



IPsec Security Support

IPsec is a security framework of open standards developed by the IETF. IPsec enables security for information that is sent over unprotected networks. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

- [Finding Feature Information, on page 1](#)
- [Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1](#)
- [IPsec Security Support, on page 2](#)
- [IPsec Security Limitations, on page 3](#)
- [Configuring IPsec Security, on page 3](#)
- [Configuring Transform Sets for IKEv2, on page 4](#)
- [Feature Information for IPsec Security Support, on page 6](#)

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/>. An account on <http://www.cisco.com/> is not required.

Hardware Compatibility Matrix for the Cisco cBR Series Routers



Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	Cisco IOS-XE Release 16.5.1 and Later Releases Cisco cBR-8 Supervisor: <ul style="list-style-type: none"> • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G 	Cisco IOS-XE Release 16.5.1 and Later Releases Cisco cBR-8 CCAP Line Cards: <ul style="list-style-type: none"> • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: <ul style="list-style-type: none"> • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: <ul style="list-style-type: none"> • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: <ul style="list-style-type: none"> • PID—CBR-D31-US-MOD

IPsec Security Support

Cisco IOS XE Amsterdam 17.2.x provides limited support for up to 16 Gbps encrypted IPsec that is sent or forwarded by cBR8.

IPsec is a security framework of open standards developed by the IETF. IPsec enables security for information that is sent over unprotected networks. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

IPsec is mainly for securing lawful intercept (LI) traffic from cBR8 to MAC Domain profile. The IPsec feature now supports:

- AES-CBC-128 encryption

- HMAC-SHA-256 authentication
- ESP tunnel mode
- IKEv2 with certificate or preshared key
- PFS (Perfect Forward Secrecy)

IPsec Security Limitations

The IPsec feature for Cisco IOS XE Amsterdam 17.2.1 has the following limitations:

- Only supported on SUP 160.
- The RX path of IPsec tunnel only supports minimum control traffic. The traffic is punted to IOSd, and is heavily rate-limited. The default limit is 200 packets/second (configurable).

Configuring IPsec Security

To configure the IPsec security, complete the following steps:

1. Use the **crypto ipsec transform-set <ts-name> esp-aes esp-sha256-hmac** command. However, note that only the following options are supported:
 - Support for **esp-aes esp-sha256-hmac**
 - Support for *mode tunnel*

You can optionally use **set pfs <dh-group-name>** to enable perfect forward secrecy in IPsec profile.

2. Use the **crypto ipsec profile <profile-name>**, where the IKEv2 profile is set into IPsec profile.
3. Use the **tunnel protection ipsec profile** tunnel interface.

To view your IPsec information, use the **show crypto ipsec sa detail** command:

```
Router# show crypto ipsec sa detail
Load for five secs: 3%/0%; one minute: 8%; five minutes: 4%
Time source is NTP, 12:40:49.195 EDT Wed Feb 26 2020

interface: Tunnel101
  Crypto map tag: Tunnel101-head-0, local addr 102.0.0.2

protected vrf: (none)
local ident (addr/mask/prot/port): (102.0.0.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (102.0.0.1/255.255.255.255/47/0)
current_peer 102.0.0.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
```

```

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (rcv) 0, #pkts verify failed: 0
#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts tagged (send): 0, #pkts untagged (rcv): 0
#pkts not tagged (send): 0, #pkts not untagged (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 102.0.0.2, remote crypto endpt.: 102.0.0.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb TenGigabitEthernet4/1/0
current outbound spi: 0xBD3A2CBF(3174706367)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xC67787E8(3329722344)
  transform: esp-aes esp-sha256-hmac ,
  in use settings =(Tunnel, )
  conn id: 2, flow_id: SW:2, sibling_flags FFFFFFFF80000040, crypto map:
Tunnel101-head-0
  sa timing: remaining key lifetime (k/sec): (4242079/86293)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xBD3A2CBF(3174706367)
  transform: esp-aes esp-sha256-hmac ,
  in use settings =(Tunnel, )
  conn id: 1, flow_id: SW:1, sibling_flags FFFFFFFF80000040, crypto map:
Tunnel101-head-0
  sa timing: remaining key lifetime (k/sec): (4242079/86293)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

```

Configuring Transform Sets for IKEv2

You can choose to configure the IKEv2 using either of the following options:

- IKEv2 with pre-shared key. This includes the following options:
 - **crypto ikev2 proposal** <proposal-name>.
 - **crypto ikev2 policy** <policy-name>
 - **crypto ikev2 keyring** <keyring-name>

Set keyring in IKEv2 profile. A configuration example using IKEv2 with pre-shared key is as shown:

```

crypto ikev2 proposal li-ikev2-proposal
  encryption aes-cbc-128
  integrity sha256

```

```

group 5 2
crypto ikev2 policy li-ikev2-policy
match address local 102.0.0.2
proposal li-ikev2-proposal
crypto ikev2 keyring li-kyr
peer li-peer
address 102.0.0.1 255.255.255.0
identity address 102.0.0.2
pre-shared-key key1
!
crypto ikev2 profile li-profile
match address local interface TenGigabitEthernet4/1/7
match identity remote address 102.0.0.1 255.255.255.255
authentication remote pre-share
authentication local pre-share key key1
keyring local li-kyr
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec profile li-ipsec-gre
set security-association lifetime seconds 86400
set transform-set TS
set pfs group14
set ikev2-profile li-profile

```

- IKEv2 with certificate authority. This includes the following steps:

1. Generate the RSA key pair.
2. Configure the PKI trustpoint. This requires the CA server supporting SCEP (Simple Certificate Enrollment Protocol).

Configure **crypto pki trustpoint** to enroll to CA. Note that the *subject-name* will be used for authentication in the example

3. Set the certificate map in IKEv2 profile by configuring **crypto pki certificate map <map-name> <id>** to match the certificate content.
4. Enroll the certificate.

To view your IPsec information, use the **show crypto ikev2 sa detail** command:

```

Router# show crypto ikev2 sa detail
Load for five secs: 3%/0%; one minute: 8%; five minutes: 4%
Time source is NTP, 12:40:57.672 EDT Wed Feb 26 2020

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 102.0.0.2/500 102.0.0.1/500 none/none READY
Encr: AES-CBC, keysize: 128, PRF: SHA256, Hash: SHA256, DH Grp:5, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/115 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: A3C274EBBD7FFF2F Remote spi: AA160367FFD29C2D
Local id: hostname=tb34-cBR8.cisco.com,cn=ANSSI Test CBR8
Remote id: hostname=cCMTS-bcl-ASR1K6-2,cn=ANSSI Test ASR1K
Local req msg id: 2 Remote req msg id: 0
Local next msg id: 2 Remote next msg id: 0
Local req queued: 2 Remote req queued: 0
Local window: 5 Remote window: 5

```

```

DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Dynamic Route Update: enabled
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

```

```
IPv6 Crypto IKEv2 SA
```



Note The IPsec and IKEv2 are configured in the same way as ASR 1000. Go through the [ASR 1000 Internet Key Exchange for IPsec VPNs Configuration Guide](#) for more information. The following limitations apply:

- Supported encryption
- Authentication algorithms
- ESP tunnel mode

Feature Information for IPsec Security Support

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the <https://cfng.cisco.com/> link. An account on the Cisco.com page is not required.



Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for IPsec Security Support

Feature Name	Releases	Feature Information
IPsec Security Support	Cisco IOS XE Amsterdam 17.2.1	This feature was integrated into Cisco IOS XE Amsterdam 17.2.1 on the Cisco cBR Series Converged Broadband Routers.