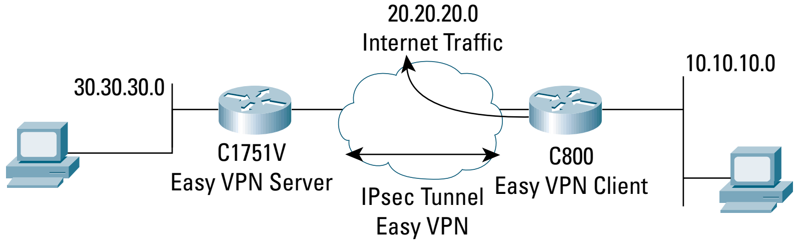
CONFIGURING CISCO IOS EASY VPN REMOTE WITH CLIENT MODE AND SPLIT TUNNELING

Figure 1
Network Diagram



INTRODUCTION

This document describes how to configure a router-to-router Easy VPN Solution based on the Cisco Easy VPN Client and Cisco IOS® Remote Access Server features. The sample configuration presented in this document uses Cisco 831 for the client and Cisco 1751 Router for the server. The Cisco Easy VPN negotiates tunnel parameters and establishes IPsec tunnels. Using split tunneling, the remote router routes the Internet-destined traffic directly, not forwarding it over the encrypted tunnel.

PREREQUISITES

The sample configuration of the router-to-router Easy VPN Solution is based on the following assumptions:

- The IP address at the Cisco Easy VPN Server is static.
- The IP address at the Cisco Easy VPN Client is static or dynamic.
- The Cisco Easy VPN Client encrypts only traffic that is forwarded to the hub.
- Traffic destined for the Internet is forwarded directly, unencrypted from the remote site.
- Traffic from the remote host is forwarded after applying Network Address Translation/Port Address Translation (NAT/PAT).

COMPONENTS USED

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

- Cisco 831 with Cisco IOS Software Release 12.3(2)XA (C831-K9O3SY6-M)
- Cisco 1751V with Cisco IOS Software Release 12.2(8)T (C1700-K9O3SV3Y7-M)

Figure 1 illustrates the network for the sample configuration.

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. In a live network, it is imperative to understand the potential impact of any command before implementing it.

EASY VPN CONFIGURATIONS

The Cisco Easy VPN configuration implements the Cisco Unity Client protocol, which simplifies configuring the detailed information on the client router because most VPN parameters are defined at the VPN remote access server. The server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or a Cisco IOS Software router that supports the Cisco Unity Client protocol.The sample configuration uses the Cisco 1751 for the Easy VPN Server.

This sample configuration also uses client mode on the remote Easy VPN Client. In client mode, the entire LAN behind the Easy VPN Client undergoes NAT to the mode config ip address that is pushed down by the Easy VPN Server.

Configured for split tunneling, the Easy VPN Client allows traffic to be sent directly to the Internet, unencrypted, while traffic destined for the VPN is encrypted. The Easy VPN Server is eliminated from the path of the Internet access. Split tunneling is enabled by the ACL command under the crypto client configuration on the Easy VPN server side. The ACL is dynamically loaded on the Easy VPN Client, and specifies exactly the networks to be permitted for encryption. The rest of the traffic is sent unencrypted.

Split tunneling uses the hub router resources efficiently, freeing the server bandwidth for additional VPN clients. However, split tunneling requires additional security and firewall configuration to ensure the security of the remote site. Refer to *Configuring Context-Based Access-Control*.

For additional information about configuring Easy VPN Client, refer to *Cisco IOS Easy VPN Client feature*.

CISCO 831 VPN ROUTER CONFIGURATION

The following configuration enables split tunneling. Additional firewall configurations or a firewall appliance is required to ensure the security of the VPN site.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Cisco831
!
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
 import all
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 option 150 ip 30.30.30.200
 dns-server 30.30.30.60
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
crypto ipsec client ezvpn hw-client
 group hw-client-groupname key hw-client-password
 mode client
 peer 20.20.20.2
!
interface Ethernet0
 description connected to BRANCH LAN
 ip address 10.10.10.1 255.255.255.0
 no cdp enable
!
interface Ethernet1
 description connected to INTERNET
 ip address 20.20.20.1 255.255.255.0
 no cdp enable
 crypto ipsec client ezvpn hw-client
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1
ip route 30.30.30.0 255.255.255.0 Ethernet1
ip http server
ip pim bidir-enable
!
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 no login
 length 0
!
scheduler max-task-time 5000
end
```

CISCO 1751V VPN ROUTER CONFIGURATION

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname Cisco1751
!
aaa new-model
!
!
aaa authorization network hw-client-groupname local
aaa session-id common
```

```
enable password cisco
!
username cisco password 0 cisco
memory-size iomem 15
clock timezone - 0 6
ip subnet-zero
no ip source-route
!
ip domain-name cisco.com
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 30.30.30.10 30.30.30.11
 wins 30.30.30.12 30.30.30.13
 domain cisco.com
 pool dynpool
 acl 150
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap isakmp authorization list hw-client-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
interface Ethernet0/0
 description connected to INTERNET
 ip address 20.20.20.2 255.255.255.0
 half-duplex
 no cdp enable
 crypto map dynmap
!
interface FastEthernet0/0
 description connected to HQ LAN
 ip address 30.30.30.1 255.255.255.0
 speed auto
 no cdp enable
!
ip local pool dynpool 30.30.30.20 30.30.30.30
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
ip pim bidir-enable
!
!
access-list 150 permit ip 30.30.30.0 0.0.0.255 any
no cdp run
!
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
!
end
```

VERIFYING THE RESULTS

This section provides information that can be used to confirm that configuration is working properly.

Verifying the Cisco 831 Status

```
Cisco1751#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : hw-client
Inside interface list: Ethernet0,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 30.30.30.20
Mask: 255.255.255.255
DNS Primary: 30.30.30.10
DNS Secondary: 30.30.30.11
NBMS/WINS Primary: 30.30.30.12
NBMS/WINS Secondary: 30.30.30.13
Default Domain: cisco.com
Split Tunnel List: 1
 Address : 30.30.30.0
 Mask : 255.255.255.0
 Protocol : 0x0
 Source Port: 0
 Dest Port : 0
Cisco831#show crypto ipsec sa
interface: Ethernet1
 Crypto map tag: Ethernet1-head-0, local addr. 20.20.20.1
 protected vrf:
 local ident (addr/mask/prot/port): (30.30.30.20/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
 current_peer: 20.20.20.2:500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 1
 #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0
 local crypto endpt.: 20.20.20.1, remote crypto endpt.: 20.20.20.2
 path mtu 1500, media mtu 1500
 current outbound spi: E89E6649
 inbound esp sas:
 spi: 0x239C766E(597456494)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 20, flow_id: 1, crypto map: Ethernet1-head-0
 sa timing: remaining key lifetime (k/sec): (4434132/3474)
 IV size: 8 bytes
 replay detection support: Y
 inbound ah sas:
 inbound pcp sas:
 outbound esp sas:
 spi: 0xE89E6649(3902694985)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 21, flow_id: 2, crypto map: Ethernet1-head-0
 sa timing: remaining key lifetime (k/sec): (4434131/3473)
 IV size: 8 bytes
 replay detection support: Y
 outbound ah sas:
 outbound pcp sas:
```

Verifying the Cisco 1751 Status

```
Cisco1751#show crypto ipsec sa
interface: Ethernet0/0
 Crypto map tag: dynmap, local addr. 20.20.20.2
 protected vrf:
 local ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (30.30.30.20/255.255.255.255/0/0)
 current_peer: 20.20.20.1:500
 PERMIT, flags={}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
 #pkts decaps: 27, #pkts decrypt: 27, #pkts verify 27
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0
 local crypto endpt.: 20.20.20.2, remote crypto endpt.: 20.20.20.1
 path mtu 1500, media mtu 1500
 current outbound spi: 239C766E
 inbound esp sas:
 spi: 0xE89E6649(3902694985)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 200, flow_id: 1, crypto map: dynmap
 sa timing: remaining key lifetime (k/sec): (4458451/3136)
 IV size: 8 bytes
 replay detection support: Y
 inbound ah sas:
 inbound pcp sas:
 outbound esp sas:
 spi: 0x239C766E(597456494)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 201, flow_id: 2, crypto map: dynmap
 sa timing: remaining key lifetime (k/sec): (4458454/3136)
 IV size: 8 bytes
 replay detection support: Y
 outbound ah sas:
 outbound pcp sas:
Cisco1751#show crypto isakmp sa
dst src state conn-id slot
20.20.20.2 20.20.20.1 QM_IDLE 1 0
Cisco1751#show crypto engine connections active
 ID Interface IP-Address State Algorithm Encrypt Decrypt
 1 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 0
 200 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 538
 201 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 133 0
```

TROUBLESHOOTING THE CONFIGURATION

Certain **show** commands are supported by the *Output Interpreter Tool* (*registered* customers only), which analyzes **show** command output.

Note: Before issuing debug commands, see Important Information about Debug Commands .

- **debug crypto isakmp**—Displays errors during Phase 1.
- **debug crypto ipsec**—Displays errors during Phase 2.
- **debug crypto engine**—Displays information from the crypto engine.
- **debug ip your routing protocol**—Displays information about routing transactions of the routing protocol.
- **clear crypto connection connection-id** [**slot** | **rsm** | **vip**]—Terminates an encrypted session currently in progress. Encrypted sessions normally terminate when the session times out. Use the **show crypto cisco connections command** to see the connection-id value.
- **clear crypto isakmp**—Clears the Phase 1 security associations.
- **clear crypto sa**—Clears the Phase 2 security associations.

RELATED INFORMATION

- IPsec Support Page
- An Introduction to IP Security (IPsec) Encryption
- Cisco VPN Client Feature
- Cisco IOS Easy VPN Server
- Configuring IPSec Network Security
- Configuring Internet Key Exchange Security Protocol
- Command Lookup Tool (registered customers only)
- Technical Support—Cisco Systems

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe