Overview of SSL/TLS proxy

Today more and more apps and data reside in the cloud. As a result, majority of internet traffic is encrypted. This may lead to malware remaining hidden and lack of control over security. The TLS proxy feature allows you to configure edge devices as transparent TLS proxy. This allows the devices to identify risks that are otherwise hidden by end-to-end encrypted TLS channel. The data is re-encrypted post inspection before being sent to its destination.

Feature Name	Release Information	Description
Configure an SD-Routing Device as an SSL/TLS Proxy	Cisco IOS XE 17.14.1a	This feature allows you to configure an autonomous device as a transparent SSL/TLS proxy. These proxy devices can then decrypt incoming and outgoing TLS traffic to enable their inspection and identify risks that are hidden by end-to-end encryption.

Traffic flow with TLS proxy

A typical TLS handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). The clients and servers must trust these CAs in order to establish trust. TLS Proxy acts as MitM and runs a CA to issue proxy certificates for the connection dynamically.

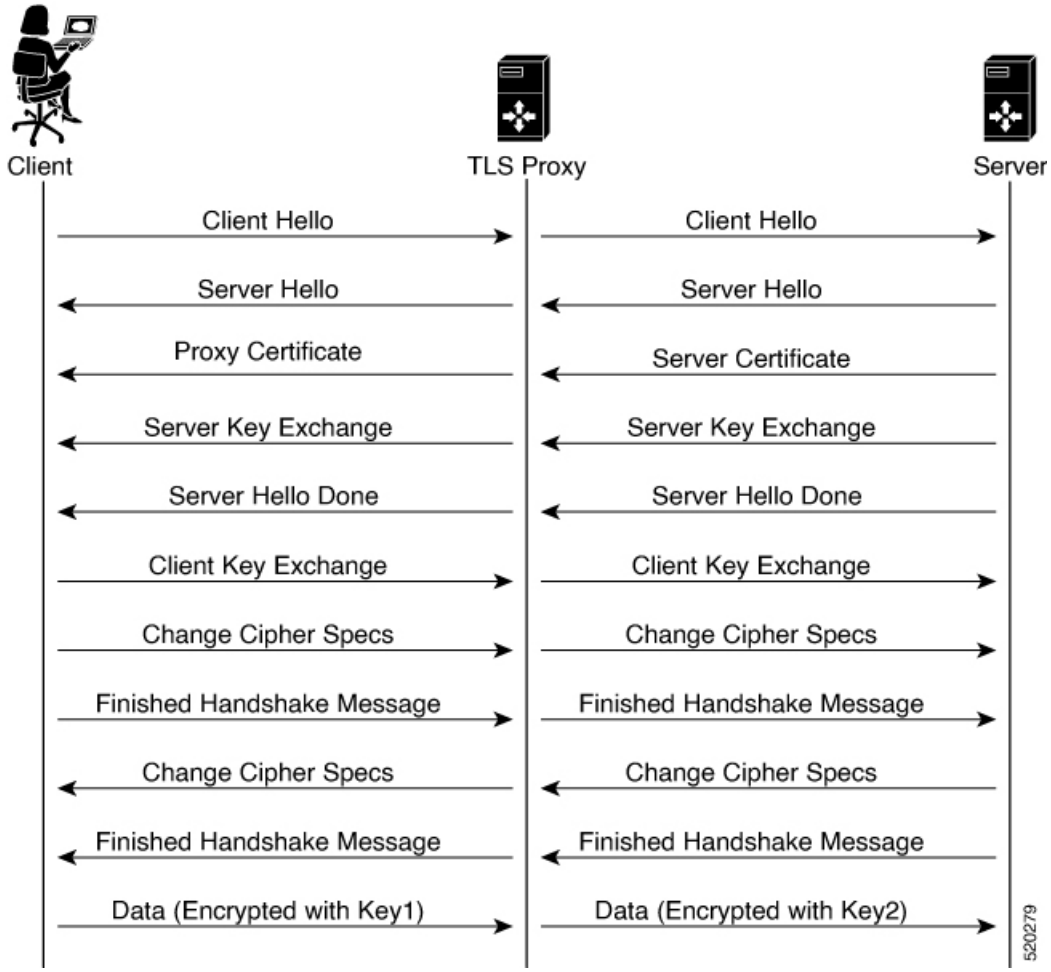
This is how traffic flows when TLS proxy is enabled:

1. A TCP connection is established between the client and the proxy, and the proxy and the server.
2. If a decryption policy is enabled for the flow, a client Hello packet is sent to the server to determine the decryption action.
3. Based on the decryption policy, one of the following actions takes place:
   - **drop:** If the verdict is drop, the hello packet from the client is dropped and the connection is reset.
   - **do-not-decrypt:** If the verdict is do-not-decrypt, the hello packet bypasses TLS proxy.

- **decrypt:** If the verdict is decrypt, the packet is forwarded to the client and goes through the following:
  a. TCP optimization for optimization of traffic
  b. Decryption of encrypted traffic through TLS proxy
  c. Re-encryption of decrypted traffic through TLS proxy

The following image shows the TLS handshake process

Figure 1: The process of TLS handshake



Supported cipher suites

The TLS Proxy feature supports the following cipher suites.

Table 1: Ciphers supported for TLS proxy

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	

Benefits of TLS proxy

- Monitoring of TLS traffic for any threats through transparent inspection
- Enforcement of security polices based on the inspection of the decrypted traffic
- Threat and malware protection for TLS traffic

Limitations TLS proxy

- Only RSA and its variant cipher suites are supported.
- Certificate Revocation List (CRL) check is not supported for server certificate validation. However, you can enable OCSP from Advanced Settings in SSL Decryption policy.
- OCSP stapling is not supported and must be explicitly disabled on the browser for the TLS session to be established.
- IPv6 traffic is not supported.
- TLS session resumption, renegotiation and client certificate authentication are not supported.
- If TLS proxy crashes, it takes up to two minutes for it to be ready to serve as proxy for TLS flows again. During this time, depending upon your security settings, the flows are either bypassed or dropped.

Supported devices and device requirements

The following devices support the SSL/TLS Proxy feature.

Table 2: Supported devices and releases

Release	Supported Devices
Cisco IOS XE Release 17.14.1a	• Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8300 Series Edge Platforms

Minimum device requirements

- The device must have a minimum of 8 GB of DRAM; 16 GB for Cisco Catalyst 8300 Series Edge Platforms.
- The device must have a minimum of 8 vCPUs.

Workflow to set up TLS proxy for SD-Routing devices

This workflow outlines the high-level steps required to set up TLS Proxy for SD-Routing devices using SD-WAN Manager. The detailed instructions are covered in the following sections.

Task	Description
Set up Time Synchronization	
Set up time synchronization between the Certificate Authority (CA) server and the device seeking the certificate.	Go to **Configuration** > **Configuration Groups** Select **System Profile** in SD-WAN Manager. Enter details to configure NTP.
Set up Certificate Authority	
Determine how to configure the CA server.	A CA issues SSL certificates to verify the authenticity and establish trust between a client and server. You can configure a CA using one of the following options: • Enterprise CA • Enterprise CA with SCEP • Cisco SD-WAN Manager as CA • Cisco SD-WAN Manager as Intermediate CA
Select devices to be configured as TLS Proxy	
Create a Configuration Group in Cisco SD-WAN Manager and associate it to the WAN edge device.	Helps to form a logical grouping of features or configurations that can be applied to one or more devices in the network.
Configure Security Policies	

Task	Description
Configure an embedded firewall security policy for inspection, prevention and decryption.	Go to **Configuration** > **Policy Groups** > **Embedded Security** > **Add Security Policy** and follow the steps to configure the security policy.
Configure additional parameters for TLS traffic decryption.	**Create an inline TLS Decryption Security Policy** Add additional parameters to the Embedded Security policy created above. To do that, select the Embedded Policy created above, go to **Additional Settings** and create a TLS/SSL Decryption policy and associate this with the Embedded Security Policy that you created above. OR **Create a Security Policy using Group of Interest** Go to **Configuration** > **Policy Groups** > **Group of Interest** > **Security**, add **TLS/SSL Decryption Policy** and follow the steps to configure the security policy. Next associate this with the Embedded Security Policy created above.
Associate the TLS Decryption Policy with a Device	
1. Associate the Embedded Security Policy (has the associated TLS/SSL Decryption Policy) to a Policy Group **2.** Associate the Policy Group with the device **3.** Deploy the device	Go to **Configuration** > **Policy Group** > **Add Policy Group**. Select the Embedded Security policy (has the associated TLS/SSL Decryption policy) and click **Save** to associate the policy with the Policy Group. Next, associate the policy group to a device and delpoy the device.
Verify the TLS Proxy Configuration	Use the following commands to verify the configuration of SSL/TLS Proxy: • **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**

Configure time synchronization

Set up time synchronization between the CA server and the device seeking the certificate.

Procedure

Step 1 Click **Configuration** > **Configuration Groups** . Select **System Profile** and enter the following details.

Field	Description
Add Server	
Hostname/IP address	Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server.
VRF to reach NTP Server*	Enter the VRF name used to reach the NTP server, can be up to 32 alphanumeric characters
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the **Trusted Key** field under **Authentication**.
Set NTP version	Enter the version number of the NTP protocol software. Range: 1 to 4 Default: 4
Set interface to use to reach NTP server	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer this NTP server*	Enable this option if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, Cisco SD-Routing chooses the one at the highest stratum level.

Step 2 Save these details.

Configure certificate authority

The following CA options are supported for configuring TLS proxy :

- Enterprise CA, on page 7
- Enterprise CA with SCEP, on page 8
- Cisco SD-WAN Manager as CA, on page 9
- Cisco SD-WAN Manager as intermediate CA, on page 9

The following sections cover the benefits and limitations of each of the supported CA options to help you make an informed decision about choosing the CA for TLS proxy.

Enterprise CA

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. For Enterprise CA that does not support Simple Certificate Enrollment Protocol (SCEP), manual enrollment is required.

Manual enrollment involves downloading a Certificate Signing Request (CSR) for your device, getting it signed by your CA, and then uploading the signed certificate to the device through Cisco SD-WAN Manager

Table 3: Enterprise CA: Benefits and limitations

Benefits	Limitations
• Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates • The client trust-store need not be updated • Provides a single location for managing all certificates issued • Certificates can be revoked and tracked through your own CA	• Maintenance creates an administrative overload. • Manual certificate deployment is required for TLS proxy • Out-of-band management is required for tracking the usage and expiry of certificates • Requires manual re-issuance of expired proxy certificates • If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated

Configure Enterprise CA

Note When configuring TLS/SSL proxy feature, trust point allows only two certificates; root certificate and certificate signed by root certificate. You cannot upload cert chain.

1. Download a CA certificate from your CA server in PEM or Base 64 format.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
3. Choose **Enterprise CA.**
4. To upload your PEM-encoded CA certificate. click **Select a file**.

   OR

   Paste the CA certificate in the Root Certificates box.
5. Verify that the fingerprint, which auto-populates after you upload the certificate, matches your CA.
6. Click **Save Certificate Authority**.
7. Configure a firewall policy to inspect and decrypt TLS traffic , on page 12.

Enterprise CA with SCEP

Simple Certificate Enrollment Protocol (SCEP) is an open source protocol that is widely used to make digital certificate issuance easier, more secure, and scalable. Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. If your CA supports SCEP, you can configure it to automate the certificate management process.

Table 4: Enterprise CA with SCEP: Benefits and limitations

Benefits	Limitations
• Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates • The client trust-store need not be updated • Provides a single location for managing all certificates issued • Certificates can be revoked and tracked through your own CA • Certificate deployment to TLS Proxy can be automated	• Maintenance creates an administrative overload. • If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated • Offers limited visibility through Cisco SD-WAN Manager • Enterprise CA have limited support for SCEP

Configure Enterprise CA with SCEP

1. Download a CA certificate from your CA server in PEM or Base 64 format.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
3. Choose **Enterprise CA.**
4. [Optional,but recommended] Check the **Simple Certificate Enrollment Protocol (SCEP)** check box.
5. Enter the SCEP server URL in the **URL Base** field.
6. [Optional] Enter the **Challenge Password/Phrase** if you have one configured.

Note If Enterprise CA is configured with SCEP, the Enterprise SCEP CA server should be reachable from the VRF.

7. To upload your PEM-encoded CA certificate. click **Select a file**

   OR

   Paste the CA certificate in the **Root Certificates** box.
8. Click **Save Certificate Authority**.
9. Configure a firewall policy to inspect and decrypt TLS traffic , on page 12

Cisco SD-WAN Manager as CA

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. For Enterprise CA that does not support Simple Certificate Enrollment Protocol (SCEP), manual enrollment is required.

Table 5: Cisco SD-WAN Manager as CA: Benefits and Limitations

Benefits	Limitations
• Certificate deployment to proxy devices is automated • Certificates are reissued and revalidated before they expire • Certificates can be monitored, tracked, and validated through Cisco SD-WAN Manager	• Cisco SD-WAN Manager certificate needs to be pushed to the client trust store

Configure Cisco SD-WAN Manager as CA

Use **SD-WAN Manager as CA** if your enterprise does not have an internal CA. With this option, Cisco SD-WAN is used as a root CA and is authorized to issue subordinate CAs to the proxy devices at the edge of the network. The certificates issued by the CA can be managed through Cisco SD-WAN Manager .

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
2. Choose **SD-WAN as CA**

Note Leave the **Set SD-WAN as Intermediate CA** check box not checked if you want to set SD-WAN Manager as CA.

3. Enter the requested details: Common Name, Organization, Organizational Unit, Locality, State/Province, Country Code, and Email.
4. Choose the certificate validity period from the drop-down list.
5. Click **Save Certificate Authority**.
6. Configure a firewall policy to inspect and decrypt TLS traffic , on page 12.

Cisco SD-WAN Manager as intermediate CA

Use this option if you have an internal enterprise CA, but would like to use Cisco SD-WAN Manager as intermediate CA to issue and manage subordinate CA certificates.

Table 6: CiscoSD-WAN Manager as Intermediate CA: Benefits and Limitations

Benefits	Limitations

• Certificate deployment to proxy devices is automated • Certificate sare reissued and revalidated before they expire • The risk associated with certificates being compromised is limited as compromised proxy certificates are revoked • Certificates can be monitored, tracked, and validated through Cisco SD-WAN Manager • No other certificates, besides your enterprise CA certificate, need to be pushed to your client trust-store	• Requires manual deployment • Maintaining two CAs causes administrative overload • Cisco SD-WAN Manager certificate usage is tracked through the enterprise CA • Deployment can be complex if your network has multiple Cisco SD-WAN Manager controllers for clusteringor redundancy

Configure SD-WAN Manager as Intermediate CA

Configure Cisco SD-WAN Manager as Intermediate CA to enable a TLS proxy device to use subordinate CA certificates issued by the Cisco SD-WAN Manager .

When Cisco SD-WAN Manager is set as intermediate CA, your enterprise CA acts as the root CA and is designated as the preferred intermediate CA to issue and manage subordinate CA certificates for a proxy device. This option is suitable for enterprises that have their own internal CA but would like to use Cisco SD-WAN Manager to automate and manage certificate issuance and renewal.

1. From the menu, choose **Configuration** > **Certificate Authority**.
2. Choose **SD-WAN Manager as CA.**
3. Check the **Set SD-WAN as Intermediate CA** check box.
4. Upload the CA certificate using the **Select a file** option.

   OR

   Paste the content of the PEM-encoded CA certificate file in the Root Certificate text box.
5. Click **Next**.
6. Under the Generate CSR area, enter the requested details, and click **Generate CSR**.

   The CSR field on the screen populates with the Certificate Signing Request (CSR).
7. Copy or download the CSR and upload it to the enterprise CA server to get it signed by the CA server as the subordinate CA certificate.

Note The process to get a CSR signed by a CA server may differ from one CA to another. Follow your standard procedure to get a CSR signed by your CA.

8. Click **Save Certificate Authority**.

9. Configure a firewall policy to inspect and decrypt TLS traffic , on page 12.

Upload a subordinate CA certificate to TLS proxy

When Cisco SD-WAN Manager is set as intermediate CA, your enterprise CA acts as the root CA and Cisco SD-WAN Manager is designated as the preferred intermediate CA to issue and manage subordinate CA certificates for a proxy device. This option is suitable for enterprises that have their own internal CA but would like to use Cisco SD-WAN Manager to automate and manage certificate issuance and renewal.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
2. Check the **Set vManage as Intermediate CA**checkbox.
3. To upload your PEM-encoded CA certificate. click **Select a file**

   OR

   Paste the CA certificate in the **Root Certificates** box.

   Click **Next**.
4. In the **Intermediate Certificate** text box, paste the content of the signed Cisco SD-WAN Manager certificate, and click **Upload**.

   OR

   Click **Select a file** and upload the CSR generated in the previous step, and click **Upload**
5. Verify that the **Finger Print**, which auto-populates after you upload the CSR, matches your CA certificate.
6. Click **Save Certificate Authority.**

Note When a Cisco public key (PKI) certificate is installed on a device, and you want to make changes to the certificate, detach the embedded security policy from the policy group and push the policy group to the device. This will remove the existing PKI certificate and configuration. After you have made changes to the PKI certificate, re-attach the embedded security policy and then push the policy group to the device. This process updates the device for any the changes to the Cisco PKI certificate

Add devices to a configuration group

Add devices to a Configuration Group.

Procedure

Step 1 Click **...** adjacent to the configuration group name and choose **Edit** >

Step 2 Click **Associated Devices** and then click **Add Devices**

Step 3 Follow the instructions. The selected devices are listed in the **Devices** table.

Configure a firewall policy to inspect and decrypt TLS traffic

Configure a firewall policy that defines the conditions to be met for traffic to flow between zones.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, go to **Configuration** > **Policy Groups** > **Embedded Security** > **Add Security Policy** and follow the steps to configure the firewall policy.

Step 2 **Create a sub-policy for source and destination zone**:

Zones establish the security borders of your network. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network.

Step 3 Create a security policy for inspection, decryption and prevention:

a) **Advanced Inspection Profile:**

An advanced inspection profile is a security inspection profile that includes Cisco UTD security features such as IPS, URLF, AMP, TLS Action, and TLS/SSL Decryption.

b) **Intrusion Prevention:**

This profile when configured detects or stops threats and attacks by flagging suspicious activities.

c) **URL Filtering:**

The URL Filtering profile enables the user to provide controlled access to Internet websites or Intranet sites by configuring the URL-based policies and filters on the device. The user can configure the URL Filtering profiles to manage the web access.

d) **Advanced Malware Protection:**

The AMP profile equips SD-Routing devices to provide protection and visibility to cover all stages of the malware lifecycle.

e) **TLS/SSL Profile:**

This profile lets your configure the action based on the kind of TLS traffic.

f) **TLS/SSL Decryption:**

A decryption policy determines how the system handles encrypted traffic on your network.

The TLS/SSL Decryption Policy can be configured in two ways. You can either configure it from the Embedded Security policy creation page or through the Group of Interest Policy creation page.

Step 4 Click on **Additional Settings** in the Security Policy creation page, to add specific parameters for TLS/SSL decryption.

Step 5 Click **Create New** from the **TLS/SSL Decryption Policy** drop-down to define the decryption policy.

Field Name	Description
Policy Name	Name of the policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	

Field Name	Description
Expired Certificate	Defines what the policy should do if the server certificate has expired. The options are: • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. The options are: • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Certificate Revocation Status	Defines whether the Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate. The options are **Enabled** or **Disabled**.
Unknown Revocation Status	Defines what the policy does, if the OCSP revocation status is **unknown**. • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Unsupported Mode Checks	
Unsupported Protocol Versions	Defines the unsupported protocol versions. • **Drop**: Drop the unsupported protocol versions. • **Decrypt**: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • **Drop**: Drop the unsupported cipher suites. • **Decrypt**: Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are close and open.
Certificate Bundle	Check the **Use default CA certificate bundle** checkbox to use the default CA.
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support. The options are: • **TLS 1.0** • **TLS 1.1** • **TLS 1.2**
Proxy Certificate Attributes	

Field Name	Description
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. The options are: • **1024 bit RSA** • **2048 bit RSA** • **4096 bit RSA**
Ec Key Type	Defines the key type. The options are: • **P256** • **P384** • **P521**
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.

Alternatively, you can also configure a TLS/SSL Decryption Policy using **Policy Group** > **Group of Interest** and add TLS/SSL Decryption Policy. Ensure that you add this policy to the Embedded policy as indicated in Step 4 above.

Step 6 Save the decryption policy.

Add security policy to Policy Group

Associate the Embeded Security Policy created above to the Policy Group. To do so:

Procedure

Step 1 Click **Policy Group** to create a new policy group. A policy group logically groups policies that can be applied to one or more sites or devices at the site in the network

Step 2 Specify **Policy Group Name** and select solution type as **SD-Routing**. Enter a description for the Policy Group. Click **Create**.

Step 3 Select an embedded security policy from the drop-down list. The embedded security policy includes policies for encryption, firewall, intrusion prevention, URL filtering, and malware.

Step 4 Click **Save** to save your configuration.

Step 5 Click the pencil icon to select a device to associate with the policy group. This association ensures that when you deploy this Policy group to a device, the device inherits all the policies associated with this Policy Group.

Step 6 Click **Deploy** to select sites and deploy the policy group.

Verify TLS proxy configuration

Use the following commands to verify the configuration for TLS proxy.

show sd-routing running	In Cisco SD-WAN Manager, run this command verify if your configuration is applied.
show sd-routing running-config	In Cisco SD-WAN Manager, run this command the device CLI through SSH
show crypto pki status	On your device CLI, run this command to verify PROXY-SIGNING-CA is present and configure device.
show sslproxy statistics	On your device CLI, run this command to view T
show sslproxy status	On your device CLI, run this command to verify was successfully configured and is enabled on C Manager. In the output , Clear Mode: FALSE denotes that successfully configured and enabled on Cisco S
show platform hardware qfp active feature utd config	On your device CLI, run this command to verify
show sd-routing running-configuration|section utd-tls-decrypt	On your device CLI, run this command to verify
show utd engine standard config	On your device CLI, run this command to verify
show utd engine standard status	On your device CLI, run this command to verify