CHAPTER 16

Configuring Cisco Easy VPN

Traditionally, Virtual Private Network (VPN) connectivity has been viewed as rather complex and requiring specialized resources to implement. While this is true from a hardware perspective, the same is not necessarily true from a software perspective. In fact, the advent of the Cisco Integrated Services Router has made VPN connectivity, well, easy.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 12-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 16-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 16-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
Cisco Easy VPN Components	1–3	
Easy VPN Connection Establishment	4–6	
Easy VPN Server Configuration	7–9	
Monitoring the Easy VPN Server	10	
Troubleshooting the Easy VPN Server	11–12	
Total Score		

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Easy VPN Remote supports three modes of operation. These include Client mode, Network Extension mode, and which of the following?
   a. Network Extension Plus mode
   b. Peer-to-peer mode
   c. Overlay mode
   d. DMVPN mode
2. To implement Easy VPN Remote capabilities, which requirement must be met?
   a. The destination peer must be a Cisco Easy VPN Server or VPN Concentrator supporting Cisco Easy VPN Server.
   b. The source peer must be a Cisco Easy VPN Server or VPN Concentrator supporting Cisco Easy VPN Server.
   c. The destination peer must be a Cisco Easy VPN Remote device.
   d. The destination peer must support all available encryption and authentication types.
3. Easy VPN Servers must support Diffie-Hellman IKE negotiation using which group?
   a. Group 1
   b. Group 2
   c. Group 3
   d. Group 4
4. When establishing a VPN connection using an Easy VPN Remote Client, which of the following occurs immediately after the IKE phase 1 initialization?
   a. SA proposal acceptance
   b. ISAKMP SA establishment
   c. user authentication
   d. RRI
5. If not using a preshared key for authentication, which mode will IKE phase 1 initiate?
   a. Aggressive mode
   b. Main mode
   c. Authorization mode
   d. Configuration mode

6. The process of creating and redistributing a static route pointing to the client subnet is known as which of the following?
   a. Reverse Path Forward
   b. Reverse Route Injection
   c. Floating Static Route
   d. Route Dampening
7. To configure the Easy VPN Server using the SDM wizard, which of the following must be configured?
   a. TACACS
   b. A user account with privilege level 15
   c. DNS
   d. NTP
8. Group Lock and Saved Password capabilities are generally associated with the configuration of which of the following?
   a. RRI
   b. IKE
   c. Xauth
   d. ISAKMP SA
9. When configuring split tunneling capabilities, which of the following should also be configured?
   a. RRI
   b. Protected subnets
   c. Personal firewall
   d. Backup servers
10. Which command will allow an administrator to view the current status of a VPN Client ISAKMP SA?
    a. **show crypto isakmp sa**
    b. **show ip isakmp sa**
    c. **show crypto ipsec sa**
    d. **show ip ipsec sa**

11. Which command will allow a network administrator to view real-time information regarding ISAKMP connections on an Easy VPN Server?

    a. **debug crypto isakmp**
    b. **debug ip isakmp**
    c. **debug crypto ipsec**
    d. **debug ip ipsec**

12. In cases where AAA services are in use, which command will allow a network administrator to monitor activity related to username and password exchanges in real time?

    a. **debug crypto isakmp**
    b. **debug crypto ipsec**
    c. **debug aaa authentication**
    d. **debug aaa authorization**

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- **11 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

The growing move toward the Service-Oriented Network Architecture (SONA) is laying down a path of evolution that will enable clients of all types to access network resources, applications, and services available to those in the corporate headquarters site. This allows enterprise networks to move further toward the goal of providing a single experience to all users regardless of the method by which they access those applications and services.

The Cisco Easy VPN solution simplifies the deployment of remote offices and teleworkers. Teleworkers, on the whole, represent one of the fastest growth areas of network users. The availability of high bandwidth at low cost is spurring a great deal of industry evolution. Along with this growth in remote connection requests comes a similar, if not greater, growth in security needs of the network.

Cisco Easy VPN serves to simplify client configuration and allow for a centralized management model of VPN Clients. This client configuration can be dynamically pushed to remote clients. Cisco Easy VPN provides a quick, efficient, and, most importantly, secure means of configuring VPN services for remote users of all kinds. It consists of two primary components, Easy VPN Remote and Easy VPN Server.

Using Internet Key Exchange (IKE) Mode Config functionality to push configuration parameters to clients, the clients can be preconfigured to conform to a set of IKE policies and IPsec transform sets. This ensures that all clients are up to date with the latest policies in place prior to establishing connections.

Cisco Easy VPN Components

The Cisco Easy VPN solution consists of two components, Server and Remote. Cisco Easy VPN Server allows Cisco IOS Routers, Cisco PIX Security Appliances, and Cisco VPN 3000 Concentrators to act as VPN headend devices in site-to-site or remote-access VPN models. Easy VPN–enabled devices can terminate IPsec tunnels initiated by teleworkers using the Cisco VPN Client software on a PC. This makes it possible for mobile and remote workers to access corporate services and applications.

Easy VPN Remote

Cisco Easy VPN Remote enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN 3000 series hardware/software clients to act as remote VPN Clients. They receive security policies from an Easy VPN Server. This minimizes the need for manual configuration tasks. Easy VPN Remote provides for automated, centralized management of the following:

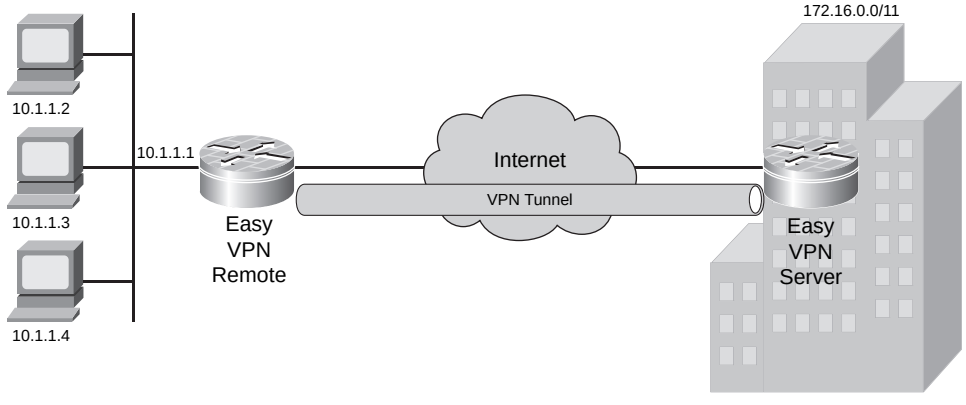
- Tunnel parameter negotiation (addresses, algorithms, and duration)
- Tunnel establishment according to set parameters
- Automatic creation of Network Address Translation (NAT) and Port Address Translation (PAT) as well as any needed access control lists (ACL)
- User authentication
- Security key management for encryption and decryption
- Tunneled data authentication, encryption, and decryption

Easy VPN Remote supports three modes of operation:

- **Client**—Specifies that NAT or PAT be used so that end stations at the remote end of the VPN tunnel do not use IP addresses in the space of the destination server. The needed security associations (SA) are created automatically for IP addresses assigned to remote hosts.
- **Network Extension**—Specifies that remote-end hosts use IP addresses that are fully routable and reachable by the destination network over the tunnel connection so that they form a single logical network. In such cases, PAT is not used, to allow remote-end PCs direct access to destination network services and applications.
- **Network Extension Plus**—Identical to Network Extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec SAs for this IP address are automatically created.

Client mode is relatively simple and is used on a regular basis in countless deployments. Figure 16-1 shows an example of the Easy VPN Client concept.

Figure 16-1 *Easy VPN Remote Client Mode*



In the figure, the hosts at the teleworker's home are all addressed with RFC 1918 addresses, as are the destination resources at the corporate office site. RFC 1918 addresses are nonroutable addresses within the public Internet; however, NAT/PAT allow them to be translated and routed across. With the VPN connection running in Client mode, routing information can pass between the customer premises equipment (CPE) and the corporate office site.

Network Extension mode is very similar in concept to Client mode. So long as the addresses in the teleworker subnet are fully routable and unique within the corporate infrastructure, Figure 16-1 can also be said to be an example of Network Extension mode. If not, there will need to be a NAT/PAT operation performed at the VPN Server to pass traffic into the corporate network and back to the teleworker premises.

Easy VPN Server Requirements

To implement Easy VPN Remote capabilities, a number of prerequisite guidelines must be met. The Cisco Easy VPN Remote feature requires that the destination peer be a Cisco Easy VPN Server or VPN Concentrator that supports the Cisco Easy VPN Server feature. Essentially, the hardware and software feature sets must be those capable of performing the roles and functions of the Easy VPN solution. To that end, a minimum Cisco IOS version is required as follows:

- **Cisco 831, 836, 837, 851, 857, 871, 876, 877, and 878 Series Routers**—Cisco IOS Software Release 12.2(8)T or later (note that 800 series routers are not supported in Cisco IOS 12.3(7)XR but are supported in 12.3(7)XR2
- **Cisco 1700 Series Routers**—Cisco IOS Software Release 12.2(8)T or later
- **Cisco 2600 Series Routers**—Cisco IOS Software Release 12.2(8)T or later
- **Cisco 3600 Series Routers**—Cisco IOS Software Release 12.2(8)T or later
- **Cisco 7100 Series VPN Routers**—Cisco IOS Software Release 12.2(8)T or later
- **Cisco 7200 Series Routers**—Cisco IOS Software Release 12.2(8)T or later
- **Cisco 7500 Series Routers**—Cisco IOS Software Release 12.2(8)T or later
- **Cisco PIX 500 Series**—PIX OS Release 6.2 or later
- **Cisco VPN 3000 Series**—Software Release 3.11 or later

Additionally, requirements for Easy VPN Servers include the need for Internet Security Association and Key Management Protocol (ISAKMP) policies using Diffie-Hellman group 2 (1024-bit) IKE negotiation. This is necessary because the Cisco Unity protocol supports only ISAKMP policies using group 2 IKE. The Cisco Unity protocol refers to a methodology VPN clients use to determine the order of events when attempting a connection to a VPN server. The

Cisco Unity protocol operates based on the notion of a client group. A Unity client must identify and authenticate itself by group first and, if XAUTH enabled, by user later. The Easy VPN Server cannot be configured for ISAKMP group 1 or 5 when used with Easy VPN Clients.

To ensure secure tunnel connections, the Cisco Easy VPN Remote feature does not support transform sets providing encryption without authentication or those providing authentication without encryption. Both encryption and authentication must be represented.

The Cisco Unity protocol does not support Authentication Header (AH) authentication but it does support Encapsulation Security Payload (ESP).

Sometimes, a VPN connection might be used as a backup connection meant to be established and used when the primary link is unavailable. Various backup capabilities are available to meet such a need, including, but not limited to, dial backup. When using dial backup scenarios with Easy VPN, it should be understood that any backup method based on line status is not supported. This means that a primary interface in up/down state will not trigger the VPN connection establishment.

Also worthy of mention at this point is the fact that NAT interoperability is not supported in Client mode when split tunneling is enabled. This is because the client will be connected to both the central site and to the local LAN, with routing enabled to both networks per the split tunneling definition. Without split tunneling, the IP address assigned by the central site will become the address of the client interface. This avoids any possibility of address overlapping. When split tunneling is enabled, this cannot always be the case. When the connection is established and a route is injected into the central site network for remote site reachability, the route must be unique. Split tunneling allows the possibility for address overlap.

Easy VPN Connection Establishment

Easy VPN connectivity is relatively straightforward. The configuration and connection phases are subject to certain restrictions as listed in the previous section. The Cisco Easy VPN Remote feature supports a two-stage process for client/server authentication:

- Stage 1 is Group Level Authentication, which represents a portion of the channel creation process. During this stage, two types of authentication can be used, either preshared keys or digital certificates.
- Stage 2 of the authentication is known as Extended Authentication, or Xauth. The remote side of the connection submits a username and password to the central site VPN device. This is the same method that is used when a Cisco VPN Software Client is prompted for a username and password to activate a VPN tunnel. However, in this case, a user is not authenticated to the central site. Instead, the Easy VPN Remote Router, itself, is authenticated. Xauth, while

optional, is typically used in order to improve security. Once the Xauth is successfully completed and the VPN tunnel is created, all PCs behind the Easy VPN Remote Router can use the connection.

The following list represents a step-by-step method used to establish Easy VPN Remote Client connectivity with an Easy VPN Server gateway:

Step 1 The VPN Client initiates IKE phase 1.

Step 2 The VPN Client establishes an ISAKMP SA.

Step 3 The Easy VPN Server accepts the SA proposal.

Step 4 The Easy VPN Server initiates user authentication.

Step 5 Mode configuration begins.

Step 6 The Reverse Route Injection (RRI) process begins.

Step 7 IPsec quick mode completes the connection.

At each step, decisions are made and/or information is exchanged. The following sections describe further details about each step in the process.

IKE Phase 1

During the initial step of the connection attempt, the IKE phase 1 process is initiated. There are two separate manners in which authentication can be performed when initiating IKE phase 1:

- **Use of a preshared key for authentication**—The VPN Client initiates aggressive mode. Each peer is aware of the key of the other peer. Preshared keys are visible in the running-config of the router or VPN device on which they reside. With this in mind, an optional encrypted preshared key option is available. An accompanying group must be entered in the configuration of the VPN Client. This group name is used to identify the group profile associated with the VPN Client.

- **Use of a digital certificate for authentication**—The VPN Client initiates main mode. Digital certificates use Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN Remote devices. This support is provided by an RSA certificate stored in a central repository or on the remote device itself. With digital certificates, an organizational unit of a distinguished name is used to identify the group profile to be used. Cisco recommends a timeout of 40 seconds when using digital certificates with Easy VPN.

When using aggressive mode for connections, the identity of the Cisco IOS VPN device should be changed using the **crypto isakmp identity hostname** command. Changing the name will have no

effect on the certificate authentication via IKE main mode. The **crypto isakmp identity** command allows the use of an address or a hostname. To set an address, use the following:

```
BM2821(config)#crypto isakmp identity address
BM2821(config)#crypto isakmp key sharedkeystring address 192.168.1.33
```

This effectively sets the ISAKMP identity to the specified IP address. To change it to use a hostname instead, use the following:

```
BM2821(config)#crypto isakmp identity hostname
BM2821(config)#crypto isakmp key sharedkeystring hostname RemoteRouter.example.com
BM2821(config)#ip host RemoteRouter.example.com 192.168.1.33
```

The two configurations essentially have identical results.

Establishing an ISAKMP SA

When a VPN Client attempts to establish an SA between peers, it sends multiple ISAKMP proposals to the Easy VPN Server. As mentioned previously, Easy VPN supports only group 2 ISAKMP policy.

The VPN Client attempts to establish an SA between the peer IP addresses through the transmission of multiple ISAKMP proposals to the Easy VPN Server.

To reduce the amount of manual configuration of devices necessary to implement and support the Easy VPN solution, ISAKMP proposals include multiple combinations of encryption and hash algorithms, authentication methods, and Diffie-Hellman group sizes.

SA Proposal Acceptance

Several proposals can compose an ISAKMP policy. When multiple proposals exist, the Easy VPN Server will make a choice by first match. For this reason, the most secure policies should be first in the list to ensure the most secure connectivity.

As mentioned, the VPN Client sends multiple proposals to the Easy VPN Server. Once a proposal is accepted (that is, the ISAKMP SA is established), the device is considered to be authenticated and user authentication begins.

Easy VPN User Authentication

Now that the SA is accepted and the device is authenticated, a challenge is issued according to the configured methodology. If the Easy VPN Server is configured (as is typical) for Xauth, the VPN Client will wait for a username/password challenge.

Obviously, some input from the user is required at this point. The username and password are entered upon receipt of the prompt. This information is checked against some authentication entity, be it local authentication or some combination of TACACS, RADIUS, and/or hard/soft token service.

Authentication, authorization, and accounting (AAA) policies define which users can perform which functions on a managed device and keeps track of the changes made. Chapter 20, "Using AAA to Scale Access Control," covers AAA in more depth.

All Easy VPN Servers should be configured to manage VPN Clients and enforce user authentication

Mode Configuration

Once the Easy VPN Server indicates a successful authentication, the VPN Client requests any remaining configuration parameters that may have been configured in the VPN Server. Mode configuration begins and parameters such as IP address, DNS, split tunneling information, and other available configuration options are downloaded to the client. The only mandatory component to be downloaded to the client is the IP addressing information. Other mentioned parameters are optional.

Reverse Route Injection

Reverse Route Injection (RRI) is the process of injecting a static route into the Interior Gateway Protocol (IGP) routing table. This static route points to the client's destination network. This is useful when per-client static IP addressing is used with VPN Clients rather than per-VPN address pools.

RRI should be enabled on the dynamic crypto map when per-user IP addresses are used in environments where multiple VPN Servers are used. The redistribution of the RRI ensures reachability to the client host(s).

IPsec Quick Mode

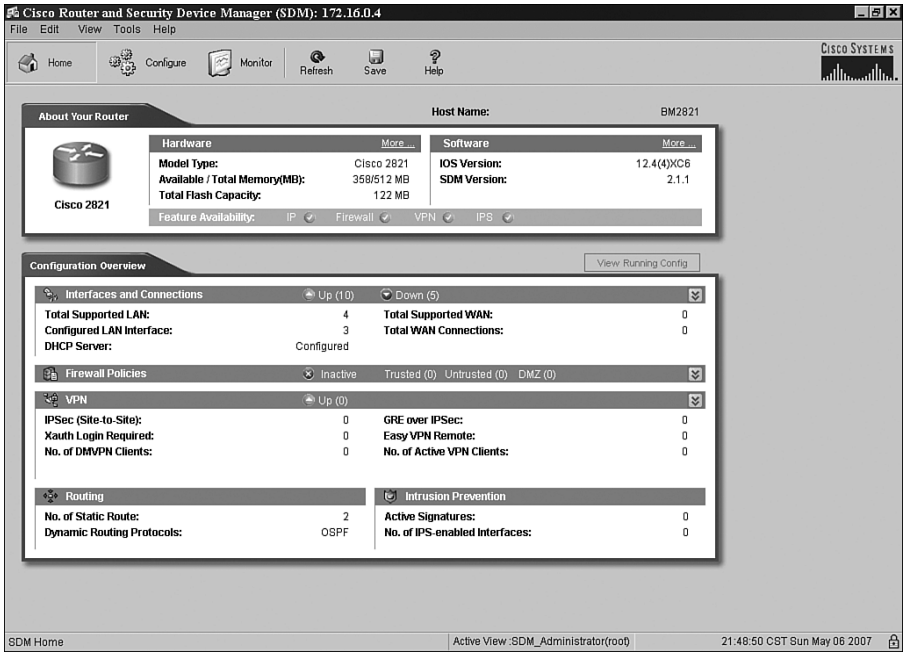
When all authentication is complete, the parameters provided from the VPN Server to the VPN Client, and the RRI is injected, IPsec quick mode is initiated to negotiate an IPsec SA establishment. This is the final step in the VPN connection establishment. Once the IPsec SA is created, the connection is complete and active.

Easy VPN Server Configuration

To configure the Easy VPN Server, some amount of information gathering is necessary. The information necessary includes the user's account information, any required enable secret passwords, AAA configuration (if not already done), and the configuration of the Easy VPN Server itself. The configuration can be done through the traditional command-line interface (CLI) or through the Security Device Manager (SDM) interface of the router itself.

SDM provides a graphical, web-based interface for configuring and monitoring an individual router. SDM also includes a number of wizards expressly for purposes of configuring common components of routing, firewall, intrusion detection/prevention, and VPN connectivity. One of the wizards associated with VPN connectivity is the Easy VPN Server Wizard. Figure 16-2 shows the home page of SDM running on a Cisco Integrated Services Router (ISR).

Figure 16-2 *Cisco SDM*



The SDM interface is quite straightforward and intuitive. The buttons across the top provide various options for configuration, monitoring, and saving configuration changes. By clicking the **Configure** button, the interface changes to the Configure page with the Tasks bar displayed down the left side of the screen. This is the primary configuration interface for the router. Figure 16-3 shows the Configure Tasks page.

By default, the SDM Configure page begins on the Interfaces and Connections page. This is where interface connectivity options and specific parameters are configured for each of the router's interfaces.

The third icon under the Tasks bar is VPN. Clicking this icon opens the page where the Easy VPN Server configuration is performed, as shown in Figure 16-4.

Figure 16-3 *SDM Configure Page*

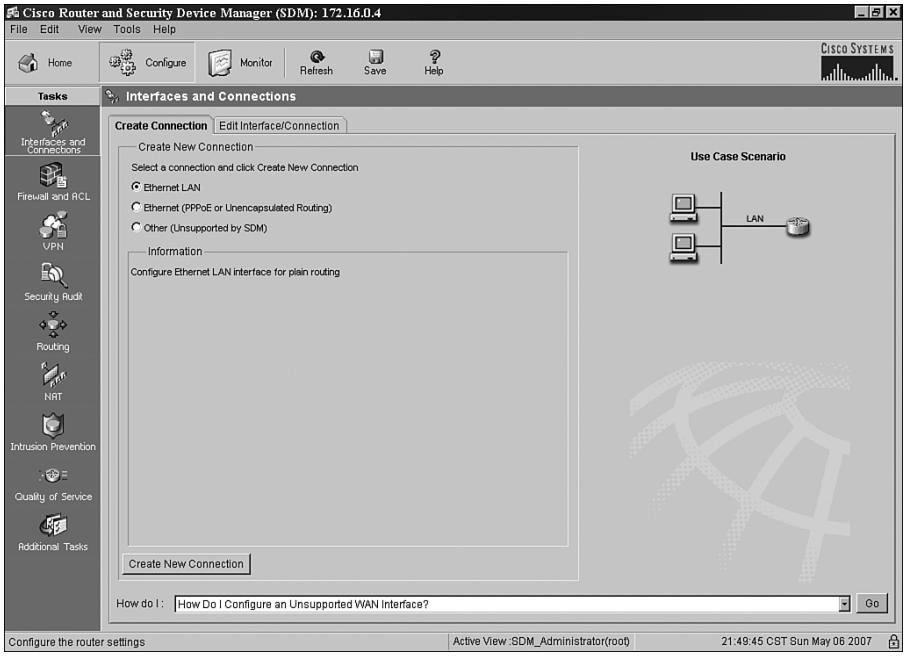
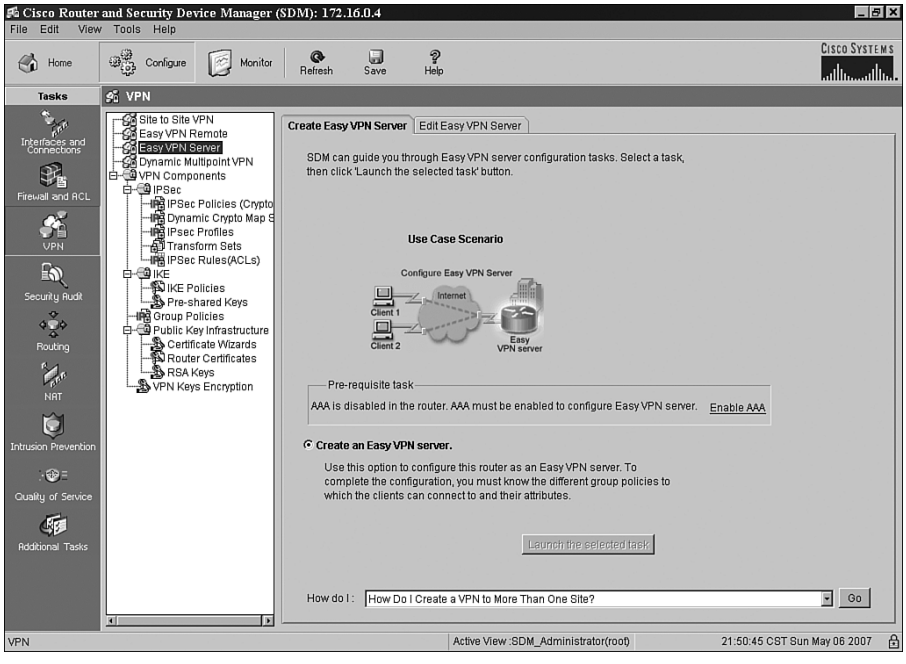


Figure 16-4 *SDM VPN Page*



Several options are available on the left side of the page. Out-of-the-box, an ISR can support Site-to-Site VPN, Easy VPN Remote, Easy VPN Server, and Dynamic Multipoint VPN (DMVPN) functionality. Obviously, the desired connection type for this discussion is Easy VPN Server. Clicking the Easy VPN Server selection opens the first page of the Easy VPN Server Wizard.

The Easy VPN Server Wizard includes a number of tasks in the configuration:

- Selection of the IPsec termination interface
- IKE policy configuration
- Group policy lookup methodology configuration
- User authentication
- Local group policy configuration
- IPsec transform set configuration

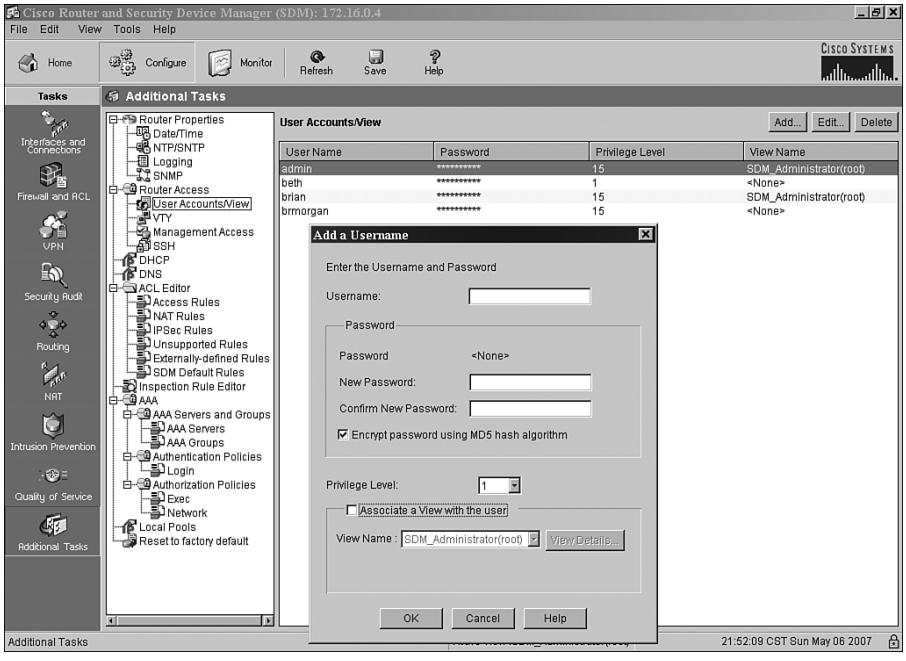
Any and all services to be used by Easy VPN Clients should be configured prior to the Easy VPN Server configuration. This includes all services to be used by AAA (RADIUS/TACACS+), IP addressing and routing for client subnets, certification authorities (CA) as needed, and additional services such as DNS and NTP settings (for proper PKI operation).

User Configuration

The configuration of users via the SDM interface is performed via the Additional Tasks button at the bottom of the Tasks bar on the Configure page. Figure 16-5 shows the User Accounts/View screen.

The figure shows the result of clicking **Additional Tasks > Router Access > User Accounts/View > Add**. The options available allow the administrator to add, edit, or delete users.

Figure 16-5 *SDM User Configuration*

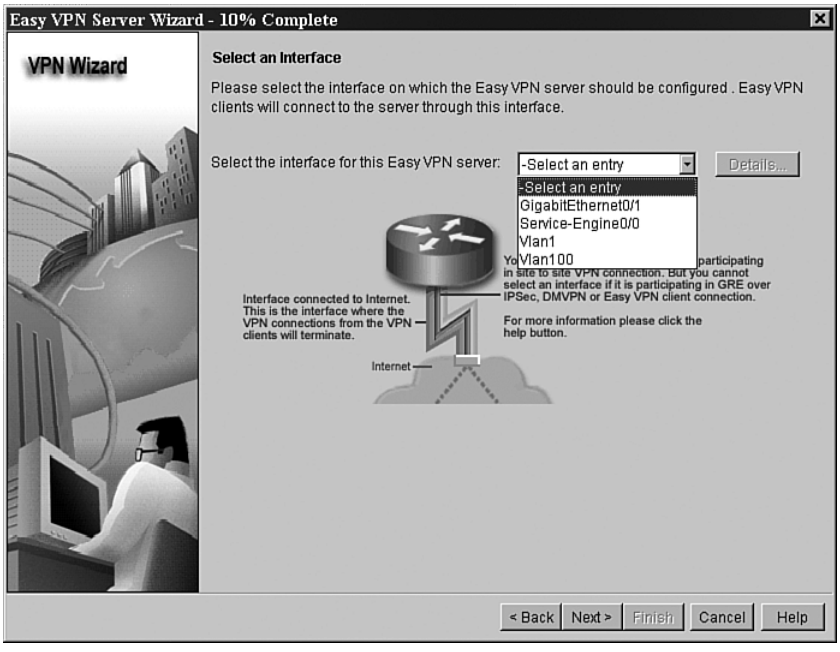


Easy VPN Server Wizard

Returning the discussion to the actual Easy VPN Server configuration, the Easy VPN Server Wizard is now ready to be run. AAA and necessary user information and privilege levels have been set. Click the **Launch the Selected Task** button on the Easy VPN Server screen to launch the wizard. The initial screen is a summary of tasks to be performed similar to that shown on the first page of the Easy VPN Server Wizard. If AAA has not already been configured, the wizard prompts you for the required AAA configuration information at this point. AAA must be enabled for Easy VPN Server to function properly. Additionally, at least one user must have privilege level 15 before enabling AAA on the device.

Click **Next** to open the Select an Interface screen, where you select the interface to be used with Easy VPN. This will be the interface through which all Easy VPN Clients connect. From the perspective of a NAT process, this is the outside interface. Figure 16-6 shows the Select an Interface screen of SDM.

Figure 16-6 *SDM Interface Selection*



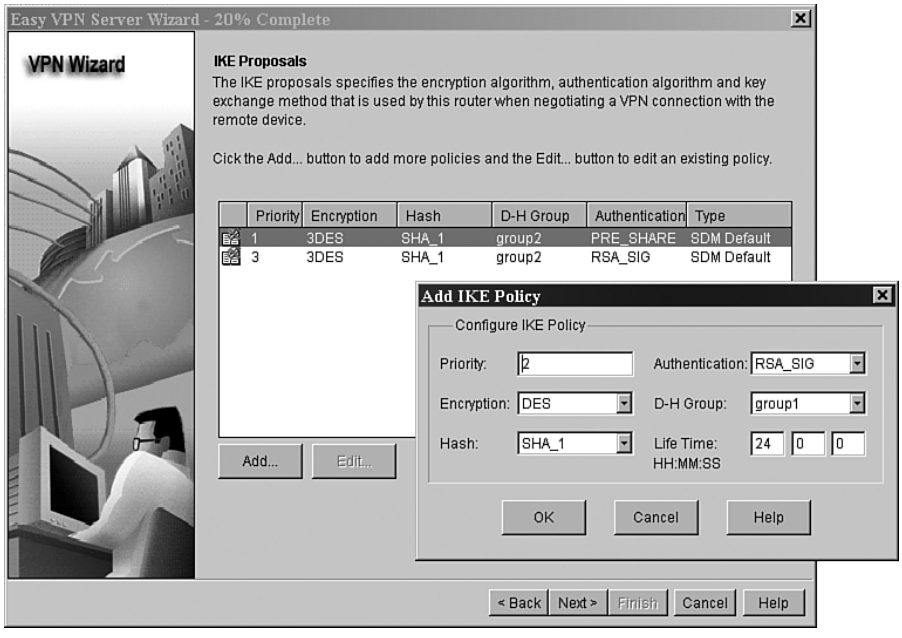
After you select the interface, click **Next** to move the wizard to the next step, where you can configure the needed IKE proposals.

You can use the default IKE proposals already configured by the wizard, or you can manually configure additional IKE proposals. Required parameters are as follows:

- IKE proposal priority
- Diffie-Hellman group (1, 2, or 5)
- Encryption algorithm (DES, 3DES, AES, or SEAL)
- HMAC (SHA-1 or MD5)
- IKE lifetime

Figure 16-7 shows the IKE Proposals page where a new proposal is being added to the list of available proposals.

Figure 16-7 *Easy VPN Server IKE Proposals*



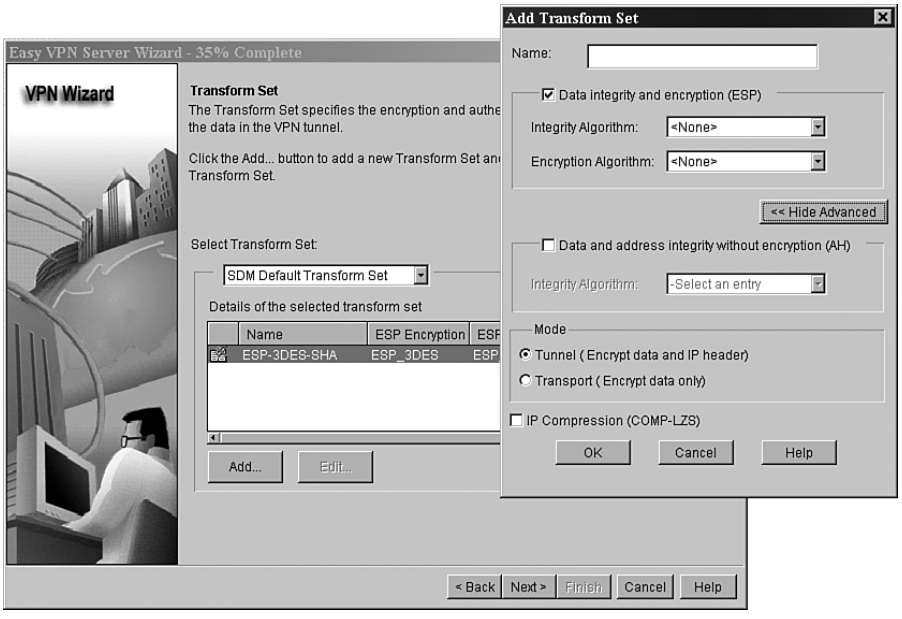
After you select all the appropriate options, click **Next** to move the wizard to the page where you can configure the transform sets.

As with IKE proposals, there is a default SDM transform set. The parameters for the transform set are as follows:

- Transform set name
- Encryption algorithm
- HMAC
- Compression (optional)
- Mode of operation (tunnel or transport)

Figure 16-8 shows the Transform Set page where a new transform set is being added to the list of available transform sets.

Figure 16-8 *Easy VPN Server Transform Sets*



With transform sets completed, the next step is group authorization/policy configuration. This is used for groups of VPN Clients who use the same authentication and configuration information. You can configure the policies on the local Easy VPN Server, an external Radius/TACACS+ server, or both. The AAA method lists will be used in defining the order in which policies are searched.

If you select local authentication, you must configure the user accounts in the Router Access portion of SDM. If you select RADIUS or TACACS+, you must configure the appropriate servers using the appropriate drop-down boxes. Once you select the option in the Method Selection box, the adjacent button becomes active and you can configure servers.

The second portion of the configuration is the method for user authentication (Xauth). Xauth is an enhancement of the existing IKE protocol. Xauth allows all Cisco IOS AAA authentication methods to perform user authentication in a separate phase after the IKE phase 1 exchange. With Xauth, IKE can provide user authentication using the device. This is possible only after the device has been successfully authenticated during normal IKE authentication. Any AAA method can be configured to accomplish this.

Figure 16-9 shows the User Authentication configuration page of the Easy VPN Server Wizard.