Revised: October 22, 2024

SD ルーティングデバイスの Secure Access の設定

Cisco Secure Access とは

Cisco Secure Access は、クラウドから提供されるネットワーク セキュリティ サービスを統合してハイブリッドワーク環境を接続するクラウド セキュリティ サービス エッジ（SSE）ソリューションです。このソリューションは、シームレスで透過的でセキュアなダイレクト インターネット アクセス（DIA）を提供し、ユーザーがあらゆるものからあらゆる場所に接続できるようにします。

Cisco IOS XE 17.14.1a では、Cisco SSE は、SD ルーティングデバイスが IPSec トンネルを使用して SSE プロバイダーに接続する機能を提供します。

機能	リリース情報	Description
Cisco Secure Access の設定	Cisco IOS XE リリース 17.14.1a	Cisco Secure Access は、シームレスで透的な、セキュアなダイレクトインターネト アクセス（DIA）を提供するクラウドセキュリティ サービス エッジ（SSE）リューションです。 このソリューションは、Cisco SD-WAN Managerのポリシーグループを使用して定できます。

機能制限

- Cisco Secure Access は API スロットリングをサポートしていません
- CiscoSecure Access を Cisco SD-Routing と統合した後、Cisco Secure Access ダッシュボードでネットワーク トンネル グループ名に変更を加えた場合、Cisco SD-WAN Manager に反映されません

Cisco Secure Access を設定するためのワークフロー

このワークフローでは、Cisco Secure Access のセットアップに必要な手順の概要を示します。手順の詳細については、次のセクションを参照してください。

タスク	説明
Cisco Secure Access ポータルでの事前設定	

タスク	説明
ポータルでログイン情報を確認し、APIログイン情報に書き込みアクセス権があることを確認します。	**[Admin]** > **[Management]** > **[API Keys]**に移動し、API キーを生成および管理します。 トンネルグループとトンネルの作成への書き込みアクセス権があることを確認します。このアクセス権により、SD-WAN Managerを使用してトンネルが設定および展開された後、Cisco Secure Access と SD-Routing デバイス間のシームレスな接続が保証されます。
Cisco SD-WAN Manager の事前設定	
設定グループを作成し、SD ルーティングデバイスに割り当てていることを確認します。	設定グループに移動
SD-WAN Manager で使用可能な CLI テンプレートを使用して、以下を設定します。	[Configuration Groups] に移動し、SD ルーティング設定グループを選択し、[Edit] をクリックして、対応する [CLI Profile] ダイアログボックスを選択します。[Add Feature Profile] ウィンドウで、[Create New] を選択し、名前と説明を入力してから、[CLI Configuration] セクションにコマンドを入力します。保存して、この機能パーセルを追加します。
• SDルーティングデバイスのDNS設定を確認します。	これにより、デバイスが DNS サーバーと対話できるようになります。 HTTPS に接続してパブリック IP アドレスを取得するデバイスに DNS サーバーを設定できます。HTTPS の送信元インターフェイスを設定するには、Cisco SD-WAN Manager で **ip http client source-interface** *name and number of the interface* コマンドを使用します。

• WAN および LAN インターフェイス（外部/内部）で NAT が有効になっていることを確認します。	これにより、情報をインターネットに転送する前に、ローカルネットワーク内の複数のプライベートアドレスがパブリック IP アドレスにマッピングされます。たとえば、*access-list nat acl1* に一致するパケットのすべての送信元アドレスは、ルータを出るときに *Loopback 1* の IP アドレスに変換されます。
	`ip nat inside source list wan-acl1 interface GigabitEthernet2 overload`
	または
	`ip nat inside source list nat_acl1 interface Loopback1 overload`

デバイスのドメインルックアップを有効にする	**[Configuration Groups]** > **[System Profile]** > **[Global]**に移動し、[Global Lookup] を有効にします。

タスク	説明
Cisco SD-WAN Manager での SSE 関連の設定	
クラウドプロバイダーのログイン情報の設定	**[Administration]** > **[Settings]** > **[Cloud Provider Credentials]** > **[Cisco SSE]**に移動します。
送信元インターフェイスアドレスの設定	**[Configuration]** > **[Configuration Groups]**に移動します。
ポリシーグループを使用した SSE ポリシーの作成	**[Configuration]** > **[Policy Groups]** > **[Secure Internet Gateway/Secure Service Edge]**に移動します。
トラフィックリダイレクトの設定	これを設定すると、SSE トンネルを介してトラフィックをリダイレクトするサービスルートが作成されます。 [Configuration Groups] に移動し、SD ルーティング設定グループを選択し、[Edit] をクリックして、対応する [CLI Profile] ダイアログボックスを選択します。[Add Feature Profile] ウィンドウで、[Create New] を選択し、名前と説明を入力してから、[CLI Configuration] セクションにコマンドを入力します。保存して、この機能パーセルを追加します。
SSE ポリシーとポリシーグループの関連付け	**[Configuration]** > **[Policy Groups]** > **[Add Policy Group]**に移動し、以前に作成した SSE ポリシーを選択し、[Save] をクリックして SSE ポリシーをポリシーグループに関連付けます。 次に、このポリシーグループをデバイスに関連付けて展開します。
SSE 設定の確認	設定を確認します。
SSE トンネルのモニタリング	**[Monitor]** > **[Audit Logs]** SSE トンネルの**[Monitor]** > **[Security]** **[Monitor]** > **[Tunnels]** > **[SSE Tunnels]**

クラウドプロバイダーのログイン情報の設定

Cisco SSE への自動トンネルプロビジョニングのために Cisco SD-WAN Manager を有効にするためのログイン情報を設定します。

Step 1 **[Administration]** > **[Settings]** > **[Cloud Credentials]** > **[Cloud Provider Credentials]**をクリックして [Cisco Secure Access] を有効にし、次の詳細を入力します。これらのログイン情報はセッションの認証を開始するために使用され、その後のセッションでも使用されます。

フィールド	説明
Organization ID	組織の Cisco Secure Access 組織 ID。
API Key	Cisco Secure Access API キー。
秘密	Cisco Secure Access API シークレット。

Step 2 これらの詳細を保存します。

送信元インターフェイスとしてのループバック インターフェイスの設定

ループバック インターフェイスを送信元として設定します。このループバック インターフェイスはどのインターフェイスにも関連付けられていないため、接続が中断されるリスクはありません。

CLI テンプレートに次のコマンドを追加します。

```
interface loopback1
no shutdown
ip nat inside
ip address 1.1.1.1 255.255.255.255
```

ポリシーグループを使用した SSE ポリシーの作成

始める前に

SSE ログイン情報が作成されていることを確認します。SD-WAN Manager でこれを行うには、**[Administration]** > **[Settings]** > **[Cloud Provider Credentials]** > **[Cisco SSE]**に移動し、詳細を入力します。

Step 1 SD-WAN Manager で、**[Configuration]** > **[Policy Groups]** > **[Secure Internet Gateway/Secure Service Edge]**に移動します。[Add Secure Service Edge (SSE)] をクリックします。

Step 2 SSE ポリシーの名前を入力し、ソリューションタイプとして **sd-routing** を指定して、[Create] をクリックします。

Step 3 トラッカーを作成します。自動トンネルの作成中に、Cisco SD-WAN Managerは、フェールオーバーパラメータのデフォルト値を使用してデフォルトのトラッカーエンドポイントを作成し、アタッチします。ただし、要件に合ったフェールオーバーパラメータを使用してカスタマイズされたトラッカーを作成することもできます。

a) [Source IP Address] フィールドに、送信元の IP アドレスをサブネットマスクとともに入力します。これは、予期しないネットワークドロップまたは遅延があるかどうかを検出するためにトラッカーエンドポイントに http プローブを送信するために使用され、vrf ID 65330 で使用されます。

b) [Add Tracker] をクリックします。[Add Tracker] ウィンドウで、次のように設定し、[Add] をクリックします。

表 *1*: トラッカーパラメータ

フィールド	説明
名前（**Name**）	トラッカーの名前。名前には 128 文字以内の英数字を使用できます。

フィールド	説明
[API URL of Endpoint]	トンネルの Secure Service Edge エンドポイントの API URL を指定します。 デフォルト：service.sig.umbrella.com
しきい値	設定されたエンドポイントがダウンしていることを宣言する前に、プローブが応答を返すまでの待機時間を入力します。 有効な範囲は 100 ～ 1000 ミリ秒で、デフォルトは 300 ミリ秒です。
プローブ間隔	設定されたエンドポイントのステータスを判断するためにプローブを送信する時間間隔を入力します。 指定できる範囲は 20 ～ 600 秒で、デフォルトは 60 秒です。
Multiplier（乗数）	トンネルがアップまたはダウンしていると判断する前にプローブを再送信する回数を入力します。 指定できる範囲は 1 ～ 10 で、デフォルトは 3 です。

Step 4 トンネルを作成します。[Configuration] をクリックします。

a) [Add Tunnel] をクリックします。

b) [Add Tunnel] ポップアップウィンドウの [Basic Settings] で、次のように設定し、[Add] をクリックします。

表 *2:* 基本設定

フィールド	説明
トンネル タイプ	Cisco Secure Access：（読み取り専用） **ipsec**
[Interface Name (1..255)]	インターフェイスの名前。
Description	インターフェイスの説明を入力します。
Tracker	デフォルトでは、トンネルの状態を監視するトラッカーがアタッチされています。
Tunnel Source Interface	トンネルの送信元インターフェイスの名前。このインターフェイスは出力インターフェイスである必要があります。通常はインターネット側のインターフェイスです。トンネル送信元インターフェイスはループバックをサポートします。目的に応じて、最大 16 のトンネル（8 つのアクティブ/8 つのバックアップ）を設定できます。
[Data-Center]	プライマリデータセンターの場合は [Primary] をクリックし、セカンダリデータセンターの場合は [Secondary] をクリックします。プライマリデータセンターへのトンネルはアクティブトンネルとして機能し、セカンダリデータセンターへのトンネルはバックアップトンネルとして機能します。

フィールド	説明
[Advanced Options]（オプション）	
Shutdown	オプションボタンをクリックしてこのオプションを有効にします。 デフォルト：無効
[Enable Tracker]	オプションボタンをクリックしてこのオプションを有効にします。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 2000 バイト デフォルト：1400 バイト
TCP MSS	TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし
DPD Interval	インターネット キー エクスチェンジ（IKE）が接続で Hello パケットを送信する間隔を指定します。 範囲：10 ～ 3600 秒 デフォルト：10
DPD Retries	ピアから Dead Peer Detection（DPD; デッドピア検出）再試行メッセージの応答がない場合に、DPD 再試行メッセージを送信する間隔を秒単位で指定します。 ピアが DPD メッセージに応答しなかった場合、ルータは状態を変更し、DPD 再試行メッセージを送信します。このメッセージは、より速い再試行間隔（DPD 再試行間の秒数）で送信されます。デフォルトで、DPD リトライ メッセージは 2 秒ごとに送信されます。5 回の DPD 再試行メッセージに応答がない場合、トンネルはダウンとしてマークされます。 範囲：2 ～ 60 秒 デフォルト：3
IKE	
[IKE Rekey Interval]	IKE キーを更新する間隔を指定します。 範囲：3600 ～ 1209600 秒（1 時間～ 14 日） デフォルト：14400 秒

フィールド	説明
IKE Cipher Suite	IKE キー交換中に使用する認証と暗号化のタイプを指定します。 次のいずれかを選択します。 • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 デフォルト：AES 256 CBC SHA1
IKE Diffie-Hellman Group	IKEv1 または IKEv2 のいずれかで、IKE キー交換で使用する Diffie-Hellman グループを指定します。
IPSec	
IPsec Rekey Interval	IPSec キーを更新する間隔を指定します。 範囲：3600 ～ 1209600 秒（1 時間～ 14 日） デフォルト：3600 秒
[IPsec Replay Window]	IPsec トンネルのリプレイウィンドウサイズを指定します。 オプション：64、128、256、512、1024、2048、4096 パケット。 デフォルト：512
IPsec Cipher Suite	IPsec トンネルで使用する認証と暗号化を指定します。 次のオプションがあります。 • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM デフォルト：AEM 256 GCM

フィールド	説明
Perfect Forward Secrecy	IPSec トンネルで使用する Perfect Forward Secrecy（PFS）設定を指定します。次の Diffie-Hellman 素数係数グループのいずれかを選択します。 • グループ 2 1024 ビット係数 • グループ 14 2048 ビット係数 • グループ 15 3072 ビット係数 • グループ 16 4096 ビット係数 • なし：PFS を無効にします

Step 5 高可用性の設定」を参照してください。アクティブトンネルとバックアップトンネルを指定して、トンネル間でトラフィックを分散するには、[High Availability] をクリックして、次の手順を実行します。

a) [Add Interface Pair] をクリックします。[Add Interface Pair] ポップアップウィンドウで、次のように設定します。

b) [Add] をクリックして設定を保存します。

フィールド	説明
Active Interface	プライマリデータセンターに接続するトンネルを選択します。
[Active Interface Weight]	ロードバランシングの重み付け（重み付けの範囲：1～255）を入力します。 ロードバランシングは、複数のトンネル間でトラフィックを分散し、ネットワーク帯域幅を増やすのに役立ちます。両方のトンネルに同じ重み付けを入力すると、トンネル全体で ECMP ロードバランシングを実現できます。ただし、トンネルに高い重みを入力すると、そのトンネルのトラフィックフローの優先順位が高くなります。 たとえば、2 つのアクティブトンネルを設定する際、最初のトンネルの重み付けを 10 に設定し、2 番目のトンネルの重み付けを 20 に設定すると、トラフィックはトンネル間で10：20の比率で負荷分散されます。
バックアップ インターフェイス	バックアップトンネルを指定するには、セカンダリデータセンターに接続するトンネルを選択します。 バックアップトンネルの指定を省略するには、[None] を選択します。

フィールド	説明
[Backup Interface Weight]	ロードバランシングの重み付け（重み付けの範囲：1～255）を入力します。 ロードバランシングは、複数のトンネル間でトラフィックを分散し、ネットワーク帯域幅を増やすのに役立ちます。同じ重み付けを入力すると、トンネル全体でECMPロードバランシングを実現できます。ただし、トンネルに高い重みを入力すると、そのトンネルのトラフィックフローの優先順位が高くなります。 たとえば、2 つのバックアップトンネルを設定する際、最初のトンネルの重み付けを 10 に設定し、2 番目のトンネルの重み付けを 20 に設定すると、トラフィックはトンネル間で10：20の比率で負荷分散されます。

Step 6 [Region] の選択：リージョンを選択すると、プライマリリージョンとセカンダリリージョンのペアが選択されます。Cisco Secure Service Edge が提供するプライマリリージョンをドロップダウンリストから選択すると、Cisco SD-WAN Manager でセカンダリリージョンが自動的に選択されます。ユニキャスト IP アドレスを持つプライマリリージョンに到達できない場合は、ユニキャスト IP アドレスを持つセカンダリリージョンに到達できます。その逆も同様です。Cisco Secure Access は、両方のリージョンが常に到達可能であることを保証します。

What's next

ルートベースのトラフィック転送の作成

トンネルが確立されたら、関連するトラフィックをトンネルに転送する必要があります。Cisco IOS XE 17.14.1a では、CLI テンプレートを使用してトラフィック転送を設定し、次のコマンドを追加します。

ip sdwan route vrf <*network*> <*subnetmask*> **service sse Cisco-Secure-Access**

例：**ip sdwan route vrf 2 0.0.0.0/0 service sse Cisco-Secure-Access**

SSEポリシーとポリシーグループの関連付けおよびデバイスへのポリシーグループの展開

ポリシーをデバイスで機能させるには、以前に作成した SSE ポリシーをポリシーグループに関連付け、後でそのデバイスに関連付ける必要があります。

Step 1 SD-WAN Manager で、**[Configuration]** > **[Policy Groups]** > **[Add Policy Group]**に移動して、SD ルーティングデバイス用の新しいポリシーグループを作成します。

Step 2 [Action] ボタンを選択し、[Policy] で、使用可能なポリシーから以前に作成した [SSE Policy] を選択します。

Step 3 [Save] をクリックして、SSE ポリシーとポリシーグループ間の関連付けを作成します。この関連付けにより、SSE ポリシーがポリシーグループの一部になります。

Step 4 ポリシーグループをデバイスに関連付けます。この関連付けにより、このポリシーグループをデバイスに展開すると、デバイスはこのポリシーグループに関連付けられているすべてのポリシーを継承します。

Step 5 ポリシーグループをデバイスに展開します。デバイスで SSE トンネルを使用する準備が整いました。

What's next

Cisco Secure Access トンネルの確認

SD ルーティングデバイス用に設定した Cisco Secure Access トンネルに関する情報を表示するには、**show sse all** コマンドを使用します。

```
Device# show sse all

************************************
   SSE  Instance Cisco-Secure-Access
************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access
```

SD-WAN Manager からの Cisco Secure Access トンネルのモニターとトラブルシューティング

次のセクションでは、SSE トンネルの問題を特定し、修正措置を講じる方法を示します。

Cisco SD-WAN Manager を使用した SSE トンネル状態のモニタリング

Cisco SD-WAN Manager の次のオプションを使用して、SSE トンネルの状態をモニターします。

- **[Monitor]** > **[Security]** > **[SIG/SSE Tunnel]** ダッシュボードに移動して、以下に関する情報を表示します。
  - 下りトンネル
  - [Degraded Tunnels]：劣化状態は、SSE トンネルが稼働しているが、トラッカーによって検出されたトンネルのレイヤ 7 正常性が、設定された SLA パラメータを満たしていないことを示します。そのため、トラフィックはトンネルを通じてルーティングされません。
  - 上りトンネル

- **[Monitor]** > **[Tunnels]** > **[SIG/SSE Tunnel]** に移動して、以下に関する情報を表示します。

  データプレーントンネル、トンネルエンドポイント、およびトンネルの正常性

Cisco SD-WAN Manager は、Cisco Secure Access に対して作成された各自動トンネルに関する次の詳細を提供するテーブルを表示します。

フィールド	説明
ホスト名	SD ルーティングデバイスのホスト名。
サイト ID	WAN エッジデバイスが展開されているサイトの ID。
トンネル ID	SIG/SSE プロバイダーによって定義されたトンネルの一意の ID。
[Transport Type]	IPSec
Tunnel Name	ローカルエンドとリモートエンドの両方でトンネルを識別するために使用できるトンネルの一意の名前。SSE プロバイダーポータルでは、トンネル名を使用して、特定のトンネルに関する詳細を見つけることができます。
HA ペア	アクティブまたはバックアップ
プロバイダー	Cisco Secure Access
宛先データセンター	トンネルが接続されている SIG/SSE プロバイダーのデータセンター。
トンネルステータス（ローカル）	デバイスによって認識されるトンネルステータス。
トンネルステータス（リモート）	SIG/SSE エンドポイントによって認識されるトンネルステータス。
イベント	トンネルのセットアップ、インターフェイス状態の変更、およびトラッカー通知に関連するイベントの数。番号をクリックすると、イベントのスライドインペインが表示されます。スライドインペインには、特定のトンネルに関連するすべてのイベントが一覧表示されます。
トラッカー	トンネル設定時に有効または無効にされます。

コマンドを使用したモニタリングとトラブルシューティング

このセクションでは、デバイスコマンドから SSE トンネルの問題を特定してトラブルシューティングする方法について詳しく説明します。

デバイス通知を使用したトラブルシューティング

（注）

デバイスシェルにアクセスするには、同意トークンが必要です。同意トークンは、ネットワーク管理者と Cisco Technical Assistance Centre（Cisco TAC）の相互の同意により、システムシェルにアクセスする組織のネットワーク管理者を認証するために使用されるセキュリティ機能です。

イベントが生成されたデバイスに関する情報を表示するには、次の手順を実行します。

1. **/opt/confd/bin/confd_cli -C -P 3010 -noaaa -g sdwan-oper** コマンドを実行します。このコマンドを使用すると、シェルにアクセスしてデバイス通知を表示するためのコマンドを実行することができます。
2. **show notification stream viptela** コマンドを実行してデバイス通知を表示します。

   Device**#show notification stream viptela**

```
notification
 eventTime 2023-11-09T06:21:19.95062+00:00
 sse-tunnel-params-absent
  severity major
  host-name vm6
  if-name TunnelSSE
  wan-if-ip 192.1.2.8
```

暗号セッションの詳細を使用したトラブルシューティング

show crypto session コマンドを実行して、暗号セッションの詳細を表示します。

Device**#show crypto session**

```
Interface: Tunnel15000010
Profile: if-ipsec10-ikev2-profile
Session status: UP-ACTIVE
Peer: 3.76.88.203 port 4500
  Session ID: 7
  IKEv2 SA: local 10.1.15.15/4500 remote 3.76.88.203/4500 Active
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

インターフェイスの詳細を使用したトラブルシューティング

show interface brief コマンドを実行します。このコマンドは、インターフェイスの詳細を表示します。

Device**#show interface brief**

```
Tunnel15000010         10.1.15.15      YES TFTP   up    up
```

エンドポイントトラッカーの詳細を使用したトラブルシューティング

show endpoint tracker コマンドを実行します。このコマンドは、すべてのエンドポイントトラッカーの詳細を表示します。

Device**#show endpoint-tracker**

```
Interface                      Record Name           Status        Address Family   RTT in msecs    Probe
ID   Next Hop
Tunnel16000002                 DefaultTracker        Up            IPv4             22              20
     None
```

トンネルの詳細を使用したトラブルシューティング

show running config|sec sse コマンドを実行します。このコマンドは、トンネルと VRF の詳細を表示します。

Device**#show running config|sec sse**

```
sse instance Cisco-Secure-Access
  ha-pairs
   interface-pair Tunnel15000010 active-interface-weight 1 None backup-interface-weight 1
```

```
!
ip sdwan route vrf 2 0.0.0.0/0 service sse Cisco-Secure-Access
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。