



# N4/Sx over IPsec

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 2](#)
- [Recommended Timers, on page 3](#)
- [Sample Configurations, on page 10](#)
- [Monitoring and Troubleshooting, on page 13](#)

## 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	<i>UCC 5G UPF Configuration and Administration Guide</i>

### Revision History

Revision Details	Release
First introduced.	2022.04.0

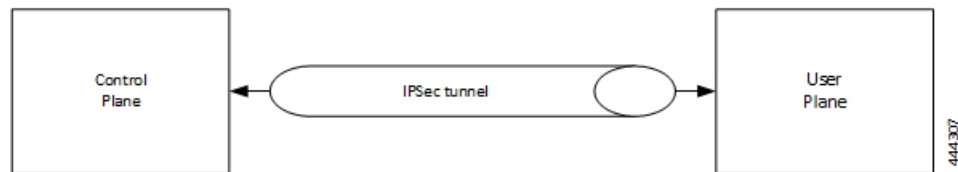
## Feature Description

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.

**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:

$$((\text{max-retransmissions} + 1) * \text{retransmission-timeout-ms}) * 2 = \text{Keep-alive interval}$$

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

### 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
```

## Recommended Timers

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

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

## 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
```

## Static Route for Multihop BFD Configuration

```

        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

```

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
ID  VPN  Local IPsec GW:Port  Remote IPsec GW:Port  State  Lifetime
===  ===  =====  =====  =====  =====  =====
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*.

