IP Security for Management Traffic

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
IP Security (IPSec) for Management Traffic	Release 7.8.1	

Feature Name	Release Information	Feature Description
		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. With IPSec, management traffic data is sent across a public network without observation, modification, or spoofing. 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.

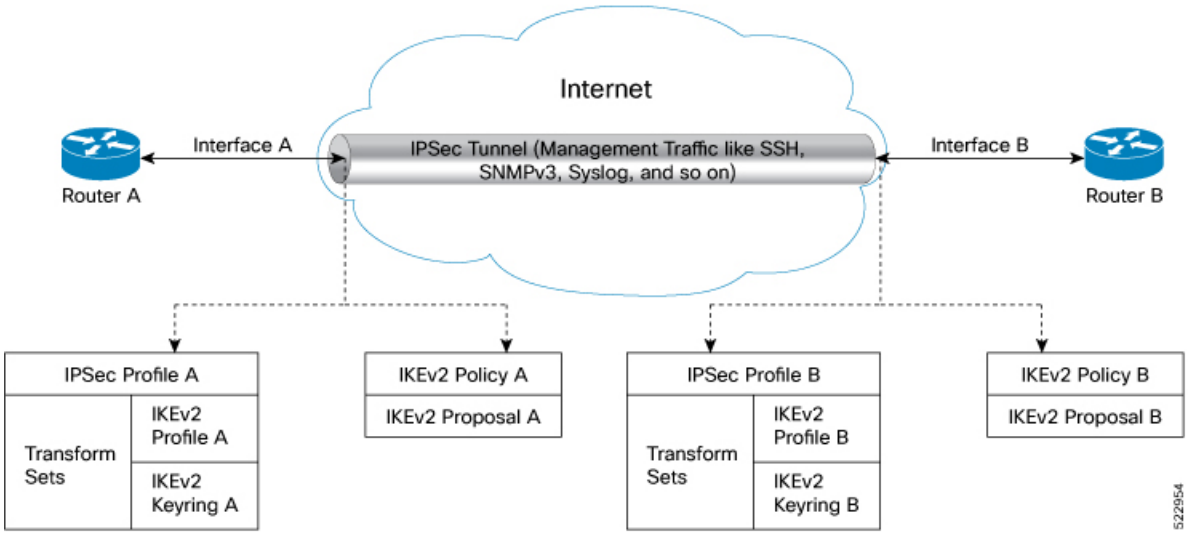
The key components in IPSec are as follows:

- **IPSec Profile**: The IPSec profile consists 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 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 the preshared keys along with the IP address of the peer tunnel for IKEv2 negotiations.

- **IKEv2 Policy**: The IKEv2 policy consists 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 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

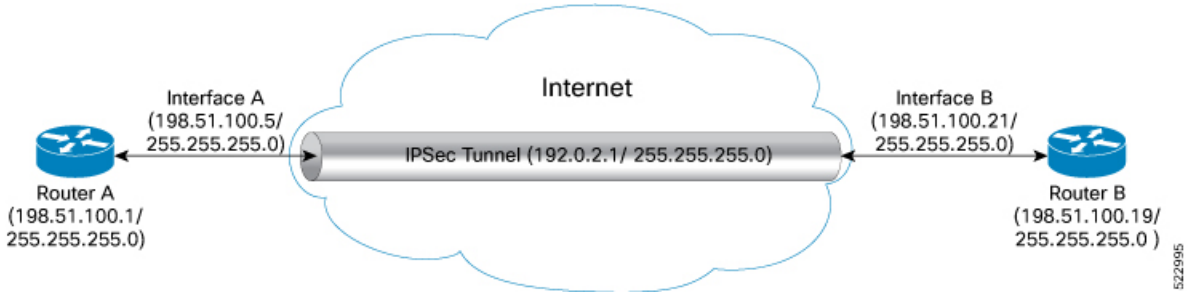
Restrictions for IP Security for Management Traffic

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.
- Router supports a maximum of 3 unique IPSec profiles.
- 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.

Configuration Example

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



Configuration

Router 1

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 198.52.100.21 255.255.255.0
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

```
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
198.52.100.21 255.255.255.0
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

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

```
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)# 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

```
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)# 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
```