IPsec Virtual Tunnel Interfaces

IPsec virtual tunnel interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify the configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Restrictions for IPsec Virtual Tunnel Interfaces

Fragmentation

Fragmentation is not supported over IPsec tunnel. You can choose to set the lower MTU on hosts to avoid packet fragments or choose to fragment the packets on any device.

IPsec Transform Set

The IPsec transform set must be configured in tunnel mode only.

IKE Security Association

The Internet Key Exchange (IKE) security association (SA) is bound to the VTI.

IPsec SA Traffic Selectors

Static VTIs (SVTIs) support only a single IPsec SA that is attached to the VTI interface. The traffic selector for the IPsec SA is always “IP any any.”

By default, Static VTIs (SVTIs) support only a single IPSec SA that is attached to the virtual tunnel interface. The traffic selector for the IPsec SA is always “IP any any”.

IPv4

This feature supports SVTIs that are configured to encapsulate IPv4 packets .

Tunnel Protection

Do not configure the **shared** keyword when using the **tunnel mode ipsec ipv4** command for IPsec IPv4 mode.

Traceroute

The traceroute function with crypto offload on VTIs is not supported.

VxLAN GPE Tunnel Interface

The VxLAN GPE Tunnel Interface cannot use the same source interface as IPsec VTI.

How to Configure IPsec Virtual Tunnel Interfaces

Configuring Static IPsec Virtual Tunnel Interfaces

```
enable
configure terminal
crypto IPsec profile PROF
set transform-set tset
exit
interface tunnel 0
ip address 10.1.1.1 255.255.255.0
tunnel mode ipsec ipv4
tunnel source loopback 0
tunnel destination 172.16.1.1
tunnel protection IPsec profile PROF
end
```

Configuration Examples for IPsec Virtual Tunnel Interfaces

Example: Verifying IPsec Static Virtual Tunnel Interface

```
Router# show interface tunnel 130

Tunnel130 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.130.1/24
  MTU 17878 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 6.6.6.130, destination 7.7.7.130
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1438 bytes
  Tunnel transmit bandwidth 8000 (kbps)
```

```
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "test")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 2d22h
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
      0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

```
Router# show crypto session

Crypto session current status

Interface: Tunnel30
Profile: 30
Session status: UP-ACTIVE
Peer: 1.1.1.50 port 500
  Session ID: 167
  IKEv2 SA: local 3.1.1.50/500 remote 1.1.1.50/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel31
Profile: 30
Session status: UP-ACTIVE
Peer: 1.1.1.51 port 500
  Session ID: 2
  IKEv2 SA: local 3.1.1.51/500 remote 1.1.1.51/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel40
Profile: 40
Session status: UP-ACTIVE
Peer: 40.40.40.2 port 500
  Session ID: 0
  IKEv1 SA: local 40.40.40.1/500 remote 40.40.40.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel41
Profile: 41
Session status: UP-ACTIVE
Peer: 41.41.41.2 port 500
  Session ID: 0
  IKEv1 SA: local 41.41.41.1/500 remote 41.41.41.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
.
.
!
```

```
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
       ia - IS-IS inter area, * - candidate default, U - per-user static ro
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 2 subnets
S        1.1.1.50 [1/0] via 101.101.101.2
S        1.1.1.51 [1/0] via 101.101.101.2
      3.0.0.0/32 is subnetted, 2 subnets
C        3.1.1.50 is directly connected, Loopback30
C        3.1.1.51 is directly connected, Loopback31
      6.0.0.0/32 is subnetted, 65 subnets
C        6.6.6.100 is directly connected, Loopback100
C        6.6.6.101 is directly connected, Loopback101
C        6.6.6.102 is directly connected, Loopback102
C        6.6.6.103 is directly connected, Loopback103

.
.
!
```