Security Compliance

Overview

Cisco Unified Border Element (CUBE) is Common Criteria (CC) and The Federal Information Processing Standards (FIPS) certified. The certification is applicable to CUBE on Cisco CSR 1000vCisco CSR 8000v platform only.

Common Criteria (CC)

Common Criteria (CC) is a global security standard to which security products are evaluated. Common Criteria product certifications are mutually recognized by 28 nations, thus an evaluation that is conducted in one country is recognized by the other countries.

The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) that guarantees product security. The organizations (Government or Enterprise IT) specify functional and assurance requirements, the vendors claim and develop specific product qualities. The testing facilities examine products to determine whether they meet those vendor claims. Common Criteria guarantees that the process of specification, execution and assessment of a product has been conducted in a stringent and standardized manner.

The Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module should be a set of hardware, software, firmware, or some combination that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain crypto algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

Feature Information

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information

Feature Name	Releases	Feature Information
Common Criteria (CC) and The Federal Information Standards (FIPS) Certification.	Cisco IOS XE Fuji Release 16.9.1	Common Criteria (CC) and The Federal Information Standards (FIPS) Certification for CUBE on Cisco CSR 1000v.

Supported Hardware and Software for Virtual CUBE

For details on prerequisites for Virtual CUBE, see Supported Hardware and Software for Virtual CUBE.

Common Criteria Configuration on Cisco CSR 1000v and C8000v

Enable Common Criteria Mode

Before you begin

- Delete existing certificates.
- Remove existing crypto keys.
- Remove existing TLS configuration (TLS version and Cipher Suites).

Step 1 **enable**

Example:

```
Router# enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **cc-mode**

Example:

```
Router(config)# cc-mode
```

Enables common criteria configuration mode.

What to do next

Common Criteria (CC) mode enforces certain security checks for cryptographic protocols such as Transport Layer Security (TLS). CUBE uses TLS to secure signaling over SIP and HTTP client for XCC providers. Configure SIP TLS and HTTP TLS in the Common Criteria (CC) mode.

SIP TLS Configuration

SIP TLS Configuration Task Flow

Following are the steps to configure SIP TLS on your Cisco CSR 1000v router in Common Criteria mode.

1. Generate RSA Public Key, on page 3
2. Configure Certificate Authority Server, on page 4
3. Configure CSR Trustpoint, on page 5
4. Configure Peer Trustpoint, on page 6
5. Add Client Verification Trustpoint, on page 7
6. Enforce Strict SRTP, on page 8

Generate RSA Public Key

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **crypto key generate rsa label** *key-label* **modulus** *modulus-size*

Example:

```
Router(config)#crypto key generate rsa general-keys label CUBE modulus 3072
```

Generates a public RSA key that is used with your CSR certificate.

- The *key-label* specifies the name that is used for an RSA key pair when they are exported.
- The *modulus-size* specifies the size of the key modulus. By default, the modulus of a Certification Authority (CA) key is 1024 bits. The size of the key modulus must be 2048 bits or higher, for it to be Common Criteria compliant.

Step 4 **exit**

Example:

```
Router(config)#exit
```

Exits global configuration mode.

Configure Certificate Authority Server

Step 1 **enable**

Example:

```
Router# enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki server** *cs-label*

Example:

```
Router(config)# crypto pki server CUBE
```

Defines a label for the Certificate Server and enters the certificate server configuration mode.

Note If you have generated the RSA key pair manually using the command **crypto key generate rsa label** *key-label* **modulus** *modulus-size* , the *cs-label* must match with the *key-label*, otherwise a certificate with the default key size of 1024 bits is generated.

Step 4 **database level complete**

Example:

```
Router(cs-server)# database level complete
```

Writes each issued certificate to the certificate enrollment database.

Step 5 **grant auto**

Example:

```
Router(cs-server)# grant auto
```

Automatically grants reenrollment requests for subordinate Certificate Authority (CA) server or Registration Authority (RA) mode Certificate Authority (CA).

Step 6 **hash sha384**

Example:

```
Router(cs-server)# hash sha384
```

Sets the hash function SHA-384 for the signature that the Cisco IOS Certificate Authority (CA) uses to sign all the certificates that are issued by the server.

Step 7 **no shut**

Example:

```
Router(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password:

Re-enter password:

% Generating 3072 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.
```

Enables or reenables the certificate server. If the subordinate certificate server is enabled for the first time, the certificate server generates the key and receives its signing certificate from the root certificate server.

After entering the passphrase (when prompted), the certificate server is enabled. This passphrase protects the private key.

Step 8 **exit**

Example:

```
Router(cs-server)# exit
```

Exits certificate server configuration mode.

Configure CSR Trustpoint

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki trustpoint** *name*

Example:

```
Router(config)#crypto pki trustpoint CUBE-TLS
```

Declares the trustpoint with the name specified and enters trustpoint configuration mode. This trustpoint is used by your Router application for the TLS communication.

Step 4 **hash sha384**

Example:

```
Router(ca-trustpoint)#hash sha384
```

Sets the hash function SHA-384 for the signature that the Cisco IOS Certificate Authority (CA) uses to sign all the certificates that are issued by the server.

A trustpoint with sample CSR certificate with subject-name "CN=Secure-Router" and "rsakeypair Router" is given below. The "rsakeypair label" must match with the label of the RSA keys that are generated in the earlier steps.

```
crypto pki trustpoint CUBE-TLS
 enrollment url http://X.X.X.X:80
 serial-number none
 fqdn none
 ip-address none
 subject-name CN=Secure-CUBE
 revocation-check none
 rsakeypair Router
```

Step 5 **exit**

Example:

```
Router(ca-trustpoint)# exit
```

Exits trustpoint configuration mode.

Configure Peer Trustpoint

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki trustpoint** *name*

Example:

```
Router(config)#crypto pki trustpoint xyzname
```

Declares the peer trustpoint with the name specified and enters trustpoint configuration mode.

Step 4 **enrollment terminal**

Example:

```
Router(ca-trustpoint)#enrollment terminal
```

Specifies manual certificate enrollment via the cut-and-paste method for trustpoint peers. The certificate request displayed on the console terminal can be manually copied.

Step 5 **revocation-check none**

Example:

```
Router(ca-trustpoint)#revocation-check none
```

Specifies that the certificate check is ignored.

Step 6 **exit**

Example:

```
Router(ca-trustpoint)#exit
```

Exits trustpoint configuration mode.

Add Client Verification Trustpoint

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **sip-ua**

Example:

```
Router(config)#sip-ua
```

Enters SIP User Agent configuration mode to configure SIP-UA related commands.

Step 4 **crypto signaling remote-addr** *remote ip address remote ip mask* **trustpoint** *CUBEs trustpoint label* **client-vtp** *verification trustpoint*

Example:

```
Router(config-sip-ua)#crypto signaling remote-addr X.X.X.X 255.255.255.255 trustpoint CUBE-TLS
client-vtp CUBE-VERIFY
```

Assigns a client verification trustpoint to SIP-UA. This client verification trustpoint is used to send Distinguished Name (DN) of the Certificate Authority (CA) server in the CUBE's client certificate request.

Step 5 **exit**

Example:

```
Router(config-sip-ua)#exit
```

Exits sip-ua configuration mode.

Enforce Strict SRTP

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **voice service voip**

Example:

```
Router(config)#voice service voip
```

Enters voice service configuration mode and specifies the encapsulation method as VoIP.

Step 4 **srtp**

Example:

```
Router(conf-voi-ser)#srtp
```

Enforces SRTP to secure the call flow through CUBE.

Step 5 **exit**

Example:

```
Router(conf-voi-ser)#exit
```

Exits voice service configuration mode.

HTTPS TLS Configuration

HTTPS TLS Configuration Task Flow

Following are the steps to configure HTTPS TLS on your Cisco CSR 1000v router in Common Criteria mode.

1. Prepare Cisco CSR 1000v Router's HTTP Server to Run in CC Mode, on page 9
2. Create Certificate Map for HTTPS Peer Trustpoint, on page 10
3. Configure HTTPS TLS Version, on page 11
4. Configure Supported Cipher Suites, on page 12
5. Apply Certificate Map to HTTPS Peer Trustpoint, on page 12

Prepare Cisco CSR 1000v Router's HTTP Server to Run in CC Mode

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **ip http server** *name*

Example:

```
Router(config)#ip http server
```

Enables the HTTP server on the Cisco CSR 1000v router, allowing the use of Cisco web browser UI to monitor the router and issue commands to it.

Step 4 **ip http authentication local**

Example:

```
Router(config)#ip http authentication local
```

Specifies the authentication method for HTTP server users. The keyword **local** indicates that the username, password, and privilege level access combination that is specified in the local system configuration should be used for authentication and authorization.

Step 5 **ip http secure-server**

Example:

```
Router(config)#ip http secure-server
```

Enables a secure HTTP server on the Cisco CSR 1000v router.

Step 6 **ip http secure-trustpoint** *trustpoint-name*

Example:

```
Router(config)#ip http secure-trustpoint CUBE-TLS
```

Specifies the trustpoint that is used for obtaining signed certificates for a secure HTTP server on the Cisco CSR 1000v router.

Step 7 **ip http secure-client-auth**

Example:

```
Router(config)#ip http secure-client-auth
```

Configures the HTTP server to request an X.509v3 certificate from the client to authenticate the client during the connection process.

Step 8 **ip http secure-peer-verify-trustpoint** *client's issuer*

Example:

```
Router(config)#ip http secure-peer-verify-trustpoint secure-clientissuer
```

Configures the client verification trustpoint for the HTTP server on the Cisco CSR 1000v router. This peer verification trustpoint is used to send Distinguished Name (DN) of Certificate Authority (CA) in the client certificate request during the TLS handshake of HTTP.

Step 9 **exit**

Example:

```
Router(config)#exit
```

Exits the global configuration mode.

Create Certificate Map for HTTPS Peer Trustpoint

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki certificate map** *label sequence-number*

Example:

```
Router(config)#crypto pki certificate map cubemap 10
```

Creates a certificate map that defines certificate-based Access Control Lists (ACLs) and enters the certificate map configuration mode. The *sequence-number* orders the ACLs with the same label. ACLs with the same label are processed from the lowest to the highest sequence number. When an ACL is matched, the processing stops with a successful result.

Step 4 **alt-subject-name eq** *match-value*

Example:

```
Router(ca-certificate-map)#alt-subject-name peername
```

Specifies the certificate fields with their matching criteria in the certificate map configuration mode. The alternate subject name that is specified in the map must be present in SAN extension of the peer id certificate.

Step 5 **exit**

Example:

```
Router(ca-certificate-map)#exit
```

Exits certificate map configuration mode.

Configure HTTPS TLS Version

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **ip http tls-version** *version*

Example:

```
Router(config)#ip http tls-version TLSv1.2
```

Configures the specified TLS version for HTTPS. Configure TLSv1.1 or TLSv1.2 to be Common Criteria compliant.

Step 4 **exit**

Example:

```
Router(config)#exit
```

Exits global configuration mode.

Configure Supported Cipher Suites

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **ip http secure-ciphersuite** *supported cipher suites*

Example:

```
Router(config)#ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
```

Specifies the cipher suites that are used for encryption over the secure HTTP connection between the client and the HTTP server. Common Criteria supports the cipher suites that are given in the preceding example. Configure all the cipher suites if you are not aware of the client cipher support.

Step 4 **exit**

Example:

```
Router(config)#exit
```

Exits global configuration mode.

Apply Certificate Map to HTTPS Peer Trustpoint

Step 1 **enable**

Example:

```
Router#enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki trustpoint** *name*

Example:

```
Router(config)#crypto pki trustpoint CUBE-HTTPS
```

Declares the HTTPS peer trustpoint for the Cisco CSR 1000v router.

Step 4 **match certificate** *map name*

Example:

```
Router(ca-trustpoint)#match certificate cubemap
```

Associates the certificate map that is defined by using the **crypto pki certificate map** command with the HTTPS trustpoint. The *map name* argument in the **match certificate** command must match the *label* argument that is specified in the previously defined **crypto pki certificate map** command.

Step 5 **match eku** *attribute*

Example:

```
Router(ca-trustpoint)#match eku client-auth server-auth
```

Allows the HTTPS peer which acts as a client and a server to validate a peer certificate only if the specified Extended Key Usage (EKU) attribute is present in the certificate. If the Cisco CSR 1000v router is a client, then you must configure server-auth. If Cisco CSR 1000v router is a server, then you must configure client-auth.

Step 6 **exit**

Example:

```
Router(ca-trustpoint)#exit
```

Exits trustpoint configuration mode.

NTP Configuration Restrictions in Common Criteria Mode

In Common Criteria mode, the following restrictions are applicable to NTP configuration.

- Do not configure NTP version 1 and 2. Following are the NTP version commands.
  - **ntp server** *ip-address* **prefer source** *interface* **version** *version*
  - **ntp peer** *ip-address* **version** *version*
- Do not configure NTP broadcast. Following are the NTP broadcast commands.
  - **ntp broadcast delay** *delay-timer*
  - **ntp broadcast client**
  - **ntp broadcast destination** *ip-address*
  - **ntp broadcast destination** *ip-address* **key** *key*

  - **ntp broadcast destination** *ip-address* **key** *key* **version** *version*
  - **ntp broadcast version** *version*

- Do not configure NTP multicast command **ntp multicast version** *version*.

FIPS Configuration on Cisco CSR 1000v and C8000v

Configuration Requirements for FIPS Compliance

There is no specific command to enable FIPS mode. For the Virtual CUBE on the Cisco CSR 1000v router to be FIPS-compliant, the following commands must be configured.

- **crypto key generate rsa modulus** *modulus-size*

  The *modulus-size* varies from 360 bits to 4096 bits. The size of the RSA key must be 2048 bit or higher for FIPS compliance.

- The Hash Algorithms that are configured using the command **hash sha384** under the configured trustpoint and the crypto pki server on the CSR must use sha384 or greater, namely sha512.