

Application Note

Cisco Router and Security Device Manager Cisco Easy VPN Remote

Introduction

This document explains how to configure a Cisco® Easy VPN Remote.

Cisco Easy VPN Introduction

Cisco Easy VPN greatly simplifies virtual private network (VPN) deployment for remote offices and teleworker. The Cisco Easy VPN solution centralizes VPN management across all Cisco VPN devices, thus reducing the management complexity of VPN deployments. Cisco Easy VPN consists of two components: Cisco Easy VPN Remote and Cisco Easy VPN Server. The Cisco Easy VPN Remote feature allows Cisco IOS routers to receive security policies upon a VPN tunnel connection from a Cisco Easy VPN Server, minimizing configuration requirements at the remote location. This cost-effective solution is ideal for remote offices with little IT support. The Cisco Easy VPN Server allows Cisco IOS routers to act as VPN head-end devices in site-to-site or remote-access VPNs, where the remote office devices are using the Cisco Easy VPN Remote feature. This feature pushes security policies defined at the central site to the remote VPN device, helping to ensure that those connections have up-to-date policies in place before the connection is established.

A Cisco Easy VPN Server-enabled device can terminate VPN tunnels initiated by Cisco Easy VPN Remote-enabled routers. The Cisco Easy VPN Remote feature allows the VPN parameters, such as internal IP addresses, internal subnet masks, Domain Name System (DNS) server addresses, Windows Internet Naming Service (WINS) server addresses, and Split Tunneling flags, to be pushed to the remote device. The centrally stored configurations allow dynamic configuration of end-user policy and require less manual configuration by end users and field technicians. This reduces errors and further service calls. The Cisco Easy VPN provides centralized security policy management and helps enable large-scale deployment with rapid user provisioning.

Cisco Easy VPN provides automatic management for negotiating tunnel parameters and establishing IP Security (IPSec) tunnels. Extended authentication (Xauth) adds another level of authentication that identifies the user who requests the IPSec connection. Split Tunneling enables the remote router to route the internet-destined traffic directly without forwarding it over the encrypted tunnel.

It is easier than ever to deploy VPNs as part of small and medium businesses or large enterprise networks with Cisco Router and Security Device Manager (SDM).

Deployment Scenario

This document demonstrates how to configure a Cisco Easy VPN Remote feature.

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

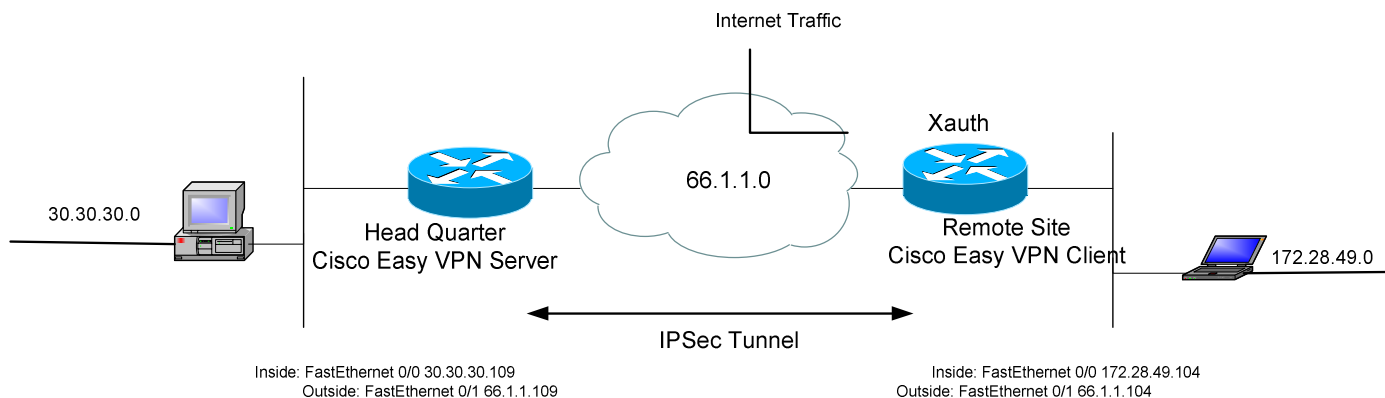
- Static IP address is at the Cisco Easy VPN Server.
- Static or Dynamic IP address is at the Cisco Easy VPN Remote.
- The Cisco Easy VPN Remote encrypts only traffic that is forwarded to the Cisco Easy VPN Server.



- Traffic destined for the Internet is forwarded directly and unencrypted from the remote site.
- Traffic from the remote site is forwarded after applying Network Address Translation/Port Address Translation (NAT/PAT).
- User level authentication is used for authorizing VPN access (Xauth¹)

Figure 1 illustrates the network for the sample configuration.

Figure 1. Network Diagram



Sample Configuration

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

Split Tunneling is configured on the Cisco Easy VPN Server and dynamically loaded on the Cisco Easy VPN Remote. Split Tunneling enables the remote router to route the Internet-destined traffic directly without forwarding it over the encrypted tunnel.

In our example, a preshared key is used to authenticate devices². Xauth provides an additional level of authentication for identifying the user requesting the IPsec connection. The remote waits for a “username/password” challenge after the Internet Key Exchange (IKE) Security Association has been established.

Prerequisite

The device started with a cleared default SDM configuration with LAN and WAN interfaces configured.

Cisco SDM Cisco Easy VPN Remote

Cisco Router and SDM allows users to easily configure the Cisco Easy VPN Remote with limited knowledge and information (usually provided by the system administrator). The following steps are used to configure the deployment scenario using Cisco SDM:

Create a Cisco Easy VPN Remote

At **Configure Mode**, Select **VPN/Easy VPN Remote/Create Easy VPN Remote** (Figure 2) to launch the Cisco Easy VPN Remote Wizard.

To configure the Connection Information, take the following steps:

¹ Xauth allows authenticating a user after authenticating the gateway (for instance, the Cisco Easy VPN Remote/Client), provides good authentication where certificates cannot be used and solves the issue of not knowing the IP address in advance.

² IPsec main mode device authentication is based on IP address and preshared key or digital certificate.



- Easy VPN tunnel name: **ToHQ**
- Easy VPN Server
 - Easy VPN server 1: **66.1.1.109**
 - Easy VPN server 2: **66.1.1.107**
- Group: **EZVPNgroup**
- Key: **cisco123** (the key is displayed encrypted on screen)
- Click **Next**

Figure 2. Cisco **Easy VPN Remote Wizard**

Easy VPN client Wizard

VPN Wizard

Connection Information

Easy VPN tunnel name:

Please obtain the following information from the server administrator.

Easy VPN Server

Easy VPN server 1: (IP address or hostname)

Easy VPN server 2: (IP address or hostname)
(Optional)

Specify the IPSec group and IPSec key value. The value of group and key must match the group and key defined on the Easy VPN server.

Group: Key:

Re-enter key:

< Back Next > Finish Cancel Help



For the Connection Characteristics Configuration, take the following steps:

- Mode: **Client**
- Control: **Auto**
- Then click **Next**

To configure the User Authentication (Xauth), enter the following (optional) information:

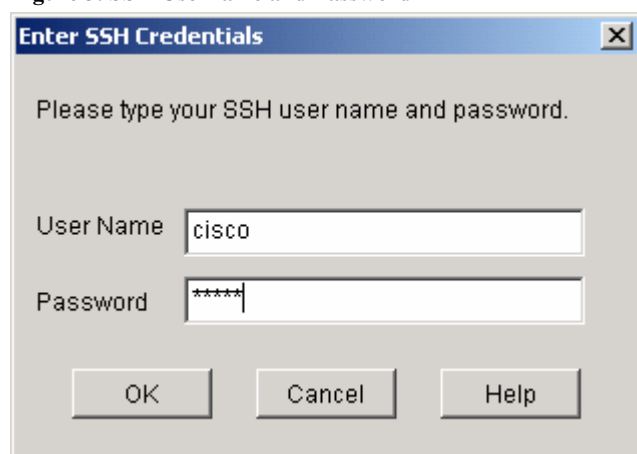
- Check **Save Xauth username and password on the router**
- Username: **sdmuser1**
- Password: **cisco123**
- Then click **Next**

For interfaces, enter the following information:

- Select the outside interface that is connected to the ISP (This example is **FastEthernet0/1**)
- Select the inside interfaces that you want to include in this VPN connection (This example is **FastEthernet0/0**)
- Then click **Next**
- You will be prompted to enable IKE. If it is disabled, click **OK**
- Click **Finish**
- Click **Deliver**

You will be directed to the **Edit Easy VPN Remote** screen and prompted for Secure Shell (SSH) Protocol username and password (Figure 3). Encrypted username and password must be sent to the device to respond Xauth challenge from Cisco Easy VPN Server.

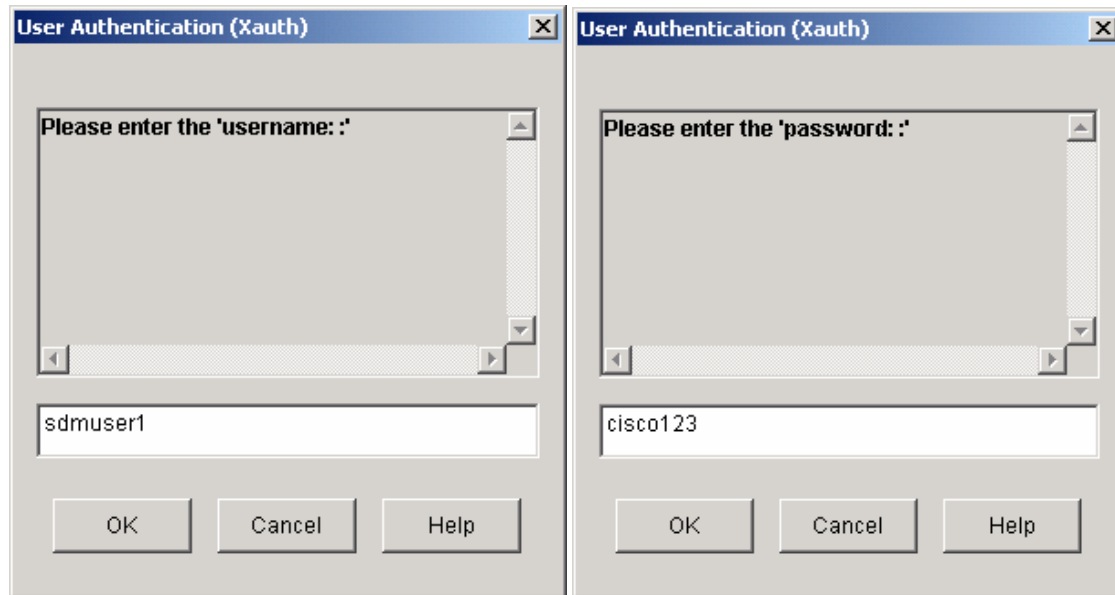
Figure 3. SSH Username and Password



After the IKE SA is successfully established, the Cisco Easy VPN Remote waits for “username/password” challenge (Figure 4) and then responds to the peer’s challenge.

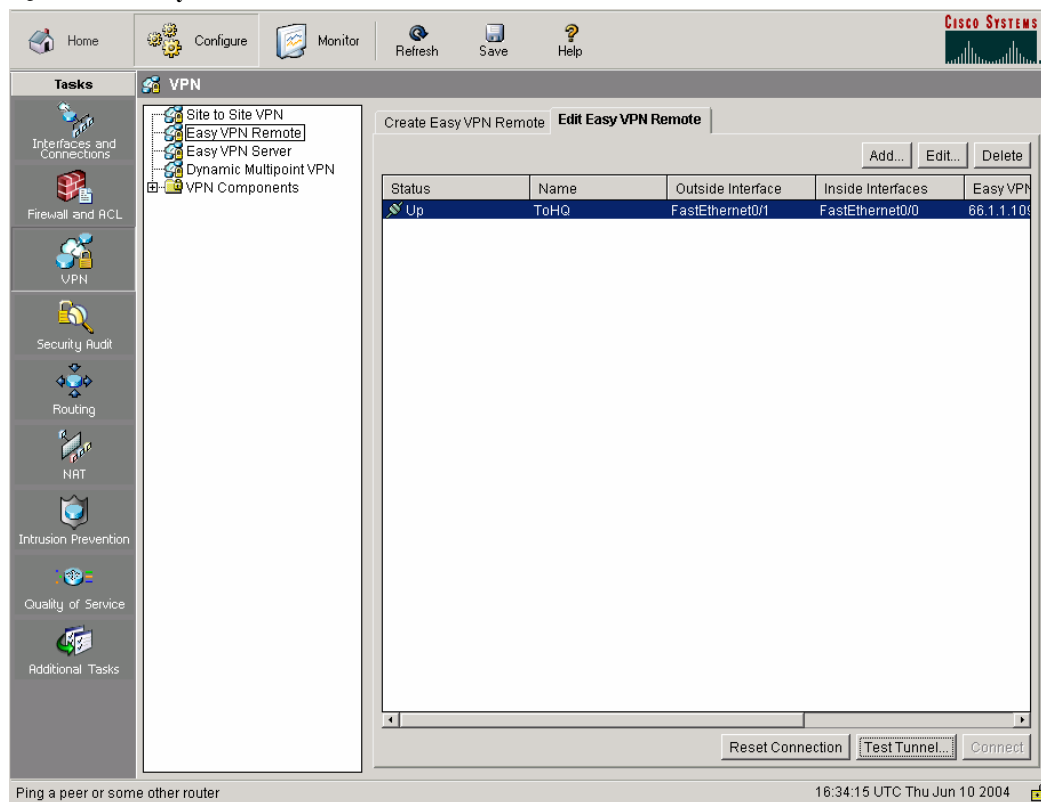


Figure 4. Xauth Username and Password



After the IPsec tunnel is established, the Status will be changed to Up (Figure 5).

Figure 5. Cisco Easy VPN Remote Status



If the Status is Down and no Xauth challenge occurs, click **Test Tunnel** to test the tunnel. Figure 6 shows the tunnel testing process.

Figure 6. Test Tunnel



VPN Troubleshooting

Tunnel Details

Interface: FastEthernet0/1 Peer: 66.1.1.109,66.1.1.107

Summary Details

Activity	Status
Checking the tunnel status...	Down
Checking interface status...	Success
Checking the configuration...	Success
Checking Routing...	Success
Checking peer connectivity...	Success
Checking Firewall...	Success
Debugging the VPN connection ...	In Progress..

Reason(s)	Recommended Action(s)
-----------	-----------------------

Stop Save Report... Close Help



Monitoring

Users can go to **Monitor Mode** and select **VPN Status** to view and verify the tunnel status. Figure 7 shows the IPsec Tunnels and IKE SA on Cisco Easy VPN Remote.

Figure 7. IPsec Tunnels and IKE SA

The screenshot displays the Cisco Easy VPN Remote monitoring interface. The top navigation bar includes Home, Configure, Monitor, Refresh, Save, and Help. The left sidebar shows Tasks: Overview, Interface Status, Firewall Status, and VPN Status. The main content area is titled 'VPN Status' and contains two tabs: 'IPsec Tunnels' and 'IKE SAs'. The 'IPsec Tunnels' tab is active, showing a table with one row of data. The 'IKE SAs' tab is also visible, showing a table with one row of data.

IPsec Tunnels

Each row represents one IPsec Tunnel

Local IP	Remote IP	Peer	Tunnel Status	Encapsulation P	Decapsulation P	Send Error Pack	Received Error P
66.1.1.104	66.1.1.109	66.1.1.109:500	Up	0	0	0	0

IKE SAs

Each row represents one IKE SA

Source IP	Destination IP	State
66.1.1.104	66.1.1.109	QM_IDLE



Cisco IOS Software Command-Line Interface (CLI)

The following CLIs are used to configure the same deployment scenario as above as opposed to the SDM.

The Cisco Easy VPN Remote Configuration

```
!  
crypto isakmp enable  
crypto ipsec client ezvpn ToHQ           ! create a Cisco Easy VPN Remote named to  
headquarters  
    connect auto  
    mode client                          ! specify that VPN client is using NAT/PAT  
    group EZVPNgroup key cisco123        ! match the group name EZVPNgroup and preshare key  
                                           ! cisco123 defined on the Cisco Easy VPN Server  
    peer 66.1.1.109                      ! primary Cisco Easy VPN Server  
    peer 66.1.1.107                      ! secondary Cisco Easy VPN Server  
    username sdmuser1 password cisco123  ! save Xauth username/password in the server if  
                                           ! the save password feature is enabled in server  
interface FastEthernet0/0  
    crypto ipsec client ezvpn toHQ inside  
interface FastEthernet0/1  
    crypto ipsec client ezvpn toHQ outside ! outside interface for the NAT/PAT translation
```

In summary, by using the Cisco SDM Cisco Easy VPN Wizards, users can generate Easy VPN Remote configuration easily and quickly with minimum knowledge of Cisco IOS® Software commands and client-server IPsec VPN.



References

Cisco Easy VPN Solution:

http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns171/ns27/networking_solutions_sub_solution_home.html

Cisco Easy VPN White Paper:

http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns171/ns27/networking_solutions_white_papers_list.html

Cisco Easy VPN Remote:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/ftzvpnr.pdf



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 • 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 2004 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, 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 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, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, 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, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0406R)

Printed in the USA