

N4/Sx over IPSec

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- Recommended Timers, on page 4
- Sample Configurations, on page 11
- Monitoring and Troubleshooting, on page 15

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

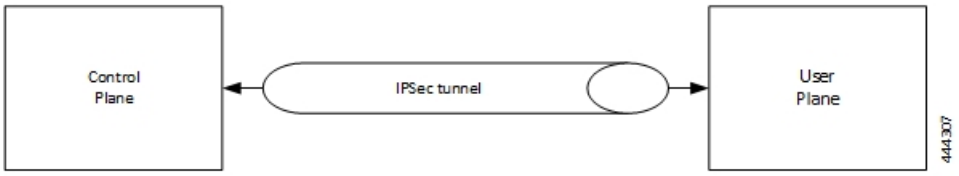
Internet Protocol Security (IPSec) is a suite of protocols that interact with one another to provide secure private communication across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams.

In Cisco Cloud Native 5G, the IPSec functionality is available in Tunnel mode both on Session Management Function (SMF) and User Plane Function (UPF). The IPSec crypto-maps are associated under the appropriate interface on respective nodes. The IPSec tunnel is created between each SMF or UPF pair explicitly. This feature supports the IPv4 and IPv6 tunneling mode. There is no change on the N4/Sx service configuration.

The IPSec tunnel mode encapsulates the entire IP packet to provide a virtual secure hop between two gateways. It forms VPN kind of functionality, where entire IP packets are encapsulated inside another and delivered to the destination. It encapsulates the full IP header as well as the payload.

The N4 over IPSec feature supports TLS 1.2 using OpenSSL certificates.

Figure 1: N4/Sx Over IPSec Tunnel



When N4/Sx over IPSec is enabled on UPF NF running VPP, then the following parameter must be used under "VPP Param" for the N4/Sx Over IPSec feature to work.

VPP_DPDK_DATA_SIZE=5120

The VPP Param is stored in the **staros_para.cfg** file on a CD-ROM and this configuration is read and applied to VPP by UPF during its boot.

Note This parameter is supported until VPP version 19.08. This parameter introduces a memory overhead of about 800 MB. You must consider this condition before using the feature. If the UPF has less RAM, then VM must be allocated with extra 1 GB of RAM memory for the feature to work properly.

For more information on IPSec support, see the StarOS *IPSec Reference*.

IKEv2 Keep-Alive Messages (Dead Peer Detection)

IPSec for N4/Sx interface supports IKEv2 keep-alive messages, also known as Dead Peer Detection (DPD), originating from both ends of an IPSec tunnel. As per RFC 3706, DPD is used to simplify the messaging required to verify communication between peers and tunnel availability.

IPSec DPD is an optional configuration. If its disabled, the IPSec node does not initiate DPD request. However, the node always responds to DPD availability messages initiated by peer node regardless of its DPD configuration.

The following method can be used to calculate the keep-alive interval value when N4/Sx over IPSec feature is configured:

```
((max-retransmissions + 1) * retransmission-timeout-ms) * 2
```

The keep-alive interval value specifies the time that the IPSec tunnel will remain up till DPD is triggered.

Example:

The following is a sample output of the **show configuration context** *context_name* **verbose** CLI command under N4/Sx service:

```
sx-service sx
   instance-type userplane
   bind ipv4-address 192.168.1.1 ipv6-address bbbb:abcd::11
   sxa max-retransmissions 4
   sxa retransmission-timeout-ms 5000
```

Here, the value of **max-retransmissions** is 4 and **retransmission-timeout-ms** is 5000. Therefore, the keep-alive interval value will be 50:

((max-retransmissions + 1) * retransmission-timeout-ms) * 2 = Keep-alive interval

((4+1) * 5000) * 2 = 50

IKESA Rekey

UPF supports both IKESA Rekey and IPSec Rekey.

For IKESA Rekey, the **lifetime** *interval* CLI must be configured under **ikev2-ikesa transform-set** *transform_set*. You must also configure **ikev2-ikesa rekey** under **crypto map** configuration. Following is a configuration example:

```
ikev2-ikesa transform-set ikesa-foo
   encryption aes-cbc-256
   group 14
   hmac sha2-256-128
   lifetime 28800
   prf sha2-256
...
...
...
crypto map foo0 ikev2-ipv4
   match address foo0
   authentication local pre-shared-key encrypted key secret_key
   authentication remote pre-shared-key encrypted key secret_key
   ikev2-ikesa max-retransmission 3
   ikev2-ikesa retransmission-timeout 15000
   ikev2-ikesa transform-set list ikesa-foo
   ikev2-ikesa rekey
   keepalive interval 50
   control-dont-fragment clear-bit
   payload foo-sa0 match ipv4
      ipsec transform-set list A-foo
      lifetime 600
      rekey keepalive
   #exit
   peer 172.19.222.2
   ikev2-ikesa policy error-notification
```

Limitations

The feature is supported only in IPv4-IPv4 tunneling mode.

Recommended Timers

The following table provides the recommended timer values for CLI commands related to IPSec, N4/Sx, and SRP.

IPSec	**SMF**	**UPF**
ikev2-ikesa max-retransmission	*3*	*3*
ikev2-ikesa retransmission-timeout	*1000*	*1000*
keepalive	**interval** *4* **timeout** *1* **num-retry** *4*	**interval** *5* **timeout** *2* **num-retry** *4*
N4/Sx	**SMF**	**UPF**
sx-protocol heartbeat interval	*10*	*10*
sx-protocol heartbeat retransmission-timeout	*5*	*5*
sx-protocol heartbeat max-retransmissions	*4*	*4*
sxa max-retransmissions	*4*	*4*
sxa retransmission-timeout-ms	*5000*	*5000*
sxb max-retransmissions	*4*	*4*
sxb retransmission-timeout-ms	*5000*	*5000*
sxab max-retransmissions	*4*	*4*
sxab retransmission-timeout-ms	*5000*	*5000*
sx-protocol association reattempt-timeout	*60*	*60*
SRP	**SMF**	**UPF**
hello-interval	*3*	*3*
dead-interval	*15*	*15*

Recommended Configurations

Following are the recommended configurations and restrictions related to N4/Sx and SRP over IPSec:

- The multihop BFD timer between SMF and UPF must be seven seconds (for Data UPFs).

- The singlehop BFD must be enabled on all the contexts (SMF GW/Billing and UPF Gn/Gi).
- Inter-chassis multihop BFD must be enabled for SMF-SMF ICSR and UPF-UPF ICSR (IMS UPF).
- The SRP-IPSec ACL must be configured for TCP protocol instead of IP protocol.
- The N4/Sx-IPSec ACL must be configured for UDP protocol instead of IP protocol.

Example Configurations in SMF

Multihop BFD Configuration VPC-DI

The following is an example of multihop BFD configuration with seven seconds timer.

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 350 min_rx 350 multiplier 20
    #exit
```

Multihop BFD Configuration VPC-SI

The following is an example of multihop BFD configuration with three seconds timer.

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 150 min_rx 150 multiplier 20
    #exit
```

BGP Configuration

The following is an example of BGP configuration with recommended timers.

```
router bgp 1111
      router-id 209.165.200.225
      maximum-paths ebgp 15
      neighbor 209.165.200.250 remote-as 1000
      neighbor 209.165.200.250 ebgp-multihop
      neighbor 209.165.200.250 update-source 209.165.200.225
      neighbor 1111:2222::101 remote-as 1000
      neighbor 1111:2222::101 ebgp-multihop
      neighbor 1111:2222::101 update-source 1111:2222::1
      bgp graceful-restart restart-time 120
      bgp graceful-restart stalepath-time 300
      timers bgp keepalive-interval 30 holdtime-interval 90 min-peer-holdtime-interval 0
server-sock-open-delay-period 10
      address-family ipv4
        redistribute connected
      #exit
      address-family ipv6
        neighbor 1111:2222::101 activate
        redistribute connected
      #exit
    #exit
```

Singlehop BFD Configuration

The following is an example of singlehop BFD configuration with three seconds timer.

```
interface bgp-sw1-2161-10
      ip address 209.165.200.233 209.165.200.255
      ipv6 address 1111:222::9/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-11
      ip address 209.165.200.234 209.165.200.255
      ipv6 address 1111:222::10/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-12
      ip address 209.165.200.235 209.165.200.255
      ipv6 address 1111:222::11/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-3
      ip address 209.165.200.226 209.165.200.255
      ipv6 address 1111:222::2/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-4
      ip address 209.165.200.227 209.165.200.255
      ipv6 address 1111:222::3/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-5
      ip address 209.165.200.228 209.165.200.255
      ipv6 address 1111:222::4/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-6
      ip address 209.165.200.229 209.165.200.255
      ipv6 address 1111:222::5/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-7
      ip address 209.165.200.230 209.165.200.255
      ipv6 address 1111:222::6/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-8
      ip address 209.165.200.231 209.165.200.255
      ipv6 address 1111:222::7/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-9
      ip address 209.165.200.232 209.165.200.255
      ipv6 address 1111:222::8/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
```

Static Route for Multihop BFD Configuration

The following is an example of static route multihop BFD configuration.

```
ip route static multihop bfd UP-5 209.165.200.240 209.165.200.245
    ip route static multihop bfd UP-6 209.165.200.240 209.165.200.246
    ip route static multihop bfd UP-9 209.165.200.240 209.165.200.247
    ip route static multihop bfd UP-10 209.165.200.240 209.165.200.248
    ip route static multihop bfd UP-7 209.165.200.240 209.165.200.249
    ip route static multihop bfd UP-8 209.165.200.240 209.165.200.250
```

Static Route for Singlehop BFD Configuration

The following is an example of static route singlehop BFD configuration.

```
ip route static bfd bgp-sw1-2161-3 209.165.200.230
    ip route static bfd bgp-sw1-2161-4 209.165.200.230
    ip route static bfd bgp-sw1-2161-5 209.165.200.230
    ip route static bfd bgp-sw1-2161-6 209.165.200.230
    ip route static bfd bgp-sw1-2161-7 209.165.200.230
    ip route static bfd bgp-sw1-2161-8 209.165.200.230
    ip route static bfd bgp-sw1-2161-9 209.165.200.230
    ip route static bfd bgp-sw1-2161-10 209.165.200.230
    ip route static bfd bgp-sw1-2161-11 209.165.200.230
    ip route static bfd bgp-sw1-2161-12 209.165.200.230
```

IPSec ACL Configuration

The following is an example IPSec ACL configuration in SMF.

```
ip access-list UP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec Transform Set Configuration

The following is an example of IPSec Transform Set configuration in SMF.

```
ikev2-ikesa transform-set ikesa-UP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256

    ipsec transform-set A-UP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14
```

IPSec Crypto Map Configuration

The following is an example of IPSec Crypto Map configuration in SMF.

```
crypto map UP-1 ikev2-ipv4
      match address UP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-UP-1
      ikev2-ikesa rekey
      keepalive interval 4 timeout 1 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-UP-1
        lifetime 300
        rekey keepalive
      #exit
      peer 209.165.200.224
      ikev2-ikesa policy error-notification
    #exit
```

N4/Sx Configuration

The following is an example of N4/Sx configuration in SMF.

```
sx-service SX-1
      instance-type controlplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
      sx-protocol supported-features load-control
      sx-protocol supported-features overload-control
    exit
end
```

Example Router Configurations

Static Routes for Interface

The following is an example configuration of static route for interface.

```
ip route 209.165.200.224/27 Vlan1111 209.165.200.225
ip route 209.165.200.224/27 Vlan1111 209.165.200.226
ip route 209.165.200.224/27 Vlan1111 209.165.200.227
ip route 209.165.200.224/27 Vlan1111 209.165.200.228
ip route 209.165.200.224/27 Vlan1111 209.165.200.229
ip route 209.165.200.224/27 Vlan1111 209.165.200.230
ip route 209.165.200.224/27 Vlan1111 209.165.200.231
ip route 209.165.200.224/27 Vlan1111 209.165.200.232
ip route 209.165.200.224/27 Vlan1111 209.165.200.233
ip route 209.165.200.224/27 Vlan1111 209.165.200.234
```

Static Routes for Singlehop BFD

The following is an example configuration of static route for singlehop BFD.

```
ip route static bfd Vlan1111 209.165.200.225
ip route static bfd Vlan1111 209.165.200.226
ip route static bfd Vlan1111 209.165.200.227
ip route static bfd Vlan1111 209.165.200.228
ip route static bfd Vlan1111 209.165.200.229
ip route static bfd Vlan1111 209.165.200.230
ip route static bfd Vlan1111 209.165.200.231
ip route static bfd Vlan1111 209.165.200.232
ip route static bfd Vlan1111 209.165.200.233
ip route static bfd Vlan1111 209.165.200.234
```

Interface for Singlehop BFD

The following is an example configuration of interface for singlehop BFD.

```
interface Vlan1111
  no shutdown
  bandwidth 10000000
  bfd interval 999 min_rx 999 multiplier 3
  no bfd echo
```

```
  ip address 209.165.200.224/27
  ipv6 address 1111:222::1/112
```

BGP Configuration

The following is an example of BGP configuration with recommended timers.

```
router bgp 1000
  router-id 209.165.200.226
  timers bgp 30 90
  timers bestpath-limit 300
  timers prefix-peer-timeout 30
  timers prefix-peer-wait 90
  graceful-restart
  graceful-restart restart-time 120
  graceful-restart stalepath-time 300
```

Example Configurations in UPF

IPSec ACL Configuration

The following is an example of IPSec ACL configuration in UPF.

```
ip access-list CP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec Transform Set Configuration

The following is an example of IPSec Transform Set configuration in UPF.

```
ipsec transform-set A-CP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14

    ikev2-ikesa transform-set ikesa-CP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256
```

IPSec Crypto Map Configuration

The following is an example of IPSec Crypto Map configuration in UPF.

```
crypto map CP-1 ikev2-ipv4
      match address CP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-CP-1
      ikev2-ikesa rekey
      keepalive interval 5 timeout 2 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-CP-1
      #exit
      peer 209.165.200.230
      ikev2-ikesa policy error-notification
    #exit
```

N4/Sx Configuration

The following is an example of N4/Sx configuration in UPF.

```
sx-service SX-1
      instance-type userplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
    exit
```

Example SRP Configurations

IPSec ACL Configuration

The following is an example of IPSec ACL configuration for SRP.

```
ip access-list SRP
      permit tcp host 209.165.200.227 host 209.165.200.228
    #exit
```

SRP Configuration

The following is an example of SRP configuration.

```
configure
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 999 min_rx 999 multiplier 3
    #exit
configure
  context srp
    service-redundancy-protocol
      chassis-mode primary
      hello-interval 3
      dead-interval 15
      monitor bfd context srp 209.165.200.226 chassis-to-chassis
      monitor bgp context gi-pgw 209.165.200.245
      monitor bgp context gi-pgw 3333:888::1
      monitor bgp context saegw 209.165.200.245
      monitor bgp context saegw 3333:888::2
      peer-ip-address 209.165.200.227
      bind address 209.165.200.228
    #exit
    ip route static multihop bfd srp 209.165.200.229 209.165.200.245
    ip route 209.165.201.1 209.165.202.129 209.165.200.230 SRP-Physical-2102
    ip route 209.165.201.2 209.165.202.130 209.165.200.231 SRP-Physical-2102
    ip route 209.165.201.3 209.165.202.131 209.165.200.232 SRP-Physical-2102
    ip igmp profile default
    #exit
  #exit
end
```

Sample Configurations

In following sample configuration, the N4/Sx and IPSec interface IP Addresses are defined as:

```
SMF N4/Sx - 192.0.2.1
UPF N4/Sx - 192.0.2.7
SMF IPSec - 198.51.100.1
UPF IPSec - 198.51.100.2
```



Note

- For this release, following are the recommended timer values on UPF:

  ```
  sx-protocol heartbeat retransmission-timeout 20
  sx-protocol heartbeat max-retransmissions 3
  ```

- For this release, following are the recommended timer values on SMF:

  ```
  sx-protocol heartbeat retransmission-timeout 20
  sx-protocol heartbeat max-retransmissions 5
  ```

Control Plane

IPSec Configuration

```
config
  context EPC-CP
    ip access-list foo0
      permit ip host 192.0.2.1 host 192.0.2.7
    #exit
    ipsec transform-set A-foo
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
    crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key key secret
      authentication remote pre-shared-key key secret
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 15000
      ikev2-ikesa notify-msg-error no-apn-subscription backoff-timer 0
      ikev2-ikesa notify-msg-error network-failure backoff-timer 0
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa configuration-attribute p-cscf-v6 private length 0
      ikev2-ikesa configuration-attribute p-cscf-v6 iana length 0
      keepalive interval 50
      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
        lifetime 300
        rekey keepalive
      #exit
      peer 198.51.100.2
      ikev2-ikesa policy error-notification
      notify-payload error-message-type ue base 0
      notify-payload error-message-type network-transient-minor base 0
      notify-payload error-message-type network-transient-major base 0
      notify-payload error-message-type network-permanent base 0
    #exit
    interface CP_IPSEC loopback
      ip address 198.51.100.1 255.255.255.0
```

```
   crypto-map foo0
    #exit
end
```

N4/Sx Configuration

```
   sx-service SX-1
      instance-type controlplane
      bind ipv4-address 192.0.2.1
      sx-protocol heartbeat retransmission-timeout 20
      sx-protocol heartbeat max-retransmissions 5
   exit
```

User Plane

IPSec Configuration

```
config
  context EPC-UP
    ip access-list foo0
      permit ip host 192.0.2.7 host 192.0.2.1
    #exit
    ipsec transform-set A-foo
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
    crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key key secret
      authentication remote pre-shared-key key secret
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 15000
      ikev2-ikesa notify-msg-error no-apn-subscription backoff-timer 0
      ikev2-ikesa notify-msg-error network-failure backoff-timer 0
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa configuration-attribute p-cscf-v6 private length 0
      ikev2-ikesa configuration-attribute p-cscf-v6 iana length 0
      keepalive interval 50
      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
      #exit
      peer 198.51.100.1
      ikev2-ikesa policy error-notification
      notify-payload error-message-type ue base 0
      notify-payload error-message-type network-transient-minor base 0
      notify-payload error-message-type network-transient-major base 0
      notify-payload error-message-type network-permanent base 0
    #exit
    interface UP_IPSEC  loopback
      ip address 198.51.100.2 255.255.255.0
   crypto-map foo0
    #exit
end
```

N4/Sx Configuration

```
   sx-service SX-1
      instance-type userplane
      bind ipv4-address 192.0.2.7 ipv6-address dddd:51:31:1:209::
      sxa max-retransmissions 12
      sxb max-retransmissions 12
      sxab max-retransmissions 12
      sx-protocol heartbeat interval 30
      sx-protocol heartbeat retransmission-timeout 20
```

```
      sx-protocol heartbeat max-retransmissions 3
    exit
```

SMI strongSwan Configuration

The following is a sample configuration to spawn the SMI strongSwan pod:

```
SMI:
addons strongswan enabled
strongswan connections N4_IPSec_RCM3
  auto add
  keyexchange ikev2
  type tunnel
  left 192.12.31.202
  right 50.50.29.5
  leftsubnet 192.12.31.202/24
  rightsubnet 50.50.29.4/32
  leftauth psk
  rightauth psk
  leftsendcert never
  psk starent
  esp aes128-sha1,aes128-sha256-prfsha256
  ike aes128-sha1-modp1024,aes128-sha256-modp1536
  reauth no
  dpdaction clear
  dpddelay 300
  dpdtimeout 60
  closeaction none
  server-cert "-----BEGIN CERTIFICATE-----MIIDjTCCAnWgAwIBAgIUF6njegbcarj2oq
/x9c2+utqPThUwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3R
hdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA5MDcwOTQ0MDdaFw0zM
jA5MDQwOTQ0MDdaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXRlMSEwHwYDVQQKDBh
JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkKA
vGj94OWcFV8j7Enpr5HHqQxakb7hD0fETPByMIb9lPA73AM/3g7YjyIuAFhhs/fx4ZbFQJKDUVjiK/
PE7Mq/Opw5vIsUAgyhors2goa3YvBEPCmTk4fPz21hkWLHZgTARKq3XkgdCAO7kB7UsJpxVBSGg0A
52bIy3bB5C8YNa4rTrafVqzzFdYrQfAama2lpLrfxI7TzoZ6qK1LUDe8U7K/Ln/LJOeqxXClGSEzz
GRBqG41FeU18u3mpJ1pDINUJj7E7r+UN58aTwMoW3/ThCL/2ou+vjTVN7TDzva6XdJPNBCMA5dKEh
0EF10rMo8nmtLzo4UW9NBKMbiv7KPAgMBAAGjdTBzMB8GA1UdIwQYMBaAFC/Lvz0LAowgIkydSpKNUwy/
wHzJMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMDgGA1UdEQQxMC+CFWNuZHAtbmFybWFkYS1tYXN0ZXIt
M4cEwAwfyocQIAFIiAGSEjEAAAAAAAACAjANBgkqhkiG9w0BAQsFAAOCAQEAB6WUQI4qgEHQ8E5sYwzP
zw5KC/zGP2WZIkBfcs8ReiGmLJlC8n8uceWH12ZbFwY75j3EBFfqkmnNXftQGmuU8oGyZsuPDpmEySo+
nE28xnQDZDGzABLZWLSZqqeR6obnYUKvDho14kd40o1hnVlaONw1mrwc/QyFvn3tOwoYnXgaktGM01Fu
cQY1Kc33DvJx3n7fOsdoOLRm9jEENYT3Dv8b6/Ezr2mMHRhAwuoaFpvOSc/eLJy0QO7RpQLpHcRmnh9n
XO+gccB+e0YzvuBS5PONt8wjNSCKl46ZW4F9jpvehR8P/rvH/3VbwDaa8c6xARHNxzNcfq5S4tK/f58RSA
==-----END CERTIFICATE-----"
  server-priv-key "$8$gFVXFkFlJplgshiCqWs222+/vkNL5suwjGgqQVwhm1HEIvNp5ViKE8Stz7NK
jubZL1uXIDuy\nTbZmSPp8gIyWFTAJadMNjSoJswWhFYHX+aYoliCIdWQEUFSnJTz2Gofjgex3kM7g8iFkw
BNb\nB6qnSOV2WwMHown1ZfIGEZQAZ6B6iNnQbIHVrOgsyAY6akkyoNzIuc1gFdijQ2W56wW6tQR1\n5EpV
5zweW/Nr0RoOma+ZjpKY8L2VDW30SZ+VwbeTWexrVVfTbYifYYURekyIr6SbK4wFwt+3\nLhBUIr/6zvOlV
QBh4GVEheB5IJid0vHSI3N91sxX+VRaBodSKyw22HpC5BgWanarhkd1KfCT\nmoLzQ7+Nw0X0UfbKTLM5G8
IhXGxqccjl8Jb8nZf490MGx+XrYMkNcFNJ7ua7bxNhl1goTyUs\n4Wbw9hcviv9ZD4leTwnSlqnv5Yfr0ED
GJVrkW2zFv808fKdkJ2rO9T843u9DOrKrFo6XMPT2\n3JU9RL6zlI6bUMTHRqy2xLDfTtDBrD5jg3joJdD7
nkQfCW6cS79cXTBSLTc79p8otX8Jy56n\nkg1uDmQvdY+PgmbByvjQLrPkFr1BQ0C/g5F1uTPSiy2bNGr9l
QF8LfV8kakQMsi+FT0BJbil\nXHxw9pMu2p9srsZRmiBUw4PMq5nQ69jqDJweoNwzjqcJKBvIV1mvKIzHll
Ha0jOqA/FqASn0\nXzmKuZwG49c8qJaE5JBTLTjxeD7tG6A5XuewKynAYWnynT/0xP0mMDMcwEPdOt4e/L4
WJUOJ\nUn4EVo9EMOeG/eRzqILwAbeo2faQtY3HR7c5qMGgnBk903zIVsxl7SP4ujR0HuRw3zq7co5y\n6O
GSmu5Q79EeHezgxn+uiCsPSBwD3gkjvCerdBi8lKPptp//J+XyFA6MdgTbjzb+MxsDXszt\nyXaojBhn9t1
RxwVepAyVesm511JdH/IeDGIYY21Q2DT/k3RT490yKQSu2U2J3n49PCsEtHTQ\nbJo0WmoBVzkysE5kkL2R
MMD6PN+oV8eSqXJHkc1lAFhTpB+TqXcUI+QM0DsLdC1KOr7I5a6P\nl7jdyFFKlbPW8bOe2BB+bKA+5lOQ0
ygb9hlM76WdKmr8hhaimIuH6covaqISrFJJ0IvXcaWS\nhiatKxAq/KhkdczeM0WS6Z8PFlUwRoqgL8X8tn
v1C6tvJbUNLOPgTbHYjkflOyEeFHgXVlXi\nnzE4iAADsRTaMT/3G5YuPjk7+0lmtiZRKHXUPy7LyRwJHNZ
vkaEY+LALhA0ukMpH4DcdDibh\n16kPVUPvWZNZ2Mw3kILH5raqICdGYDDuW1SwCLBeV2pqMuaTzFiSPpLt
5AFXKtF5u9vA+VIC\nJcWP77XVbPTkbsnSBtxFy32RlZY5rx6hLEf/XsMnPAOJvprZvWuc7F+KzrexMmYAY
bJbKE3S\n8POaPet9r8+mPkQf+F5NQD7r3iz0iZ7Hj4IVzm5cvlo9yfatvm03cDplBhVAvsa5dTRuJCq+\
```

```
n0UMpf6PbcZI3vhVjIGm7iR+SVSVrq27+lGW76MpnpGwffm/gnyVvg97wl21LmPuool6vKljs\nc9DBybr
dOIwf6gkHkfwDPITGZEbc0SiH3AnIc8Z6HPiCqm1jLJ+2PfC6xnJdLRgkB8sJA1UC\n1VikR2YOvSR26Z6
PI5x7Nhq73jlRMr2N7cvrbBgfjmQyluHa0H/fnOYh4/D6Va8ROWCM4Ca3\nGOPeGn/oJAY1qogLSad33OI
DLsExvyh52x8KvrhdBCRRY5EabXa97XG0TtRTgt6NDd9NwZZ0\n2xxE06VUMS307UBAmyQn7vuezVqcHtv
3H9NnDFPRVLsnyreNo04VjZN6PHtqqOei/sLfL1GK\nVzvleeNGfSAvh1kmFh13f9p1jXgnTwt4iFErpaR
1lvk5K1RoF/+Sjo0HYhETvJFxA/yd/2I0\nZQe3ob/W4hBqI069yQjHbk+9L6kGWzQl3Tl8Lw1/YU/2AXS
zW8V9wCV0OhNLwQezt7a8EBm4\nX3CsPNVhhixhdvC/rSrXFPJnXy0mrcuCXhqLitWRA5VO6883Yry7ldP
uHzcVTyLCxYm0PWaT\nif4TQ6BxvT/gz7Ic6F3dO/QwMKoyeA7RoRR3XpnFcN1QMNTrF17jg17hDFjJwBO
dsq1gfau5\nUDeG6HihvcggYwnbkTprwaHflK/tsTCReNi+j/+ei+4DIe0f2vFgqaGjHdaa6qGkpSXks4L
R\nhyVd9/y+"
  nodes master-3
  exit
 exit
strongswan connections N4_IPSec_V6
  auto add
  keyexchange ikev2
  type tunnel
  left 2001:4888:192:1231::202
  right 2001:4888:50:50::22
  leftsubnet 2001:4888:192:1231::202/64
  rightsubnet 2001:4888:50:50::21/128
  leftauth psk
  rightauth psk
  leftsendcert never
  psk starent
  esp aes128-sha1,aes128-sha256-prfsha256
  ike aes128-sha1-modp1024,aes128-sha256-modp1536
  reauth no
  dpdaction clear
  dpddelay 300
  dpdtimeout 60
  closeaction none
  server-cert "-----BEGIN CERTIFICATE-----MIIDjTCCAnWgAwIBAgIUF6njegbcarj2oq
/x9c2+utqPThUwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3R
hdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA5MDcwOTQ0MDdaFw0zM
jA5MDQwOTQ0MDdaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBh
JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkKA
vGj94OWcFV8j7Enpr5HHqQxakb7hD0fETPByMIb9lPA73AM/3g7YjyIuAFhhs/fx4ZbFQJKDUVjiK/
PE7Mq/Opw5vIsUAgyhors2goa3YvBEPCmTk4fPz21hkWLHZgTARKq3XkgdCAO7kB7UsJpxVBSGg0A
52bIy3bB5C8YNa4rTrafVqzzFdYrQfAama2lpLrfxI7TzoZ6qK1LUDe8U7K/Ln/LJOeqxXClGSEzz
GRBqG41FeU18u3mpJ1pDINUJj7E7r+UN58aTwMoW3/ThCL/2ou+vjTVN7TDzva6XdJPNBCMA5dKEh
0EF10rMo8nmtLzo4UW9NBKMbiv7KPAgMBAAGjdTBzMB8GA1UdIwQYMBaAFC/Lvz0LAowgIkydSpKNUwy/
wHzJMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMDgGA1UdEQQxMC+CFWNuZHAtbmFybWFkYS1tYXN0ZXIt
M4cEwAwfyocQIAFIiAGSEjEAAAAAAAACAjANBgkqhkiG9w0BAQsFAAOCAQEAB6WUQI4qgEHQ8E5sYwzP
zw5KC/zGP2WZIkBfcs8ReiGmLJlC8n8uceWH12ZbFwY75j3EBFfqkmnNXftQGmuU8oGyZsuPDpmEySo+
nE28xnQDZDGzABLZWLSZqqeR6obnYUKvDho14kd40o1hnVlaONw1mrwc/QyFvn3tOwoYnXgaktGM01Fu
cQY1Kc33DvJx3n7fOsdoOLRm9jEENYT3Dv8b6/Ezr2mMHRhAwuoaFpvOSc/eLJy0QO7RpQLpHcRmnh9n
XO+gccB+e0YzvuBS5PONt8wjNSCKl46ZW4F9jpvehR8P/rvH/3VbwDaa8c6xARHNxzNcfq5S4tK/f58RSA
==-----END CERTIFICATE-----"
  server-priv-key "$8$jW1TFB0/rJW4V6NrVjk4+1KE7Dw6ynkP3Bqtiwp2k+GQDrI4bX2n+a6Yvyeq
zzKdQ+EQLuy6\ncj9xOrxtNflmzaptNF9Ku786m934ID9hzmC8ISya6/4f2Xu+WdG6uIJl2jDhB/3B2PIc
b6VQ\nV7c4GmwPRNBlIZTVMvTS/2xiUx9bdXIQTVzl2Sc3bZqwLJ6ho/qr4r++T7blVZ16j5sYxUI6\nat
ZKNMMk8+0aoH4UaOd5vtoSkhXCLXkfyrGYagx4KceKxPxSciSEptAzM36py7hDqazW5epU\nFaAnw3PMhq
Ut1r790CaG3VZR5WpcJVkHbdpf0iMCt6pJjNeNlL7BTvns+vo16Mcgt0pyi6Rj\nBAo5lSzog9max0EiRk
spb4a91DFX8mV4tzTy0RCzbgkuzdZ3ecbB9OOvrkWOv7dLiWsZe66Q\nrQA4SLH7eOkgRQvDzqmx3DpqXP
7rebptkLAGXAxZV5uvUuyivdal0EPiB6fu3OwP+gJweZIg\nLjIVbJsREgN7YdukihOmk/xbSMK25Eu3X3
yI1Y55vvQfsY08WEfKBO+Alzjrvz4ABydVJcEE\nqywkSUK/j0VksGvN4lzgely07tpz22VjMTrxJvoWB+
5j9j183T/C1Wgf53miFz2z8ak0NYYe\n2AEP9NNs4tFkB9bY9JQsFv6zY3J+2hQ8iyCiYIROd5ItRyLenO
Bt1fKGp5FHg7dlPuOz0VoI\nUm7GlEexMIycNEr9rzOqzBbMiH5c53htY4iQWFvOARHhw2f5GWPZOIe8Z8
uTq4k5iUjWmaLa\nfhNMXIGX2QNgoduZwXiX6yv3gCpK8WDgF4dlvPjFB+f+iA+QyBlc5AYZuE/2yjYRCr
aaPkzx\ndrWm+Uh18d1YdmQq4ss/rUY4Q0DxDblv94Xx64NIq8dbnY7Zehjs9LXXHk2X6daSTC/FYIY+\n
J/Sks+tmnZ489Tojo/F5dS9iVVstP68MdKOl4OC53lDkqcNl0xhniu2nneS6HTlzUrKFSi4I\n3eRW0FwK
ONKrePxKdObZFB+FvV+xOa2UKnXBbpIh/ENFE0XnADP7Ljox3YsZZpvnXTcz7OcE\nq1b8ggtLt6KyWDb0
tdZljLAb4posj1NioJQzyxHT0gsdfkZxtWiqgt65gqXS/iDo9XXdFEj1\n1Gr07SoE+HwoJIPzAG/8fNhm
```

```
27CCYaUW1uWJAOUt9I5UCbER+2kFaVC+odEY2W5/Hfc/gWAy\nSRd6/46kvjN/SzabIdb1yqr68G4LIrHg
1kEBoAf9hXSkD7WY2SMSjl950Co4Cq6zVbk6PAcX\n2ET02FhFewiq+TamVNr0/ruyPohyr1Cpgjqzvx6s
+s7EMWOPJh+XEh8PPBKY+DcDEr2RBIcZ\n4O9uAzwiYTm1x4u8dw5kKRd+H8HFobgaQ18i3IfCdZ4DXyrq
mMrxOw52fGIuAd3Ln2j/AitZ\nQP61dlQlwWPHX7ykvXqCP6oZnfbMUVW3iIdFauZLiCDZkX98UXY3IZUi
Eq13GL6KZtKwFAbu\nqHYEtb5OJRiHRZnqmoOf7BQjC3cdDTBpmPd/s9JCSejqSahlSaSl4Qghbba35HIG
o9PVyks3\nGny6P6twYnDCHLdXbmfE+HE71MnRRPd63CNp+SeX/pP5nBhu6RU/K61ovPrSqcsmo8GiytZB
\ndtVH7nYk3ZUWan04us/bd5zNZfrQ1mCF4rS4KGprQ0N7xWSCilMI49aIxSCNM9WkYl8HAEWA\n1IceEZ
RxHxeltl3JMNTxwFlkP4i4IEalf//Tidrd13jka0NnnjOsboUgn7lay3LvsC6zsIGN\nkP0sTGI1hHj9OL
1iKkw6IhTS1Py5Bjof+XPE844QwOY6Qj6GTd5F/GQJOOD3rL2J/S651TvJ\nsnKM5roovBVb1dUANC/Eay
frpC/2w8wjqPQ/O02SzVNSbZOIPn8P8BV3Ql+NC8rEWL1FZMkI\nkM1AsZTx8BQ0Z1Haf4uhtV5+/29ula
EqEiTH1x2QDV9idWPekqr7eC3009YoGESWHuIH/JE/\n76Rr2zi4wK0JVecxbCGDOynIRFE3I3gRdxgtTi
GrOMe2WdqsUDvDkcijCVpHo0JS3jFVONR8\nxbEo7RpxdrQJ5Zr/u/vx1jnQV/bXTzwlkqoy1g9C3V1m4m
NrqYz62taNTF7+NEVyWC/cp5CU\n5SDuAs3JmFyLaRvyU5SsmDbzlyj+z3DUaByHWlWtC5+klwXYoZOKIy
8zNj+1Kzxosk1wiVX1\nqT4CoAKX"
```

To validate the IPSec tunnel CLI on the SMF protocol pod and validate the *ipsec.yaml* file on SMF, see the *Interfaces Support > N4 Interface* chapter for sample SMI strongSwan configuration.

For the latest strongSwan configurations, see the *Ultra Cloud Core Subscriber Microservices Infrastructure Operations Guide*.

Monitoring and Troubleshooting

This section contains the sample CLI command output of show commands for the N4/Sx over IPSec feature in both SMF and UPF.

show crypto ikev2-ikesa security-associations summary

```
I - Initiator
  R - Responder
Mgr                                                                    Lifetime
ID  VPN Local IPSec GW:Port   Remote IPSec GW:Port  State             /Remaining
=== === ==================== ==================== ================ ===========
54  2   192.168.170.55 :500   192.168.196.55 :500   AUTH_COMPLETE(I) 86400/16448

1 IKEv2 Security Association found in this context.
```

show crypto ipsec security-associations summary

```
+------ SA state:           (E) - Established
      |                         (P) - Partially Established
      |                         (N) - No SAs
      |
      |+----- Rekey/Keepalive:    (D) - Rekey Disabled
      ||                          (E) - Rekey Enabled/No Keepalive
      ||                          (K) - Rekey Enabled/Keepalive
      ||
      ||+---- Crypto Type:        (D) - Dynamic Map
      |||                         (I) - IKEv1 Map
      |||                         (J) - IKEv2 Map
      |||                         (M) - Manual Map
      |||                         (C) - CSCF Map
      |||
      |||
      VVV           Map Name                                                 Rekeys En Pkts
    De Pkts
===== === ============================================================== ====== ==========
 ==========
1     EDJ foo0                                                              0      3496
     3496
```

```
1 Crypto Map Found.
1 Crypto Map Established.
```

To validate the IPSec tunnel CLI on the SMF protocol pod and validate the *ipsec.yaml* file on SMF, see the *Interfaces Support > N4 Interface* chapter for sample SMI strongSwan configuration.

For the latest strongSwan configurations, see the *Ultra Cloud Core Subscriber Microservices Infrastructure Operations Guide*.

SMI strongSwan Validation

The following is a sample SMI strongSwan configuration to validate the IPSec tunnel CLI on SMF protocol pod:

```
cloud-user@cndp-narmada-master-1:~$ kubectl exec -ti strongswan-d7zzp -n smi-strongswan --
 ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.3, Linux 5.4.0-122-generic, x86_64):
uptime: 14 days, since Sep 19 16:36:02 2022
malloc: sbrk 6221824, mmap 0, used 3867536, free 2354288
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 15
loaded plugins: charon aesni aes des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation
constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl af-alg fips-prf
gmp curve25519 xcbc cmac hmac ccm gcm drbg curl files attr kernel-netlink resolve
socket-default stroke vici updown eap-identity eap-dynamic eap-tls xauth-generic counters
Listening IP addresses:
10.105.90.166
2001:420:5504:2004::90:18
71.71.71.15
71.71.71.70
71.71.71.72
71.71.71.73
192.12.31.21
2001:4888:192:1231:42a6:b7ff:fe3b:7161
2001:4888:192:1231::21
192.12.31.203
192.12.31.206
192.12.31.207
192.12.31.208
192.12.31.209
192.12.31.210
192.12.31.211
192.12.31.213
192.12.31.214
192.12.31.215
2001:4888:192:1231::203
2001:4888:192:1231::206
2001:4888:192:1231::207
2001:4888:192:1231::208
2001:4888:192:1231::209
2001:4888:192:1231::210
2001:4888:192:1231::211
2001:4888:192:1231::213
2001:4888:192:1231::214
2001:4888:192:1231::215
2001:4888:192:1231::121
192.12.31.121
192.12.31.205
192.12.31.212
2001:4888:192:1231::205
2001:4888:192:1231::212
192.12.31.202
192.12.31.221
192.12.31.222
```

```
2001:4888:192:1231::202
2001:4888:192:1231::221
2001:4888:192:1231::222
192.50.0.1
fd00::1
192.115.3.37
Connections:
N4_IPSec_RCM1: 192.12.31.202...50.50.27.5 IKEv2, dpddelay=300s
N4_IPSec_RCM1: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM1: remote: [50.50.27.5] uses pre-shared key authentication
N4_IPSec_RCM1: child: 192.12.31.0/24 === 50.50.27.4/32 TUNNEL, dpdaction=clear
N4_IPSec_RCM2: 192.12.31.202...50.50.28.5 IKEv2, dpddelay=300s
N4_IPSec_RCM2: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM2: remote: [50.50.28.5] uses pre-shared key authentication
N4_IPSec_RCM2: child: 192.12.31.0/24 === 50.50.28.4/32 TUNNEL, dpdaction=clear
N4_IPSec_RCM3: 192.12.31.202...50.50.29.5 IKEv2, dpddelay=300s
N4_IPSec_RCM3: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM3: remote: [50.50.29.5] uses pre-shared key authentication
N4_IPSec_RCM3: child: 192.12.31.0/24 === 50.50.29.4/32 TUNNEL, dpdaction=clear
N4_IPSec_V6: 2001:4888:192:1231::202...2001:4888:50:50::22 IKEv2, dpddelay=300s
N4_IPSec_V6: local: [2001:4888:192:1231::202] uses pre-shared key authentication
N4_IPSec_V6: remote: [2001:4888:50:50::22] uses pre-shared key authentication
N4_IPSec_V6: child: 2001:4888:192:1231::/64 === 2001:4888:50:50::21/128 TUNNEL,
dpdaction=clear
N4_IPSec: 192.12.31.202...50.50.21.5 IKEv2, dpddelay=300s
N4_IPSec: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec: remote: [50.50.21.5] uses pre-shared key authentication
N4_IPSec: child: 192.12.31.0/24 === 50.50.21.4/32 TUNNEL, dpdaction=clear
Security Associations (5 up, 0 connecting):
N4_IPSec_RCM1[1345]: ESTABLISHED 96 minutes ago,
192.12.31.202[192.12.31.202]...50.50.27.5[50.50.27.5]
N4_IPSec_RCM1[1345]: IKEv2 SPIs: bc79a16793c7d7eb_i 087bb5cd20fd2f34_r*, rekeying in 72
minutes
N4_IPSec_RCM1[1345]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM1{2501}: INSTALLED, TUNNEL, reqid 2, ESP SPIs: cd664851_i 13009213_o
N4_IPSec_RCM1{2501}: AES_CBC_128/HMAC_SHA2_256_128, 900 bytes_i (17 pkts, 16s ago), 829
bytes_o (17 pkts, 16s ago), rekeying in 36 minutes
N4_IPSec_RCM1{2501}: 192.12.31.202/32 === 50.50.27.4/32
N4_IPSec_RCM3[1343]: ESTABLISHED 97 minutes ago,
192.12.31.202[192.12.31.202]...50.50.29.5[50.50.29.5]
N4_IPSec_RCM3[1343]: IKEv2 SPIs: 1a50e1d11dfeacb7_i 7be50275473937a3_r*, rekeying in 65
minutes
N4_IPSec_RCM3[1343]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM3{2499}: INSTALLED, TUNNEL, reqid 5, ESP SPIs: cd6f47ec_i 13009213_o
N4_IPSec_RCM3{2499}: AES_CBC_128/HMAC_SHA2_256_128, 1328 bytes_i (25 pkts, 26s ago), 1217
bytes_o (25 pkts, 26s ago), rekeying in 30 minutes
N4_IPSec_RCM3{2499}: 192.12.31.202/32 === 50.50.29.4/32
N4_IPSec_RCM2[1341]: ESTABLISHED 103 minutes ago,
192.12.31.202[192.12.31.202]...50.50.28.5[50.50.28.5]
N4_IPSec_RCM2[1341]: IKEv2 SPIs: 26fd8455c09927ab_i 78c5379f6559be4b_r*, rekeying in 60
minutes
N4_IPSec_RCM2[1341]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM2{2500}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6f5243c_i 13009213_o
N4_IPSec_RCM2{2500}: AES_CBC_128/HMAC_SHA2_256_128, 1026 bytes_i (19 pkts, 0s ago), 917
bytes_o (19 pkts, 0s ago), rekeying in 34 minutes
N4_IPSec_RCM2{2500}: 192.12.31.202/32 === 50.50.28.4/32
N4_IPSec_V6[1339]: ESTABLISHED 2 hours ago,
2001:4888:192:1231::202[2001:4888:192:1231::202]...2001:4888:50:50::22[2001:4888:50:50::22]
N4_IPSec_V6[1339]: IKEv2 SPIs: 64e5d5e102e885e7_i 9062914577d9eb95_r*, rekeying in 36 minutes
N4_IPSec_V6[1339]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_V6{2498}: INSTALLED, TUNNEL, reqid 3, ESP SPIs: c25a2531_i 0f009d13_o
N4_IPSec_V6{2498}: AES_CBC_128/HMAC_SHA2_256_128, 6817 bytes_i (89 pkts, 17s ago), 6326
bytes_o (89 pkts, 17s ago), rekeying in 17 minutes
N4_IPSec_V6{2498}: 2001:4888:192:1231::202/128 === 2001:4888:50:50::21/128
```

```
N4_IPSec[1337]: ESTABLISHED 2 hours ago, 192.12.31.202[192.12.31.202]...50.50.21.5[50.50.21.5]
N4_IPSec[1337]: IKEv2 SPIs: 9af4e1f24dcc0edb_i 6fcea88758803d37_r*, rekeying in 26 minutes
N4_IPSec[1337]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec{2497}: INSTALLED, TUNNEL, reqid 4, ESP SPIs: cc7c3bf1_i 0f009c13_o
N4_IPSec{2497}: AES_CBC_128/HMAC_SHA2_256_128, 6844 bytes_i (121 pkts, 19s ago), 5693 bytes_o
 (121 pkts, 19s ago), rekeying in 4 minutes
N4_IPSec{2497}: 192.12.31.202/32 === 50.50.21.4/32
cloud-user@cndp-narmada-master-1:~$
```

The following is a sample SMI strongSwan configuration to validate the *ipsec.yaml* file on SMF:

```
cloud-user@cndp-narmada-master-1:~$ kubectl exec -ti strongswan-d7zzp -n smi-strongswan --
 cat /etc/ipsec.conf
conn N4_IPSec_RCM1
leftcert=/etc/ipsec.d/certs/N4_IPSec_RCM1.cert.pem
auto=add
closeaction=none
compress=no
dpdaction=clear
dpddelay=300
dpdtimeout=60
esp=aes128-sha1,aes128-sha256-prfsha256
ike=aes128-sha1-modp1024,aes128-sha256-modp1536
ikedscp=000000
ikelifetime=3h
keyexchange=ikev2
left=192.12.31.202
leftallowany=no
leftauth=psk
leftsendcert=never
leftsubnet=192.12.31.202/24
lifetime=1h
mobike=yes
reauth=no
rekey=yes
right=50.50.27.5
rightallowany=no
rightauth=psk
rightsubnet=50.50.27.4/32
sha256_96=no
type=tunnel
```