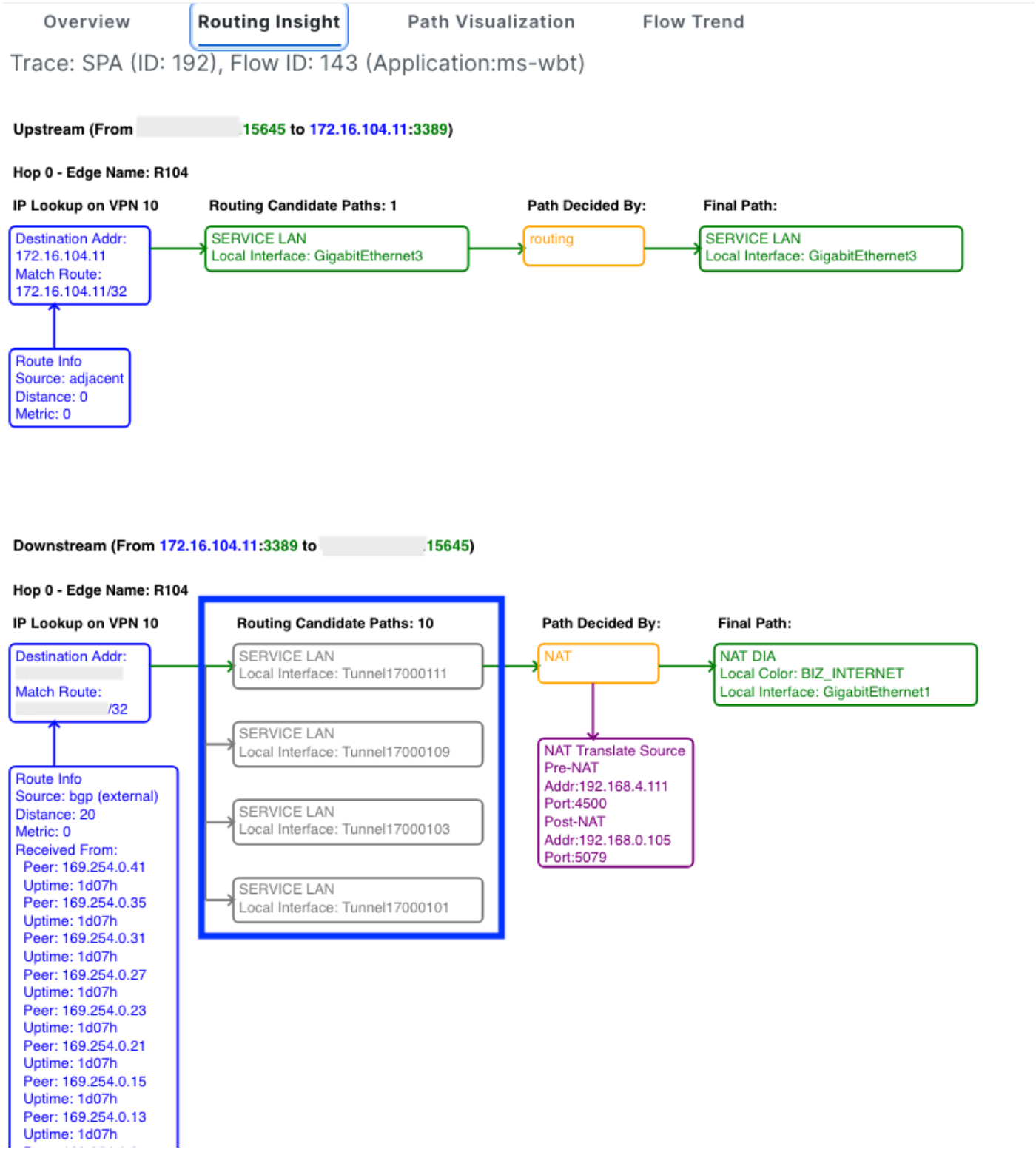
- トレース名:（オプション）トレース名を指定します
- サイト：プライベートリソースがあるサイトを選択します
- VPN：プライベートリソースがあるVPN IDを選択します
- 送信元/宛先アドレス:（オプション）IPを入力するか、空白のままにして、サイトおよびVPNchoosenに基づいてフィルタリングされたすべてのトラフィックをキャプチャします

トレースの開始

トラフィックフローを探し、Insights列にあるViewをクリックします



routing Insights列には、候補パスと、セキュアアクセスへのIPSecトンネルが表示されます



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
- 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

- 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。