HTTP CONNECT

簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1*：機能の履歴

機能名	リリース情報	説明
HTTP CONNECT	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、AppQoE での HTTP CONNECT メソッドの処理がサポートされるようになります。このサポートにより、SSL プロキシや DRE などのサービスで、HTTP CONNECT 暗号化トラフィックが最適化されます。

HTTP CONNECT に関する情報

HTTP CONNECT メソッドを使用すると、送信元サーバーは、明示的なプロキシサーバーを使用して宛先サーバーとの双方向通信を開始できます。HTTP CONNECT を使用して、送信元サーバーと宛先サーバー間の TCP 接続を介した HTTP プロキシトンネルを作成できます。HTTP CONNECT トラフィック処理により、SSL プロキシと DRE は、HTTP トンネル内の暗号化データを最適化できます。

SSL/TLS プロキシの詳細については、「Information about SSL/TLS Proxy」[英語] を参照してください。

HTTP CONNECT の前提条件

- Cisco IOS XE Catalyst SD-WAN デバイス が Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a を実行していることを確認します。
- HTTP CONNECT 要求をブロードキャストするには、リモートサーバーでホストされている明示的なプロキシが必要です。

HTTP CONNECT に関する制約事項

- HTTP CONNECT 要求は、プロキシサーバーにのみ送信されることを目的としています。
- HTTP CONNECT 要求は、標準ポートであるポート 80、8080、および 8088 を使用してのみ送信できます。
- HTTP CONNECT は、United Threat Defense（UTD）ではサポートされていません。そのため、UTD が有効になっている場合、設定はブロックされます。

HTTP CONNECT の使用例

HTTP CONNECT を使用しない SSL プロキシトラフィック

データの復号化がない Cisco IOS XE Catalyst SD-WAN リリース 17.x リリースの場合、DRE がフロー内の繰り返しパターンを把握できず、DRE圧縮は効果的ではありません。そのため、フローに対して DRE をバイパスすることが必須になります。あるいは、DRE に流れ込むデータをクリアテキストにする必要があります。HTTP CONNECT 要求が送信されるときに、SSL プロキシは HTTP CONNECT SSL トラフィックを復号しないため、暗号化されたトラフィックが DRE に流れ込みます。その結果、トラフィックの最適化に失敗します。

HTTP CONNECT を使用した SSL プロキシトラフィック

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以降、AppQoE での HTTP CONNECT の処理により、SSL プロキシはクリアテキストデータを復号化して DRE に送信するようになり、さらなる最適化が可能になります。

CLI アドオンテンプレートを使用した HTTP CONNECT の設定

はじめる前に

新しい CLI アドオンテンプレートを作成するか、既存の CLI アドオンテンプレートを編集します。

CLI Add-on Feature Templates の詳細については、「CLI Add-on Feature Templates」を参照してください。

CLI を使用した HTTP CONNECT の設定

1. コンフィギュレーション モードを入力します。

   ```
   config-transaction
   ```

2. HTTP CONNECT を有効にします。

   ```
   sdwan appqoe http-connect enable server-port <port-number>
   ```

（注） HTTP CONNECT を有効にするために入力できる標準サーバーポート番号は、80、8080、および 8088 のみです。

標準ポート番号を入力しない場合、サーバーポート番号 80 がデフォルトと見なされます。

3. 変更を確定します。

   ```
   commit
   ```

   次に例を示します。

   ```
   sdwan appqoe http-connect enable server-port80
   ```

4. CLI アドオンテンプレートをそれぞれのデバイスにアタッチします。

HTTP CONNECT 設定の確認

次に、**show sslproxy statistics** コマンドの出力例を示します。

```
Device# show sslproxy statistics
============================================================

              SSL Proxy Statistics

============================================================

Connection Statistics:

Total Connections                  : 3

Proxied Connections                : 0

Non-proxied Connections            : 3

Clear Connections                  : 0

Active Proxied Connections         : 0

Active Non-proxied Connections     : 2

Active Clear Connections           : 0

Max Conc Proxied Connections       : 0

Max Conc Non-proxied Connections   : 2

Max Conc Clear Connections         : 0

Tunneled Proxied Connections       : 2

Tunneled Non-proxied Connections   : 0

Active Tunneled Proxied Flows      : 1

Active Tunneled Non-proxied Flows  : 0

Max Conc Tunneled Proxied Flows    : 1

Max Conc Tunneled Non-proxied Flows: 0

SSL Encrypted marked Non SSL Flows : 0

Total Closed Connections           : 2
```

この出力で、**Tunnel Proxied Connections** と **Tunneled Non-proxied Connections** は、HTTP CONNECT 要求が成功したことを示しています。

CLI を使用した HTTP CONNECT のモニター

デバイスの HTTP CONNECT をモニターするには、**show sdwan appqoe flow flow-id** コマンドを使用します。次に出力例を示します。

```
Device# show sdwan appqoe flow flow-id 4278327056727738
Flow ID: 4278327056727738
VPN: 1  APP: 0 [Client 192.0.2.0:49470 - Server 192.0.2.24:8080]

HTTP Connect: 1
TCP stats
---------
```

```
Client Bytes Received   : 215
Client Bytes Sent       : 46
Server Bytes Received   : 208
Server Bytes Sent       : 193

Client Bytes sent to SSL: 215
Server Bytes sent to SSL: 168

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 152
S2C HTX to DRE Pkts     : 4
C2S DRE to HTX Bytes    : 70
C2S DRE to HTX Pkts     : 3
S2C DRE to HTX Bytes    : 46
S2C DRE to HTX Pkts     : 2

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 129
S2C SVC Bytes to SSL    : 46
C2S SSL to TCP Tx Pkts  : 6
C2S SSL to TCP Tx Bytes : 193
S2C SSL to TCP Tx Pkts  : 2
S2C SSL to TCP Tx Bytes : 46
```

この出力で、**HTTP Connect: 1** は HTTP CONNECT 要求が成功したことを示します。

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。