



## Managing VPN Remote Access

---

This chapter describes how to configure the PIX Firewall as an Easy VPN Server and how to configure Easy VPN Remote software clients. It also describes how to use the PIX Firewall with Point-to-Point Tunneling Protocol (PPTP) clients. This chapter includes the following sections:

- [Using the PIX Firewall as an Easy VPN Server, page 8-1](#)
- [Configuring Extended Authentication \(Xauth\), page 8-5](#)
- [Configuring Easy VPN Remote Devices with IKE Mode Config, page 8-7](#)
- [Using an Easy VPN Remote Device with Pre-Shared Keys, page 8-8](#)
- [Using an Easy VPN Remote Device with Digital Certificates, page 8-13](#)
- [Using PPTP for Remote Access, page 8-19](#)



**Note**

To enable remote access to the firewall, you must use a dynamic crypto map when configuring IPSec. A dynamic crypto map acts as a template where the missing parameters are dynamically assigned based on the IKE negotiation. For more information about configuring dynamic crypto maps, see [“Using Dynamic Crypto Maps”](#) in [Chapter 6, “Configuring IPSec and Certification Authorities.”](#)

---

### Using the PIX Firewall as an Easy VPN Server

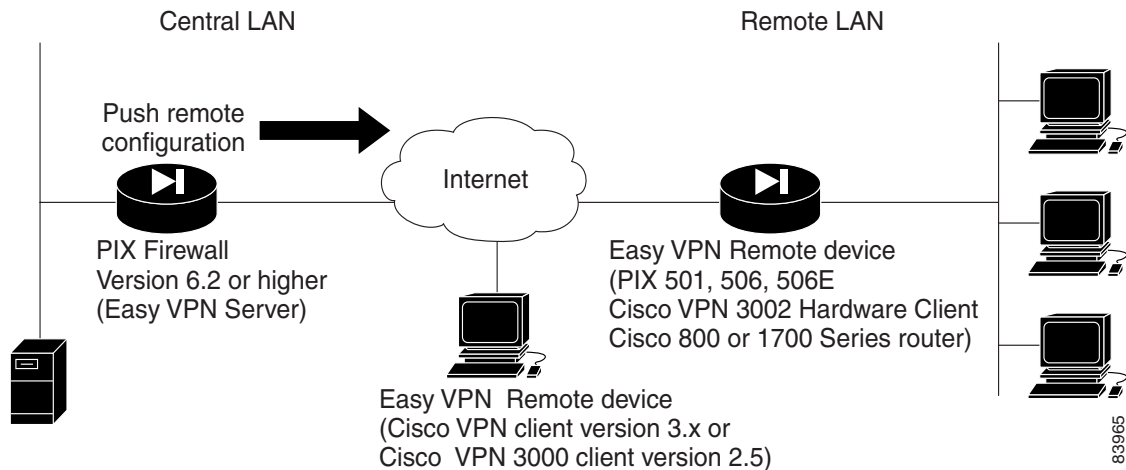
This section describes how to use the PIX Firewall as an Easy VPN Server and includes the following topics:

- [Overview, page 8-2](#)
- [Enabling Redundancy, page 8-4](#)
- [Configuring Secure Unit Authentication, page 8-4](#)
- [Configuring Individual User Authentication, page 8-4](#)
- [Bypassing AAA Authentication, page 8-5](#)

## Overview

With software Version 6.2 and later releases, you can configure the PIX Firewall as an Easy VPN Server. When used as an Easy VPN Server, the firewall can push VPN configuration to any Easy VPN Remote device, which greatly simplifies configuration and administration. [Figure 8-1](#) illustrates how an Easy VPN Server can be used in a Virtual Private Network (VPN).

**Figure 8-1 Using the PIX Firewall as an Easy VPN Server**



Using the PIX Firewall as an Easy VPN Server lets you configure your VPN policy in a single location on the PIX Firewall and then push this configuration to multiple Easy VPN Remote devices. The following are the different types of Easy VPN Remote devices you can use with a PIX Firewall configured as an Easy VPN Server:

- Software clients—Connect directly to the Easy VPN Server but require prior installation and configuration of client software on each host computer. These include the following:
  - Cisco VPN Client Version 3.x (also known as Unity Client 3.x)
  - Cisco VPN 3000 Client version 2.5 (also known as the Altiga VPN Client Version 2.5)
- Hardware clients—Allow multiple hosts on a remote network to access a network protected by an Easy VPN Server without any special configuration or software installation on the remote hosts. These include the following:
  - PIX 501 or PIX 506/506E
  - Cisco VPN 3002 Hardware Client
  - Cisco IOS-based Easy VPN Remote devices (for example, Cisco 800 series and Cisco 1700 series routers)

You use the **vpngroup** command to associate security policy attributes with a VPN group name. These attributes are pushed to any Easy VPN Remote devices assigned to the group. The subsequent sections and examples in this chapter describe how to use this command for implementing different options and scenarios. See the *Cisco PIX Firewall Command Reference* for the complete command syntax.

The configuration instructions and examples in this chapter assume that you are using an Easy VPN Remote device (except for the [“Using PPTP for Remote Access”](#) section on page 8-19). For information about using a PIX 501 or PIX 506/506E as an Easy VPN Remote device, refer to [Chapter 4, “Using PIX Firewall in SOHO Networks.”](#)

**Note**

PIX Firewall Version 6.3 introduces a feature that lets you establish 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 [“Connecting to PIX Firewall Over a VPN Tunnel”](#) in Chapter 9, [“Accessing and Monitoring PIX Firewall.”](#)

For information about configuring remote access for other VPN software clients, including L2TP, Windows 2000, and Cisco Secure VPN Client Version 1.1, refer to [Appendix B, “Configuration Examples for Other Remote Access Clients.”](#)

**Note**

Before you install the Cisco VPN 3000 Client Version 2.5 or the Cisco VPN Client Version 3.x on a remote host computer, uninstall any Cisco Secure VPN Client Version 1.1 software and clear the associated directories.

The configuration of the PIX Firewall as an Easy VPN Server is similar regardless of the type of Easy VPN Remote device that you are using. However, certain Easy VPN Server features and options only apply when using an Easy VPN Remote hardware client.

For instance, when using a hardware client, two different modes of operation can be enabled on the Easy VPN Remote device:

- Client mode
- Network extension mode

Client mode causes VPN connections to be initiated by traffic from the Easy VPN Remote device, so resources are only used on demand. In client mode, the Easy VPN Remote device applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the Easy VPN Remote device.

Network extension mode keeps VPN connections open even when not required for transmitting traffic and no address translation is applied. In network extension mode, the IP addresses of clients on the inside interface of the Easy VPN Remote device are sent without change to the Easy VPN Server.

**Note**

Client mode and network extension mode are configured on the Easy VPN Remote device. For more information, refer to [“Using PIX Firewall as an Easy VPN Remote Device”](#) in Chapter 4, [“Using PIX Firewall in SOHO Networks.”](#)

The PIX Firewall uses the IKE Mode Config protocol to download the attributes to the Easy VPN Remote device, including the following:

- DNS, WINS, and default domain (in client mode)
- Split tunnel mode attributes

The split tunnel mode allows the PIX Firewall to define a policy for encrypting certain traffic and transmitting other traffic in clear text. With split tunnelling enabled, the VPN client PC can access the Internet while the VPN client is running. For more information about configuring these parameters, refer to [“Configuring Easy VPN Remote Devices with IKE Mode Config”](#) in Chapter 8, [“Managing VPN Remote Access.”](#)

## Enabling Redundancy

PIX Firewall Version 6.3 introduces support for redundancy among Easy VPN Servers. You can define a list of servers on an Easy VPN Server that can be pushed to the Easy VPN Remote. When no backup Easy VPN Server is configured, what happens after a failure to connect to the Easy VPN server depends on SUA status and whether the Easy VPN Remote device is in client mode or network extension mode. In client mode, without SUA, traffic continues to trigger subsequent connections to the Easy VPN Server. In network extension mode, without SUA, the Easy VPN Remote device continually tries to reconnect to the primary server. With SUA, a connection failure message is displayed and all connection attempts must be manually triggered.

To define a list of backup servers, enter the following command on the PIX Firewall used as the Easy VPN Server:

```
vpngroup groupname backup-server ipaddr1 [ipaddr2 .. ipaddr10]
```

To clear the current client configuration, enter the following command on the PIX Firewall used as the Easy VPN Server:

```
vpngroup groupname backup-server clear-client-cfg
```

## Configuring Secure Unit Authentication

Secure Unit Authentication (SUA) provides increased security when allowing access to an Easy VPN Server from an Easy VPN Remote device. With SUA, one-time passwords, two-factor authentication, and similar authentication schemes can be used to authenticate the Easy VPN Remote device during Extended Authentication (Xauth). SUA is specified in the VPN Policy on the Easy VPN Server and is downloaded to the Easy VPN Remote device. This enables SUA and determines the connection behavior of the Easy VPN Remote device.

To add SUA to the VPN policy for a VPN group, enter the following command at the CLI of the Easy VPN Server:

```
vpngroup groupname secure-unit-authentication
```

This command enables SUA for the VPN group identified by *groupname*.

To disable SUA for a VPN policy, remove the configuration for the corresponding VPN group. Note that VPN policy changes are updated on Easy VPN Remote devices only after the next connection following the policy configuration change.

## Configuring Individual User Authentication

Individual User Authentication (IUA) supports individually authenticating clients on the inside network of the Easy VPN Remote, based on the IP address of each inside client. IUA supports both static and OTP authentication mechanisms.

IUA is enabled by means of the downloaded VPN policy and it cannot be configured locally. To enable IUA on a PIX Firewall used as the Easy VPN Server, enter the following command:

```
vpngroup groupname user-authentication
```

This command enables individual user authentication for the VPN group identified by *groupname*.

To specify the length of time that a VPN tunnel can remain open without user activity, enter the following command:

```
vpngroup groupname user-idle-timeout {hh:mm:ss}
```

This command specifies the length of time for the specified VPN group in hours, minutes, and seconds (hh:mm:ss).

Once a downloaded VPN policy activates SUA on an Easy VPN Remote, this policy is stored locally in the FLASH memory of the PIX Firewall used as an Easy VPN Remote device.

When using IUA with a PIX Firewall, the Easy VPN Remote device sends its authentication request directly to the AAA server.

To specify the AAA server to use for IUA on a PIX Firewall being used as the Easy VPN Server, enter the following command:

```
vpngroup groupname authentication-server server_tag
```

This command specifies the AAA server identified by *server\_tag* for the VPN group identified by *groupname*.

## Bypassing AAA Authentication

PIX Firewall Version 6.3 lets you use Media Access Control (MAC) addresses to bypass authentication for devices, such as Cisco IP Phones, that do not support AAA authentication.

When MAC-based AAA exemption is enabled the Easy VPN Remote 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. Authorization services are automatically disabled when you bypass authentication. Accounting records are still generated (if enabled), but the username is not displayed.

To enable this feature for a specific Easy VPN Remote device, enter the following command:

```
vpngroup groupname device-pass-through
```



### Note

When using this feature with a PIX Firewall acting as an Easy VPN Remote device, the remote administrator must identify the MAC addresses that are exempt from authentication. For information about how to perform this configuration on the remote PIX Firewall, refer to “[Using MAC-Based AAA Exemption](#)” in [Chapter 3, “Controlling Network Access and Use.”](#)

## Configuring Extended Authentication (Xauth)

The PIX Firewall supports the Extended Authentication (Xauth) feature within the IKE protocol. Xauth lets you deploy IPSec VPNs using TACACS+ or RADIUS as your user authentication method.

This feature, which is designed for VPN clients, provides user authentication by prompting the user for username and password and verifies them with the information stored in your TACACS+ or RADIUS database. Xauth is negotiated between IKE Phase 1 (IKE device authentication phase) and IKE Phase 2 (IPSec SA negotiation phase). If the Xauth fails, the IPSec security association will not be established and the IKE security association will be deleted.

**Note**

The IKE Mode Config feature also is negotiated between IKE Phase 1 and 2. If both features are configured, Xauth is performed first.

The Xauth feature is optional and is enabled using the **crypto map *map-name* client authentication *aaa-group-tag*** command. AAA must be configured on the PIX Firewall using the **aaa-server *group\_tag* (*if\_name*) host *server\_ip* key *timeout seconds*** command before Xauth is enabled. Use the same AAA server name within the **aaa-server** and **crypto map client authentication** command statements. See the **aaa-server** command and the **crypto map** command in the *Cisco PIX Firewall Command Reference* for more information.

Follow these steps to configure Xauth on your PIX Firewall:

**Step 1** Set up your basic AAA Server:

```
aaa-server group_tag (if_name) host server_ip key
```

For example:

```
aaa-server TACACS+ (outside) host 10.0.0.2 secret123
```

This example specifies that the authentication server with the IP address 10.0.0.2 resides on the outside interface and is in the default TACACS+ server group. The key “secret123” is used between the PIX Firewall and the TACACS+ server for encrypting data between them.

**Step 2** Enable Xauth. Be sure to specify the same AAA server group tag within the **crypto map client authentication** command statement as was specified in the **aaa-server** command statement.

```
crypto map map-name client authentication aaa-group-tag
```

For example:

```
crypto map mymap client authentication TACACS+
```

In this example, Xauth is enabled at the crypto map “mymap” and the server specified in the TACACS+ group will be used for user authentication.

**Step 3** (Optional) Perform this step for each site-to-site VPN peer that shares the same interface as the VPN client(s) and is configured to use a pre-shared key. This step allows the PIX Firewall to make an exception to the Xauth feature for the given site-to-site VPN peer.

```
isakmp key keystring address ip-address [netmask mask] [no-xauth] [no-config-mode]
```

For example:

```
isakmp key secretkey1234 address 10.2.2.2 netmask 255.255.255.255 no-xauth
```

**Step 4** (Optional) To make an exception to the Xauth feature for the given site-to-site VPN peer, enter the following command:

```
isakmp peer fqdn fqdn [no-xauth] [no-config-mode]
```

Perform this step for each site-to-site VPN peer that shares the same interface as the VPN client(s) and is configured to use RSA-signatures.

For example:

```
isakmp peer fqdn hostname1.example.com no-xauth
```

# Configuring Easy VPN Remote Devices with IKE Mode Config

A PIX Firewall used as an Easy VPN Server uses the IKE Mode Configuration (Config) protocol to download an IP address and other network level configuration to an Easy VPN Remote device as part of the IKE negotiation. During this exchange, the PIX Firewall gives an IP address to the Easy VPN Remote device that is used as an “inner” IP address encapsulated under IPSec. This provides a known IP address for the Easy VPN Remote device, which can then be matched against the IPSec policy on the Easy VPN Server.



## Note

If you use IKE Mode Config on the PIX Firewall, the routers handling the IPSec traffic must also support IKE Mode Config. Cisco IOS Release 12.0(7)T and higher supports IKE Mode Config.

To configure IKE Mode Config, use the following command:

```
vpngroup groupname option
```

Replace *groupname* with an identifier to be used when configuring a particular group of Easy VPN Remote devices. The administrator of each Easy VPN Remote device enters a specific group name to access the Easy VPN Remote server.

Replace *option* with the different options required in your VPN implementation. Some of these options are required when using network extension mode, which allow central configuration of additional parameters, such as the address of the DNS server. You also use options with the **vpngroup** command to enable various Easy VPN features such as SUA, IUA, and backup servers, as described in the “Using the PIX Firewall as an Easy VPN Server” section on page 8-1.



## Note

For step-by-step procedures using the **vpngroup** command to implement Easy VPN Remote devices in different scenarios, refer to the examples later in this chapter.

Table 8-1 summarizes the required and optional parameters used when configuring IKE Mode Config.

**Table 8-1 Required and Optional IKE Mode Config Parameters**

Option	Description	Usage
<b>address-pool</b> <i>poolname</i>	Pool of local addresses to be assigned to the VPN group. Use the <b>ip local range</b> command to identify a range of IP addresses.	Required.
<b>dns-server</b> <i>address</i>	IP address of a DNS server to download to the Cisco Easy VPN Remote device.	Required for network extension mode.
<b>wins-server</b> <i>address</i>	IP address of a WINS server to download to the Cisco Easy VPN Remote device.	Required for network extension mode.
<b>default-domain</b> <i>domain-name</i>	Default domain name to download to the Cisco Easy VPN Remote device.	Required for network extension mode.
<b>split-tunnel</b> <i>access-list</i>	Split tunneling allows both encrypted and clear traffic between the Cisco Easy VPN Remote device and the PIX Firewall.	Optional.
<b>idle-time</b> <i>seconds</i>	Inactivity timeout setting for the Cisco Easy VPN Remote device. The default is 30 minutes.	Optional.

When the Cisco Easy VPN Remote device initiates ISAKMP with the PIX Firewall, the VPN group name and pre-shared key (or certificate) are sent to the PIX Firewall. The PIX Firewall then uses the group name to look up the configured client policy attributes for the given Cisco Easy VPN Remote device and downloads the matching policy attributes to the client during the IKE negotiation.

If you are using a remote client other than a Cisco Easy VPN Remote device, you can still assign IP addresses dynamically, as long as the remote client supports the IKE Mode Config protocol within IPSec. For configuration examples for clients other than Easy VPN Remote devices, refer to [Appendix B, “Configuration Examples for Other Remote Access Clients”](#)

## Using an Easy VPN Remote Device with Pre-Shared Keys

This example shows use of the following supported features:

- Extended Authentication (Xauth) for user authentication
- RADIUS authorization for user services authorization
- IKE Mode Config for VPN IP address assignment
- Wildcard pre-shared key for IKE authentication

This section shows use of eXtended Authentication (Xauth), RADIUS authorization, IKE Mode Config, and a wildcard, pre-shared key for IKE authentication between a PIX Firewall and an Easy VPN Remote software client.



### Note

The PIX Firewall configuration provided in the first section applies to any Easy VPN Remote device. However the last section describes the configuration required for software clients. For configuration instructions when using a PIX Firewall as an Easy VPN Remote device, refer to [“Using PIX Firewall as an Easy VPN Remote Device”](#) in [Chapter 4, “Using PIX Firewall in SOHO Networks.”](#)

This section includes the following topics:

- [Scenario Description, page 8-8](#)
- [Configuring the PIX Firewall, page 8-10](#)
- [Configuring the Easy VPN Remote Software Client, page 8-12](#)

## Scenario Description

With the **vpngroup** command set, you configure the PIX Firewall for a specified group of Cisco Easy VPN Remote devices, using the following parameters:

- Group name for a given group of Cisco Easy VPN Remote devices.
- Pre-shared key or group password used to authenticate your VPN access to the remote server (PIX Firewall).



### Note

This pre-shared key is equivalent to the password entered in the Group Password box of Cisco Easy VPN Remote software clients while configuring the group access information for a connection entry.

- Pool of local addresses to be assigned to the VPN group.
- (Optional) IP address of a DNS server to download to the Cisco Easy VPN Remote device.
- (Optional) IP address of a WINS server to download to the Cisco Easy VPN Remote device.
- (Optional) Default domain name to download to the Cisco Easy VPN Remote device.
- (Optional) Split tunneling enabled on the PIX Firewall allowing both encrypted and clear traffic between the Cisco Easy VPN Remote device and the PIX Firewall.



**Note** If split tunneling is not enabled, all traffic between the Cisco Easy VPN Remote device and the PIX Firewall will be encrypted.

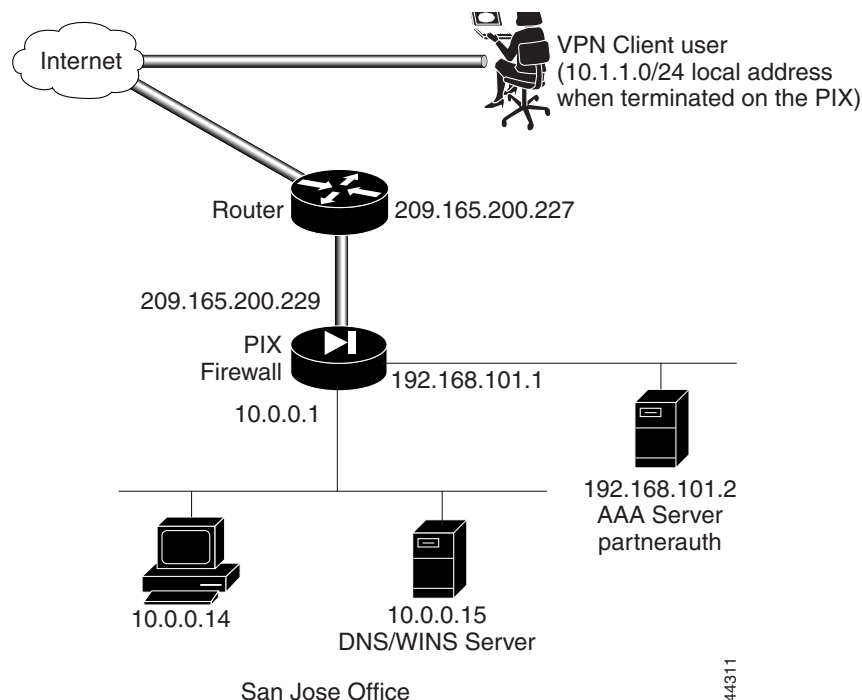
- (Optional) Inactivity timeout setting for the Cisco Easy VPN Remote device. The default is 30 minutes.

On the Cisco Easy VPN Remote device, you would configure the `vpngroup` name and group password to match that which you configured on the PIX Firewall.

When the Cisco Easy VPN Remote device initiates ISAKMP with the PIX Firewall, the VPN group name and pre-shared key are sent to the PIX Firewall. The PIX Firewall then uses the group name to look up the configured client policy attributes for the given Cisco Easy VPN Remote device and downloads the matching policy attributes to the client during the IKE negotiation.

Figure 8-2 illustrates the example network.

**Figure 8-2 Cisco Easy VPN Remote Device Access**



## Configuring the PIX Firewall

Follow these steps to configure the PIX Firewall to interoperate with the Cisco Easy VPN Remote device using Xauth, IKE Mode Config, AAA authorization with RADIUS, and a wildcard, pre-shared key:

**Step 1** Define AAA related parameters:

```
aaa-server radius protocol radius
aaa-server partnerauth protocol radius
aaa-server partnerauth (dmz) host 192.168.101.2 abcdef timeout 5
```

**Step 2** Configure the IKE policy:

```
isakmp enable outside
isakmp policy 8 encr 3des
isakmp policy 8 hash md5
isakmp policy 8 authentication pre-share
```



**Note** To configure the Cisco VPN Client Version 3.x, include the **isakmp policy 8 group 2** command in this step.

**Step 3** Configure a wildcard, pre-shared key:

```
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
```

**Step 4** Configure the pool of local addresses to be assigned to remote VPN clients:

```
ip local pool dealer 10.1.1.1-10.1.1.254
```



**Note** To configure the Cisco VPN 3000 Client Version 2.5, include the **crypto map partner-map client configuration address initiate** command in this step.

**Step 5** Exempt inside hosts from using NAT when communicating with VPN clients:

```
access-list 80 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
nat (inside) 0 access-list 80
```

**Step 6** Create access lists that define the services the VPN clients are authorized to use. The RADIUS server returns this access list ID to enable authorization.

```
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq telnet
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq ftp
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq http
```



**Note** Configure the authentication server with the vendor-specific `acl=acl_ID` identifier to specify the access-list ID. In this example, the access-list ID is 100. The entry in the authentication server would then be `acl=100`.

**Step 7** Configure a transform set that defines how the traffic will be protected:

```
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac
```

**Step 8** Create a dynamic crypto map:

```
crypto dynamic-map cisco 4 set transform-set strong-des
```

Specify which transform sets are allowed for this dynamic crypto map entry.

- Step 9** Add the dynamic crypto map set into a static crypto map set:

```
crypto map partner-map 20 ipsec-isakmp dynamic cisco
```

- Step 10** Apply the crypto map to the outside interface:

```
crypto map partner-map interface outside
```

- Step 11** Enable Xauth:

```
crypto map partner-map client authentication partnerauth
```

- Step 12** Configure Cisco Easy VPN Remote device policy attributes to download:

```
vpngroup superteam address-pool dealer
vpngroup superteam dns-server 10.0.0.15
vpngroup superteam wins-server 10.0.0.15
vpngroup superteam default-domain example.com
vpngroup superteam split-tunnel 80
vpngroup superteam idle-time 1800
```

The keyword “superteam” is the name of a VPN group. You will enter this VPN group name within an Easy VPN Remote software client as part of the group access information.

- Step 13** Tell PIX Firewall to implicitly permit IPsec traffic:

```
sysopt connection permit-ipsec
```

[Example 8-1](#) provides the complete PIX Firewall configuration.

**Example 8-1** *VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Wildcard Pre-Shared Key*

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SanJose
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 209.165.200.229 255.255.255.224
ip address inside 10.0.0.1 255.255.255.0
ip address dmz 192.168.101.1 255.255.255.0
no failover
failover ip address outside 0.0.0.0
```

```

failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
arp timeout 14400
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-list 80 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq telnet
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq ftp
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq http
nat (inside) 0 access-list 80
global (outside) 1 209.165.200.45-209.165.200.50 netmask 255.255.255.224
route outside 0.0.0.0 0.0.0.0 209.165.200.227 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
ip local pool dealer 10.1.1.1-10.1.1.254
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partnerauth protocol tacacs+
aaa-server partnerauth (dmz) host 192.168.101.2 abcdef timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
crypto map partner-map client configuration address initiate;
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac
crypto dynamic-map cisco 4 set transform-set strong-des
crypto map partner-map 20 ipsec-isakmp dynamic cisco
crypto map partner-map client authentication partnerauth
crypto map partner-map interface outside
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
isakmp enable outside
isakmp policy 8 authentication pre-share
isakmp policy 8 encryption 3des
isakmp policy 8 hash md5
isakmp policy 8 group 2
vpngroup superteam address-pool dealer
vpngroup superteam dns-server 10.0.0.15
vpngroup superteam wins-server 10.0.0.15
vpngroup superteam default-domain example.com
vpngroup superteam split-tunnel 80
vpngroup superteam idle-time 1800
sysopt connection permit-ipsec
telnet timeout 5
terminal width 80

```

**Note**

The **crypto map partner-map client configuration address initiate** command is only required to configure the Cisco VPN 3000 Client Version 2.5. The **isakmp policy 8 group 2** command is only required to configure the Cisco VPN Client Version 3.x.

## Configuring the Easy VPN Remote Software Client

This section describes how to configure an Easy VPN Remote software client to match the configurations in “[Configuring the PIX Firewall](#).” It is assumed the Easy VPN Remote software client is already installed on your system and is configured for general use. You can find the Easy VPN Remote software client documentation online at the following website:

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm>

To allow the Easy VPN Remote software client to gain VPN access to the PIX Firewall using a pre-shared key, create one connection entry for the Easy VPN Remote software client that identifies the following:

- Host name or IP address of the remote server you want to access, which in this case is a PIX Firewall
- Name of the VPN group you belong to
- Pre-shared key or password of the VPN group you belong to

Refer to the *VPN Client User Guide* for the detailed steps to configure the Easy VPN Remote software client.

## Using an Easy VPN Remote Device with Digital Certificates

This example shows use of the following supported features:

- Extended Authentication (Xauth) for user authentication
- IKE Mode Config for VPN IP address assignment
- Digital certificates for IKE authentication

This section shows use of Xauth, IKE Mode Config, and digital certificates for IKE authentication between a PIX Firewall and an Easy VPN Remote software client.



### Note

The PIX Firewall configuration provided in the first section applies to any Easy VPN Remote device. However, the last section describes the configuration required for software clients. For configuration instructions when using a PIX Firewall as an Easy VPN Remote device, refer to the [“Using PIX Firewall as an Easy VPN Remote Device”](#) section on page 4-1.

This section includes the following topics:

- [Client Verification of the Easy VPN Server Certificate, page 8-13](#)
- [Scenario Description, page 8-14](#)
- [Configuring the PIX Firewall, page 8-15](#)
- [Configuring the Easy VPN Remote Software Client, page 8-19](#)



### Note

Both the PIX Firewall and the Easy VPN Remote device must obtain digital certificates from the same CA server so that both are certified by the same root CA server. The PIX Firewall only supports use of one root CA server per VPN peer.

## Client Verification of the Easy VPN Server Certificate

PIX Firewall Version 6.3 introduces a method for verifying the distinguished name (DN) of the Easy VPN Server during ISAKMP negotiation. If the DN of the certificate received by the Easy VPN Remote device does not match, the negotiation fails. We recommend using this feature to prevent a “man-in-the-middle” attack. To identify the DN of the PIX Firewall on a PIX Firewall used as an Easy VPN hardware client, refer to [“Verifying the DN of an Easy VPN Server”](#) section on page 4-11.

To identify the DN of the PIX Firewall on an Easy VPN software client, create a .pcf file and use the CertSubjectName keyword. On the line following the CertSubjectName keyword, enter the following parameter:

```
VerifyCertDn=x500 string
```

For example, consider the following entry:

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

This entry causes the receiving Easy VPN software client to accept certificates with a DN having the following attributes:

- Common name (CN) contains the string *myvpn*
- Organizational unit (OU) equals *myou*
- Organization (O) equals *myorg*
- State (ST) equals *CA*
- Country (C) equals *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.


**Note**


---

The verification of the DN fails unless every attribute matches exactly.

---

For details about using a .pcf file for creating a connection profile for an Easy VPN software client, refer to the VPN Client Administrator Guide.

## Scenario Description

For example purposes, the PIX Firewall is shown to interoperate with the Entrust CA server. The specific CA-related commands you enter depend on the CA you are using.


**Note**


---

The PIX Firewall supports CA servers developed by VeriSign, Entrust, Baltimore Technologies, and Microsoft. See [“Using Certification Authorities”](#) in [Chapter 6, “Configuring IPSec and Certification Authorities,”](#) for general configuration procedures. See [Chapter 7, “Site-to-Site VPN Configuration Examples,”](#) for examples showing how to interoperate with different PIX Firewall-supported CA servers.

---

On the PIX Firewall, configure the unit to interoperate with the CA server to obtain a digital certificate. With the **vpngroup** command set, configure the PIX Firewall for a specified group of Easy VPN Remote devices, using the following parameters:

- Pool of local addresses to be assigned to the VPN group
- (Optional) IP address of a DNS server to download to the Easy VPN Remote device
- (Optional) IP address of a WINS server to download to the Easy VPN Remote device
- (Optional) Default domain name to download to the Easy VPN Remote device

- (Optional) Split tunneling on the PIX Firewall, which allows both encrypted and clear traffic between the Easy VPN Remote device and the PIX Firewall.



**Note** If split tunnelling is not enabled, all traffic between the Easy VPN Remote device and the PIX Firewall will be encrypted.

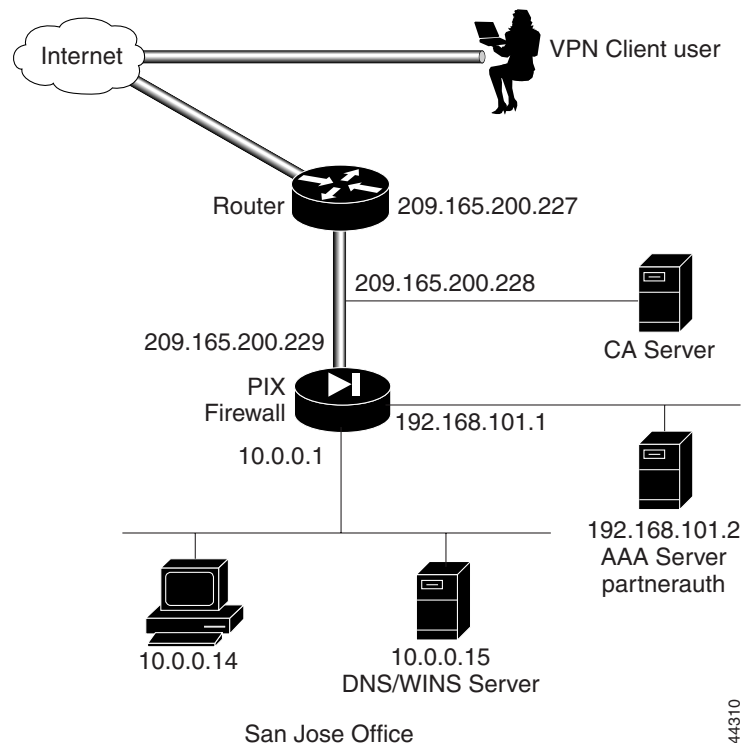
- (Optional) Inactivity timeout for the Easy VPN Remote device. The default is 30 minutes.

On the Easy VPN Remote device, configure the client to obtain a digital certificate. After obtaining the certificate, set the Easy VPN Remote software client connection entry to use the digital certificate.

When the Easy VPN Remote device initiates ISAKMP with the PIX Firewall, the digital certificate is sent to the PIX Firewall. The PIX Firewall uses the digital certificate to look up the configured client policy attributes for the given Easy VPN Remote device and downloads the matching policy attributes to the client during the IKE negotiation.

Figure 8-3 illustrates the example network.

**Figure 8-3 Easy VPN Remote Software Client Access**



## Configuring the PIX Firewall

Follow these steps to configure the PIX Firewall to interoperate with the Easy VPN Remote device:

- Step 1** Define AAA related parameters:
- ```
aaa-server TACACS+ protocol tacacs+
```

```
aaa-server partnerauth protocol tacacs+
aaa-server partnerauth (dmz) host 192.168.101.2 abcdef timeout 5
```

**Step 2** Define a host name:

```
hostname SanJose
```

**Step 3** Define the domain name:

```
domain-name example.com
```

**Step 4** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 5** Declare a CA:

```
ca identity abcd 209.165.200.228 209.165.200.228
```

This command is stored in the configuration.

**Step 6** Configure the parameters of communication between the PIX Firewall and the CA:

```
ca configure abcd ra 1 20 crloptional
```

This command is stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

**Step 7** Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration:

**Step 8** Request signed certificates from your CA for your PIX Firewall's RSA key pair:

```
ca enroll abcd cisco
```

Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate(s):

“cisco” is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

**Step 9** Verify that the enrollment process was successful using the **show ca certificate** command:

```
show ca certificate
```

**Step 10** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```




---

**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

---

**Step 11** Set the system clock.

The clock must be accurate if you are using certificates. Enter the following command to update the system clock.

```
clock set
```

**Step 12** Configure the IKE policy:

```
isakmp enable outside
isakmp policy 8 encr 3des
isakmp policy 8 hash md5
isakmp policy 8 authentication rsa-sig
```

**Step 13** Create an access list that defines the local network(s) requiring IPsec protection:

```
access-list 90 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

**Step 14** Configure NAT 0:

```
nat (inside) 0 access-list 90
```

**Step 15** Configure a transform set that defines how the traffic will be protected:

```
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac
```

**Step 16** Create a dynamic crypto map. Specify which transform sets are allowed for this dynamic crypto map entry:

```
crypto dynamic-map cisco 4 set transform-set strong-des
```

**Step 17** Add the dynamic crypto map into a static crypto map:

```
crypto map partner-map 20 ipsec-isakmp dynamic cisco
```

**Step 18** Apply the crypto map to the outside interface:

```
crypto map partner-map interface outside
```

**Step 19** Configure the firewall to permit IPsec traffic:

```
sysopt connection permit-ipsec
```

**Step 20** Enable Xauth:

```
crypto map partner-map client authentication partnerauth
```

**Step 21** Configure IKE Mode parameters:

```
ip local pool dealer 10.1.1.1-10.1.1.254
crypto map partner-map client configuration address initiate
```

**Step 22** Configure Easy VPN Remote device policy attributes to download to the Easy VPN Remote device:

```
vpngroup superteam address-pool dealer
vpngroup superteam dns-server 10.0.0.15
vpngroup superteam wins-server 10.0.0.15
vpngroup superteam default-domain example.com
vpngroup superteam split-tunnel access-list 90
vpngroup superteam idle-time 1800
```



**Note**

When configuring the VPN group name, make sure it matches the Organization Unit (OU) field in the Easy VPN Remote device certificate. The PIX Firewall uses the VPN group name to match a given VPN client policy. For example, you would use the VPN group “superteam” if the OU field is “superteam.”

[Example 8-2](#) shows the command listing. PIX Firewall default configuration and certain CA commands do not appear in configuration listings.

**Example 8-2 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Digital Certificates**

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SanJose
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 209.165.200.229 255.255.255.224
ip address inside 10.0.0.1 255.255.255.0
ip address dmz 192.168.101.1 255.255.255.0
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
arp timeout 14400
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-list 90 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq telnet
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq ftp
access-list 100 permit tcp 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 eq http
nat (inside) 0 access-list 90
global (outside) 1 209.165.200.45-209.165.200.50 netmask 255.255.255.224
route outside 0.0.0.0 0.0.0.0 209.165.200.227 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
ip local pool dealer 10.1.1.1-10.1.1.254
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partnerauth protocol tacacs+
aaa-server partnerauth (dmz) host 192.168.101.2 abcdef timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac
crypto dynamic-map cisco 4 set transform-set strong-des
crypto map partner-map 20 ipsec-isakmp dynamic cisco
crypto map partner-map client authentication partnerauth
crypto map partner-map interface outside
isakmp enable outside
isakmp policy 8 encryption 3des
isakmp policy 8 hash md5
isakmp policy 8 authentication rsa-sig
vpngroup superteam address-pool dealer
vpngroup superteam dns-server 10.0.0.15

```

```
vpngroup superteam wins-server 10.0.0.15
vpngroup superteam default-domain example.com
vpngroup superteam split-tunnel 90
vpngroup superteam idle-time 1800
ca identity abcd 209.165.200.228 209.165.200.228
ca configure abcd ra 1 100 crloptional
sysopt connection permit-ipsec
telnet timeout 5
terminal width 80
```

**Note**

The `crypto map partner-map client configuration address initiate` command is only required to configure the Cisco VPN client Version 2.5.

## Configuring the Easy VPN Remote Software Client

This section describes how to configure the Easy VPN Remote software client to match the configurations in “[Configuring the PIX Firewall](#).” It is assumed the Easy VPN Remote software client is already installed on your system and is configured for general use. You can find the Easy VPN Remote software client documentation online at the following website:

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm>

For the Easy VPN Remote software client to gain VPN access to the PIX Firewall using a digital certificate, obtain a digital certificate from a CA server. Once you have this certificate, create a VPN client connection entry that identifies the following:

- Host name or IP address of the remote server you want to access, which in this case is a PIX Firewall.
- Certificate name. (This should already be installed on your Easy VPN Remote software client.)

This section does not cover how to obtain a digital certificate for the Easy VPN Remote software client. For information about obtaining a certificate for the Easy VPN Remote software client, refer to the chapter “Enrolling and Managing Certificates” within the *VPN Client User Guide*.

To obtain the detailed steps to follow when configuring the Easy VPN Remote software client, refer to the chapter “Configuring and Managing Connection Entries” in the *VPN Client User Guide*.

## Using PPTP for Remote Access

This section describes how to implement the Point-to-Point Tunneling Protocol (PPTP) using the PIX Firewall. It contains the following topics:

- [Overview, page 8-20](#)
- [PPTP Configuration, page 8-20](#)
- [PPTP Configuration Example, page 8-21](#)

## Overview

The firewall provides support for Microsoft PPTP, which is an alternative to IPSec handling for VPN clients. While PPTP is less secure than IPSec, PPTP may be easier in some networks to implement and maintain.

The **vpdn** command implements the PPTP feature for inbound connections between the firewall and a Windows client. Point-to-Point Tunneling Protocol (PPTP) is a Layer 2 tunneling protocol, which lets a remote client use a public IP network to communicate securely with servers at a private corporate network. PPTP tunnels the IP protocol. RFC 2637 describes the PPTP protocol.

Support is provided for only inbound PPTP and only one firewall interface can have the **vpdn** command enabled.

Supported authentication protocols include: PAP, CHAP, and MS-CHAP using external AAA (RADIUS or TACACS+) servers or the firewall local username and password database. Through the PPP IPCP protocol negotiation, the firewall assigns a dynamic internal IP address to the PPTP client allocated from a locally defined IP address pool.

The firewall PPTP VPN supports standard PPP CCP negotiations with Microsoft Point-To-Point Encryption (MPPE) extensions using RSA/RC4 algorithm. MPPE currently supports 40-bit and 128-bit session keys. MPPE generates an initial key during user authentication and refreshes the key regularly. In this release, compression is not supported.

When you specify MPPE, use the MS-CHAP PPP authentication protocol. If you are using an external AAA server, the protocol should be RADIUS and the external RADIUS server should be able to return the Microsoft MSCHAP\_MPPE\_KEY attribute to the firewall in the RADIUS Authentication Accept packet. See RFC 2548, "Microsoft Vendor Specific RADIUS Attributes," for more information on the MSCHAP\_MPPE\_KEY attribute.

Cisco Secure ACS 2.5/2.6 and higher releases support the MS-CHAP/MPPE encryption.

The firewall PPTP VPN has been tested with the following Microsoft Windows products: Windows 95 with DUN1.3, Windows 98, Windows NT 4.0 with SP6, and Windows 2000.



### Note

If you configure the firewall for 128-bit encryption and if a Windows 95 or Windows 98 client does not support 128-bit or greater encryption, then the connection to the firewall is refused. When this occurs, the Windows client moves the dial-up connection menu down to the screen corner while the PPP negotiation is in progress. This gives the appearance that the connection is accepted when it is not. When the PPP negotiation completes, the tunnel terminates and the firewall ends the connection. The Windows client eventually times out and disconnects.

## PPTP Configuration

Use the **vpdn** command with the **sysopt connection permit-pptp** command to allow PPTP traffic to bypass checking of **access-list** command statements.

The **show vpdn** command lists tunnel and session information.

The **clear vpdn** command removes all **vpdn** commands from the configurations and stops all the active PPTP tunnels. The **clear vpdn all** command lets you remove all tunnels, and the **clear vpdn id tunnel\_id** command lets you remove tunnels associated with *tunnel\_id*. (You can view the *tunnel\_id* with the **show vpdn** command.)

The **clear vpdn group** command removes all the **vpdn group** commands from the configuration. The **clear vpdn username** command removes all the **vpdn username** commands from the configuration. The **clear vpdn** command removes all **vpdn** commands from the configuration.

You can troubleshoot PPTP traffic with the **debug ppp** and **debug vpdn** commands.

## PPTP Configuration Example

[Example 8-3](#) shows a simple configuration, which lets a Windows PPTP client dial in without any authentication (not recommended). Refer to the **vpdn** command page in the *Cisco PIX Firewall Command Reference* for more examples and descriptions of the **vpdn** commands and the command syntax.

### Example 8-3 PPTP Configuration Example

```
ip local pool my-addr-pool 10.1.1.1-10.1.1.254
vpdn group 1 accept dialin pptp
vpdn group 1 client configuration address local my-addr-pool
vpdn enable outside
static (inside, outside) 209.165.201.2 192.168.0.2 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.2 eq telnet
access-group acl_out in interface outside
```

The **ip local pool** command specifies the IP addresses assigned to each VPN client as they log in to the network. The Windows client can Telnet to host 192.168.0.2 through the global IP address 209.165.201.2 in the **static** command statement. The **access-list** command statement permits Telnet access to the host.

