

IPSec 経由の N4/Sx

- 機能の概要と変更履歴 （1 ページ）
- 機能説明 （2 ページ）
- 推奨タイマー （4 ページ）
- 設定例 （11 ページ）
- モニタリングおよびトラブルシューティング （13 ページ）

機能の概要と変更履歴

要約データ

表 *1*: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.04.0

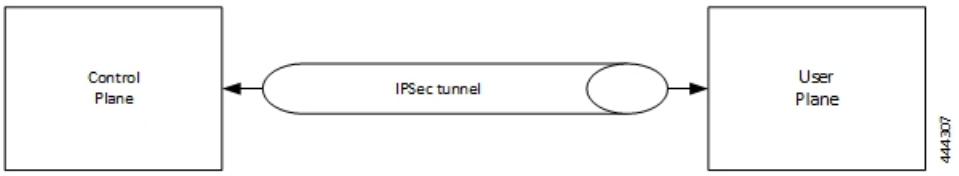
機能説明

Internet Protocol Security（IPSec）は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピア セキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

Cisco Cloud Native 5G では、セッション管理機能（SMF）とユーザープレーン機能（UPF）の両方でトンネルモードで IPSec 機能を使用できます。IPSec 暗号マップは、それぞれのノードの適切なインターフェイスで関連付けられます。IPSec トンネルは、各 SMF または UPF のペア間に明示的に作成されます。この機能は、IPv4 および IPv6 トンネリングモードをサポートします。N4/Sx サービスの構成に変更はありません。

IPSec トンネルモードは、IP パケット全体をカプセル化して、2 つのゲートウェイ間で仮想セキュアホップを提供します。これは、VPN のような機能を形成し、IP パケット全体を別のパケット内にカプセル化して接続先に配信します。完全な IP ヘッダーとペイロードがカプセル化されます。

図 *1 : IPSec* トンネル経由の *N4/Sx*



VPP を実行している UPF NF で IPSec 経由の N4/Sx が有効になっている場合、IPSec 経由の N4/Sx 機能を機能させるには、「VPP パラメータ」で次のパラメータを使用する必要があります。

VPP_DPDK_DATA_SIZE=5120

VPP パラメータは CD-ROM の **staros-para.cfg** ファイルに保存されます。この構成は、起動時に UPF によって読み取られ、VPP に適用されます。

（注） このパラメータは、VPP バージョン 19.08 までサポートされます。このパラメータにより、約 800 MB のメモリオーバーヘッドが発生します。この機能を使用する前に、この条件を考慮する必要があります。UPF の RAM が少ない場合、機能が正常に動作するように追加の 1 GB の RAM メモリを VM に割り当てる必要があります。

IPSec のサポートに関する詳細については、StarOS の「*IPSec* リファレンス」を参照してください。

IKEv2 キープアライブメッセージ（デッドピア検出）

N4/Sxインターフェイス向けIPSecは、IPSecトンネルの両端から発信される、Dead Peer Detection（DPD; デッドピア検出）とも呼ばれる IKEv2 キープアライブメッセージをサポートします。RFC 3706 に従い、DPD はピア間の通信とトンネルの可用性を検証するために必要なメッセージングを簡素化するために使用されます。

IPSec DPD は、任意構成です。無効になっている場合、IPSec ノードは、DPD 要求を開始しません。ただし、ノードはそのDPD構成に関係なく、常にピアノードが開始するDPD Availabilityメッセージに応答します。

次の方法を使用して、IPSec 経由の N4/Sx 機能が設定されている場合のキープアライブ間隔値を計算できます。

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

キープアライブ間隔値は、DPDがトリガされるまでIPSecトンネルが稼働状態を維持する時間を指定します。

例：

次に、N4/Sx サービスでの **show configuration context** *context-name* **verbose** CLI コマンドの出力例を示します。

```
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
```

ここでは、**max-retransmissions** の値は 4、**retransmission-timeout-ms** は 5000 です。したがって、キープアライブ間隔の値は 50 になります。

((max-retransmissions + 1) * retransmission-timeout-ms) * 2 = キープアライブ間隔

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

IKESA キー再生成

UPF は、IKESA キー再生成とIPSecキー再生成の両方をサポートします。

IKESA キー再生成の場合は、**lifetime** *interval* CLI を **ikev2-ikesa transform-set** *transform-set* で設定する必要があります。**crypto map** 構成で、**ikev2-ikesa rekey** を構成する必要もあります。次に、構成例を示します。

```
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
```

推奨タイマー

次の表に、IPSec、N4/Sx、およびSRPに関連するCLIコマンドの推奨タイマー値を示します。

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*

推奨設定

以下に、N4/Sx および SRP over IPSec に関連する推奨構成と制限事項を示します。

- SMF と UPF 間のマルチホップ BFD タイマーは、7 秒に設定する必要があります（データ UPF の場合）。
- シングルホップ BFD は、すべてのコンテキスト（SMF GW/課金情報および UP Gn/Gi）で有効にする必要があります。
- シャーシ間マルチホップ BFD は、SMF-SMF ICSR および UPF-UPF ICSR（IMS UPF）に対して有効にする必要があります。
- SRP-IPSec ACL は、IP プロトコルではなく TCP プロトコル用に設定する必要があります。
- N4/Sx-IPSec ACL は、IP プロトコルではなく UDP プロトコル向けに設定する必要があります。

SMF の構成例

マルチホップ BFD 設定 VPC-DI

次に、7 秒タイマーを使用したマルチホップ BFD の設定例を示します。

```
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
```

マルチホップ BFD 設定 VPC-SI

次に、タイマーが 3 秒のマルチホップ BFD 設定の例を示します。

```
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 の設定

以下に、推奨タイマーを使用した BGP の設定例を示します。

```
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
```

シングルホップ BFD 設定

タイマーが 3 秒のシングルホップ BFD の設定例を以下に示します。

```
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
```

マルチホップ BFD 設定のスタティックルート

次に、スタティック ルート マルチホップ BFD 設定の例を示します。

```
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
```

シングルホップ BFD 設定用のスタティックルート

次に、スタティックルートのシングルホップ BFD 設定の例を示します。

```
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 の設定

以下に、SMF での IPSec ACL の構成例を示します。

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

IPSec トランスフォームセットの設定

SMF での IPSec トランスフォームセットの設定例を以下に示します。

```
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 クリプトマップの設定

SMF での IPSec 暗号化マップの設定例を以下に示します。

```
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 の構成

以下は、SMF での N4/Sx 構成例です。

```
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
```

ルータの設定例

インターフェイスのスタティックルート

次に、インターフェイスのスタティックルートの設定例を示します。

```
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
```

シングルホップ BFD のスタティックルート

次に、シングルホップ BFD のスタティックルートの設定例を示します。

```
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
```

シングルホップ BFD のインターフェイス

シングルホップ BFD のインターフェイスの設定例を以下に示します。

```
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 の設定

以下に、推奨タイマーを使用した BGP の設定例を示します。

```
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
```

UPF の構成例

IPSec ACL の設定

UPF での IPSec ACL の構成例を以下に示します。

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

IPSec トランスフォームセットの設定

以下に、UP での IPSec Transform Set の構成例を示します。

```
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 クリプトマップの設定

UPF での IPSec 暗号マップの構成例を以下に示します。

```
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 の構成

以下は、UPF における N4/Sx の構成例です。

```
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
```

SRP の設定例

IPSec ACL の設定

次に、SRP の IPSec ACL 設定の例を示します。

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

SRP の設定

SRP の設定例を以下に示します。

```
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
```

設定例

次の構成例では、N4/Sx および IPSec インターフェイスの IP アドレスは次のように定義されています。

```
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
```

（注）

- このリリースでの UPF の推奨タイマー値は次のとおりです。

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

- このリリースでの SMF の推奨タイマー値は次のとおりです。

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

コントロール プレーン

IPSecの設定

```
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 の構成

```
   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
```

ユーザープレーン

IPSecの設定

```
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 の構成

```
   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
```

SMF プロトコル Pod で IPSec トンネル CLI を検証し、SMF で *ipsec.yaml* ファイルを検証するには、SMI StrongSwan 構成例に関する「インターフェイスサポート」>「*N4* インターフェイス」章を参照してください。

最新の strongSwan 構成については、『*Ultra Cloud Core* サブスクライバ マイクロサービス インフラストラクチャ操作ガイド』を参照してください。

モニタリングおよびトラブルシューティング

この項では、SMF と UPF の両方の IPSec 経由の N4/Sx 機能に対する show コマンドの CLI コマンド出力例を示します。

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.
```

SMF プロトコル Pod で IPSec トンネル CLI を検証し、SMF で *ipsec.yaml* ファイルを検証するには、SMI StrongSwan 構成例に関する「インターフェイスサポート」>「*N4* インターフェイス」章を参照してください。

最新の strongSwan 構成については、『*Ultra Cloud Core* サブスクライバ マイクロサービス インフラストラクチャ操作ガイド』を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。