



Configuration Examples for Other Remote Access Clients

This appendix describes different scenarios and examples of using PIX Firewall with different remote access clients and configuration options. It includes the following sections:

- [Xauth with RSA Ace/Server and RSA SecurID, page B-1](#)
- [L2TP with IPSec in Transport Mode, page B-8](#)
- [Windows 2000 Client with IPSec and L2TP, page B-11](#)
- [Using Cisco VPN Client Version 1.1, page B-16](#)

Xauth with RSA Ace/Server and RSA SecurID

This section contains the following topics:

- [Terminology, page B-1](#)
- [Introduction, page B-2](#)
- [PIX Firewall Configuration, page B-3](#)
- [SecurID with Cisco VPN Client Version 3.x, page B-4](#)
- [SecurID with Cisco VPN 3000 Client Version 2.5, page B-5](#)
- [SecurID with Cisco Secure VPN Client Version 1.1 \(3DES\), page B-7](#)

Terminology

ACE/Server: AAA server from RSA security.

ACE/Agent: A software program that makes it possible for workstations and third-party devices such as communication servers and firewalls to be clients of an ACE/Server.

RSA SecurID: Provides strong, two-factor authentication using tokens in conjunction with the RSA ACE/Server.

Token: Usually refers to a handheld device, such as an RSA SecurID Standard Card, Key Fob, or Pinpad Card that display a value called tokencode. User password, RSA SecurID Smart Cards, and Software Tokens are token types with individual characteristics. The token is one of the factors in the RSA SecurID authentication system. The other factor is the user's PIN.

Tokencode: The code displayed by the token. The tokencode along with the PIN make up the RSA SecurID authentication system.

PIN: The user's personal identification number.

Two-Factor authentication: The authentication method used by the RSA ACE/Server system in which the user enters a secret PIN (personal identification number) and the current code generated by the user's assigned SecurID token.

PASSCODE: The PIN and the tokencode make up the PASSCODE.

Token Mode: The state the token is in. The token can be Enabled, Disabled, or be in the New PIN Mode, Next Tokencode Mode.

New PIN mode: When the server puts a token in this mode, the user is required to receive or create a new PIN to gain access to an RSA SecurID-protected system.

Next Tokencode mode: When the user attempts authentication with a series of incorrect PASSCODEs, the server puts the token in this mode so that the user, after finally entering the correct code, is prompted for another tokencode before being allowed access.

Pinpads: A SecurID hardware token that allows entering the PIN via a Pinpad and displays the tokencode in an LCD display.

Key Fobs: Another form of SecurID hardware token, that displays the current tokencode.

Software Token: A software token is similar to the Pinpad, which can be installed on the user's machine.

Introduction

The RSA Ace/Server and RSA SecurID combination can be used to provide authentication for the Cisco VPN Client Version 3.x, the Cisco VPN 3000 Client Version 2.5, and the Cisco Secure VPN Client Version 1.1, which are supported by PIX Firewall. SecurID provides a token-based authentication method in the form of Software Tokens, Pinpads, or Key Fobs. The user is assigned a token and uses that value from the token, called the tokencode, for authentication. A PIN is used along with the tokencode to obtain the Passcode.

The different modes that a token can use are:

- Enabled.
- Next Tokencode mode.
- New PIN mode.

The PIN length and type are as defined in the system parameters of the ACE/Server, and some parameters can also be set on a per-user basis. When a token is assigned, it is enabled and is in a New PIN mode. The PIN could be pre-assigned, or the RSA ACE/Server configuration can decide who can create that PIN. The options for PINs are as follows:

- User-created PINs allowed
- User-created PINs required

These options can also be decided on a per-user basis by selecting the appropriate check box on the **Edit User** panel provided by the ACE/Server master database administration tool.

The "User-created PINs allowed" option provides a choice between the system generating the PIN, and then providing it to the user, or the user selecting the PIN.

The "User-created PINs required" option requires the user to select the PIN.

PIX Firewall Configuration

Following is a sample configuration that is necessary for using token-based Xauth by the PIX Firewall for the VPN clients using RSA ACE/Server and RSA SecurID as the AAA server to establish a secure connection.

Step 1 Create a pool of IP addresses for your clients to use:

```
ip local pool mypool 3.3.48.100-3.3.48.200
```

Step 2 Create the RADIUS servers:

```
aaa-server partner-auth protocol radius
aaa-server partner-auth (inside) host 10.100.48.43 MYSECRET timeout 20
```



Note The word “partner-auth” in the **aaa-server** command in Step 2 is a keyword that needs to match the keyword in the following **crypto map** command.

Step 3 Create an ISAKMP policy and define the hash algorithm:

```
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto dynamic-map mydynmap 10 set transform-set myset
crypto map newmap 10 ipsec-isakmp dynamic mydynmap
crypto map newmap client configuration address initiate
crypto map newmap client configuration address respond
crypto map newmap client token authentication partner-auth
```



Note The word “token” in the **crypto map newmap client token authentication partner-auth** command is optional for the Cisco VPN Client Version 3.x, and the Cisco Secure VPN Client Version 1.1.

```
crypto map newmap interface outside
isakmp enable outside
isakmp key mysecretkey address 0.0.0.0 netmask 0.0.0.0
isakmp identity hostname
isakmp client configuration address-pool local mypool outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
```

Step 4 For the Cisco VPN Client Version 3.x, you may need to change the existing IKE/ISAKMP policy or add another policy depending on the requirements, using the following command:

```
isakmp policy policy number vpngroup 2
```

Step 5 For the Cisco VPN 3000 Client Version 2.5 and the Cisco VPN Client Version 3.x, the **vpngroup** command configuration is also required:

```
vpngroup Cisco address-pool mypool
vpngroup Cisco dns-server 10.100.48.44
vpngroup Cisco wins-server 10.100.48.45
vpngroup Cisco default-domain Cisco.com
vpngroup Cisco split-tunnel myaccesslist
vpngroup Cisco password mysecretkey
```

SecurID with Cisco VPN Client Version 3.x

This section describes how to use the Cisco VPN Client Version 3.x in the three token modes. It contains the following topics:

- [Token Enabled, page B-4](#)
- [Next Tokencode Mode, page B-4](#)
- [New PIN Mode, page B-5](#)

Token Enabled

When a connection is being established to the PIX Firewall with the Cisco VPN Client Version 3.x, the user is prompted to enter the username and the password.

Enter the PIN in the **Software Token** dialog box or on the Pinpad, and enter the password in the box indicated for the password entry (see [Figure B-1](#)).

Figure B-1 Software Token Dialog Box—Cisco VPN Client Version 3



Next Tokencode Mode

If the user enters an incorrect password, then the token status is changed to the Next Tokencode mode. In this case, when the user tries to connect the next time, and enters a correct password in the first **Software Token** dialog box, and then another **Software Token** dialog box appears, prompting the user to enter the next tokencode.

New PIN Mode

This mode is seen when the user is first assigned a token and needs to connect before a PIN can be assigned or created by the user (Case 1), or if for some reason the administrator puts the token in the New PIN Mode (Case 2).

Case 1: User has no previous PIN or the PIN has been cleared.

In this case, enter the value that is currently being displayed on the token in the prompt that requests the username and password.

Case 2: User has an existing PIN and needs to change it.

In this case, enter the PIN in the **Software Token** dialog box or on the Pinpad, and use the value thus obtained as the password in the **User Authentication** dialog box that requests the username and password.

The next prompt, in either case, is for the New PIN. If the user is configured for user-created PIN allowed, enter **y** if the user wants the system to generate the PIN. In this case, the system sends the PIN in the next prompt to the client. If **n** is entered, the user is prompted to select the PIN. If the user is configured for user-created PIN required, then the prompt requests that the user select the PIN.

The next prompt requires the user to enter the password using the new PIN. Enter the newly created PIN in the **Software Token** dialog box or Pinpad and use the value thus obtained.

For a system generated PIN:

A **y** should be entered at this point. The server then sends a PIN message to the user. Enter the next tokencode using the new PIN.

The user creates the PIN, or the user is required to create the PIN if the user enters **n** in the prompt that asks whether the system should generate the PIN or when the user is required to create the PIN.

After the PIN is entered, and is accepted by the server, another **Software Token** dialog box appears.

Enter the next tokencode, using the new PIN, in the **Software Token** dialog box.

SecurID with Cisco VPN 3000 Client Version 2.5

This section describes how to use the Cisco VPN 3000 Client Version 2.5 in the three token modes. It includes the following topics:

- [Token Enabled, page B-6](#)
- [Next Tokencode Mode, page B-6](#)
- [New PIN Mode, page B-6](#)

Token Enabled

When a connection is being established to the PIX Firewall, the user is prompted to enter the username and passcode. The client can recognize that a Software Token has been installed on Windows NT systems (provided the Token Software is installed), such that if the PIN is entered, then the passcode is automatically obtained by the client Software Token, and is sent to the AAA server through the PIX Firewall. With a Pinpad, or on operating systems other than Windows NT, the prompt requests a username and passcode. Enter the PIN on the Pinpad or in the **Software Token** dialog box and use the passcode displayed on the token (See [Figure B-2](#)).

Figure B-2 Software Token Dialog Box—Cisco VPN 3000 Client Version 2.5



Next Tokencode Mode

If the user enters an incorrect passcode or PIN, the token status is changed to the Next Tokencode mode. In this case, when the user tries to connect the next time, and enters a correct passcode in the first prompt, another prompt requests the user to enter the next tokencode.

New PIN Mode

This mode is seen when the user is first assigned a token and needs to connect before a PIN can be assigned or created by the user (Case 1), or if, for some reason, the administrator puts the token in the New PIN Mode (Case 2).

Case 1: User has no PIN's previously assigned or the PIN has been cleared.

In this case, enter the value that is currently being displayed in the **SecurID** message box.

Case 2: User has an existing PIN and needs to change it.

In this case, enter the PIN in the **Software Token** dialog box or on the Pinpad and use the value thus obtained as the passcode when prompted for username and passcode. On a Windows NT operating system, enter the username and PIN instead of passcode.

The next prompt, in either case, is for the new PIN. If the user is configured for user-created PIN required, the prompt requests that the user select the PIN.

The prompt following thereafter requires the user to enter the passcode using the new PIN. Use the newly created PIN on the **Software Token** dialog box or on the Pinpad and use the value thus obtained. On a Windows NT operating system, enter the new PIN in the **SecurID New Pin Mode** dialog box.



Note

Only the user-created PIN required option works on the Cisco VPN 3000 Client.

The next prompt requests that the user enter the next tokencode using the new PIN.

SecurID with Cisco Secure VPN Client Version 1.1 (3DES)

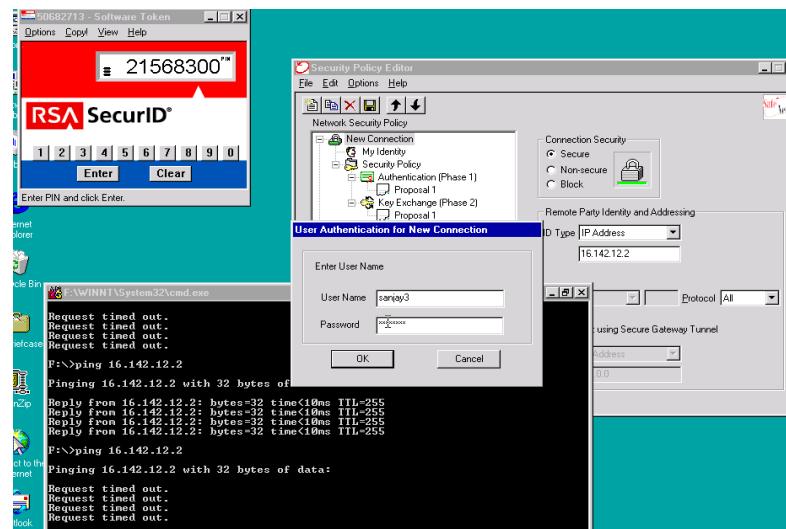
This section provides a reference for using the Cisco Secure VPN Client Version 1.1 in the three token modes. It includes the following topics:

- [Token Enabled, page B-7](#)
- [Next Tokencode Mode, page B-8](#)
- [New PIN Mode, page B-8](#)

Token Enabled

When a connection is being established to the PIX Firewall with the Cisco Secure VPN Client Version 1.1, the user is prompted to enter the username and the password. Enter the PIN in the **Software Token** dialog box or on the Pinpad, and enter the password in the box indicated for the password entry (see [Figure B-3](#)).

Figure B-3 Software Token Dialog Box—Cisco Secure VPN Client Version 1.1



Next Tokencode Mode

If the user enters an incorrect passcode, then the token status is changed to the Next Tokencode mode. In this case, when the user tries to connect the next time, and enters a correct password in the first **Software Token** dialog box, another **Software Token** dialog box appears, prompting the user to enter the next tokencode.

New PIN Mode

This mode is seen when the user is first assigned a token and needs to connect before a PIN can be assigned or created by the user (Case 1), or if for some reason the administrator puts the token in the New PIN Mode (Case 2).

Case 1: User has no PINs previously assigned, or the PIN has been cleared.

In this case, enter the value that is currently being displayed in the **Software Token** dialog box that requests a username and password.

Case 2: User has an existing PIN and needs to change it.

In this case, enter the PIN in the **Software Token** dialog box or on the Pinpad, and use the value thus obtained as the password.

The next prompt, in either case, is for the new PIN. If the user is configured for user-created PIN allowed, enter **y** if the user wants the system to generate the PIN. The system sends the PIN in the next prompt to the client. If **n** is entered, the user is prompted to select the PIN. If the user is configured for user-created PIN required, then the prompt requests the user to select the PIN.

The next prompt requires the user to enter the password using the new PIN. Enter the newly created PIN in the **Software Token** dialog box or on the Pinpad, and use the value thus obtained.

1. For the system generated PIN:

When a **y** is entered, the system sends the PIN and requires the user to use the PIN to enter the next tokencode.

2. The user creates the PIN, or a user-created PIN is required. When **n** is entered in the **Generate PIN** dialog box, or if the user is required to generate the PIN, the **User Authentication for New Connection** dialog box appears.

Once the user enters the PIN and it is accepted by the server, the following **Software Token** dialog box appears. Enter the next tokencode using the new PIN.

L2TP with IPSec in Transport Mode

This section describes how to use IPSec in transport mode to enable L2TP. It includes the following topics:

- [L2TP Overview, page B-9](#)
- [IPSec Transport and Tunnel Modes, page B-9](#)
- [Configuring L2TP with IPSec in Transport Mode, page B-10](#)

For an L2TP configuration example, see “[Xauth with RSA Ace/Server and RSA SecurID.](#)”

L2TP Overview

Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol which allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP protocol is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft Windows 2000.

PIX Firewall with L2TP/IPSec support provides the capability to deploy and administer an L2TP VPN solution alongside the IPSec VPN and PIX Firewall services in a single platform. To implement L2TP, perform the following steps:

1. Configure IPSec transport mode to enable IPSec with L2TP.
2. Configure L2TP with a virtual private dial-up network VPDN group.

The primary benefit of configuring L2TP with IPSec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, enabling remote access from virtually anywhere with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required.

The configuration of L2TP with IPSec supports certificates using the pre-shared keys or RSA signature methods, and the use of dynamic (as opposed to static) crypto maps. This summary of tasks assumes completion of IKE, as well as pre-shared keys or RSA signature configuration. See [“Xauth with RSA Ace/Server and RSA SecurID”](#) for the steps to configure pre-shared keys, RSA, and dynamic crypto maps.

**Note**

L2TP with IPSec, as introduced with PIX Firewall Version 6.0, allows the L2TP LNS to interoperate with the Windows 2000 L2TP client. Interoperability with LACs from Cisco and other vendors is currently not supported. Only L2TP with IPSec is supported, native L2TP itself is not supported on PIX Firewall.

If the PIX Firewall IPSec lifetime is set to less than 300 seconds, then the Windows 2000 client ignores it and replaces it with a 300 second lifetime because the minimum IPSec lifetime supported by the Windows 2000 client is 300 seconds.

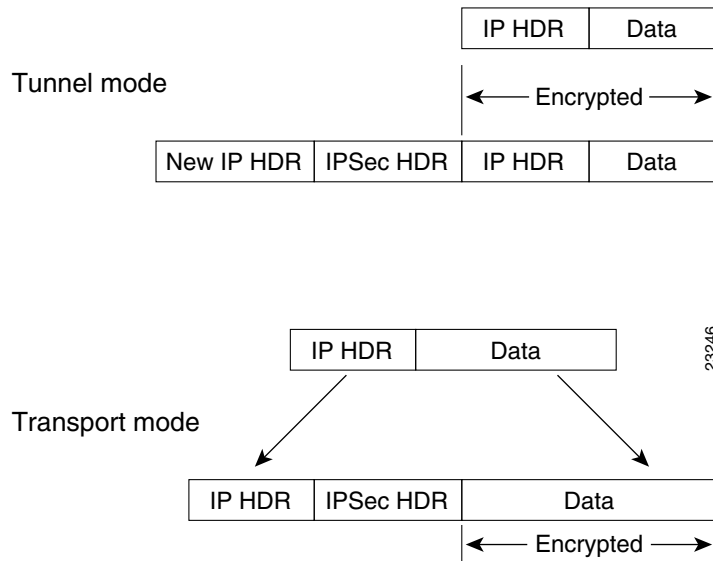
IPSec Transport and Tunnel Modes

IPSec can be configured in tunnel mode or transport mode. In IPSec tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPSec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPSec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

In IPSec transport mode, only the IP payload is encrypted, and the original IP headers are left intact. (See [Figure B-4](#).) This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. With this capability, you can enable special processing (for example, QoS) on the intermediate network based on the

information in the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, transmitting the IP header in clear text, transport mode allows an attacker to perform some traffic analysis.

Figure B-4 IPSec in Tunnel and Transport Modes



Windows 2000 uses IPsec transport mode when tunneling L2TP data. Transport mode should be configured on the PIX Firewall to receive the L2TP IPsec transport mode data from a Windows 2000 client.

Configuring L2TP with IPsec in Transport Mode

To configure L2TP with IPsec in transport mode, perform the following steps:

-
- Step 1** Specify IPsec to use transport mode rather than tunnel mode:

```
crypto ipsec transform-set trans_name mode transport
```
 - Step 2** Allow L2TP traffic to bypass conduit/access list checking:

```
sysopt connection permit-ipsec
sysopt connection permit-l2tp
```
 - Step 3** Instruct the PIX Firewall to accept L2TP dial-in requests:

```
vpdn group group_name accept dial-in l2tp
```
 - Step 4** Specify PPP protocol and authentication protocol (PAP, CHAP, or MS-CHAP):

```
vpdn group group_name ppp authentication pap/chap/mschap
```
 - Step 5** Specify the local address pool used to allocate the IP address to the client:

```
vpdn group group_name client configuration address local address_pool_name
```
 - Step 6** (Optional) Instruct the PIX Firewall to send DNS server IP addresses to the client:

```
vpdn group group_name client configuration dns dns_server_ip1 dns_server_ip2
```

- Step 7** (Optional) Instruct the PIX Firewall to send WINS server IP addresses to the client:
- ```
vpdn group group_name client configuration wins wins_server_ip1 wins_server_ip2
```
- Step 8** Specify authentication using the PIX Firewall local username/password database. If set to aaa, authenticate using the AAA server.
- ```
vpdn group group_name client authentication aaa aaa_server_tag  
or  
vpdn group group_name client authentication local
```
- Step 9** (Optional) Generate a AAA accounting start and stop record for an L2TP (and PPTP) session:
- ```
vpdn group group_name client accounting aaa_server_tag
```
- Step 10** If local authentication is used, the following command specifies username/password entries:
- ```
vpdn username username password password
```
- Step 11** (Optional) Specify the L2TP keep-alive/hello timeout value:
- ```
vpdn group_name l2tp tunnel hello hello timeout
```
- The default timeout value is 60, and the lower and upper limits are 10 and 300, respectively.
- Step 12** Enable **vpdn** function on a PIX Firewall interface:
- ```
vpdn enable ifname
```
-

Windows 2000 Client with IPSec and L2TP

This section provides an example of how to configure the PIX Firewall for interoperability with a Windows 2000 client. It includes the following topics:

- [Overview, page B-12](#)
- [Configuring the PIX Firewall, page B-12](#)
- [Enabling IPSec Debug, page B-15](#)
- [Getting Additional Information, page B-15](#)



Note

The PIX Firewall will not establish an L2TP/IPSec tunnel with a Windows 2000 client if either the Cisco VPN Client or the Cisco VPN 3000 Client Version 2.5 is installed. To work around this problem, disable the “Cisco Systems, Inc.VPN Service” from the Services panel in Windows 2000. To open the Services panel, click **Start>Programs>Administrative Tools>Services**. Then restart the “IPSec Policy Agent Service” from the Services panel, and reboot the machine.

Overview

The example shows the use of IPSec with L2TP, which requires that IPSec be configured in transport mode. For detailed command reference information, refer to the *Cisco PIX Firewall Command Reference*.



Note

For information on configuring the PIX Firewall for RSA signatures or pre-shared keys as the authentication method, refer to the **isakmp** command in page within the *Cisco PIX Firewall Command Reference*. For information on obtaining certificates for RSA signature authentication from a CA, refer to “[Using Certification Authorities](#)” in [Chapter 6, “Configuring IPSec and Certification Authorities.”](#)”

Configuring the PIX Firewall

In this example, PIX Firewall uses PAP and AAA authentication. No conduits/access lists are included, because the **sysopt connection permit-l2tp** option, which permits L2TP traffic, is set in Step 23.

Follow these steps to configure the PIX Firewall to interoperate with the Windows 2000 client:

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
```



Note

Steps 2-10 use RSA signatures as the authentication method for ISAKMP negotiation. If you want to use pre-shared keys as the authentication method, skip Steps 2-10 and configure the following: **isakmp my secretkey address 0.0.0.0 netmask 0.0.0.0** and **isakmp policy 1 authentication pre-share**.

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
```

The second address is configured if LDAP is used by that CA server. 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 must 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 Configure the IKE policy:

```
isakmp policy 1 authentication rsa-sig
isakmp policy 1 encryption des
isakmp policy 1 hash sha
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
```



Note Always configure the IKE lifetime on PIX Firewall for the same or more time than the IKE lifetime configured on the Windows 2000 L2TP/IPSec client, or the IKE negotiation will fail (CSCdt 48570).

Step 12 Configure ISAKMP identity:

```
isakmp identity hostname
```

Step 13 Enable ISAKMP on the outside interface:

```
isakmp enable outside
```

Step 14 Create an access list that defines the PIX Firewall 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 15 Bind the access list to NAT 0:

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

Step 16 Configure a transform set that defines how the traffic will be protected:

```
crypto ipsec transform-set basic esp-des esp-md5-hmac
crypto ipsec transform-set basic mode transport
```



Note The Windows 2000 L2TP/IPSec client uses IPSec transport mode, so transport mode should be selected on the transform set.

Step 17 Create a dynamic crypto map, and specify which transform sets are allowed for this dynamic crypto map entry:

```
crypto dynamic-map cisco 4 set transform-set basic
```



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

Step 18 Add the dynamic crypto map into a static crypto map:

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

Step 19 Apply the crypto map to the outside interface:

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

Step 20 Configure the IP local pool:

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

Step 21 Configure the VPDN group for L2TP:

```
vpdn group 1 accept dialin l2tp
vpdn group 1 ppp authentication pap
vpdn group 1 client configuration address local dealer
vpdn group 1 client configuration dns 10.0.0.15
vpdn group 1 client configuration wins 10.0.0.16
vpdn group 1 client authentication aaa partnerauth
```



Note The AAA server used for accounting does not need to be the same server as the AAA authentication server.

```
vpdn group 1 l2tp tunnel hello
```

Step 22 Enable the VPDN function on the outside interface of the PIX Firewall:

```
vpdn enable outside
```

Step 23 Configure the PIX Firewall to implicitly permit L2TP traffic and bypass conduit/access list checking:

```
sysopt connection permit-l2tp
```

Step 24 (Optional) If AAA authentication is not required, local authentication can be used by configuring the username and password on the PIX Firewall:

```
vpdn username user1 password test1
```

Step 25 The following debug commands (some of which can only be used from the console) can be used for troubleshooting:

```
debug cry isa
debug cry ipsec
debug cry ca
debug vpdn packet
debug vpdn event
debug vpdn error
debug ppp error
debug ppp negotiation
```

Step 26 Verify/display tunnel configuration:

```
show vpdn tunnel
```

**Note**

The PIX Firewall does not establish an L2TP/IPSec tunnel with Windows 2000 if either the Cisco VPN Client Version 3.x or the Cisco VPN 3000 Client Version 2.5 is installed. Disable the *Cisco VPN Service* for the Cisco VPN Client Version 3.x, or the *ANetIKE Service* for the Cisco VPN 3000 Client Version 2.5 from the Services panel in Windows 2000 (click **Start>Programs>Administrative Tools>Services**). Then restart the IPSec Policy Agent Service from the **Services** panel, and reboot the machine.

Enabling IPSec Debug

IPSec debug information can be added to a Windows 2000 client by adding the following registry:

-
- Step 1** Run the Windows 2000 registry editor: REGEDIT.
- Step 2** Locate the following registry entry:
MyComputer\HKEY_LOCAL_MACHINE\CurrentControlSet\Services\PolicyAgent
- Step 3** Create the key by entering **oakley**.
- Step 4** Create the DWORD by entering **EnableLogging**.
- Step 5** Set the “EnableLogging” value to “1”.
- Step 6** Stop and Start the IPSec Policy Agent (click **Start>Programs>Administrative Tools>Services**). The debug file will be found at “%windir%\debug\oakley.log”.
-

Getting Additional Information

Additional information on various topics can be found at www.microsoft.com:

<http://support.microsoft.com/support/kb/articles/Q240/2/62.ASP>

How to Configure an L2TP/IPSec Connection Using Pre-Shared Keys Authentication:

<http://support.microsoft.com/support/kb/articles/Q253/4/98.ASP>

How to Install a Certificate for Use with IP Security (IPSec):

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/sag_VPN_us26.htm

How to use a Windows 2000 Machine Certificate for L2TP over IPSec VPN Connections:

<http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp#heading3>

How to Create a Custom MMC Console and Enabling Audit Policy for Your Computer:

<http://support.microsoft.com/support/kb/articles/Q259/3/35.ASP>

Using Cisco VPN Client Version 1.1

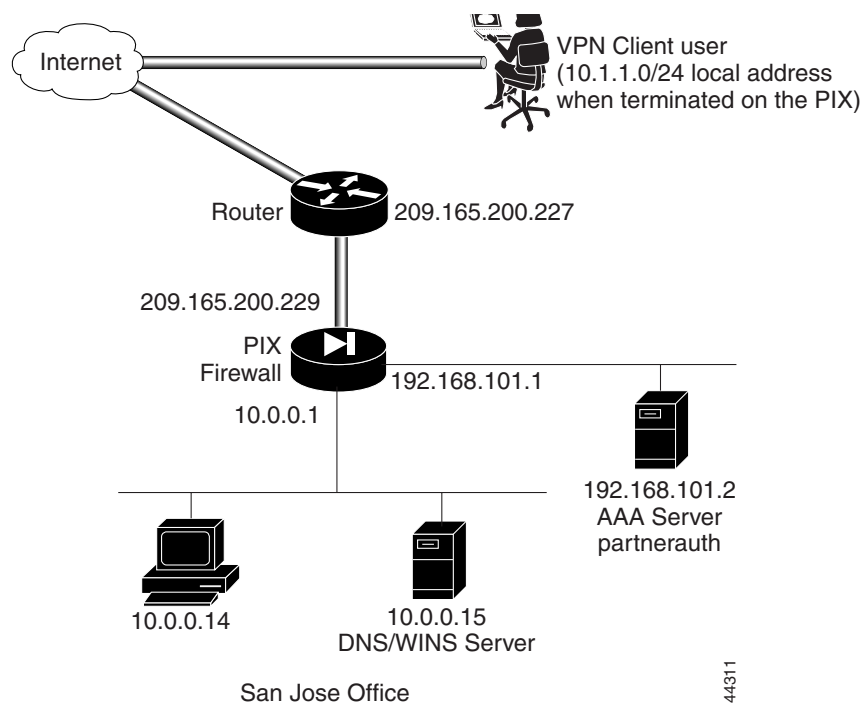
The example in this section shows use of Extended Authentication (Xauth), IKE Mode Config and a wildcard, pre-shared key for IKE authentication between a PIX Firewall and a Cisco Secure VPN Client, Version 1.1.

This section includes the following topics:

- [Configuring the PIX Firewall, page B-17](#)
- [Configuring the Cisco Secure VPN Client Version 1.1, page B-19](#)

Figure B-5 illustrates the example network.

Figure B-5 VPN Client Access



44311

Configuring the PIX Firewall

Follow these steps to configure the PIX Firewall to interoperate with the Cisco Secure VPN Client:

-
- 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** Configure the IKE policy:
- ```
isakmp enable outside
isakmp policy 8 encr 3des
isakmp policy 8 hash md5
isakmp policy 8 authentication pre-share
```
- Step 3** Configure a wildcard, pre-shared key:
- ```
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
```
- Step 4** Create access lists that define the virtual IP addresses for VPN clients:
- ```
access-list 80 permit ip host 10.0.0.14 host 192.168.15.1
access-list 80 permit ip host 10.0.0.14 host 192.168.15.2
access-list 80 permit ip host 10.0.0.14 host 192.168.15.3
access-list 80 permit ip host 10.0.0.14 host 192.168.15.4
access-list 80 permit ip host 10.0.0.14 host 192.168.15.5
```
- Step 5** Configure NAT 0:
- ```
nat 0 access-list 80
```
- Step 6** Configure a transform set that defines how the traffic will be protected:
- ```
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac
```
- Step 7** 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 8** Add the dynamic crypto map into a static crypto map:
- ```
crypto map partner-map 20 ipsec-isakmp dynamic cisco
```
- Step 9** Apply the crypto map to the outside interface:
- ```
crypto map partner-map interface outside
```
- Step 10** Enable Xauth:
- ```
crypto map partner-map client authentication partnerauth
```
- Step 11** Configure IKE Mode Config related parameters:
- ```
ip local pool dealer 192.168.15.1-192.168.15.5
isakmp client configuration address-pool local dealer outside
crypto map partner-map client configuration address initiate
```

**Step 12** Tell PIX Firewall to implicitly permit IPsec traffic:

```
sysopt connection permit-ipsec
```

---

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

**Example B-1 PIX Firewall with VPN Client and Manual IP Address**

```
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 host 10.0.0.14 host 192.168.15.1
access-list 80 permit ip host 10.0.0.14 host 192.168.15.2
access-list 80 permit ip host 10.0.0.14 host 192.168.15.3
access-list 80 permit ip host 10.0.0.14 host 192.168.15.4
access-list 80 permit ip host 10.0.0.14 host 192.168.15.5
nat 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 192.168.15.1-192.168.15.5
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
isakmp client configuration address-pool local dealer outside
```

```

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
sysopt connection permit-ipsec
telnet timeout 5
terminal width 80

```

## Configuring the Cisco Secure VPN Client Version 1.1

This section describes how to configure the Cisco Secure VPN Client for use with the PIX Firewall. Refer to the *Release Notes for the Cisco Secure VPN Client Version 1.1* or higher for the most current information. Before performing the information in this section, install the VPN client as described in the Cisco Secure VPN Client release notes. You can find the Cisco Secure VPN Client release notes online at the following website:

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

Follow these steps to configure the Cisco Secure VPN Client Version 1.1:

- 
- Step 1** Click **Start>Programs>Cisco Secure VPN Client>Security Policy Editor**.
  - Step 2** Click **Options>Secure>Specified Connections**.
  - Step 3** In the Network Security Policy window, click **Other Connection** and then click **Non-Secure** in the panel on the right.
  - Step 4** Click **File>New Connection**. Rename New Connection. For example, **ToSanJose**.
  - Step 5** Under **Connection Security**, click **Secure**.
  - Step 6** Under **Remote Party Identity and Addressing**, set the following preferences in the panel on the right:
    - a. ID Type—Click **IP address**.
    - b. Enter the IP address of the internal host within the PIX Firewall unit's internal network to which the VPN client will have access. Enter **10.0.0.14**.
    - c. Click **Connect using Secure Gateway Tunnel**.
    - d. ID Type—Click **IP address**.
    - e. Enter the IP address of the outside interface of the PIX Firewall. Enter **209.165.200.229**.
  - Step 7** In the Network Security Policy window, click the plus sign beside the ToSanJose entry to expand the selection, and click **My Identity**. Set the following preferences in the panel on the right:
    - a. Select Certificate—Click **None**.
    - b. ID Type—Click **IP address**.
    - c. Port—Click **All**.
    - d. Local Network Interface—Click **Any**.
    - e. Click **Pre-Shared Key**. When the Pre-Shared Key dialog box appears, click **Enter Key** to make the key box editable. Enter **cisco1234** and click **OK**.

- Step 8** In the Network Security Policy window, expand Security Policy and set the following preferences in the panel on the right:
- Under **Select Phase 1 Negotiation Mode**, click **Main Mode**.
  - Select the **Enable Replay Detection** check box.
- Leave any other values as they were in the panel.
- Step 9** Click **Security Policy>Authentication (Phase 1)>Proposal 1** and set the following preferences in the panel on the right:
- Authentication Method—Click **Pre-shared Key**.
  - Encrypt Alg—Click **Triple DES**.
  - Hash Alg—Click **MD5**.
  - SA Life—Click **Unspecified** to accept the default values.
  - Key Group—Click **Diffie-Hellman Group 1**.
- Step 10** Click **Security Policy>Key Exchange (Phase 2)>Proposal 1** and select the following values in the panel on the right:
- Select the **Encapsulation Protocol (ESP)** check box.
  - Encryption Alg—Click **Triple DES**.
  - Hash Alg—Click **SHA-1**.
  - Encapsulation—Click **Tunnel**.
- Step 11** Click **File>Save Changes**.
- The VPN client is now activated.
- 

You can view connection process by right-clicking the SafeNet/Soft-PK icon on the Windows taskbar. Unless the taskbar is changed, this icon appears in lower right of the screen. Click **Log Viewer** to display the View Log feature.

[Example B-2](#) shows a typical View Log session.

#### **Example B-2 View Log Session**

```
time_stamp ToSanJose - Deleting IKE SA
time_stamp ToSanJose - SENDING>>>>ISAKMP OAK QM *(HASH, SA, NON, ID, ID)
time_stamp ToSanJose - RECEIVED<<<ISAKMP OAK TRANS *(HASH, ATTR)
time_stamp ToSanJose - Received Private IP Address = 192.168.15.3
time_stamp ToSanJose - SENDING>>>>ISAKMP OAK TRANS *(HASH, ATTR)
time_stamp ToSanJose - RECEIVED<<<ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME)
time_stamp ToSanJose - SENDING>>>> ISAKMP OAK QM *(HASH)
time_stamp ToSanJose - Loading IPsec SA keys...
time_stamp
```

## Making an Exception to Xauth for a Site-to-Site VPN Peer

If you have both a site-to-site VPN peer and VPN client peers terminating on the same interface, and have the Xauth feature configured, configure the PIX Firewall to make an exception to this feature for the site-to-site VPN peer. With this exception, the PIX Firewall will not challenge the site-to-site peer for a username and password. The command that you employ to make an exception to the Xauth feature depends on the authentication method you are using within your IKE policies.

Table B-1 summarizes the guidelines to follow.

**Table B-1** Configuring no-xauth

| IKE Authentication Method | no-xauth Related Command to Use                                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pre-shared key            | <b>isakmp key</b> <i>keystring</i> <b>address</b> <i>ip-address</i> [ <i>netmask</i> ] [ <b>no-xauth</b> ] [ <b>no-config-mode</b> ]<br>See the <b>isakmp</b> command page within the <i>Cisco PIX Firewall Command Reference</i> for more information. |
| rsa signatures            | <b>isakmp peer fqdn</b> <i>fqdn</i> [ <b>no-xauth</b> ] [ <b>no-config-mode</b> ]<br>See the <b>isakmp</b> command page within the <i>Cisco PIX Firewall Command Reference</i> for more information.                                                    |

## Making an Exception to IKE Mode Config for Site-to-Site VPN Peers

If you have both a site-to-site VPN peer and VPN clients terminating on the same interface, and have the IKE Mode Config feature configured, configure the PIX Firewall to make an exception to this feature for the site-to-site VPN peer. With this exception, the PIX Firewall will not attempt to download an IP address to the peer for dynamic IP address assignment. The command that you employ to bypass the IKE Mode Config feature depends on the authentication method you are using within your IKE policies. See Table B-2 for the guidelines to follow.

**Table B-2** Configuring no-config-mode

| IKE Authentication Method | no-config-mode Related Command to Use                                                                                                                                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pre-shared key            | <b>isakmp key</b> <i>keystring</i> <b>address</b> <i>ip-address</i> [ <i>netmask</i> ] [ <b>no-xauth</b> ] [ <b>no-config-mode</b> ]<br>See the <b>isakmp</b> command page in the <i>Cisco PIX Firewall Command Reference</i> for more information. |
| rsa signatures            | <b>isakmp peer fqdn</b> <i>fqdn</i> [ <b>no-xauth</b> ] [ <b>no-config-mode</b> ]<br>See the <b>isakmp</b> command page in the <i>Cisco PIX Firewall Command Reference</i> for more information.                                                    |

