

HTTP CONNECT

Table 1: Feature History

Feature Name	Release Information	Description
HTTP CONNECT	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature introduces support for handling the HTTP CONNECT method in AppQoE. With this support, services such as SSL Proxy and DRE optimize HTTP CONNECT encrypted traffic.

- Information About HTTP CONNECT, on page 1
- Prerequisites for HTTP CONNECT, on page 1
- Restrictions For HTTP CONNECT, on page 2
- Use Cases Of HTTP CONNECT, on page 2
- Configure HTTP CONNECT Using a CLI Add-On Template, on page 2
- Configure HTTP CONNECT Using CLI, on page 2
- Verify HTTP CONNECT Configuration, on page 3
- Monitor HTTP CONNECT Using the CLI, on page 4

Information About HTTP CONNECT

HTTP CONNECT method enables the source server to start two-way communications with the destination server using an explicit proxy server. Using the HTTP CONNECT you can create a HTTP proxy tunnel over a TCP connection between the source and destination servers. The HTTP CONNECT traffic handling enables SSL Proxy and DRE to optimize the encrypted data in the HTTP Tunnel.

For more information on SSL/TLS Proxy see, Information about SSL/TLS Proxy.

Prerequisites for HTTP CONNECT

- Ensure that the Cisco IOS XE Catalyst SD-WAN Devices are running the Cisco IOS XE Catalyst SD-WAN Release 17.9.1a.
- An explicit proxy hosted on a remote server is required to broadcast a HTTP CONNECT request.

Restrictions For HTTP CONNECT

- A HTTP CONNECT request is intended to be sent only to a proxy server.
- A HTTP CONNECT request can be sent only using the following standard ports Port 80, 8080, and 8088.
- HTTP CONNECT is not supported by United Threat Defense (UTD). Hence the configuration is blocked if UTD is enabled.

Use Cases Of HTTP CONNECT

SSL Proxy Traffic without HTTP CONNECT

In Cisco IOS XE Catalyst SD-WAN Release 17.x releases, without the decryption of data, DRE fails to observe repeating patterns in a flow and the DRE compression is not effective. And hence, bypassing the DRE for the flow is mandatory or the data flowing to the DRE should be in clear text. When a HTTP CONNECT request is placed, the SSL Proxy doesn't decrypt the HTTP CONNECT SSL traffic, which results in the encrypted traffic flowing to the DRE, that fails to optimize the traffic.

SSL Proxy Traffic with HTTP CONNECT

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, HTTP CONNECT handling in AppQoE enables the SSL Proxy to decrypt and send clear text data to the DRE for further optimizing.

Configure HTTP CONNECT Using a CLI Add-On Template

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure HTTP CONNECT Using CLI

1. Enter configuration mode.

   ```
   config-transaction
   ```

2. Enable HTTP CONNECT

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



Note You can only enter the following standard server port numbers to enable HTTP CONNECT: 80, 8080, and 8088.

If you don't enter a standard port number, the default server-port number is assumed as 80.

3. Commit the changes

   commit

   For example,

   sdwan appqoe http-connect enable server-port80

4. Attach the CLI add-on template to the respective device.

Verify HTTP CONNECT Configuration

The following is a sample output from the **show sslproxy statistics** command:

```
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
```

In this output, **Tunnel Proxied Connections** and **Tunneled Non-proxied Connections** indicate that HTTP CONNECT request is successful.

Monitor HTTP CONNECT Using the CLI

Use the **show sdwan appqoe flow flow-id** command to monitor HTTP CONNECT on a device. The following is an example output:

```
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
```

In this output, **HTTP Connect: 1** indicates that HTTP CONNECT request is successful.