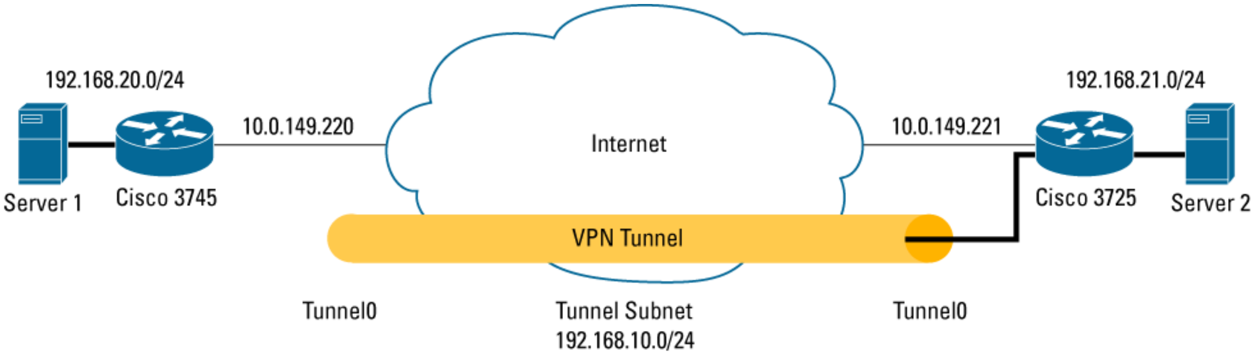
DEPLOYMENT GUIDE

CONFIGURING A VIRTUAL TUNNEL INTERFACE WITH IP SECURITY

This document provides a sample configuration for a virtual tunnel interface (VTI) with IP Security (IPSec). This configuration uses RIP version 2 routing protocol to propagate routes across the VTI. With a VTI, VPN traffic is forwarded to the IPSec virtual tunnel for encryption and then sent out of the physical interface. This sample configuration also demonstrates the use of Cisco Quality of Service with VTIs.

Figure 1 illustrates the network for the sample configuration.

Figure 1. Network Diagram



VIRTUAL TUNNEL INTERFACES

Cisco® IPSec VTIs are a new tool that customers can use to configure IPSec-based VPNs between site-to-site devices. IPSec VTI tunnels provide a designated pathway across a shared WAN and encapsulate traffic with new packet headers, which helps to ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. In addition, IPSec provides true confidentiality (as does encryption) and can carry encrypted traffic.

With IPSec VTIs, users can provide highly secure connectivity for site-to-site 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.

BENEFITS

- **Simplifies management**---Customers can use the Cisco IOS® Software virtual tunnel constructs to configure an IPSec virtual tunnel interface, thus simplifying VPN configuration complexity, which translates into reduced costs because the need for local IT support is minimized. In addition, existing management applications that can monitor interfaces can be used for monitoring purposes.
- **Supports multicast encryption**---Customers can use the Cisco IOS Software IPSec VTIs to transfer the multicast traffic, control traffic, or data traffic---for example, many voice and video applications---from one site to another securely.
- **Provides a routable interface**---Cisco IOS Software IPSec VTIs can support all types of IP routing protocols. Customers can use these VTI capabilities to connect larger office environments---for example, a branch office, complete with a private branch exchange (PBX) extension.
- **Improves scaling**---IPSec VTIs need fewer established security associations to cover different types of traffic, both unicast and multicast, thus enabling improved scaling.

- **Offers flexibility in defining features**---An IPSec VTI is an encapsulation within its own interface. This offers flexibility of defining features to run on either the physical or the IPSec interface.

CONFIGURATION SUMMARY

An IPSec virtual tunnel configuration does not require a static mapping of IPSec sessions to a physical interface. This allows for the flexibility of sending and receiving encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted when it is forwarded from or to the tunnel interface. The traffic is forwarded to or from the tunnel interface by virtue of the IP routing table. Dynamic or static IP routing can be used to route the traffic to the encryption engine. Using IP routing to forward the traffic to encryption simplifies the IPSec VPN configuration when compared with using access control lists (ACLs) with the crypto map in native IPSec configuration.

- **Dynamic routing**---Dynamic routing is used in this configuration to propagate the remote network addresses to the local site. Using dynamic routing simplifies manageability of the IPSec network and enables it to expand without having to manually maintain reach information.
- **Quality of service (QoS)**---QoS can be used to improve the performance of different applications across the network. In this configuration, traffic shaping is used between the two sites to limit the total amount of traffic that should be transmitted between the two sites. Additionally, the QoS configuration can support any combination of QoS features offered in Cisco IOS Software to support any of the voice, video, or data applications.

Note: The QoS configuration in this guide is for demonstration only . It is expected that the VTI scalability results will be similar to the p2p GRE over IPsec. For scaling and performance considerations please contact your Cisco representative.

LIMITATIONS

This guide provides the VTI configuration only. It does not cover the following configuration:

- Full security audit on the router. It is recommended that users run a Cisco Router and Security Device Manager (SDM) security audit in wizard mode to lock down and secure the router.
- An initial router configuration step is not shown in the steps. The full configuration is shown in the following section.
- This configuration guide uses private addresses only. When using private addresses and connecting to the Internet, an appropriate Network Address Translation (NAT) or Port Address Translation (PAT) configuration is required to provide connectivity over the Internet.

COMPONENTS USED

The sample configuration uses the following releases of the software and hardware:

- Cisco IOS Software Release 12.3(14)T for the Cisco 3700 Series Multiservice Access Router.

The information presented in this document was created from devices in a specific lab environment. All of the devices started with a cleared (default) configuration. If you are working in a live network, it is imperative to understand the potential impact of any command before implementing it.

ROUTER CONFIGURATION

Cisco 3745-20 Router Configuration

Current configuration:

```
!
version 12.3
!
hostname c3745-20
!
no aaa new-model
!
```

```
ip subnet-zero
ip cef
!
!
!
!
policy-map FOO
 class class-default
  shape average 128000
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key ******** address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile VTI
 set transform-set TSET
!
!
interface Tunnel0
 ip address 192.168.10.2 255.255.255.0
 tunnel source 10.0.149.220
 tunnel destination 10.0.149.221
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output FOO
!
interface FastEthernet0/0
 ip address 10.0.149.220 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
!
router rip
 version 2
 network 192.168.10.0
 network 192.168.20.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.149.1
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

c3745-20#
```

Cisco 3725-21 Router Configuration

Current configuration:

```
!
version 12.3
!
hostname c3725-21
!
!
!
no aaa new-model
!
!
ip subnet-zero
ip cef
!
!
policy-map FOO
 class class-default
  shape average 128000
!
!
!
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key ********  address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile VTI
 set transform-set TSET
!
!
interface Tunnel0
 ip address 192.168.10.1 255.255.255.0
 tunnel source 10.0.149.221
 tunnel destination 10.0.149.220
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output FOO
!
interface FastEthernet0/0
 ip address 10.0.149.221 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.21.1 255.255.255.0
 duplex auto
 speed auto
!
router rip
 version 2
 network 192.168.10.0
 network 192.168.21.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.149.1
!
line con 0
line aux 0
line vty 0 4
```

```
!
end
```

VERIFYING THE RESULTS

This section provides information you can use to confirm that your configuration is working properly.

Verifying the Status of the Cisco 3745 Router

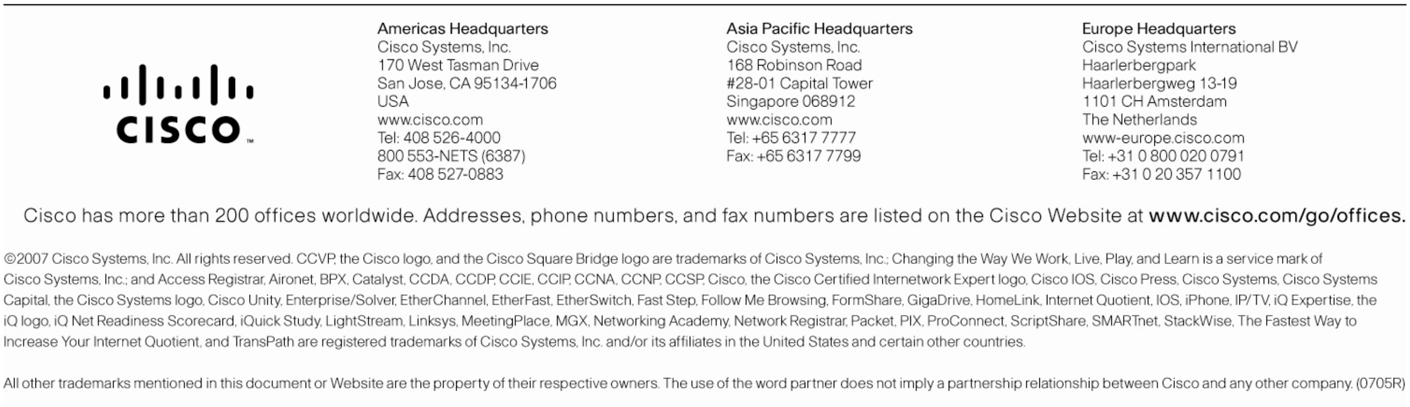
```
c3745-20#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.10.2/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.149.220, destination 10.0.149.221
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "VTI")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (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
     4096 packets input, 406332 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
     4136 packets output, 408752 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out

c3745-20#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication
```

```
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.221 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.0.149.221
      Desc: (none)
  IKE SA: local 10.0.149.220/500 remote 10.0.149.221/500 Active
          Capabilities:D connid:38 lifetime:23:11:43
  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
        Inbound:  #pkts dec’ed 4094 drop 0 life (KB/Sec) 4534080/704
        Outbound: #pkts enc’ed 4134 drop 0 life (KB/Sec) 4534076/704

c3745-20#show policy-map interface tunnel 0
 Tunnel0

  Service-policy output: FOO

    Class-map: class-default (match-any)
      3093 packets, 305516 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
           128000/128000    1984   7936      7936      62        992

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -     0         0         0         0         0         no

c3745-20#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 10.0.149.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, Tunnel0
R    192.168.21.0/24 [120/1] via 192.168.10.1, 00:00:14, Tunnel0
C    192.168.20.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.149.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.0.149.1
```

RELATED INFORMATION

- IPSec Support Page
- An Introduction to IP Security (IPSec) Encryption
- Configuring IPSec Network Security
- Configuring Internet Key Exchange Security Protocol
- Command Lookup Tool (registered customers only)
- Technical Support---Cisco Systems®



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**