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.

IP Security for Management Traffic

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Support for FQDN Identity in IKEv2	Release 24.3.1	You can now configure the IKEv2 profile and keyring commands to allow IPSec peers to identify themselves using the FQDN or domain names. Before Cisco IOS XR Release 24.2.1, IPsec peers identified each other through their IP addresses. The command **Ikev2 profile** supports the following options: • **remote fqdn | fqdn domain** • **local fqdn** The **keyring** command supports the following keyword and options: • **identity fqdn | fqdn domain**

Feature Name	Release Information	Feature Description
IP Security (IPSec) for Management Traffic	Release 7.8.1	You can now use IP Security (IPSec), a protocol suite that authenticates and encrypts packets of data to provide secure communication over an unprotected network for all management traffic flows between routers. This feature introduces the following commands: • **ikev2 policy** • **ikev2 profile** • **ikev2 proposal** • **ipsec profile** • **ipsec transform-set** • **keyring** • **show ikev2 session detail** • **show ikev2 session** • **show ikev2 summary** • **show ipsec sa** This feature modifies the **tunnel mode** command for tunneled interfaces.

Note The IPSec and IKEv2 commands apply to the below listed Cisco NCS 540 series routers only:

- N540X-12Z16G-SYS-D
- N540X-12Z16G-SYS-A

The key components in IPSec are as follows:

- **IPSec Profile**: The IPSec profile consists of the details about the Internet Key Exchange Version 2 (IKEv2) profile and transform set for IPSec communication.
- **Transform Set**: A transform set includes the encapsulation mode and Encapsulating Security Payload (ESP) transform needed for the IPSec network.
- **IKEv2 Profile**: The IKEv2 profile details the keyring, lifetime period of the security association (SA), authentication method for identifying the IPSec Peer, and the IP address or Fully Qualified Domain Name (FQDN) or Domain Name of the IPSec Peer. IKEv2 profile supports both Preshared Secret Keys (PSK) and X.509v3 Certificate (RSA Signature) based authentication.

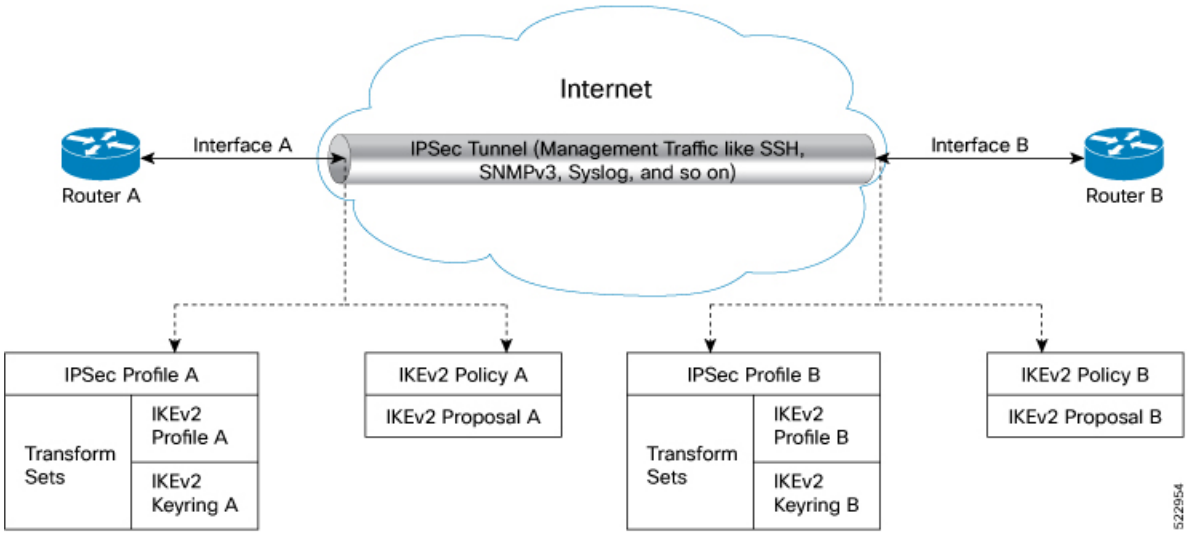
- **IKEv2 Keyring**: The IKEv2 keyring consists of the preshared keys along with the IP address or FQDN or Domain Name for IKEv2 negotiations used to establish the peer tunnel.

Note IKE profiles support multiple IPv4 addresses or FQDNs as remote identities. If multiple profiles have the same remote identity, an incoming IKE initiator request can potentially match any of these profiles. The profile configuration, such as keyring peer entry or authentication methods, must be consistent with the initiator's configuration. Any discrepancy between the initiator and responder configurations will result in the IKE negotiation failing to establish a connection.

- **IKEv2 Policy**: The IKEv2 policy consists of the proposals that detail the encryption, integrity, pseudo-random function (PRF) algorithms, and Diffie-Hellman (DH) group in the IKE SAs exchange along with the IP address for the IPSec tunnel interface.
- **IKEv2 Proposal**: The IKEv2 proposal consists of the parameters for negotiation of Internet Key Exchange (IKE) security associations (SA). The parameters used in the IKE SA negotiation are encryption, integrity, PRF algorithms, and dh-group.

In the IPSec feature, a tunnel is established between the peer routers and all management traffic packets flows through it. The IPSec tunnel is created over the physical interfaces in the peer routers. The individual tunnel interfaces in the routers are associated with an IPSec profile. Overall the IPSec profile details the information regarding the parameters used for encapsulation or decapsulation along with the authentication parameter that ensures the packets following in the tunnel are secure to be transmitted over unprotected networks.

Figure 1: IPSec for Management Traffic Flow Between Two Routers



When you configure the IPSec features on Interface A in Router A and Interface B in Router B, this feature ensures all the management traffic flowing between interfaces A, and B is encrypted and transferred through a virtual IPSec tunnel. The routers use the IPSec profile to establish a virtual IPSec tunnel and for traffic encryption and decryption. The IPSec configuration on interface A contains the source address (IP address for interface A), source interface type, destination address (IP address for interface B), IPSec profile, and tunnel mode. Similar parameters are available in the IPSec configuration for interface B. Further interfaces A and B negotiate the conditions to establish the virtual IPSec tunnel. This negotiation is encrypted and

decrypted using the IKEv2 Policy. The IKEv2 Policy includes the local interface address and the IKEv2 Proposal. The IKEv2 Proposal has the traffic type, authentication, encryption, integrity, Pseudo-Random Function (PRF), and DH-Group values. After successfully establishing the virtual IPSec tunnel, the peer interfaces (Interfaces A and B) authenticate each other using the keyring value obtained from the IKEv2 Profile. Once authentication is complete, all the management traffic between interface A and B flow through the virtual IPSec tunnel until the keyring expiry. The management traffic following through the IPSec virtual tunnel is encrypted using the Transform Set. The Transform Set includes the IPSec data communication mode and encryption algorithm.

Feature Highlights

- IPSec feature works on virtual tunnel interfaces (VTI) as the endpoints of the virtual network. All traffic passing through a tunnel interface is sent to the IPSec processing. All traffic matching the IPSec criteria routes into a VTI interface via static or dynamic routing rules
- IPSec feature can be applied to any number of interfaces in the router, given you configure the IPSec feature on both the endpoints.
- The IPSec feature supports the following security features:
  - IKEv2 Negotiations for virtual IPSec tunnel:
    - **Encryption algorithms:** AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, and AES-GCM-256
    - **Authentication methods:** Preshared Secret Keys (PSK) and X.509v3 Certificate (RSA Signature)
    - **Integrity algorithms:** HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512
    - **Pseudo Random Functions:** HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512
    - **Diffie-Hellman(DH) Group:** 19, 20, and 21
  - Management traffic flow:
    - **Encryption algorithms:** AES-CBC-128, AES-CBC-192, and AES-CBC-256
    - **Integrity algorithms:** HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512
    - **Perfect Forward Secrecy (PFS)- Diffie-Hellman(DH) Group:** 19, 20, and 21

Restrictions for IP Security for Management Traffic

The following are some basic restrictions and limitations of the IPSec feature:

- IPSec feature is supported only on N540X-12Z16G-SYS-A chassis.
- IPsec feature is available for IPv4 traffic only.
- IPSec feature is available only in tunnel mode.
- IPSec is supported only on locally sourced traffic.
- IPSec feature supports the management traffic over Management interfaces and Data ports.

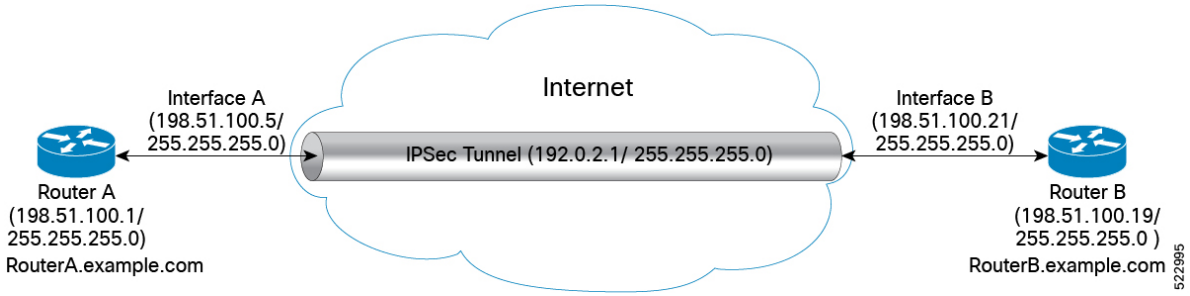
- IPSec tunnel failure results in packet loss.
- IPSec process restart is stateless and results in packet loss.

FQDN-Based Rules for IKEv2 Profile and Keyring Identities

- FQDN names and FQDN domain names are case insensitive. IKEv2 applies case-insensitive comparison when using FQDN identities during session start-up. For example, the initiator expecting remote identity x.cisco.com and the responder presenting the identity of X.CISCO.COM does not affect the session start-up.
- The FQDN matches all peers to the configured FQDN. The FQDN domain name matches all peers with the same domain name in the FQDN. The match is an aggregate of FQDN with the same domain name and not a wildcard match. Multiple peers cannot have the same FQDN or FQDN domain configured within a keyring. But the same string can be configured as FQDN in one peer and as FQDN domain name in another.
- For FQDN domain name match, the peers always expect an expression before the configured domain. For example, if the identity is configured as “identity domain cisco.com”, then *.cisco.com is expected as an identity for the match, and not cisco.com.

Configuration Example

The following example details how to establish IPSec between two routers:



Configuration

Router 1-Initiator

1. Configure the parameters in IKEv2 Proposal

```
Router# config
Router (config)# ikev2 proposal ikev2_proposal_P1 prf sha-256
Router (config)# ikev2 proposal ikev2_proposal_P1 dh-group 20
Router (config)# ikev2 proposal ikev2_proposal_P1 integrity sha-256
Router (config)# ikev2 proposal ikev2_proposal_P1 encryption aes-cbc-256
Router (config)# commit
```

2. Configure the IKEv2 Policy

```
Router# config
Router (config)# ikev2 policy ikev2_policy_P1 match address local 198.51.100.5
Router (config)# ikev2 policy ikev2_policy_P1 match fvrf any
Router (config)# ikev2 policy ikev2_policy_P1 proposal ikev2_proposal_P1
Router (config)# commit
```

3. Configure the IKEv2 Keyring

```
Router# config
Router (config)# keyring key_mgmt_P1 peer ACADIA-2 address 198.51.100.21 255.255.255.0
Router (config)# keyring key_mgmt_P1 peer ACADIA-2 pre-shared-key cisco123
Router (config)# commit
```

Note The pre-shared-key in key must be the same on both the interfaces of the IPSec tunnel.

4. Configure the IKEv2 Profile

Example of matching the initiator profile identity with the responder IPv4 address.

```
Router# config
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 keyring key_mgmt_P1
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 lifetime 600
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 authentication local pre-shared
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 match identity remote address
198.51.100.21 255.255.255.0
Router (config)# commit
```

Example of matching the initiator profile identity with the responder FQDN.

```
Router# config
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 keyring key_mgmt_P1
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 lifetime 600
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 authentication local pre-shared
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 match identity remote fqdn
RouterB.example.com
Router (config)# identity local fqdn RouterA.example.com
Router (config)# commit
```

Example of matching the initiator profile identity with the responder domain name.

```
Router# config
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 keyring key_mgmt_P1
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 lifetime 600
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 authentication local pre-shared
Router (config)# ikev2 profile ikev2_prof_mgmt_P1 match identity remote domain example.com
Router (config)# commit
```

5. Configure the IPSec Transform set

```
Router# config
Router (config)# ipsec transform-set ts_mgmt_P1 mode tunnel
Router (config)# ipsec transform-set ts_mgmt_P1 transform esp-256-aes esp-hmac-sha-256
Router (config)# commit
```

6. Configure the IPSec Profile

```
Router# config
Router (config)# ipsec profile set ikev2 profile ikev2_prof_mgmt_P1
Router (config)# ipsec profile set pfs group19
Router (config)# ipsec profile set security-association lifetime seconds 600
Router (config)# ipsec profile set transform-set ts_mgmt_P1
Router (config)# commit
```

7. Configure the IP Profile for the IPSec Tunnel

```
Router# config
Router (config)# interface tunnel-ip1 ipv4 address 192.0.2.1 255.255.255.0
Router (config)# interface tunnel-ip1 tunnel mode ipsec ipv4
Router (config)# interface tunnel-ip1 tunnel source MgmtEth0/RP0/CPU0/0
Router (config)# interface tunnel-ip1 tunnel destination 198.52.100.21
```

```
Router (config)# interface tunnel-ip1 tunnel protection ipsec profile ipsec_prof_mgmt_P1
Router (config)# commit
```

Router 2-Responder

1. Configure the parameters in IKEv2 Proposal

```
Router# config
Router (config)# ikev2 proposal ikev2_proposal_P2 prf sha-256
Router (config)# ikev2 proposal ikev2_proposal_P2 dh-group 20
Router (config)# ikev2 proposal ikev2_proposal_P2 integrity sha-256
Router (config)# ikev2 proposal ikev2_proposal_P2 encryption aes-cbc-256
Router (config)# commit
```

2. Configure the IKEv2 Policy

```
Router# config
Router (config)# ikev2 policy ikev2_policy_P2 match address local 198.52.100.21
Router (config)# ikev2 policy ikev2_policy_P2 match fvrf any
Router (config)# ikev2 policy ikev2_policy_P2 proposal ikev2_proposal_P2
Router (config)# commit
```

3. Configure the IKEv2 Keyring

   Keyring with IP address.

```
Router# config
Router (config)# keyring key_mgmt_P2 peer ACADIA-1 address 198.52.100.5 255.255.255.0
Router (config)# keyring key_mgmt_P2 peer ACADIA-1 pre-shared-key cisco123
Router (config)# identity address 198.51.100.1 255.255.255.0
Router (config)# commit
```

   Keyring with FQDN.

```
Router# config
Router (config)# keyring key_mgmt_P1 peer ACADIA-2 pre-shared-key cisco123
Router (config)# identity fqdn RouterA.example.com
Router (config)# commit
```

   Keyring with domain name.

```
Router# config
Router (config)# keyring key_mgmt_P1 peer ACADIA-2 pre-shared-key cisco123
Router (config)# identity domain example.com
Router (config)# commit
```

Note

- The pre-shared-key in key must be the same on both the interfaces of the IPSec tunnel.
- The identity is available for key lookup on the IKEv2 responder only.

4. Configure the IKEv2 Profile

```
Router# config
Router (config)# ikev2 profile ikev2_prof_mgmt_P2 keyring key_mgmt_P2
Router (config)# ikev2 profile ikev2_prof_mgmt_P2 lifetime 600
Router (config)# ikev2 profile ikev2_prof_mgmt_P2 authentication local pre-shared
Router (config)# ikev2 profile ikev2_prof_mgmt_P2 match identity remote address
198.52.100.5 255.255.255.0
Router (config)# commit
```

5. Configure the IPSec Transform set

```
Router# config
Router (config)# ipsec transform-set ts_mgmt_P2 mode tunnel
Router (config)# ipsec transform-set ts_mgmt_P2 transform esp-256-aes esp-hmac-sha-256
Router (config)# commit
```

6. Configure the IPSec Profile

```
Router# config
Router (config)# ipsec profile set ikev2 profile ikev2_prof_mgmt_P2
Router (config)# ipsec profile set pfs group19
Router (config)# ipsec profile set security-association lifetime seconds 600
Router (config)# ipsec profile set transform-set ts_mgmt_P2
Router (config)# ipsec profile set responder-only           >>> This command sets the
router as a responder and will not initiate an IPSec session.
Router (config)# commit
```

7. Configure the IP Profile for the IPSec Tunnel

```
Router# config
Router (config)# interface tunnel-ip1 ipv4 address 192.0.2.1 255.255.255.0
Router (config)# interface tunnel-ip1 tunnel mode ipsec ipv4
Router (config)# interface tunnel-ip1 tunnel source MgmtEth0/RP0/CPU0/0
Router (config)# interface tunnel-ip1 tunnel destination 5.22.16.25
Router (config)# interface tunnel-ip1 tunnel protection ipsec profile ipsec_prof_mgmt_P2
Router (config)# commit
```

Running Configuration

Router 1

```
ikev2 proposal ikev2_proposal_mgmt_P1
prf sha-256
dh-group 20
integrity sha-256
encryption aes-cbc-256
exit
!
ikev2 policy ikev2_policy_mgmt_P1
match address local 198.51.100.5
proposal ikev2_proposal_mgmt_P1
exit
keyring key_mgmt_P1
peer Acadia2
  pre-shared-key cisco123
  address 198.52.100.21 255.255.255.0
  exit
!
exit
!
ikev2 profile ikev2_prof_mgmt_P1
authentication local pre-shared
keyring key_mgmt
lifetime 600
match identity remote address 198.52.100.21 255.255.255.0
exit
!
ipsec transform-set ts_mgmt_P1
mode tunnel
transform esp-256-aes esp-hmac-sha-256
exit
!
ipsec profile ipsec_prof_mgmt_P1
set ikev2-profile ikev2_prof_mgmt_P1
```

```
set pfs group19
set security-association lifetime seconds 600
 set transform-set ts_mgmt_P1
exit
!
interface tunnel-ip1
ipv4 address 192.0.2.1 255.255.255.0
tunnel mode ipsec ipv4
tunnel source MgmtEth0/RP0/CPU0/0
tunnel destination 5.22.16.25
tunnel protection ipsec profile ipsec_prof_mgmt_P1
exit
!
```

Router 2

```
ikev2 proposal ikev2_proposal_mgmt_P2
prf sha-256
dh-group 20
integrity sha-256
encryption aes-cbc-256
exit
!
ikev2 policy ikev2_policy_mgmt_P2
match address local 198.52.100.21
proposal ikev2_proposal_mgmt_P2
exit
keyring key_mgmt_P2
peer Acadia1
  pre-shared-key cisco123
  address 198.52.100.21 255.255.255.0
 exit
 !
exit
!
ikev2 profile ikev2_prof_mgmt_P2
authentication local pre-shared
keyring key_mgmt_P2
lifetime 600
match identity remote address 198.52.100.5 255.255.255.0
exit
!
ipsec transform-set ts_mgmt_P2
mode tunnel
transform esp-256-aes esp-hmac-sha-256
exit
!
ipsec profile ipsec_prof_mgmt_P2
set ikev2-profile ikev2_prof_mgmt_P2
set pfs group19
set security-association lifetime seconds 600
 set transform-set ts_mgmt_P2
exit
!
interface tunnel-ip1
ipv4 address 192.0.2.1 255.255.255.0
tunnel mode ipsec ipv4
tunnel source MgmtEth0/RP0/CPU0/0
tunnel destination 5.22.16.52
tunnel protection ipsec profile ipsec_prof_mgmt_P2
exit
!
```

Verification

```
Router# show ipsec sa
Tue Oct  5 15:45:55.597 IST
If/name             SA-Id   Inbound SPI   Outbound SPI
------------------------------------------------------------
tunnel-ip1        804     0x2c378849    0xa9ed8828

Router# show ikev2 session
Session ID                     : 1
==================================
Status                       : UP-ACTIVE
IKE Count                      : 1
Child Count                    : 1
IKE SA ID                      : 1
------------------------------------------------
Local                          : 1.1.1.1/500
Remote                         : 1.1.1.2/500
Status(Description)            : READY (Negotiation done)
Role                           : Initiator
Child SA
------------------------------------------------
Local Selector                 : 1.1.1.1/1000 - 1.1.1.1/1000
Remote Selector                : 1.1.1.2/1000 - 1.1.1.2/1000
ESP SPI IN/OUT                 : 0x6c7b15b7 / 0xbf55acd7

Router# show ikev2 summary
IKEv2 Session Summary
------------------------------------------------
Total Sa (Active/Negotiation)                  : 2 (1/1)
Total Outgoing Sa (Active/Negotiation)         : 2 (1/1)
Total Incoming Sa (Active/Negotiation)         : 0 (0/0)

P/0/RP0/CPU0:ios# show ikev2 session detail
Session ID                        : 1
============================================================
 Status                           : UP-ACTIVE
 IKE Count                        : 1
 Child Count                      : 1
 IKE SA ID                        : 1
------------------------------------------------------------------------
  Local                             : 1.1.1.1/500
  Remote                            : 1.1.1.2/500
  Status(Description)               : READY (Negotiation done)
  Role                              : Initiator
  Encryption/Keysize              : AES-CBC/128
  PRF/Hash/DH Group               : SHA1/SHA256/20
  Authentication(Sign/Verify)     : PSK/PSK
  Authentication(Sign/Verify)     : RSA/RSA (for certificate based)
  Life/Active Time(sec)             : 86400/2043
  Session ID                        : 1
  Local SPI                         : 3B95C7FCC6A69D0A
  Remote SPI                        : F44C4DBCFEE67F07
  Local ID                          : 1.1.1.1
  Remote ID                         : 1.1.1.2

 Child SA
------------------------------------------------------------------------
   Local Selector                 : 1.1.1.1/1000 - 1.1.1.1/1000
   Remote Selector                : 1.1.1.2/1000 - 1.1.1.2/1000
   ESP SPI IN/OUT                 : 0x6c7b15b7 / 0xbf55acd7
   Encryption                   : AES-GCM
   Keysize                      : 256
   ESP HMAC                       : None
```

```
Router# show ipsec sa interface tunnel-ip1
Sun Feb 6 12:10:40.908 IST
-------------------------------------
Interface Name      : tunnel-ip1
Interface handle    : 0x800090
SA id               : 713
Mode             : Tunnel
-------------------------------------
Inbound SA
SPI                    : 0xab487871
Protocol             : ESP
Encrypt Algorithm    : ESP_192_AES
Auth Algorithm       : HMAC_SHA_256
Rekey (After Seconds): 37
-------------------------------------
Outbound SA
SPI                    : 0x1488529e
Protocol             : ESP
Encrypt Algorithm    : ESP_192_AES
Auth Algorithm       : HMAC_SHA_256
Rekey (After Seconds): 37
```

This command shows the Local and Remote IDs and their corresponding FQDNs.

```
Router# show ikev2 session session-id 1 detail
Session ID                      : 1
=============================================
   Status                       : UP-ACTIVE
   IKE Count                    : 1
   Child Count                  : 1
   IKE SA ID                    : 1
-------------------------------------------------------------------------------
  Local                        : 1.1.1.1/500
  Remote                       : 1.1.1.2/500
  Status(Description)          : READY (Negotiation done)
  Role                         : Initiator
  Encryption/Keysize           : AES-CBC/128
  PRF/Hash/DH Group            : SHA1/SHA256/20
  Authentication(Sign/Verify)  : PSK/PSK  (for preshared key based)
  Authentication(Sign/Verify)  : RSA/RSA (for certificate based)
  Life/Active Time(sec)        : 86400/2222
  Session ID                   : 1
  Local SPI                    : 3B95C7FCC6A69D0A
  Remote SPI                   : F44C4DBCFEE67F07
  Local ID                     : 1.1.1.1
  Remote ID                    : 1.1.1.2
  Local ID                   : RouterA.example.com (if FQDN identity used)
  Remote ID                     : RouterB.example.com (if FQDN identity used)

 Child SA
-------------------------------------------------------------------------------
   Local Selector              : 1.1.1.1/1000 - 1.1.1.1/1000
   Remote Selector             : 1.1.1.2/1000 - 1.1.1.2/1000
   ESP SPI IN/OUT              : 0x6c7b15b7 / 0xbf55acd7
   Encryption                  : AES-GCM
   Keysize                     : 256
   ESP HMAC                    : None
```

Quantum-Safe Encryption Using Postquantum Preshared Keys

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Support for Post-Quantum Security	Release 24.1.1	The Internet Key Exchange Protocol Version 2 (IKEv2) is now enhanced to bring post-quantum security. Quantum computers are a threat to existing cryptographic algorithms, and to address this problem, Postquantum Preshared Keys (PPKs) are used. You can generate both manual and dynamic PPKs. This feature introduces the following changes: **CLI:** • The **ppk manual/dynamic** keyword is introduced in the **keyring** command. • The **keyring ppk** keyword is introduced in the **ikev2 profile** command. **YANG Data Model:** • `Cisco-IOS-XR-um-ikev2-cfg.yang` See (GitHub, Yang Data Models Navigator) **Supported Platforms:** • N540X-12Z16G-SYS-D • N540X-12Z16G-SYS-A

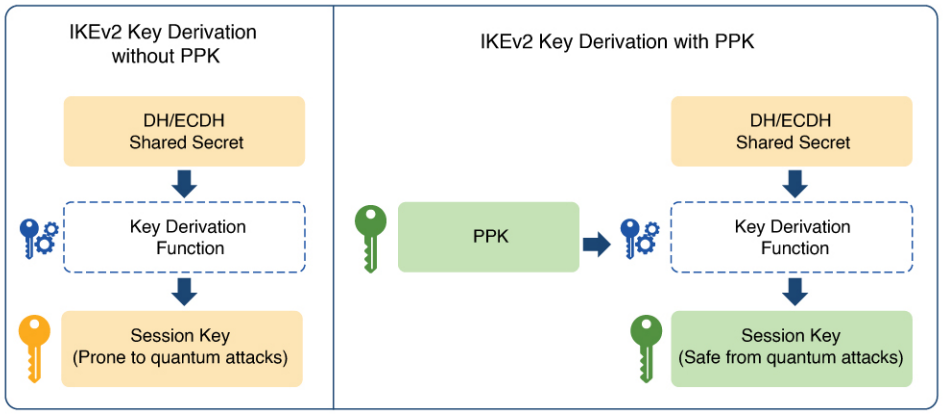
The IKEv2 protocol uses preshared keys to establish a secure connection between the initiator and responder of the IPsec tunnel. These preshared keys use algorithms such as Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). A quantum computer can solve these algorithms in polynomial time, and this can compromise the security of existing IKEv2 systems. To mitigate this, Postquantum Preshared Keys (PPKs) are added to the IKEv2 protocol to ensure that traffic is safe against future quantum computers.

This feature implements RFC 8784 and Cisco Secure Key Integration Protocol (SKIP) for quantum-safe encryption of IKEv2 and IPsec packets using PPKs.

Postquantum Preshared Keys

Postquantum Preshared Key (PPK) is a 64-bit long secret key that is shared between an initiator and responder of the IPsec tunnel. The existing authentication method in IKEv2 sends a shared secret to the key derivation function, which generates the session keys. These session keys are not quantum safe. When session keys are derived after sending PPKs as input to the key derivation function, they protect the system from future quantum attackers.

Figure 2: IKEv2 Key Derivation - With and Without PPK



DH: Diffie-Hellman
ECDH: Elliptic-curve Diffie-Hellman
PPK: Postquantum Preshared Key

PPKs can be configured in two ways:

- Dynamic PPK
- Manual PPK

Dynamic PPK

Dynamic PPKs are imported from an external key source, which can be in the form of a Quantum Key Distribution (QKD) device, software, or cloud-based key source or service. Dynamic PPKs are generated using the Cisco Secure Key Integration Protocol (SKIP). It is an HTTPS-driven protocol designed to enable encryption devices like routers to import PPKs from an external key source. These externally imported dynamic PPKs, provide advantages such as automated provisioning and updates, as well as improved PPK entropy.

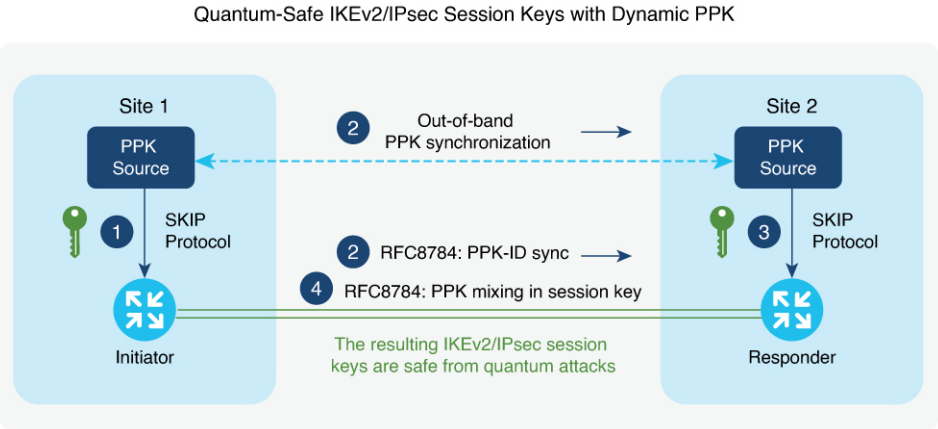
The PPK ID is the only information that is shared between the initiator and responder over the public network. The PPKs are not shared between the initiator and responder through the public network.

We recommend that encryption devices have the SKIP client and the external key source have the SKIP server for PPK to function as expected. The external key source must meet the following expectations to be SKIP-compliant:

- Implement the SKIP protocol or API, as specified in the Cisco SKIP specification.
- Provide the same PPK to the encryption device pair—initiator and responder—using an out-of-band synchronization mechanism.

The figure shows quantum-safe IKEv2 and IPsec session keys using dynamic PPK.

Figure 3: Quantum-Safe IKEv2 and IPsec Session Keys with Dynamic PPK



The IKEv2 initiator and responder are connected to their respective local key sources. They are configured with the SKIP client that specifies the IP address and port of the key source, as well as the preshared key. The PPK sources are also configured with the SKIP parameters, which include the local key source identity and a list of identities of the peer key sources.

The following is a high-level operation of the Cisco SKIP protocol:

1. The IKEv2 initiator places a request for a PPK from its key source. The key source replies with a PPK and the corresponding PPK ID.
2. The initiator-side key source synchronizes the PPK to the responder-side key source using an out-of-band mechanism that is specific to the type of key source. The IKEv2 initiator communicates the PPK ID to the IKEv2 responder over IKEv2 using the RFC 8784 extensions.
3. The IKEv2 responder requests from its key source, the PPK corresponding to the PPK ID received from the IKEv2 initiator. The key source replies with the PPK corresponding to the PPK ID.
4. The IKEv2 initiator and responder mix the PPK in the key derivation, as specified in RFC 8784. The resulting IKEv2 and IPsec session keys are quantum-safe.

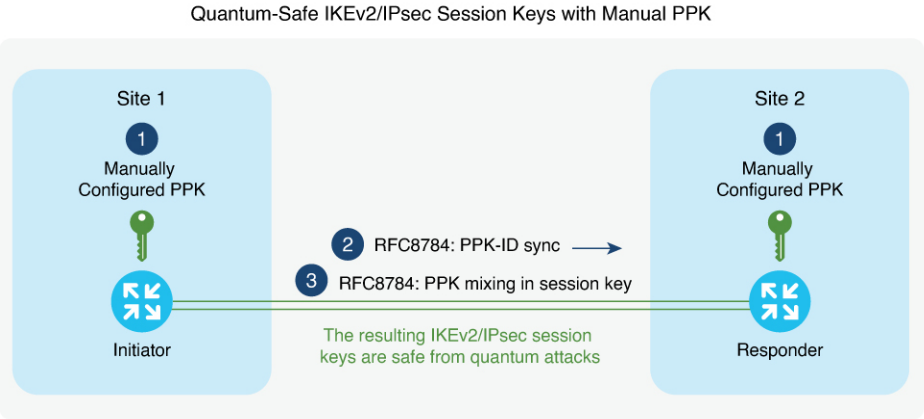
Manual PPK

Manual PPKs are configured by providing the PPK ID and password in the keyring configuration of the initiator and responder. The password is encrypted using type-7 encryption. Each IKE peer has a list of PPKs along with their identifiers (PPK_ID). Any potential IKE initiator selects which PPK to use with any specific responder.

If you do not have an external server to import PPKs, and still want to give additional protection, you can use manual PPKs. It is important to ensure that a manual PPK is of sufficient size, entropy, and is frequently rotated by the administrator.

In the figure, you can see the session keys of quantum-safe IKEv2 and IPsec, which are obtained through a manual PPK.

Figure 4: Quantum-Safe IKEv2 and IPsec Session Keys with Manual PPK



Configure Quantum-Safe Encryption Using PPK

The following sections describe the processes involved in configuring quantum-safe encryption using dynamic and manual postquantum preshared keys.

Configuring IPsec Tunnels with Dynamic PPK Initiator

Initiator Configuration: The PPK configuration is done in addition to the IPsec configuration.

The following steps describe how to create the IP profile, keyring, IKEv2 profile, transform set, SKS profile, and IPsec profile. The keyring and IKEv2 profile contains the PPK configuration.

Procedure

Step 1 Enable the IP profile for the IPsec tunnel.

```
Router#config
Router(config)#interface tunnel-ip1
Router(config)#ipv4 address 209.165.200.225 255.255.255.224
Router(config)#tunnel mode ipsec ipv4
Router(config)#tunnel source GigabitEthernet0/1/0/2
Router(config)#tunnel destination 10.10.10.1
Router(config)#tunnel protection ipsec profile test3
Router(config)#interface GigabitEthernet0/1/0/2
Router(config)#ipv4 address 10.10.10.3 255.255.255.0
```

Step 2 Create the keyring and add the PPK for post-quantum security along with the preshared key

```
Router(config)#keyring k3
Router(config-ikev2-keyring)#peer init
Router(config-ikev2-keyring-peer))#ppk dynamic Qkd required
Router(config-ikev2-keyring-peer)#pre-shared-key password 0822455D0A16
Router(config-ikev2-keyring-peer)#address 10.10.10.1 255.255.255.0
```

Note If the required **keyword** is not used, and an error is encountered while establishing the session, then IKEv2 will fall back to normal authentication without the use of PPKs.

Step 3 Create the IKEv2 profile and include the IKEv2 keyring.

```
Router(config)#ikev2 profile p3
Router(config-ikev2-profile-p3)#keyring k3
Router(config-ikev2-profile-p3)#keyring ppk k3
Router(config-ikev2-profile-p3)#match identity remote address 10.10.10.1 255.255.255.0
```

Step 4 Define the IPsec transform set for the IPsec security association negotiation. The 256-bit Advanced Encryption Standard (AES) is used for the encryption and Secure Hash Algorithm (SHA) as the hash algorithm for data protection for the preshared keys.

```
Router(config)#ipsec transform-set ts3
Router(config)#transform esp-hmac-sha-384 esp-256-aes
Router(config)#mode tunnel
```

The peers agree on this transform set and it is used to protect the data flow between them.

Step 5 Configure the Session Key Service (SKS) profile with the IP address of the Key Management Entity (KME) server that manages cryptographic keys.

```
Router(config)#sks profile Qkd type remote
Router(config-sks-profile)#kme server ipv4 192.0.2.34 port 10001
```

Note Key source vendors, such as QKD vendors, should contact their Cisco representative to implement the Cisco SKIP protocol.

Step 6 Add the IKEv2 profile and transform set in the IPsec profile.

```
Router(config)#ipsec profile test3
Router(config)#set ikev2-profile p3
Router(config)#set transform-set ts3
```

What to do next

Configure IPsec tunnel with dynamic PPK on the responder.

Configuring IPsec Tunnels with Dynamic PPK Responder

Responder Configuration: The PPK configuration is done in addition to the IPsec configuration.

The following steps describe how to create the IP profile, keyring, IKEv2 profile, transform set, SKS profile, and IPsec profile. The keyring and IKEv2 profile contains the PPK configuration.

Procedure

Step 1 Enable the IP profile for the IPsec tunnel.

```
Router#config
Router(config)#interface tunnel-ip1
Router(config)#ipv4 address 209.165.200.226 255.255.255.224
Router(config)#tunnel mode ipsec ipv4
Router(config)#tunnel source GigabitEthernet0/1/0/2
Router(config)#tunnel destination 10.10.10.3
Router(config)#tunnel protection ipsec profile test3
Router(config)#interface GigabitEthernet0/1/0/2
Router(config)#ipv4 address 10.10.10.1 255.255.255.0
```

Step 2 Create the keyring and add the PPK for post-quantum security along with the preshared key

```
Router(config-ikev2-keyring)#keyring k3
Router(config-ikev2-keyring)#peer init
Router(config-ikev2-keyring-peer)#ppk dynamic Qkd required
Router(config-ikev2-keyring-peer)#pre-shared-key password 0822455D0A16
Router(config-ikev2-keyring-peer)#address 10.10.10.1 255.255.255.0
```

Note If the required **keyword** is not used, and an error is encountered while establishing the session, then IKEv2 will fall back to normal authentication without the use of PPKs.

Step 3 Create the IKEv2 profile and include the IKEv2 keyring.

```
Router(config)#ikev2 profile p3
Router(config-ikev2-profile-p3)#keyring ppk k3
Router(config-ikev2-profile-p3)#keyring k3
Router(config-ikev2-profile-name)#match identity remote address 10.10.10.3 255.255.255.0
```

Step 4 Define the IPsec transform set for the IPsec security association negotiation. The 256-bit Advanced Encryption Standard (AES) is used for the encryption and Secure Hash Algorithm (SHA) as the hash algorithm for data protection for the preshared keys.

```
Router(config)#ipsec transform-set ts1
Router(config)#transform esp-hmac-sha-256 esp-192-aes
Router(config)#mode tunnel
```

The peers agree on this transform set and it is used to protect the data flow between them.

Step 5 Configure the Session Key Service (SKS) profile with the IP address of the Key Management Entity (KME) server that manages cryptographic keys.

```
Router(config)#sks profile Qkd type remote
Router(config-sks-profile)#kme server ipv4 192.0.2.34 port 10001
```

Note Key source vendors, such as QKD vendors, should contact their Cisco representative to implement the Cisco SKIP protocol.

Step 6 Add the IKEv2 profile and transform set in the IPsec profile.

```
Router(config)#ipsec profile test3
Router(config)#set ikev2-profile p3
Router(config)#set transform-set ts3
Router(config)#set responder-only
```

Verifying Dynamic PPK Configuration

To verify the dynamic PPK configuration on the Initiator:

```
Router#show ikev2 session
Mon Feb 12 10:29:44.738 IST

Session ID                              : 9
================================================================================
 Status                                 : UP-ACTIVE
 IKE Count                              : 1
 Child Count                            : 1
 IKE SA ID                              : 21077
--------------------------------------------------------------------------------
  Local                                 : 10.10.10.3/500
  Remote                                : 10.10.10.1/500
  Status(Description)                   : READY (Negotiation done)
  Role                                  : Initiator
  Fvrf                                  : Default
  Quantum resistance                    : Enabled with dynamic PPK

 Child SA
--------------------------------------------------------------------------------
   Local Selector                       : 0.0.0.0/0 - 255.255.255.255/65535
   Remote Selector                      : 0.0.0.0/0 - 255.255.255.255/65535
   ESP SPI IN/OUT                       : 0x50571841 / 0x190c759d


Router#show ikev2 sa
Mon Feb 12 10:30:16.806 IST

IKE SA ID                               : 21077
--------------------------------------------------------------------------------
 Local                                  : 10.10.10.3/500
 Remote                                 : 10.10.10.1/500
 Status(Description)                    : READY (Negotiation done)
 Role                                   : Initiator
 Fvrf                                   : Default
 Quantum resistance                     : Enabled with dynamic PPK


Router#show ipsec sa interface tunnel-ip3
Mon Feb 12 10:30:42.091 IST
-------------------------------------
Interface Name      : tunnel-ip3
Interface handle    : 0x8000b0
SA id               : 641
Mode                : Tunnel
PFS enabled         : No
PFS group           : None
Quantum resistant   : Yes
-------------------------------------
Inbound SA
SPI                             : 0x50571841
Protocol                        : ESP
Encrypt Algorithm               : ESP_256_AES
Auth Algorithm                  : HMAC_SHA_384
Lifetime (expire After Seconds) : 10927
-------------------------------------
Outbound SA
SPI                             : 0x190c759d
Protocol                        : ESP
Encrypt Algorithm               : ESP_256_AES
Auth Algorithm                  : HMAC_SHA_384
Lifetime (expire After Seconds) : 10927
```

Configuring IPsec Tunnels with Manual PPK Initiator

Initiator Configuration: The PPK configuration is done in addition to the IPsec configuration.

The following steps describe how to create the IP profile, keyring, IKEv2 profile, transform set, and IPsec profile. The keyring and IKEv2 profile contains the PPK configuration. In manual PPK configuration, the PPK is not received from an external server.

Procedure

Step 1 Enable the IP profile for the IPsec tunnel.

```
Router#config
Router(config)#interface tunnel-ip1
Router(config)#ipv4 address 209.165.200.225 255.255.255.224
Router(config)#tunnel mode ipsec ipv4
Router(config)#tunnel source GigabitEthernet0/1/0/0
Router(config)#tunnel destination 10.10.10.1
Router(config)#tunnel protection ipsec profile test1
Router(config)#interface GigabitEthernet0/1/0/0
Router(config)#ipv4 address 10.10.10.3 255.255.255.0
```

Step 2 Create the keyring and add the PPK for post-quantum security along with the preshared key

```
Router(config)#keyring k1
Router(config-ikev2-keyring)#peer init
Router(config-ikev2-keyring-peer)#ppk manual id 123 key password 060506324F41584B56 required
Router(config-ikev2-keyring-peer)#pre-shared-key password 0822455D0A16
Router(config-ikev2-keyring-peer)#address 10.10.10.1 255.255.255.0
```

Note If the required **keyword** is not used, and an error is encountered while establishing the session, then IKEv2 will fall back to normal authentication without the use of PPKs.

Step 3 Create the IKEv2 profile and include the IKEv2 keyring.

```
Router(config)#ikev2 profile p1
Router(config-ikev2-profile-p1)#keyring k1
Router(config--ikev2-profile-p1)#keyring ppk k1
Router(config-ikev2-profile-name)#match identity remote address 10.10.10.1 255.255.255.0
```

Step 4 Define the IPsec transform set for the IPsec security association negotiation. The 256-bit Advanced Encryption Standard (AES) is used for the encryption and Secure Hash Algorithm (SHA) as the hash algorithm for data protection for the preshared keys.

```
Router(config)#ipsec transform-set ts1
Router(config)#transform esp-hmac-sha-256 esp-192-aes
Router(config)#mode tunnel
```

The peers agree on this transform set and it is used to protect the data flow between them.

Step 5 Add the IKEv2 profile and transform set in the IPsec profile.

```
Router(config)#ipsec profile test1
```

```
Router(config)#set ikev2-profile p1
Router(config)#set transform-set ts1
```

What to do next

Configure IPsec tunnels with manual PPK on the responder.

Configuring IPsec Tunnels with Manual PPK Responder

Responder Configuration: The PPK configuration is done in addition to the IPsec configuration.

The following steps describe how to create the IP profile, keyring, IKEv2 profile, transform set, and IPsec profile. The keyring and IKEv2 profile contains the PPK configuration. In manual PPK configuration, the PPK is not received from an external server.

Procedure

Step 1 Enable the IP profile for the IPsec tunnel.

```
Router#config
Router(config)#interface tunnel-ip1
Router(config)#ipv4 address 209.165.200.226 255.255.255.224
Router(config)#tunnel mode ipsec ipv4
Router(config)#tunnel source GigabitEthernet0/1/0/0
Router(config)#tunnel destination 10.10.10.3
Router(config)#tunnel protection ipsec profile test1
Router(config)#interface GigabitEthernet0/1/0/0
Router(config)#ipv4 address 10.10.10.1 255.255.255.0
```

Step 2 Create the keyring and add the PPK for post-quantum security along with the preshared key

```
Router(config)#keyring k1
Router(config-ikev2-keyring)#peer init
Router(config-ikev2-keyring-init)#ppk manual id 123 key password 104D000A061843595F required
Router(config-ikev2-keyring-init)#pre-shared-key password 0822455D0A16
Router(config-ikev2-profile-name)#address 10.10.10.1 255.255.255.0
```

Note If the required **keyword** is not used, and an error is encountered while establishing the session, then IKEv2 will fall back to normal authentication without the use of PPKs.

Step 3 Create the IKEv2 profile and include the IKEv2 keyring.

```
Router(config)#ikev2 profile p1
Router(config-ikev2-profile-p1)#keyring ppk k1
Router(config-ikev2-profile-p1)keyring k1
Router(config-ikev2-profile-name)#match identity remote address 10.10.10.3 255.255.255.0
```

Step 4 Define the IPsec transform set for the IPsec security association negotiation. The 256-bit Advanced Encryption Standard (AES) is used for the encryption and Secure Hash Algorithm (SHA) as the hash algorithm for data protection for the preshared keys.

```
Router(config)#ipsec transform-set ts1
```

```
Router(config)#transform esp-hmac-sha-256 esp-192-aes
Router(config)#mode tunnel
```

The peers agree on this transform set and it is used to protect the data flow between them.

Step 5 Add the IKEv2 profile and transform set in the IPsec profile.

```
Router(config)#ipsec profile test1
Router(config)#set ikev2-profile p1
Router(config)#set transform-set ts1
Router(config)#set responder-only
```

Verifying Manual PPK Configuration

Execute the following commands to verify the manual PPK configuration.

```
Router#show ikev2 session
Mon Feb 12 10:27:53.785 IST

Session ID                          : 10
================================================================================
 Status                             : UP-ACTIVE
 IKE Count                          : 1
 Child Count                        : 1
 IKE SA ID                          : 18620
--------------------------------------------------------------------------------
  Local                             : 10.10.10.1/500
  Remote                            : 10.10.10.3/500
  Status(Description)               : READY (Negotiation done)
  Role                              : Responder
  Fvrf                              : Default
  Quantum resistance                : Enabled with manual PPK

 Child SA
--------------------------------------------------------------------------------
   Local Selector                   : 0.0.0.0/0 - 255.255.255.255/65535
   Remote Selector                  : 0.0.0.0/0 - 255.255.255.255/65535
   ESP SPI IN/OUT                   : 0xb3843a2d / 0xbb5d58fa


Router#show ikev2 sa
Mon Feb 12 10:28:02.643 IST

IKE SA ID                          : 18620
--------------------------------------------------------------------------------
 Local                             : 10.10.10.1/500
 Remote                            : 10.10.10.3/500
 Status(Description)               : READY (Negotiation done)
 Role                              : Responder
 Fvrf                              : Default
 Quantum resistance                : Enabled with manual PPK


Router#show ipsec sa interface tunnel-ip1
Mon Feb 12 10:28:15.921 IST
-------------------------------------
Interface Name      : tunnel-ip1
Interface handle    : 0x800090
SA id               : 759
Mode                : Tunnel
PFS enabled         : No
```

```
PFS group           : None
Quantum resistant   : Yes
-------------------------------------
Inbound SA
SPI                              : 0xb3843a2d
Protocol                         : ESP
Encrypt Algorithm                : ESP_192_AES
Auth Algorithm                   : HMAC_SHA_256
Lifetime (expire After Seconds) : 11107
-------------------------------------
Outbound SA
SPI                              : 0xbb5d58fa
Protocol                         : ESP
Encrypt Algorithm                : ESP_192_AES
Auth Algorithm                   : HMAC_SHA_256
Lifetime (expire After Seconds) : 11107
```