Implementing IPSec

IP Security (IPSec) provides security for transmission of sensitive management information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers.

IPSec for management traffic

An IPSec for management-plane feature is a platform-native capability that

- supports management protocols, including SSH, SNMP, syslog, and NETCONF.
- uses IKEv2 and IPSec with Tunnel MA and associated virtual tunnel interfaces to provide encryption on the route processor and support VRF-aware operation, and
- integrates with IOS XR tunnel infrastructure and cryptographic profiles to protect management traffic.

IPSec management traffic is processed on the route processor and is not a line-card capability. This release supports IPv4 management traffic only.

Table 1: Table 1. Feature History Table

Feature Name	Release Information	Feature Description
IPSec for management traffic	Release 26.3.1	Introduced in this release on: NCS 5500 fixed port routers (select variants only*); NCS 5700 fixed port routers (select variants only*); NCS 5500 modular routers IPSec for management traffic protects eligible management traffic generated by or destined for the router. The feature uses IKEv2, IPSec, Tunnel MA, and associated virtual tunnel interfaces. *This feature is supported on NCS 5500: • NCS-5501 • NCS-5501-SE • NCS-55A1-36H • NCS-55A1-24Q6H-S • NCS-55A1-24Q6H • NCS-55A1-48Q6H • NCS-55A2-MOD-S *This feature is supported on NCS 5700: • NCS-57B1-6D24 • NCS-57B1-5DSE • NCS-57C1-48Q6 • NCS-57D2-18DD

Management traffic through an IPSec tunnel

IPSec tunnels protect management traffic routed through supported tunnel interfaces. Correct configuration of IKEv2 and IPSec parameters on both routers is required before establishing a security association.

The release enables the existing IPSec management-traffic workflow on supported platforms. The configuration and verification workflow is unchanged.

Depending on the platform and hardware variant, IPSec management tunnels are supported through either the management interface only or through both the management interface and data ports.

The protected management traffic can include these protocols:

- SSH or CLI access

- SNMPv3, syslog, and NETCONF

Note An IPSec tunnel failure or stateless IPSec process restart can result in packet loss.

IPSec management traffic support and restrictions

This information identifies IPSec management-traffic support and restrictions.

Table 2: IPSec management traffic restrictions

Restriction	Requirement
IP traffic	Configure IPSec management traffic for IPv4 traffic only.
IPSec mode	Configure IPSec in tunnel mode.
Traffic direction	Protect management traffic generated by or destined for the router.
SSH authentication through an IPSec tunnel	If SSH authentication traffic uses the IPSec tunnel, configure `default-route software-forwarding` in the VRF that contains the tunnel. Use the default VRF for a tunnel in the global routing table; otherwise, use the user-defined VRF associated with the tunnel.
Peer configuration	Configure compatible IKEv2 and IPSec parameters, including the same preshared key when you use preshared-key authentication, on both peers.
RP switchover on dual-RP modular chassis for supported platforms	An IPSec tunnel that uses the active RP physical management-interface address as its source is disrupted after an RP switchover.

Table 3: Cryptographic requirements

Function	Required values
IPSec security association	AES-CBC-256 encryption, SHA-256 or SHA-384 integrity, and PFS group 20.
IKEv2 security association	AES-GCM-256 or AES-CBC-256 encryption, SHA-256 or SHA-384 integrity and PRF, and DH group 20.
IKEv2 authentication	Preshared key or X.509 certificate authentication that uses RSA or ECDSA.

Note For dual-RP modular chassis, configure a virtual IP address as the IPSec tunnel source to maintain management connectivity after an RP switchover. For the virtual IP address configuration procedure, see Configure the management port.

Configure IPSec for management traffic

Secure management-plane protocols by encrypting device-originated and inbound management traffic over untrusted networks.

Management-plane IPSec uses native IOS XR features to deliver end-to-end encryption for management traffic. This solution uses IKEv2, IPSec, Tunnel MA, and associated virtual tunnel interfaces to protect management traffic.

Before you begin

- Verify your router series supports IPSec management traffic.
- IPSec functionality is included in the K9sec package.
- Verify reachability to the peer router.
- Identify the management VRF and IP addresses for management traffic.
- Ensure you have the peer address and preshared key.
- Preconfigure IKEv2 profiles on both initiator and responder for tunnel establishment.
- Have peer device and tunnel destination details available.

Follow these steps to configure IPSec for management traffic

Procedure

Step 1 Configure the IKEv2 proposal to define the security parameters.

Example:

```
Router# config
Router (config)# ikev2 proposal <proposal-name> prf sha-256
Router (config)# ikev2 proposal <proposal-name> dh-group 20
Router (config)# ikev2 proposal <proposal-name> integrity sha-256
Router (config)# ikev2 proposal <proposal-name> encryption aes-cbc-256
Router (config)# commit
```

Step 2 Configure the IKEv2 policy to specify matching criteria and proposal.

Example:

```
Router# config
Router (config)# ikev2 policy <policy-name> match address local <local-peer-address>
Router (config)# ikev2 policy <policy-name> match fvrf any
Router (config)# ikev2 policy <policy-name> proposal <proposal-name>
Router (config)# commit
```

Step 3 Configure the IKEv2 keyring with the peer address and preshared key.

Example:

```
Router# config
Router (config)# keyring <keyring-name> peer <peer-name> address <peer-address> <mask>
Router (config)# keyring <keyring-name> peer <peer-name> pre-shared-key <preshared-key>
Router (config)# commit
```

Use the same preshared key on both IPSec peers.

Step 4 Configure the IKEv2 profile and specify authentication and peer matching.

Example:

```
Router# config
Router (config)# ikev2 profile <ikev2-profile-name> keyring <keyring-name>
Router (config)# ikev2 profile <ikev2-profile-name> lifetime <seconds>
Router (config)# ikev2 profile <ikev2-profile-name> authentication local pre-shared
Router (config)# ikev2 profile <ikev2-profile-name> match identity remote address <peer-address>
<mask>
Router (config)# commit
```

Step 5 Configure the IPSec transform set to define encryption and authentication methods.

Example:

```
Router# config
Router (config)# ipsec transform-set <transform-set-name> mode tunnel
Router (config)# ipsec transform-set <transform-set-name> transform esp-256-aes esp-hmac-sha-256
Router (config)# commit
```

Step 6 Configure the IPSec profile and reference the IKEv2 profile and transform set.

Example:

```
Router# config
Router (config)# ipsec profile <ipsec-profile-name> set ikev2-profile <ikev2-profile-name>
Router (config)# ipsec profile <ipsec-profile-name> set pfs group20
Router (config)# ipsec profile <ipsec-profile-name> set security-association lifetime seconds <seconds>
Router (config)# ipsec profile <ipsec-profile-name> set transform-set <transform-set-name>
Router (config)# commit
```

To configure a responder-only router, enter `ipsec profile ipsec_prof_mgmt_P1 set responder-only` and `commit`. A responder-only router waits for the peer to initiate the IPSec session.

Step 7 Configure the IPSec tunnel interface for management traffic.

Example:

```
Router# config
Router (config)# interface <tunnel-interface> ipv4 address <tunnel-ip-address> <mask>
Router (config)# interface <tunnel-interface> tunnel mode ipsec ipv4
Router (config)# interface <tunnel-interface> tunnel source <local-peer-address>
Router (config)# interface <tunnel-interface> tunnel destination <peer-address>
Router (config)# interface <tunnel-interface> tunnel protection ipsec profile <ipsec-profile-name>
Router (config)# commit
```

Step 8 Route management traffic through the IPSec tunnel.

Use the deployment routing design to send management traffic generated by or destined for the router through tunnel-ip1.

Management traffic is protected by an IKEv2-negotiated IPSec tunnel, securing protocols such as SSH, SNMP, SYSLOG and NETCONF. Verify tunnel establishment by confirming IKEv2 sessions and IPSec security associations.

What to do next

- Test tunnel connectivity and verify management traffic is encrypted.
- Monitor IPSec tunnel status for successful negotiation and traffic flows.

Verify IPSec management traffic

Confirm that the management tunnel established IKEv2 and IPSec security associations.

Management tunnels use IKEv2 and IPSec security associations to protect remote management traffic. Verifying these associations helps ensure secure, reliable connectivity between management devices.

Before you begin

- Ensure you have configured IPSec management traffic on the device
- Confirm the peer device is reachable and available to establish the tunnel.

Follow these steps to verify management-plane IPSec security associations:

Procedure

Step 1 Display the IKEv2 session summary.

Example:

```
Router# show ikev2 summary
```

Confirm that the summary identifies active IKEv2 security associations and no unexpected negotiation state.

Step 2 Display the IKEv2 session state and details.

Example:

```
Router# show ikev2 session
Router# show ikev2 session detail
```

Confirm that Status displays UP-ACTIVE and Status(Description) displays READY (Negotiation done). Review the negotiated encryption, PRF, Diffie-Hellman group, and authentication values.

Step 3 Display the IPSec security associations.

Example:

```
Router# show ipsec sa
```

Confirm that the output lists the tunnel interface and inbound and outbound security parameter indexes.

Step 4 Display detailed IPSec security-association information for the tunnel interface.

Example:

```
Router# show ipsec sa interface <tunnel-interface>
```

Confirm that the output identifies tunnel mode and displays inbound and outbound security associations.

If all associations are confirmed as active, your IPSec management tunnel is correctly established and secure.

If any associations are missing or inactive, review configuration steps or troubleshooting logs and repeat the checks.