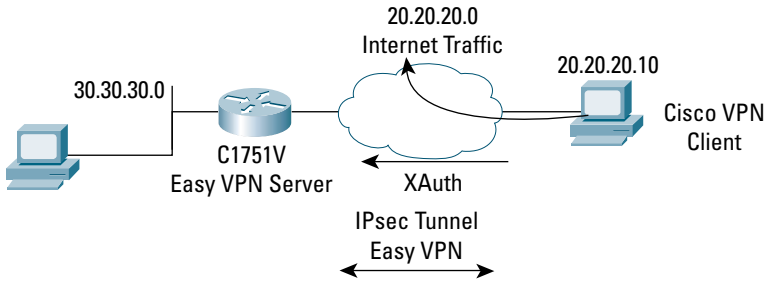
CONFIGURING CISCO VPN CLIENT AND EASY VPN SERVER WITH XAUTH AND SPLIT TUNNELING

Figure 1
Network Diagram



INTRODUCTION

This document describes how to configure a host to router Easy VPN Solution, based Cisco VPN Client, and Easy VPN Server. The sample configuration presented in this document uses Cisco VPN Client and Cisco 1751 for the server. The Cisco Easy VPN negotiates tunnel parameters and establishes IPsec tunnels. Xauth adds another level of authentication that identifies the user who requests the IPsec connection. Split tunneling enables the remote client to forward the Internet-destined traffic directly without forwarding it over the encrypted tunnel.

PREREQUISITES

The sample configuration is based on the following assumptions:

- The IP address at the Cisco Easy VPN Server is static.
- The IP address at the Cisco 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, unencrypted, directly from the remote site.
- Traffic from the remote host is forwarded after applying Network Address Translation/Port Address Translation (NAT/PAT).
- User level authentication is used for authorizing VPN access.

COMPONENTS USED

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

- Cisco VPN Client Version 3.5
- 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 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 also uses client mode on the Cisco 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.

Using the Xauth feature, the client waits for a "username/password" challenge after the IKE SA has been established. When the end user responds to the challenge, the response is forwarded to the IPsec peers for an additional level of authentication. The information that is entered is checked against the AAA server.

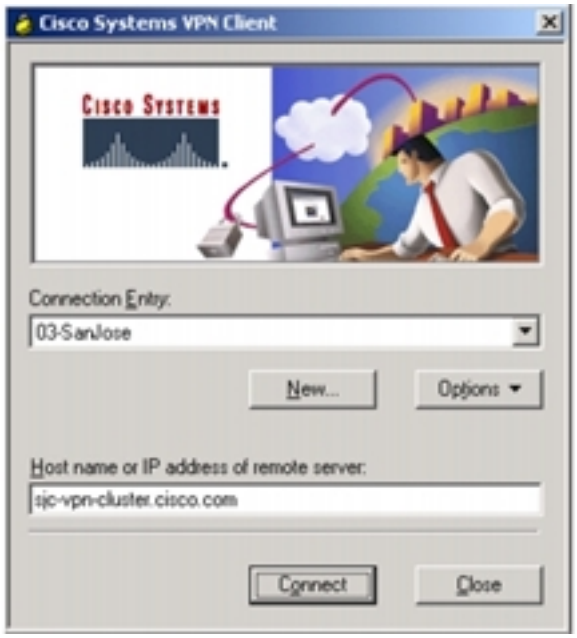
Configured for split tunneling, the Easy VPN Client allows traffic to be sent directly to the Internet, unencrypted, while traffic destined for the VPN is encrypted. The Easy VPN Server is eliminated from the path of the Internet access. Split tunneling is enabled by the ACL command under the crypto 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. For additional information about configuring the Cisco VPN Client, refer to *Cisco VPN Client User Guide Books—Cisco Systems*.

Configuring the Cisco VPN Client

Follow the steps in this section to configure the Cisco VPN Client.

Step 1. After installing the Cisco VPN Client, launch the application.

The Cisco Systems VPN Client dialog box is displayed.



Step 2. Click New. The New Connection Entry Wizard is displayed.

Step 3. Enter the name of the new connection entry: Ez VPN Server

Step 4. Click Next.

The prompt for the host name or IP address of the server is displayed.

Step 5. Enter 20.20.20.2 and click Next.

A request for authentication parameters is displayed.

Step 6. Enter the following values:

Name: hw-client-groupname

Password: hw-client-password

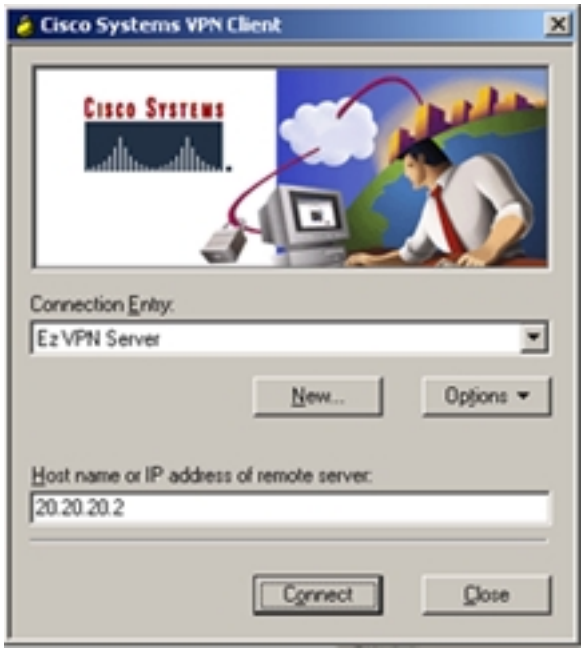
Confirm password: hw-client-password

Step 7. Click Next.

A message saying you succeeded in creating the VPN connection is displayed.

Step 8. Click Finish.

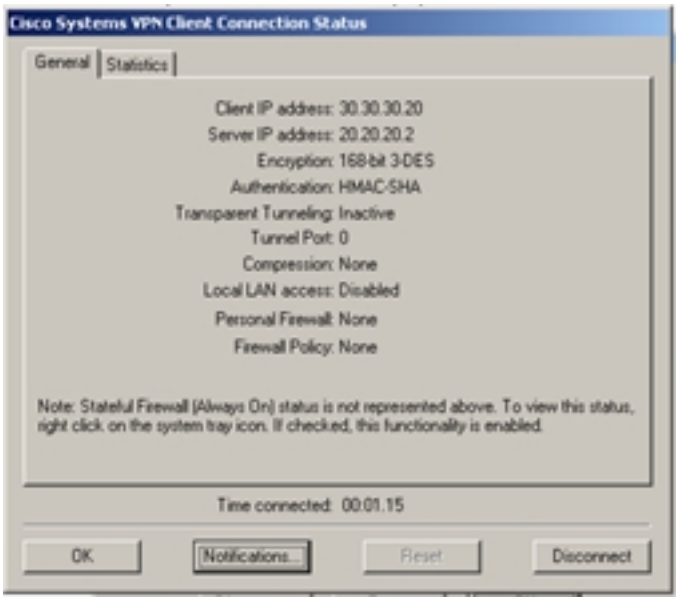
The Cisco Systems VPN Client dialog box is displayed.



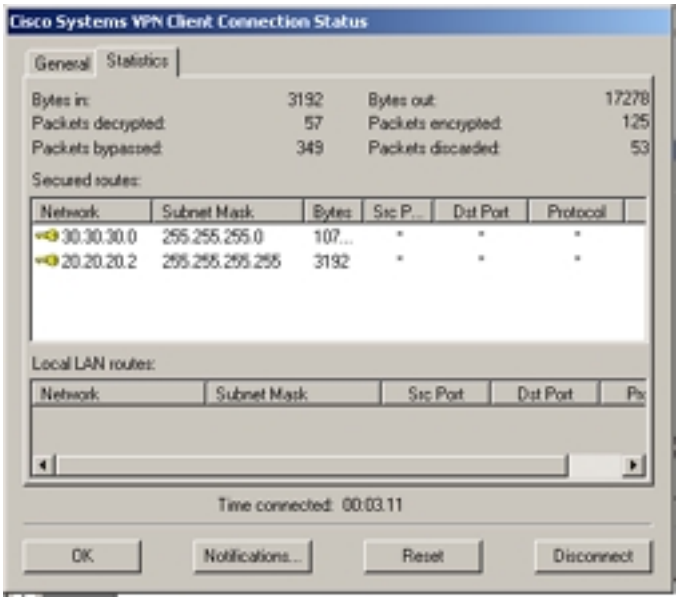
Step 9. Click Connect.

The connecting message is displayed, and then a request for authentication information is displayed.

After the connection is made, the connection status is displayed.



The following is a view of the connection statistics and the secured routes. In this example, only routes to the private segment 30.30.30.0 are secured.



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 authentication login userlist local
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 xauth timeout 60
!
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 client authentication list userlist
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 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): (20.20.20.2/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port): (30.30.30.20/255.255.255.255/0/0)
 current_peer: 20.20.20.10:500
 PERMIT, flags={}
 #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
 #pkts decaps: 0, #pkts decrypt: 0, #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.: 20.20.20.2, remote crypto endpt.: 20.20.20.10
 path mtu 1500, media mtu 1500
 current outbound spi: B5FC3352
 inbound esp sas:
 spi: 0xD175BCD6(3514154198)
 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): (4524962/3583)
 IV size: 8 bytes
 replay detection support: Y
 inbound ah sas:
 inbound pcp sas:
 outbound esp sas:
 spi: 0xB5FC3352(3053204306)
 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): (4524961/3583)
 IV size: 8 bytes
 replay detection support: Y
 outbound ah sas:
 outbound pcp sas:
 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: 20.20.20.10:500
 PERMIT, flags={}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
 #pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25
```

```
 #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.: 20.20.20.10
 path mtu 1500, media mtu 1500
 current outbound spi: 57FC29E7
 inbound esp sas:
 spi: 0x82934851(2190690385)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 202, flow_id: 3, crypto map: dynmap
 sa timing: remaining key lifetime (k/sec): (4595750/3584)
 IV size: 8 bytes
 replay detection support: Y
 inbound ah sas:
 inbound pcp sas:
 outbound esp sas:
 spi: 0x57FC29E7(1476143591)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 203, flow_id: 4, crypto map: dynmap
 sa timing: remaining key lifetime (k/sec): (4595754/3582)
 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 20.20.20.10 QM_IDLE 3 0
Cisco1751#show crypto engine connections active
 ID Interface IP-Address State Algorithm Encrypt Decrypt
 3 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 0
 201 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 54 0
 202 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 118
 203 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 0
Cisco1751#
```

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
- Download Cisco VPN Client from CCO
- Cisco VPN Client
- 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 • V enezuela • Vietnam • Zimbabwe

204026_ETMG_SH_06.04