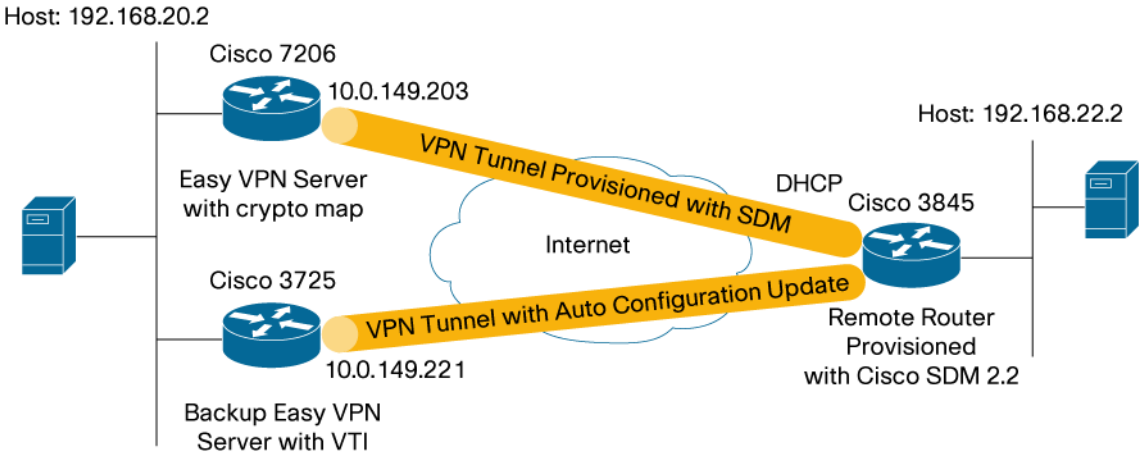
Overview

Configuring Dual Tunnel with Cisco IOS Easy VPN Using Auto Configuration Update

This document demonstrates dual tunnel configuration with Cisco® Easy VPN. The user configures the first Easy VPN tunnel with the Cisco Router and Security Device Manager (SDM). When the first Easy VPN tunnel is established, the Auto Configuration Update feature causes the router to download instructions for the second tunnel into the running memory. The second tunnel has an Enhanced Easy VPN configuration with Virtual Tunnel Interface (VTI). Figure 1 shows a sample configuration.

Figure 1. Network Diagram



DUAL TUNNEL SUPPORT

Cisco Easy VPN now supports the ability to configure two Easy VPN tunnels having the same inside and outside interfaces. The feature, called the Easy VPN Dual Tunnel, was introduced in Cisco IOS® Software Release 12.4(4)T. Configuring multiple tunnels on a single remote device can be accomplished in several ways. This configuration guide discusses the configuration of a second Easy VPN tunnel using Auto Configuration Update. The second tunnel is using Enhanced Easy VPN Tunnel with VTI. Please refer to the Cisco Easy VPN Remote feature documentation for further discussion on this feature.

There are two possible combinations in which the dual tunnels can be used.

- Dual Easy VPN tunnels that have one tunnel using a non-split tunnel policy and the other tunnel using a split tunnel policy that has been pushed from the respective headend.
- Dual Easy VPN tunnels in which both tunnels are using an independent split tunnel policy that has been pushed from the respective headend.

The Easy VPN dual tunnel makes use of route injections to direct the appropriate traffic through the correct Easy VPN VTI. When the Easy VPN tunnel on the remote device “comes up,” it “learns” the split or non-split policy from the headend. The Easy VPN Remote device injects routes in its routing table that correspond to the non-split networks that have been learned. If the headend pushes a non-split tunnel policy to the Easy VPN Remote device, the device installs a default route in its routing table that directs all traffic out of the Easy VPN virtual interface that corresponds to

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

this Easy VPN tunnel. If the headend pushes split-tunnel networks to the remote device, the remote device installs specific routes to the split networks in its routing table, directing the traffic to these networks out of the VTI.

AUTO CONFIGURATION UPDATE

Auto Configuration Update is a new feature, introduced in Cisco IOS Software Release 12.4(4)T, that allows any configuration change to be pushed to any number of Cisco IOS Software-based Easy VPN hardware clients (Cisco routers running as Easy VPN Remote, for example). Auto Configuration Update also provides zero-touch provisioning of any feature (voice, routing, etc.). It can be used to enable any feature on the fly, such as enabling access control lists (ACLs), firewalls, IPSs, and quality of service (QoS). Auto Configuration Update has two components—one deals with configuration and the other deals with monitoring and reporting.

Configuration Manageability Component

The configuration component addresses the changes or additional configuration needs to be pushed on Cisco IOS Easy VPN Remote devices. Two new attributes—"configuration url" and "configuration version"—were introduced in the IPSec policy push, also called "MODCFG".

During IPSec phase 2 the "configuration url" push attribute is pushed to the Easy VPN Client, which it applies it right away. Use the following command on the Easy VPN Server to specify the URL that the remote device must use to get the configuration file:

configuration url https://IPaddress/router.cfg

The configuration URL can use any of the following protocols: SCP, TFTP, FTP, HTTP, or HTTPS.

The "configuration version" attribute maintains the version of the configuration file. The remote router must use the new configuration file, if it has a lower configuration version number.

Configuration changes are required on the remote router. Both the server and the remote router must meet the minimum software version requirements.

Monitoring and Reporting Component

As soon as the configuration changes apply at Cisco Easy VPN Remote, an update notification will be generated. This update notification comprises detailed information about Easy VPN Remote, including:

- Platform
- Memory size/available memory
- Flash size/available flash
- Public IP addresses
- Assigned IP address
- Cisco IOS image
- Serial number
- Configuration version
- Hostname

This information will be available via CLI at the Easy VPN Server. It can be easily written to Cisco Secure Access Control Server (ACS) or to any standard RADIUS server. Easy VPN Server writes records to the RADIUS server using Cisco AV-Pair via RADIUS accounting; this requires activating RADIUS accounting at the Easy VPN Server.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

CONFIGURATION SUMMARY

Using Easy VPN with VTI, the traffic is forward to or from the IPSec tunnel interface by virtue of the IP routing table lookup. Routes are dynamically learned during IKE Mode Configuration exchange, and inserted into the routing table pointing to the virtual access interface.

This configuration allows for split tunneling. With split tunneling, remote users can send traffic destined for the Internet directly, without going onto the IPSec tunnel.

The remote router uses a static IP address for the WAN interface. Dynamic IP addresses can be used for typical DSL and cable connectivity configurations. Also, the remote router is in User Mode. In this mode, the remote subnet can be a private IP network that is invisible to the hub network. All traffic sent from the remote subnet uses Network Address Translation (NAT) to translate an IP address downloaded from the Easy VPN Server. An alternative would be to use Network Extension mode in this configuration to enable the support of devices such as VoIP phones located at the remote site.

This configuration shows two types of Easy VPN tunnels: a traditional Easy VPN tunnel using the primary path, and an Enhanced Easy VPN tunnel with DVTI using the backup path. The two different types of tunnels were used for purpose of demonstration only; both tunnels can be of the same type. With traditional Easy VPN tunnel, one or more IPSec security associations are created for each IPSec tunnel (depending on the server configuration) with each IPSec security association allowing a specific source and destination IP address on the IPSec tunnel. With Enhanced Easy VPN, only one IPSec security association is created for each IPSec tunnel with any source to any destination IP addresses.

For more information about the IPSec DVTI feature, see the document IPSec Virtual Tunnel Interface; a hyperlink is provided in the Related Information section of this document.

PREREQUISITES

The sample configuration is based on the following assumptions:

- The remote router is configured with IP addresses and the router can reach the Internet.
- IP NAT is configured on the remote router on the interfaces only. Easy VPN dynamically creates the global NAT configuration to provide connectivity to end users when Easy VPN is connected.
- A static IP address on the remote router is not required and DHCP can be used instead.
- Split tunneling for end-user traffic is enabled, allowing Internet traffic to go directly to the Internet.

LIMITATIONS

This guide provides a sample of Cisco Easy VPN configuration. 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 secure the router.
- This configuration guide enables split tunneling. Split tunneling is enabled on the hub by the ACL 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. Only one Easy VPN Server can have split tunneling disabled with Easy VPN dual tunnel support.
- The Easy VPN Remote router is configured with Port Address Translation (PAT) to provide Internet connectivity. The Easy VPN Remote router configuration requires Cisco IOS Software Release 12.4(4)T to work.
- This configuration uses Network Extension Mode. For details on configuring User Mode, please review documentation for Cisco Easy VPN Remote or Server.
- This configuration guide shows how an end user can use Cisco SDM to bring up basic IPSec configuration to allow the Auto Configuration Update from the Easy VPN Server to download the branch.cfg file into the running configuration. The Cisco SDM version used in this configuration guide does not manage dual tunnel configurations on the easy VPN remote router.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

COMPONENTS USED

The sample configuration uses the following software and hardware releases:

- Cisco IOS Software Release 12.4(4)T
- Cisco 3725, 3845, and 7206 routers
- Cisco SDM Version 2.2

Figure 1 illustrates the sample network 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. If you are working in a live network, it is imperative to understand the potential impact of any command before implementing it.

IMPLEMENTING DUAL EASY VPN TUNNEL WITH AUTO CONFIGURATION UPDATE

This section contains the following steps:

- Initial remote router configuration
- Cisco SDM configuration steps
- branch.cfg configuration file
- Final remote router configuration
- Remote router status
- Primary Cisco Easy VPN Server configuration
- Primary Cisco Easy VPN Server status

Initial Remote Router Configuration

```
version 12.4
!
hostname c3845-31
!
no aaa new-model
!
ip subnet-zero
!
ip cef
!
ip domain name yourdomain.com
!
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.248
!
interface GigabitEthernet0/1
 ip address 172.19.196.39 255.255.255.0
!
interface FastEthernet1/0
 description $FW_OUTSIDE$
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
 ip address 10.0.35.231 255.255.255.0
 ip verify unicast reverse-path
 ip nat outside
 ip virtual-reassembly
 duplex full
 speed 100
!
interface FastEthernet1/1
 ip address 192.168.22.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Virtual-Template1 type tunnel
 no ip address
 ip virtual-reassembly
!
interface Vlan1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.35.216
!
!
ip http server
ip http authentication local
ip http secure-server
!
end
```

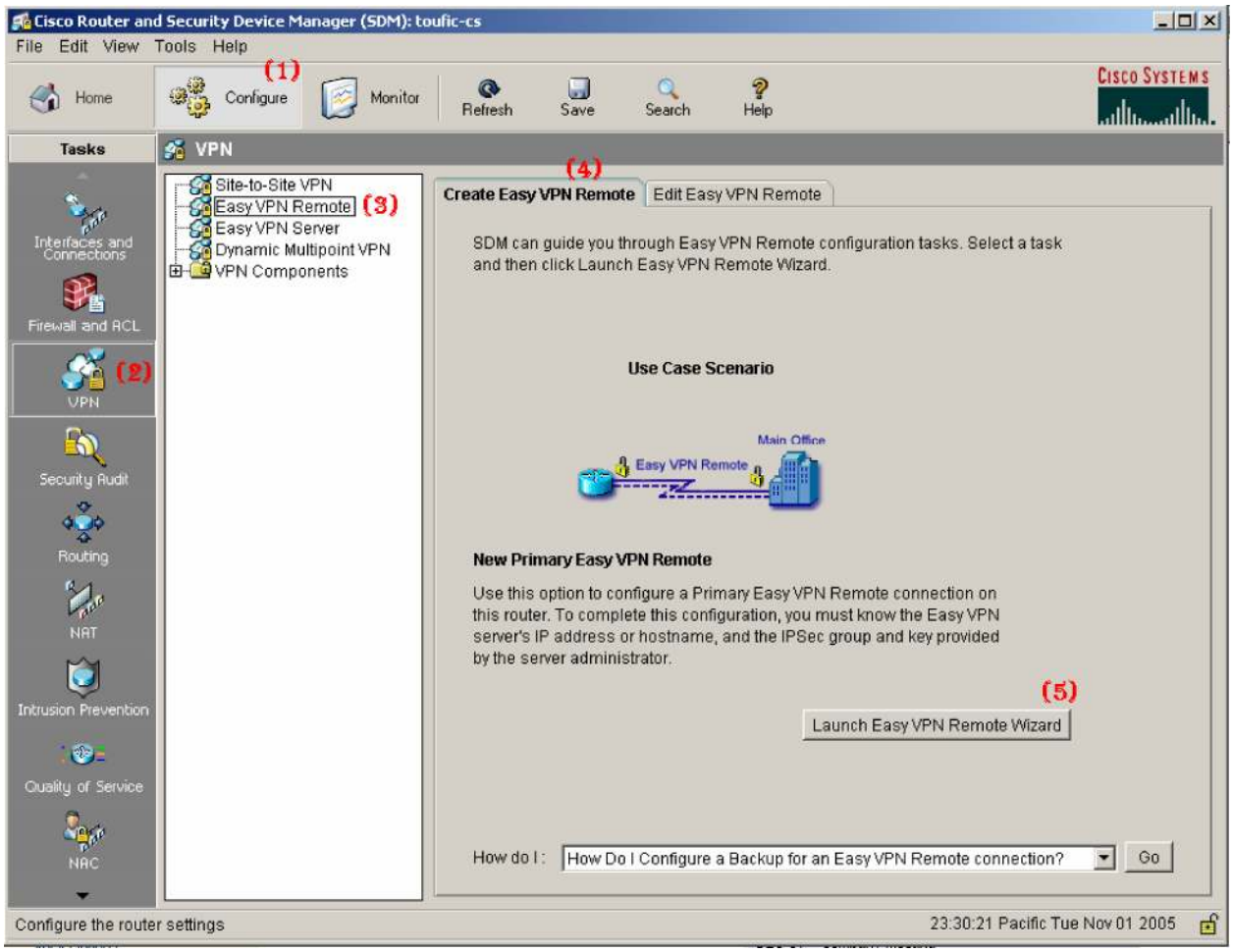
© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Cisco SDM Configuration Steps

Step 1: Launch Easy VPN Remote Configuration Wizard.

From the main Cisco SDM window, select as shown in Figure 2: Configure (1), VPN (2), Easy VPN Remote (3), Create Easy VPN Remote (4), and the Launch Easy VPN Remote Wizard (5).

Figure 2. Launch Cisco Easy VPN Remote Wizard

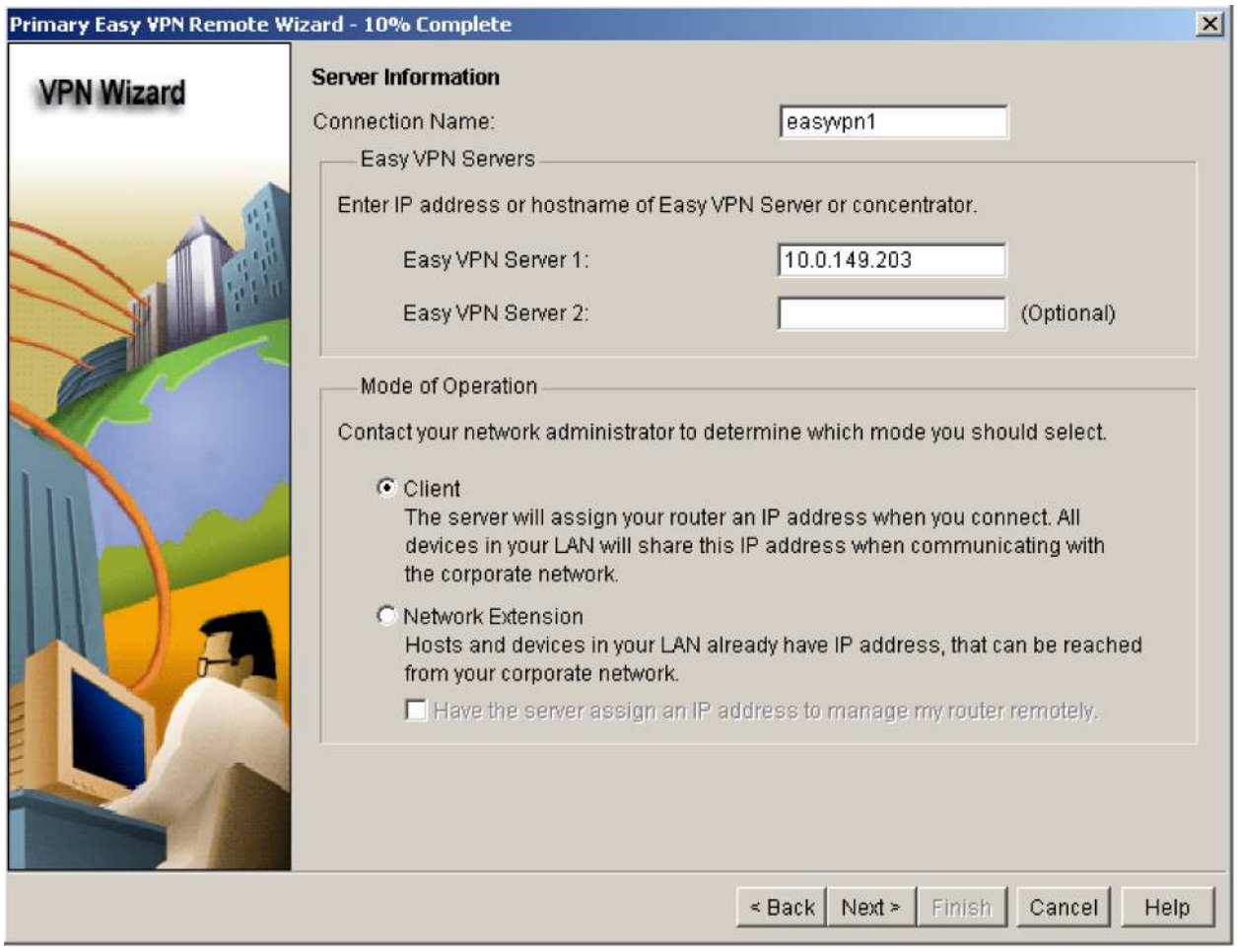


Step 2: Select “Next” on the “Configure a Primary Easy VPN Remote Connection” window.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Step 3: Enter connection name and Easy VPN Server 1 IP address as shown in Figure 3. Then, select “Next”.

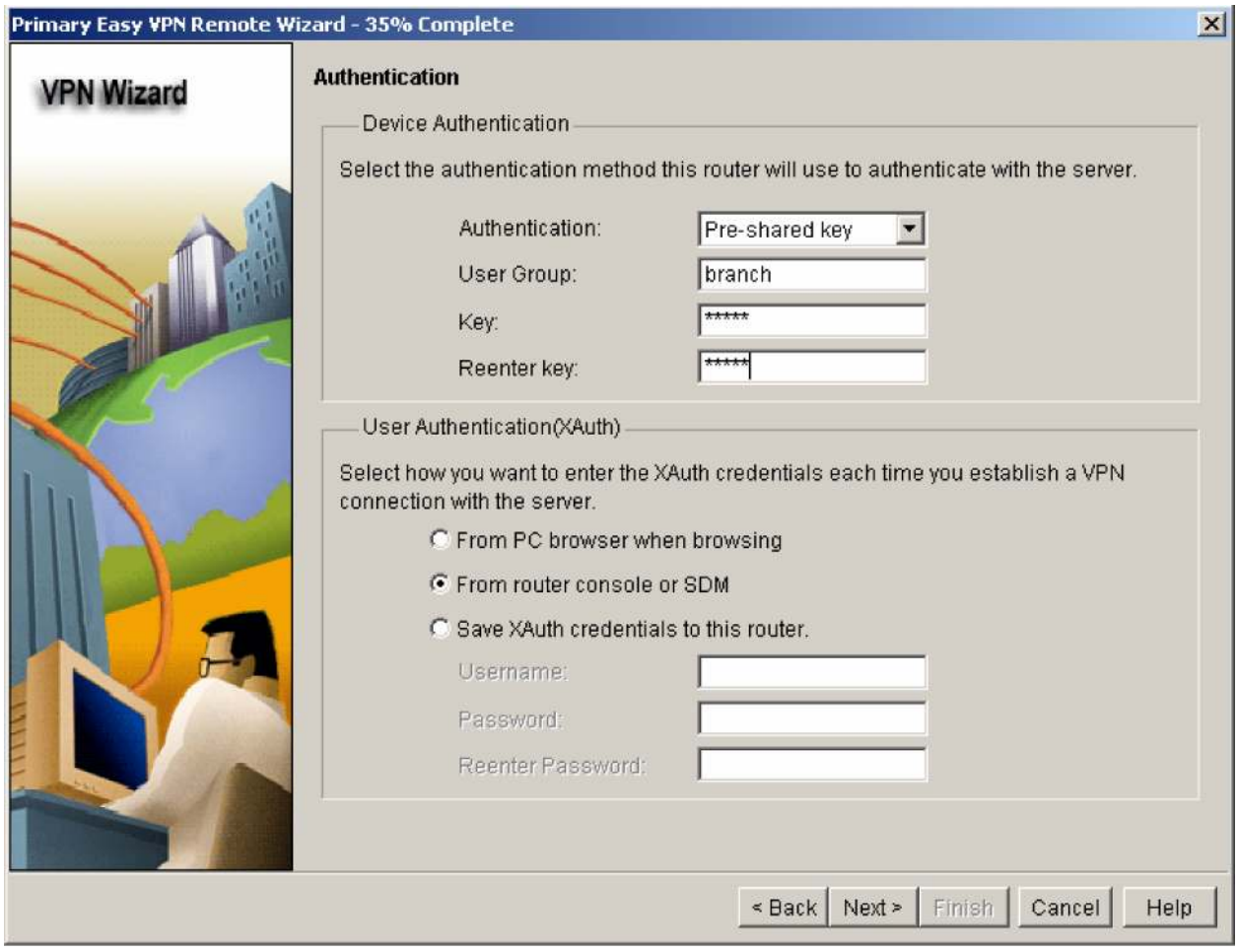
Figure 3. Server Information Window



© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Step 4: Enter the device authentication information as shown in Figure 4. Then, click “Next”.

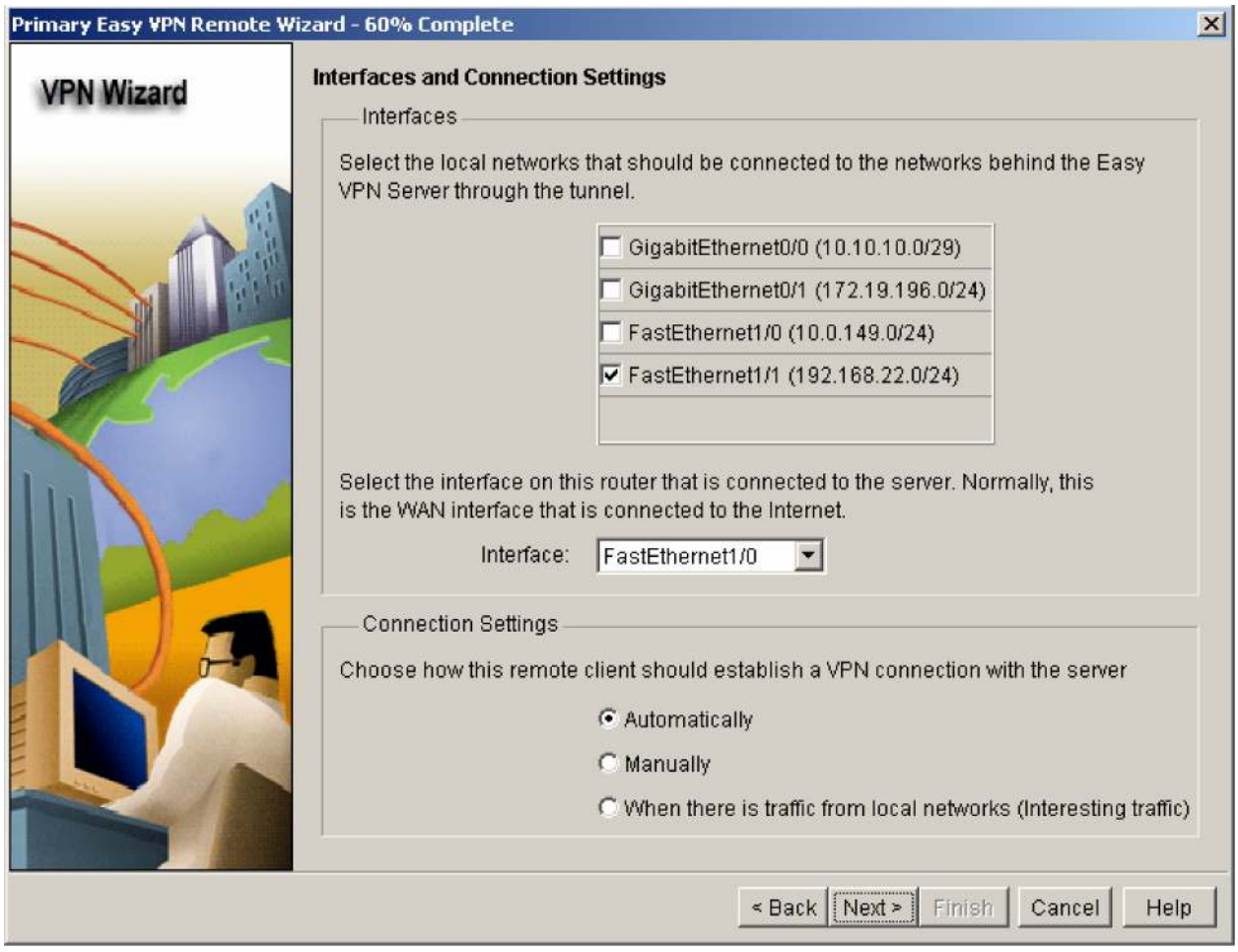
Figure 4. Device Authentication



© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Step 5: Select the local networks connected to the Easy VPN tunnel and to the WAN interface as shown in Figure 5. Then, select "Next".

Figure 5. Interface and Connection Settings Window



Step 6: Review the summary of the configuration window. Next, select "Finish".

Step 7: Following is the list of commands delivered to the router:

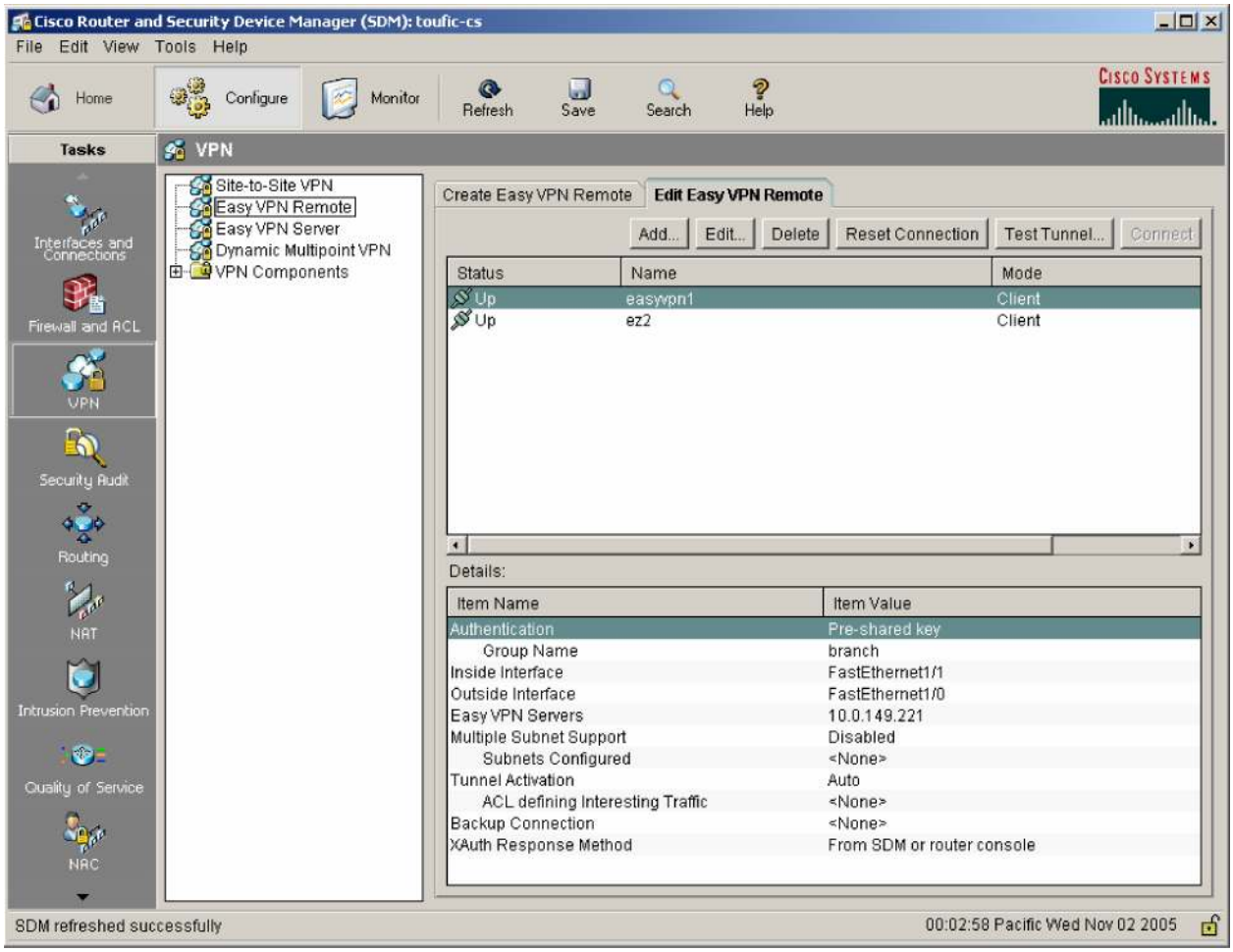
```
!
crypto ipsec client ezvpn easyvpn1
 group branch key 0 *****
 peer 10.0.149.203
 exit
interface FastEthernet1/1
 crypto ipsec client ezvpn easyvpn1 inside
 exit
interface FastEthernet1/0
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
 crypto ipsec client ezvpn easyvpn1 outside
 exit
!
```

Step 8: Once the configuration generated by the wizard has been delivered by the router, review the edited Easy VPN Remote tab for the router status. (Note: Cisco SDM may show one tunnel at first. Selecting “Refresh” may be required to view both tunnels).

Figure 6. Easy VPN Remote Status with Configured easyvpn1 Tunnel, and ez2 Tunnel Configuration Downloaded from the Easy VPN Server; Both Tunnels status shows are “Up”.



branch.cfg Configuration File

Following is the configuration file downloaded from the Easy VPN Server. The configuration file can contain any Cisco IOS commands to reconfigure the remote router—configuration such as QoS, routing, or even multicast. Note: This configuration is downloaded to the running memory. To store the configuration to the startup configuration, users have to use the “do” keyword for applying certain commands like “do write mem”.

```
!
interface Virtual-Template1 type tunnel
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
exit
!
crypto ipsec client ezvpn ez2
 connect auto
 group cisco key cisco
 local-address FastEthernet1/0
 mode client
 peer 10.0.149.221
 virtual-interface 1
 xauth userid mode interactive
exit
!
interface Ethernet0
interface FastEthernet1/1
 crypto ipsec client ezvpn ez2 inside
!
interface FastEthernet1/0
 crypto ipsec client ezvpn ez2
!
```

Final Remote Router Configuration

```
version 12.4
!
hostname c3845-31
!
no aaa new-model
ip subnet-zero
!
ip cef
!
p domain name yourdomain.com
ip name-server 6.0.0.2
!
crypto isakmp keepalive 10 periodic
!
crypto ipsec client ezvpn ez2
 connect auto
 group cisco key cisco
 local-address FastEthernet1/0
 mode client
 peer 10.0.149.221
 virtual-interface 1
 xauth userid mode interactive
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
crypto ipsec client ezvpn easyvpn1
 connect auto
 group branch key cisco
 mode client
 peer 10.0.149.203
 xauth userid mode interactive
!
!
!
!
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.248
!
interface GigabitEthernet0/1
 ip address 172.19.196.39 255.255.255.0
!
interface FastEthernet1/0
 description $FW_OUTSIDE$
 ip address 10.0.35.231 255.255.255.0
 ip verify unicast reverse-path
 ip nat outside
 ip virtual-reassembly
 duplex full
 speed 100
 crypto ipsec client ezvpn ez2
 crypto ipsec client ezvpn easyvpn1
!
interface FastEthernet1/1
 ip address 192.168.22.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto ipsec client ezvpn ez2 inside
 crypto ipsec client ezvpn easyvpn1 inside
!
interface Virtual-Template1 type tunnel
 no ip address
 ip virtual-reassembly
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.35.216
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
ip http server
ip http authentication local
ip http secure-server
!
end
```

Remote Router Status

```
c3845-31#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: FastEthernet1/0
Session status: UP-ACTIVE
Peer: 10.0.149.203 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.0.149.203
      Desc: (none)
  IKE SA: local 10.0.35.231/500 remote 10.0.149.203/500 Active
         Capabilities:CD connid:1001 lifetime:23:36:54
  IPSEC FLOW: permit ip host 30.30.30.25 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound: #pkts dec'ed 1345 drop 0 life (KB/Sec) 4444433/2244
        Outbound: #pkts enc'ed 1345 drop 0 life (KB/Sec) 4444433/2244

Interface: FastEthernet1/0
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 10.0.35.231/500 remote 10.0.149.221/500 Active
         Capabilities:CD connid:1002 lifetime:23:37:30
  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 1342 drop 0 life (KB/Sec) 4462716/2247
        Outbound: #pkts enc'ed 1342 drop 0 life (KB/Sec) 4462716/2247

c3845-31#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
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
       ia—IS-IS inter area, *—candidate default, U—per-user static route
       o—ODR, P—periodic downloaded static route

Gateway of last resort is 10.0.35.216 to network 0.0.0.0
S    192.168.72.0/24 [1/0] via 0.0.0.0, Virtual-Access2
     5.0.0.0/32 is subnetted, 1 subnets
C       5.0.0.3 is directly connected, Loopback1
     172.19.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.19.196.0/24 is directly connected, GigabitEthernet0/1
S    192.168.20.0/24 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.35.0/24 is directly connected, FastEthernet1/0
S       10.0.149.221/32 [1/0] via 10.0.35.216
C    192.168.22.0/24 is directly connected, FastEthernet1/1
     30.0.0.0/32 is subnetted, 1 subnets
C       30.30.30.25 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 10.0.35.216

c3845-31#show crypto ipsec client ez
Easy VPN Remote Phase: 6

Tunnel name : easyvpn1
Inside interface list: FastEthernet1/1
Outside interface: FastEthernet1/0
Current State: IPSEC_ACTIVE
Last Event: CONN_UP
Address: 30.30.30.25
Mask: 255.255.255.255
Default Domain: branch.com
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 192.168.20.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Split Tunnel List: 2
       Address    : 192.168.71.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Configuration URL [version]: tftp://10.0.149.203/branch.cfg [21]
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
Config status: applied, Last successfully applied version: 21
Current EzVPN Peer: 10.0.149.203

Tunnel name : ez2
Inside interface list: FastEthernet1/1
Outside interface: Virtual-Access2 (bound to FastEthernet1/0)
Current State: IPSEC_ACTIVE
Last Event: CONN_UP
Address: 5.0.0.3
Mask: 255.255.255.255
DNS Primary: 6.0.0.2
NBMS/WINS Primary: 7.0.0.1
Default Domain: cisco.com
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 192.168.20.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Split Tunnel List: 2
       Address    : 192.168.72.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 10.0.149.221

c3845-31#show interface virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (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 0x44, loopback not set
  Keepalive not set
  Tunnel source 10.0.35.231 (FastEthernet1/0), destination 10.0.149.221
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
  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, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     1477 packets input, 94528 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
     1479 packets output, 94656 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Primary Cisco Easy VPN Server Configuration

```
!
crypto isakmp client configuration group branch
 key cisco
 domain branch.com
 pool dynpool
 acl 150
 configuration url tftp://10.0.149.203/branch.cfg
 configuration version 21
!
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 default
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
interface Ethernet3/0
 ip address 10.0.149.203 255.255.255.0
 ip accounting output-packets
 ip route-cache flow
 load-interval 30
 duplex full
 crypto map dynmap
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
!
access-list 150 permit ip 192.168.20.0 0.0.0.255 any log-input
access-list 150 permit ip 192.168.71.0 0.0.0.255 any log-input
!
```

Primary Cisco Easy VPN Server Status

```
c7200-3#show crypto isakmp peers config

Client-Public-Addr=10.0.35.231:500; Client-Assigned-Addr=30.30.30.25; Client-Gro
up=branch; Client-User=; Client-Hostname=c3845-31.yourdomain.com; Client-Platfor
m=Cisco 3845; Client-Serial=FHK0848F19B; Client-Config-Version=21; Client-Flash=
63885312; Client-Available-Flash=14819328; Client-Memory=226492416; Client-Free-
Memory=139450512; Client-Image=flash:c3845-advsecurityk9-mz.124-3.9.T9;
```

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

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

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 Website 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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

205233.CD_ETMG_KS_11.05

Printed in the USA

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.