



## 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](#)
- [Using the PIX Firewall PPPoE Client](#)
- [Using the PIX Firewall DHCP Server](#)
- [Using the PIX Firewall DHCP Client](#)

### 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](#)
- [Establishing Connectivity](#)
- [Configuration Procedure](#)

#### Overview

PIX Firewall version 6.2 lets you use PIX Firewall as an Easy VPN Remote device when connecting to an Easy VPN Server, such as a Cisco VPN 3000 Concentrator or a PIX Firewall. This 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.

You must select one of the following modes of operation when you enable the PIX Firewall as an Easy VPN Remote device:

- **Client mode**—In this mode, VPN connections are 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](#).”
- **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 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” later in this chapter
- DHCP client—Refer to “Using the PIX Firewall DHCP Client” later in this chapter
- Static IP address configuration—Refer to Chapter 2, “Establishing Connectivity”

## 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** Define the VPN group and password by entering the following command:

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

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.

**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 ten Easy VPN Servers is supported (one primary and up to nine secondary).

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

```
vpnclient enable
```

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

```
show vpnclient
```

---

## Using the PIX Firewall PPPoE Client

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

- [Overview](#)
- [Configuring the PPPoE Client Username and Password](#)
- [Enabling PPPoE on the PIX Firewall](#)
- [Using PPPoE with a Fixed IP Address](#)
- [Monitoring and Debugging the PPPoE Client](#)
- [Using Related Commands](#)

### 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 AC by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication (PAP) protocol. 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 AC, 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
```

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

---

## 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 AC. 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 5-1 shows the kind of information provided by this command.

#### Example 5-1 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
pix1#
```

## 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 AC 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 for use on its inside interface. It includes the following topics:

- [Overview](#)
- [Configuring the DHCP Server Feature](#)
- [Using Cisco IP Phones with a DHCP Server](#)

## 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.



### Note

The PIX Firewall DHCP server can only be enabled on the inside interface.

The DHCP server within the PIX Firewall is typically used within a SOHO environment with a PIX 501 or PIX 506 unit. Connecting to the PIX Firewall are PC clients and other network devices (DHCP clients) that establish network connections that are either insecure (unencrypted) or secure (encrypted using IPSec) to access an enterprise or corporate network. As a DHCP server, the PIX Firewall provides network configuration parameters to the DHCP clients through the use of DHCP. These configuration parameters provide a DHCP client the networking parameters used to access the enterprise network, and once in the network, the network services to use, such as the DNS server.

[Table 5-1](#) lists the number of DHCP clients that can be supported concurrently by different models and versions of the PIX Firewall.

**Table 5-1 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 higher	PIX 501	32
	PIX 501 with optional 50-user license	128
	PIX 506/506E	256
	All other platforms	256

**Note**

A host is considered active when the host has passed traffic through the PIX Firewall within the period defined by the **xlate timeout** command, or 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 **inside** interface using the **ip address** command prior to enabling the DHCP server feature.

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. The default is the **inside** interface.

For example:

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

- Step 2** (Optional) 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) 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** 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. Currently, you can only enable the DHCP server feature on the **inside** interface, which is the default.

For example:

```
dhcpcd enable inside
```

[Example 5-2](#) shows a configuration listing for the previous procedure:

**Example 5-2 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
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
dhcpcd dns 209.165.200.227
dhcpcd enable
```

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
dhcpcd auto_config
dhcpcd enable
```

[Example 5-3](#) 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 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 5-3 Configuration for DHCP Server with IPSec**

```
! configure interface ip address
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 address
dhcpd address 172.17.1.100-172.17.1.109
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
! 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 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 introduces the following new 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

The PIX Firewall 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.

# 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](#)
- [Configuring the DHCP Client](#)
- [Releasing and Renewing the DHCP Lease](#)
- [Monitoring and Debugging the DHCP Client](#)

## 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.