Revised: October 22, 2024

SSL/TLS プロキシとしての SD ルーティングデバイスの設定

SSL/TLS プロキシの概要

今日、クラウドに存在するアプリケーションとデータはますます増えています。その結果、インターネットトラフィックの大部分が暗号化されます。これにより、マルウェアが隠れたままになり、セキュリティを制御できなくなる可能性があります。TLS プロキシ機能を使用すると、エッジデバイスを透過的な TLS プロキシとして設定できます。これにより、デバイスは、エンドツーエンドの暗号化された TLS チャネルによって隠されているリスクを特定できます。インスペクションの後、データは再暗号化されてから宛先に送信されます。

機能名	リリース情報	説明
SSL/TLS プロキシとしての SD ルーティングデバイスの設定	Cisco IOS XE 17.14.1a	この機能を使用すると、自律デバイスをトランスペアレント SSL/TLS プロキシとして設定できます。これらのプロキシデバイスは、着信および発信 TLS トラフィックを復号してインスペクションを有効にし、エンドツーエンドの暗号化によって隠されているリスクを特定できます。

TLS プロキシを使用したトラフィックフロー

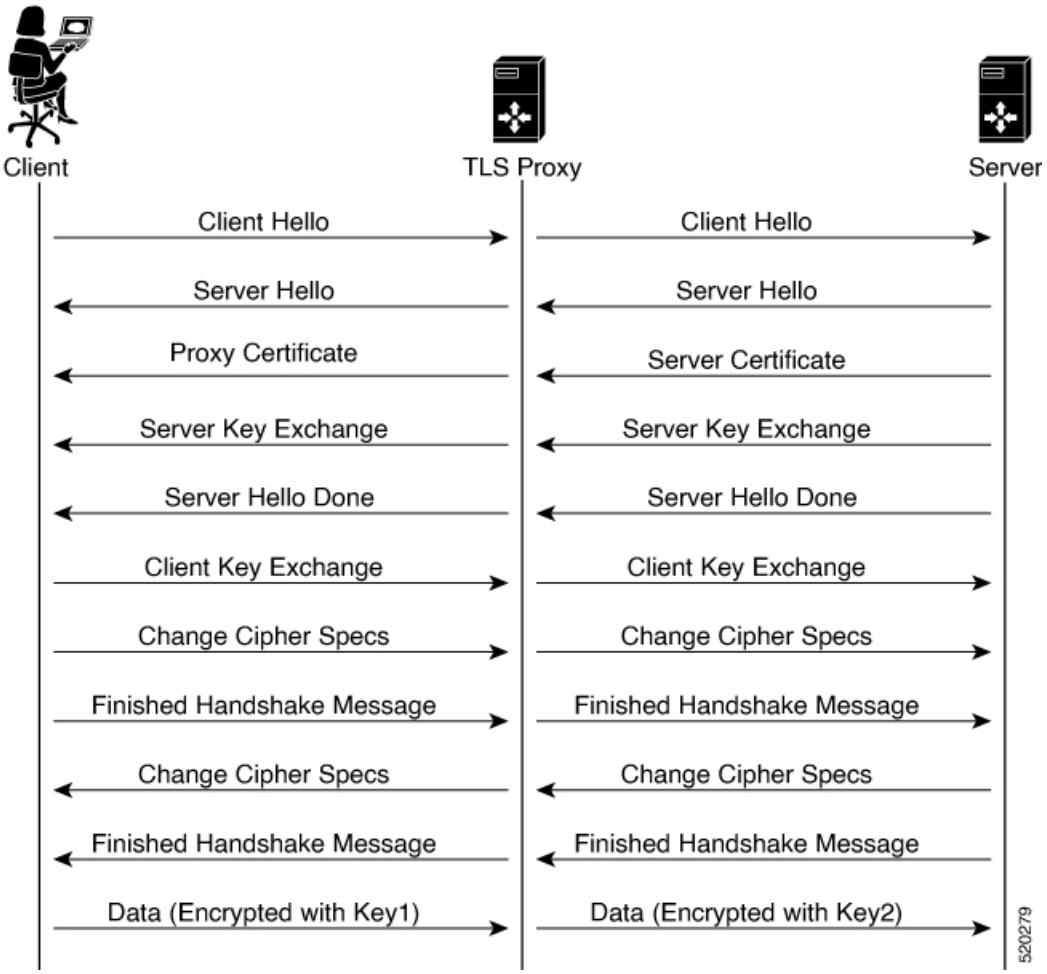
一般的な TLS ハンドシェイクには、信頼できるサードパーティ認証局（CA）によって署名された証明書を使用した認証が含まれます。クライアントとサーバーは、信頼を確立するためにこれらの CA を信頼する必要があります。TLS プロキシは MitM として機能し、CA を実行して接続のプロキシ証明書を動的に発行します。

TLS プロキシが有効になっている場合のトラフィックフローは次のとおりです。

1. クライアントとプロキシの間、およびプロキシとサーバーの間で TCP 接続が確立されます。
2. フローに対して復号ポリシーが有効になっている場合、クライアントの Hello パケットがサーバーに送信され、復号アクションが決定されます。
3. 復号ポリシーに基づいて、次のいずれかのアクションが実行されます。
   - **drop**：判定が drop の場合、クライアントの hello パケットはドロップされ、接続がリセットされます。
   - **do-not-decrypt**：判定が do-not-decrypt の場合、hello パケットは TLS プロキシをバイパスします。
   - **decrypt**：判定が decrypt の場合、パケットはクライアントに転送され、次が実行されます。
     1. トラフィックの最適化のための TCP 最適化
     2. TLS プロキシを介した暗号化トラフィックの復号
     3. TLS プロキシを介した復号されたトラフィックの再暗号化

次の図は、TLS ハンドシェイクプロセスを示しています。

図 *1* : *TLS* ハンドシェイクのプロセス



サポートされる暗号スイート

TLS プロキシ機能は、次の暗号スイートをサポートします。

表 *1* : *TLS* プロキシでサポートされる暗号方式

TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_SEED_CBC_SHA	TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	

TLS プロキシの利点

- 透過的なインスペクションによる TLS トラフィックの脅威のモニタリング
- 復号されたトラフィックのインスペクションに基づくセキュリティポリシーの適用
- 脅威とマルウェアから TLS トラフィックを保護

TLS プロキシの制限事項

- RSA とそのバリアント暗号スイートのみがサポートされます。
- 証明書失効リスト（CRL）チェックは、サーバー証明書の検証ではサポートされていません。ただし、SSL復号ポリシーの詳細設定から OCSP を有効にすることができます。
- OCSP ステープリングはサポートされていないため、TLSセッションを確立するには、ブラウザで明示的に無効にする必要があります。
- IPv6 トラフィックはサポートされていません。
- TLS セッションの再開、再ネゴシエーション、およびクライアント証明書認証はサポートされていません。
- TLS プロキシがクラッシュした場合、再び TLS フローのプロキシとして機能できるようになるまでに最大 2 分かかります。この間、セキュリティ設定に応じて、フローはバイパスされるかドロップされます。

サポートされるデバイスとデバイスの要件

次のデバイスは、SSL/TLS プロキシ機能をサポートしています。

表 *2:* 対応デバイスとリリース

リリース	サポートされるデバイス数
Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a	• Cisco Catalyst 8000V Edge ソフトウェア • Cisco Catalyst 8300 シリーズ エッジ プラットフォーム

デバイスの最小要件

- デバイスには 8 GB 以上の DRAM が必要です（Cisco Catalyst 8300 シリーズ エッジ プラットフォームの場合は 16 GB）。
- デバイスには少なくとも 8 個の vCPU が必要です。

SD ルーティングデバイスの TLS プロキシを設定するためのワークフロー

このワークフローでは、SD-WAN Manager を使用して SD ルーティングデバイスの TLS プロキシを設定するため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
時刻同期の設定	
認証局（CA）サーバーと証明書を要求するデバイス間の時刻同期を設定します。	**[Configuration]** > **[Configuration Groups]**に移動します。 SD-WAN Manager で [System Profile] を選択します。詳細を入力して NTP を設定します。
認証局の設定	
CA サーバーの設定方法を決定します。	CA は、真正性を検証し、クライアントとサーバー間の信頼を確立するために SSL 証明書を発行します。 次のいずれかのオプションを使用して CA を設定できます。 • エンタープライズ CA • SCEP を備えたエンタープライズ CA • CA としての Cisco SD-WAN Manager • 中間 CA としての Cisco SD-WAN Manager
TLS プロキシとして設定するデバイスの選択	
Cisco SD-WAN Manager で設定グループを作成し、WAN エッジデバイスに関連付けます。	ネットワーク内の 1 つ以上のデバイスに適用できる機能または設定の論理グループを作成するのに役立ちます。
セキュリティポリシーの設定	
インスペクション、防止、および復号のための組み込みファイアウォール セキュリティ ポリシーを設定します。	**[Configuration]** > **[Policy Groups]** > **[Embedded Security]** > **[Add Security Policy]**の順に選択し、手順に従ってセキュリティポリシーを設定します。

タスク	説明
TLS トラフィック復号の追加パラメータを設定します。	**インライン TLS 復号セキュリティポリシーの作成** 上記で作成した組み込みセキュリティポリシーにパラメータを追加します。これを行うには、上記で作成した組み込みポリシーを選択し、[Additional Settings] に移動して TLS/SSL 復号ポリシーを作成し、これを上記で作成した組み込みセキュリティポリシーに関連付けます。 または **対象グループを使用したセキュリティポリシーの作成** **[Configuration]** > **[Policy Groups]** > **[Group of Interest]** > **[Security]**の順に選択し、[TLS/SSL Decryption Policy] を追加して、手順に従ってセキュリティポリシーを設定します。次に、これを上記で作成した組み込みセキュリティポリシーに関連付けます。
TLS 復号ポリシーとデバイスの関連付け	
1. 組み込みセキュリティポリシー（関連付けられた TLS/SSL 復号ポリシーがある）のポリシーグループへの関連付け **2.** ポリシーグループとデバイスの関連付け **3.** デバイスの展開	**[Configuration]** > **[Policy Group]** > **[Add Policy Group]**に移動します。（関連付けられた TLS/SSL 復号ポリシーがある）組み込みセキュリティポリシーを選択し、[Save] をクリックしてポリシーをポリシーグループに関連付けます。次に、ポリシーグループをデバイスに関連付け、デバイスを展開します。
TLS プロキシ設定の確認	SSL/TLS プロキシの設定を確認するには、次のコマンドを使用します。 • **show sd-routing running** • **show sd-routing running-config** • **show crypto pki status** • **show sslproxy statistics** • **show sslproxy status** • **show platform hardware qfp active feature utd config** • **show sd-routing running-configuration|section utd-tls-decrypt** • **show utd engine standard config** • **show utd engine standard status**

時刻同期の設定

CA サーバーと証明書を要求するデバイス間の時刻同期を設定します。

Step 1 **[Configuration]** > **[Configuration Groups]**をクリックします。[System Profile] を選択し、次の詳細を入力します。

フィールド	説明
サーバの追加（Add Server）	
Hostname/IP address	NTP サーバーの IP アドレスか、NTP サーバーへの到達方法を認識している DNS サーバーの IP アドレスを入力します。
VRF to reach NTP Server*	NTP サーバーに到達するために使用する VRF 名を入力します。32 文字以内の英数字で指定します
Set authentication key for the server	MD5 認証を有効にするために、NTP サーバーに関連付けられた MD5 キーを指定します。 キーを有効にするには、[Authentication] の [Trusted Key] フィールドでキーを「trusted」とマークする必要があります。
Set NTP version	NTP プロトコルソフトウェアのバージョン番号を入力します。 範囲：1 ～ 4 デフォルト：4
Set interface to use to reach NTP server	NTP パケットの発信に使用する特定のインターフェイスの名前を入力します。このインターフェイスは、NTP サーバーと同じ VPN 内にある必要があります。そうでない場合、設定は無視されます。
Prefer this NTP server*	複数の NTP サーバーが同じストラタムレベルにあり、そのうちの 1 つを優先する場合は、このオプションを有効にします。別のストラタムレベルのサーバーについては、Cisco SD ルーティングは最上位のストラタムレベルのサーバーを選択します。

Step 2 これらの詳細を保存します。

認証局の設定

TLS プロキシの設定では、次の CA オプションがサポートされています。

- エンタープライズ CA （7 ページ）
- SCEP を備えたエンタープライズ CA （8 ページ）
- CA としての Cisco SD-WAN Manager （9 ページ）
- 中間 CA としての Cisco SD-WAN Manager （9 ページ）

次のセクションでは、TLSプロキシ用のCAの選択について十分な情報に基づいて決定するのに役立つよう、サポートされている各 CA オプションの利点と制限事項について説明します。

エンタープライズ CA

このオプションは、エンタープライズCAまたは独自の内部CAを介して証明書の発行を管理するために使用します。Simple Certificate Enrollment Protocol（SCEP）をサポートしていないエンタープライズCAの場合は、手動登録が必要です。

手動登録には、デバイスの証明書署名要求（CSR）をダウンロードすること、CA による署名を受けること、Cisco SD-WAN Manager を介して署名付き証明書をデバイスにアップロードすることが含まれます。

表 *3*：エンタープライズ *CA*：利点と制限事項

利点	制限事項
• 既存のエンタープライズCAおよび証明書管理インフラストラクチャを使用して、証明書の使用状況、有効期限、および有効性をモニタリングできる • クライアントの信頼ストアを更新する必要がない • 発行されたすべての証明書を単一の場所で管理できる • 独自の CA を介して証明書を失効および追跡できる	• 維持することで管理上の負荷が増える。 • TLS プロキシには手動による証明書の展開が必要 • 証明書の使用状況と有効期限を追跡するにはアウトオブバンド管理が必要 • 期限切れのプロキシ証明書を手動で再発行する必要がある • エンタープライズCA証明書が失効または侵害された場合、発行されたすべての証明書が無効になる

エンタープライズ CA の設定

（注）

TLS/SSL プロキシ機能を設定する場合、トラストポイントは、ルート証明書およびルート証明書によって署名された証明書の 2 つの証明書のみを許可します。証明書チェーンはアップロードできません。

1. CA サーバーから CA 証明書を PEM または Base 64 形式でダウンロードします。
2. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificate Authority]** の順に選択します。
3. [Enterprise CA] を選択します。
4. PEM エンコードされた CA 証明書をアップロードします。 [Select a file] をクリックします。

   または

   [Root Certificates] ボックスに CA 証明書を貼り付けます。
5. 証明書のアップロード後に自動入力されるフィンガープリントが CA と一致することを確認します。
6. [Save Certificate Authority] をクリックします。

7. TLS トラフィックを検査および復号するためのファイアウォールポリシーの設定 （12 ページ）。

SCEP を備えたエンタープライズ CA

Simple Certificate Enrollment Protocol（SCEP）は、デジタル証明書の発行をより容易に、より安全で、スケーラブルにするために広く使用されているオープンソースプロトコルです。このオプションは、エンタープライズCAまたは独自の内部 CA を介して証明書の発行を管理するために使用します。CA が SCEP をサポートしている場合は、証明書管理プロセスを自動化するように設定できます。

表 *4 : SCEP* を備えたエンタープライズ *CA*：利点と制限事項

利点	制限事項
• 既存のエンタープライズCAおよび証明書管理インフラストラクチャを使用して、証明書の使用状況、有効期限、および有効性をモニタリングできる • クライアントの信頼ストアを更新する必要がない • 発行されたすべての証明書を単一の場所で管理できる • 独自の CA を介して証明書を失効および追跡できる • TLS プロキシへの証明書の展開を自動化できる	• 維持することで管理上の負荷が増える。 • エンタープライズCA証明書が失効または侵害された場合、発行されたすべての証明書が無効になる • Cisco SD-WAN Manager による限定的な可視性を提供 • エンタープライズ CA では SCEP のサポートが制限される

SCEP を備えたエンタープライズ CA の設定

1. CA サーバーから CA 証明書を PEM または Base 64 形式でダウンロードします。
2. Cisco SD-WAN Manager のメニューから、[Configuration] > [Certificate Authority] の順に選択します。
3. [Enterprise CA] を選択します。
4. （オプション、ただし推奨）[Simple Certificate Enrollment Protocol (SCEP)] チェックボックスをオンにします。
5. [URL Base] フィールドに、SCEP サーバーの URL を入力します。
6. （オプション）[Challenge Password/Phrase] を入力します（設定済みの場合）。

（注）

エンタープライズ CA が SCEP で設定されている場合、エンタープライズ SCEP CA サーバーは VRF から到達可能である必要があります。

7. PEM エンコードされた CA 証明書をアップロードします。 [Select a file] をクリックします。

   または

   [Root Certificates] ボックスに CA 証明書を貼り付けます。
8. [Save Certificate Authority] をクリックします。

9. TLS トラフィックを検査および復号するためのファイアウォールポリシーの設定 （12 ページ）

CA としての Cisco SD-WAN Manager

このオプションは、エンタープライズ CA または独自の内部 CA を介して証明書の発行を管理するために使用します。Simple Certificate Enrollment Protocol（SCEP）をサポートしていないエンタープライズ CA の場合は、手動登録が必要です。

表 *5 : CA* としての *Cisco SD-WAN Manager*：利点と制限事項

利点	制限事項
• プロキシデバイスへの証明書の展開が自動化される • 証明書が期限切れになる前に再発行および再検証される • Cisco SD-WAN Manager を介して証明書をモニター、追跡、および検証できる	• Cisco SD-WAN Manager 証明書をクライアントの信頼ストアにプッシュする必要がある

CA としての Cisco SD-WAN Manager の設定

企業に内部 CA がない場合は、[SD-WAN Manager as CA] を使用します。このオプションでは、Cisco SD-WAN がルート CA として使用され、ネットワークのエッジにあるプロキシデバイスに下位 CA を発行する権限が付与されます。CA によって発行された証明書は、Cisco SD-WAN Manager を使用して管理できます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificate Authority]** の順に選択します。
2. [SD-WAN as CA] を選択します。

（注）

SD-WAN Manager を CA として設定する場合は、[Set SD-WAN as Intermediate CA] チェックボックスをオフのままにします。

3. 要求された詳細情報（共通名、組織、組織単位、地域、都道府県、国コード、電子メール）を入力します。
4. 証明書の有効期限をドロップダウンリストから選択します。
5. [Save Certificate Authority] をクリックします。
6. TLS トラフィックを検査および復号するためのファイアウォールポリシーの設定 （12 ページ）。

中間 CA としての Cisco SD-WAN Manager

内部エンタープライズ CA があるが、Cisco SD-WAN Manager を中間 CA として使用して下位 CA 証明書を発行および管理したい場合は、このオプションを使用します。

表 *6 :* 中間 *CA* としての *CiscoSD-WAN Manager*：利点と制限事項

利点	制限事項
• プロキシデバイスへの証明書の展開が自動化される • 証明書が期限切れになる前に再発行および再検証される • 侵害されたプロキシ証明書は失効するため、証明書の侵害に関連するリスクが限定される • Cisco SD-WAN Manager を介して証明書をモニター、追跡、および検証できる • エンタープライズ CA 証明書以外の証明書をクライアントの信頼ストアにプッシュする必要がない	• 手動展開が必要 • 2 つの CA を維持することで管理上の負荷が増える • Cisco SD-WAN Manager 証明書の使用状況は、エンタープライズ CA を介して追跡される • ネットワークにクラスタリングまたは冗長性のために複数の Cisco SD-WAN Manager コントローラがある場合、展開が複雑になる可能性がある

中間 CA としての SD-WAN Manager の設定

TLS プロキシデバイスが Cisco SD-WAN Manager によって発行された下位 CA 証明書を使用できるようにするには、Cisco SD-WAN Manager を中間 CA として設定します。

Cisco SD-WAN Manager が中間 CA として設定されている場合、エンタープライズ CA はルート CA として機能し、プロキシデバイスの下位 CA 証明書を発行および管理するための優先中間 CA として指定されます。このオプションは、独自の内部 CA があるが、Cisco SD-WAN Manager を使用して証明書の発行と更新を自動化および管理したい企業に適しています。

1. メニューから、 [Configuration] > [Certificate Authority] の順に選択します。
2. [SD-WAN Manager as CA] を選択します。
3. [Set SD-WAN as Intermediate CA] チェックボックスをオンにします。
4. [Select a file] オプションを使用して CA 証明書をアップロードします。

   または

   [Root Certificate] テキストボックスに PEM エンコードされた CA 証明書ファイルの内容を貼り付けます。
5. [Next] をクリックします。
6. [Generate CSR] 領域で、必要な詳細情報を入力し、[Generate CSR] をクリックします。

   画面の [CSR] フィールドに証明書署名要求（CSR）が入力されます。
7. CSR をコピーまたはダウンロードし、エンタープライズ CA サーバーにアップロードして、下位 CA 証明書として CA サーバーに署名してもらいます。

（注）

CA サーバーによって署名された CSR を取得するプロセスは、CA ごとに異なる場合があります。標準の手順に従って、CA によって署名された CSR を取得します。

8. [Save Certificate Authority] をクリックします。
9. TLS トラフィックを検査および復号するためのファイアウォールポリシーの設定 （12 ページ）。

下位 CA 証明書の TLS プロキシへのアップロード

Cisco SD-WAN Manager が中間 CA として設定されている場合、エンタープライズ CA はルート CA として機能し、Cisco SD-WAN Manager はプロキシデバイスの下位 CA 証明書を発行および管理するための優先中間 CA として指定されます。このオプションは、独自の内部 CA があるが、Cisco SD-WAN Manager を使用して証明書の発行と更新を自動化および管理したい企業に適しています。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificate Authority]** の順に選択します。
2. **[Set vManage as Intermediate CA]** チェックボックスをオンにします。
3. PEM エンコードされた CA 証明書をアップロードします。 [Select a file] をクリックします。

   または

   [Root Certificates] ボックスに CA 証明書を貼り付けます。

   [Next] をクリックします。
4. [Intermediate Certificate] テキストボックスに、署名済み Cisco SD-WAN Manager 証明書の内容を貼り付け、[Upload] をクリックします。

   または

   [Select a file] をクリックし、前の手順で生成した CSR をアップロードし、[Upload] をクリックします。
5. CSR のアップロード後に自動入力される [Finger Print] が CA 証明書と一致することを確認します。
6. [Save Certificate Authority] をクリックします。

（注）

Cisco 公開キー（PKI）証明書がデバイスにインストールされており、証明書を変更する場合は、ポリシーグループから組み込みセキュリティポリシーを切り離し、ポリシーグループをデバイスにプッシュします。これにより、既存の PKI 証明書と設定が削除されます。PKI 証明書に変更を加えた後、組み込みセキュリティポリシーを再アタッチし、ポリシーグループをデバイスにプッシュします。このプロセスにより、Cisco PKI 証明書の変更に応じてデバイスが更新されます。

設定グループへのデバイスの追加

設定グループにデバイスを追加します。

Step 1 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。

Step 2 [Associated Devices] をクリックして、[Add Devices] をクリックします。

Step 3 指示に従って操作します。選択したデバイスが [Devices] テーブルにリストされます。

TLS トラフィックを検査および復号するためのファイアウォールポリシーの設定

トラフィックがゾーン間を流れるために満たすべき条件を定義するファイアウォールポリシーを設定します。

Step 1 [Cisco SD-WAN Manager] メニューから、**[Configuration]** > **[Policy Groups]** > **[Embedded Security]** > **[Add Security Policy]**の順に選択し、手順に従ってファイアウォールポリシーを設定します。

Step 2 **送信元ゾーンと宛先ゾーンのサブポリシーの作成：**

ゾーンは、ネットワークのセキュリティ境界を設定します。ゾーンは、トラフィックがネットワークの別の領域に移動するときにポリシー制限の対象となる境界を定義します。

Step 3 検査、復号、および防止のためのセキュリティポリシーの作成：

a) **高度なインスペクション プロファイル：**

高度なインスペクション プロファイルは、IPS、URLF、AMP、TLS アクション、TLS/SSL 復号などの Cisco UTD セキュリティ機能を含むセキュリティ インスペクション プロファイルです。

b) **侵入防御：**

このプロファイルを設定すると、疑わしいアクティビティにフラグを付けることで、脅威と攻撃を検出または阻止します。

c) **URL フィルタリング：**

URL フィルタリングプロファイルを使用すると、URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトまたはイントラネットサイトへのアクセスを制御できます。ユーザーは、Web アクセスを管理する URL フィルタリングプロファイルを設定できます。

d) **Advanced Malware Protection:**

AMP プロファイルは、マルウェアのライフサイクルのすべての段階をカバーする保護と可視性を提供するために SD ルーティングデバイスを実装します。

e) **TLS/SSL プロファイル：**

このプロファイルを使用すると、TLS トラフィックの種類に基づいてアクションを設定できます。

f) **TLS/SSL 復号：**

復号ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。

TLS/SSL 復号ポリシーは、2 つの方法で設定できます。これは、組み込みセキュリティポリシーの作成ページから、または対象グループポリシーの作成ページから設定できます。

Step 4 [Security Policy] の作成ページで [Additional Settings] をクリックして、TLS/SSL 復号の特定のパラメータを追加します。

Step 5 [TLS/SSL Decryption Policy] ドロップダウンから [Create New] をクリックして、復号ポリシーを定義します。

フィールド名	説明
Policy Name	ポリシーの名前。名前は、最大32文字まで使用できます。
[Server Certificate Checks]	
Expired Certificate	サーバー証明書の有効期限が切れた場合のポリシーの動作を定義します。次のオプションがあります。 • [Drop]：トラフィックをドロップします。 • [Decrypt]：トラフィックを復号します。
[Untrusted Certificate]	サーバー証明書が信頼されていない場合のポリシーの動作を定義します。次のオプションがあります。 • [Drop]：トラフィックをドロップします。 • [Decrypt]：トラフィックを復号します。
[Certificate Revocation Status]	サーバー証明書の失効ステータスをチェックするためにオンライン証明書ステータスプロトコル（OCSP）を使用するかどうかを定義します。オプションは、[Enabled] または [Disabled] です。
[Unknown Revocation Status]	OCSP失効ステータスが不明な場合のポリシーの動作を定義します。 • [Drop]：トラフィックをドロップします。 • [Decrypt]：トラフィックを復号します。
[Unsupported Mode Checks]	
[Unsupported Protocol Versions]	サポートされていないプロトコルのバージョンを定義します。 • [Drop]：サポートされていないプロトコルバージョンをドロップします。 • [Decrypt]：サポートされていないプロトコルバージョンを復号します。

フィールド名	説明
[Unsupported Cipher Suites]	サポートされていない暗号スイートを定義します。 • [Drop]：サポートされていない暗号スイートをドロップします。 • [Decrypt]：サポートされていない暗号スイートを復号します。
[Failure Mode]	障害モードを定義します。オプションは、[close] と [open] です。
[Certificate Bundle]	デフォルトの CA を使用するには、[Use default CA certificate bundle] チェックボックスをオンにします。
[Minimum TLS Version]	プロキシがサポートする必要のある TLS の最小バージョンを設定します。次のオプションがあります。 • **TLS 1.0** • **TLS 1.1** • **TLS 1.2**
[Proxy Certificate Attributes]	
[RSA Keypair Modules]	プロキシ証明書の RSA キー係数を定義します。次のオプションがあります。 • [1024 bit RSA] • [2048 bit RSA] • [4096 bit RSA]
[Ec Key Type]	キータイプを定義します。次のオプションがあります。 • [P256] • [P384] • [P521]
[Certificate Lifetime (in Days)]	プロキシ証明書の有効期間を日数で設定します。

または、**[Policy Group]** > **[Group of Interest]**を使用して TLS/SSL 復号ポリシーを設定し、TLS/SSL 復号ポリシーを追加することもできます。上記のステップ 4 に示すように、このポリシーを組み込みポリシーに追加してください。

Step 6 復号ポリシーを保存します。

ポリシーグループへのセキュリティポリシーの追加

上記で作成した埋め込みセキュリティポリシーをポリシーグループに関連付けます。次の手順を実行します。

Step 1 [Policy Group] をクリックして新しいポリシーグループを作成します。ポリシーグループは、ネットワーク内の 1 つ以上のサイトまたはサイトのデバイスに適用できるポリシーを論理的にグループ化します。

Step 2 [Policy Group Name] を指定し、ソリューションタイプとして [SD-Routing] を選択します。ポリシーグループの説明を入力します。[Create] をクリックします。

Step 3 ドロップダウンリストから組み込みセキュリティポリシーを選択します。組み込みセキュリティポリシーには、暗号化、ファイアウォール、侵入防御、URL フィルタリング、およびマルウェアのポリシーが含まれます。

Step 4 [Save] をクリックして設定を保存します。

Step 5 鉛筆アイコンをクリックして、ポリシーグループに関連付けるデバイスを選択します。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 6 [Deploy] をクリックしてサイトを選択し、ポリシーグループを展開します。

TLS プロキシ設定の確認

TLS プロキシの設定を確認するには、次のコマンドを使用します。

show sd-routing running	Cisco SD-WAN Manager で、CLI モードで次のコマンドを実行して、設定が適用されているかどうかを確認します。
show sd-routing running-config	Cisco SD-WAN Manager で、SSH 経由でデバイスの CLI に接続して、次のコマンドを実行します。
show crypto pki status	デバイスの CLI で次のコマンドを実行し、デバイスに PROXY-SIGNING-CA が存在し、正しく設定されていることを確認します。
show sslproxy statistics	デバイスの CLI で、次のコマンドを実行して TLS プロキシの統計情報を表示します。
show sslproxy status	デバイスの CLI で次のコマンドを実行して、TLS プロキシが正常に設定され、Cisco SD-WAN Manager で有効になっているかどうかを確認します。 出力の Clear Mode: FALSE は、TLS プロキシが正常に設定され、Cisco SD-WAN Manager で有効になっていることを示します。
show platform hardware qfp active feature utd config	デバイスの CLI で、次のコマンドを実行して設定を確認します。
show sd-routing running-configuration|section utd-tls-decrypt	デバイスの CLI で、次のコマンドを実行して設定を確認します。

show utd engine standard config	デバイスのCLIで、次のコマンドを実行して設定を確認します。
show utd engine standard status	デバイスのCLIで、次のコマンドを実行して設定を確認します。

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。