# IPSec Virtual Tunnel Interface

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

### History for the IPSec Virtual Tunnel Interface Feature

| Release | Modification |
|---|---|
| 12.3(14)T | This feature was introduced. |
| 12.4(2)T | Dynamic Virtual Tunnel Interfaces were added. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents




Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

# Restrictions for IPSec Virtual Tunnel Interface

### Stateful Failover

IPSec stateful failover is not supported with IPSec virtual tunnel interfaces.

### Proxy

Only strict IP ANY ANY proxy is supported.

### 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 virtual tunnel interface. Because IKE SA is bound to the virtual tunnel interface, the same IKE SA cannot be used for a crypto map.

### VTI versus GRE Tunnels

The IPSec virtual tunnel interface is limited to IP unicast and multicast traffice only, as opposed to GRE tunnels, which have a wider application for IPSec implementation.

# Information About IPSec Virtual Tunnel Interfaces

The IPSec virtual tunnel interface greatly simplifies the configuration process when you need to provide protection for remote access and provides an simpler alternative to using GRE or L2TP tunnels for encapsulation and crypto maps with IPSec. A major benefit associated with IPSec virtual tunnel interfaces is the reduction in overhead because the configuration does not require a static mapping of IPSec sessions to a physical interface: The IPSec VTI allows for the flexibility of sending and receiving both IP unicast and multicast encrypted traffic on any physical interface, such as in the case of multiple paths (multicast routing).

The following sections provide details about the IPSec virtual tunnel interface:

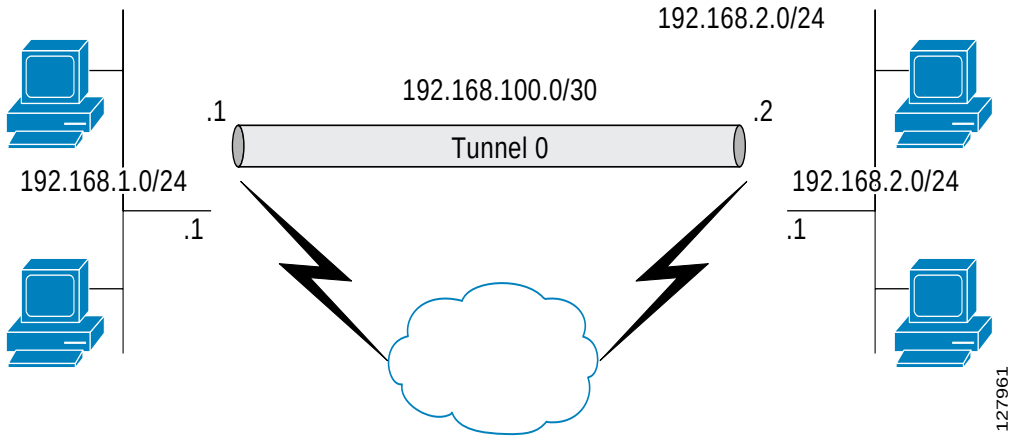
- Routing with IPSec Virtual Tunnel Interfaces, page 1234
- Traffic Encryption with the IPSec Virtual Tunnel Interface, page 1235
- IPSec Packet Flow, page 1235

## Routing with IPSec Virtual Tunnel Interfaces

You can enable routing protocols on the tunnel interface so that routing information can be propagated over the virtual tunnel. The router can establish neighbor relationships over the virtual tunnel interface. Multicast packets can be encrypted, and interoperability with standard-based IPSec installations is possible through the use of IP ANY ANY proxy. The static IPSec interface, will negotiate and accept **permit IP ANY ANY** proxies.

Figure 82 illustrates how a static virtual tunnel interface is used.

*Figure 82 IPSec Static Virtual Tunnel Interface*




The IPSec virtual tunnel interface supports native IPSec tunneling and exhibits most of the properties of a physical interface.

# Traffic Encryption with the IPSec Virtual Tunnel Interface

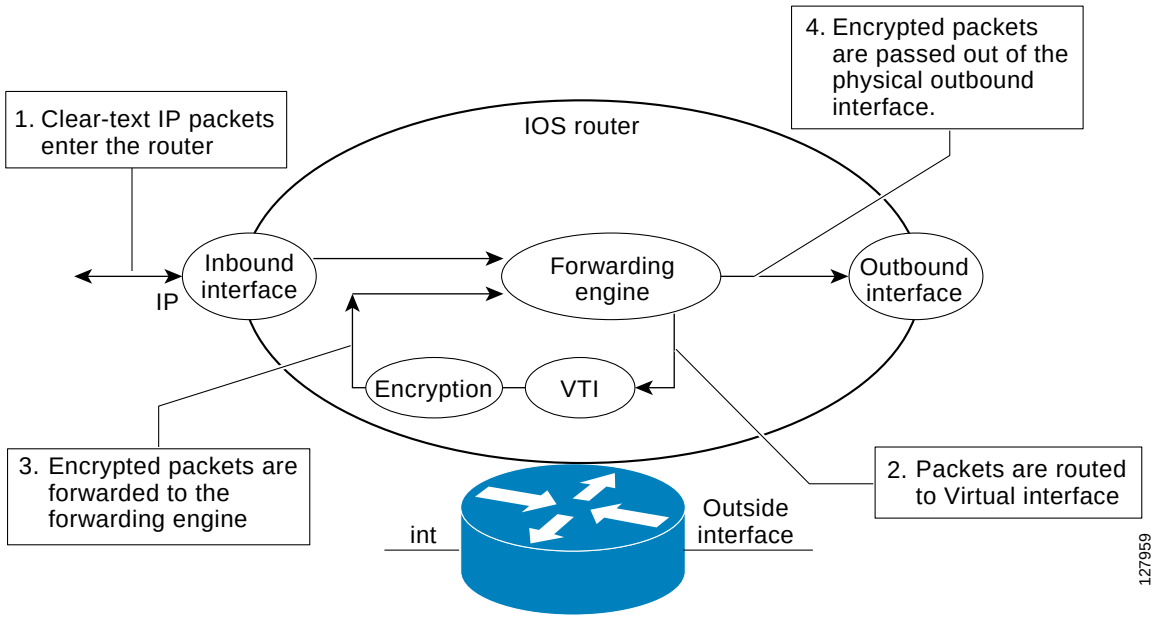
In the IPSec virtual tunnel interface encryption occurs in the tunnel. Traffic is encrypted when it is forwarded to the tunnel interface. Traffic forwarding is handled by the IP routing table, and dynamic or static IP routing can be used to route the traffic to the virtual tunnel interface. Using IP routing to forward the traffic to encryption simplifies the IPSec Virtual Private Network (VPN) configuration because the use of access control lists (ACLs) with a crypto map in native IPSec configurations not required. The IPSec virtual tunnel also allows you to encrypt multicast traffic with IPSec.

IPSec VTIs allow you to separate the interface context to apply pre- and post-encryption features. Features on the clear-text packets are configured on the VTI; Features for encrypted packets are applied on the physical outbound interface  When IPSec virtual tunnel interfaces are used, you can separate application of Network Address Translation (NAT), ACLs, Quality of Service (QoS) and apply them to clear text or encrypted text, or both. When crypto maps are used, there is no easy way to specify forced encryption features.

# IPSec Packet Flow

IPSec packet flow going into the IPSec tunnel is illustrated in Figure 83.

*Figure 83 Packet Flow Going Into the IPSec Tunnel*

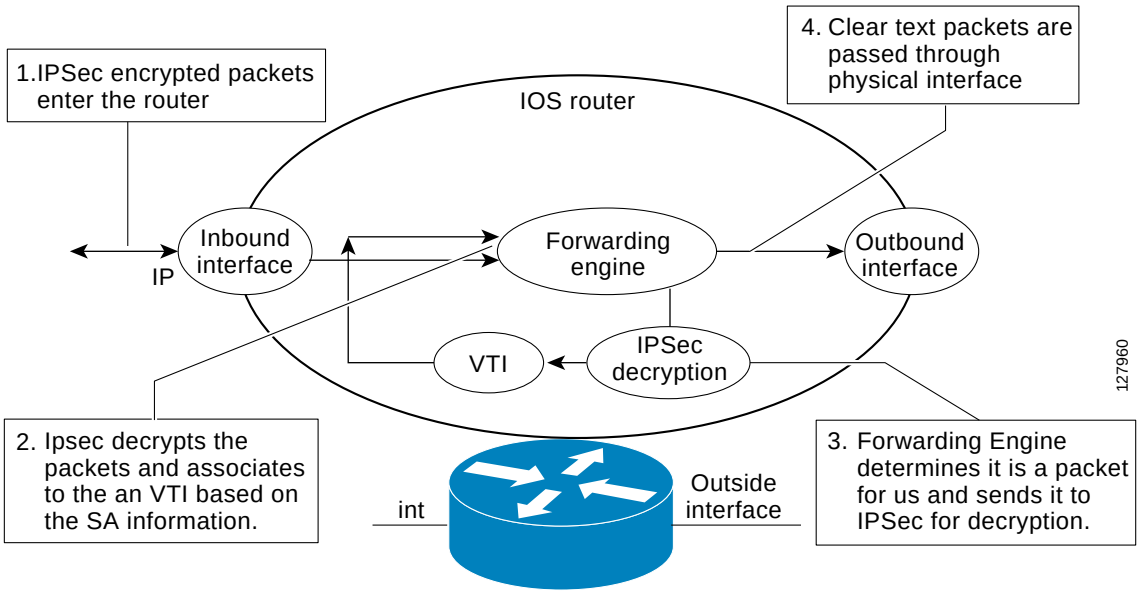



In Figure 83, shows the flow of packets in the egress path.

After packets arrive on the inbound interface, the forwarding engine switches the packets to the virtual tunnel interface where they are encrypted. The encrypted packets are handed back to the forwarding engine where they are switched through the outbound interface.

Figure 84 shows the packet flow out of the IPSec tunnel.

*Figure 84 Packet Flow Out of the IPSec Tunnel*



# Dynamic Virtual Tunnel Interfaces

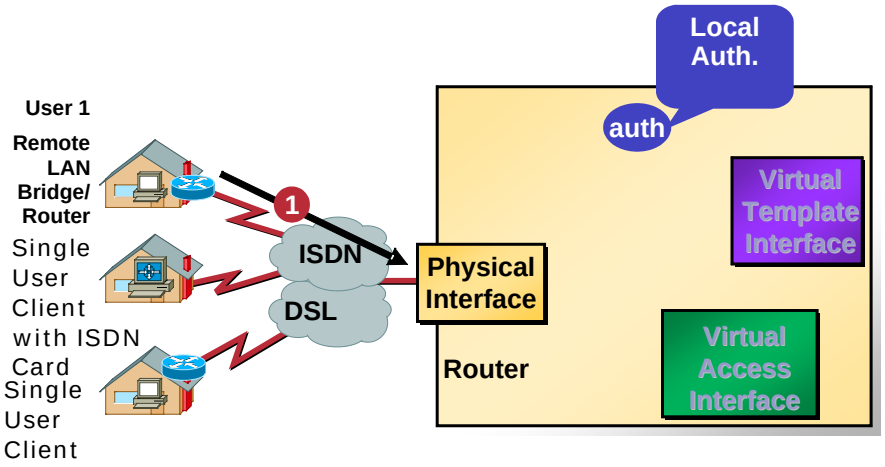
Dynmic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. Dynamic VTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using Xauth User or Unity group, or it can be derived from a certificate. Dynamic VTI is standards-based, so interoperability in a multiple-vendor environment is supported. IPSec Dynamic VTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco AVVID (Architecture for Voice, Video and Integrated Data) to deliver converged voice, video, and data over IP networks.The dynamic VTI simplifies VRF-aware IPSec deployment. The VRF is configured on the interface.

Quality of Service features can be used to improve the performance of various applications across the network. Traffic shaping is used between sites to limit the total amount of traffic that should be transmitted between two sites. Additionally, any combination of QoS features offered in Cisco IOS software can be used to support voice, video, or data applications.

Dynamic VTI reduces overhead by requiring minimal configuration on the router. A single virtual template can be configured and cloned, as opposed to the crypto requirement of one virtual template per VRF.

The dynamic VTI creates an interfce for IPSec sessions and uses the virtual template infrastructure for dynamic instantiation and management of IPSec interfaces. Dynamic VTIs ae used in hub-and-spoke configurations. A single dynamic VTI can support several staic VTIs. Decisions are made through routing updates. Figure 85 illustrates the dynamic VTI authentication path.

***Figure 85 Dynamic IPSec Virtual Tunnel Interface***




The authentication shown in Figure 85 follows this path:

1. User 1 calls the router.
2. Router 1 checks authentication locally.
3. Authentication succeeds.
4. Clones virtual access interface from virtual template Interface.

## Profile Definitions and Policy Define the Dynamic Virtual Tunnel Interface Life Cycle

IPSec profiles define policy for dynamic VTIs. The dynamic interface is created at the end of IKE Phase 1. The IKE Phase 1.5 exchange is driven by the virtual template configuration in the ISAKAMP profile. The interface is deleted when the IPSec session to the peer is closed. The IPSec session is closed when both IKE and IPSec SAs to the peer are deletted.

# How to Configure IPSec Virtual Tunnels



## Configuring IPSec Static Tunnels

This configuration shows how to configure a static IPSec virtual tunnel interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface** *type number*
6. **ip address** *address mask*
7. **tunnel mode** *mode*
8. **tunnel source** *interface*
9. **tunnel destination** *ip-address*
10. **tunnel protection ipsec profile** *profile-name* [**shared**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **crypto ipsec profile** *profile-name*<br><br>**Example:**<br>`Router(config)# crypto ipsec profile PROF` | Defines the IP Security (IPSec) parameters that are to be used for IPSec encryption between two IPSec routers |
| **Step 4** | **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]<br><br>**Example:**<br>`Router(config)# set transform tset` | Specifies which transform sets can be used with the crypto map entry |
| **Step 5** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface tunnel0` | Specifies the interface on which the tunnel will be configured and enters interface configuration mode. |
| **Step 6** | **ip address** *address mask*<br><br>**Example:**<br>`Router(config-if)# ip address 10.1.1.1 255.255.255.0` | Specifies the IP address and mask. |
| **Step 7** | **tunnel mode** *mode*<br><br>**Example:**<br>`Router(config-if)# tunnel mode ipsec ipv4` | Defines the mode for the tunnel. |
| **Step 8** | **tunnel source** *interface*<br><br>**Example:**<br>`Router(config-if)# tunnel source loopback0` | Specifies the tunnel source as a loopback interface. |
| **Step 9** | **tunnel destination** *ip-address*<br><br>**Example:**<br>`Router(config-if)# tunnel destination 172.1.1.1` | Identifies the IP address of the tunnel destination. |
| **Step 10** | **tunnel protection** ipsec profile *profile-name* [**shared**]<br><br>**Example:**<br>`Router(config-if)# tunnel protection ipsec profile PROF` | Associates a tunnel interface with an IP Security (IPSec) profile. |

# Configuring Dynamic Virtual Tunnel Interfaces

This configuration shows how to configure a dynamic IPSec virtual tunnel interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface virtual-template** *number*
6. **ip unnumbered loopback** *number*
7. **tunnel mode** *mode*
8. **tunnel protection ipsec profile** *profile-name* [**shared**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **crypto ipsec profile** *profile-name*<br><br>**Example:**<br>`Router(config)# crypto ipsec profile PROF` | Defines the IP Security (IPSec) parameters that are to be used for IPSec encryption between two IPSec routers |
| **Step 4** | **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]<br><br>**Example:**<br>`Router(config)# set transform tset` | Specifies which transform sets can be used with the crypto map entry |
| **Step 5** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface tunnel0` | Specifies the interface on which the tunnel will be configured and enters interface configuration mode. |
| **Step 6** | **ip address** *address mask*<br><br>**Example:**<br>`Router(config-if)# ip address 10.1.1.1 255.255.255.0` | Specifies the IP address and mask. |
| **Step 7** | **tunnel mode** *mode*<br><br>**Example:**<br>`Router(config-if)# tunnel mode ipsec ipv4` | Defines the mode for the tunnel. |
| **Step 8** | **tunnel source** *interface*<br><br>**Example:**<br>`Router(config-if)# tunnel source loopback0` | Specifies the tunnel source as a loopback interface. |
| **Step 9** | **tunnel destination** *ip-address*<br><br>**Example:**<br>`Router(config-if)# tunnel destination 172.1.1.1` | Identifies the IP address of the tunnel destination. |
| **Step 10** | **tunnel protection** ipsec profile *profile-name* [**shared**]<br><br>**Example:**<br>`Router(config-if)# tunnel protection ipsec profile PROF` | Associates a tunnel interface with an IP Security (IPSec) profile. |

# Configuration Examples for IPSec Virtual Tunnel Interfaces

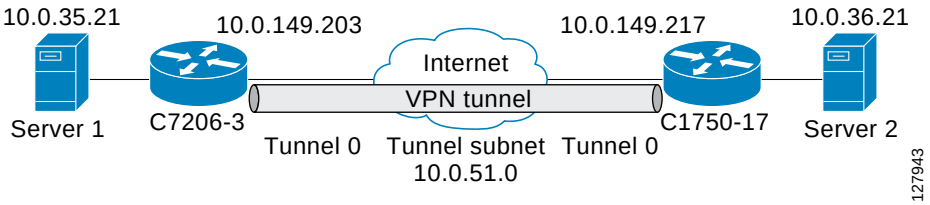
The following examples are provided to illustrate configuration scenarios for IPSec virtual tunnel interfaces:

- Static Virtual Tunnel Interface with IPSec: Example, page 1242
- Dynamic Virtual Tunnel Interface with IPSec for Simple Hub-and-Spoke Configuration: Example

## Static Virtual Tunnel Interface with IPSec: Example

The following example configuration uses a preshared key for authentication between peers. VPN traffic is forwarded to the IPSec virtual tunnel interface for encryption and then sent out of the physical interface. The tunnel on subnet 10 checks packets for IPSec policy and passes them to the Crypto Engine (CE) for IPSec encapsulation. Figure 86 illustrates the IPSec VTI configuration.

***Figure 86 Virtual Tunnel Interface with IPSec***




**C7206 Router Configuration**

```
version 12.3

service timestamps debug datetime
service timestamps log datetime
hostname 7200-3
no aaa new-model
ip subnet-zero
ip cef
controller ISA 6/1
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-sha-hmac
crypto ipsec profile P1
set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.203 255.255.255.0
 ip ospf mtu-ignore
 load-interval 30
 tunnel source 10.0.149.203
 tunnel destination 10.0.149.217
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
interface Ethernet3/0
```

```
 ip address 10.0.149.203 255.255.255.0
 duplex full
!
interface Ethernet3/3
 ip address 10.0.35.203 255.255.255.0
 duplex full
!
ip classless
ip route 10.0.36.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end
```

#### C1750 Router Configuration

```
version 12.3

hostname c1750-17
no aaa new-model
ip subnet-zero
ip cef
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2

crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-sha-hmac
crypto ipsec profile P1
set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 ip ospf mtu-ignore
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv
 tunnel protection ipsec profile P1
!
interface FastEthernet0/0
 ip address 10.0.149.217 255.255.255.0
 speed 100
 full-duplex
!
interface Ethernet1/0
 ip address 10.0.36.217 255.255.255.0
 load-interval 30
 full-duplex
!
ip classless
ip route 10.0.35.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end
```

## Verifying the Results for IPSec Virtual Tunnel Interface Example

This section provides information you can use to confirm that your configuration is working properly. In this display, Tunnel 0 is “up,” and the line protocol is “up.” If the line protocol is “down”, the session is not active.

### Verifying the C7206 Status

```
7200-3#show interface tunnel 0

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport IPSEC/IP, key disabled, sequencing disabled
Tunnel TTL 255

Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPSec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

7200-3#show crypto session

Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4, origin: crypto map

7200-3#show ip route

Codes: 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-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

# Dynamic Virtual Tunnel Interface with IPSec for Simple Hub-and-Spoke Configuration: Example

This example shows the basic configuration of a dynamic VTI for a simple hub-and-spoke network configuration.

```
enable
configure terminal
crypto isakmp profile red
 virtual -template 1
!
crypto ipsec profile red
 set transform-set red
!
interface virtual-template1 tunnel
 ip unnumbered loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile red
```

# VRF-Aware Ipsec with Dynamic VTI: Example

This example shows how to configure VRF-Aware IPSec to take advantage of the dynamic VTI.

```
!
Crypto isakmp profile BLUE
 …
 virtual-template 1
!
Crypto isakmp profile RED
 …
 virtual-template 2
!
Interface virtual-template1 type tunnel
 ip vrf forwarding BLUE
 …
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile BLUE
!
Interface virtual-template1 type tunnel
 ip vrf forwarding RED
 …
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile RED
```

# QoS Service Policy Per Instance with Dynamic VTI: Example

```
Policy-map map1
 class class-default
  shape average 8000
!
Crypto isakmp profile map1
 virtual-template 1
 .
 .
 .
```

```
!
Interface Virtual-Template1 type tunnel
 …
 service-policy output map1
!
```

# Additional References

The following sections provide references related to IPSec virtual tunnel interface.

## Related Documents

| Related Topic | Document Title |
|---|---|
| IPSec, security issues | *Cisco IOS Security Configuration Guide* |
| Security commands | *Cisco IOS Security Command Reference* |
| VPN configuration | *Cisco IOS Easy VPN Server* |

## Standards

| Standards | Title |
|---|---|
| No standards were | |
| | |

## MIBs

| MIBs | MIBs Link |
|---|---|
| • No MIBs were created or modified to support this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

## RFCs

| RFCs | Title |
|---|---|
| RFC 2401 | *Security Architecture for The Internet Protocol* |
| RFC 2408 | *Internet Security Association and Key Management Protocol* |
| RFC 2409 | *The Internet Key Exchange (IKE)* |

# Technical Assistance

| Description | Link |
|---|---|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/public/support/tac/home.shtml |

# Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **crypto isakmp profile**
- **tunnel mode**
- **virtual-template**