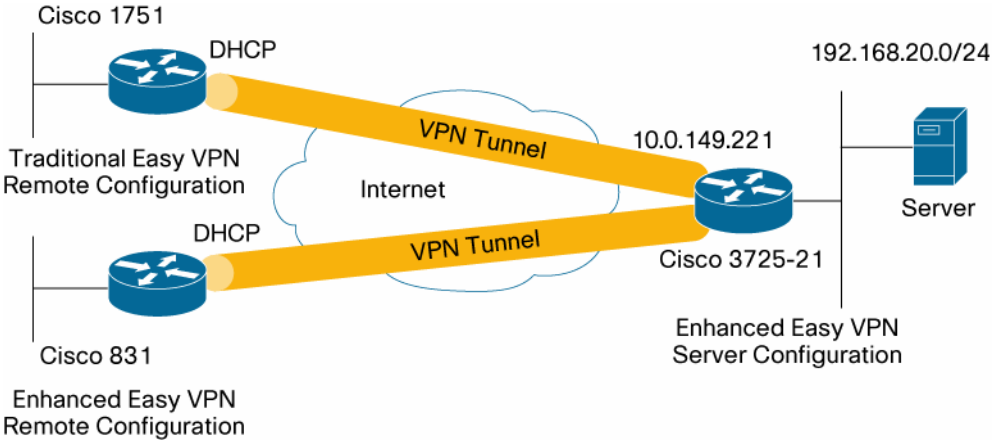
# Configuring Cisco Easy VPN with IPSec Dynamic Virtual Tunnel Interface (DVTI)

This document provides a sample configuration for enhanced Cisco® Easy VPN Server and Easy VPN Remote configuration using the IPSec Dynamic Virtual Tunnel Interface (DVTI). Cisco Easy VPN Remote is configured with User Extension Mode and is assigned a dynamic IP address from the Easy VPN Server. Cisco Easy VPN with DVTI configuration provides a routable interface for forwarding traffic based on IP routing tables. Cisco Easy VPN uses a virtual access interface, which is created during the initial configuration. The VPN traffic is forwarded to the virtual access interface for encryption and then sent out of the physical interface. This sample configuration also demonstrates the use of quality of service (QoS) with virtual tunnel interfaces.

Figure 1 shows the sample configuration.

**Figure 1.** Cisco Easy VPN Configuration with IPSec DVTI




## Cisco Easy VPN with DVTI

Cisco DVTI is a new method that can be used by customers with Cisco Easy VPN for both the Server and Remote configuration. The tunnels provide an on-demand separate virtual access interface for each Easy VPN connection. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPSec configuration and any Cisco IOS® Software feature configured on the virtual template interface, such as QoS, NetFlow, or access control lists (ACLs).

With IPSec DVTIs and Cisco Easy VPN, users can provide highly secure connectivity for remote-access VPNs that 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 virtual template to clone, on demand, new virtual access interfaces for IPSec, thus simplifying VPN configuration complexity, which translates into reduced costs. In addition, existing management applications now can monitor separate interfaces for different sites for monitoring purposes.
- **Provides a Routable Interface:** Cisco IPSec VTIs can support all types of IP routing protocols. Customers can use these capabilities to connect larger office environments, such as branch offices.
- **Improves Scaling:** IPSec VTIs use single security associations per site, which cover different types of traffic, enabling improved scaling.
- **Offers Flexibility in Defining Features:** An IPSec VTI is an encapsulation within its own interface. This offers flexibility of defining features for clear-text traffic on IPSec VTIs, and defining features for encrypted traffic on physical interfaces.

## Configuration Summary

The Cisco Easy VPN with DVTI configuration provides a routable interface to selectively send traffic to different destinations, such as an Easy VPN concentrator, a different site-to-site peer, or the Internet. IPSec DVTI 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. Routes are dynamically learned during Internet Key Exchange (IKE) Mode Configuration and inserted into the routing table pointing to the DVTI. Dynamic IP routing can be used to propagate routes across the VPN. Using IP routing to forward the traffic to encryption simplifies the IPSec VPN configuration when compared with using ACLs with the crypto map in native IPSec configuration.

Before Cisco IOS Release 12.4(2)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden. With the Dynamic Virtual Tunnel Interface Support feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up time. Features that are applied to the traffic (before encryption) going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up).

When the Easy VPN negotiation is successful, the line protocol state of the virtual access interface gets changed to up. When the Easy VPN tunnel goes down because the security association expires or is deleted, the line protocol state of the virtual access interface changes to down.

The routing tables act as traffic selectors in an Easy VPN virtual interface configuration—that is, the routes replace the access list on the crypto map. In a virtual interface configuration, Easy VPN negotiates a single IPSec security association if the Easy VPN Server has been configured with an IPSec DVTI. This single security association is created regardless of the Easy VPN mode that is configured.

After the security association is established, routes that point to the virtual access interface are added to direct traffic to the corporate network. Easy VPN also adds a route to the VPN concentrator so that IPSec-encapsulated packets get routed to the corporate network. A default route that points to the virtual access interface is added in the case of a nonsplit mode. When the Easy VPN server “pushes” the split tunnel, the split tunnel subnet becomes the destination to which the routes that point to the virtual access are added. In either case, if the peer (VPN concentrator) is not directly connected, Easy VPN adds a route to the peer.

**Note:** Most routers that run the Cisco Easy VPN Client software have a default route configured. The default route that is configured must have a metric value greater than 1—Easy VPN adds a default route that has a metric value of 1. The route points to the virtual access interface so that all traffic is directed to the corporate network when the concentrator does not “push” the split tunnel attribute.

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 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.

A link to more information about IPSec DVTI is provided in the Related Information section of this document.

**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. for additional information, check the Virtual Tunnel Interface (VTI) Design guide: http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd8029d629_ps6635_Products_White_Paper.html

### Limitations

This guide provides a sample of Easy VPN configuration with DVTI configuration only. It does not cover the following configurations:

- 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 enables split tunneling. The split tunneling is enabled on the hub by the ACL 101 command under the crypto isakmp client configuration mode. To disable the split tunneling on the remote, remove the ACL command from the Easy VPN Server. The spoke is configured with Port Address Translation (PAT) to provide connectivity over the Internet.
- This configuration uses User Extension Mode. For details on configuring this mode, please review Cisco Easy VPN Remote or Server documentations.
- This configuration does not include multicast.

### Restrictions

DVTI is only supported in the context of Enhanced Easy VPN. Routing with DVTIs is not supported or recommended. A DVTI interface on the headend router cannot terminate on an SVTI interface on the remote peer. An SVTI interface can only terminate on another SVTI interface.

### Components Used

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

- Cisco IOS Software, 3700 Software (C3745-ADVSECURITYK9-M), Release 12.4(2)T
- Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Release 12.4(4)T
- Cisco IOS Software, C1700 Software (C1700-K9O3SV8Y7-M), Release 12.3(11)T3

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

### C3725 Easy VPN Hub Router Configuration

```
version 12.4
!
hostname c3725-21
!
aaa new-model
!
aaa authentication login default local
aaa authorization network default local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
ip cef
!
!
username cisco privilege 15 password 0 cisco
!
policy-map FOO
 class class-default
  shape average 1280000
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
```

```
 key cisco
 dns 6.0.0.2
 wins 7.0.0.1
 domain cisco.com
 pool dpool
 acl 101
crypto isakmp profile vi
   match identity group cisco
   isakmp authorization list default
   client configuration address respond
   virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
interface FastEthernet0/0
 ip address 10.0.149.221 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.21 255.255.255.0
 duplex auto
 speed 100
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered FastEthernet0/0
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
 service-policy output FOO
!
```

```
router eigrp 1
 network 192.168.1.0
 network 192.168.20.0
 no auto-summary
!
ip local pool dpool 5.0.0.1 5.0.0.3
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.149.207
!
access-list 101 permit ip 192.168.20.0 0.0.0.255 any
!
control-plane
!
!
end
```

**C831 Spoke Router with DVTI Configuration**

**C1751 Spoke Router with Traditional Easy VPN Configuration**

```
version 12.3
!
hostname c1751-16
!
enable password lab
!
username cisco privilege 15 password 0 cisco
!
no aaa new-model
ip subnet-zero
!
!
ip cef
ip domain name cisco.com
!
crypto isakmp policy 1
 encr 3des
```

```
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec client ezvpn ez
 connect manual
 group cisco key cisco
 local-address FastEthernet0/0
 mode client
 peer 10.0.149.221
!

interface Loopback0
 ip address 5.0.0.3 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.16.1 255.255.255.0
  half-duplex
 crypto ipsec client ezvpn ez inside
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$
 ip address dhcp
 speed 100
 full-duplex
 crypto ipsec client ezvpn ez
!
ip classless
ip route 10.0.149.0 255.255.255.0 dhcp
!
end
```

## Verifying the Results

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

### Verifying the C3725 Router with Virtual Tunnel Status

```
c3725-21#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: Virtual-Access4
Session status: UP-ACTIVE
Peer: 10.0.150.8 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: cisco
      Desc: (none)
  IKE SA: local 10.0.149.221/500 remote 10.0.150.8/500 Active
         Capabilities:CD connid:1114 lifetime:21:36:30
  IPSEC FLOW: permit ip 192.168.20.0/255.255.255.0 host 5.0.0.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 9 drop 0 life (KB/Sec) 4599662/3571
        Outbound: #pkts enc'ed 9 drop 0 life (KB/Sec) 4599662/3571

Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 10.0.150.7 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: cisco
      Desc: (none)
  IKE SA: local 10.0.149.221/500 remote 10.0.150.7/500 Active
         Capabilities:CD connid:1117 lifetime:23:54:26
  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 15 drop 0 life (KB/Sec) 4577539/3267
        Outbound: #pkts enc'ed 15 drop 0 life (KB/Sec) 4577539/3267

c3725-21#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 10.0.149.207 to network 0.0.0.0

     5.0.0.0/32 is subnetted, 2 subnets
S       5.0.0.1 [1/0] via 0.0.0.0, Virtual-Access4
S       5.0.0.3 [1/0] via 0.0.0.0, Virtual-Access2
     8.0.0.0/24 is subnetted, 1 subnets
C       8.8.8.0 is directly connected, Loopback8
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
D    192.168.2.0/24 [90/2818560] via 192.168.20.20, 6w0d, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 10.0.149.207

c3725-21#show interface virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of FastEthernet0/0 (10.0.149.221)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel source 10.0.149.221 (FastEthernet0/0), destination 10.0.150.7
  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 "vi")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 01:52:19
  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
     15 packets input, 1500 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
     15 packets output, 1500 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out

c3725-21#show policy-map interface virtual-2
 Virtual-Access2

  Service-policy output: FOO

    Class-map: class-default (match-any)
      15 packets, 1500 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)
          1280000/1280000   8000   32000     32000     25        4000

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         15        1500      0         0         no
```

**Verifying the C831 Router with Virtual Tunnel Status**

```
c831-27#crypto ipsec client ezvpn connect
EZVPN(ez): IPSec connection terminated
c831-27#
*Jul 17 20:37:37.772: %CRYPTO-6-
EZVPN_CONNECTION_DOWN: (Client)  User=  Group=cisco  Server_public_addr=10.0.149.221
*Jul 17 20:37:38.840: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=cisc
o  Server_public_addr=10.0.149.221  Assigned_client_addr=5.0.0.3
*Jul 17 20:37:40.760: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jul 17 20:37:41.760: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
 changed state to up
```

```
c831-27#ping 192.168.20.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.21, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

c831-27#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: Ethernet1
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 10.0.150.7/500 remote 10.0.149.221/500 Active
         Capabilities:CD connid:3012 lifetime:23:58:43
  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 5 drop 0 life (KB/Sec) 4456688/3567
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4456688/3567

c831-27#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 10.0.150.207 to network 0.0.0.0

     5.0.0.0/32 is subnetted, 1 subnets
```

```
C       5.0.0.3 is directly connected, Loopback0
C    192.168.27.0/24 is directly connected, Ethernet0
S    192.168.20.0/24 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.150.0 is directly connected, Ethernet1
S       10.0.149.0 [1/0] via 10.0.150.207
S*   0.0.0.0/0 [254/0] via 10.0.150.207

c831-27#show interface virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback0 (5.0.0.3)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x0, loopback not set
  Keepalive not set
  Tunnel source UNKNOWN, 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)
  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
     2149 packets input, 214900 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
     2150 packets output, 215000 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

```
c831-27#show policy-map interface virtual-access 2
 Virtual-Access2

  Service-policy output: FOO

    Class-map: class-default (match-any)
      2140 packets, 214280 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         2140      214000    0         0         no

c831-27#show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 4 extended)
Outside interfaces:
  Ethernet1, Virtual-Access2
Inside interfaces:
  Ethernet0, Virtual-Template1
Hits: 307  Misses: 33
CEF Translated packets: 330, CEF Punted packets: 19
Expired translations: 28
Dynamic mappings:
-- Inside Source
[Id: 17] access-list internet-list interface Ethernet1 refcount 2
[Id: 16] access-list enterprise-list pool ez refcount 2
 pool ez: netmask 255.255.255.0
        start 5.0.0.3 end 5.0.0.3
        type generic, total addresses 1, allocated 1 (100%), misses 0
Queued Packets: 0
```

## Related Information

- IPSec Support Page
- Cisco Easy VPN Remote
- Easy VPN Server
- IPSec Virtual Tunnel Interface
- 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.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.



Printed in USA C11-539894-00 05/09