



Using PIX Firewall in SOHO Networks

This chapter describes features provided by the PIX Firewall that are used in the small office, home office (SOHO) environment. It includes the following sections:

- [Using PIX Firewall as an Easy VPN Remote Device, page 4-1](#)
- [Using the PIX Firewall PPPoE Client, page 4-12](#)
- [Using the PIX Firewall DHCP Server, page 4-16](#)
- [Using DHCP Relay, page 4-21](#)
- [Using the PIX Firewall DHCP Client, page 4-22](#)

Using PIX Firewall as an Easy VPN Remote Device

This section describes the commands and procedures required to configure the PIX Firewall as an Easy VPN Remote device. It includes the following topics:

- [Overview, page 4-2](#)
- [Establishing Network Connectivity, page 4-4](#)
- [Basic Configuration Procedure, page 4-4](#)
- [Viewing Downloaded Configuration, page 4-5](#)
- [Controlling Remote Administration, page 4-6](#)
- [Using Secure Unit Authentication, page 4-6](#)
- [Using Individual User Authentication, page 4-9](#)
- [Using X.509 Certificates, page 4-10](#)
- [Verifying the DN of an Easy VPN Server, page 4-11](#)

For information about configuring the PIX Firewall as an Easy VPN Server, refer to [Chapter 8](#), “Managing VPN Remote Access.”



Note

PIX Firewall Version 6.3 allows a management connection to the inside interface of a PIX Firewall over a VPN tunnel. This feature is designed for remote management of a PIX Firewall used as an Easy VPN Remote device, which typically has an IP address dynamically assigned to its outside interface. For further information, refer to the [“Connecting to PIX Firewall Over a VPN Tunnel”](#) section on page 9-1.

Overview

When used with PIX Firewall Versions 6.2 and higher, you can use a PIX Firewall 501 or PIX 506/506E as an Easy VPN Remote device when connecting to an Easy VPN Server, such as a Cisco VPN 3000 Concentrator or another PIX Firewall.

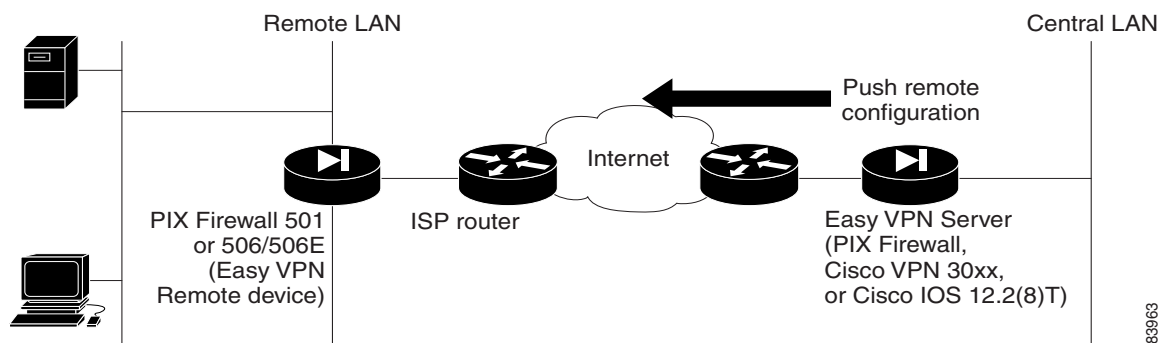


Note

PIX Firewall 506/506E platforms, when used as Easy VPN remote devices, do not support the use of logical VLAN interfaces for sending traffic across a VPN tunnel. Only the actual eth0 and eth1 physical interfaces on the PIX Firewall 506/506E are supported when used as an Easy VPN remote device.

Figure 4-1 illustrates how Easy VPN Remote devices can be used in a Virtual Private Network (VPN).

Figure 4-1 Using the PIX Firewall as an Easy VPN Remote Device



Easy VPN Remote device functionality, sometimes called a “hardware client,” allows the PIX Firewall to establish a VPN tunnel to the Easy VPN Server. Hosts running on the LAN behind the PIX Firewall can connect through the Easy VPN Server without individually running any VPN client software.

PIX Firewall Version 6.3 or higher used as an Easy VPN Remote device can make use of load balancing and redundancy features among two or more Easy VPN Servers. To implement redundancy, a list of backup servers is configured on an Easy VPN Server and is downloaded to your Easy VPN Remote device. The Easy VPN Remote device automatically redirects its connection request to the next backup server on its list if it does not receive a response after five seconds.

Load balancing requires the use of Cisco 3000 Series VPN Concentrators for the Easy VPN Servers. With load balancing, you configure a virtual IP address for the destination of your Easy VPN Remote device connection. Easy VPN Servers that share a virtual IP address form a load balancing cluster, with one of the members acting as the master server. The master server receives request, calculates the optimal server, and directs the connection request to that server.

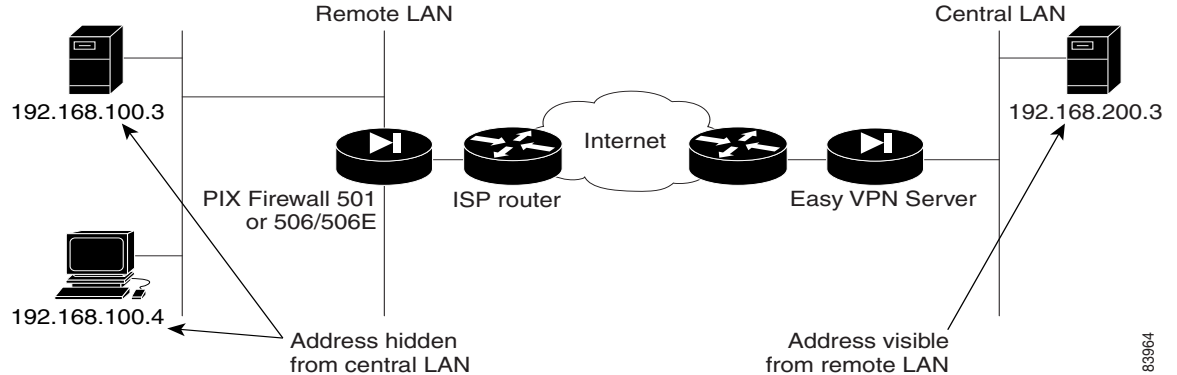
Two different modes of operation are supported when using the PIX Firewall as an Easy VPN Remote device:

- Client mode
- Network extension mode

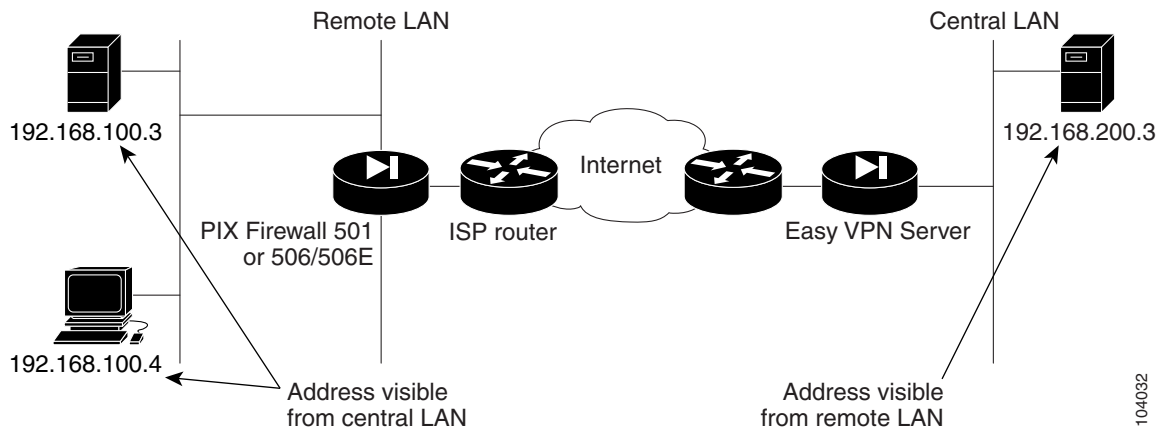


Note

If Cisco IP Phones are connected over the VPN tunnel and Session Initiation Protocol (SIP) proxy is used on the network protected by the Easy VPN Server, you must use network extension mode.

Figure 4-2 Using the PIX Firewall in Client Mode

As shown in [Figure 4-2](#), client mode causes VPN connections to be initiated by traffic, so resources are only used on demand. In client mode, the PIX Firewall applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the PIX Firewall. To use this mode, you must also enable the DHCP server on the inside interface, as described in “[Using the PIX Firewall DHCP Server.](#)”

Figure 4-3 Using the PIX Firewall in Network Extension Mode

[Figure 4-3](#) illustrates network extension mode. In this mode, VPN connections are kept open even when not required for transmitting traffic. This option does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the PIX Firewall.

In network extension mode, the IP addresses of clients on the inside interface are received without change at the Easy VPN Server. If these addresses are registered with the Network Information Center (NIC), they may be forwarded to the public Internet without further processing. Otherwise, they may be translated by the Easy VPN Server or forwarded to a private network without translation.

Establishing Network Connectivity

Before you can connect the PIX Firewall Easy VPN Remote device to the Easy VPN Server, you must establish network connectivity between both devices through your Internet service provider (ISP). After connecting your PIX Firewall to the DSL or Cable modem, you should follow the instructions provided by your ISP to complete the network connection. Basically, there are three methods of obtaining an IP address when establishing connectivity to your ISP:

- PPPoE client—Refer to [“Using the PIX Firewall PPPoE Client”](#) section on page 4-12.
- DHCP client—Refer to [“Using the PIX Firewall DHCP Client”](#) section on page 4-22.
- Static IP address configuration—Refer to the [“Assigning an IP Address and Subnet Mask”](#) section on page 2-5, in Chapter 2, [“Establishing Connectivity.”](#)

Basic Configuration Procedure

The Easy VPN Server controls the policy enforced on the PIX Firewall Easy VPN Remote device. However, to establish the initial connection to the Easy VPN Server, you must complete some configuration locally.

You can perform this configuration by using Cisco PIX Device Manager (PDM) or by using the command-line interface as described in the following steps:

Step 1 If you are using pre-shared keys, enter the following command:

```
vpnclient vpngroup {groupname} password {preshared_key}
```



Note This command is not required if you are using X.509 certificates.

Replace *groupname* with an alphanumeric identifier for the VPN group. Replace *preshared_key* with the encryption key to use for securing communications to the Easy VPN Server.

Step 2 (Optional) If the Easy VPN Server uses extended authentication (Xauth) to authenticate the PIX Firewall client, enter the following command:

```
vpnclient username {xauth_username} password {xauth_password}
```

Replace *xauth_username* with the username assigned for Xauth. Replace *xauth_password* with the password assigned for Xauth.



Note If the Easy VPN Server is configured for prompting for Xauth on rekey, the prompt is not displayed on the PIX Firewall acting as the Easy VPN remote device, and the connection is terminated.

Step 3 Identify the remote Easy VPN Server by entering the following command:

```
vpnclient server {ip_primary} [ip_secondary_n]
```

Replace *ip_primary* with the IP address of the primary Easy VPN Server. Replace *ip_secondary_n* with the IP address of one or more Easy VPN Servers. A maximum of eleven Easy VPN Servers are supported (one primary and up to ten secondary).

Step 4 Set the Easy VPN Remote device mode by entering the following command:

```
vpnclient mode {client-mode | network-extension-mode}
```

- Client mode applies NAT to all IP addresses of clients connected to the inside (higher security) interface of the PIX Firewall.
- Network extension mode—This option does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the PIX Firewall.

Step 5 Enable the Easy VPN Remote device by entering the following command:

```
vpnclient enable
```

Step 6 (Optional) To display the current status and configuration of Easy VPN Remote device, enter the following command:

```
show vpnclient
```

Viewing Downloaded Configuration

There are two different flash memory areas for saving configuration information. The downloaded configuration is stored in a separate area that is only visible when using the **show vpn detail** command. To view all the configuration (static, dynamic, flash-private storage area FPSA-related) associated with the Easy VPN Remote device, enter the following command:

```
remotepix(config)#show vpnclient detail
```

The output from this command after the Easy VPN Remote device is connected to the Easy VPN Server includes the following (this output has been abridged and annotated for clarity):

```
LOCAL CONFIGURATION
vpnclient server 80.0.0.1
vpnclient mode client-mode
vpnclient vpngroup unity password *****
vpnclient username maruthitacacs password *****
vpnclient management tunnel 10.0.0.0 255.255.255.0
vpnclient enable

DOWNLOADED DYNAMIC POLICY
Current Server                : 80.0.0.1
NAT addr                      : 90.0.0.10
Primary DNS                   : 10.0.0.21
Default Domain                : example.com
PFS Enabled                   : Yes
Secure Unit Authentication Enabled : No
User Authentication Enabled   : Yes
User Authentication Server    : 10.0.0.3
User Authentication Server Port : 1645
User Authentication Idle Timeout : 2:46:40
Device Pass Through Enabled  : Yes
Split Networks                : 10.0.0.0/255.255.255.0 110.0.0.0/255.255.255.0
Split DNS                     : example.com
Backup Servers                : None

STORED POLICY
Secure Unit Authentication Enabled : No
Split Networks                : 10.0.0.0/255.255.255.0 110.0.0.0/255.255.255.0
Backup Servers                : 80.0.0.30
```

```

RELATED CONFIGURATION
sysopt connection permit-ipsec
global (outside) 10 interface
global (outside) 65001 90.0.0.10
nat (inside) 10 60.0.0.0 255.255.255.0 0 0
access-list _vpnc_pat_acl permit ip any 10.0.0.0 255.255.255.0
access-list _vpnc_pat_acl permit ip any 110.0.0.0 255.255.255.0
access-list _vpnc_acl permit ip host 90.0.0.10 10.0.0.0 255.255.255.0
access-list _vpnc_acl permit ip host 90.0.0.10 110.0.0.0 255.255.255.0
access-list _vpnc_acl permit ip host 80.0.0.2 10.0.0.0 255.255.255.0
access-list _vpnc_acl permit ip host 80.0.0.2 host 10.0.0.3
access-list _vpnc_iaa_acl permit ip any 10.0.0.0 255.255.255.0
access-list _vpnc_iaa_acl permit ip any 110.0.0.0 255.255.255.0
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius

```

Controlling Remote Administration

PIX Firewall Version 6.3 introduces a feature that improves administrative security by letting you identify the networks from which your PIX Firewall can be remotely managed or by preventing remote management altogether.

If you do not enable this feature, any host that has access to the outside interface of your PIX Firewall through a VPN tunnel can manage it remotely.

To enable this feature, enter the following command:

```
vpnclient management tunnel ip_addr_1 ip_mask_1 [[ip_addr_2 ip_mask_2] ... ]]
```

Replace *ip_addr_1* and *ip_mask_1* with the IP address and subnet mask of the remote host you would like to allow to remotely manage your PIX Firewall. Use additional IP addresses and subnet masks to enable remote management from more than one host.

To completely prevent remote management using the outside interface of your PIX Firewall, enter the following command:

```
vpnclient management clear
```

After entering this command, no remote management connection is allowed over a VPN tunnel to the outside interface of the PIX Firewall. By default, the PIX Firewall can only be remotely managed by connecting to its outside interface over a secure VPN tunnel. To enable a remote management connection to the inside interface of your PIX Firewall, refer to the [“Connecting to PIX Firewall Over a VPN Tunnel”](#) section on page 9-1 in Chapter 9, [“Accessing and Monitoring PIX Firewall.”](#)

Using Secure Unit Authentication

This section describes how Secure Unit Authentication (SUA) affects the behavior of a PIX Firewall used as an Easy VPN Remote device, and how you can manage this behavior. It includes the following topics:

- [Overview, page 4-7](#)
- [Establishing a Connection with SUA Enabled, page 4-8](#)
- [Managing Connection Behavior with SUA, page 4-8](#)

Overview

Secure unit authentication (SUA) is a feature introduced with PIX Firewall Version 6.3 to improve security when using a PIX Firewall as an Easy VPN Remote device. With SUA, one-time passwords, two-factor authentication, and similar authentication schemes can be used to authenticate the remote PIX Firewall before establishing a VPN tunnel to an Easy VPN Server.

Secure Unit Authentication (SUA) is configured as part of the VPN policy on the Easy VPN Server and cannot be configured directly on the Easy VPN Remote device. After connecting to the Easy VPN Server, the Easy VPN Remote device downloads the VPN policy, which then enables or disables SUA.

When SUA is disabled and the PIX Firewall is in network extension mode, a connection is automatically initiated. When SUA is disabled with client mode, the connection is automatically initiated whenever any traffic is sent through the PIX Firewall to a network protected by the Easy VPN Server.

When SUA is enabled, static credentials included in the local configuration of the Easy VPN Remote device are ignored. A connection request is initiated as soon as an HTTP request is sent from the remote network to the network protected by the Easy VPN Server. All other traffic to the network protected by the Easy VPN Server is dropped until a VPN tunnel is established. You can also initiate a connection request from the CLI of the Easy VPN Remote device.

Establishing a Connection with SUA Enabled

After SUA is enabled and before a VPN tunnel is established, any HTTP request to the network protected by the Easy VPN Server is redirected to the URL as follows:

```
https://inside-ipaddr/vpnclient/connstatus.html
```

Where *inside-ipaddr* is replaced by the IP address of the inside interface of the PIX Firewall used as the Easy VPN Remote device. You can activate the connection by manually entering this URL in the Address or Location box of a browser, and you can use this URL to check the status of the VPN tunnel.

This URL provides a page containing a Connect link that displays an authentication page. If authentication is successful, the VPN tunnel is established. After the VPN tunnel is established, other users on the network protected by the Easy VPN Remote device can access the network protected by the Easy VPN Server without further authentication. If you want to control access by individual users, you can implement Individual User Authentication, as described in the [“Using Individual User Authentication” section on page 4-9](#).

You can manually initiate a connection from the CLI of the PIX Firewall used as an Easy VPN Remote device, by entering the following command:

```
vpnclient connect
```

To close a connection using the CLI, enter the following command:

```
vpnclient disconnect
```

This causes the Easy VPN Remote device to disconnect from the Easy VPN Server and to tear down the IKE tunnel. You can use the **vpnclient connect** and **vpnclient disconnect** commands to force an update of the downloaded policy by disconnecting and reconnecting to the Easy VPN Server.

Managing Connection Behavior with SUA

After the VPN policy is downloaded, the PIX Firewall used as an Easy VPN Remote device stores the downloaded policy, including the status of SUA, in a private area of the FLASH memory. This lets the Easy VPN Remote device determine its connection behavior for the next connection attempt. After downloading a VPN policy that changes its SUA status, the PIX Firewall automatically disconnects from the Easy VPN Server. This allows the Easy VPN Remote device to immediately implement the change in its SUA status.

**Note**

After enabling SUA, your local PIX Firewall will not require static credentials because credentials are entered manually each time a connection is made. However, if SUA is disabled for any reason at the Easy VPN Server, you will need static credentials to make a VPN connection. For this reason, if you have static credentials in your local configuration, do not remove them unless you have a good reason to do so.

The following CLI clears the stored policy, as well as the currently running SUA configuration.

```
clear vpnclient
```

After entering this command (or before connecting a PIX Firewall to an Easy VPN Server for the first time) the PIX Firewall is in “SUA_Unspecified” state. In this state, SUA is enabled if static authentication credentials are not included in the configuration of the local PIX Firewall. Otherwise, if static authentication credentials are *included*, SUA is disabled.

As mentioned earlier, the connection behavior of the PIX Firewall used as an Easy VPN Remote device varies depending on whether it is in client mode or network extension mode. It also varies depending on whether the local configuration contains static credentials (configured using the command **vpnclient username user password pass**), and depending on its SUA state. This behavior is summarized in [Table 4-1](#).

Table 4-1 PIX Firewall Behavior in Different SUA States

PIX Firewall State	Client Mode	Network Extension Mode
SUA_Unspecified and the local configuration contains static credentials.	Traffic from or through the PIX Firewall initiates the VPN tunnel.	The VPN tunnel is initiated automatically.
SUA_Unspecified and the local configuration does <i>not</i> contain static credentials.	Manual connection is required.	Manual connection is required.
SUA_Disabled. Static credentials are required.	Traffic from or through the PIX Firewall initiates the VPN tunnel.	The VPN tunnel is initiated automatically and is maintained in an open state.
SUA_Enabled. Static credentials are not required.	Manual connection is required.	Manual connection is required.

Using Individual User Authentication

Individual User Authentication (IUA) causes clients on the inside network of the Easy VPN Remote to be individually authenticated based on the IP address of the inside client. IUA supports authentication with both static and dynamic password mechanisms.

IUA is enabled by means of the downloaded VPN policy and it cannot be configured locally. For information about enabling IUA on a PIX Firewall used as an Easy VPN Server, refer to the [“Configuring Individual User Authentication” section on page 8-4](#).

When IUA is enabled, each user on the network protected by the Easy VPN Remote device is prompted for a user name and password when trying to initiate a connection. A PIX Firewall acting as an Easy VPN Server downloads the contact information for the AAA server to the Easy VPN Remote device, which sends each authentication request directly to the AAA server. A Cisco 3000 Series VPN Concentrator used as an Easy VPN Server performs proxy authentication to the AAA server. The Easy VPN Remote device sends each authentication request to the Cisco 3000 Series VPN Concentrator.

PIX Firewall Version 6.3 or higher lets you use Media Access Control (MAC) addresses to bypass authentication for devices, such as Cisco IP Phones, that do not support this type of authentication. When MAC-based AAA exemption is enabled, the PIX Firewall bypasses the AAA server for traffic that matches both the MAC address of the device and the IP address that has been dynamically assigned by a DHCP server.

This feature, like IUA, is enabled or disabled on the Easy VPN Server. For information about enabling this feature on a PIX Firewall used as an Easy VPN Server, refer to the [“Bypassing AAA Authentication” section on page 8-5](#).

To configure this feature on a PIX Firewall used as an Easy VPN Remote device, refer to the [“Using MAC-Based AAA Exemption” section on page 3-13](#) in Chapter 3, “Controlling Network Access and Use.”

Using X.509 Certificates

PIX Firewall Version 6.3 allows the use of IPsec Main Mode by providing RSA-SIG support for X.509 certificates.



Note

To establish a VPN tunnel using certificates, an Easy VPN Server using Cisco IOS software needs to be running IOS version 122-13.T1 or later. Earlier versions of Cisco IOS software do not support the XAUTH RSA-SIG policy that is required for using certificates to establish a VPN tunnel.

With previous versions of PIX Firewall used as an Easy VPN Remote, IPsec Aggressive Mode was required so that `vpngroup` to key mappings could be performed at the Easy VPN Server. With RSA-SIG support, this restriction no longer applies and IPsec Main Mode can be used. Aggressive Mode is used for pre-shared keys and Main Mode is used for RSA-SIG based key exchange.

With PIX Firewall Version 6.3, the default option is RSA-SIG. To use pre-shared keys, enter the following command:

```
vpnclient vpngroup groupname password preshared_key
```

PIX Firewall Version 6.3 introduces additional encryption options for use by the Easy VPN Remote. These include Advanced Encryption Standard (AES) and Diffie-Hellman Group 5. Use of these protocols is determined by licensing (3DES, AES) and the use of Main Mode or Aggressive Mode. Diffie-Hellman groups are negotiable only in Main Mode.



Note

A PIX Firewall used as an Easy VPN Remote device does not check to determine if the certificate of the Easy VPN Server is revoked.

PIX Firewall Version 6.3 introduces optional X.500 support. The certificate enrollment process is enhanced to configure X.500 directory content.

To configure X.500 directory content, enter the following command:

```
ca subject-name ca-nickname [x500_DN]
```

You can either enter the full X.500 distinguished name (DN) or if this parameter is omitted, the PIX Firewall prompts you for the required information.

For example, the following command includes the DN:

```
pixfirewall(config)# ca subject-name cn=pixfirewall.example.com,ou=VSEC BU,o=Cisco  
System,c=US,e=klee@example.com
```

The following command omits the DN, and as a result the PIX Firewall prompts for this information:

```
pixfirewall(config)# ca subject-name
Common name (cn) [pixfirewall.example.com] :pixfirewall.example.com
Department (ou) []: VSEC BU
Company(o) []:Cisco System
State (st) []:CA
Country (c) []:US
Email (e) []:klee@example.com
Proceed with the above information [no]: yes
```

To display information about the current certification configuration, enter the following command:

```
pixfirewall(config)# show ca cert
...(PIX device cert)
Certificate
  Status: Available
  Certificate Serial Number: 45a490250000000000fa
  Key Usage: General Purpose
  Subject Name:
    CN = myvpn01.example.com
    OU = VSEC BU
    O = Cisco System INC
    UNSTRUCTURED NAME = myvpn01.example.com
  Validity Date:
    start date: 22:35:58 UTC Aug 16 2002
    end   date: 22:45:58 UTC Aug 16 2003
```

Verifying the DN of an Easy VPN Server

PIX Firewall Version 6.3, when used as an Easy VPN Remote device, lets you specify the DN of the certificate used to establish a VPN tunnel. We recommend enabling this feature to prevent a possible “man-in-the-middle” attack.

To verify the DN of the certificate received by your PIX Firewall, enter the following command:

```
ca verifycertdn x500 string
```



Note

Every attribute must match exactly to verify the certificate received and to establish a VPN tunnel.

For example, a PIX Firewall used as an Easy VPN Remote Server might have the following certificate:

```
Certificate
  Status: Available
  Certificate Serial Number: 4ebdbd400000000000a2
  Key Usage: General Purpose
  Subject Name:
    CN = myvpn01.myorg.com
    OU = myou
    O = myorg
    ST = CA
    C = US
    UNSTRUCTURED NAME = myvpn01.myorg.com
  Validity Date:
    start date: 23:48:00 UTC Feb 18 2003
    end   date: 23:58:00 UTC Feb 18 2004
-----
```

To establish a VPN tunnel with this server, enter the following command on the PIX Firewall used as an Easy VPN Remote device:

```
ca verifycertdn cn*myvpn, ou=myou, o=myorg, st=ca, c=US
```

This command causes the receiving PIX Firewall to accept certificates with any DN having the following attributes:

- Common Name (CN) containing the string *myvpn*
- Organizational Unit (OU) equal to *myou*
- Organization (O) equal to *myorg*
- State (ST) equal to *CA*
- Country (C) equal to *US*

You could be more restrictive by identifying a specific common name, or less restrictive by omitting the CN attribute altogether.

You can use an asterisk (*) to match an attribute containing the string following the asterisk. Use an exclamation mark (!) to match an attribute that does not contain the characters following the exclamation mark.

Using the PIX Firewall PPPoE Client

This section describes how to use the PPPoE client provided with PIX Firewall Version 6.2 and higher. It includes the following topics:

- [Overview, page 4-12](#)
- [Configuring the PPPoE Client Username and Password, page 4-13](#)
- [Enabling PPPoE on the PIX Firewall, page 4-14](#)
- [Using PPPoE with a Fixed IP Address, page 4-14](#)
- [Monitoring and Debugging the PPPoE Client, page 4-15](#)
- [Using Related Commands, page 4-16](#)

Overview

Point-to-Point Protocol over Ethernet (PPPoE) combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. PPPoE clients are typically personal computers connected to an ISP over a remote broadband connection, such as DSL or cable service. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.

PIX Firewall Version 6.2 introduces PPPoE client functionality. This allows small office, home office (SOHO) users of the PIX Firewall to connect to ISPs using DSL modems.

**Note**

The PIX Firewall PPPoE client can only be enabled on the outside interface.

PPPoE provides a standard method of employing the authentication methods of the Point-to-Point Protocol (PPP) over an Ethernet network. When used by ISPs, PPPoE allows authenticated assignment of IP addresses. In this type of implementation, the PPPoE client and server are interconnected by Layer 2 bridging protocols running over a DSL or other broadband connection.

PPPoE is composed of two main phases:

- **Active Discovery Phase**—In this phase, the PPPoE client locates a PPPoE server, called an access concentrator. During this phase, a Session ID is assigned and the PPPoE layer is established.
- **PPP Session Phase**—In this phase, PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method, allowing data to be transferred over the PPP link within PPPoE headers.

At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication protocol (PAP). Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Configuring the PPPoE Client Username and Password

To configure the username and password used to authenticate the PIX Firewall to the access concentrator, use the PIX Firewall **vpdn** command. The **vpdn** command is used to enable remote access protocols, such as L2TP, PPTP, and PPPoE. To use the **vpdn** command, you first define a VPDN group and then create individual users within the group.

To configure a PPPoE username and password, perform the following steps:

Step 1 Define the VPDN group to be used for PPPoE, by entering the following command:

```
vpdn group group_name request dialout pppoe
```

In this command, replace *group_name* with a descriptive name for the group, such as “pppoe-sbc.”

Step 2 If your ISP requires authentication, select an authentication protocol by entering the following command:

```
vpdn group group_name ppp authentication PAP|CHAP|MSCHAP
```

Replace *group_name* with the same group name you defined in the previous step. Enter the appropriate keyword for the type of authentication used by your ISP:

- **PAP**—Password Authentication Protocol
- **CHAP**—Challenge Handshake Authentication Protocol
- **MS-CHAP**—Microsoft Challenge Handshake Authentication Protocol



Note When using CHAP or MS-CHAP, the username may be referred to as the remote system name, while the password may be referred to as the CHAP secret.

Step 3 Associate the username assigned by your ISP to the VPDN group by entering the following command:

```
vpdn group group_name localname username
```

Replace *group_name* with the VPDN group name and *username* with the username assigned by your ISP.

Step 4 Create a username and password pair for the PPPoE connection by entering the following command:

```
vpdn username username password pass [store-local]
```

Replace *username* with the username and *pass* with the password assigned by your ISP.



Note

The **store-local** option stores the username and password in a special location of NVRAM on the PIX Firewall. If an Auto Update Server sends a **clear config** command to the PIX Firewall and the connection is then interrupted, the PIX Firewall can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

Enabling PPPoE on the PIX Firewall



Note

You must complete the configuration using the **vpdn** command, described in “[Configuring the PPPoE Client Username and Password](#),” before enabling PPPoE.

The PPPoE client functionality is turned off by default. To enable the PPPoE client, enter the following command.

```
ip address ifName pppoe [setroute]
```

Reenter this command to clear and restart the PPPoE session. The current session will be shut down and a new one will be restarted.

For example:

```
ip address outside pppoe
```

The PPPoE client is only supported on the outside interface of the PIX Firewall. PPPoE is not supported in conjunction with DHCP because with PPPoE the IP address is assigned by PPP. The **setroute** option causes a default route to be created if no default route exists. The default router will be the address of the access concentrator. The maximum transmission unit (MTU) size is automatically set to 1492 bytes, which is the correct value to allow PPPoE transmission within an Ethernet frame.

Using PPPoE with a Fixed IP Address

You can also enable PPPoE by manually entering the IP address, using the command in the following format:

```
ip address ifname ipaddress mask pppoe
```

This command causes the PIX Firewall to use the specified address instead of negotiating with the PPPoE server to assign an address dynamically. To use this command, replace *ifname* with the name of the outside interface of the PIX Firewall connected to the PPPoE server. Replace *ipaddress* and *mask* with the IP address and subnet mask assigned to your PIX Firewall.

For example:

```
ip address outside 201.n.n.n 255.255.255.0 pppoe
```



Note

The **setroute** option is an option of the **ip address** command that you can use to allow the access concentrator to set the default routes when the PPPoE client has not yet established a connection. When using the **setroute** option, you cannot have a statically defined route in the configuration.

Monitoring and Debugging the PPPoE Client

Use the following command to display the current PPPoE client configuration information:

```
show ip address outside pppoe
```

Use the following command to enable debugging for the PPPoE client:

```
[no] debug pppoe event | error | packet
```

The following summarizes the function of each keyword:

- **event**—Displays protocol event information
- **error**—Displays error messages
- **packet**—Displays packet information

Use the following command to view the status of PPPoE sessions:

```
show vpdn session [l2tp|pptp|pppoe] [id sess_id] packets|state|window]
```

[Example 4-1](#) shows the kind of information provided by this command.

Example 4-1 show vpdn session Command Output

```
pix1# sh vpdn
Tunnel id 0, 1 active sessions
    time since change 65862 secs
    Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
    6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
Session state is SESSION_UP
    Time since event change 65865 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
pix1#
pix1# sh vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
    Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
pix1#
pix1# sh vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
    time since change 65901 secs
    Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
```

```
6 packets sent, 6 received, 84 bytes sent, 0 received
pixl#
```

Using Related Commands

Use the following **vpdn** command to set the PPP parameters used during the PPP session:

```
vpdn group group_name ppp authentication [PAP|CHAP|MSCHAP]
```

Use the following command to cause the DHCP server to use the WINS and DNS addresses provided by the access concentrator as part of the PPP/IPCP negotiations:

```
dhcpcd auto_config [client_ifx_name]
```

This command is only required if the service provider provides this information as described in RFC 1877. The *client_ifx_name* parameter identifies the interface supported by the DHCP **auto_config** option. At this time, this keyword is not required because the PPPoE client is only supported on a single outside interface.

Using the PIX Firewall DHCP Server

This section describes how to use the DHCP server provided by the PIX Firewall. It includes the following topics:

- [Overview, page 4-16](#)
- [Configuring the DHCP Server Feature, page 4-18](#)
- [Using Cisco IP Phones with a DHCP Server, page 4-20](#)

Overview

PIX Firewall supports Dynamic Host Configuration Protocol (DHCP) servers and DHCP clients. DHCP is a protocol that supplies automatic configuration parameters to Internet hosts. This protocol has two components:

- Protocol for delivering host-specific configuration parameters from a DHCP server to a host (DHCP client)
- Mechanism for allocating network addresses to hosts

A DHCP server is simply a computer that provides configuration parameters to a DHCP client, and a DHCP client is a computer or network device that uses DHCP to obtain network configuration parameters.

As a DHCP server, the PIX Firewall provides network configuration parameters, including dynamically assigned IP addresses, to DHCP clients. These configuration parameters provide a DHCP client the networking parameters required to access an enterprise network and network services, such as DNS.

[Table 4-2](#) lists the number of DHCP clients that can be supported concurrently by different models and versions of the PIX Firewall.

Table 4-2 DHCP Clients Supported by PIX Firewall

PIX Firewall Version	PIX Firewall Platform	Maximum Number of DHCP Client Addresses (Active Hosts)
Version 5.2 and earlier	All platforms	10
Version 5.3 to Version 6.0	PIX 506/506E	32
	All other platforms	256
Version 6.1 and 6.2	PIX 501	32
	PIX 501 with optional 50-user license	128
	PIX 506/506E	256
	All other platforms	256
Version 6.3 and higher	PIX 501	32
	PIX 501 with optional 50-user license	128
	PIX 501 with optional unlimited license	256
	PIX 506/506E	256
	All other platforms	256 per interface

**Note**

A host is considered active when the host has passed traffic through the PIX Firewall within the number of seconds currently configured for the xlate timeout interval. It is also considered active if it has an established NAT/PAT through the PIX Firewall, or it has an established TCP connection or UDP session through the PIX Firewall, or it has an established user authentication through the PIX Firewall.

You cannot configure a DHCP server for 256 clients, using a Class C netmask. For example, if a company has a Class C network address of 172.17.1.0 with netmask 255.255.255.0, then 172.17.1.0 (network IP) and 172.17.1.255 (broadcast) cannot be in the DHCP address pool range. Further, one address is used up for the PIX Firewall interface. Thus, if a user uses a Class C netmask, they can only have up to 253 DHCP Clients.

**Note**

The PIX Firewall DHCP server does not support BOOTP requests. The current version of the DHCP server also does not support failover configurations.

The PIX Firewall commands used to implement the DHCP server feature are described in the **dhcpcd** command page and the **debug** command page in the *Cisco PIX Firewall Command Reference*. Refer to these command pages for more information.

Configuring the DHCP Server Feature

Be sure to configure the IP address and the subnet mask of the interface using the **ip address** command prior to enabling the DHCP server feature.


Note

With PIX Firewall Version 6.3 and higher, the DHCP server can be enabled on any interface. With earlier versions, the DHCP server can only be enabled on the inside interface.

Follow these steps to enable the DHCP server feature on a given PIX Firewall interface:

- Step 1** Specify a DHCP address pool using the **dhcpcd address** command. The PIX Firewall will assign to a client one of the addresses from this pool to use for a given length of time.

For example:

```
dhcpcd address 10.0.1.101-10.0.1.110 inside
```


Note

When using Network Extension Mode, do *not* enable the DHCP server on the inside interface. Also, in Network Extension Mode, the following two steps (Step 2 and Step 3) are not required because the DNS and WINS information is part of the policy that is downloaded from the Easy VPN Server.

- Step 2** (Optional) If you are using client mode, specify the IP address(es) of the DNS server(s) the client will use. You can specify up to two DNS servers.

For example:

```
dhcpcd dns 209.165.201.2 209.165.202.129
```

- Step 3** (Optional) If you are using client mode, specify the IP address(es) of the WINS server(s) the client will use. You can specify up to two WINS servers.

For example:

```
dhcpcd wins 209.165.201.5
```

- Step 4** (Optional) Specify the lease length to be granted to the client. This lease equals the amount of time (in seconds) the client can use its allocated IP address before the lease expires. The default value is 3600 seconds.

For example:

```
dhcpcd lease 3000
```

- Step 5** (Optional) Configure the domain name the client will use by entering the following command:

```
dhcpcd domain example.com
```

Step 6 Enable the DHCP daemon within the PIX Firewall to listen for DHCP client requests on the enabled interface.

For example:

```
dhcpcd enable inside
```

Step 7 (Optional) To display debugging information about the DHCP server, enter the following command:

```
debug dhcpcd event
debug dhcpcd packet
```

[Example 4-2](#) shows a configuration listing for the previous procedure:

Example 4-2 DHCP Server Configuration

```
! set the ip address of the inside interface
ip address inside 10.0.1.2 255.255.255.0
! configure the network parameters the client will use once in the corporate network and
dhcpcd address 10.0.1.101-10.0.1.110 inside
dhcpcd dns 209.165.201.2 209.165.202.129
dhcpcd wins 209.165.201.5
dhcpcd lease 3000
dhcpcd domain example.com
! enable dhcp server daemon on the inside interface
dhcpcd enable inside
```

The following example shows the configuration of a DHCP address pool and a DNS server address with the inside interface being enabled for the DHCP server feature:

```
dhcpcd address 10.0.1.100-10.0.1.108 inside
dhcpcd dns 209.165.200.227
dhcpcd enable inside
```

The following example shows the configuration of a DHCP address pool and uses the **auto_config** command to configure the dns, wins, and domain parameters:

```
dhcpcd address 10.0.1.100-10.0.1.108 inside
dhcpcd auto_config outside
dhcpcd enable inside
```

[Example 4-3](#) is a partial configuration example of the DHCP server and IPSec features configured on a PIX Firewall that is within a remote office. The PIX 506/506E unit's VPN peer is another PIX Firewall that has an outside interface IP address of 209.165.200.228 and functions as a gateway for a corporate network.

Example 4-3 Configuration for DHCP Server with IPSec

```
! configure interface ip address on the inside and outside interfaces
ip address outside 209.165.202.129 255.255.255.0
ip address inside 172.17.1.1 255.255.255.0
! configure ipsec with corporate pix
access-list ipsec-peer permit ip 172.17.1.0 255.255.255.0 192.168.0.0 255.255.255.0
ipsec transform-set myset esp-des esp-sha-hmac
crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address ipsec-peer
crypto map mymap 10 set transform-set myset
crypto map mymap 10 set peer 209.165.200.228
```

```

crypto map mymap interface outside
sysopt connection permit-ipsec
nat (inside) 0 access-list ipsec-peer
isakmp policy 10 authentication preshare
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 3600
isakmp key 12345678 address 0.0.0.0 netmask 0.0.0.0
isakmp enable outside
!configure dhcp server pool of addresses
dhcpd address 172.17.1.100-172.17.1.109 inside
dhcpd dns 192.168.0.20
dhcpd wins 192.168.0.10
dhcpd lease 3000
dhcpd domain example.com
! enable dhcp server on inside interface
dhcpd enable inside
! use outside interface ip as PAT global address
nat (inside) 1 0 0
global (outside) 1 interface

```

Using Cisco IP Phones with a DHCP Server

Enterprises with small branch offices implementing a Cisco IP Telephony VoIP solution typically implement Cisco CallManager at a central office to control Cisco IP Phones at small branch offices. This implementation allows centralized call processing, reduces the equipment required, and eliminates the administration of additional Cisco CallManager and other servers at branch offices.

Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers
- DHCP option 66, defined in RFC 2132 (DHCP Options and BOOTP Vendor Extensions), gives the IP address or the host name of a single TFTP server.

Cisco IP Phones may include both option 150 and 66 in a single request. In this case, the PIX Firewall DHCP server provides values for both options in the response if they are configured on the PIX Firewall.

Cisco IP Phones may also include DHCP option 3 in their requests. PIX Firewall Version 6.0(1) added support for this option, which lists the IP addresses of default routers.

PIX Firewall Version 6.2 and higher provides the following options for the **dhcpd** command:

```

dhcpd option 66 ascii server_name
dhcpd option 150 ip server_ip1 [server_ip2]

```

When using option 66, replace *server_name* with the TFTP host name. A single TFTP server can be identified using option 66.

When using option 150, replace *server_ip1* with the IP address of the primary TFTP server and replace *server_ip2* with the IP address of the secondary TFTP server. A maximum of two TFTP servers can be identified using option 150.

To disable option 66 or option 150, enter one of the following commands:

```

no dhcpd option 66
no dhcpd option 150

```

**Note**

With PIX Firewall Version 6.2 and lower, the DHCP server can only be enabled on the inside interface and therefore can only respond to DHCP option 150 and 66 requests from Cisco IP Phones or other network devices on the internal network. With PIX Firewall Version 6.3 and higher, the DHCP server can be enabled on any interface and with as many instances as required.

Using DHCP Relay

PIX Firewall Version 6.3 provides a DHCP relay agent. This allows the PIX Firewall to assist in dynamic configuration of IP device hosts on any Ethernet interface. Acting as a DHCP relay agent, when the PIX Firewall receives a request from a host on an interface, it forwards the request to a user-configured DHCP server on another interface.

With previous versions of PIX Firewall, hosts on the inside interfaces must be statically configured or use addresses provided by the PIX Firewall DHCP Server.

The following restrictions apply to the use of the DHCP relay agent:

- The relay agent accepts and responds to client requests on any interface.
- The relay agent cannot be enabled if the PIX Firewall DHCP server is enabled.
- The relay agent will forward requests if IPSec is configured. VPN negotiations will be initiated if a tunnel does not exist.
- Clients must be directly connected to the PIX Firewall and cannot send requests through another relay agent or a router.
- DHCP relay will not work in client mode.

**Note**

Some type of NAT must be specified to allow forwarding of a DHCP release message from a client to a DHCP server.

Use the following command to enable the DHCP relay agent:

```
[no] dhcprelay enable interface
```

Replace *interface* with the name of the interface connected to the DHCP clients.

Use the following command to configure a DHCP server address for the relay agent:

```
[no] dhcprelay server dhcp_server_ip server_ifc
```

Replace *dhcp_server_ip* with the IP address of the DHCP server. Replace *server_ifc* with the interface connected to the DHCP server. You can use this command to identify up to four servers.

By default, the default gateway used by the DHCP server is configured on the DHCP server. To specify the default gateway to be used by the DHCP server in the PIX Firewall configuration, enter the following command:

```
[no] dhcprelay setroute client_ifc
```

Replace *client_ifc* with the PIX Firewall interface to be used as the default gateway by DHCP clients for reaching the DHCP server.

To set the timeout, use the following command:

```
[no] dhcprelay timeout seconds
```

Replace *seconds* with the number of seconds allowed for relay address negotiation.

You can use the following commands to display debugging information for the DHCP Relay Agent:

```
Debug dhcprelay event
Debug dhcprelay error
Debug dhcprelay packet
```

Using the PIX Firewall DHCP Client

This section describes how to enable and manage the DHCP client on a PIX Firewall. It includes the following topics:

- [Overview, page 4-22](#)
- [Configuring the DHCP Client, page 4-22](#)
- [Releasing and Renewing the DHCP Lease, page 4-23](#)
- [Monitoring and Debugging the DHCP Client, page 4-23](#)

Overview

DHCP client support within the PIX Firewall is designed for use within a small office, home office (SOHO) environment using a PIX Firewall that is directly connected to a DSL or cable modem that supports the DHCP server function.



Note

The PIX Firewall DHCP client can only be enabled on the outside interface.

With the DHCP client feature enabled on a PIX Firewall, the PIX Firewall functions as a DHCP client to a DHCP server allowing the server to configure the outside interface with an IP address, subnet mask, and optionally a default route. Use of the DHCP client feature to acquire an IP address from a generic DHCP server is not supported. Also, the PIX Firewall DHCP client does not support **failover** configurations.

The DHCP-acquired IP address on the outside interface can also be used as the PAT global address. This makes it unnecessary for the ISP to assign a static IP address to the PIX Firewall. Use the **global** command with the **interface** keyword to enable PAT to use the DHCP-acquired IP address of outside interface. For more information about the **global** command, see the **global** command page in the *Cisco PIX Firewall Command Reference*.

Configuring the DHCP Client

To enable the DHCP client feature on a given PIX Firewall interface and set the default route via the DHCP server, enter the following command:

```
ip address outside dhcp [setroute] [retry retry_cnt]
```

The **ip address dhcp** command enables the DHCP client feature on the outside PIX Firewall interface. The optional **setroute** argument tells the PIX Firewall to set the default route using the default gateway parameter the DHCP server returns. If the **setroute** argument is configured, the **show route** command displays the default route set by the DHCP server.

**Note**

Do not configure the PIX Firewall with a default route when using the **setroute** argument of the **ip address dhcp** command.

Releasing and Renewing the DHCP Lease

To view current information about the DHCP lease, enter the following command:

```
show ip address dhcp
```

To release and renew the DHCP lease from the PIX Firewall, reenter the **ip address** command, as follows:

```
ip address outside dhcp [setroute] [retry retry_cnt]
```

Replace *retry_cnt* with the number of times the request should be issued before terminating. To clear the DHCP default route, use the **clear route static** command.

**Note**

The **clear ip** command can be also used to release and renew the DHCP lease, but this clears the configuration of every PIX Firewall interface.

Monitoring and Debugging the DHCP Client

The following commands provide debugging tools for the DHCP client feature:

- **debug dhcpc packet**
- **debug dhcpc detail**
- **debug dhcpc error**

The PIX Firewall commands used to debug the DHCP client are described in the **debug** command pages in the *Cisco PIX Firewall Command Reference*. Refer to these command pages for more information.

