



Sx Over IPSec

- [Revision History](#), on page 1
- [Feature Description](#), on page 1
- [Recommended Timers](#), on page 3
- [Sample Configurations](#), on page 10
- [Monitoring and Troubleshooting](#), on page 12

Revision History



Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

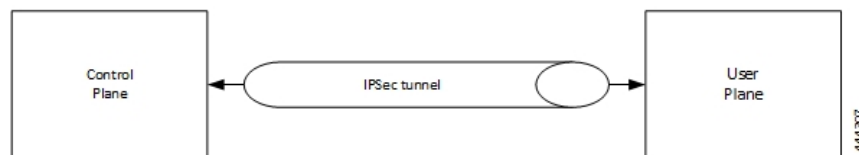
Feature Description

IPSec is a suite of protocols that interact with one another to provide secure private communications 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 CUPS, the functionality is available with IPSec in Tunnel mode both on Control Plane (CP) and User Plane (UP) nodes. The IPSec crypto-maps are associated under the appropriate interface on respective nodes. The IPSec tunnel is created between each CP or UP pair explicitly. There is no change that is required on Sx service configuration.

IPSec Tunnel Mode encapsulates the entire IP packet to provide a virtual secure hop between two gateways. It forms more familiar 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: Sx Over IPSec tunnel



When Sx over IPSec is enabled on UP node running VPP, then following parameter must be used under “UPP Param” for Sx over IPSec feature to work.

```
VPP_DPDK_DATA_SIZE=5120
```

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

**Note**

This parameter introduces a memory overhead of about 800 MB. The user must consider this condition before using the feature. If the UP 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, refer StarOS *IPSec Reference*.

IKEv2 Keep-Alive Messages (Dead Peer Detection)

IPSec for Sx interface supports IKEv2 keep-alive messages, also known as Dead Peer Detection (DPD), originating from both ends of an IPSec tunnel. 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 doesn't initiate DPD request. However, the node always responds to DPD availability messages initiated by peer node regardless of its DPD configuration.

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

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

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 for `show configuration context context_name verbose` CLI command under 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

CUPS 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 following is the known limitation of Sx Over IPsec feature:

- 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, Sx, and SRP.

IPSEC	CP	UP
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
Sx	CP	UP

IPSEC	CP	UP
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	CP	UP
hello-interval	3	3
dead-interval	15	15

Recommended Configurations

Following are the recommended configurations and restrictions related to Sx and SRP over IPsec:

- The multihop BFD timer between CP and UP must be seven seconds (for Data UPs).
- The singlehop BFD must be enabled on all the contexts (CP GW/Billing and UP Gn/Gi).
- Inter-chassis multihop BFD must be enabled for CP-CP ICSR and UP-UP ICSR (IMS UP).
- The SRP-IPsec ACL must be configured for TCP protocol instead of IP protocol.
- The Sx-IPsec ACL must be configured for UDP protocol instead of IP protocol.

Example Configurations in CP

Multihop BFD Configuration VPC DI

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

```
bfd-protocol
  bfd multihop-peer 192.1.1.1 interval 350 min_rx 350 multiplier 20
  bfd multihop-peer 192.1.2.1 interval 350 min_rx 350 multiplier 20
  bfd multihop-peer 192.1.0.1 interval 350 min_rx 350 multiplier 20
  bfd multihop-peer 192.1.6.1 interval 350 min_rx 350 multiplier 20
  bfd multihop-peer 192.1.3.1 interval 350 min_rx 350 multiplier 20
  bfd multihop-peer 192.1.4.1 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 192.1.1.1 interval 150 min_rx 150 multiplier 20
  bfd multihop-peer 192.1.2.1 interval 150 min_rx 150 multiplier 20
  bfd multihop-peer 192.1.0.1 interval 150 min_rx 150 multiplier 20
  bfd multihop-peer 192.1.6.1 interval 150 min_rx 150 multiplier 20
  bfd multihop-peer 192.1.3.1 interval 150 min_rx 150 multiplier 20
  bfd multihop-peer 192.1.4.1 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 192.0.0.1
  maximum-paths ebgp 15
  neighbor 192.0.0.101 remote-as 1000
  neighbor 192.0.0.101 ebgp-multihop
  neighbor 192.0.0.101 update-source 192.0.0.1
  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 192.0.1.9 255.111.222.0
  ipv6 address 1111:222::9/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-11
  ip address 192.0.1.10 255.111.222.0
  ipv6 address 1111:222::10/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-12
  ip address 192.0.1.11 255.111.222.0
  ipv6 address 1111:222::11/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-3
  ip address 192.0.1.2 255.111.222.0
  ipv6 address 1111:222::2/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-4
  ip address 192.0.1.3 255.111.222.0
```

Static Route for Multihop BFD Configuration

```

        ipv6 address 1111:222::3/112 secondary
        bfd interval 999 min_rx 999 multiplier 3
    #exit
interface bgp-sw1-2161-5
    ip address 192.0.1.4 255.111.222.0
    ipv6 address 1111:222::4/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
    #exit
interface bgp-sw1-2161-6
    ip address 192.0.1.5 255.111.222.0
    ipv6 address 1111:222::5/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
    #exit
interface bgp-sw1-2161-7
    ip address 192.0.1.6 255.111.222.0
    ipv6 address 1111:222::6/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
    #exit
interface bgp-sw1-2161-8
    ip address 192.0.1.7 255.111.222.0
    ipv6 address 1111:222::7/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
    #exit
interface bgp-sw1-2161-9
    ip address 192.0.1.8 255.111.222.0
    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-5 192.111.1.10 192.111.11.10
ip route static multihop bfd UP-6 192.111.1.10 192.111.12.10
ip route static multihop bfd UP-9 192.111.1.10 192.111.10.10
ip route static multihop bfd UP-10 192.111.1.10 192.111.16.10
ip route static multihop bfd UP-7 192.111.1.10 192.111.13.10
ip route static multihop bfd UP-8 192.111.1.10 192.111.14.10

```

Static Route for Singlehop BFD Configuration

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

```

ip route static bfd bgp-sw1-2161-3 192.0.1.1
ip route static bfd bgp-sw1-2161-4 192.0.1.1
ip route static bfd bgp-sw1-2161-5 192.0.1.1
ip route static bfd bgp-sw1-2161-6 192.0.1.1
ip route static bfd bgp-sw1-2161-7 192.0.1.1
ip route static bfd bgp-sw1-2161-8 192.0.1.1
ip route static bfd bgp-sw1-2161-9 192.0.1.1
ip route static bfd bgp-sw1-2161-10 192.0.1.1
ip route static bfd bgp-sw1-2161-11 192.0.1.1
ip route static bfd bgp-sw1-2161-12 192.0.1.1

```

IPSec ACL Configuration

The following is an example IPSec ACL configuration in CP.

```

ip access-list UP-1
    permit udp host 192.0.1.1 host 192.0.1.2
    #exit

```

IPSec Transform Set Configuration

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

```
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 CP.

```
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 192.1.1.1
  ikev2-ikesa policy error-notification
#exit
```

Sx Configuration

The following is an example of Sx configuration in CP.

```
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 192.1.1.1/32 Vlan1111 192.1.1.2
ip route 192.1.1.1/32 Vlan1111 192.1.1.3
ip route 192.1.1.1/32 Vlan1111 192.1.1.4
ip route 192.1.1.1/32 Vlan1111 192.1.1.5
ip route 192.1.1.1/32 Vlan1111 192.1.1.6
ip route 192.1.1.1/32 Vlan1111 192.1.1.7
ip route 192.1.1.1/32 Vlan1111 192.1.1.8
ip route 192.1.1.1/32 Vlan1111 192.1.1.9
ip route 192.1.1.1/32 Vlan1111 192.1.1.10
ip route 192.1.1.1/32 Vlan1111 192.1.1.11
```

Static Routes for Singlehop BFD

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

```
ip route static bfd Vlan1111 192.1.1.2
ip route static bfd Vlan1111 192.1.1.3
ip route static bfd Vlan1111 192.1.1.4
ip route static bfd Vlan1111 192.1.1.5
ip route static bfd Vlan1111 192.1.1.6
ip route static bfd Vlan1111 192.1.1.7
ip route static bfd Vlan1111 192.1.1.8
ip route static bfd Vlan1111 192.1.1.9
ip route static bfd Vlan1111 192.1.1.10
ip route static bfd Vlan1111 192.1.1.11
```

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 192.1.1.1/24
  ipv6 address 1111:222::1/112
```

BGP Configuration

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

```
router bgp 1000
  router-id 192.1.1.1
  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 UP

IPSec ACL Configuration

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

```
ip access-list CP-1
    permit udp host 192.0.1.1 host 192.0.1.2
#exit
```

IPSec Transform Set Configuration

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

```
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 UP.

```
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 192.1.1.2
    ikev2-ikesa policy error-notification
#exit
```

Sx Configuration

The following is an example of Sx configuration in UP.

```
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 192.1.1.1 host 192.1.1.2
#exit

```

SRP Configuration

The following is an example of SRP configuration.

```

configure
  context srp
    bfd-protocol
      bfd multihop-peer 192.1.1.1 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 192.1.1.6 chassis-to-chassis
      monitor bgp context gi-pgw 192.1.1.7
      monitor bgp context gi-pgw 3333:888::1
      monitor bgp context saegw 192.1.1.7
      monitor bgp context saegw 3333:888::2
      peer-ip-address 192.1.1.6
      bind address 192.0.1.6
    #exit
  ip route static multihop bfd srp 192.0.1.7 192.1.1.7
  ip route 192.2.2.2 255.0.0.1 192.2.2.3 SRP-Physical-2102
  ip route 192.2.2.4 255.0.0.2 192.2.2.5 SRP-Physical-2102
  ip route 192.2.2.6 255.0.0.3 192.2.2.7 SRP-Physical-2102
  ip igmp profile default
  #exit
#exit
end

```

Sample Configurations

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

```

CP Sx - 20.0.0.101
UP Sx - 20.0.0.106
CP IPSec - 192.168.4.1
UP IPSec - 192.168.4.2

```

**Note**

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

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

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

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

On Control Plane**IPSec Configuration**

```
config
context EPC-CP
  ip access-list foo0
    permit ip host 20.0.0.101 host 20.0.0.106
  #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 192.168.4.2
    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 192.168.4.1 255.255.255.255
  crypto-map foo0
  #exit
end
```

Sx Configuration

```
sx-service SX-1
  instance-type controlplane
  bind ipv4-address 20.0.0.101
  sx-protocol heartbeat retransmission-timeout 20
  sx-protocol heartbeat max-retransmissions 5
exit
```

On User Plane

IPSec Configuration

```

config
  context EPC-UP
    ip access-list foo0
      permit ip host 20.0.0.106 host 20.0.0.101
    #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 192.168.4.1
      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 192.168.4.2 255.255.255.255
  crypto-map foo0
  #exit
end

```

Sx Configuration

```

sx-service SX-1
  instance-type userplane
  bind ipv4-address 20.0.0.106 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

```

Monitoring and Troubleshooting

This section contains sample CLI command output of show commands available for the Sx over IPSec feature in both CP and UP.

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.

