GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Implementing Site-to-Site VPNs using Cisco Secure PIX firewalls
Travis Lay
GSEC Practical Version 1.4b
June 01, 2003

Summary

In today's market companies need to protect and connect their remote networks to the corporate office by using a stable and secure solution. The Cisco Secure PIX firewall is a firewall that secures the Local Area Network from the Internet by using stateful inspection to filter traffic. Along with protecting your network the PIX firewall can also act as a VPN device that will connect your remote offices to the corporate office. There are a couple of different methods to establish a site-to-site VPN using the Cisco Pix firewalls. First you have the option of establishing the tunnel using manual ipsec, which requires you to configure matching security associations on both firewalls being used in the tunnel. Second you have the option of using the Cisco Easy VPN solution that requires you to setup a VPN server at the corporate office and a VPN hardware client at each remote site. The information in this document will help you configure a site-to-site VPN using the Easy VPN method. There are 2 methods to configure the Easy VPN, one is by using the Command Line Interface (CLI) and the second is by using the Cisco PIX Device Manager (PDM). The examples in this document will illustrate both methods.

Hardware and Software Requirements

To use the Easy VPN method for establishing your VPN tunnel you will have to meet the hardware and software requirements developed by Cisco. The easy VPN method was released in PIX firewall version 6.2, so if your current firewall doesn't have this version or higher you will need to download the newest version from Cisco's website and upgrade your PIX by using a tftp server.

Depending on the user needs at each site, you will decide which firewall to choose. There are many different Cisco PIX platforms that you can use for your Easy VPN server and Easy VPN client. Some of these are the PIX 501, 506/506e, 515/515e, 520, and 525. In the example below we have a remote site that has 4 users that need to have access to the corporate network. Since the remote site only has 4 users we can go with the PIX 501 firewall since, the Easy VPN client supports up to 10 users. Now for the corporate office we will need to supply a firewall that meets the needs of the users there and the connecting remote office. We will use the PIX 506e firewall as the Easy VPN server in the example below.

To check what Firewall version you are running on your firewall connect a console cable to the console port of the firewall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

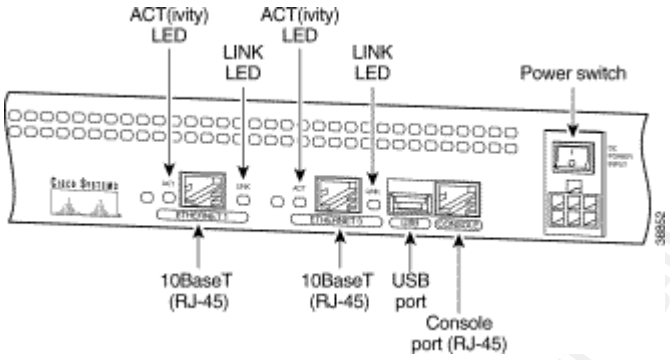


Figure 1 PIX 506 firewall example (9)

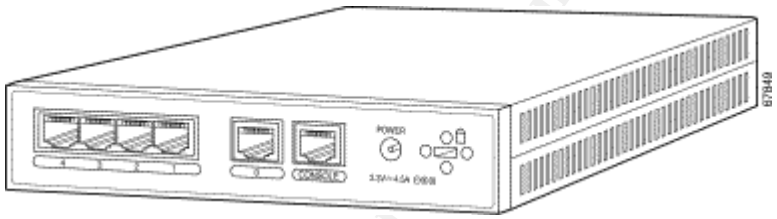


Figure 2 PIX 501 firewall example (8)

Once you are connected to the console port, use a terminal application like HyperTerminal to connect to the firewall. After you are connected to the firewall via the console cable enter the prompts below.

firewallname# show version

Cisco PIX Firewall Version 6.2(2)
Cisco PIX Device Manager Version 2.1(1)

Compiled on Fri 07-Jun-02 17:49 by morlee
firewallname up 35 days 23 hours

Hardware: PIX-506E, 32 MB RAM, CPU Pentium II 300 MHz
Flash E28F640J3 @ 0x300, 8MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

0: ethernet0: address is 000b.4693.2d0f, irq 10
1: ethernet1: address is 000b.4693.2d10, irq 11
Licensed Features:
Failover: Disabled
VPN-DES: Enabled

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

VPN-3DES: Enabled
Maximum Interfaces: 2
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Limited
IKE peers: Unlimited

Serial Number: 806413834 (0x3010e60a)
Running Activation Key: 0x66f5be8e 0x90aa3f99 0x0863d913 0x0d48512f
Configuration last modified by enable_15 at 08:14:24.094 UTC Tue May 6 2003

The show version command will show you what version of Firewall and what version of PIX Device Manager or "PDM" running. It will also show you the other options PIX firewall options you have available to you, such as, 3DES, user licenses and URL filtering.

If your firewall version is not 6.2 or higher you will need to upgrade before starting the configuration of the Easy VPN. You can download the newest firewall versions and PDM versions from Cisco website. If you currently do not have a tftp server they are many free ones on the internet that you can download, you will need to get one of these first and then upgrade your firewall. The following commands will allow you to upgrade to the latest version.

firewallname# ***copy tftp flash***

To upgrade to the newest PDM you will use the following command.

firewallname# ***copy tftp flash:pdm***

If you have any problems upgrading your firmware try these.

- Make sure your tftp server has been started
- Make sure you place the .bin files in the root directory of your tftp server
- Make sure you have a cross-over cable plugged in the firewall to your laptop and you can ping the firewall

Implementing the Site-to-Site VPN

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

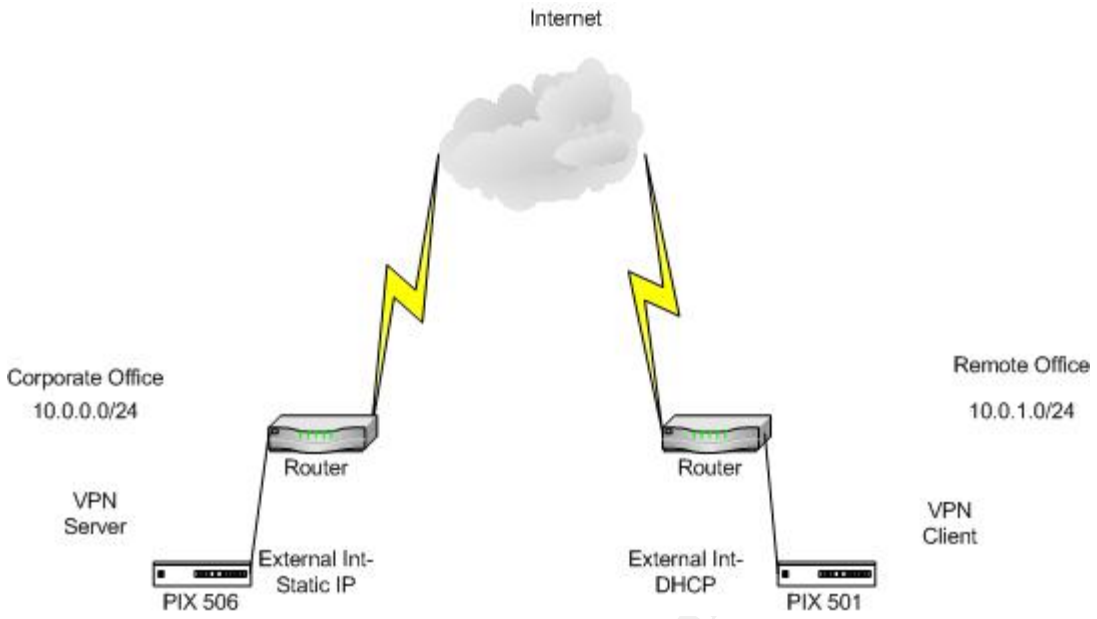


Figure 3 Site-to-Site VPN example

When setting up a site-to-site VPN we first need to configure IPSec. IPSec provides authentication and encryption services to protect unauthorized viewing or modification of data from your Local Area Network as it is transferred over Internet. IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity. These are bulk encryption algorithms, Diffie-Hellman key exchange, and Keyed hash algorithms. IPSec operates in two phases to allow the confidential exchange of a shared secret:

- Phase 1, which handles the negotiation of security parameters required to establish a secure channel between two IPSec peers. Phase 1 is generally implemented through the Internet Key Exchange (IKE) protocol. If the remote IPSec peer cannot perform IKE, you can use manual configuration with pre-shared keys to complete Phase 1.
- Phase 2, which uses the secure tunnel established in Phase 1 to exchange the security parameters required to actually transmit user data.

IKE is a protocol used by IPSec for completion of Phase 1. IKE negotiates and assigns Security Associations (SAs) for each IPSec peer, which provides a secure channel for the negotiation of the IPSec SAs in Phase 2. “A Security Association (SA) is a simplex “connection” that affords security services to the traffic carried by it.” (4)

IKE provides the following benefits:

- Eliminates the need to manually specify all the IPSec security parameters at both peers
- Lets you specify a lifetime for the IKE SAs

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Allows encryption keys to change during IPSec sessions
- Allows IPSec to provide anti-replay services
- Enables CA support for a manageable, scalable IPSec implementation
- Allows dynamic authentication of peers

You can select specific values for each IKE parameter per the IKE standard. You choose one value over another, based on the security level you desire and the type of IPSec peer to which you will connect. There are five parameters to define in each IKE policy, as outlined in Table 1.

Parameter	**Accepted Values**	**Keyword**	**Default Value**
Encryption algorithm	56-bit DES-CBC 168-bit DES	Des 3des	56-bit DES-CBC 168-bit DES
Hash algorithm	SHA-1 (HMAC variant	Sha	SHA-1
Authentication method	RSA signatures RSA encrypted nonces Pre-shared keys	Rsa-sig Rsa-encr Pre-share	RSA signatures
Diffie-Hellman group	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1 2	768 bit Diffie-Hellman
Security association's lifetime	Any number of seconds	--	86400 seconds (one-day)

Table 1: IKE Policy Parameters (3)

The parameter you choose here may affect the system performance of the firewall. An example of this is when you 3DES over DES, since 3DES is 3 times stronger that DES it takes the firewall's processor more time to encrypt and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

decrypt the data. So keep in mind the IKE parameters when you are designing your VPN. When the IKE negotiation begins, the peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer checks each of its policies in the order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime—from the remote peer's policy—will be used. If no acceptable match is found, IKE refuses negotiation and the tunnel will not be established. By using the Easy VPN solution the VPN client looks at the VPN server to define encryption, hash, authentication, and Diffie-Hellman parameter values. Once the client gets the parameters from the VPN server they then negotiate the tunnel.

Easy VPN works in 2 different modes:

- Client Mode- In this mode, VPN connections are initiated by traffic, so resources are used only on demand. This mode may be effective if you pay by the hour for your internet connection. This option applies NAT to all internal IP addresses.
- Network Extension Mode- In this mode, VPN connections are kept open even when not required in transmitting traffic. This option does not apply NAT to any inside IP addresses.

In the example below we will use Network Extension Mode.

Split-Tunneling is another option to consider when using the Easy VPN solution. Split-Tunneling is configured on the VPN server so that it will allow users behind the Easy VPN client to access items on the internet without going through the VPN tunnel. In the example below we will enable split-tunneling on the Easy VPN server so that the remote VPN client can access the internet without having to go through the corporate Network, which can cause excessive traffic on the corporate network. Although enabling split-tunneling has its advantages it also has its disadvantages. For an example say the remote user is on the corporate network through the VPN and also downloading files from the internet. The files that were downloaded from the remote user’s computer could be infected by a virus or Trojan, which could in turn spread to the corporate network or worse steal sensitive data.

Configuring the Easy VPN server using the Command Line Interface (CLI)

Basic configuration steps will need to be done before you start configuring the firewall as the VPN server.

The PIX Firewall provides three administrative access modes:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Unprivileged mode is available when you first access the PIX Firewall and displays the ">" prompt. This mode lets you view restricted settings.
- Privileged mode displays the "#" prompt and lets you change current settings. Any unprivileged command also works in privileged mode. Use the **enable** command to start privileged mode and the **disable**, **exit**, or **quit** commands to exit.
- Configuration mode displays the "(config)#" prompt and lets you change system configurations. All privileged, unprivileged, and configuration commands work in this mode. Use the **configure terminal** command to start configuration mode and the **exit** or **quit** commands to exit. (5)

Some important configurations steps to remember are:

- Always test your running configuration before you use the ***write memory*** command to save to flash.
- After you test the status of the firewall and VPN backup your firewall configurations to a tftp server.

You will need to be in configuration mode to enter the commands for the easy VPN below. If you run into any problems you can access the help menu by typing part of the command along with the question mark "?". Now lets get started configuring the Easy VPN.

1. This command permits the remote subnet access to the internal subnet at the corporate office.

firewallname# ***access-list easyvpn permit ip 10.0.0.0 255.255.0.0 10.0.1.0 255.255.0.0***

Replace 10.0.0.0 with the internal subnet at your corporate office and then 10.0.1.0 with the internet subnet of the VPN client.

2. This command permits access for the split tunnel.

firewallname# ***access-list splitt permit ip 10.0.0.0 255.255.0.0 10.0.1.0 255.255.0.0***

Replace 10.0.0.0 with the internal subnet at your corporate office and then 10.0.1.0 with the internet subnet of the VPN client.

3. This command enables NAT for the easy VPN.

firewallname# ***nat (inside) 0 access-list easyvpn***

Replace easyvpn with the name you specified in the previous commands.

4. The crypto map specifies the values to be used for the key management protocol.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

firewallname# ***sysopt connection permit-ipsec***
firewallname# ***crypto ipsec transform-set myset esp-des esp-md5-hmac***
firewallname# ***crypto dynamic-map outside_dyn_map 10 set transform-set myset***
firewallname# ***crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map***

Replace myset with the transform-set with you would like to use. Just make sure you keep the naming schemes the same in each command.

5. This command maps the IPSec policy to the outside interface. Without this the policy will not take affect.

firewallname# ***crypto map outside_map interface outside***

6. These commands enable phase 1 negotiation for the tunnel.

firewallname# ***isakmp enable outside***
firewallname# ***isakmp identity address***

7. You use this to enable a pre-shared key for the authentication method

firewallname# ***isakmp policy 10 authentication pre-share***

8. This defines the encryption method to DES, this can also be 3DES

firewallname# ***isakmp policy 10 encryption des***

Replace DES with the encryption method that you want.

9. This defines the hash algorithm to MD5, this can also be SHA.

firewallname# isakmp ***policy 10 hash md5***

Replace md5 with SHA if you choose to use it as your hash.

10. This defines which Diffie-Hellman group to use.

firewallname# ***isakmp policy 10 group 2***

Replace 2 with 1 if you choose to use Diffie-Hellman Group 1.

11. This defines the Security Association Lifetime to use.

firewallname# ***isakmp policy 10 lifetime 86400***

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Replace 86400 with the number of seconds you want the lifetime to be.

12. This defines the DNS server for the easy VPN client

firewallname# ***vpngroup easyvpn dns-server 10.0.0.44***

Replace 10.0.0.44 with the internal DNS server at the corporate office.

13. This defines the WINS server for the easy VPN client

Replace 10.0.0.44 with the internal WINS server at the corporate office.

firewallname# ***vpngroup easyvpn wins-server 10.0.0.44***

14. This defines the default domain for the easy vpn client

firewallname# ***vpngroup easyvpn default-domain baileynet.com***

Replace baileynet.com with your domain name.

15. This defines that you want to enable split-tunneling. If you do not want to enable split-tunneling leave this command out of the configuration.

firewallname# ***vpngroup easyvpn split-tunnel splitt***

16. This defines the Idle Timeout for the VPN tunnel. You can set this if you have bandwidth concerns and do not want to keep the tunnel up when no traffic is transmitting across it

firewallname# ***vpngroup easyvpn idle-time 1800***

17. This defines the easy VPN password for the tunnel; this is also the pre-shared key.

firewallname# ***vpngroup easyvpn password changeme***

Replace change me with the pre-shared key you choose.

18. This command saves the running configuration to flash memory.

firewallname# ***write memory***

Configuring Easy VPN client using the Command Line Interface (CLI)

Now that we have the VPN server configured, we will need to configure the remote firewall to be an Easy VPN client.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1. First you need to define the VPN group and password.

firewallname# ***vpnclient vpngroup easyvpn password changeme***

Replace easyvpn and changeme with your group name and shared key.

2. You then need to define the VPN server by typing in the Easy VPN server's address

firewallname# ***vpnclient server 10.0.0.1***

Replace 10.0.0.1 with the VPN server's IP address.

3. The next command will define what VPN client mode you want, network-extension-mode or client mode.

firewallname# ***vpnclient mode network-extension-mode***

Replace network-extension-mode with client-mode.

4. The next command enables the firewall as a VPN client.

firewallname# vpnclient enable

The following commands are optional but if you do add the extended authentication to your VPN tunnel you will need to add this line. I recommend that you do this just for a secondary security measure.

firewallname# ***vpnclient username test password test***

Replace test with the username and replace the password test with the password of the username you choose.

Testing connectivity through the tunnel

To test and make sure the tunnel is up and traffic is passing through the tunnel use the ping utility. First try to ping the remote router and then a remote workstation or server. If you get responses back you know the tunnel is allowing traffic through. You will still need to check and make sure traffic is being encrypted and that you are not getting any errors over the tunnel. Use the ***show ipsec sa*** command to show the encryption statistics.

Configuring the Easy VPN Server using the PIX Device Manager (PDM)

To configure the VPN server using the PDM, start your Internet Explorer and type in the location bar https://10.0.0.1 were 10.0.0.1 is the IP address of the firewall.

© SANS Institute 2003, Author retains full rights.

You will then see the following screen in figure 4 prompting to login to the firewall. Login to the firewall using a blank username and the enable password you setup earlier.

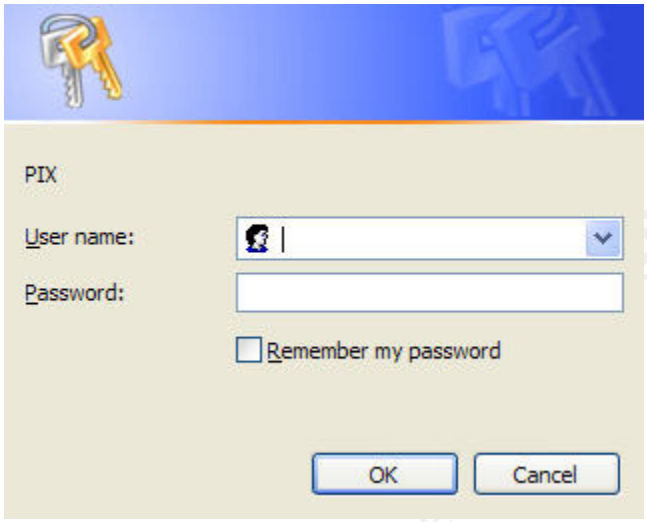


Figure 4 PIX Device Manager Authentication (PDM)

Now you are ready to configure the server.

1. Go to the VPN tab, and then highlight Remote Access.

2. Select Cisco VPN client and click add

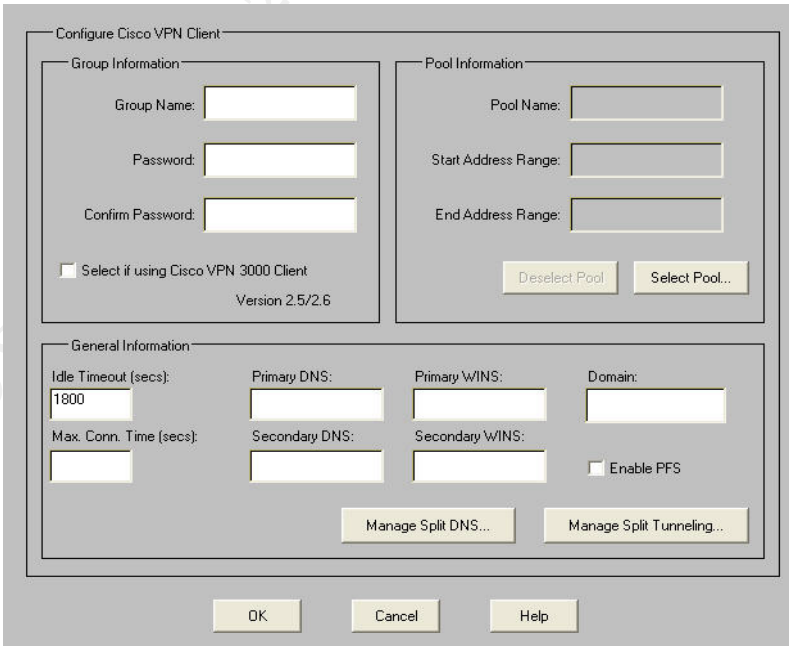


Figure 5 Adding the Remote Access Client

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. Type in the VPN group name of easyvpn.

Replace easyvpn with your actual VPN group name.

4. Type in the VPN password of changeme.

Replace the password with your group password. It is recommended that you use a strong password scheme when creating your password.

5. Next you will configure the Primary DNS and WINS servers.

Just add the internal IP addresses of the servers here. This will allow name resolution over the tunnel.

6. You can also add and manage the split-tunnel from this screen.

Now click ok and click apply. This will now save the configuration to the running-configuration on the firewall. Before we can configure the Easy VPN client you will need to add some access rules from the access lists tab to allow access to your network from the remote network subnet.

7. To add the inside-to-outside access rule you will need to click on the first icon on the menu bar that states to add a new rule. You will then select the action to permit, under the source network you will select inside, and type in your source network address. In our example it will be 10.0.0.0 and then follow that with the subnet of 255.255.255.0. Next under the destination subnet, you will select outside. This will be the remote VPN client network subnet, such as, in our example it is 10.0.1.0 with the mask of 255.255.255.0. The last step in adding your inside-to-outside access rule is to define what protocols the corporate network should allow out from within the Local Area Network. For our example we will select IP and then, ANY- ANY for the source and destination ports.

8. Now you will need to add an outside-to-inside access rule that allows the remote VPN client to access the corporate network. First click on add new rule, and select permit. Under Source host/network we will select outside and type in the Remote VPN network subnet and subnet mask, under Destination network, select inside and use the corporate network subnet and mask. Then finish up by allowing which protocols to allow into the network. We will use ANY, ANY again in our example. Click ok and then apply.

9. The last step is to save the running-configuration to flash by going to file and save running configuration to flash.

The easy VPN server is now configured on the PIX 506 firewall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Configuring the Easy VPN Client using the PIX Device Manager (PDM)

To configure the Easy VPN client we will launch the PDM using Internet Explorer and continue to login. Before we start you should already have an internet connection going through your firewall for internet connectivity to the Internal Network. If this is a brand new firewall install you might need to enable Port Address Translation (PAT) for internet access. For information on this please refer to the Cisco PIX Documentation. Now lets configure the VPN client to connect back to the VPN server.

1. Select the VPN tab within the PDM and then highlight the Easy VPN remote at the bottom left.

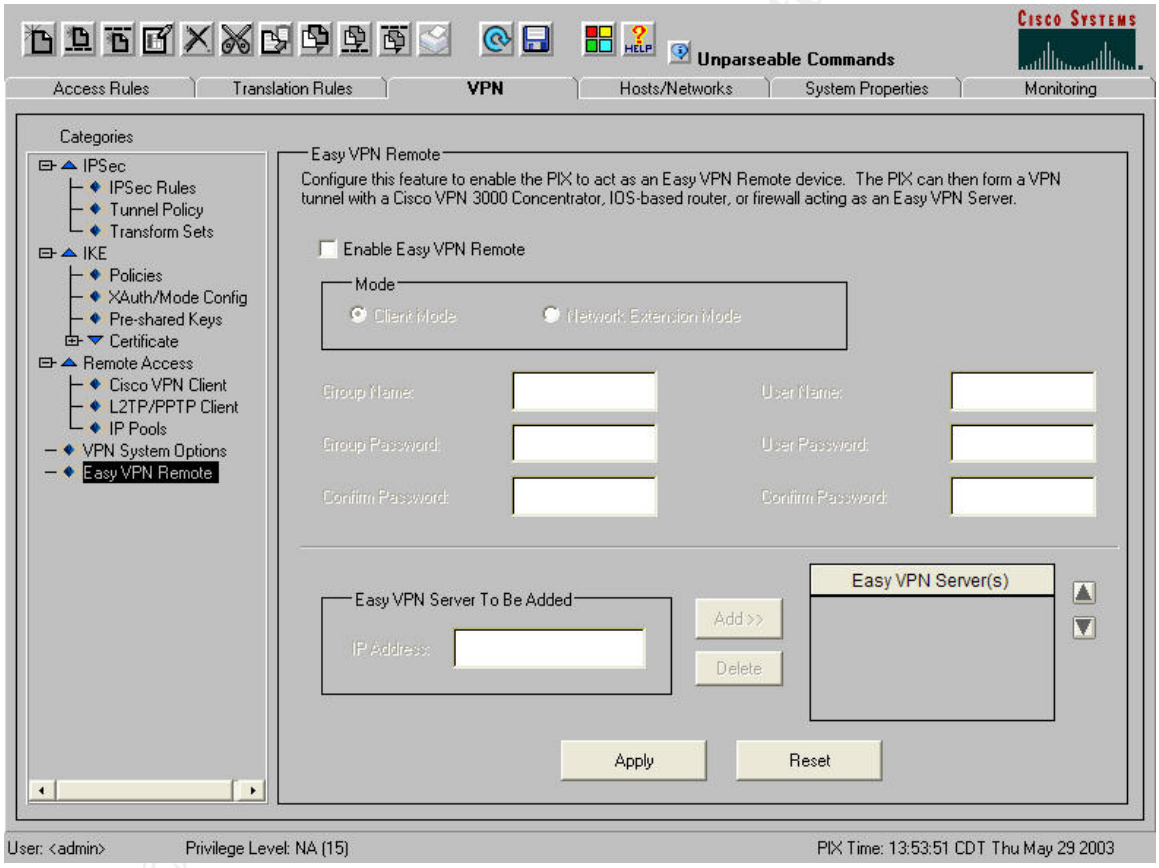


Figure 6 Easy VPN

2. Click on Enable Easy VPN Remote

3. Next you will decide to use network extension mode or client mode. We will use network Extension mode in our example.

4. Now you will type in the Group Name and then the Group password.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. If you have radius enable on the Easy VPN server for Authentication you will need to type in a username and password the fields on the left.

6. Next type in the VPN server to be added to the list and click add. You can also add multiple VPN servers for fault tolerance purposes.

7. Next you will click apply to save it to the running-configuration.

8. Now we need to add the inbound and outbound access rules the same way as we added them to the VPN server. Just this time the inside network will be 10.0.1.0 or the remote office and the outside network will be 10.0.0.0 or the corporate office.

9. After you get the access rules added, go to file, and save the configuration to flash.

The easy VPN client is now ready to use. If setup correctly you will now be able to ping and transmit data across the tunnel.

Troubleshooting the Site-to-Site VPN tunnel

If you were unsuccessful in testing your VPN tunnel try using the PIX commands below.

This command will show the current status of the Easy VPN remote client.

firewall# ***show vpnclient***

To see all available VPN connections in use you can use the command below. If you see the active tunnel here but are not able to ping anything then there may be a problem with an access rule on the remote sight.

firewall# ***show isakmp sa***

To view the statistics of encryption and decryption use this command.

firewall# ***show ipsec sa***

Security aspects to consider

By enabling split-tunneling you could be allowing security threats into your corporate network depending on the security policy you have in place.

© SANS Institute 2003, Author retains full rights.

Some things to have in your corporate security policy to protect from split-tunneling are:

- Place business pc's at home for business use only; this might control what people access from home.
- Require anti-virus to be installed and updated on the remote PC.
- Require some sort of host based firewall to be installed. (6)

Consider using an Intrusion Detection System "IDS" to monitor traffic flow transmitting through your network.

Conclusion

This paper provides detailed configuration steps on setting up a site-to-site VPN using the Cisco Easy VPN solution. You now should have enough information to configure the tunnel using the Command Line Interface or by using the PIX Device Manager. This paper also gives you information on how the VPN establishes the tunnel and what type of encryption standards to choose from. If you have any further questions you can go to the Cisco Web Site for documentation and configuration examples on setting up a site-to-site VPN using the PIX firewall.

Bibliography

[1]. Cisco- Deploying IPSec Virtual Private Networks
http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns142/networking_solutions_white_paper09186a0080117919.shtml

[2]. Cisco- Cisco Easy VPN solution
http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns27/networking_solutions_package.html

[3]. Ives, Millie- Implementing Site-to-Site VPNS using Cisco Routers
http://www.giac.org/practical/gsec/Millie_Ives_GSEC.pdf

[4]. Kent & Atkinson- "Security Architecture for the Internet Protocol" RFC 2401
http://www.ietf.com/rfc/rfc2401.txt

[5]. Cisco- Basic Firewall configuration
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b0.html#18406

[6]. Stines, Michael- Remote Access VPN "Security Concerns and Policy Enforcement"
http://www.sans.org/rr/paper.php?id=881

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[7]. InformIT- Configuring PIX Firewall IPSec Support
http://www.informit.com/content/index.asp?session_id={B06B8A70-3054-42EA-BA01-9C27CCEA59C0}&product_id={C3973763-6B7D-495F-95EB-E2DB6279D332}

[8]. Cisco- PIX 501
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_installation_guide_chapter09186a00800dff13.html

[9]. Cisco- Installing a PIX firewall
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_installation_guide_chapter09186a0080089883.html

[10]. Cisco- IPSEC
http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm

[11]. Cisco- Firewall Software Version 6.2
http://www.cisco.com/en/US/products/sw/secursw/ps2120/ps3917/index.html

[12]. Holcomb, Jason- “Using the Cisco PIX Device Manager”
http://www.sans.org/rr/papers/21/889.pdf

© SANS Institute 2003, Author retains full rights.